# Gestire Cloud Volumes ONTAP

## Cloud Manager 3.8

NetApp
March 25, 2024

# Sommario

# Gestire Cloud Volumes ONTAP

## Scopri

### 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. Offre storage di livello Enterprise con le seguenti funzionalità principali:

- 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 Cloud Backup Service per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.

- 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.

- 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 conformità al cloud ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

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"

# Storage

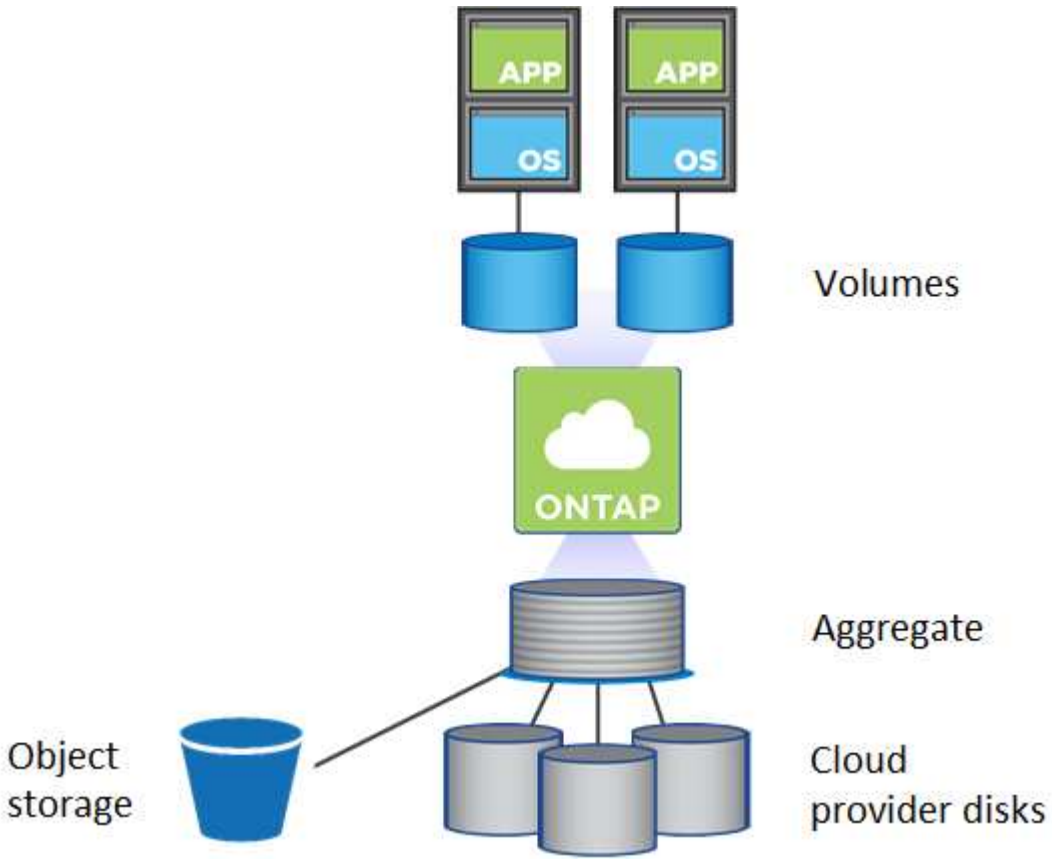
## Dischi e aggregati

Comprendere come Cloud Volumes ONTAP utilizza il cloud storage può aiutarti a comprendere i costi dello storage.

Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da Cloud Manager. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti per i provider di cloud.

### Panoramica

Cloud Volumes ONTAP utilizza lo storage del cloud provider come dischi e li raggruppa in uno o più aggregati. Gli aggregati forniscono storage a uno o più volumi.




Sono supportati diversi tipi di dischi cloud. Quando si crea un volume e si sceglie il tipo di disco e la dimensione predefinita del disco quando si implementa Cloud Volumes ONTAP.

La quantità totale di storage acquistata da un cloud provider è la *capacità raw*. La *capacità utilizzabile* è inferiore perché circa il 12-14% è un overhead riservato all'utilizzo di Cloud Volumes ONTAP. Ad esempio, se Cloud Manager crea un aggregato da 500 GB, la capacità utilizzabile è di 442.94 GB.

#### Storage AWS

In AWS, Cloud Volumes ONTAP utilizza lo storage EBS per i dati dell'utente e lo storage NVMe locale come cache flash su alcuni tipi di istanze EC2.

### Storage EBS

In AWS, un aggregato può contenere fino a 6 dischi delle stesse dimensioni. La dimensione massima del disco è di 16 TB.

Il tipo di disco EBS sottostante può essere SSD General Purpose, SSD IOPS con provisioning, HDD ottimizzato per il throughput o HDD freddo. È possibile associare un disco EBS con Amazon S3 a. "eseguire il tier dei dati inattivi per lo storage a oggetti a basso costo".

Ad un livello elevato, le differenze tra i tipi di dischi EBS sono le seguenti:

- I dischi SSD per uso generico bilanciano costi e performance per un'ampia gamma di carichi di lavoro. Le performance sono definite in termini di IOPS.
- I dischi SSD IOPS con provisioning sono destinati ad applicazioni critiche che richiedono le massime performance a un costo più elevato.
- I dischi HDD_ ottimizzati per il throughput sono per carichi di lavoro con accesso frequente che richiedono un throughput rapido e coerente a un prezzo inferiore.
- I dischi *Cold HDD* sono destinati ai backup o ai dati a cui si accede raramente, perché le performance sono molto basse. Come i dischi HDD ottimizzati per il throughput, le performance sono definite in termini di throughput.

  I dischi rigidi Cold non sono supportati con configurazioni ha e con tiering dei dati.

### Storage NVMe locale

Alcuni tipi di istanze EC2 includono lo storage NVMe locale, utilizzato da Cloud Volumes ONTAP "Flash cache".

### Link correlati

- "Documentazione AWS: Tipi di volume EBS"
- "Scopri come scegliere i tipi di dischi e le dimensioni dei dischi per i tuoi sistemi in AWS"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in AWS"
- "Analisi delle configurazioni supportate per Cloud Volumes ONTAP in AWS"

#### Storage Azure

In Azure, un aggregato può contenere fino a 12 dischi delle stesse dimensioni. Il tipo di disco e le dimensioni massime dipendono dall'utilizzo di un sistema a nodo singolo o di una coppia ha:

### Sistemi a nodo singolo

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.

  Ogni tipo di disco gestito ha una dimensione massima di 32 TB.

  È possibile associare un disco gestito con lo storage Azure Blob a. "eseguire il tier dei dati inattivi per lo storage a oggetti a basso costo".

**Coppie HA**

Le coppie HA utilizzano i blob di pagina Premium, che hanno una dimensione massima del disco di 8 TB.

**Link correlati**

- "Documentazione di Microsoft Azure: Introduzione allo storage Microsoft Azure"
- "Scopri come scegliere i tipi di dischi e le dimensioni dei dischi per i tuoi sistemi in Azure"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in Azure"

#### Storage GCP

In GCP, un aggregato può contenere fino a 6 dischi delle stesse dimensioni. La dimensione massima del disco è di 16 TB.

Il tipo di disco può essere *dischi persistenti SSD Zonal* o *dischi persistenti standard Zonal*. È possibile associare dischi persistenti con un bucket di storage Google a. "eseguire il tier dei dati inattivi per lo storage a oggetti a basso costo".

**Link correlati**

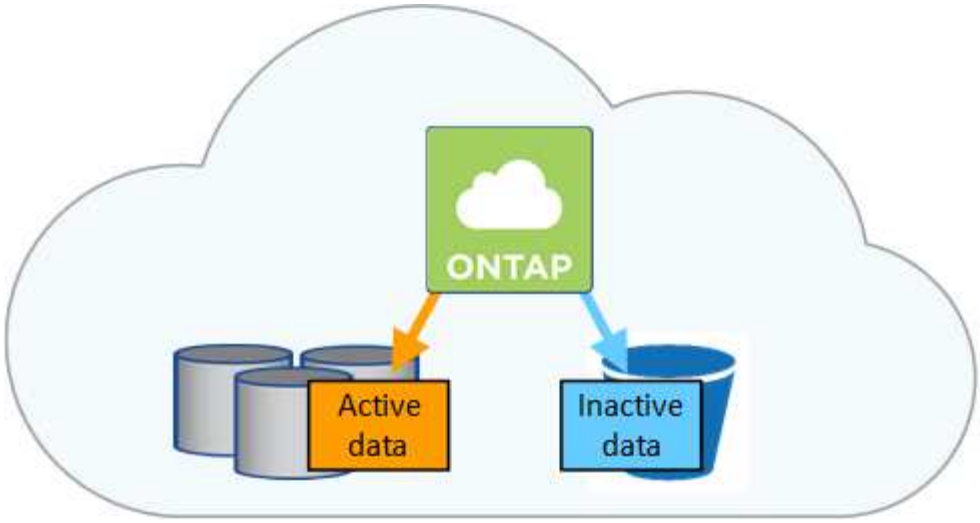
- "Documentazione di Google Cloud Platform: Opzioni di storage"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in GCP"

#### Tipo RAID

Il tipo di RAID per ciascun aggregato Cloud Volumes ONTAP è RAID0 (striping). Non sono supportati altri tipi di RAID. Cloud Volumes ONTAP si affida al cloud provider per la disponibilità e la durata dei dischi.

### Panoramica sul tiering dei dati

Riduci i costi di storage abilitando il tiering automatizzato dei dati inattivi su storage a oggetti a basso costo. I dati attivi rimangono in SSD o HDD ad alte prestazioni, mentre i dati inattivi vengono suddivisi in livelli per lo storage a oggetti a basso costo. In questo modo è possibile recuperare spazio sullo storage primario e ridurre lo storage secondario.




Cloud Volumes ONTAP supporta il tiering dei dati in AWS, Azure e Google Cloud Platform. Il tiering dei dati è basato sulla tecnologia FabricPool.

Non è necessario installare una licenza per le funzionalità per abilitare il tiering dei dati (FabricPool).

#### Tiering dei dati in AWS

Quando si abilita il tiering dei dati in AWS, Cloud Volumes ONTAP utilizza EBS come Tier di performance per i dati hot e AWS S3 come Tier di capacità per i dati inattivi.

**Tier di performance**

Il livello di performance può essere SSD General Purpose, SSD IOPS con provisioning o HDD ottimizzati per il throughput.

**Tier di capacità**

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi su un singolo bucket S3 utilizzando la classe di storage *Standard*. Standard è ideale per i dati ad accesso frequente memorizzati in più zone di disponibilità.

Cloud Manager crea un singolo bucket S3 per ogni ambiente di lavoro e lo nomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket S3 diverso per ciascun volume.

**Classi di storage**

La classe di storage predefinita per i dati Tiered in AWS è *Standard*. Se non si prevede di accedere ai dati inattivi, è possibile ridurre i costi di storage cambiando la classe di storage in una delle seguenti opzioni: *Intelligent Tiering*, *One-zone infrequent Access* o *Standard-infrequent Access*. Quando si modifica la classe di storage, i dati inattivi vengono avviati nella classe di storage Standard e vengono passati alla classe di storage selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi tenere in considerazione questo aspetto prima di modificare la classe di storage. "Scopri di più sulle classi di storage Amazon S3".

È possibile selezionare una classe di storage quando si crea l'ambiente di lavoro e modificarla in qualsiasi momento. Per ulteriori informazioni sulla modifica della classe di storage, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

La classe di storage per il tiering dei dati è estesa a tutto il sistema, non per volume.

#### Tiering dei dati in Azure

Quando abiliti il tiering dei dati in Azure, Cloud Volumes ONTAP utilizza i dischi gestiti da Azure come Tier di performance per i dati hot e lo storage Blob Azure come Tier di capacità per i dati inattivi.

**Tier di performance**

Il Tier di performance può essere SSD o HDD.

**Tier di capacità**

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi in un singolo container blob utilizzando il Tier di storage Azure *hot*. Il Tier hot è ideale per i dati ad accesso frequente.

> Cloud Manager crea un nuovo account storage con un singolo container per ogni ambiente di lavoro Cloud Volumes ONTAP. Il nome dell'account di storage è casuale. Non viene creato un container diverso per ogni volume.

**Tier di accesso allo storage**

Il Tier di accesso allo storage predefinito per i dati a più livelli in Azure è il *hot* Tier. Se non intendi accedere ai dati inattivi, puoi ridurre i costi di storage passando al Tier di storage *COOL*. Quando si modifica il Tier di storage, i dati inattivi vengono avviati nel Tier di storage hot e vengono passati al Tier di storage cool, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi è necessario prendere in considerazione questo aspetto prima di modificare il Tier di storage. "Scopri di più sui Tier di accesso allo storage Azure Blob".

È possibile selezionare un Tier di storage quando si crea l'ambiente di lavoro e modificarlo in qualsiasi momento. Per ulteriori informazioni sulla modifica del Tier di storage, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

Il Tier di accesso allo storage per il tiering dei dati è esteso a tutto il sistema, non per volume.

#### Tiering dei dati in GCP

Quando abiliti il tiering dei dati in GCP, Cloud Volumes ONTAP utilizza i dischi persistenti come Tier di performance per i dati hot e un bucket di storage cloud di Google come Tier di capacità per i dati inattivi.

**Tier di performance**

Il Tier di performance può essere SSD o HDD (dischi standard).

**Tier di capacità**

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi in un singolo bucket di storage cloud di Google utilizzando la classe di storage *regionale*.

> Cloud Manager crea un singolo bucket per ogni ambiente di lavoro e lo nomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket diverso per ogni volume.

**Classi di storage**

La classe di storage predefinita per i dati a più livelli è la classe *Standard Storage*. Se l'accesso ai dati non è frequente, puoi ridurre i costi di storage passando a *Nearline Storage* o *Coldline Storage*. Quando si modifica la classe di storage, i dati inattivi vengono avviati nella classe di storage standard e vengono

passati alla classe di storage selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi tenere in considerazione questo aspetto prima di modificare la classe di storage. "Scopri di più sulle classi di storage per Google Cloud Storage".

È possibile selezionare un Tier di storage quando si crea l'ambiente di lavoro e modificarlo in qualsiasi momento. Per ulteriori informazioni sulla modifica della classe di storage, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

La classe di storage per il tiering dei dati è estesa a tutto il sistema, non per volume.

#### Tiering dei dati e limiti di capacità

Se si abilita il tiering dei dati, il limite di capacità di un sistema rimane invariato. Il limite viene distribuito tra il Tier di performance e il Tier di capacità.

#### Policy di tiering dei volumi

Per attivare il tiering dei dati, è necessario selezionare una policy di tiering dei volumi quando si crea, modifica o replica un volume. È possibile selezionare un criterio diverso per ciascun volume.

Alcuni criteri di tiering hanno un periodo di raffreddamento minimo associato, che imposta il tempo in cui i dati dell'utente in un volume devono rimanere inattivi per essere considerati "freddi" e spostati al livello di capacità.

Cloud Manager consente di scegliere tra le seguenti policy di tiering dei volumi quando si crea o modifica un volume:

**Solo Snapshot**

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei dati cold user delle copie Snapshot non associate al file system attivo al Tier di capacità. Il periodo di raffreddamento è di circa 2 giorni.

In lettura, i blocchi di dati cold sul Tier di capacità diventano hot e vengono spostati sul Tier di performance.

**Tutto**

Tutti i dati (non inclusi i metadati) vengono immediatamente contrassegnati come cold e tiered per lo storage a oggetti il più presto possibile. Non è necessario attendere 48 ore affinché i nuovi blocchi di un volume si raffreddino. Tenere presente che i blocchi situati nel volume prima dell'impostazione del criterio All richiedono 48 ore per diventare freddi.

In caso di lettura, i blocchi di dati cold nel Tier cloud restano freddi e non vengono riscritti nel Tier di performance. Questo criterio è disponibile a partire da ONTAP 9.6.

**Automatico**

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei blocchi di dati cold in un volume fino a raggiungere un livello di capacità. I dati cold non includono solo le copie Snapshot, ma anche i dati cold user dal file system attivo. Il periodo di raffreddamento è di circa 31 giorni.

Questo criterio è supportato a partire da Cloud Volumes ONTAP 9.4.

Se letti in modo casuale, i blocchi di dati cold nel Tier di capacità diventano hot e passano al Tier di performance. Se letti in base a letture sequenziali, come quelle associate a scansioni di indice e antivirus, i blocchi di dati cold rimangono freddi e non passano al livello di performance.

**Nessuno**

Mantiene i dati di un volume nel Tier di performance, evitando che vengano spostati nel Tier di capacità.

Quando si replica un volume, è possibile scegliere se eseguire il Tier dei dati sullo storage a oggetti. In questo caso, Cloud Manager applica il criterio **Backup** al volume di protezione dei dati. A partire da Cloud Volumes ONTAP 9.6, la policy di tiering **all** sostituisce la policy di backup.

### La disattivazione di Cloud Volumes ONTAP influisce sul periodo di raffreddamento

I blocchi di dati vengono raffreddati mediante scansioni di raffreddamento. Durante questo processo, i blocchi che non sono stati utilizzati hanno spostato la temperatura del blocco (raffreddato) al valore successivo più basso. Il tempo di raffreddamento predefinito dipende dalla policy di tiering del volume:

- Auto: 31 giorni
- Solo snapshot: 2 giorni

Affinché la scansione di raffreddamento funzioni, è necessario che Cloud Volumes ONTAP sia in esecuzione. Se Cloud Volumes ONTAP è disattivato, anche il raffreddamento si interrompe. Di conseguenza, potrebbero verificarsi tempi di raffreddamento più lunghi.

#### Impostazione del tiering dei dati

Per istruzioni e un elenco delle configurazioni supportate, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

## Gestione dello storage

Cloud Manager offre una gestione semplificata e avanzata dello storage Cloud Volumes ONTAP.

> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da Cloud Manager. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti per i provider di cloud.

#### Provisioning dello storage

Cloud Manager semplifica il provisioning dello storage per Cloud Volumes ONTAP acquistando dischi e gestendo aggregati per te. È sufficiente creare volumi. Se lo si desidera, è possibile utilizzare un'opzione di allocazione avanzata per eseguire il provisioning degli aggregati.

### Provisioning semplificato

Gli aggregati forniscono lo storage cloud ai volumi. Cloud Manager crea aggregati per te quando avvii un'istanza e quando esegui il provisioning di volumi aggiuntivi.

Quando crei un volume, Cloud Manager esegue una delle tre operazioni seguenti:

- Posiziona il volume su un aggregato esistente con spazio libero sufficiente.
- Il volume viene inserito in un aggregato esistente acquistando più dischi per tale aggregato.
- L'IT acquista dischi per un nuovo aggregato e colloca il volume su tale aggregato.

Cloud Manager determina dove posizionare un nuovo volume prendendo in considerazione diversi fattori: La dimensione massima di un aggregato, l'attivazione del thin provisioning e le soglie di spazio libero per gli aggregati.

L'amministratore dell'account può modificare le soglie di spazio libero dalla pagina **Impostazioni**.

### Selezione delle dimensioni dei dischi per gli aggregati in AWS

Quando Cloud Manager crea nuovi aggregati per Cloud Volumes ONTAP in AWS, aumenta gradualmente la dimensione del disco in un aggregato, con l'aumentare del numero di aggregati nel sistema. Cloud Manager consente di utilizzare la capacità massima del sistema prima che raggiunga il numero massimo di dischi dati consentito da AWS.

Ad esempio, Cloud Manager può scegliere le seguenti dimensioni dei dischi per gli aggregati in un sistema Cloud Volumes ONTAP Premium o BYOL:

| Numero aggregato | Dimensioni del disco | Capacità aggregata massima |
|---|---|---|
| 1 | 500 MB | 3 TB |
| 4 | 1 TB | 6 TB |
| 6 | 2 TB | 12 TB |

È possibile scegliere autonomamente le dimensioni del disco utilizzando l'opzione Advanced allocation (allocazione avanzata).

### Allocazione avanzata

Invece di consentire a Cloud Manager di gestire gli aggregati per te, puoi farlo da solo. "Dalla pagina **allocazione avanzata**", è possibile creare nuovi aggregati che includono un numero specifico di dischi, aggiungere dischi a un aggregato esistente e creare volumi in aggregati specifici.

#### Gestione della capacità

L'account Admin può scegliere se Cloud Manager notifica le decisioni relative alla capacità dello storage o se Cloud Manager gestisce automaticamente i requisiti di capacità per te. Potrebbe essere utile comprendere il funzionamento di queste modalità.

### Gestione automatica della capacità

Per impostazione predefinita, Capacity Management Mode (modalità di gestione della capacità) è impostata su Automatic (automatica). In questa modalità, Cloud Manager acquista automaticamente nuovi dischi per le istanze di Cloud Volumes ONTAP quando è necessaria una maggiore capacità, elimina raccolte di dischi inutilizzate (aggregati), sposta i volumi tra aggregati quando necessario e tenta di eliminare i dischi guasti.

I seguenti esempi illustrano il funzionamento di questa modalità:

- Se un aggregato con 5 o meno dischi EBS raggiunge la soglia di capacità, Cloud Manager acquista automaticamente nuovi dischi per quell'aggregato in modo che i volumi possano continuare a crescere.
- Se un aggregato con 12 dischi Azure raggiunge la soglia di capacità, Cloud Manager sposta automaticamente un volume da tale aggregato a un aggregato con capacità disponibile o a un nuovo aggregato.

Se Cloud Manager crea un nuovo aggregato per il volume, sceglie una dimensione del disco che si adatta alle dimensioni del volume.

Si noti che lo spazio libero è ora disponibile sull'aggregato originale. I volumi esistenti o nuovi volumi possono utilizzare tale spazio. In questo scenario, non è possibile restituire lo spazio ad AWS, Azure o GCP.

- Se un aggregato non contiene volumi per più di 12 ore, Cloud Manager lo elimina.

#### Gestione delle LUN con gestione automatica della capacità

La gestione automatica della capacità di Cloud Manager non si applica alle LUN. Quando Cloud Manager crea un LUN, disattiva la funzione di crescita automatica.

#### Gestione degli inode con gestione automatica della capacità

Cloud Manager monitora l'utilizzo dell'inode su un volume. Quando viene utilizzato il 85% degli inode, Cloud Manager aumenta le dimensioni del volume per aumentare il numero di inode disponibili. Il numero di file che un volume può contenere è determinato dal numero di inode.

#### Gestione manuale della capacità

Se l'account Admin imposta la modalità di gestione della capacità su manuale, Cloud Manager visualizza i messaggi azione richiesta quando è necessario prendere decisioni in merito alla capacità. Gli stessi esempi descritti nella modalità automatica si applicano alla modalità manuale, ma spetta all'utente accettare le azioni.

### Flash cache

Alcune configurazioni Cloud Volumes ONTAP in AWS e Azure includono lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance.

#### Cos'è Flash cache?

Flash cache accelera l'accesso ai dati attraverso il caching intelligente in tempo reale dei dati utente recentemente letti e dei metadati NetApp. È efficace per i carichi di lavoro a lettura intensiva, inclusi database, e-mail e file service.

#### Istanze supportate in AWS

Selezionare uno dei seguenti tipi di istanze EC2 con un sistema Cloud Volumes ONTAP Premium o BYOL nuovo o esistente:

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

#### Tipo di VM supportato in Azure

Selezionare il tipo di macchina virtuale Standard_L8s_v2 con un sistema BYOL Cloud Volumes ONTAP a nodo singolo in Azure.

#### Limitazioni

- La compressione deve essere disattivata su tutti i volumi per sfruttare i miglioramenti delle prestazioni di Flash cache.

  Scegli l'assenza di efficienza dello storage durante la creazione di un volume da Cloud Manager, oppure crea un volume e poi "Disattivare la compressione dei dati utilizzando l'interfaccia CLI".

- Il ripristino della cache dopo un riavvio non è supportato con Cloud Volumes ONTAP.

### Storage WORM

È possibile attivare lo storage WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP per conservare i file in forma non modificata per un periodo di conservazione specificato. Lo storage WORM è basato sulla tecnologia SnapLock in modalità Enterprise, il che significa che i file WORM sono protetti a livello di file.

Una volta che un file è stato salvato nello storage WORM, non può essere modificato, anche dopo la scadenza del periodo di conservazione. Un clock a prova di manomissione determina quando è trascorso il periodo di conservazione di un file WORM.

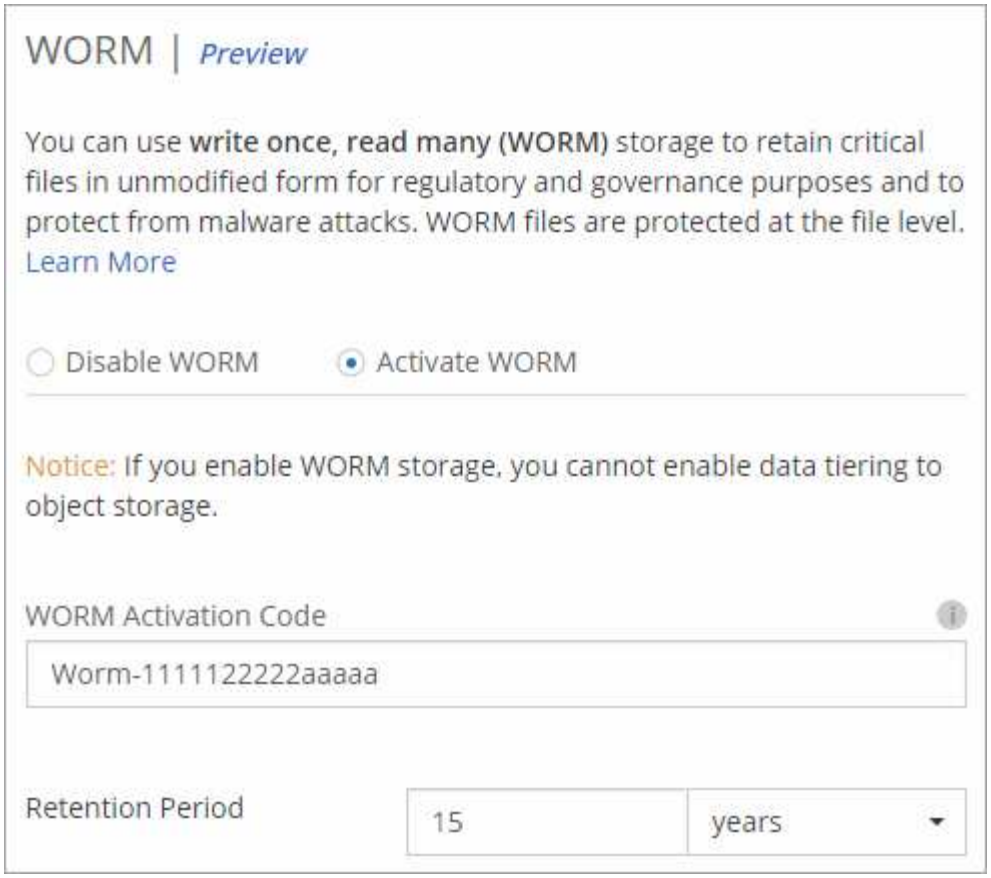
Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari.

#### Attivazione dello storage WORM

È possibile attivare lo storage WORM su un sistema Cloud Volumes ONTAP quando si crea un nuovo ambiente di lavoro. Ciò include la specifica di un codice di attivazione e l'impostazione del periodo di conservazione predefinito per i file. È possibile ottenere un codice di attivazione utilizzando l'icona della chat in basso a destra dell'interfaccia di Cloud Manager.

Non è possibile attivare lo storage WORM su singoli volumi. WORM deve essere attivato a livello di sistema.

L'immagine seguente mostra come attivare lo storage WORM durante la creazione di un ambiente di lavoro:




#### Commit dei file in WORM

È possibile utilizzare un'applicazione per il commit dei file in WORM su NFS o CIFS oppure utilizzare l'interfaccia utente di ONTAP per il commit automatico dei file in WORM. È inoltre possibile utilizzare un file .WORM appendibile per conservare i dati scritti in modo incrementale, ad esempio le informazioni di log.

Dopo aver attivato lo storage WORM su un sistema Cloud Volumes ONTAP, è necessario utilizzare l'interfaccia utente di ONTAP per la gestione dello storage WORM. Per istruzioni, fare riferimento a. "Documentazione ONTAP".

Il supporto Cloud Volumes ONTAP per lo storage WORM equivale alla modalità aziendale SnapLock.

#### Limitazioni

- Se si elimina o si sposta un disco direttamente da AWS o Azure, è possibile eliminare un volume prima della data di scadenza.
- Quando lo storage WORM è attivato, non è possibile abilitare il tiering dei dati sullo storage a oggetti.
- Per abilitare lo storage WORM, è necessario disattivare il backup su cloud.

## Coppie ad alta disponibilità

#### Coppie ad alta disponibilità in AWS

Una configurazione Cloud Volumes ONTAP ad alta disponibilità (ha) offre operazioni senza interruzioni e tolleranza agli errori. In AWS, i dati vengono sottoposti a mirroring

sincrono tra i due nodi.

#### Panoramica

In AWS, le configurazioni Cloud Volumes ONTAP ha includono i seguenti componenti:

- Due nodi Cloud Volumes ONTAP i cui dati vengono sottoposti a mirroring sincrono l'uno con l'altro.
- Istanza di mediatore che fornisce un canale di comunicazione tra i nodi per assistere nei processi di acquisizione e giveback dello storage.

> L'istanza del mediatore esegue il sistema operativo Linux su un'istanza t2.micro e utilizza un disco magnetico EBS di circa 8 GB.

### Takeover e giveback dello storage

Se un nodo non funziona, l'altro nodo può servire i dati per il proprio partner per fornire un servizio dati continuo. I client possono accedere agli stessi dati dal nodo partner perché i dati sono stati sottoposti a mirroring sincrono con il partner.

Dopo il riavvio del nodo, il partner deve risincronizzare i dati prima di poter restituire lo storage. Il tempo necessario per la risincronizzazione dei dati dipende dalla quantità di dati modificati mentre il nodo era inattivo.

### RPO e RTO

Una configurazione ad alta disponibilità dei dati viene mantenuta come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi. I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.
- L'obiettivo del tempo di ripristino (RTO) è di 60 secondi. In caso di interruzione, i dati devono essere disponibili in 60 secondi o meno.

### Modelli di implementazione HA

È possibile garantire l'elevata disponibilità dei dati implementando una configurazione ha in più zone di disponibilità (AZS) o in un singolo AZ. Per scegliere la configurazione più adatta alle proprie esigenze, è necessario esaminare ulteriori dettagli su ciascuna configurazione.

#### Cloud Volumes ONTAP ha in più zone di disponibilità

L'implementazione di una configurazione ha in zone di disponibilità multiple (AZS) garantisce un'elevata disponibilità dei dati in caso di guasto con un'istanza AZ o che esegue un nodo Cloud Volumes ONTAP. È necessario comprendere in che modo gli indirizzi IP NAS influiscono sull'accesso ai dati e sul failover dello storage.

### Accesso ai dati NFS e CIFS

Quando una configurazione ha viene distribuita in più zone di disponibilità, *indirizzi IP mobili* abilitano l'accesso al client NAS. Gli indirizzi IP mobili, che devono essere al di fuori dei blocchi CIDR per tutti i VPC della regione, possono migrare tra i nodi in caso di guasti. Non sono accessibili in modo nativo ai client che si trovano al di fuori del VPC, a meno che non si "Configurare un gateway di transito AWS".

Se non è possibile configurare un gateway di transito, gli indirizzi IP privati sono disponibili per i client NAS esterni al VPC. Tuttavia, questi indirizzi IP sono statici e non possono eseguire il failover tra i nodi.

Prima di implementare una configurazione ha in più zone di disponibilità, è necessario esaminare i requisiti per gli indirizzi IP mobili e le tabelle di routing. È necessario specificare gli indirizzi IP mobili quando si implementa la configurazione. Gli indirizzi IP privati vengono creati automaticamente da Cloud Manager.

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

### Accesso ai dati iSCSI

La comunicazione dati tra più VPC non è un problema, poiché iSCSI non utilizza indirizzi IP mobili.

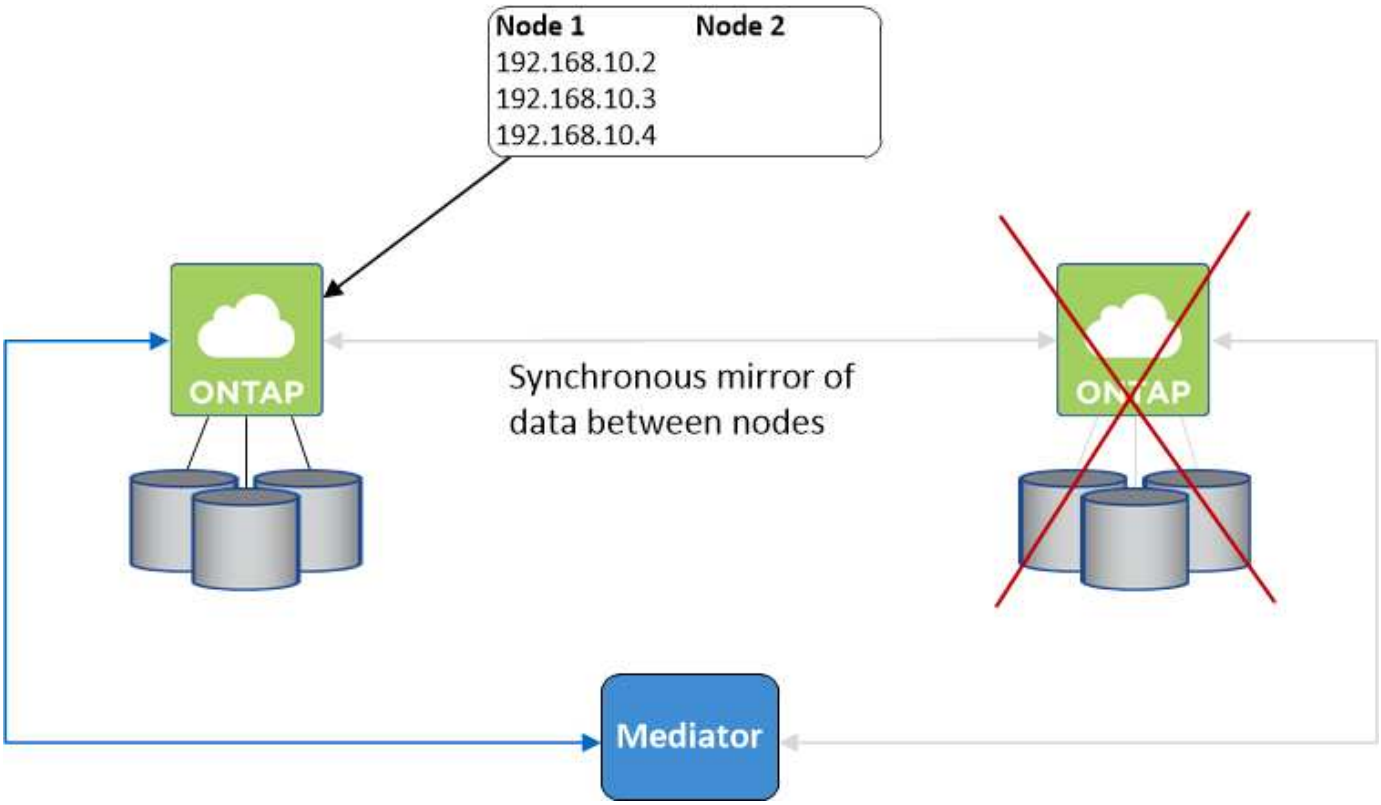
### Takeover e giveback dello storage per iSCSI

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

> Per informazioni su quali configurazioni host specifiche supportano ALUA, consultare "Tool di matrice di interoperabilità NetApp" E la guida all'installazione e all'installazione delle utility host per il sistema operativo host.

### Takeover e giveback dello storage per NAS

Quando l'acquisizione avviene in una configurazione NAS utilizzando IP mobili, l'indirizzo IP mobile del nodo utilizzato dai client per accedere ai dati viene spostato nell'altro nodo. L'immagine seguente mostra l'acquisizione dello storage in una configurazione NAS utilizzando IP mobili. Se il nodo 2 non funziona, l'indirizzo IP mobile per il nodo 2 passa al nodo 1.




Gli IP dei dati NAS utilizzati per l'accesso VPC esterno non possono migrare tra i nodi in caso di guasti. Se un nodo non è in linea, è necessario rimontarlo manualmente sui client esterni al VPC utilizzando l'indirizzo IP sull'altro nodo.

Una volta che il nodo guasto torna in linea, rimontare i client sui volumi utilizzando l'indirizzo IP originale. Questo passaggio è necessario per evitare il trasferimento di dati non necessari tra due nodi ha, che può causare un impatto significativo sulle performance e sulla stabilità.

È possibile identificare facilmente l'indirizzo IP corretto da Cloud Manager selezionando il volume e facendo clic su **Mount Command**.

#### Cloud Volumes ONTAP ha in una singola zona di disponibilità

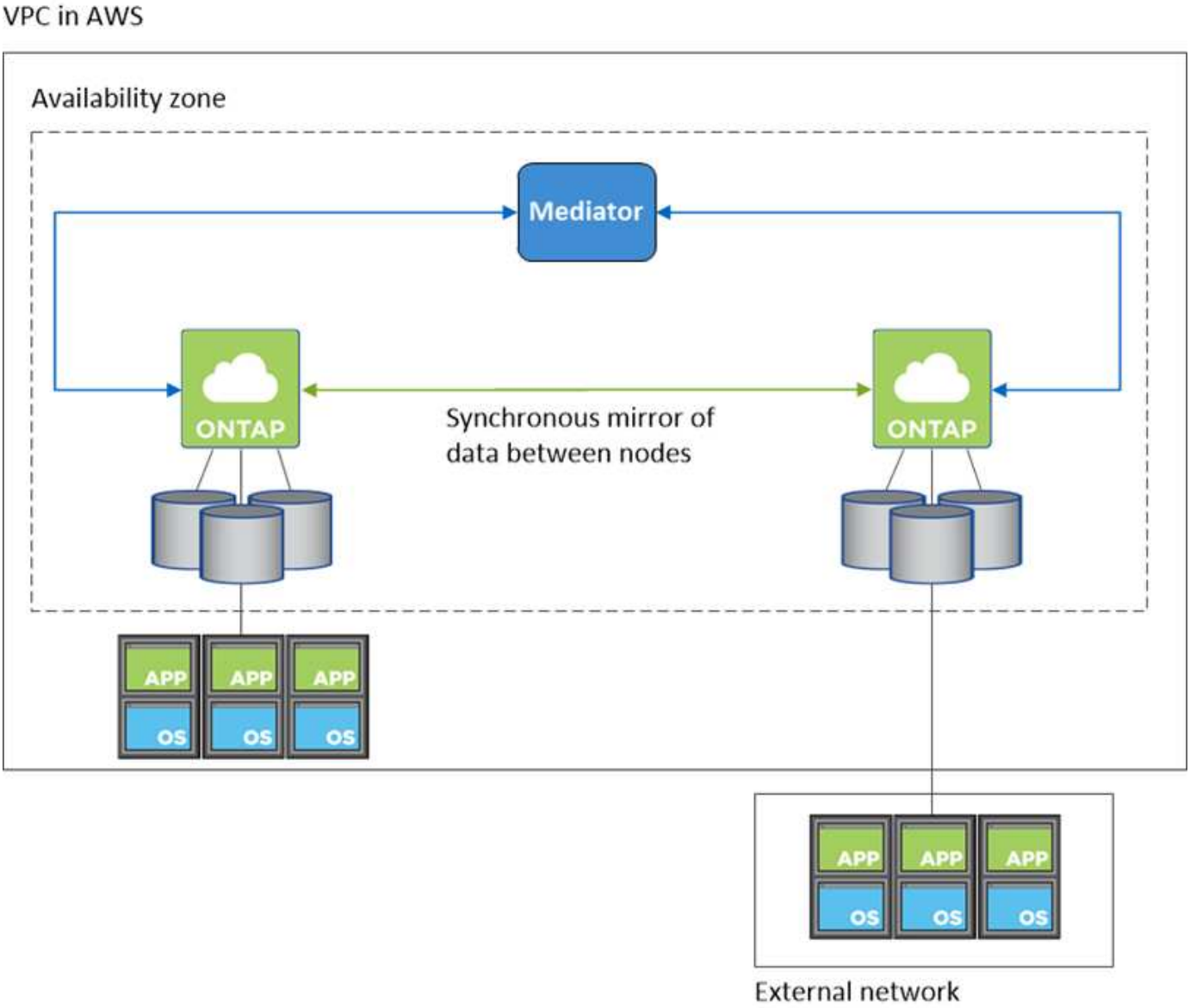
L'implementazione di una configurazione ha in una singola zona di disponibilità (AZ) può garantire un'elevata disponibilità dei dati in caso di guasto di un'istanza che esegue un nodo Cloud Volumes ONTAP. Tutti i dati sono accessibili in modo nativo dall'esterno del VPC.

> Cloud Manager crea un "Gruppo di posizionamento AWS Spread" E lancia i due nodi ha in quel gruppo di posizionamento. Il gruppo di posizionamento riduce il rischio di guasti simultanei distribuendo le istanze su hardware sottostante distinto. Questa funzionalità migliora la ridondanza dal punto di vista del calcolo e non dal punto di vista del guasto del disco.

### Accesso ai dati

Poiché questa configurazione si trova in un singolo AZ, non richiede indirizzi IP mobili. È possibile utilizzare lo stesso indirizzo IP per l'accesso ai dati dall'interno del VPC e dall'esterno del VPC.

La seguente immagine mostra una configurazione ha in un singolo AZ. I dati sono accessibili dall'interno del VPC e dall'esterno del VPC.




### Takeover e giveback dello storage

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

Per informazioni su quali configurazioni host specifiche supportano ALUA, consultare "Tool di matrice di interoperabilità NetApp" E la guida all'installazione e all'installazione delle utility host per il sistema operativo host.

Per le configurazioni NAS, gli indirizzi IP dei dati possono migrare tra i nodi ha in caso di guasti. In questo modo si garantisce l'accesso del client allo storage.

#### Come funziona lo storage in una coppia ha

A differenza di un cluster ONTAP, lo storage in una coppia Cloud Volumes ONTAP ha non viene condiviso tra i nodi. I dati vengono invece sottoposti a mirroring sincrono tra i nodi in modo che siano disponibili in caso di guasto.

### Allocazione dello storage

Quando si crea un nuovo volume e sono necessari dischi aggiuntivi, Cloud Manager assegna lo stesso numero di dischi a entrambi i nodi, crea un aggregato mirrorato e crea il nuovo volume. Ad esempio, se sono necessari due dischi per il volume, Cloud Manager assegna due dischi per nodo per un totale di quattro dischi.

### Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto lo storage per il nodo attivo.

È possibile impostare una configurazione Active-Active solo quando si utilizza Cloud Manager nella vista del sistema di storage.

### Aspettative di performance per una configurazione ha

Una configurazione Cloud Volumes ONTAP ha replica in modo sincrono i dati tra i nodi, consumando la larghezza di banda della rete. Di conseguenza, rispetto a una configurazione Cloud Volumes ONTAP a nodo singolo, è possibile aspettarsi le seguenti performance:

- Per le configurazioni ha che servono dati da un solo nodo, le prestazioni di lettura sono paragonabili alle prestazioni di lettura di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono inferiori.
- Per le configurazioni ha che servono dati da entrambi i nodi, le performance di lettura sono superiori rispetto alle performance di lettura di una configurazione a nodo singolo e le performance di scrittura sono uguali o superiori.

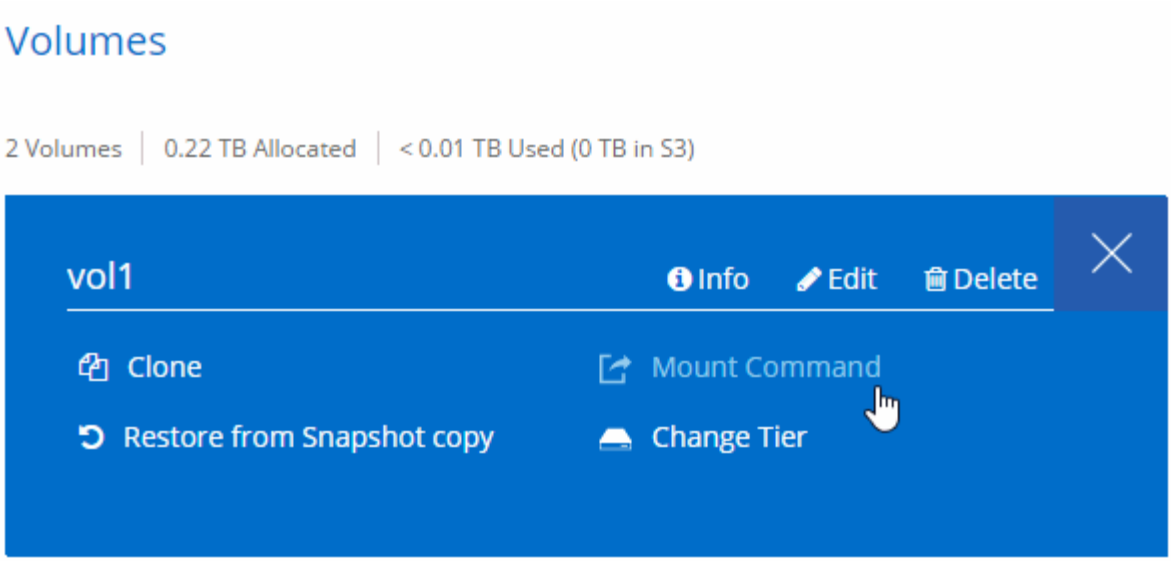
Per ulteriori informazioni sulle prestazioni di Cloud Volumes ONTAP, vedere "Performance".

### Accesso client allo storage

I client devono accedere ai volumi NFS e CIFS utilizzando l'indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l'indirizzo IP del nodo partner, il traffico passa tra entrambi i nodi, riducendo le performance.

Se si sposta un volume tra nodi in una coppia ha, è necessario rimontarlo utilizzando l'indirizzo IP dell'altro nodo. In caso contrario, si possono ottenere prestazioni ridotte. Se i client supportano i riferimenti NFSv4 o il reindirizzamento delle cartelle per CIFS, è possibile attivare tali funzionalità sui sistemi Cloud Volumes ONTAP per evitare di rimontare il volume. Per ulteriori informazioni, consultare la documentazione di ONTAP.

È possibile identificare facilmente l'indirizzo IP corretto da Cloud Manager:

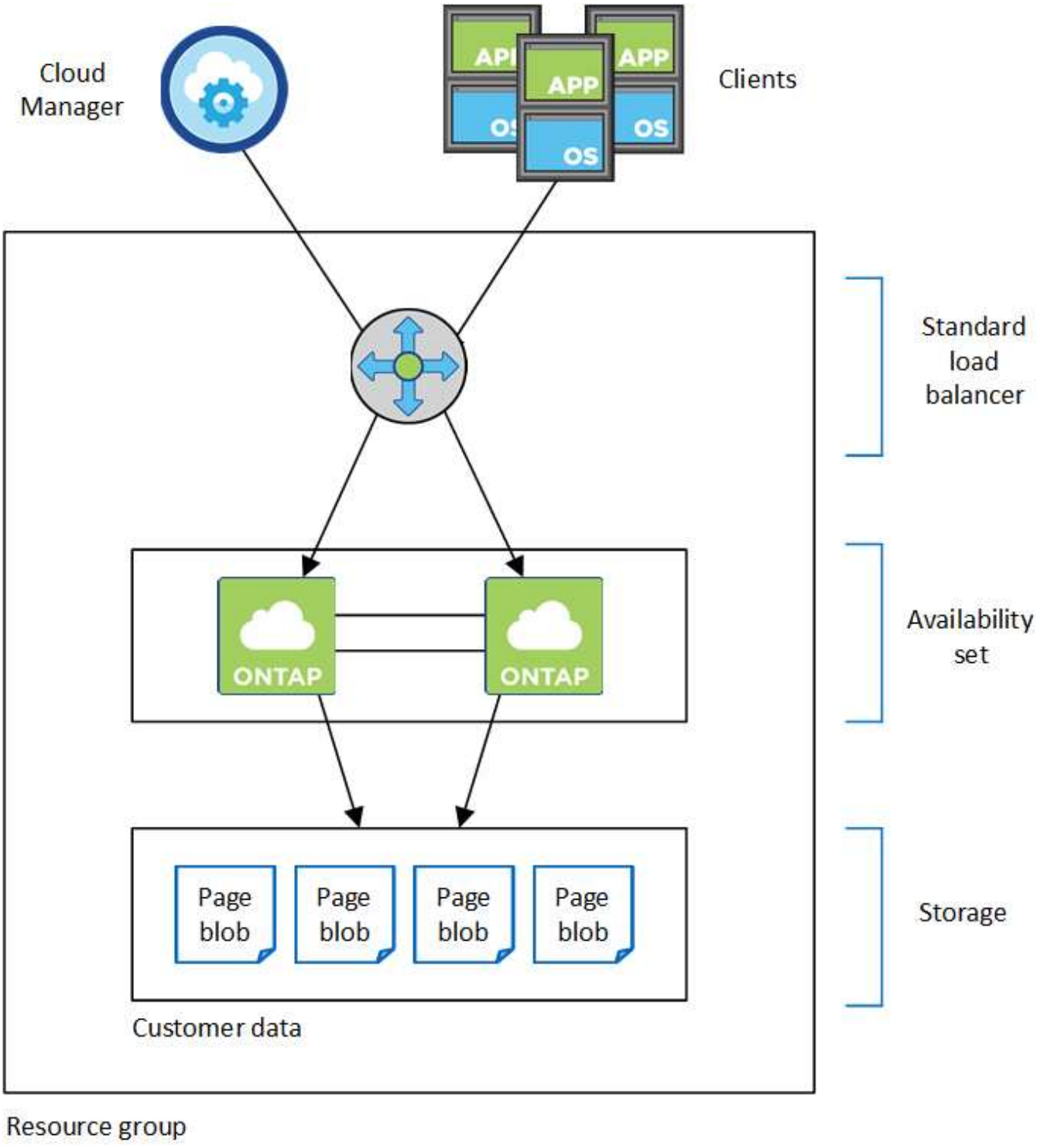



#### Coppie ad alta disponibilità in Azure

Una coppia Cloud Volumes ONTAP ad alta disponibilità (ha) offre affidabilità aziendale e operazioni continue in caso di guasti nel tuo ambiente cloud. In Azure, lo storage viene condiviso tra i due nodi.

##### Componenti HA

Una configurazione Cloud Volumes ONTAP ha in Azure include i seguenti componenti:




Tenere presente quanto segue sui componenti di Azure implementati da Cloud Manager:

**Bilanciamento del carico standard Azure**

Il bilanciamento del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP ha.

**Set di disponibilità**

Il set di disponibilità garantisce che i nodi si trovino in diversi domini di errore e aggiornamento.

### Dischi

I dati dei clienti si trovano nelle pagine di Premium Storage. Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre richiesto storage aggiuntivo per "dati di boot, root e core".

### Account storage

- Per i dischi gestiti è necessario un account di storage.
- Per le pagine blob dello storage Premium sono necessari uno o più account di storage, in quanto viene raggiunto il limite di capacità del disco per account di storage.

  "Documentazione di Azure: Obiettivi di scalabilità e performance dello storage Azure per gli account storage".

- Per il tiering dei dati sullo storage Azure Blob è necessario un account storage.
- A partire da Cloud Volumes ONTAP 9.7, gli account storage creati da Cloud Manager per le coppie ha sono account storage v2 generici.
- Durante la creazione di un ambiente di lavoro, è possibile attivare una connessione HTTPS da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage 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.

#### RPO e RTO

Una configurazione ad alta disponibilità dei dati viene mantenuta come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi. I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.
- L'obiettivo del tempo di ripristino (RTO) è di 60 secondi. In caso di interruzione, i dati devono essere disponibili in 60 secondi o meno.

#### Takeover e giveback dello storage

Analogamente a un cluster ONTAP fisico, lo storage in una coppia Azure ha viene condiviso tra i nodi. Le connessioni allo storage del partner consentono a ciascun nodo di accedere allo storage dell'altro in caso di *takeover*. I meccanismi di failover del percorso di rete garantiscono che client e host continuino a comunicare con il nodo esistente. Il partner _restituisce lo storage quando il nodo viene riportato in linea.

Per le configurazioni NAS, gli indirizzi IP dei dati migrano automaticamente tra i nodi ha in caso di guasti.

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

Per informazioni su quali configurazioni host specifiche supportano ALUA, consultare "Tool di matrice di interoperabilità NetApp" E la guida all'installazione e all'installazione delle utility host per il sistema operativo host.

#### Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto lo storage per il nodo attivo.

#### Limitazioni DI HA

Le seguenti limitazioni influiscono sulle coppie Cloud Volumes ONTAP ha in Azure:

- Le coppie HA sono supportate con Cloud Volumes ONTAP standard, Premium e BYOL. Esplora non è supportato.
- NFSv4 non è supportato. NFSv3 è supportato.
- Le coppie HA non sono supportate in alcune regioni.

  "Consulta l'elenco delle aree Azure supportate".

"Scopri come implementare un sistema ha in Azure".

## Valutazione

È possibile valutare Cloud Volumes ONTAP prima di pagare il software. Il modo più comune è quello di lanciare LA versione PAYGO del tuo primo sistema Cloud Volumes ONTAP per ottenere una prova gratuita di 30 giorni. Una licenza BYOL di valutazione è anche un'opzione.

Se hai bisogno di assistenza per la prova di concetto, contatta "Il team di vendita" oppure contattatelo tramite l'opzione di chat disponibile all'interno del sito "NetApp Cloud Central" E da Cloud Manager.

#### 30 giorni di prova gratuita per PAYGO

È disponibile una versione di prova gratuita di 30 giorni se si prevede di pagare per Cloud Volumes ONTAP a consumo. Puoi iniziare una prova gratuita di 30 giorni di Cloud Volumes ONTAP da Cloud Manager creando il tuo primo sistema Cloud Volumes ONTAP nell'account del pagante.

Non sono previsti costi di licenza software oraria per l'istanza, ma i costi di infrastruttura del provider cloud continuano a essere applicati.

Una versione di prova gratuita viene convertita automaticamente in un abbonamento oraria a pagamento alla scadenza. Se si termina l'istanza entro il limite di tempo, l'istanza successiva che si implementa non fa parte della versione di prova gratuita (anche se viene implementata entro 30 giorni).

Le versioni di prova pay-as-you-go vengono assegnate tramite un cloud provider e non sono estendibili in alcun modo.

#### Licenze di valutazione per BYOL

Una licenza BYOL di valutazione è un'opzione per i clienti che prevedono di pagare per Cloud Volumes ONTAP acquistando una licenza denominata da NetApp. Puoi ottenere una licenza di valutazione dal tuo account team, dal tuo Sales Engineer o dal tuo partner.

La chiave di valutazione è valida per 30 giorni e può essere utilizzata più volte, ciascuna per 30 giorni (indipendentemente dal giorno di creazione).

Alla fine di 30 giorni, si verificheranno arresti giornalieri, quindi è meglio pianificare in anticipo. È possibile applicare una nuova licenza BYOL alla licenza di valutazione per un aggiornamento in-place (ciò richiede il riavvio dei sistemi a nodo singolo). I dati ospitati vengono eliminati **non** al termine del periodo di prova.

Non è possibile aggiornare il software Cloud Volumes ONTAP quando si utilizza una licenza di valutazione.

## Licensing

Ogni sistema Cloud Volumes ONTAP BYOL deve disporre di una licenza di sistema con un abbonamento attivo. Cloud Manager semplifica il processo gestendo le licenze e avvisandovi prima della scadenza. Le licenze BYOL sono disponibili anche per il backup nel cloud.

### Licenze di sistema BYOL

È possibile acquistare più licenze per un sistema Cloud Volumes ONTAP BYOL per allocare più di 368 TB di capacità. Ad esempio, è possibile acquistare due licenze per allocare fino a 736 TB di capacità a Cloud Volumes ONTAP. Oppure puoi acquistare quattro licenze per ottenere fino a 1.4 PB.

Il numero di licenze che è possibile acquistare per un sistema a nodo singolo o una coppia ha è illimitato.

Tenere presente che i limiti dei dischi possono impedire di raggiungere il limite di capacità utilizzando solo i dischi. È possibile superare il limite di dischi di "tiering dei dati inattivi sullo storage a oggetti". Per informazioni sui limiti dei dischi, fare riferimento a. "Limiti di storage nelle note di rilascio di Cloud Volumes ONTAP".

#### Gestione delle licenze per un nuovo sistema

Quando si crea un sistema BYOL, Cloud Manager richiede il numero di serie della licenza e l'account NetApp Support Site. Cloud Manager utilizza l'account per scaricare il file di licenza da NetApp e installarlo sul sistema Cloud Volumes ONTAP.

"Scopri come aggiungere account NetApp Support Site a Cloud Manager".

Se Cloud Manager non riesce ad accedere al file di licenza tramite la connessione Internet sicura, è possibile ottenere il file da solo e caricarlo manualmente in Cloud Manager. Per istruzioni, vedere "Gestione delle licenze BYOL per Cloud Volumes ONTAP".

#### Avviso di scadenza della licenza

Cloud Manager ti avvisa 30 giorni prima della scadenza della licenza e di nuovo alla scadenza della stessa. La seguente immagine mostra un avviso di scadenza di 30 giorni:


È possibile selezionare l'ambiente di lavoro per rivedere il messaggio.

Se la licenza non viene rinnovata in tempo, il sistema Cloud Volumes ONTAP si spegne automaticamente. Se viene riavviato, si spegne di nuovo.

Cloud Volumes ONTAP può anche inviare notifiche tramite e-mail, un host trapSNMP o un server syslog utilizzando le notifiche degli eventi EMS (sistema di gestione degli eventi). Per istruzioni, consultare "Guida rapida alla configurazione EMS di ONTAP 9".

#### Rinnovo della licenza

Quando rinnovi un abbonamento BYOL contattando un rappresentante NetApp, Cloud Manager ottiene automaticamente la nuova licenza da NetApp e la installa sul sistema Cloud Volumes ONTAP.

Se Cloud Manager non riesce ad accedere al file di licenza tramite la connessione Internet sicura, è possibile ottenere il file da solo e caricarlo manualmente in Cloud Manager. Per istruzioni, vedere "Gestione delle licenze BYOL per Cloud Volumes ONTAP".

### Licenze di backup BYOL

Una licenza di backup BYOL consente di acquistare una licenza da NetApp per utilizzare Backup to Cloud per un determinato periodo di tempo e per una quantità massima di spazio di backup. Una volta raggiunto il limite, è necessario rinnovare la licenza.

"Scopri di più sulla licenza BYOL per il backup nel cloud".

## Sicurezza

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

### Crittografia dei dati inattivi

Cloud Volumes ONTAP supporta le seguenti tecnologie di crittografia:

- Soluzioni di crittografia NetApp (NVE e NAE)
- Servizio di gestione delle chiavi AWS
- Azure Storage Service Encryption
- Crittografia predefinita di Google Cloud Platform

È possibile utilizzare le soluzioni di crittografia NetApp con crittografia nativa da AWS, Azure o GCP, che crittografano i dati a livello di hypervisor. In questo modo si fornirebbe una doppia crittografia, che potrebbe essere utile per i dati molto sensibili. Quando si accede ai dati crittografati, questi vengono crittografati due volte, una volta a livello di hypervisor (utilizzando le chiavi del cloud provider) e poi di nuovo utilizzando le soluzioni di crittografia NetApp (utilizzando le chiavi di un gestore di chiavi esterno).

#### Soluzioni di crittografia NetApp (NVE e NAE)

Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp (NVE) e la crittografia aggregata NetApp (NAE) con un gestore di chiavi esterno. NVE e NAE sono soluzioni basate su software che consentono la crittografia dei volumi (data-at-rest) conforme a FIPS 140-2.

- NVE crittografa i dati inattivi un volume alla volta. Ogni volume di dati dispone di una chiave di crittografia univoca.
- NAE è un'estensione di NVE, che crittografa i dati per ogni volume e i volumi condividono una chiave nell'aggregato. NAE consente inoltre di deduplicare i blocchi comuni di tutti i volumi dell'aggregato.

Sia NVE che NAE utilizzano la crittografia AES a 256 bit.

"Scopri di più su NetApp Volume Encryption e NetApp aggregate Encryption".

A partire da Cloud Volumes ONTAP 9.7, i nuovi aggregati avranno la crittografia aggregata NetApp (NAE) attivata per impostazione predefinita dopo aver configurato un gestore di chiavi esterno. I nuovi volumi che non fanno parte di un aggregato NAE avranno NetApp Volume Encryption (NVE) abilitato per impostazione predefinita (ad esempio, se si dispone di aggregati creati prima di impostare un gestore di chiavi esterno).

La configurazione di un gestore di chiavi supportato è l'unica operazione necessaria. Per istruzioni sulla configurazione, vedere "Crittografia dei volumi con le soluzioni di crittografia NetApp".

#### Servizio di gestione delle chiavi AWS

Quando si avvia un sistema Cloud Volumes ONTAP in AWS, è possibile attivare la crittografia dei dati utilizzando "AWS Key Management Service (KMS)". Cloud Manager richiede le chiavi dati utilizzando una chiave master del cliente (CMK).

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

Se si desidera utilizzare questa opzione di crittografia, assicurarsi che AWS KMS sia configurato correttamente. Per ulteriori informazioni, vedere "Configurazione di AWS KMS".

#### Azure Storage Service Encryption

"Azure Storage Service Encryption" Per i dati inattivi è attivato per impostazione predefinita per i dati Cloud Volumes ONTAP in Azure. Non è richiesta alcuna configurazione.

È possibile crittografare i dischi gestiti da Azure su sistemi Cloud Volumes ONTAP a nodo singolo utilizzando chiavi esterne di un altro account. Questa funzionalità è supportata tramite le API di Cloud Manager.

È sufficiente aggiungere quanto segue alla richiesta API quando si crea il sistema a nodo singolo:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

Le chiavi gestite dal cliente non sono supportate con le coppie Cloud Volumes ONTAP ha.

#### Crittografia predefinita di Google Cloud Platform

"Crittografia dei dati inattivi di Google Cloud Platform" È attivato per impostazione predefinita per Cloud Volumes ONTAP. Non è richiesta alcuna configurazione.

Mentre Google Cloud Storage crittografa sempre i tuoi dati prima che vengano scritti su disco, puoi utilizzare le API di Cloud Manager 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. "Scopri di più".

### Scansione virus ONTAP

È possibile utilizzare la funzionalità antivirus integrata nei sistemi ONTAP per proteggere i dati da virus o altri codici dannosi.

La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

Per informazioni su vendor, software e versioni supportate da Vscan, consultare "Matrice di interoperabilità NetApp".

Per informazioni su come configurare e gestire la funzionalità antivirus sui sistemi ONTAP, consultare "Guida alla configurazione antivirus di ONTAP 9".

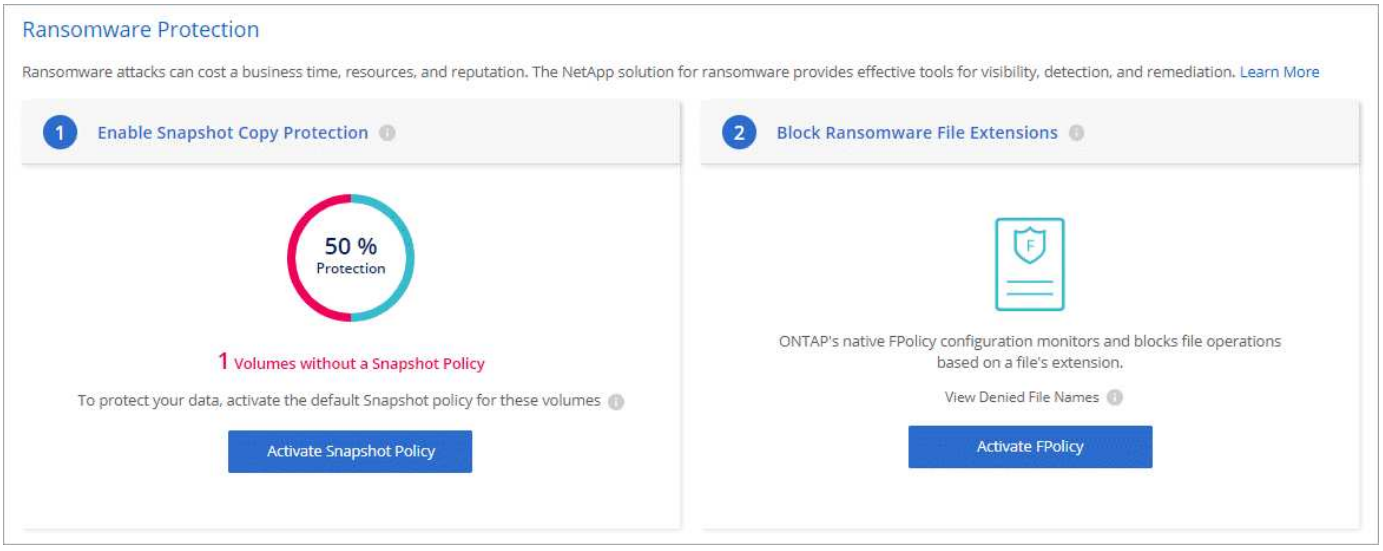
### Protezione ransomware

Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. Cloud Manager consente di implementare la soluzione NetApp per ransomware, che fornisce strumenti efficaci per visibilità, rilevamento e risoluzione dei problemi.

- Cloud Manager identifica i volumi che non sono protetti da una policy Snapshot e consente di attivare la policy Snapshot predefinita su tali volumi.

  Le copie Snapshot sono di sola lettura, impedendo la corruzione del ransomware. Possono inoltre offrire la granularità necessaria per creare immagini di una singola copia di file o di una soluzione completa di disaster recovery.

- Cloud Manager consente inoltre di bloccare le estensioni di file ransomware comuni attivando la soluzione FPolicy di ONTAP.




"Scopri come implementare la soluzione NetApp per ransomware".

## Performance

Puoi esaminare i risultati delle performance per aiutarti a decidere quali carichi di lavoro sono appropriati per Cloud Volumes ONTAP.

- Cloud Volumes ONTAP per AWS

  "Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni".

- Cloud Volumes ONTAP per Microsoft Azure

  "Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi".

- Cloud Volumes ONTAP per Google Cloud

  "Report tecnico NetApp 4816: Caratterizzazione delle performance di Cloud Volumes ONTAP per Google Cloud".

## Configurazione predefinita per Cloud Volumes ONTAP

La configurazione predefinita di Cloud Volumes ONTAP consente di configurare e amministrare i sistemi, in particolare se si conosce ONTAP perché la configurazione predefinita di Cloud Volumes ONTAP è diversa da ONTAP.

### Valori predefiniti

- Cloud Volumes ONTAP è disponibile come sistema a nodo singolo in AWS, Azure e GCP e come coppia ha in AWS e Azure.
- Cloud Manager crea una VM di storage per il servizio dei dati quando implementa Cloud Volumes ONTAP. Alcune configurazioni supportano macchine virtuali storage aggiuntive. "Scopri di più sulla gestione delle VM di storage".
- Cloud Manager installa automaticamente le seguenti licenze ONTAP Feature su Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - NetApp Volume Encryption (solo per sistemi BYOL o PAYGO registrati)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Per impostazione predefinita, vengono create diverse interfacce di rete:
  - Una LIF di gestione del cluster
  - Un LIF intercluster
  - LIF di gestione SVM su sistemi ha in Azure, sistemi a nodo singolo in AWS e, facoltativamente, su sistemi ha in più zone di disponibilità AWS
  - Una LIF di gestione dei nodi
  - Una LIF di dati iSCSI

- Una LIF di dati CIFS e NFS

> Il failover LIF è disattivato per impostazione predefinita per Cloud Volumes ONTAP a causa dei requisiti EC2. La migrazione di una LIF a una porta diversa interrompe la mappatura esterna tra gli indirizzi IP e le interfacce di rete sull'istanza, rendendo la LIF inaccessibile.

- Cloud Volumes ONTAP invia i backup della configurazione al connettore utilizzando HTTPS.

  I backup sono accessibili da https://ipaddress/occm/offboxconfig/ Dove *ipaddress* è l'indirizzo IP dell'host del connettore.

- Cloud Manager imposta alcuni attributi di volume in modo diverso rispetto ad altri strumenti di gestione (ad esempio, System Manager o CLI).

  La tabella seguente elenca gli attributi del volume impostati da Cloud Manager in modo diverso dai valori predefiniti:

| Attributo | Valore stabilito da Cloud Manager |
|---|---|
| Modalità di dimensionamento automatico | crescere |
| Dimensionamento automatico massimo | 1,000%<br>L'amministratore dell'account può modificare questo valore dalla pagina Impostazioni. |
| Stile di sicurezza | NTFS per CIFS Volumes UNIX per NFS Volumes |
| Stile garanzia di spazio | nessuno |
| Autorizzazioni UNIX (solo NFS) | 777 |

  Per informazioni su questi attributi, consulta la pagina man *volume create*.

### Dati di boot e root per Cloud Volumes ONTAP

Oltre allo storage per i dati degli utenti, Cloud Manager acquista anche lo storage cloud per i dati di boot e root su ogni sistema Cloud Volumes ONTAP.

#### AWS

- Due dischi per nodo per i dati di boot e root:
  - 9.7: Disco io1 da 160 GB per i dati di avvio e disco gp2 da 220 GB per i dati root
  - 9.6: Disco io1 da 93 GB per i dati di avvio e disco gp2 da 140 GB per i dati root
  - 9.5: Disco io1 da 45 GB per i dati di avvio e disco gp2 da 140 GB per i dati root

- Un'istantanea EBS per ogni disco di boot e disco root
- Per le coppie ha, un volume EBS per l'istanza Mediator, che è di circa 8 GB

#### Azure (nodo singolo)

- Tre dischi SSD Premium:
  - Un disco da 10 GB per i dati di avvio
  - Un disco da 140 GB per i dati root
  - Un disco da 128 GB per NVRAM

    Se la macchina virtuale scelta per Cloud Volumes ONTAP supporta gli SSD Ultra, il sistema utilizza un SSD Ultra per la NVRAM, anziché un SSD Premium.
- Un disco HDD standard da 1024 GB per il risparmio dei core
- Uno snapshot Azure per ogni disco di boot e disco root

#### Azure (coppie ha)

- Due dischi SSD Premium da 10 GB per il volume di boot (uno per nodo)
- Due blob di pagina Premium Storage da 140 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GB per il risparmio di core (uno per nodo)
- Due dischi SSD Premium da 128 GB per NVRAM (uno per nodo)
- Uno snapshot Azure per ogni disco di boot e disco root

#### GCP

- Un disco persistente standard da 10 GB per i dati di avvio
- Un disco persistente standard da 64 GB per i dati root
- Un disco persistente standard da 500 GB per NVRAM
- Un disco persistente standard da 216 GB per il risparmio dei core
- Uno snapshot GCP per il disco di boot e il disco root

#### Dove risiedono i dischi

Cloud Manager definisce lo storage come segue:

- I dati di avvio risiedono su un disco collegato all'istanza o alla macchina virtuale.

  Questo disco, che contiene l'immagine di avvio, non è disponibile per Cloud Volumes ONTAP.
- I dati root, che contengono la configurazione del sistema e i log, risiedono in aggr0.
- Il volume root della macchina virtuale di storage (SVM) risiede in aggr1.
- I volumi di dati risiedono anche in aggr1.

#### Crittografia

I dischi di boot e root sono sempre crittografati in Azure e Google Cloud Platform perché la crittografia è attivata per impostazione predefinita in tali provider cloud.

Quando si attiva la crittografia dei dati in AWS utilizzando il servizio di gestione delle chiavi (KMS), vengono crittografati anche i dischi di avvio e i dischi root per Cloud Volumes ONTAP. Questo include il disco di boot per l'istanza del mediatore in una coppia ha. I dischi vengono crittografati utilizzando la CMK selezionata quando si crea l'ambiente di lavoro.

# Inizia ad utilizzare AWS

## Introduzione a Cloud Volumes ONTAP per AWS

Inizia a utilizzare Cloud Volumes ONTAP per 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".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

### Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. 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 in modo che il connettore e Cloud Volumes ONTAP possano contattare diversi endpoint.

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "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.

"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 Cloud Manager**

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**

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

## Pianificazione della configurazione 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.

### Scelta di un tipo di licenza

Cloud Volumes ONTAP è disponibile in due opzioni di prezzo: Pay-as-you-go e Bring Your Own License (BYOL). Per il pay-as-you-go, puoi scegliere tra tre licenze: Explore, Standard o Premium. Ogni licenza offre diverse capacità e opzioni di calcolo.

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 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 9.7 in AWS"

### Dimensionamento del 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**

Gli SSD General Purpose sono il tipo di disco più comune per Cloud Volumes ONTAP. Per visualizzare i casi di utilizzo dei dischi EBS, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".

**Dimensione del disco EBS**

Quando si avvia un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. Dopo di che, è possibile "Lascia che Cloud Manager gestisca la capacità di un sistema per te", ma se lo si desidera "costruisci gli 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 da 4 TB), 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".

Guarda il seguente video per ulteriori dettagli sul dimensionamento del tuo sistema Cloud Volumes ONTAP in AWS:

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

### Scelta di una configurazione che supporti Flash cache

Alcune configurazioni Cloud Volumes ONTAP in AWS includono lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance. "Scopri di più su Flash cache".

### Foglio di lavoro delle informazioni di rete AWS

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.

#### Informazioni di rete per Cloud Volumes ONTAP

| Informazioni AWS | Il tuo valore |
|---|---|
| Regione | |
| VPC | |
| Subnet | |
| Gruppo di sicurezza (se si utilizza il proprio) | |

**Informazioni di rete per una coppia ha in più AZS**

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

**Scelta della velocità di scrittura**

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. 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.

**Differenza tra la velocità di scrittura normale e l'alta velocità di scrittura**

Quando si sceglie la normale velocità di scrittura, i dati vengono scritti direttamente su disco, riducendo così la probabilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati nel buffer prima che vengano scritti su disco, garantendo prestazioni di scrittura più rapide. A causa di questo caching, vi è la possibilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

La quantità di dati che è possibile perdere in caso di interruzione non pianificata del sistema è l'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'azione di scrittura dei dati bufferizzati su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale condizione si verifica per prima). Tuttavia, le performance del volume di AWS EBS possono influire sul tempo di elaborazione dei punti di coerenza.

#### Quando utilizzare un'elevata velocità di scrittura

L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide e se si può resistere al rischio di perdita di dati in caso di un'interruzione non pianificata del sistema.

#### Consigli quando si utilizza un'elevata velocità di scrittura

Se si attiva l'alta velocità di scrittura, è necessario garantire la protezione in scrittura a livello di applicazione.

#### Scelta di 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 crei un volume in Cloud Manager, puoi scegliere un profilo che abiliti queste funzionalità o un profilo che le disabiliti. 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

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

#### Requisiti generali per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in AWS.

**Accesso a Internet in uscita per nodi Cloud Volumes ONTAP**

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

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

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

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

"Scopri come configurare 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)".

### Numero di indirizzi IP

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

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

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

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

### Gruppi di sicurezza

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

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

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

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

In caso di problemi, vedere "AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"

### Connessioni a sistemi ONTAP in altre reti

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

### DNS e Active Directory per CIFS

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

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

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

#### Requisiti 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 Cloud Manager.

Per informazioni sul funzionamento delle coppie ha, vedere "Coppie ad alta disponibilità".

### Zone di disponibilità

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

### Indirizzi IP mobili per dati NAS e gestione cluster/SVM

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

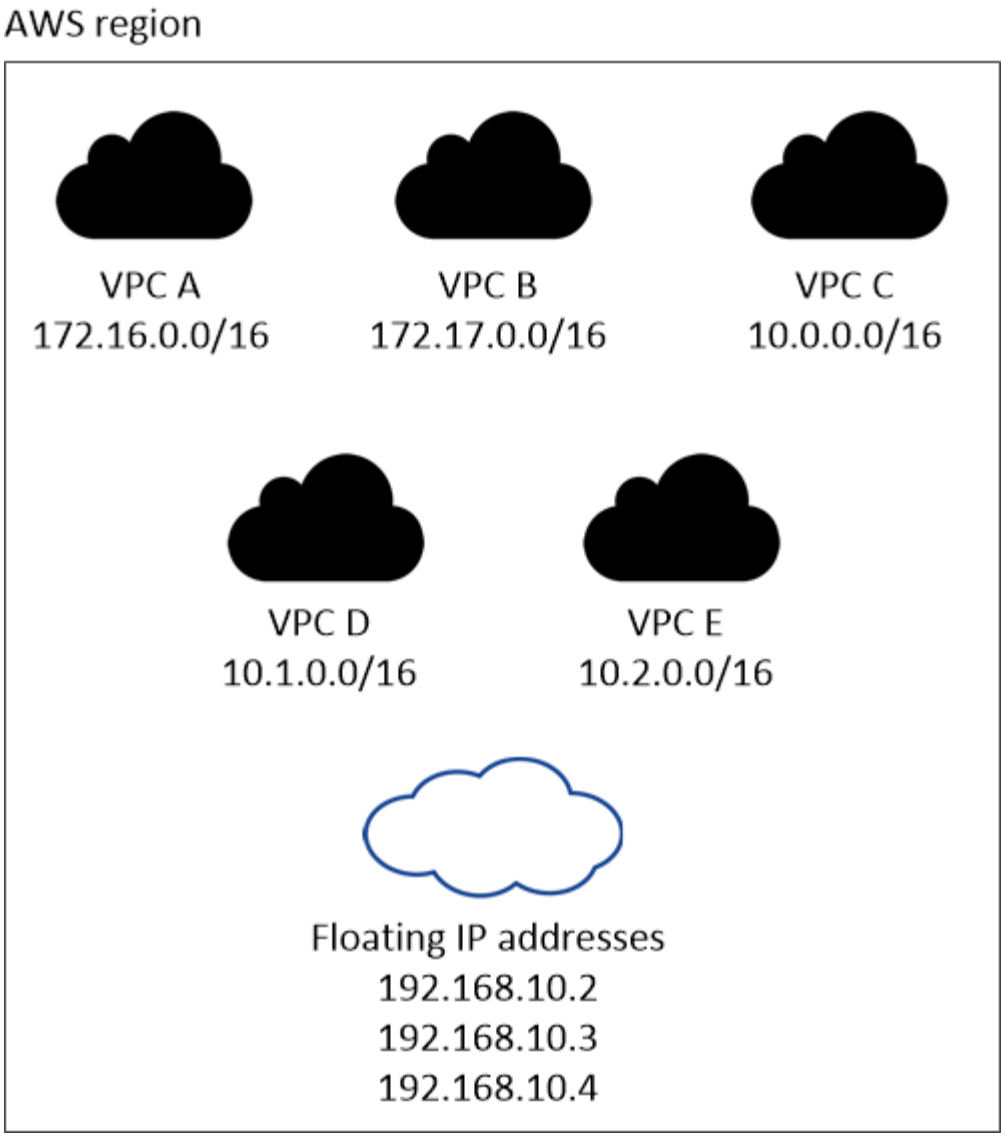
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

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

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

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

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




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

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

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

**Tabelle di percorso**

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

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

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

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

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

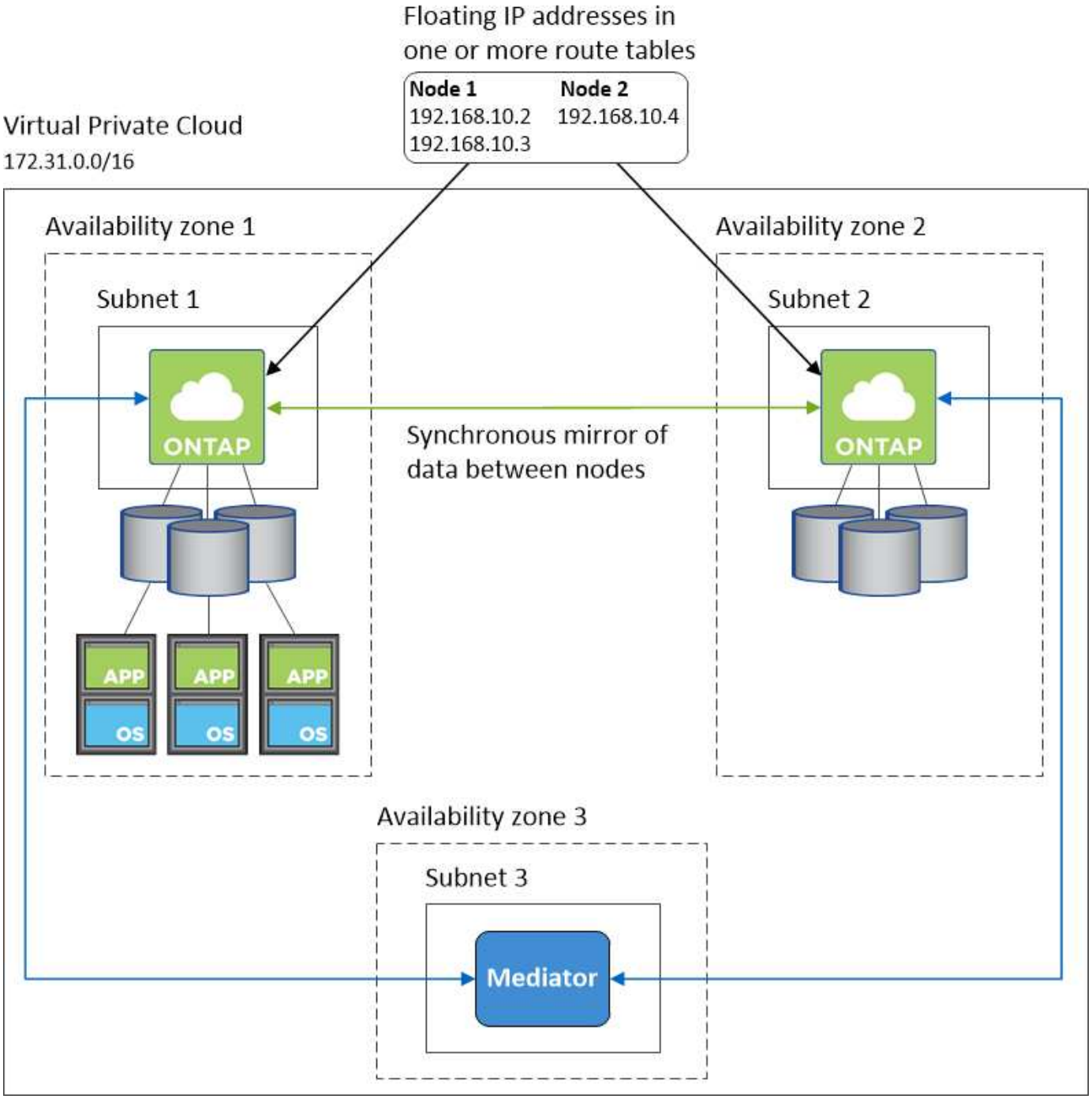
### Connessione ai tool di gestione NetApp

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

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

### Esempio di configurazione ha

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




**Requisiti per il connettore**

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.

Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

### Connessione alle reti di destinazione

Un connettore richiede una connessione di rete ai VPC e ai VNet in cui si desidera implementare Cloud

Volumes ONTAP.

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

### Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in AWS:

| Endpoint | Scopo |
|---|---|
| Servizi AWS (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Servizio di gestione delle chiavi (KMS)<br>• Servizio token di sicurezza (STS)<br>• S3 (Simple Storage Service)<br>L'endpoint esatto dipende dalla regione in cui viene implementato Cloud Volumes ONTAP. "Per ulteriori informazioni, fare riferimento alla documentazione AWS." | Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP in AWS. |
| https://api.services.cloud.netapp.com:443 | Richieste API a NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Fornisce l'accesso a immagini, manifesti e modelli software. |
| https://repo.cloud.support.netapp.com | Utilizzato per scaricare le dipendenze di Cloud Manager. |
| http://repo.mysql.com/ | Utilizzato per scaricare MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP. |
| https://cloudmanagerinfraprod.azurecr.io | Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di eseguire lo streaming dei dati dai record di audit. |
| https://cloudmanager.cloud.netapp.com | Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central. |
| https://netapp-cloud-account.auth0.com | Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata. |
| https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist | Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3. |

| Endpoint | Scopo |
| --- | --- |
| https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup | Comunicazione con NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema. |
| https://ipa-signer.cloudmanager.netapp.com | Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident. |
| Varie sedi di terze parti, ad esempio:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Le sedi di terze parti sono soggette a modifiche. | Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti. |

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

| Endpoint | Scopo |
| --- | --- |
| L'host del connettore | Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.<br>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:<br>• Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale<br>• Un IP pubblico funziona in qualsiasi scenario di rete<br>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati. |
| https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com | Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central. |

| Endpoint | Scopo |
| --- | --- |
| https://widget.intercom.io | Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp. |

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

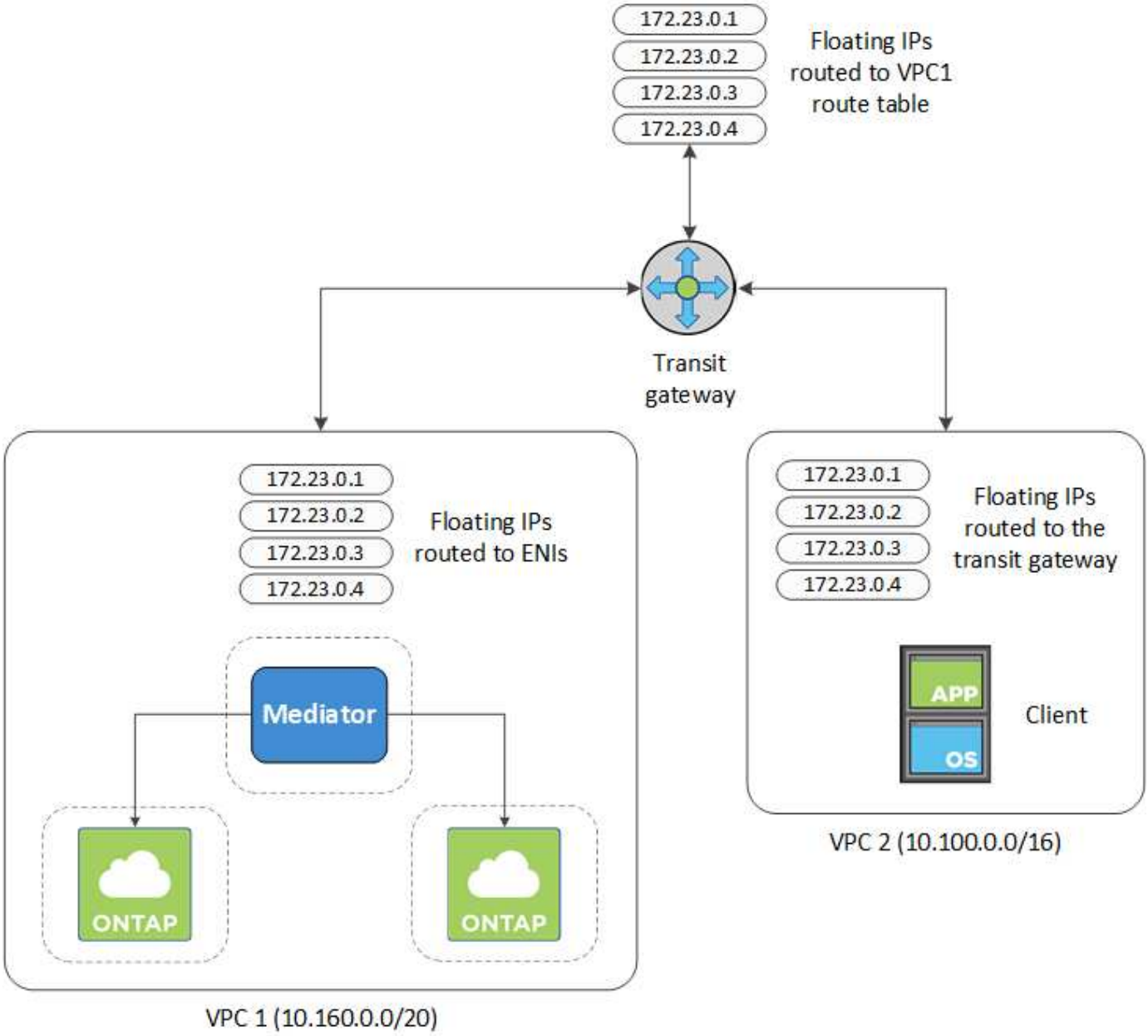
## Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha "Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

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.

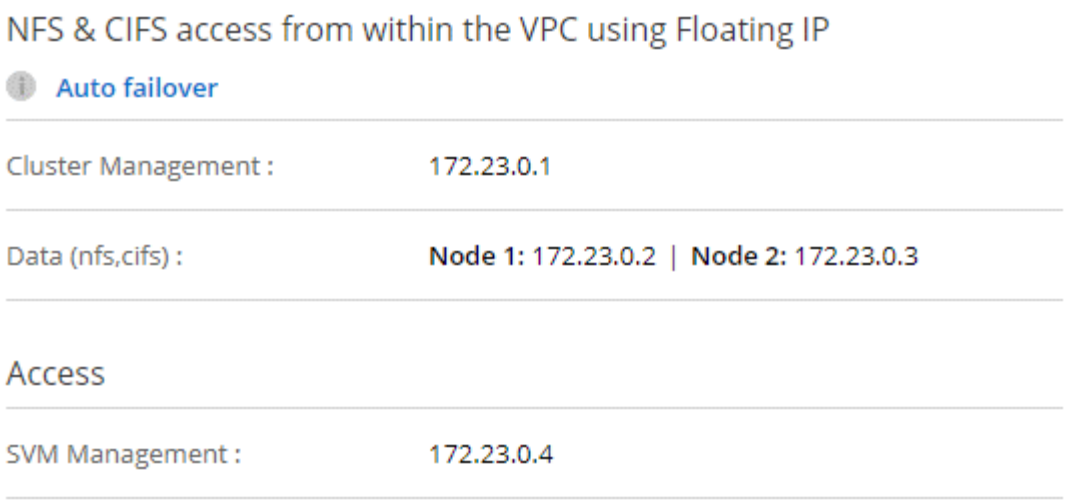



La seguente procedura illustra come configurare una configurazione simile.

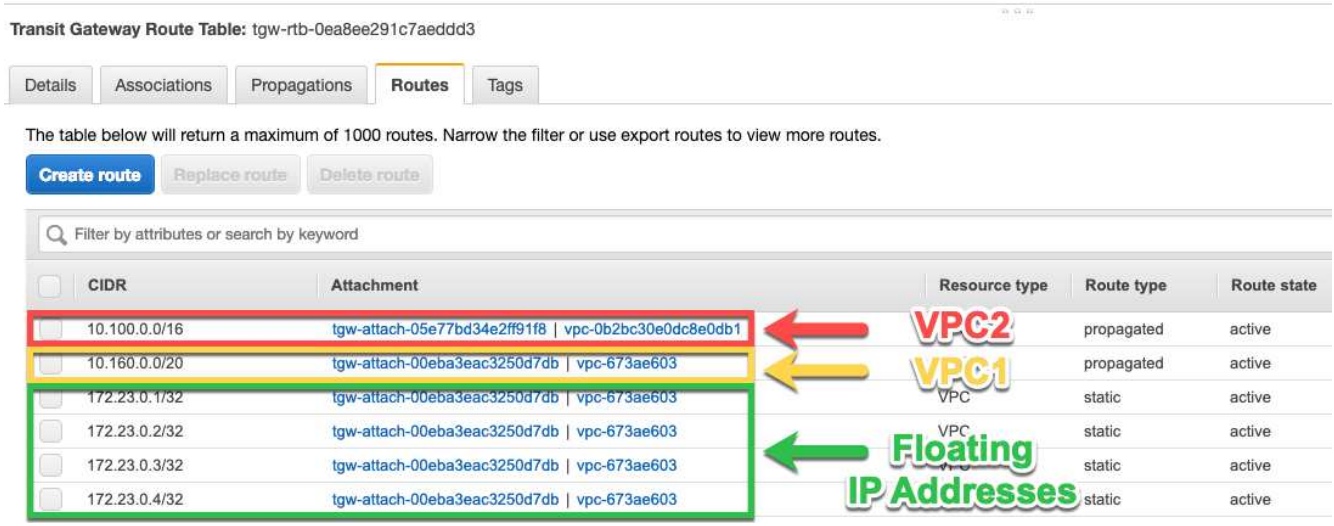
**Fasi**

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

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




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.

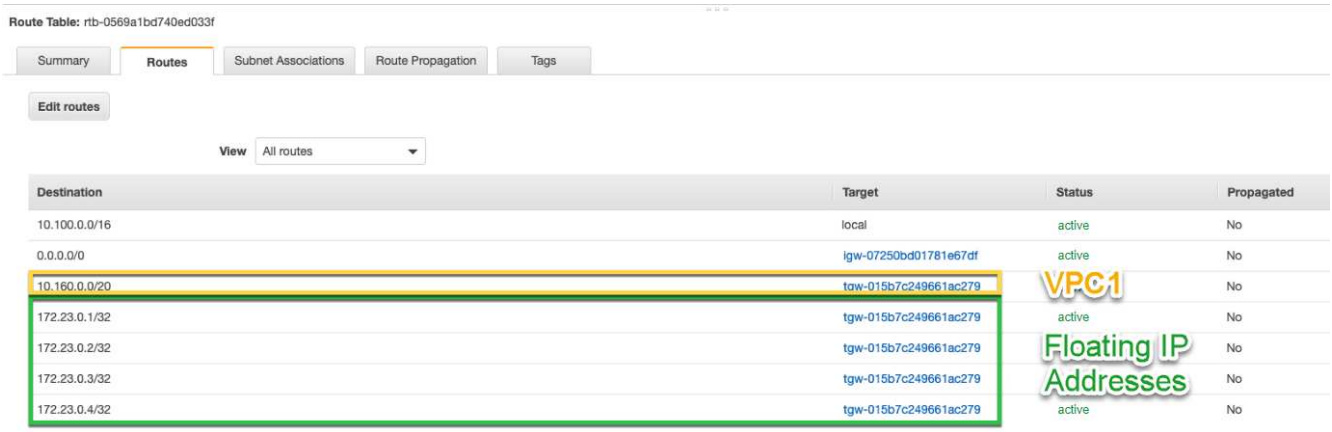



3. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.

   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.

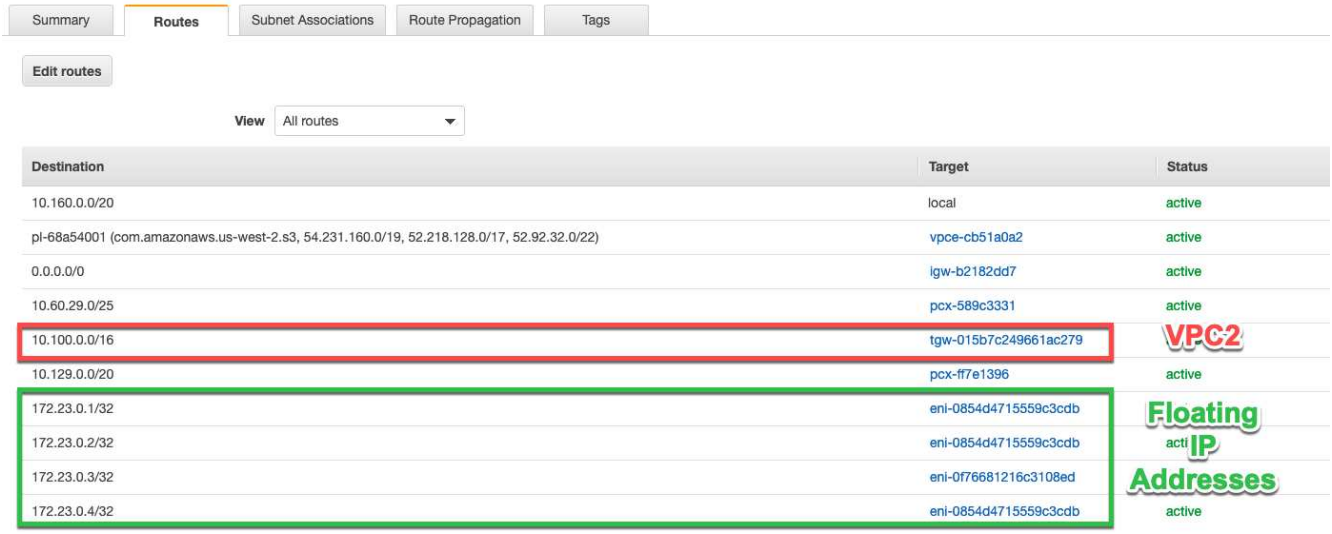
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.




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

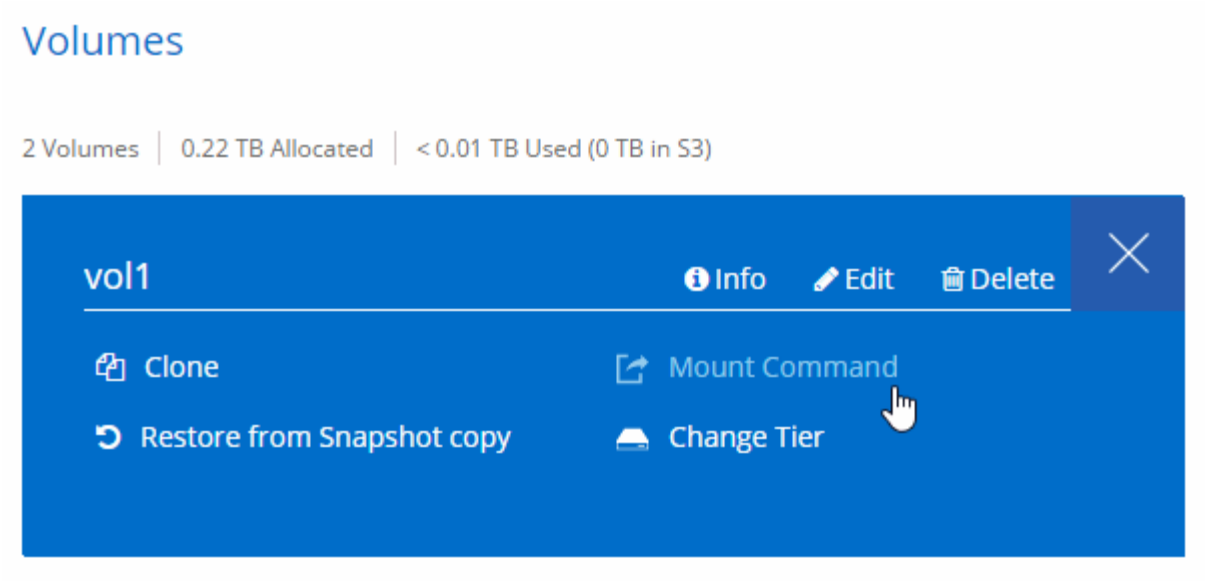
   Questo passaggio è importante perché completa il routing tra i VPC.

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




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

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




**Link correlati**

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

### Regole del gruppo di sicurezza per AWS

Cloud Manager crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita necessarie per il corretto funzionamento di Connector e Cloud Volumes ONTAP. 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

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

| Protocollo | Porta | Scopo |
|---|---|---|
| Tutti gli ICMP | Tutto | Eseguire il ping dell'istanza |
| HTTP | 80 | Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster |
| HTTPS | 443 | Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster |
| SSH | 22 | Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi |
| TCP | 111 | Chiamata a procedura remota per NFS |

| Protocollo | Porta | Scopo |
|---|---|---|
| TCP | 139 | Sessione del servizio NetBIOS per CIFS |
| TCP | 161-162 | Protocollo di gestione di rete semplice |
| TCP | 445 | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| TCP | 635 | Montaggio NFS |
| TCP | 749 | Kerberos |
| TCP | 2049 | Daemon del server NFS |
| TCP | 3260 | Accesso iSCSI tramite LIF dei dati iSCSI |
| TCP | 4045 | Daemon di blocco NFS |
| TCP | 4046 | Network status monitor per NFS |
| TCP | 10000 | Backup con NDMP |
| TCP | 11104 | Gestione delle sessioni di comunicazione tra cluster per SnapMirror |
| TCP | 11105 | Trasferimento dei dati SnapMirror con LIF intercluster |
| UDP | 111 | Chiamata a procedura remota per NFS |
| UDP | 161-162 | Protocollo di gestione di rete semplice |
| UDP | 635 | Montaggio NFS |
| UDP | 2049 | Daemon del server NFS |
| UDP | 4045 | Daemon di blocco NFS |
| UDP | 4046 | Network status monitor per NFS |
| UDP | 4049 | Protocollo NFS rquotad |

### Regole in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP 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 |
|---|---|---|---|---|---|
| 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) |
| DHCP | UDP | 68 | LIF di gestione dei nodi | DHCP | Client DHCP per la prima installazione |
| DHCPS | UDP | 67 | LIF di gestione dei nodi | DHCP | Server DHCP |
| DNS | UDP | 53 | LIF di gestione dei nodi e LIF dei dati (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | LIF di gestione dei nodi | Server di destinazione | Copia NDMP |
| SMTP | TCP | 25 | LIF di gestione dei nodi | Server di posta | Gli avvisi SMTP possono essere utilizzati per AutoSupport |
| 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

L'origine delle regole in entrata è 0.0.0.0/0.

| Protocollo | Porta | Scopo |
|---|---|---|
| SSH | 22 | Connessioni SSH al mediatore ha |
| TCP | 3000 | 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 | Scarica gli aggiornamenti per il mediatore |
| HTTPS | 443 | Servizi API AWS | Assistenza per il failover dello storage |
| UDP | 53 | Servizi API AWS | 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 del 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 |

#### Regole per il connettore

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

### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

| 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 e alle connessioni da Cloud Compliance |
| HTTPS | 443 | Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale |
| TCP | 3128 | Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy |

### Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 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 |

### 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 la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

| Servizio | Protocollo | Porta | Destinazione | Scopo |
|---|---|---|---|---|
| Active Directory | TCP | 88 | Insieme di strutture di Active Directory | Autenticazione Kerberos V. |
| | TCP | 139 | Insieme di strutture di Active Directory | Sessione del servizio NetBIOS |
| | TCP | 389 | Insieme di strutture di Active Directory | LDAP |
| | TCP | 445 | Insieme di strutture di Active Directory | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| | TCP | 464 | Insieme di strutture di Active Directory | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Insieme di strutture di Active Directory | Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS) |
| | UDP | 137 | Insieme di strutture di Active Directory | Servizio nomi NetBIOS |
| | UDP | 138 | Insieme di strutture di Active Directory | Servizio datagramma NetBIOS |
| | UDP | 464 | Insieme di strutture di Active Directory | Amministrazione delle chiavi Kerberos |
| Chiamate API e AutoSupport | HTTPS | 443 | LIF gestione cluster ONTAP e Internet in uscita | Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp |
| Chiamate API | TCP | 3000 | LIF gestione cluster ONTAP | Chiamate API a ONTAP |
| | TCP | 8088 | Backup su S3 | API chiama il backup in S3 |
| DNS | UDP | 53 | DNS | Utilizzato per la risoluzione DNS da parte di Cloud Manager |
| Conformità al cloud | HTTP | 80 | Istanza di Cloud Compliance | Conformità del cloud per Cloud Volumes ONTAP |

## 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 Cloud Manager e Cloud Volumes ONTAP o in un altro account AWS.

   "Documentazione AWS: Customer Master Keys (CMK)"

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

   L'aggiunta del ruolo IAM come utente chiave consente a Cloud Manager di utilizzare la 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.

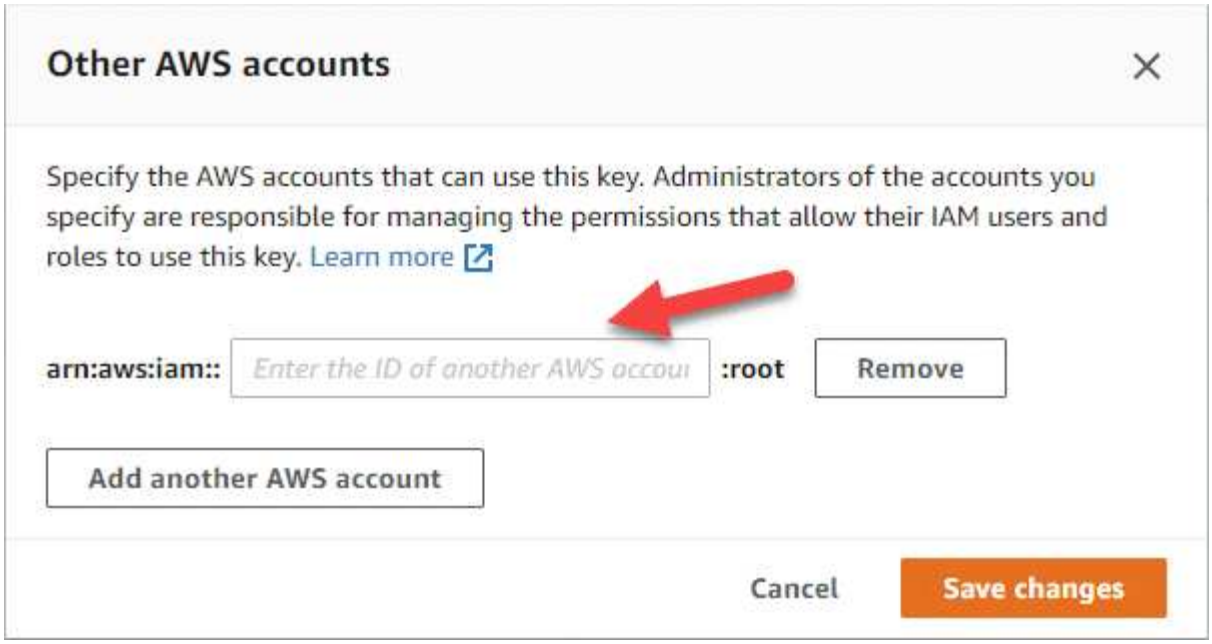
   b. Selezionare la chiave.

   c. Nel riquadro **General Configuration** (Configurazione generale), copiare l'ARN della chiave.

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

   d. Nel riquadro **altri account AWS**, aggiungere l'account AWS che fornisce le autorizzazioni a Cloud Manager.

      Nella maggior parte dei casi, si tratta dell'account in cui risiede Cloud Manager. Se Cloud Manager non fosse installato in AWS, sarebbe l'account per cui hai fornito le chiavi di accesso AWS a Cloud Manager.




e. Passare ora all'account AWS che fornisce le autorizzazioni a Cloud Manager e aprire la console IAM.

f. Creare un criterio IAM che includa le autorizzazioni elencate di seguito.

g. Allegare il criterio al ruolo IAM o all'utente IAM che fornisce le autorizzazioni a Cloud Manager.

   Il seguente criterio fornisce le autorizzazioni necessarie a Cloud Manager 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: Consentire agli account AWS esterni di accedere a un CMK".

## 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.

### 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 Cloud Manager.

#### Prima di iniziare

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- 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".
- Se si desidera avviare un sistema BYOL, è necessario disporre del numero di serie a 20 cifre (chiave di licenza).
- Se si desidera utilizzare CIFS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP in AWS".

#### A proposito di questa attività

Subito dopo aver creato l'ambiente di lavoro, Cloud Manager avvia un'istanza di test nel VPC specificato per verificare la connettività. Se l'esito è positivo, Cloud Manager termina immediatamente l'istanza e avvia l'implementazione del sistema Cloud Volumes ONTAP. Se Cloud Manager 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. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP nodo singolo**.
3. **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:

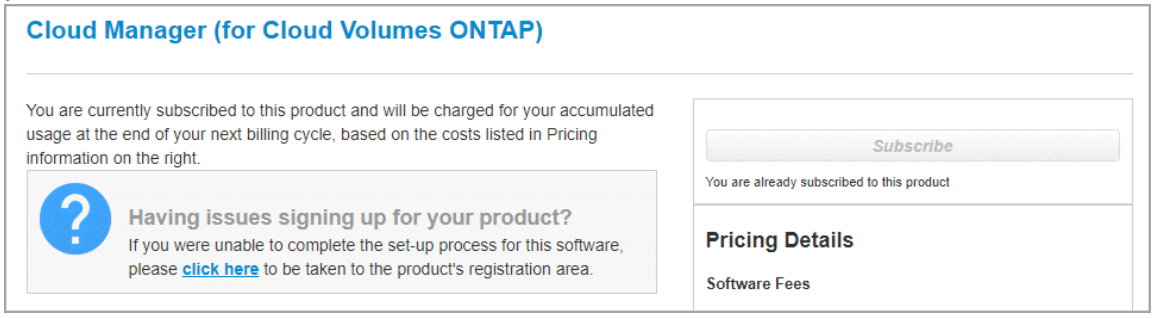
| Campo | Descrizione |
|---|---|
| Nome ambiente di lavoro | Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione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

| Campo | Descrizione |
| --- | --- |
| Aggiungere tag | I tag AWS sono metadati per le risorse AWS. Cloud Manager aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ogni 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 di OnCommand o la relativa CLI. |
| 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 abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, selezionare le credenziali AWS associate a un abbonamento a Cloud Volumes ONTAP dal marketplace AWS. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata."Scopri come aggiungere ulteriori credenziali AWS a Cloud Manager". |

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

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

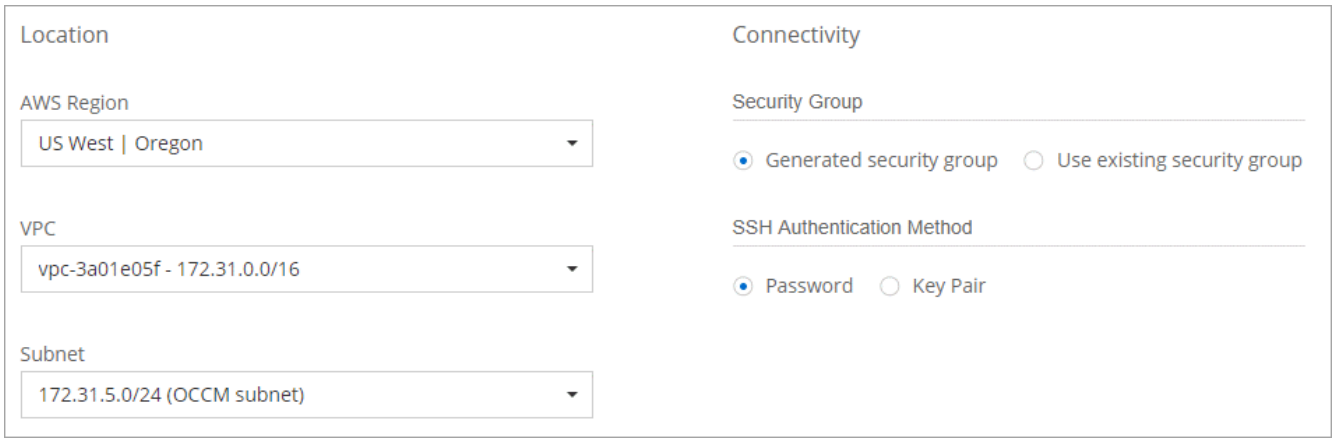
Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS Marketplace informa gli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi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




4. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla conformità al cloud".
   - "Scopri di più sul backup nel cloud".
   - "Scopri di più sul monitoraggio".

5. **Location & Connectivity** (posizione e connettività): Inserire le informazioni di rete registrate nel foglio di lavoro AWS.

   La seguente immagine mostra la pagina compilata:




6. **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".

7. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

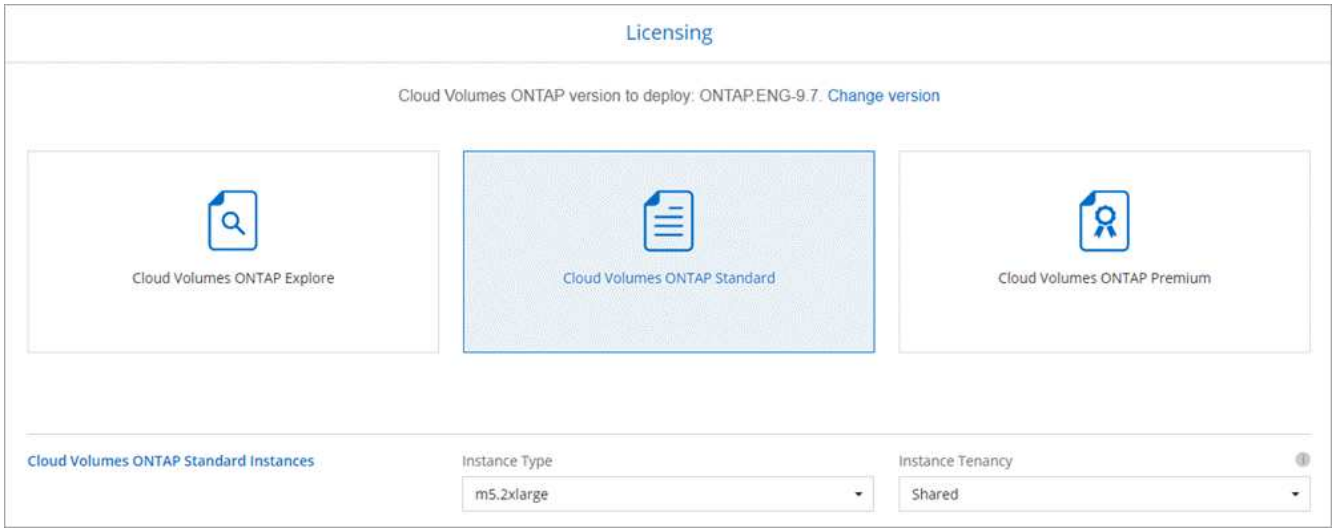
8. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

9. **Ruolo IAM**: Devi mantenere l'opzione predefinita per consentire a Cloud Manager 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".

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




Se le esigenze cambiano dopo l'avvio dell'istanza, è possibile modificare il tipo di licenza o di istanza in un secondo momento.

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager 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 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release 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, una dimensione per ciascun disco e se attivare il tiering dei dati.

    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 eventuali aggregati aggiuntivi creati da Cloud Manager 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 AWS".

    - 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".

12. **Write Speed & WORM**: Scegliere **Normal** o **High** write speed e attivare lo storage write once, Read Many (WORM), se lo si desidera.

    La scelta di una velocità di scrittura è supportata solo nei sistemi a nodo singolo.

    "Scopri di più sulla velocità di scrittura".

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

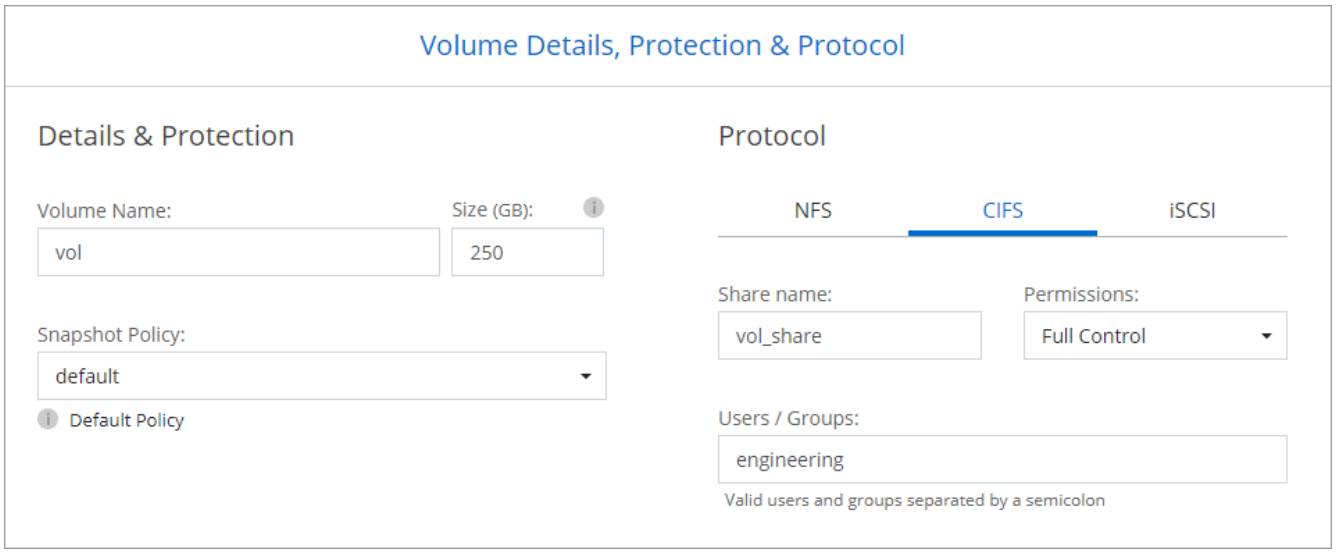
"Scopri di più sullo storage WORM".

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

    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, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella 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, Cloud Manager 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:




14. **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 "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni. |

15. **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".

16. **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 rivedere i dettagli sul supporto e le risorse AWS che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

**Risultato**

Cloud Manager 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 lanciare una coppia Cloud Volumes ONTAP ha in AWS, è necessario creare un ambiente di lavoro ha in Cloud Manager.

**Prima di iniziare**

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

  > Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- 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".
- Se sono state acquistate licenze BYOL, è necessario disporre di un numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.
- Se si desidera utilizzare CIFS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP in AWS".

**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, Cloud Manager avvia un'istanza di test nel VPC specificato per verificare la connettività. Se l'esito è positivo, Cloud Manager termina immediatamente l'istanza e avvia

l'implementazione del sistema Cloud Volumes ONTAP. Se Cloud Manager 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. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP nodo singolo**.
3. **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.

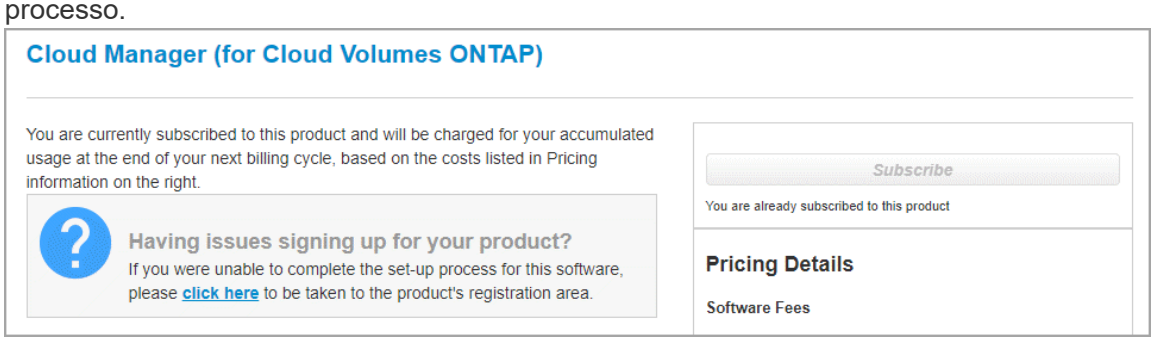
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

| Campo | Descrizione |
|---|---|
| Nome ambiente di lavoro | Cloud Manager 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. Cloud Manager aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ogni 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 di OnCommand o la relativa CLI. |
| 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 abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, selezionare le credenziali AWS associate a un abbonamento a Cloud Volumes ONTAP dal marketplace AWS. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata."Scopri come aggiungere ulteriori credenziali AWS a Cloud Manager". |

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

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

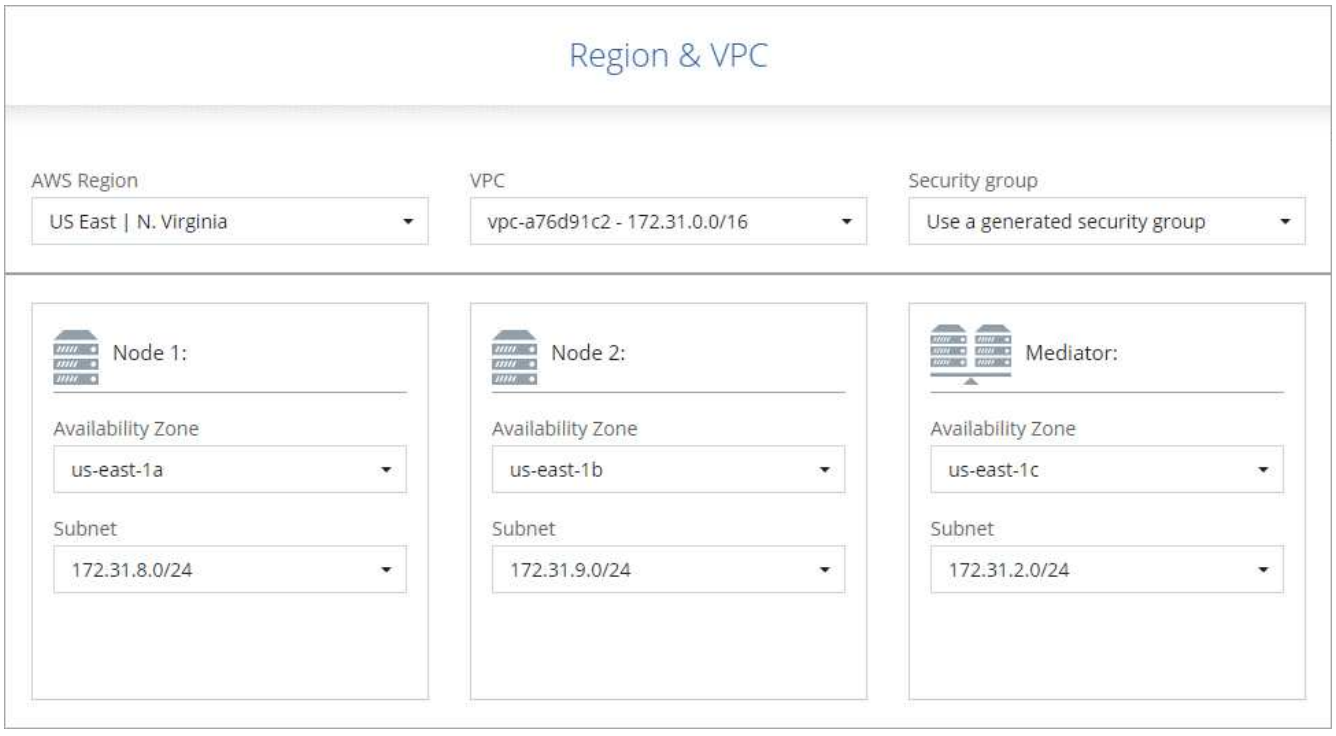
Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS Marketplace informa gli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi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




4. **Servizi**: Consente di abilitare o disabilitare i singoli servizi che non si desidera utilizzare con questo sistema Cloud Volumes ONTAP.
   - "Scopri di più sulla conformità al cloud".
   - "Scopri di più sul backup nel cloud".
   - "Scopri di più sul monitoraggio".
5. **Modelli di implementazione ha**: Scegliere una configurazione ha.

   Per una panoramica dei modelli di implementazione, vedere "Cloud Volumes ONTAP ha per AWS".
6. **Regione e VPC**: Inserire le informazioni di rete registrate nel foglio di lavoro AWS.

   La seguente immagine mostra la pagina compilata per una configurazione AZ multipla:



7. **Connettività e autenticazione SSH**: Scegliere i metodi di connessione per la coppia ha e il mediatore.
8. **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".

9. **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".

10. **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".

11. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

    Per informazioni sul funzionamento delle licenze, vedere "Licensing".

    Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

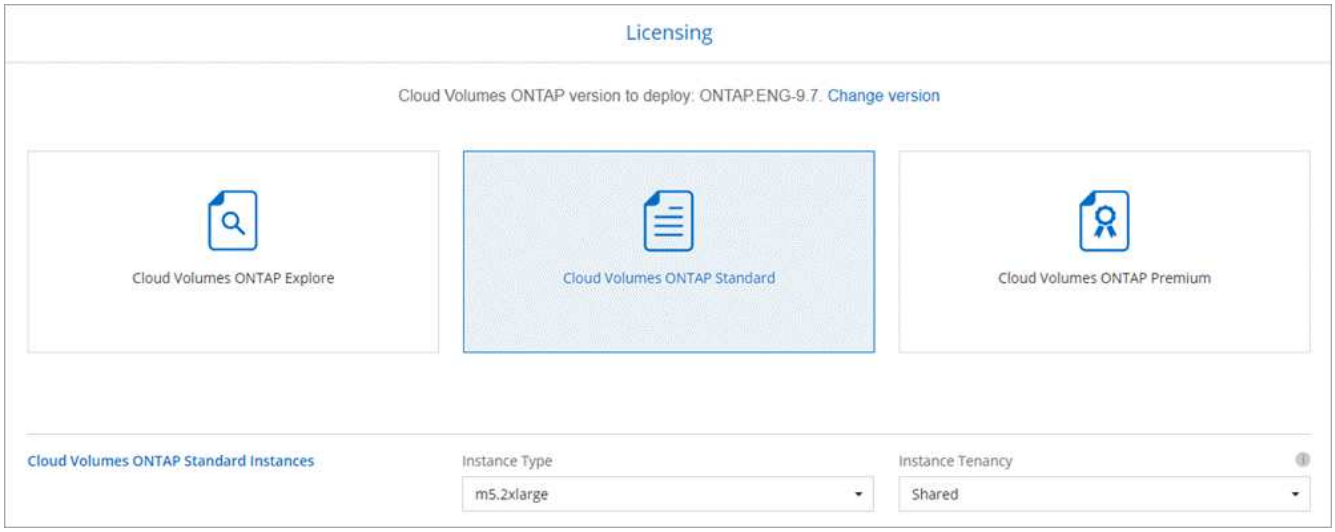
12. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

13. **Ruolo IAM**: Devi mantenere l'opzione predefinita per consentire a Cloud Manager di creare i ruoli 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".

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




Se le esigenze cambiano dopo l'avvio delle istanze, è possibile modificare il tipo di licenza o di istanza in un secondo momento.

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager 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 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

15. **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.

    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 eventuali aggregati aggiuntivi creati da Cloud Manager 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 AWS".

    - 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".

16. **WORM**: Attivare lo storage write once, Read Many (WORM), se lo si desidera.

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

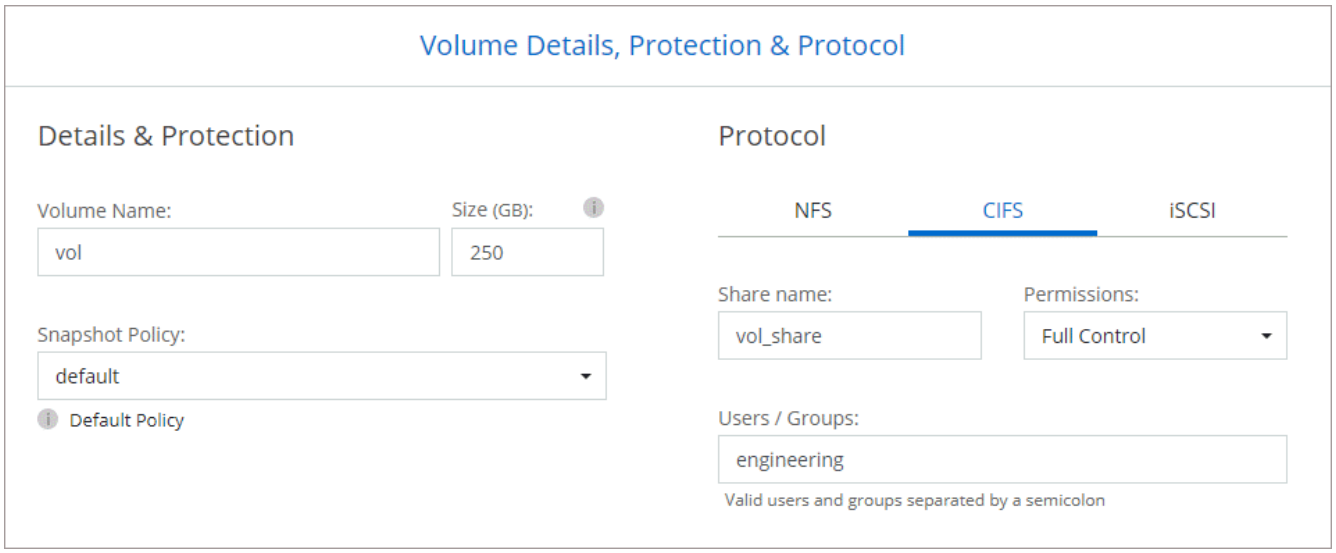
    "Scopri di più sullo storage WORM".

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

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, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella 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, Cloud Manager 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:




18. **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 "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni. |

19. **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".

20. **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 rivedere i dettagli sul supporto e le risorse AWS che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

**Risultato**

Cloud Manager 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 ad utilizzare Azure

## Introduzione a Cloud Volumes ONTAP per 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".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

### Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

### 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 VNET di destinazione in modo che il connettore e Cloud Volumes ONTAP possano contattare diversi endpoint.

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "Il connettore e Cloud Volumes ONTAP".

"Scopri di più sui requisiti di rete".

**Avviare Cloud Volumes ONTAP utilizzando Cloud Manager**

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**

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

## Pianificazione della 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.

### Scelta di un tipo di licenza

Cloud Volumes ONTAP è disponibile in due opzioni di prezzo: Pay-as-you-go e Bring Your Own License (BYOL). Per il pay-as-you-go, puoi scegliere tra tre licenze: Explore, Standard o Premium. Ogni licenza offre diverse capacità e opzioni di calcolo.

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 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 9.7 in Azure"

### Dimensionamento del 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

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

I sistemi HA utilizzano i blob di pagina Premium. Nel frattempo, i sistemi a nodo singolo possono utilizzare due 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?".

### Dimensioni del disco Azure

Quando si avviano le istanze di Cloud Volumes ONTAP, è necessario scegliere la dimensione predefinita del disco per gli aggregati. Cloud Manager 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 dischi da 1 TB può offrire prestazioni migliori rispetto ai dischi da 500 GB, 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"

### Scelta di una configurazione che supporti Flash cache

Una configurazione Cloud Volumes ONTAP in Azure include lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance. "Scopri di più su Flash cache".

### Foglio di lavoro con le informazioni di rete di Azure

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) | |

### Scelta della velocità di scrittura

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. 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.

### Differenza tra la velocità di scrittura normale e l'alta velocità di scrittura

Quando si sceglie la normale velocità di scrittura, i dati vengono scritti direttamente su disco, riducendo così la probabilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati nel buffer prima che vengano scritti su disco, garantendo prestazioni di scrittura più rapide. A causa di questo caching, vi è la possibilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

La quantità di dati che è possibile perdere in caso di interruzione non pianificata del sistema è l'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'azione di scrittura dei dati bufferizzati su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale condizione si verifica per prima). Tuttavia, le performance del volume di AWS EBS possono influire sul tempo di elaborazione dei punti di coerenza.

### Quando utilizzare un'elevata velocità di scrittura

L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide e se si può resistere al rischio di perdita di dati in caso di un'interruzione non pianificata del sistema.

### Consigli quando si utilizza un'elevata velocità di scrittura

Se si attiva l'alta velocità di scrittura, è necessario garantire la protezione in scrittura a livello di applicazione.

### Scelta di 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 crei un volume in Cloud Manager, puoi scegliere un profilo che abiliti queste funzionalità o un profilo che le disabiliti. 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 implementare e gestire Cloud Volumes ONTAP in Azure

Configura la tua rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente. Ciò include il collegamento in rete per il connettore e Cloud Volumes ONTAP.

### Requisiti per Cloud Volumes ONTAP

I seguenti requisiti di rete devono essere soddisfatti in Azure.

**Accesso a Internet in uscita per Cloud Volumes ONTAP**

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

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

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

"Scopri come configurare AutoSupport".

**Gruppi di sicurezza**

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento alle regole del gruppo di protezione elencate di seguito.

**Numero di indirizzi IP**

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

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

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

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

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

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

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

Queste autorizzazioni sono incluse nella versione più recente "Policy di Cloud Manager".

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

### Connessioni a sistemi ONTAP in altre reti

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

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

### Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.

Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

#### Connessioni alle reti di destinazione

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

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

#### Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in Azure:

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

| Endpoint | Scopo |
| --- | --- |
| https://management.microsoftazure.de https://login.microsoftonline.de | Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania. |
| https://management.usgovcloudapi.net https://login.microsoftonline.com | Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov. |
| https://api.services.cloud.netapp.com:443 | Richieste API a NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Fornisce l'accesso a immagini, manifesti e modelli software. |
| https://repo.cloud.support.netapp.com | Utilizzato per scaricare le dipendenze di Cloud Manager. |
| http://repo.mysql.com/ | Utilizzato per scaricare MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP. |
| https://cloudmanagerinfraprod.azurecr.io | Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di eseguire lo streaming dei dati dai record di audit. |
| https://cloudmanager.cloud.netapp.com | Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central. |
| https://netapp-cloud-account.auth0.com | Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata. |
| https://mysupport.netapp.com | Comunicazione con NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema. |
| https://ipa-signer.cloudmanager.netapp.com | Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident. |
| *.blob.core.windows.net | Richiesto per coppie ha quando si utilizza un proxy. |

| Endpoint | Scopo |
| --- | --- |
| Varie sedi di terze parti, ad esempio:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Le sedi di terze parti sono soggette a modifiche. | Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti. |

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

| Endpoint | Scopo |
| --- | --- |
| L'host del connettore | Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.<br>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:<br>• Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale<br>• Un IP pubblico funziona in qualsiasi scenario di rete<br>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati. |
| https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com | Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central. |
| https://widget.intercom.io | Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp. |

### Regole del gruppo di sicurezza per Cloud Volumes ONTAP

Cloud Manager crea gruppi di sicurezza Azure che includono le regole in entrata e in uscita necessarie per il corretto funzionamento di Cloud Volumes ONTAP. 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.

#### Regole in entrata per sistemi a nodo singolo

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

| 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 |
| 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 | 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 |

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

#### Regole in entrata per i sistemi ha

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

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 | 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 |
| 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) |
| DHCP | 68 | UDP | LIF di gestione dei nodi | DHCP | Client DHCP per la prima installazione |

| Servizio | Porta | Protocollo | Origine | Destinazione | Scopo |
|---|---|---|---|---|---|
| DHCPS | 67 | UDP | LIF di gestione dei nodi | DHCP | 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 |

### Regole del gruppo di sicurezza per il connettore

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

#### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

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

#### Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 connettore 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 la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

| Servizio | Porta | Protocollo | Destinazione | Scopo |
|---|---|---|---|---|
| Active Directory | 88 | TCP | Insieme di strutture di Active Directory | Autenticazione Kerberos V. |
| | 139 | TCP | Insieme di strutture di Active Directory | Sessione del servizio NetBIOS |
| | 389 | TCP | Insieme di strutture di Active Directory | LDAP |
| | 445 | TCP | Insieme di strutture di Active Directory | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| | 464 | TCP | Insieme di strutture di Active Directory | Kerberos V change & set password (SET_CHANGE) |
| | 749 | TCP | Insieme di strutture di Active Directory | Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS) |
| | 137 | UDP | Insieme di strutture di Active Directory | Servizio nomi NetBIOS |
| | 138 | UDP | Insieme di strutture di Active Directory | Servizio datagramma NetBIOS |
| | 464 | UDP | Insieme di strutture di Active Directory | Amministrazione delle chiavi Kerberos |

| Servizio | Porta | Protocollo | Destinazione | Scopo |
|---|---|---|---|---|
| Chiamate API e AutoSupport | 443 | HTTPS | LIF gestione cluster ONTAP e Internet in uscita | Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp |
| Chiamate API | 3000 | TCP | LIF gestione cluster ONTAP | Chiamate API a ONTAP |
| DNS | 53 | UDP | DNS | Utilizzato per la risoluzione DNS da parte di Cloud Manager |

## 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 Cloud Manager.

### Prima di iniziare

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- 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".
- Per implementare un sistema BYOL, è necessario il numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.

### A proposito di questa attività

Quando Cloud Manager crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti Azure, come 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**
>
> L'implementazione di Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente non è consigliata a causa del rischio di perdita di dati. Sebbene il rollback sia attualmente disattivato per impostazione predefinita quando si utilizza l'API per la distribuzione in un gruppo di risorse esistente, l'eliminazione di Cloud Volumes ONTAP potenzialmente eliminerà altre risorse da quel gruppo condiviso.
>
> La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Questa è l'opzione predefinita e consigliata solo quando si implementa Cloud Volumes ONTAP in Azure da Cloud Manager.

### Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Microsoft Azure** e **nodo singolo Cloud Volumes ONTAP** o **alta disponibilità Cloud Volumes ONTAP**.
3. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e la sottoscrizione di Azure, specificare il nome del cluster e del gruppo di risorse, aggiungere tag, se necessario, quindi specificare le credenziali.

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

| Campo | Descrizione |
|---|---|
| Nome ambiente di lavoro | Cloud Manager 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. |
| Nome gruppo di risorse | Mantenere il nome predefinito per il nuovo gruppo di risorse o deselezionare **Usa predefinito** e immettere il proprio nome per il nuovo gruppo di risorse. 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 utilizzando l'API, non è consigliabile a causa del rischio di perdita di dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. |
| Tag | I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, Cloud Manager 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 di OnCommand o la relativa CLI. |
| 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/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla conformità al cloud".
   - "Scopri di più sul backup nel cloud".
5. **Location & Connectivity** (posizione e connettività): Selezionare una posizione e un gruppo di sicurezza e selezionare la casella di controllo per confermare la connettività di rete tra Cloud Manager e la posizione di destinazione.

6. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

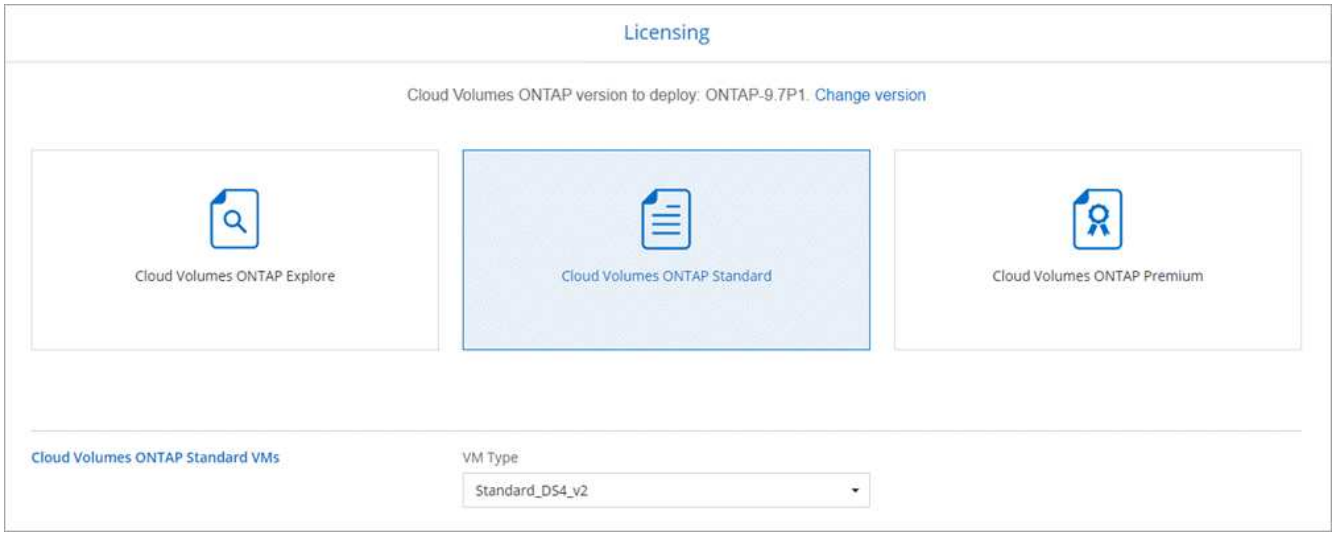
   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

7. **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.

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




   Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

   > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager 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 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

9. **Iscriviti al marketplace Azure**: Segui la procedura se Cloud Manager non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
10. **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 eventuali aggregati aggiuntivi creati da Cloud Manager 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".

11. **Write Speed & WORM** (solo sistemi a nodo singolo): Scegliere **normale** o **alta** velocità di scrittura e attivare lo storage WORM (Write Once, Read Many), se desiderato.

    La scelta di una velocità di scrittura è supportata solo nei sistemi a nodo singolo.

    "Scopri di più sulla velocità di scrittura".

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

    "Scopri di più sullo storage WORM".

12. **Secure Communication to Storage & WORM** (solo ha): 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 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".

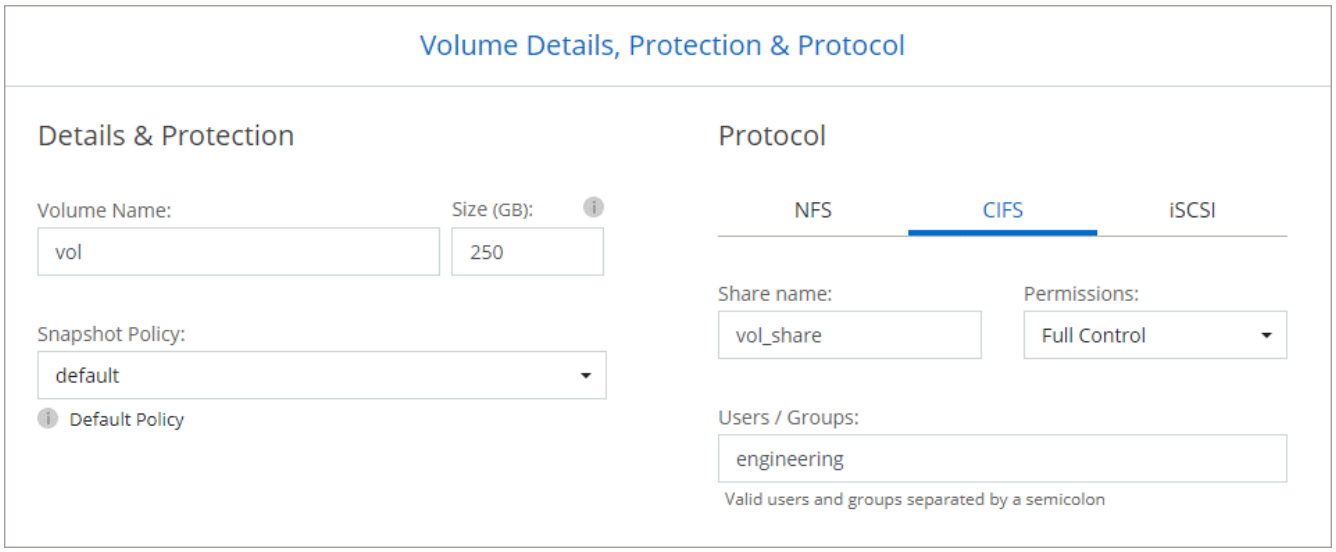
13. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    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, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella 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. |

| Campo | Descrizione |
| --- | --- |
| 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, Cloud Manager 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:




14. **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. |

| Campo | Descrizione |
| --- | --- |
| 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.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["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 "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni. |

15. **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".

16. **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 rivedere i dettagli sul supporto e le risorse di Azure che Cloud Manager acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

**Risultato**

Cloud Manager 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 GCP

## Introduzione a Cloud Volumes ONTAP per Google Cloud

Inizia a utilizzare Cloud Volumes ONTAP per GCP 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 GCP".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

### Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. 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 in modo che il connettore e Cloud Volumes ONTAP possano contattare diversi endpoint.

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "Il connettore e Cloud Volumes ONTAP".

"Scopri di più sui requisiti di rete".

### Configurare GCP per il tiering dei dati

È necessario soddisfare due requisiti per tierare i dati cold da Cloud Volumes ONTAP a uno storage a oggetti a basso costo (un bucket di storage cloud di Google):

1. "Configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google".
2. "Impostare un account di servizio per il tiering dei dati":
   - Assegnare il ruolo predefinito *Storage Admin* all'account del servizio di tiering.
   - Aggiungere l'account del servizio Connector come *Service account User* all'account del servizio di tiering.

     È possibile fornire il ruolo dell'utente "nel passaggio 3 della procedura guidata quando si crea l'account

del servizio di tiering", o. "assegnare il ruolo dopo la creazione dell'account di servizio".

Sarà necessario selezionare l'account del servizio di tiering in un secondo momento quando si crea un ambiente di lavoro Cloud Volumes ONTAP.

Se non si attiva il tiering dei dati e si seleziona un account di servizio quando si crea il sistema Cloud Volumes ONTAP, è necessario spegnere il sistema e aggiungere l'account di servizio a Cloud Volumes ONTAP dalla console GCP.

**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)

**Avviare Cloud Volumes ONTAP utilizzando Cloud Manager**

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**

- "Valutazione"
- "Creazione di un connettore da Cloud Manager"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa Cloud Manager con le autorizzazioni GCP"

## Pianificazione della 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.

### Scelta di un tipo di licenza

Cloud Volumes ONTAP è disponibile in due opzioni di prezzo: Pay-as-you-go e Bring Your Own License (BYOL). Per il pay-as-you-go, puoi scegliere tra tre licenze: Explore, Standard o Premium. Ogni licenza offre diverse capacità e opzioni di calcolo.

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 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 9.7 in GCP"

### Dimensionamento del 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 *dischi persistenti SSD Zonal* o *dischi persistenti standard Zonal*.

I dischi persistenti SSD sono ideali per i carichi di lavoro che richiedono elevati tassi di IOPS casuali, mentre 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)".

#### Dimensione del disco GCP

Quando si implementa un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. In seguito, puoi lasciare che Cloud Manager 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"

### Foglio di lavoro delle informazioni di rete GCP

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

### Scelta della velocità di scrittura

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. 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.

#### Differenza tra la velocità di scrittura normale e l'alta velocità di scrittura

Quando si sceglie la normale velocità di scrittura, i dati vengono scritti direttamente su disco, riducendo così la probabilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati nel buffer prima che vengano scritti su disco, garantendo prestazioni di scrittura più rapide. A causa di questo caching, vi è la possibilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

La quantità di dati che è possibile perdere in caso di interruzione non pianificata del sistema è l'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'azione di scrittura dei dati bufferizzati su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale condizione si verifica per prima). Tuttavia, le performance del volume di AWS EBS possono influire sul tempo di elaborazione dei punti di coerenza.

#### Quando utilizzare un'elevata velocità di scrittura

L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide e se si può resistere al rischio di perdita di dati in caso di un'interruzione non pianificata del sistema.

#### Consigli quando si utilizza un'elevata velocità di scrittura

Se si attiva l'alta velocità di scrittura, è necessario garantire la protezione in scrittura a livello di applicazione.

### Scelta di 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 crei un volume in Cloud Manager, puoi scegliere un profilo che abiliti queste funzionalità o un profilo che le disabiliti. 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 implementare e gestire Cloud Volumes ONTAP in GCP

Configura la tua rete della piattaforma cloud Google in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente. Ciò include il collegamento in rete per il connettore e Cloud Volumes ONTAP.

### Requisiti per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in GCP.

**Cloud privato virtuale**

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

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".

L'unico requisito per l'utilizzo di un VPC condiviso è fornire "Ruolo di Compute Network User" All'account del servizio Connector. Cloud Manager necessita di queste autorizzazioni per eseguire query su firewall, VPC e subnet nel progetto host.

**Accesso a Internet in uscita per Cloud Volumes ONTAP**

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

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

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

"Scopri come configurare AutoSupport".

**Numero di indirizzi IP**

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

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

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

### Regole del firewall

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

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

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

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

### Connessioni a sistemi ONTAP in altre reti

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

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

## Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.

Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

#### Connessione alle reti di destinazione

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

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

#### Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in GCP:

| Endpoint | Scopo |
|---|---|
| https://www.googleapis.com | Consente al connettore di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP. |
| https://api.services.cloud.netapp.com:443 | Richieste API a NetApp Cloud Central. |

| Endpoint | Scopo |
| --- | --- |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Fornisce l'accesso a immagini, manifesti e modelli software. |
| https://repo.cloud.support.netapp.com | Utilizzato per scaricare le dipendenze di Cloud Manager. |
| http://repo.mysql.com/ | Utilizzato per scaricare MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP. |
| https://cloudmanagerinfraprod.azurecr.io | Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di eseguire lo streaming dei dati dai record di audit. |
| https://cloudmanager.cloud.netapp.com | Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central. |
| https://netapp-cloud-account.auth0.com | Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata. |
| https://mysupport.netapp.com | Comunicazione con NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema. |
| https://ipa-signer.cloudmanager.netapp.com | Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident. |
| Varie sedi di terze parti, ad esempio:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Le sedi di terze parti sono soggette a modifiche. | Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti. |

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

| Endpoint | Scopo |
| --- | --- |
| L'host del connettore | Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.<br><br>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:<br><br>• Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale<br>• Un IP pubblico funziona in qualsiasi scenario di rete<br><br>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati. |
| https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com | Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central. |
| https://widget.intercom.io | Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp. |

### Regole firewall per Cloud Volumes ONTAP

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

Le regole del firewall per Cloud Volumes ONTAP richiedono regole sia in entrata che in uscita.

#### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

| Protocollo | Porta | Scopo |
| --- | --- | --- |
| Tutti gli ICMP | Tutto | Eseguire il ping dell'istanza |
| HTTP | 80 | Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster |
| HTTPS | 443 | Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster |
| SSH | 22 | Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi |
| TCP | 111 | Chiamata a procedura remota per NFS |
| 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 |

| Protocollo | Porta | Scopo |
|---|---|---|
| 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 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 |
|---|---|---|---|---|---|
| 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) |
| DHCP | UDP | 68 | LIF di gestione dei nodi | DHCP | Client DHCP per la prima installazione |
| DHCPS | UDP | 67 | LIF di gestione dei nodi | DHCP | Server DHCP |
| DNS | UDP | 53 | LIF di gestione dei nodi e LIF dei dati (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | LIF di gestione dei nodi | Server di destinazione | Copia NDMP |
| SMTP | TCP | 25 | LIF di gestione dei nodi | Server di posta | Gli avvisi SMTP possono essere utilizzati per AutoSupport |
| 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 firewall per il connettore

Le regole firewall per il connettore richiedono regole sia in entrata che in uscita.

#### Regole in entrata

L'origine delle regole in entrata nelle regole firewall predefinite è 0.0.0.0/0.

| 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

Le regole firewall predefinite per il connettore aprono 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

Le regole firewall predefinite per il connettore includono 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 richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

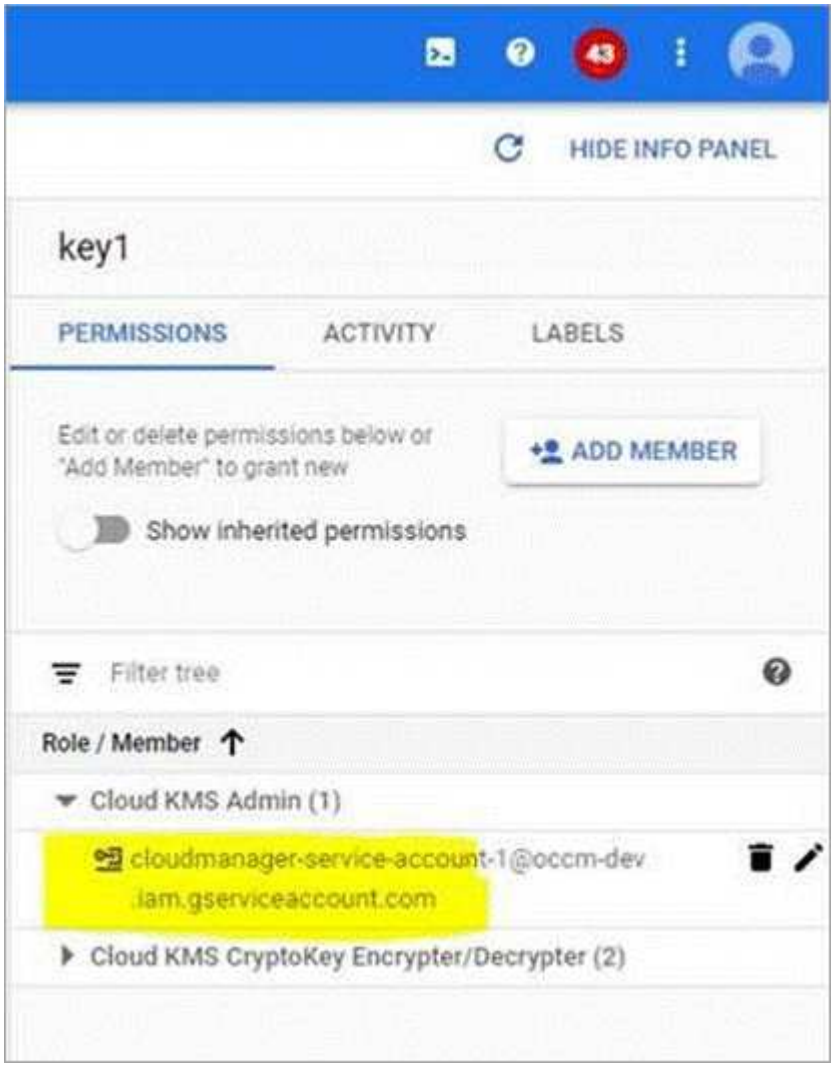
| Servizio | Protocollo | Porta | Destinazione | Scopo |
|---|---|---|---|---|
| Active Directory | TCP | 88 | Insieme di strutture di Active Directory | Autenticazione Kerberos V. |
| | TCP | 139 | Insieme di strutture di Active Directory | Sessione del servizio NetBIOS |
| | TCP | 389 | Insieme di strutture di Active Directory | LDAP |
| | TCP | 445 | Insieme di strutture di Active Directory | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| | TCP | 464 | Insieme di strutture di Active Directory | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Insieme di strutture di Active Directory | Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS) |
| | UDP | 137 | Insieme di strutture di Active Directory | Servizio nomi NetBIOS |
| | UDP | 138 | Insieme di strutture di Active Directory | Servizio datagramma NetBIOS |
| | UDP | 464 | Insieme di strutture di Active Directory | Amministrazione delle chiavi Kerberos |
| Chiamate API e AutoSupport | HTTPS | 443 | LIF gestione cluster ONTAP e Internet in uscita | Chiamate API a GCP e ONTAP e invio di messaggi AutoSupport a NetApp |
| Chiamate API | TCP | 3000 | LIF gestione cluster ONTAP | Chiamate API a ONTAP |
| DNS | UDP | 53 | DNS | Utilizzato per la risoluzione DNS da parte di Cloud Manager |

## 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 le API di Cloud Manager 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. Assegnare all'account del servizio Connector l'autorizzazione per utilizzare la chiave di crittografia.




2. Ottenere l'id della chiave richiamando il comando get per l'API /gcp/vsa/metadata/gcp-Encryption-keys.
3. Utilizzare il parametro "GcpEncryption" con la richiesta API durante la creazione di un ambiente di lavoro.

**Esempio**

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

Fare riferimento a. "Guida per sviluppatori API" Per ulteriori informazioni sull'utilizzo del parametro "GcpEncryption".

## Avvio di Cloud Volumes ONTAP in GCP

È possibile avviare un sistema Cloud Volumes ONTAP a nodo singolo in GCP creando un ambiente di lavoro.

**Di cosa hai bisogno**

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- Si dovrebbe aver scelto una configurazione e ottenuto le informazioni di rete GCP dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Per implementare un sistema BYOL, è necessario il numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.
- Le seguenti 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)

**Fasi**

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Google Cloud** e **Cloud Volumes ONTAP**.
3. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, 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 | Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza della VM GCP. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito. |
| Aggiungi etichette | Le etichette sono metadati per le risorse GCP. Cloud Manager aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse GCP 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. |

| 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 Cloud Manager.<br><br>Se non vedi altri progetti nell'elenco a discesa, non hai ancora associato l'account del servizio Cloud Manager ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account di servizio con il ruolo di Cloud Manager a quel progetto. Dovrai ripetere questo passaggio per ogni progetto.<br><br>Questo è l'account di servizio configurato per Cloud Manager, "come descritto nel passo 2b di questa pagina".<br><br>Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento.<br><br>Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, devi selezionare un progetto GCP associato a un abbonamento a Cloud Volumes ONTAP dal mercato GCP. |

Il video seguente mostra come associare un abbonamento al Marketplace pay-as-you-go al progetto GCP:

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **Posizione e connettività**: Selezionare una posizione, scegliere un criterio firewall e selezionare la casella di controllo per confermare la connettività di rete allo storage Google Cloud per il tiering dei dati.

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

5. **License & Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

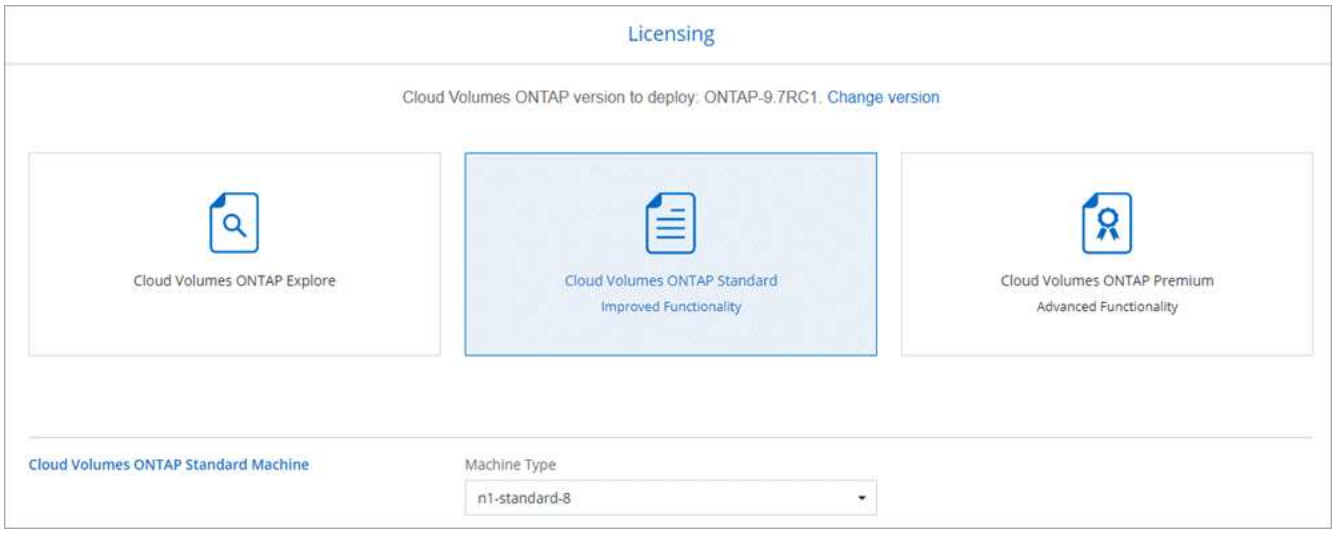
   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

6. **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.

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




Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager 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 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

8. **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 eventuali aggregati aggiuntivi creati da Cloud Manager 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 GCP".

9. **Write Speed & WORM**: Scegliere **Normal** o **High** write speed e attivare lo storage write once, Read Many (WORM), se lo si desidera.

   La scelta di una velocità di scrittura è supportata solo nei sistemi a nodo singolo.

   "Scopri di più sulla velocità di scrittura".

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

   "Scopri di più sullo storage WORM".

10. **Tiering dei dati nella piattaforma 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 di amministratore dello storage predefinito (richiesto per Cloud Volumes ONTAP 9.7) oppure selezionare un account GCP (richiesto per Cloud Volumes ONTAP 9.6).

    Tenere presente quanto segue:

- Cloud Manager 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 Cloud Manager come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da Cloud Manager.
- Per informazioni sull'aggiunta di un account GCP, vedere "Impostazione e aggiunta di account GCP 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 GCP.

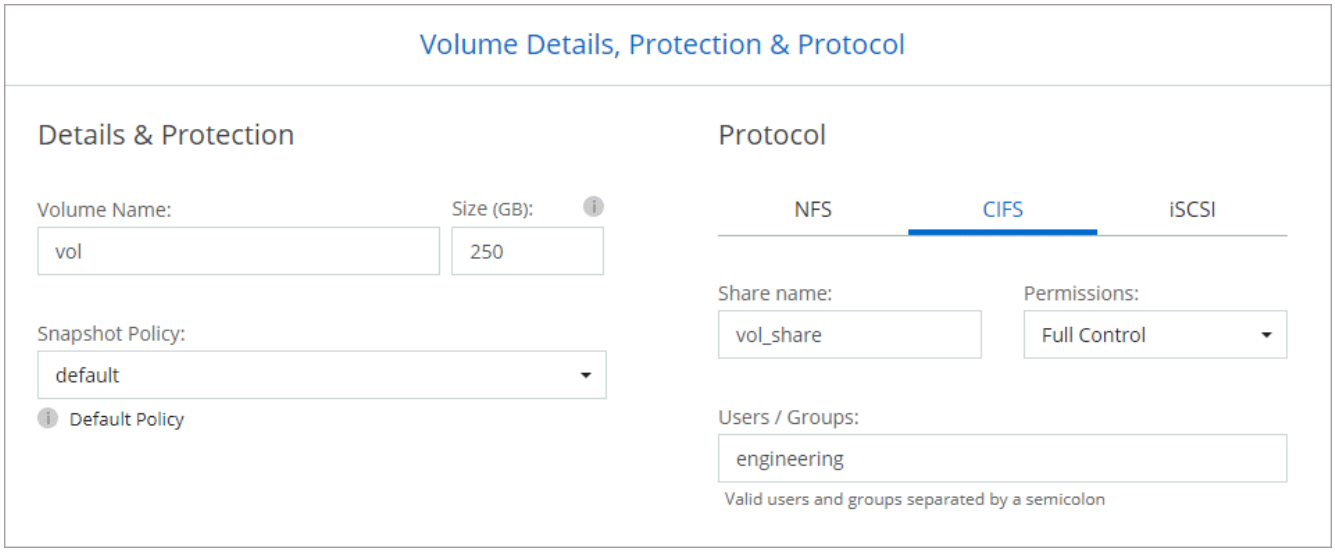
  "Scopri di più sul tiering dei dati".

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

    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, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella 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, Cloud Manager 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:




12. **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. |
| 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 "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni. |

13. **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".

14. **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 rivedere i dettagli sul supporto e le risorse GCP che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

**Risultato**

Cloud Manager 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.

# Provisioning e gestione dello storage

## Provisioning dello storage

Puoi eseguire il provisioning di storage aggiuntivo per i tuoi sistemi Cloud Volumes ONTAP da Cloud Manager gestendo volumi e aggregati.

Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da Cloud Manager. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti per i provider di cloud.

### Creazione di volumi FlexVol

Se hai bisogno di più storage dopo il lancio di un sistema Cloud Volumes ONTAP, puoi creare nuovi volumi FlexVol per NFS, CIFS o iSCSI da Cloud Manager.

**A proposito di questa attività**

Quando si crea un volume iSCSI, Cloud Manager 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.

È possibile creare ulteriori LUN da System Manager o dall'interfaccia CLI.

**Prima di iniziare**

Se si desidera utilizzare CIFS in AWS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP per AWS".

**Fasi**

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera eseguire il provisioning dei volumi FlexVol.
2. Creare un nuovo volume su qualsiasi aggregato o su un aggregato specifico:

| Azione | Fasi |
| --- | --- |
| Crea un nuovo volume e lascia che Cloud Manager scelga l'aggregato contenente | Fare clic su **Add New Volume** (Aggiungi nuovo volume). |
| Creare un nuovo volume su un aggregato specifico | a. Fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.<br>b. Fare clic sul menu per un aggregato.<br>c. Fare clic su **Create volume** (Crea volume). |

3. Inserire i dettagli del nuovo volume, quindi fare clic su **continua**.

   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, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella 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, Cloud Manager 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". |

4. Se si sceglie il protocollo CIFS e il server CIFS non è stato configurato, specificare i dettagli del server nella finestra di dialogo Crea un server CIFS, quindi fare clic su **Salva e continua**:

| 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.<br>• Per configurare AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.<br>• 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.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["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. |

| 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 "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni. |

5. Nella pagina Usage Profile (Profilo di utilizzo), Disk Type (tipo di disco) e Tiering Policy (criterio di tiering), scegliere se attivare le funzionalità di efficienza dello storage, scegliere un tipo di disco e modificare il criterio di tiering, se necessario.

   Per assistenza, fare riferimento a quanto segue:

   - "Comprensione dei profili di utilizzo dei volumi"
   - "Dimensionamento del sistema in AWS"
   - "Dimensionamento del sistema in Azure"
   - "Panoramica sul tiering dei dati"
6. Fare clic su **Go**.

**Risultato**

Cloud Volumes ONTAP esegue il provisioning del volume.

**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, è necessario utilizzare System Manager o la 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.

### Creazione di volumi FlexVol sul secondo nodo in una configurazione ha

Per impostazione predefinita, Cloud Manager crea volumi sul primo nodo in una configurazione ha. Se è necessaria una configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, è necessario creare aggregati e volumi sul secondo nodo.

**Fasi**

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome dell'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi su **Avanzate > allocazione avanzata**.
3. Fare clic su **Add aggregate** (Aggiungi aggregato), quindi creare l'aggregato.
4. Per nodo principale, scegliere il secondo nodo della coppia ha.
5. Dopo che Cloud Manager ha creato l'aggregato, selezionarlo e fare clic su **Create volume** (Crea volume).
6. Inserire i dettagli del nuovo volume, quindi fare clic su **Create** (Crea).

**Al termine**

Se necessario, è possibile creare volumi aggiuntivi su questo aggregato.

Per le coppie ha implementate in più zone di disponibilità AWS, è necessario montare il volume sui client utilizzando l'indirizzo IP mobile del nodo su cui risiede il volume.

### Creazione di aggregati

È possibile creare aggregati o lasciare che Cloud Manager lo faccia per te quando crea volumi. Il vantaggio della creazione di aggregati consiste nella possibilità di scegliere la dimensione del disco sottostante, che consente di dimensionare l'aggregato in base alla capacità o alle performance necessarie.

**Fasi**

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome dell'istanza di Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
3. Fare clic su **Add aggregate** (Aggiungi aggregato), quindi specificare i dettagli per l'aggregato.

   Per informazioni sul tipo di disco e sulle dimensioni del disco, vedere "Pianificazione della configurazione".

4. Fare clic su **Go**, quindi su **Approve and Purchase** (approva e acquista).

### Connessione di un LUN a un host

Quando si crea un volume iSCSI, Cloud Manager 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.

Tenere presente quanto segue:

1. La gestione automatica della capacità di Cloud Manager non si applica alle LUN. Quando Cloud Manager crea un LUN, disattiva la funzione di crescita automatica.
2. È possibile creare ulteriori LUN da System Manager o dall'interfaccia CLI.

**Fasi**

1. Nella pagina ambienti di lavoro, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire i volumi.
2. Selezionare un volume, quindi fare clic su **Target IQN**.
3. Fare clic su **Copy** (Copia) per copiare il nome IQN.
4. Impostare una connessione iSCSI dall'host al LUN.
   - "Configurazione iSCSI Express di ONTAP 9 per Red Hat Enterprise Linux: Avvio delle sessioni iSCSI con la destinazione"
   - "Configurazione iSCSI Express di ONTAP 9 per Windows: Avvio di sessioni iSCSI con la destinazione"

### Utilizzo di FlexCache Volumes per accelerare l'accesso ai dati

Un volume FlexCache è un volume di storage che memorizza nella cache i dati di lettura NFS da un volume di origine (o di origine). Le successive letture dei dati memorizzati nella cache consentono un accesso più rapido a tali dati.

È possibile utilizzare i volumi FlexCache per accelerare l'accesso ai dati o per trasferire il traffico dai volumi ad accesso elevato. I volumi FlexCache aiutano a migliorare le performance, soprattutto quando i client devono accedere ripetutamente agli stessi dati, perché i dati possono essere gestiti direttamente senza dover

accedere al volume di origine. I volumi FlexCache funzionano bene per i carichi di lavoro di sistema che richiedono un uso intensivo della lettura.

Cloud Manager non fornisce attualmente la gestione dei volumi FlexCache, ma è possibile utilizzare l'interfaccia CLI di ONTAP o Gestione di sistema di ONTAP per creare e gestire i volumi FlexCache:

- "Guida all'alimentazione di FlexCache Volumes per un accesso più rapido ai dati"
- "Creazione di volumi FlexCache in Gestore di sistema"

A partire dalla versione 3.7.2, Cloud Manager genera una licenza FlexCache per tutti i nuovi sistemi Cloud Volumes ONTAP. La licenza include un limite di utilizzo di 500 GB.

Per generare la licenza, Cloud Manager deve accedere a https://ipa-signer.cloudmanager.netapp.com. Assicurarsi che questo URL sia accessibile dal firewall.


## Gestione dello storage esistente

Cloud Manager consente di gestire volumi, aggregati e server CIFS. Inoltre, richiede di spostare i volumi per evitare problemi di capacità.

### Gestione dei volumi esistenti

Puoi gestire i volumi esistenti in base alle tue esigenze di storage. È possibile visualizzare, modificare, clonare, ripristinare ed eliminare i volumi.

#### Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire i volumi.
2. Gestisci i tuoi volumi:

| Attività | Azione |
| --- | --- |
| Consente di visualizzare informazioni su un volume | Selezionare un volume, quindi fare clic su **Info**. |
| Modifica di un volume (solo volumi di lettura/scrittura) | a. Selezionare un volume, quindi fare clic su **Modifica**.<br>b. Modificare la policy Snapshot del volume, la versione del protocollo NFS, l'elenco di controllo dell'accesso NFS o le autorizzazioni di condivisione, quindi fare clic su **Update** (Aggiorna).<br>Se sono necessarie policy Snapshot personalizzate, è possibile crearle utilizzando System Manager. |
| Clonare un volume | a. Selezionare un volume, quindi fare clic su **Clone**.<br>b. Modificare il nome del clone secondo necessità, quindi fare clic su **Clone**.<br>Questo processo crea un volume FlexClone. Un volume FlexClone è una copia point-in-time scrivibile efficiente in termini di spazio, in quanto utilizza una piccola quantità di spazio per i metadati e consuma solo spazio aggiuntivo quando i dati vengono modificati o aggiunti.<br>Per ulteriori informazioni sui volumi FlexClone, vedere "Guida alla gestione dello storage logico di ONTAP 9". |
| Ripristinare i dati da una copia Snapshot a un nuovo volume | a. Selezionare un volume, quindi fare clic su **Restore from Snapshot copy** (Ripristina da copia Snapshot).<br>b. Selezionare una copia Snapshot, immettere un nome per il nuovo volume, quindi fare clic su **Restore** (Ripristina). |
| Crea una copia Snapshot on-demand | a. Selezionare un volume, quindi fare clic su **Crea una copia Snapshot**.<br>b. Modificare il nome, se necessario, quindi fare clic su **Crea**. |
| Scarica il comando NFS mount | a. Selezionare un volume, quindi fare clic su **comando di montaggio**.<br>b. Fare clic su **Copy** (Copia). |
| Visualizzare l'IQN di destinazione per un volume iSCSI | a. Selezionare un volume, quindi fare clic su **Target IQN**.<br>b. Fare clic su **Copy** (Copia).<br>c. "Utilizzare IQN per connettersi al LUN dagli host". |

| Attività | Azione |
| --- | --- |
| Modificare il tipo di disco sottostante | a. Selezionare un volume, quindi fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering).<br>b. Selezionare il tipo di disco, quindi fare clic su **Cambia**.<br>Cloud Manager sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato oppure crea un nuovo aggregato per il volume. |
| Modificare la policy di tiering | a. Selezionare un volume, quindi fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering).<br>b. Fare clic su **Edit Policy** (Modifica policy).<br>c. Selezionare un altro criterio e fare clic su **Cambia**.<br>Cloud Manager sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato con il tiering oppure crea un nuovo aggregato per il volume. |
| Eliminare un volume | a. Selezionare un volume, quindi fare clic su **Delete** (Elimina).<br>b. Fare nuovamente clic su **Delete** per confermare. |

### Gestione degli aggregati esistenti

Gestisci gli aggregati aggiungendo dischi, visualizzando informazioni sugli aggregati ed eliminandoli.

#### Prima di iniziare

Se si desidera eliminare un aggregato, è necessario prima eliminare i volumi nell'aggregato.

#### A proposito di questa attività

Se un aggregato sta esaurendo lo spazio, è possibile spostare i volumi in un altro aggregato utilizzando Gestione di sistema di OnCommand.

#### Fasi

1. Nella pagina Working Environments (ambienti di lavoro), fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi su **Avanzate > allocazione avanzata**.
3. Gestisci i tuoi aggregati:

| Attività | Azione |
| --- | --- |
| Visualizzare informazioni su un aggregato | Selezionare un aggregato e fare clic su **Info**. |
| Creare un volume su un aggregato specifico | Selezionare un aggregato e fare clic su **Create volume** (Crea volume). |

| Attività | Azione |
| --- | --- |
| Aggiungere dischi a un aggregato | a. Selezionare un aggregato e fare clic su **Aggiungi dischi AWS** o **Aggiungi dischi Azure**.<br>b. Selezionare il numero di dischi che si desidera aggiungere e fare clic su **Aggiungi**.<br>Tutti i dischi di un aggregato devono avere le stesse dimensioni. |
| Eliminare un aggregato | a. Selezionare un aggregato che non contiene volumi e fare clic su **Delete** (Elimina).<br>b. Fare nuovamente clic su **Delete** per confermare. |

### Modifica del server CIFS

Se si modificano i server DNS o il dominio Active Directory, è necessario modificare il server CIFS in Cloud Volumes ONTAP in modo che possa continuare a fornire storage ai client.

#### Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > CIFS setup**.
2. Specificare le impostazioni per il server CIFS:

| Attività | Azione |
| --- | --- |
| 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. |

| Attività | Azione |
| --- | --- |
| 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 "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni. |

3. Fare clic su **Save** (Salva).

**Risultato**

Cloud Volumes ONTAP aggiorna il server CIFS con le modifiche.

### Spostamento di un volume

Spostare i volumi per l'utilizzo della capacità, migliorare le performance e soddisfare i service level agreement.

È possibile spostare un volume in System Manager selezionando un volume e l'aggregato di destinazione, avviando l'operazione di spostamento del volume e monitorando facoltativamente il processo di spostamento del volume. Quando si utilizza System Manager, l'operazione di spostamento del volume termina automaticamente.

**Fasi**

1. Utilizzare System Manager o CLI per spostare i volumi nell'aggregato.

   Nella maggior parte dei casi, è possibile utilizzare System Manager per spostare i volumi.

   Per istruzioni, consultare "Guida rapida per lo spostamento del volume di ONTAP 9".

### Spostamento di un volume quando Cloud Manager visualizza un messaggio Action Required (azione richiesta)

Cloud Manager potrebbe visualizzare un messaggio Action Required (azione richiesta) che indica che lo spostamento di un volume è necessario per evitare problemi di capacità, ma che non può fornire consigli per correggere il problema. In questo caso, è necessario identificare come correggere il problema e spostare uno o più volumi.

**Fasi**

1. Identificare come risolvere il problema.
2. In base alla tua analisi, sposta i volumi per evitare problemi di capacità:
   - Spostare i volumi in un altro sistema.
   - Spostare i volumi in un altro aggregato sullo stesso sistema.

#### Identificare come correggere i problemi di capacità

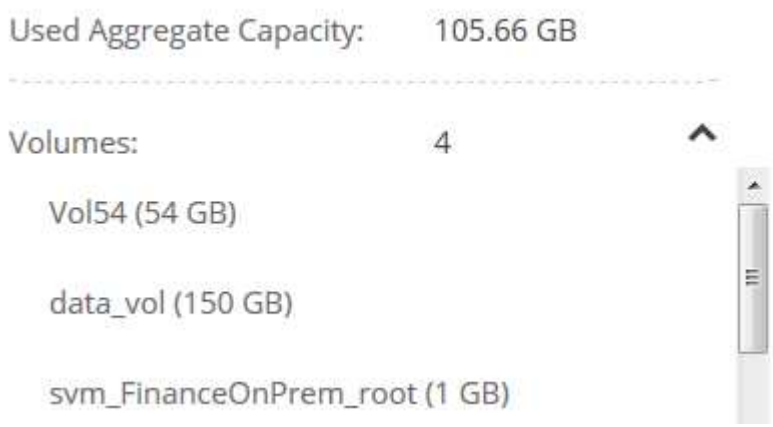
Se Cloud Manager non è in grado di fornire consigli per lo spostamento di un volume per evitare problemi di capacità, è necessario identificare i volumi da spostare e se è necessario spostarli in un altro aggregato sullo stesso sistema o in un altro sistema.

**Fasi**

1. Visualizzare le informazioni avanzate nel messaggio Action Required (azione richiesta) per identificare l'aggregato che ha raggiunto il limite di capacità.

Ad esempio, le informazioni avanzate dovrebbero dire qualcosa di simile a quanto segue: L'aggregato aggr1 ha raggiunto il suo limite di capacità.

2. Identificare uno o più volumi da spostare fuori dall'aggregato:
   a. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
   b. Selezionare l'aggregato, quindi fare clic su **Info**.
   c. Espandere l'elenco dei volumi.




   d. Esaminare le dimensioni di ciascun volume e scegliere uno o più volumi da spostare fuori dall'aggregato.

      È necessario scegliere volumi sufficientemente grandi da liberare spazio nell'aggregato in modo da evitare ulteriori problemi di capacità in futuro.

3. Se il sistema non ha raggiunto il limite di dischi, spostare i volumi in un aggregato esistente o in un nuovo aggregato sullo stesso sistema.

   Per ulteriori informazioni, vedere "Spostamento dei volumi in un altro aggregato per evitare problemi di capacità".

4. Se il sistema ha raggiunto il limite di dischi, eseguire una delle seguenti operazioni:
   a. Eliminare eventuali volumi inutilizzati.
   b. Riorganizzare i volumi per liberare spazio su un aggregato.

      Per ulteriori informazioni, vedere "Spostamento dei volumi in un altro aggregato per evitare problemi di capacità".

   c. Spostare due o più volumi in un altro sistema con spazio.

      Per ulteriori informazioni, vedere "Spostamento dei volumi in un altro sistema per evitare problemi di capacità".

#### Spostamento dei volumi in un altro sistema per evitare problemi di capacità

È possibile spostare uno o più volumi in un altro sistema Cloud Volumes ONTAP per evitare problemi di capacità. Potrebbe essere necessario eseguire questa operazione se il sistema ha raggiunto il limite di dischi.

**A proposito di questa attività**

È possibile seguire la procedura descritta in questa attività per correggere il seguente messaggio Action Required (azione richiesta):

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Fasi
. Identificare un sistema Cloud Volumes ONTAP con capacità disponibile o
implementare un nuovo sistema.
. Trascinare e rilasciare l'ambiente di lavoro di origine nell'ambiente di
lavoro di destinazione per eseguire una replica dei dati del volume una
tantum.
```

+
Per ulteriori informazioni, vedere "Replica dei dati tra sistemi".

1. Accedere alla pagina Replication Status (Stato replica), quindi interrompere la relazione SnapMirror per convertire il volume replicato da un volume di protezione dati a un volume di lettura/scrittura.

   Per ulteriori informazioni, vedere "Gestione delle pianificazioni e delle relazioni di replica dei dati".

2. Configurare il volume per l'accesso ai dati.

   Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati, consultare "Guida rapida per il disaster recovery dei volumi di ONTAP 9".

3. Eliminare il volume originale.

   Per ulteriori informazioni, vedere "Gestione dei volumi esistenti".

#### Spostamento dei volumi in un altro aggregato per evitare problemi di capacità

È possibile spostare uno o più volumi in un altro aggregato per evitare problemi di capacità.

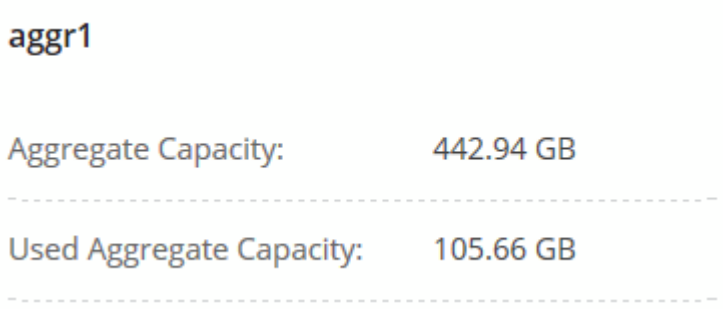
**A proposito di questa attività**

È possibile seguire la procedura descritta in questa attività per correggere il seguente messaggio Action Required (azione richiesta):

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Fasi
. Verificare se un aggregato esistente dispone di capacità disponibile per
i volumi da spostare:
```

+
.. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
.. Selezionare ciascun aggregato, fare clic su **Info**, quindi visualizzare la capacità disponibile (capacità aggregata meno capacità aggregata utilizzata).

+




1. Se necessario, aggiungere dischi a un aggregato esistente:
   a. Selezionare l'aggregato, quindi fare clic su **Aggiungi dischi**.
   b. Selezionare il numero di dischi da aggiungere, quindi fare clic su **Aggiungi**.
2. Se nessun aggregato dispone di capacità, creare un nuovo aggregato.

   Per ulteriori informazioni, vedere "Creazione di aggregati".
3. Utilizzare System Manager o CLI per spostare i volumi nell'aggregato.
4. Nella maggior parte dei casi, è possibile utilizzare System Manager per spostare i volumi.

   Per istruzioni, consultare "Guida rapida per lo spostamento del volume di ONTAP 9".

**Motivi per cui lo spostamento di un volume potrebbe risultare lento**

Lo spostamento di un volume potrebbe richiedere più tempo del previsto se una delle seguenti condizioni è vera per Cloud Volumes ONTAP:

- Il volume è un clone.
- Il volume è il padre di un clone.
- L'aggregato di origine o di destinazione dispone di un disco HDD (st1) ottimizzato per il throughput singolo.
- Il sistema Cloud Volumes ONTAP è in AWS e un aggregato utilizza uno schema di denominazione precedente per gli oggetti. Entrambi gli aggregati devono utilizzare lo stesso formato dei nomi.

  Viene utilizzato uno schema di denominazione precedente se il tiering dei dati è stato attivato su un aggregato nella versione 9.4 o precedente.
- Le impostazioni di crittografia non corrispondono sugli aggregati di origine e destinazione, oppure è in corso una rekey.
- L'opzione *-tiering-policy* è stata specificata nello spostamento del volume per modificare il criterio di tiering.
- L'opzione *-generate-destination-key* è stata specificata durante lo spostamento del volume.

## Tiering dei dati inattivi su storage a oggetti a basso costo

È possibile ridurre i costi di storage per Cloud Volumes ONTAP combinando un Tier di performance SSD o HDD per i dati hot con un Tier di capacità dello storage a oggetti per i dati inattivi. Per una panoramica generale, vedere "Panoramica sul tiering dei dati".

Per impostare il tiering dei dati, è sufficiente eseguire le seguenti operazioni:

### Scegliere una configurazione supportata

Sono supportate la maggior parte delle configurazioni. Se si dispone di un sistema Cloud Volumes ONTAP standard, Premium o BYOL con la versione più recente, si consiglia di procedere. "Scopri di più".

### Garantire la connettività tra Cloud Volumes ONTAP e lo storage a oggetti

- Per AWS, è necessario un endpoint VPC per S3. Scopri di più.
- Per Azure, non dovrai fare nulla finché Cloud Manager dispone delle autorizzazioni necessarie. Scopri di più.
- Per GCP, è necessario configurare la subnet per Private Google Access e impostare un account di servizio. Scopri di più.

### Scegliere un criterio di tiering quando si crea, modifica o replica un volume

Cloud Manager richiede di scegliere una policy di tiering quando si crea, modifica o si replica un volume.

- "Tiering dei dati sui volumi di lettura/scrittura"
- "Tiering dei dati sui volumi di protezione dei dati"

**Cosa non è richiesto per il tiering dei dati? (8217**

- Non è necessario installare una licenza per le funzionalità per abilitare il tiering dei dati.
- Non è necessario creare il Tier di capacità (un bucket S3, un container Azure Blob o un bucket GCP). Cloud Manager fa tutto questo per te.

#### Configurazioni che supportano il tiering dei dati

È possibile abilitare il tiering dei dati quando si utilizzano configurazioni e funzionalità specifiche:

- Il tiering dei dati è supportato con Cloud Volumes ONTAP standard, Premium e BYOL, a partire dalle seguenti versioni:
  - Versione 9.2 in AWS
  - Versione 9.4 in Azure con sistemi a nodo singolo
  - Versione 9.6 in Azure con coppie ha
  - Versione 9.6 in GCP

  Il tiering dei dati non è supportato in Azure con il tipo di macchina virtuale DS3_v2.
- In AWS, il Tier di performance può essere SSD General Purpose, SSD IOPS con provisioning o HDD ottimizzati per il throughput.
- In Azure, il Tier di performance può essere costituito da dischi gestiti da SSD Premium, dischi gestiti da SSD Standard o dischi gestiti da HDD Standard.
- In GCP, il Tier di performance può essere SSD o HDD (dischi standard).

- Il tiering dei dati è supportato dalle tecnologie di crittografia.
- Il thin provisioning deve essere attivato sui volumi.

**Requisiti per il tiering dei dati cold in AWS S3**

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?".

**Requisiti per il tiering dei dati cold nello storage Azure Blob**

Non è necessario configurare una connessione tra il Tier di performance e il Tier di capacità, purché Cloud Manager disponga delle autorizzazioni necessarie. Cloud Manager abilita un endpoint del servizio VNET se la policy di Cloud Manager dispone delle seguenti autorizzazioni:

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

Le autorizzazioni sono incluse nella versione più recente "Policy di Cloud Manager".

**Requisiti per tierare i dati cold in un bucket di storage Google Cloud**

- 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".
- È necessario disporre di un account di servizio con il ruolo di amministratore dello storage predefinito. Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, è necessario selezionare questo account di servizio.

  "Impostare questo account del servizio di tiering come indicato di seguito":

  a. Assegnare il ruolo predefinito *Storage Admin* all'account del servizio di tiering.
  b. Aggiungere l'account del servizio Connector come *Service account User* all'account del servizio di tiering.

     È possibile fornire il ruolo dell'utente "nel passaggio 3 della procedura guidata quando si crea l'account del servizio di tiering", o. "assegnare il ruolo dopo la creazione dell'account di servizio".

     Sarà necessario selezionare l'account del servizio di tiering in un secondo momento quando si crea un ambiente di lavoro Cloud Volumes ONTAP.

  Se non si attiva il tiering dei dati e si seleziona un account di servizio quando si crea il sistema Cloud Volumes ONTAP, è necessario spegnere il sistema e aggiungere l'account di servizio a Cloud Volumes

ONTAP dalla console GCP.

### Tiering dei dati dai volumi di lettura/scrittura

Cloud Volumes ONTAP è in grado di tierare i dati inattivi su volumi di lettura/scrittura per uno storage a oggetti conveniente, liberando il Tier di performance per i dati hot.

**Fasi**

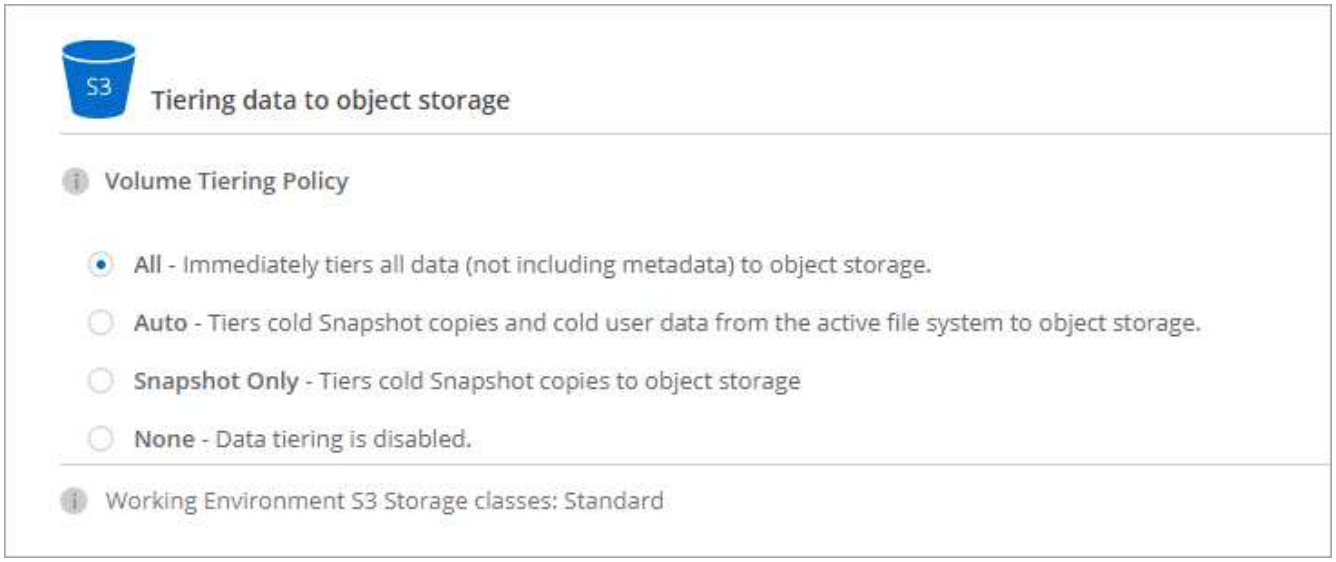
1. Nell'ambiente di lavoro, creare un nuovo volume o modificare il livello di un volume esistente:

| Attività | Azione |
|---|---|
| Creare un nuovo volume | Fare clic su **Add New Volume** (Aggiungi nuovo volume). |
| Modificare un volume esistente | Selezionare il volume e fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering). |

2. Selezionare una policy di tiering.

   Per una descrizione di questi criteri, vedere "Panoramica sul tiering dei dati".

   **Esempio**




   Cloud Manager crea un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering dei dati.

   Se preferisci creare aggregati, puoi abilitare il tiering dei dati sugli aggregati quando li crei.

### Tiering dei dati dai volumi di protezione dei dati

Cloud Volumes ONTAP può eseguire il tiering dei dati da un volume di protezione dei dati a un livello di capacità. Se si attiva il volume di destinazione, i dati si spostano gradualmente al livello di performance man mano che vengono letti.

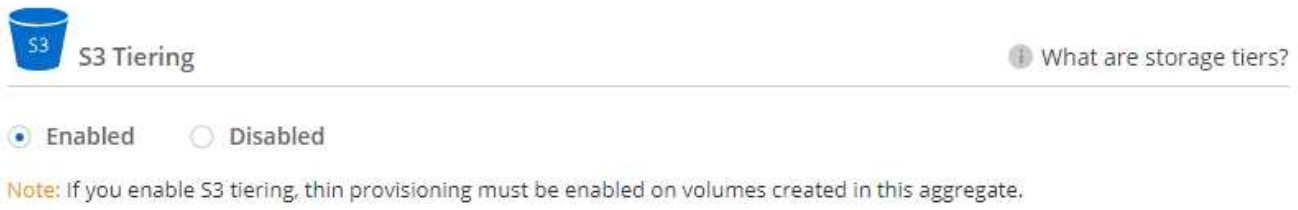
**Fasi**

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi

trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume.

2. Seguire le istruzioni fino a raggiungere la pagina di tiering e abilitare il tiering dei dati allo storage a oggetti.

**Esempio**




Per assistenza nella replica dei dati, vedere "Replica dei dati da e verso il cloud".

#### Modifica della classe di storage per i dati a più livelli

Dopo aver implementato Cloud Volumes ONTAP, è possibile ridurre i costi di storage modificando la classe di storage per i dati inattivi a cui non è stato effettuato l'accesso per 30 giorni. I costi di accesso sono più elevati se si accede ai dati, pertanto è necessario prendere in considerazione questo aspetto prima di modificare la classe di storage.

La classe di storage per i dati a più livelli è estesa a tutto il sistema, non a it per volume.

Per informazioni sulle classi di storage supportate, vedere "Panoramica sul tiering dei dati".

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **Storage CLASSES** o **Blob Storage Tiering**.
2. Scegliere una classe di storage e fare clic su **Save** (Salva).

#### È possibile abilitare il tiering dei dati su un aggregato esistente?

No, non è possibile abilitare il tiering dei dati su un aggregato esistente. È possibile attivare il tiering dei dati solo su nuovi aggregati.

È possibile abilitare il tiering dei dati su un nuovo aggregato "creando un aggregato" oppure creando un nuovo volume con il tiering dei dati attivato. Cloud Manager creerebbe quindi un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering dei dati.

## Gestione delle VM di storage

Una VM di storage è una macchina virtuale in esecuzione in ONTAP che fornisce servizi di storage e dati ai client. Potresti sapere che si tratta di un *SVM* o di un *vserver*. Cloud Volumes ONTAP è configurato con una VM di storage per impostazione predefinita, ma alcune configurazioni supportano altre VM di storage.

#### Numero di VM storage supportate

Cloud Volumes ONTAP 9.7 supporta più macchine virtuali storage in AWS con determinate configurazioni e una licenza aggiuntiva. "Visualizza il numero di VM di storage supportate in AWS". Contattare il proprio account team per ottenere una licenza add-on SVM.

Tutte le altre configurazioni Cloud Volumes ONTAP supportano una VM di storage per il servizio dati e una VM di storage di destinazione utilizzata per il disaster recovery. È possibile attivare la VM di storage di destinazione per l'accesso ai dati in caso di interruzione della VM di storage di origine.

Una VM di storage copre l'intero sistema Cloud Volumes ONTAP (coppia ha o nodo singolo).

### Creazione di VM storage aggiuntive

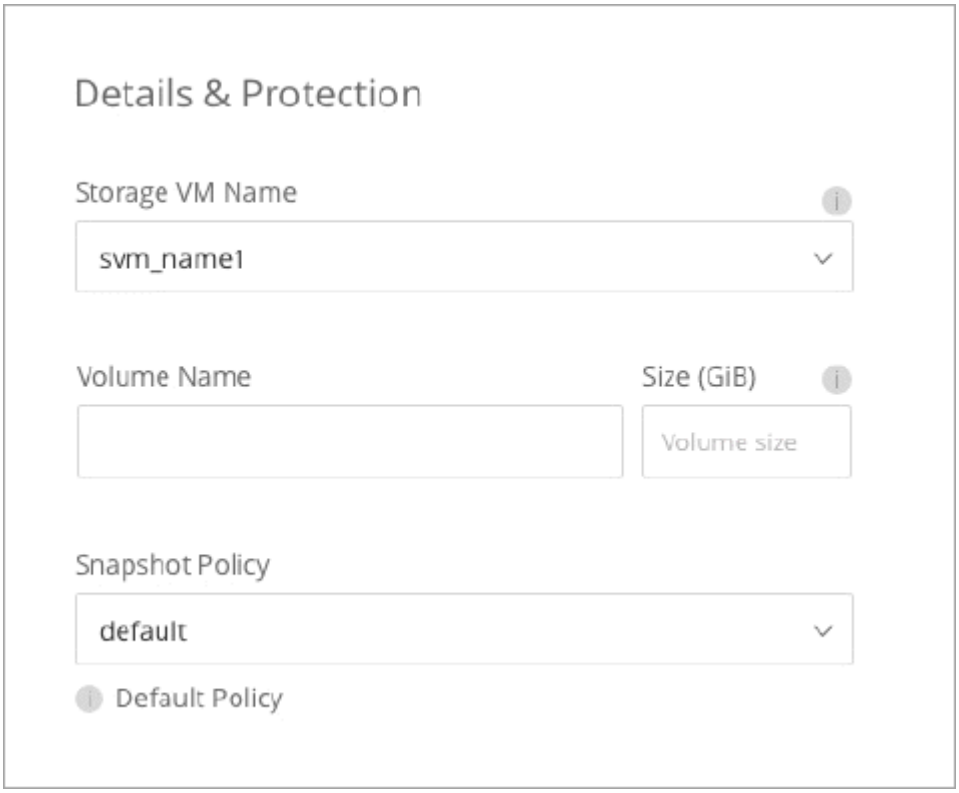
Se supportato dalla configurazione, è possibile creare ulteriori VM di storage utilizzando "System Manager o CLI".

- "Creazione di una SVM per l'accesso SMB"
- "Creazione di una SVM per l'accesso NFS"
- "Creazione di una SVM per l'accesso iSCSI"
- "Creazione di una SVM di destinazione per il disaster recovery"

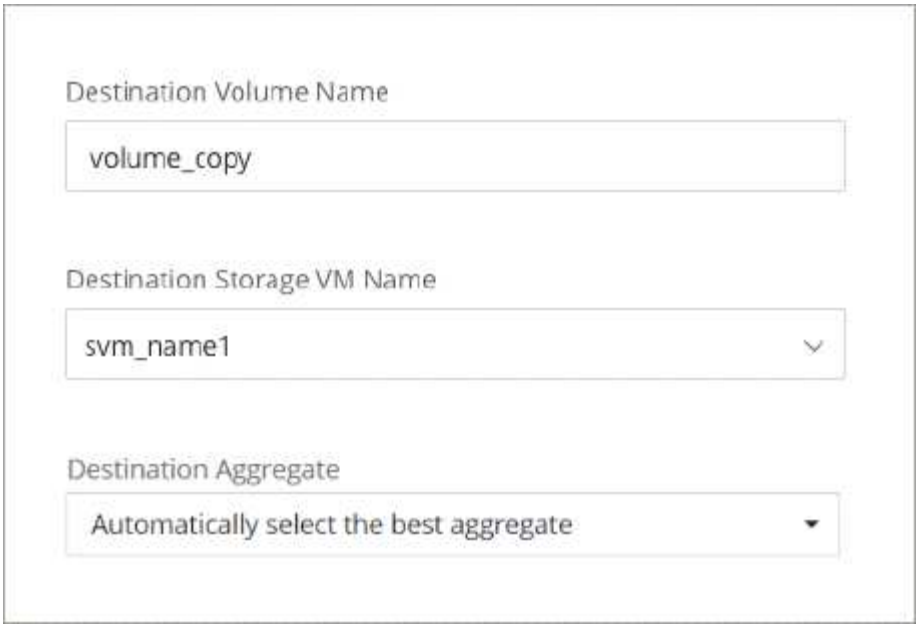
### Utilizzo di più macchine virtuali storage in Cloud Manager

Cloud Manager supporta tutte le VM di storage aggiuntive create da System Manager o CLI.

Ad esempio, l'immagine seguente mostra come scegliere una VM di storage quando si crea un volume.




L'immagine seguente mostra come scegliere una VM di storage durante la replica di un volume su un altro sistema.




### Gestione del disaster recovery delle macchine virtuali dello storage

Cloud Manager non fornisce alcun supporto di configurazione o orchestrazione per il disaster recovery delle macchine virtuali dello storage. È necessario utilizzare System Manager o la CLI.

- "Guida rapida alla preparazione del disaster recovery per SVM"
- "Guida di SVM Disaster Recovery Express"

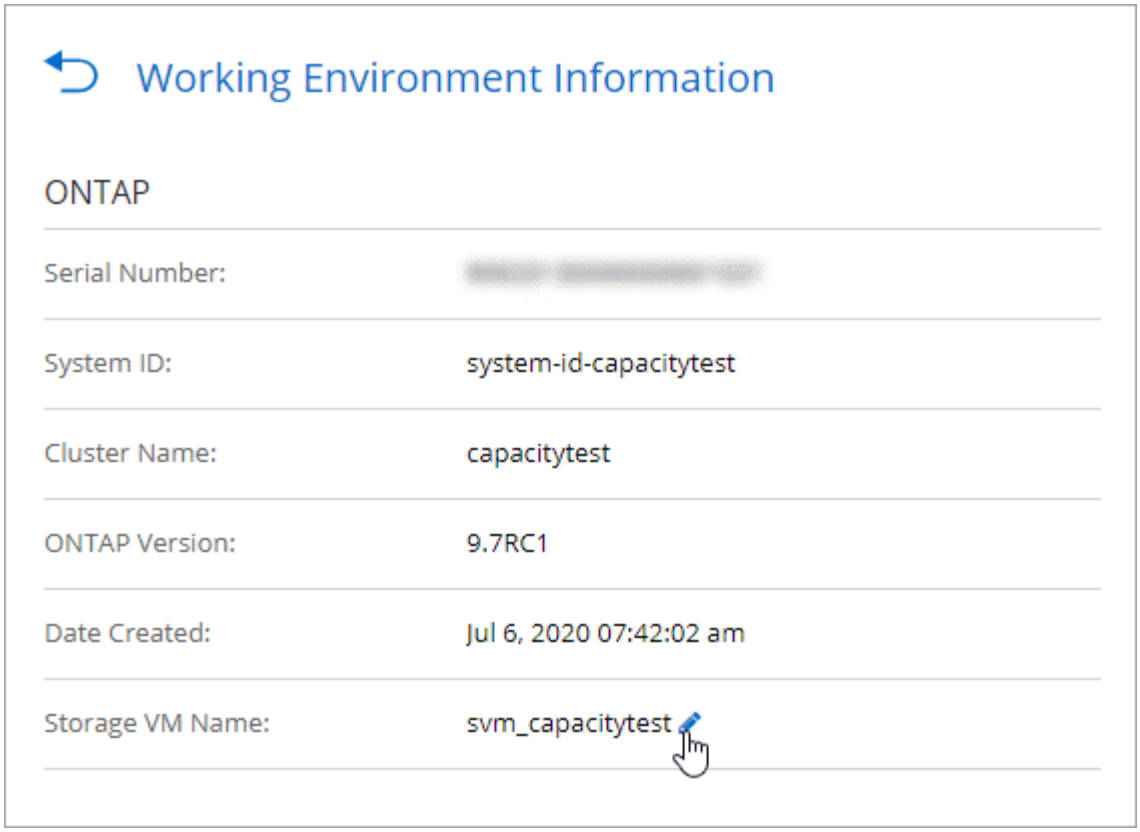
### Modifica del nome della VM di storage

Cloud Manager assegna automaticamente un nome alla singola VM di storage creata per Cloud Volumes ONTAP. È possibile modificare il nome della VM di storage se si dispone di standard di denominazione rigorosi. Ad esempio, è possibile che il nome corrisponda a quello delle VM di storage per i cluster ONTAP.

Se hai creato altre VM di storage per Cloud Volumes ONTAP, non puoi rinominare le VM di storage da Cloud Manager. È necessario eseguire questa operazione direttamente da Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **informazioni**.
2. Fare clic sull'icona di modifica a destra del nome della VM di storage.




3. Nella finestra di dialogo Modify SVM Name (Modifica nome SVM), modificare il nome, quindi fare clic su **Save** (Salva).

## Utilizzo di Cloud Volumes ONTAP come storage persistente per Kubernetes

Cloud Manager può automatizzare l'implementazione di NetApp Trident sui cluster Kubernetes, in modo da poter utilizzare Cloud Volumes ONTAP come storage persistente per i container.

Trident è un progetto open source completamente supportato gestito da NetApp. Trident si integra in modo nativo con Kubernetes e il suo framework per volumi persistenti per eseguire il provisioning e la gestione dei volumi da sistemi che eseguono qualsiasi combinazione delle piattaforme storage NetApp. "Scopri di più su Trident".

La funzionalità Kubernetes non è supportata dai cluster ONTAP on-premise. È supportato solo con Cloud Volumes ONTAP.

### Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

### 1 Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti, che includono connettività tra cluster Kubernetes e Cloud Volumes ONTAP, connettività tra cluster Kubernetes e un connettore, una versione minima di Kubernetes 1.14,

almeno un nodo di lavoro in un cluster e molto altro ancora. Consulta l'elenco completo.

### Aggiungi i tuoi cluster Kubernetes a Cloud Manager

In Cloud Manager, fai clic su **Kubernetes** e scopri i cluster direttamente dal servizio gestito del tuo provider di cloud oppure importa un cluster fornendo un file kubeconfig.

### Connetti i tuoi cluster a Cloud Volumes ONTAP

Dopo aver aggiunto un cluster Kubernetes, fare clic su **connessione all'ambiente di lavoro** per connettere il cluster a uno o più sistemi Cloud Volumes ONTAP.

### Avviare il provisioning dei volumi persistenti

Richiedere e gestire volumi persistenti utilizzando interfacce e costrutti Kubernetes nativi. Cloud Manager crea classi di storage NFS e iSCSI da utilizzare per il provisioning di volumi persistenti.

"Scopri di più sul provisioning del tuo primo volume con Trident for Kubernetes".

## Verifica dei prerequisiti

Prima di iniziare, assicurati che i cluster Kubernetes e il connettore soddisfino requisiti specifici.

#### Requisiti del cluster Kubernetes

- È necessaria la connettività di rete tra un cluster Kubernetes e il connettore e tra un cluster Kubernetes e Cloud Volumes ONTAP.

  Sia il connettore che Cloud Volumes ONTAP necessitano di una connessione all'endpoint API di Kubernetes:

  - Per i cluster gestiti, impostare un percorso tra il VPC di un cluster e il VPC in cui risiedono il connettore e Cloud Volumes ONTAP.
  - Per gli altri cluster, l'indirizzo IP del nodo master o del bilanciamento del carico (come indicato nel file kubeconfig) deve essere raggiungibile dal connettore e da Cloud Volumes ONTAP e deve presentare un certificato TLS valido.
- Un cluster Kubernetes può trovarsi in qualsiasi posizione che disponga della connettività di rete indicata sopra.
- Un cluster Kubernetes deve eseguire almeno la versione 1.14.

  La versione massima supportata è definita da Trident. "Fare clic qui per visualizzare la versione massima supportata di Kubernetes".
- Un cluster Kubernetes deve avere almeno un nodo di lavoro.
- Per i cluster in esecuzione in Amazon Elastic Kubernetes Service (Amazon EKS), ciascun cluster richiede l'aggiunta di un ruolo IAM per risolvere un errore di permessi. Dopo aver aggiunto il cluster, Cloud Manager richiederà l'esatto comando eksctl che risolve l'errore.

"Scopri i limiti delle autorizzazioni IAM".

- Per i cluster in esecuzione in Azure Kubernetes Service (AKS), a tali cluster deve essere assegnato il ruolo *Azure Kubernetes Service RBAC Cluster Admin*. Questo è necessario per consentire a Cloud Manager di installare Trident e configurare le classi di storage sul cluster.
- Per i cluster in esecuzione in Google Kubernetes Engine (GKE), questi cluster non devono utilizzare il sistema operativo predefinito ottimizzato per i container. Si consiglia di passare all'utilizzo di Ubuntu.

  Per impostazione predefinita, GKE utilizza Google "immagine ottimizzata per container", Che non dispone delle utility di cui Trident ha bisogno per montare i volumi.

#### Requisiti del connettore

Assicurarsi che il connettore disponga delle seguenti autorizzazioni e connessioni di rete.

### Networking

- Il connettore necessita di una connessione Internet in uscita per accedere ai seguenti endpoint durante l'installazione di Trident:

  https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

  Cloud Manager installa Trident su un cluster Kubernetes quando si connette un ambiente di lavoro al cluster.

### Autorizzazioni necessarie per rilevare e gestire i cluster EKS

Il connettore necessita delle autorizzazioni di amministratore per rilevare e gestire i cluster Kubernetes in esecuzione in Amazon Elastic Kubernetes Service (EKS):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

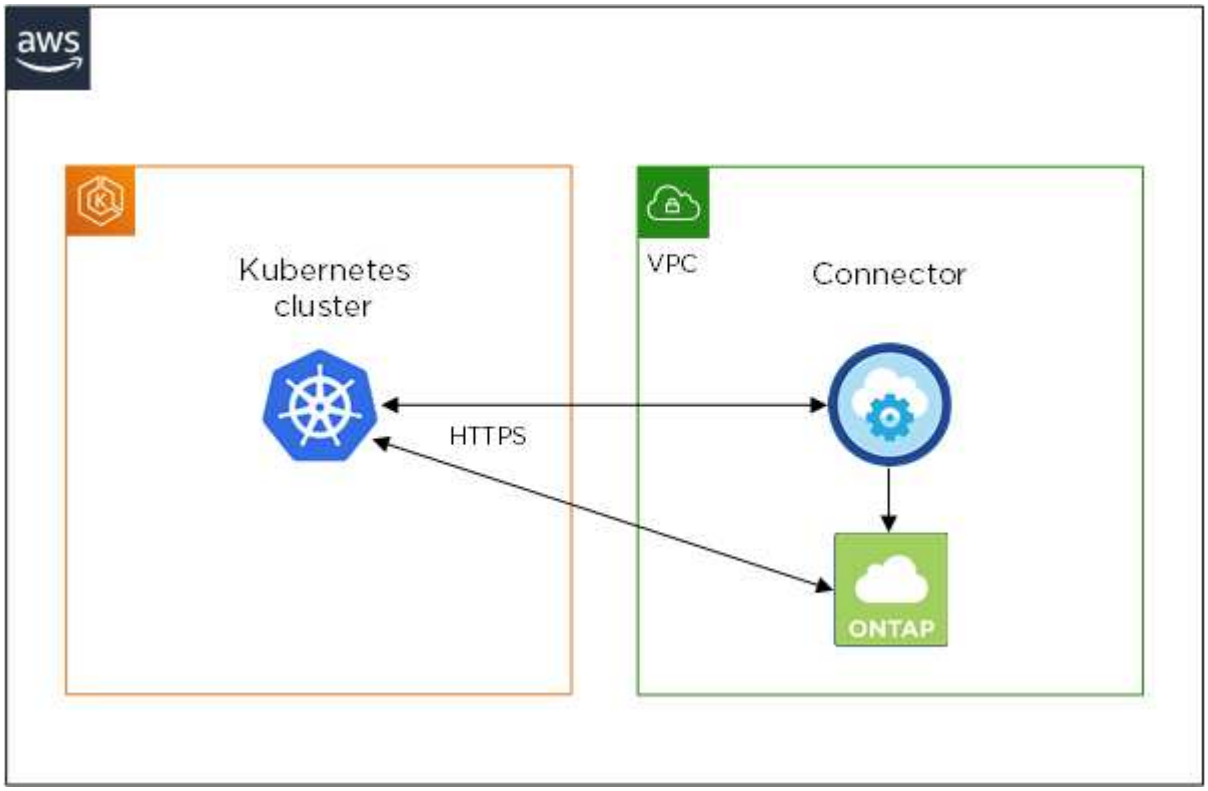
### Autorizzazioni necessarie per rilevare e gestire i cluster GKE

Il connettore necessita delle seguenti autorizzazioni per rilevare e gestire i cluster Kubernetes in esecuzione in Google Kubernetes Engine (GKE):

```
container.*
```

#### Esempio di configurazione

L'immagine seguente mostra un esempio di cluster Kubernetes in esecuzione in Amazon Elastic Kubernetes Service (Amazon EKS) e le relative connessioni a Connector e Cloud Volumes ONTAP.




### Aggiunta di cluster Kubernetes

Aggiungi i cluster Kubernetes a Cloud Manager scoprendo i cluster in esecuzione nel servizio Kubernetes gestito dal tuo provider cloud o importando il file kuberconfig di un cluster.

#### Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic su **Aggiungi cluster**.
3. Scegliere una delle opzioni disponibili:
   - Fare clic su **Discover Clusters** (Discover Clusters) per scoprire i cluster gestiti a cui Cloud Manager ha accesso in base alle autorizzazioni fornite al connettore.

     Ad esempio, se il connettore è in esecuzione in Google Cloud, Cloud Manager utilizza le autorizzazioni dell'account di servizio del connettore per rilevare i cluster in esecuzione in Google Kubernetes Engine (GKE).

   - Fare clic su **Import Cluster** (Importa cluster) per importare un cluster utilizzando un file kubeconfig.

     Dopo aver caricato il file, Cloud Manager verifica la connettività al cluster e salva una copia crittografata del file kubeconfig.

#### Risultato

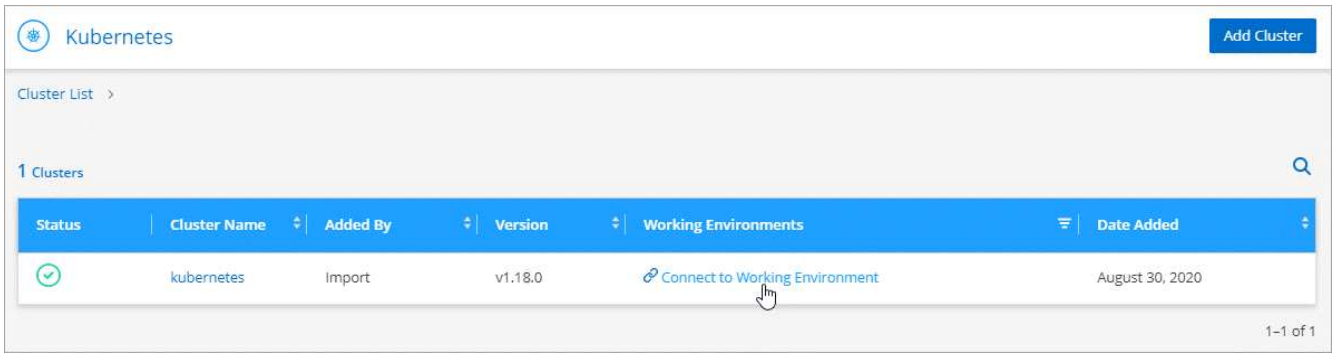
Cloud Manager aggiunge il cluster Kubernetes. È ora possibile collegare il cluster a Cloud Volumes ONTAP.

### Connessione di un cluster a Cloud Volumes ONTAP

Collega un cluster Kubernetes a Cloud Volumes ONTAP in modo da poter utilizzare Cloud Volumes ONTAP come storage persistente per i container.

#### Fasi

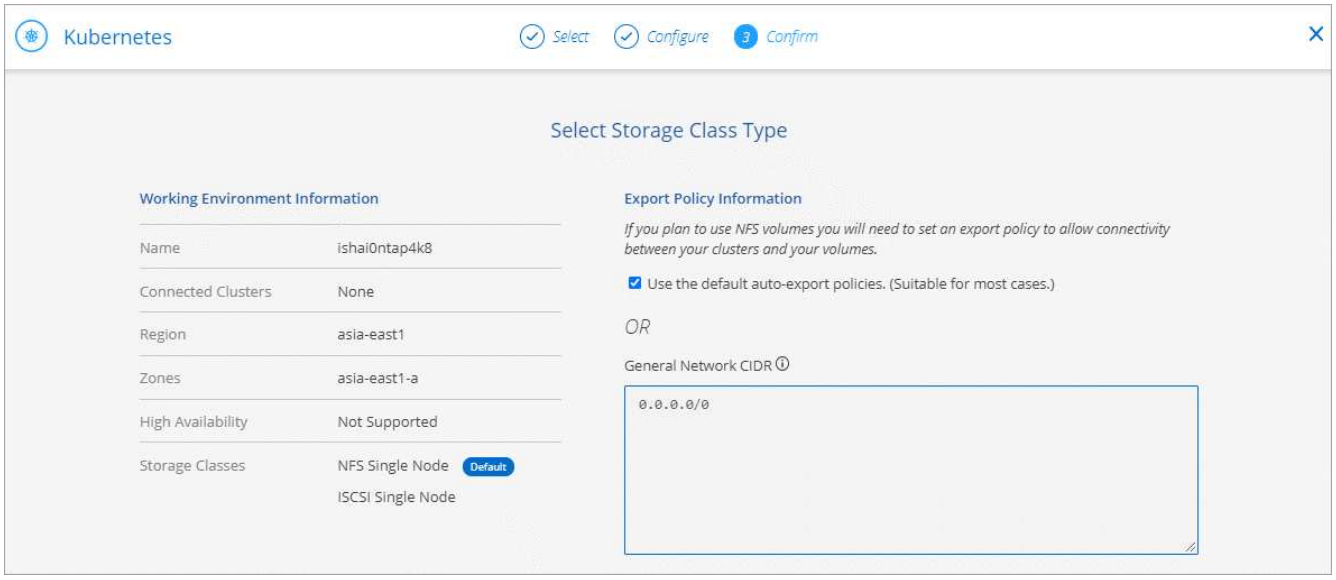
1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic su **Connect to Working Environment** (Connetti all'ambiente di lavoro) per il cluster appena aggiunto.




3. Selezionare un ambiente di lavoro e fare clic su **continua**.
4. Scegliere la classe di storage NetApp da utilizzare come classe di storage predefinita per il cluster Kubernetes e fare clic su **continua**.

   Quando un utente crea un volume persistente, il cluster Kubernetes può utilizzare questa classe di storage come storage back-end per impostazione predefinita.

5. Scegliere se utilizzare i criteri di esportazione automatica predefiniti o se aggiungere un blocco CIDR personalizzato.




6. Fare clic su **Aggiungi ambiente di lavoro**.

#### Risultato

Cloud Manager connette l'ambiente di lavoro al cluster, che può richiedere fino a 15 minuti.

## Gestione dei cluster

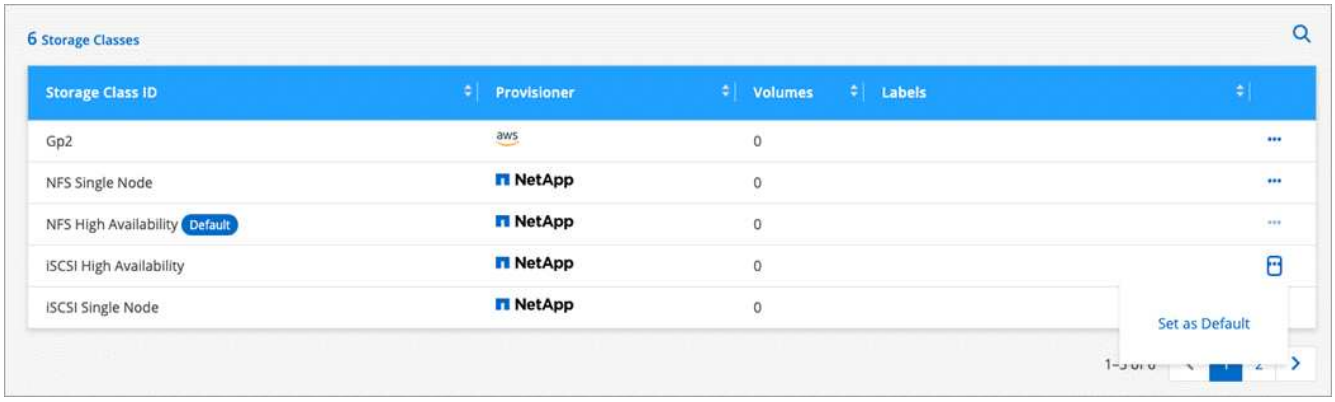
Cloud Manager consente di gestire i cluster Kubernetes modificando la classe di storage predefinita, aggiornando Trident e molto altro ancora.

### Modifica della classe di storage predefinita

Assicurarsi di aver impostato una classe di storage Cloud Volumes ONTAP come classe di storage predefinita, in modo che i cluster utilizzino Cloud Volumes ONTAP come storage back-end.

**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Nella tabella **Storage CLASSES**, fare clic sul menu delle azioni all'estrema destra per la classe di storage che si desidera impostare come predefinita.




4. Fare clic su **Set as Default** (Imposta come predefinito).

### Aggiornamento di Trident

Puoi aggiornare Trident da Cloud Manager quando è disponibile una nuova versione di Trident.

**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Se è disponibile una nuova versione, fare clic su **Upgrade** (Aggiorna) accanto alla versione di Trident.


### Aggiornamento del file kubeconfig

Se hai aggiunto il cluster a Cloud Manager importando il file kubeconfig, puoi caricare l'ultimo file kubeconfig su Cloud Manager in qualsiasi momento. Questa operazione può essere eseguita se le credenziali sono state aggiornate, se sono stati modificati utenti o ruoli o se qualcosa è stato modificato in modo da influire sul

cluster, sull'utente, sugli spazi dei nomi o sull'autenticazione.

**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Fare clic su **Update Kubeconfig** (Aggiorna Kubeconfig*).
4. Quando richiesto dal browser Web, selezionare il file kubeconfig aggiornato e fare clic su **Open** (Apri).

**Risultato**

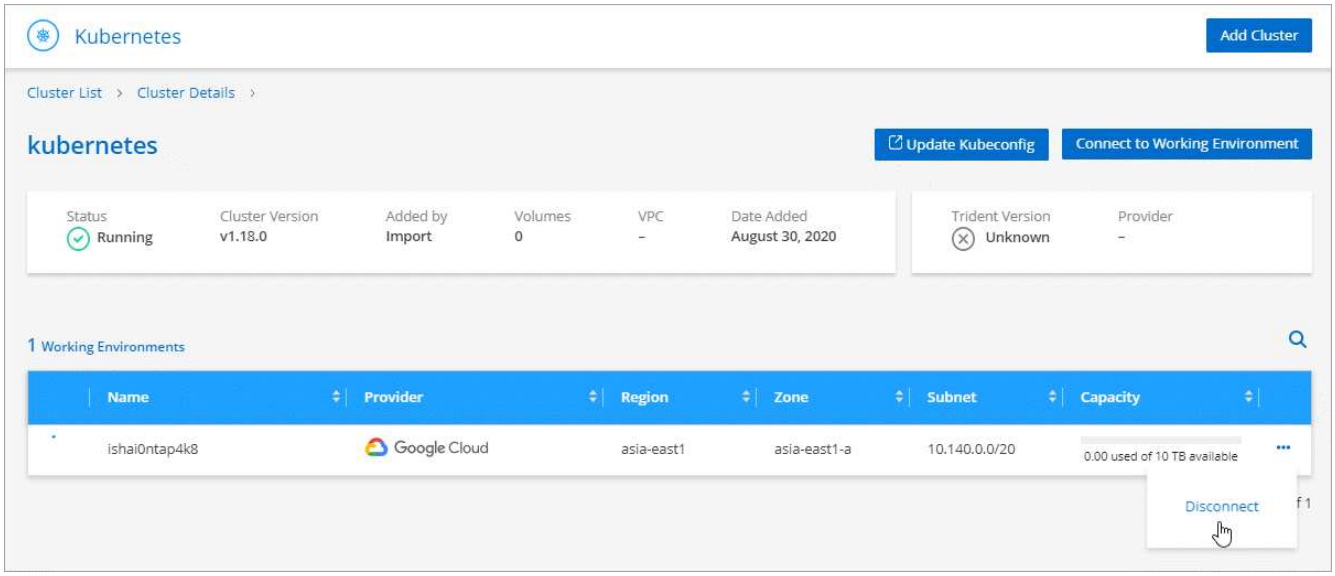
Cloud Manager aggiorna le informazioni sul cluster Kubernetes in base all'ultimo file kubeconfig.

#### Disconnessione di un cluster

Quando si disconnette un cluster da Cloud Volumes ONTAP, non è più possibile utilizzare tale sistema Cloud Volumes ONTAP come storage persistente per i container. I volumi persistenti esistenti non vengono cancellati.

**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Nella tabella **ambienti di lavoro**, fare clic sul menu delle azioni a destra dell'ambiente di lavoro che si desidera disconnettere.




4. Fare clic su **Disconnetti**.

**Risultato**

Cloud Manager disconnette il cluster dal sistema Cloud Volumes ONTAP.

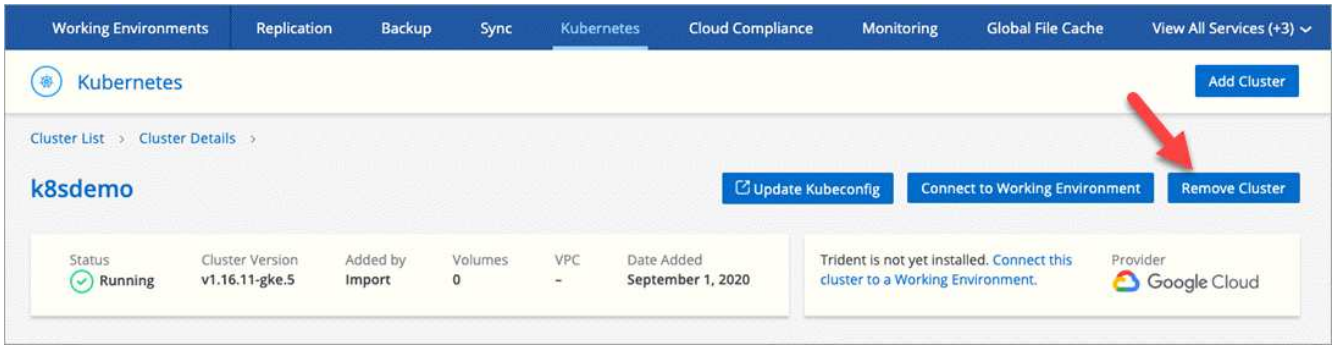
#### Rimozione di un cluster

Rimuovere i cluster decommissionati da Cloud Manager dopo aver scollegato tutti gli ambienti di lavoro dal cluster.

**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.

2. Fare clic sul nome del cluster Kubernetes.
3. Fare clic su **Remove Cluster** (Rimuovi cluster).




## Crittografia dei volumi con le soluzioni di crittografia NetApp

Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp (NVE) e la crittografia aggregata NetApp (NAE) con un gestore di chiavi esterno. NVE e NAE sono soluzioni basate su software che consentono la crittografia dei volumi (data-at-rest) conforme a FIPS 140-2. "Scopri di più su queste soluzioni di crittografia".

A partire da Cloud Volumes ONTAP 9.7, i nuovi aggregati avranno attivato NAE per impostazione predefinita dopo aver configurato un gestore di chiavi esterno. I nuovi volumi che non fanno parte di un aggregato NAE avranno NVE abilitato per impostazione predefinita (ad esempio, se si dispone di aggregati già creati prima della configurazione di un gestore di chiavi esterno).

Cloud Volumes ONTAP non supporta la gestione delle chiavi integrata.

### Di cosa hai bisogno

Il sistema Cloud Volumes ONTAP deve essere registrato presso il supporto NetApp. A partire da Cloud Manager 3.7.1, una licenza per la crittografia dei volumi NetApp viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp.

- "Aggiunta di account NetApp Support Site a Cloud Manager"
- "Registrazione di sistemi pay-as-you-go"

Cloud Manager non installa la licenza NVE sui sistemi che risiedono nell'area geografica Cina.

### Fasi

1. Esaminare l'elenco dei Key Manager supportati in "Tool di matrice di interoperabilità NetApp".

   Cercare la soluzione **Key Manager**.

2. "Connettersi all'interfaccia utente di Cloud Volumes ONTAP".
3. Installare i certificati SSL e connettersi ai server di gestione delle chiavi esterni.

   "ONTAP 9 Guida all'alimentazione per la crittografia NetApp: Configurazione della gestione esterna delle chiavi"

# Replica dei dati tra sistemi

È possibile replicare i dati tra ambienti di lavoro scegliendo una replica dei dati una tantum per il trasferimento dei dati o una pianificazione ricorrente per il disaster recovery o la conservazione a lungo termine. Ad esempio, è possibile configurare la replica dei dati da un sistema ONTAP on-premise a Cloud Volumes ONTAP per il disaster recovery.

Cloud Manager semplifica la replica dei dati tra volumi su sistemi separati utilizzando le tecnologie SnapMirror e SnapVault. È sufficiente identificare il volume di origine e il volume di destinazione, quindi scegliere una policy e una pianificazione di replica. Cloud Manager acquista i dischi richiesti, configura le relazioni, applica la policy di replica e avvia il trasferimento di riferimento tra i volumi.

Il trasferimento di riferimento include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di origine.

Cloud Manager consente la replica dei dati tra i seguenti tipi di ambienti di lavoro:

- Da un sistema Cloud Volumes ONTAP a un altro sistema Cloud Volumes ONTAP
- Tra un sistema Cloud Volumes ONTAP e un cluster ONTAP on-premise
- Da un cluster ONTAP on-premise a un altro cluster ONTAP on-premise

## Requisiti di replica dei dati

Prima di poter replicare i dati, è necessario verificare che i requisiti specifici siano soddisfatti sia per i sistemi Cloud Volumes ONTAP che per i cluster ONTAP.

### Requisiti di versione

Prima di eseguire la replica dei dati, verificare che i volumi di origine e di destinazione eseguano versioni ONTAP compatibili. Per ulteriori informazioni, vedere "Guida all'alimentazione per la protezione dei dati".

### Requisiti specifici di Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105.

  Queste regole sono incluse nel gruppo di protezione predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).
- Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e un sistema in Azure, è necessario disporre di una connessione VPN tra AWS VPC e Azure VNET.

### Requisiti specifici dei cluster ONTAP

- È necessario installare una licenza SnapMirror attiva.
- Se il cluster si trova all'interno della propria sede, si dovrebbe disporre di una connessione dalla rete aziendale ad AWS o Azure, che in genere è una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Per ulteriori informazioni, consultare la Guida rapida di peering di cluster e SVM per la versione di ONTAP in uso.

# Configurazione della replica dei dati tra sistemi

Puoi replicare i dati tra sistemi Cloud Volumes ONTAP e cluster ONTAP scegliendo una replica dei dati una tantum, che può aiutarti a spostare i dati da e verso il cloud, o una pianificazione ricorrente, che può aiutarti con il disaster recovery o la conservazione a lungo termine.

### A proposito di questa attività

Cloud Manager supporta configurazioni di protezione dei dati semplici, fanout e a cascata:

- In una configurazione semplice, la replica avviene dal volume A al volume B.
- In una configurazione fanout, la replica avviene dal volume A a più destinazioni.
- In una configurazione a cascata, la replica avviene dal volume A al volume B e dal volume B al volume C.

È possibile configurare configurazioni fanout e a cascata in Cloud Manager impostando più repliche di dati tra sistemi. Ad esempio, replicando un volume dal sistema A al sistema B e replicando lo stesso volume dal sistema B al sistema C.

### Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume:


2. Se vengono visualizzate le pagine Source (origine) e Destination peering Setup (Configurazione peering destinazione), selezionare tutte le LIF dell'intercluster per la relazione peer del cluster.

   La rete intercluster deve essere configurata in modo che i peer del cluster dispongano di una *connettività full-mesh a coppie*, il che significa che ogni coppia di cluster in una relazione peer del cluster dispone di connettività tra tutte le proprie LIF intercluster.

   Queste pagine vengono visualizzate se l'origine o la destinazione è un cluster ONTAP con più LIF.

3. Nella pagina Source Volume Selection (selezione volume di origine), selezionare il volume che si desidera replicare.
4. Nella pagina Destination Volume Name and Tiering (Nome volume di destinazione e tiering), specificare il nome del volume di destinazione, scegliere un tipo di disco sottostante, modificare una delle opzioni avanzate e fare clic su **Continue** (continua).

   Se la destinazione è un cluster ONTAP, è necessario specificare anche la SVM di destinazione e l'aggregato.

5. Nella pagina velocità di trasferimento massima, specificare la velocità massima (in megabyte al secondo) alla quale trasferire i dati.
6. Nella pagina Replication Policy (Criteri di replica), scegliere uno dei criteri predefiniti o fare clic su **Additional Policies** (Criteri aggiuntivi), quindi selezionare uno dei criteri avanzati.

Per ulteriori informazioni, vedere "Scelta di un criterio di replica".

Se si sceglie un criterio di backup personalizzato (SnapVault), le etichette associate al criterio devono corrispondere alle etichette delle copie Snapshot sul volume di origine. Per ulteriori informazioni, vedere "Come funzionano le policy di backup".

7. Nella pagina Pianificazione, scegliere una copia singola o una pianificazione ricorrente.

   Sono disponibili diverse pianificazioni predefinite. Se si desidera una pianificazione diversa, è necessario creare una nuova pianificazione nel cluster *destination* utilizzando System Manager.

8. Nella pagina Review (esamina), rivedere le selezioni, quindi fare clic su **Go** (Vai).

**Risultato**

Cloud Manager avvia il processo di replica dei dati. È possibile visualizzare i dettagli relativi alla replica nella pagina Replication Status (Stato replica).

## Gestione delle pianificazioni e delle relazioni di replica dei dati

Dopo aver configurato la replica dei dati tra due sistemi, è possibile gestire la pianificazione e la relazione della replica dei dati da Cloud Manager.

**Fasi**

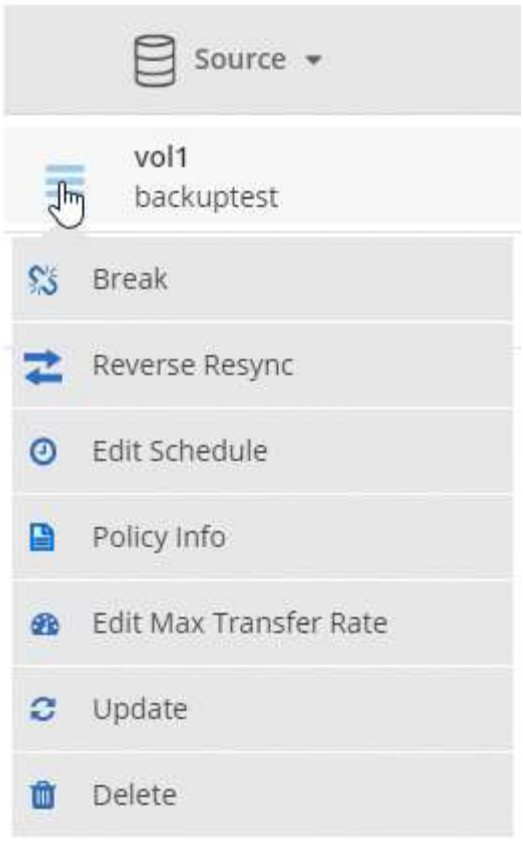
1. Nella pagina ambienti di lavoro, visualizzare lo stato della replica per tutti gli ambienti di lavoro nell'area di lavoro o per un ambiente di lavoro specifico:

| Opzione | Azione |
|---|---|
| Tutti gli ambienti di lavoro nello spazio di lavoro | Nella parte superiore di Cloud Manager, fare clic su **Replication**. |
| Un ambiente di lavoro specifico | Aprire l'ambiente di lavoro e fare clic su **Replications** (repliche). |

2. Esaminare lo stato delle relazioni di replica dei dati per verificare che siano integre.

   Se lo stato di una relazione è inattivo e lo stato di mirroring non è inizializzato, è necessario inizializzare la relazione dal sistema di destinazione per eseguire la replica dei dati in base alla pianificazione definita. È possibile inizializzare la relazione utilizzando System Manager o l'interfaccia della riga di comando (CLI). Questi stati possono essere visualizzati quando il sistema di destinazione non funziona e poi torna in linea.

3. Selezionare l'icona del menu accanto al volume di origine, quindi scegliere una delle azioni disponibili.




La seguente tabella descrive le azioni disponibili:

| Azione | Descrizione |
|---|---|
| Rompere | Interrompe la relazione tra i volumi di origine e di destinazione e attiva il volume di destinazione per l'accesso ai dati. Questa opzione viene generalmente utilizzata quando il volume di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline. Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati e la riattivazione di un volume di origine, consultare la Guida rapida al disaster recovery di ONTAP 9. |
| Risincronizzare | Consente di ripristinare una relazione interrotta tra i volumi e di riprendere la replica dei dati in base alla pianificazione definita.<br><br>Quando si risincronizzano i volumi, i contenuti del volume di destinazione vengono sovrascritti dai contenuti del volume di origine.<br><br>Per eseguire una risincronizzazione inversa, che risincronizza i dati dal volume di destinazione al volume di origine, vedere la "Guida rapida per il disaster recovery dei volumi di ONTAP 9". |
| Risincronizzazione inversa | Inverte i ruoli dei volumi di origine e di destinazione. Il contenuto del volume di origine originale viene sovrascritto dal contenuto del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline. Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati. |

| Azione | Descrizione |
| --- | --- |
| Modifica pianificazione | Consente di scegliere una pianificazione diversa per la replica dei dati. |
| Info policy | Mostra il criterio di protezione assegnato alla relazione di replica dei dati. |
| Modifica velocità di trasferimento massima | Consente di modificare la velocità massima (in kilobyte al secondo) alla quale è possibile trasferire i dati. |
| Aggiornare | Avvia un trasferimento incrementale per aggiornare il volume di destinazione. |
| Eliminare | Elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione, il che significa che la replica dei dati non avviene più tra i volumi. Questa azione non attiva il volume di destinazione per l'accesso ai dati. Questa azione elimina anche la relazione peer del cluster e la relazione peer SVM (Storage Virtual Machine), se non sono presenti altre relazioni di protezione dei dati tra i sistemi. |

**Risultato**

Dopo aver selezionato un'azione, Cloud Manager aggiorna la relazione o la pianificazione.

## Scelta di un criterio di replica

Quando si imposta la replica dei dati in Cloud Manager, potrebbe essere necessario un aiuto nella scelta di una policy di replica. Un criterio di replica definisce il modo in cui il sistema storage replica i dati da un volume di origine a un volume di destinazione.

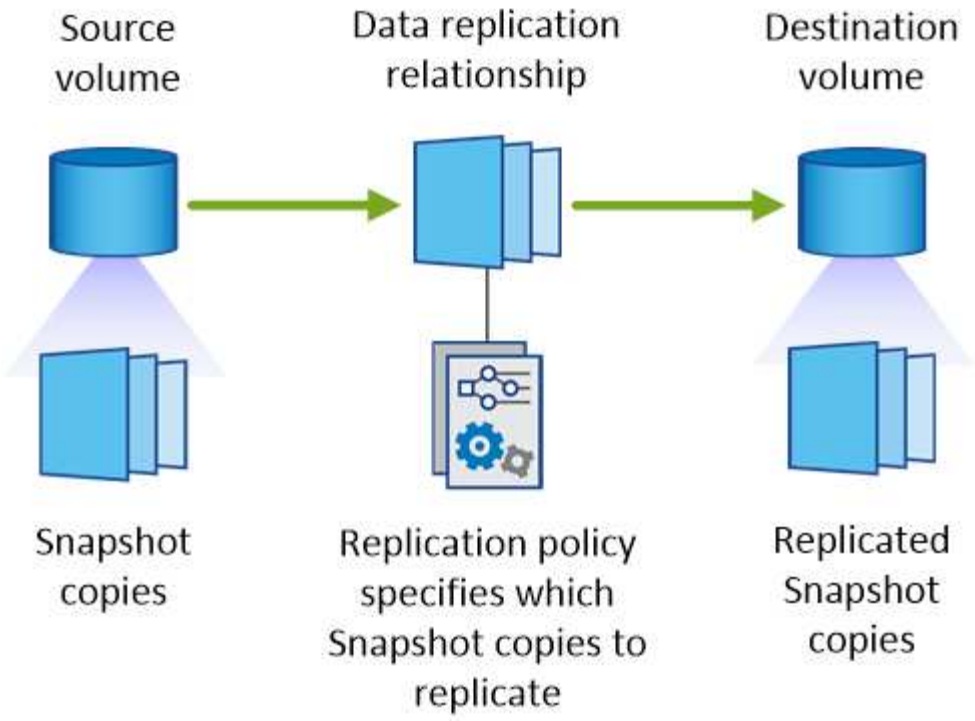
### Quali sono le funzioni delle policy di replica

Il sistema operativo ONTAP crea automaticamente i backup denominati copie Snapshot. Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato del file system in un momento specifico.

Quando si replicano i dati tra sistemi, si replicano le copie Snapshot da un volume di origine a un volume di destinazione. Un criterio di replica specifica quali copie Snapshot replicare dal volume di origine al volume di destinazione.

Le policy di replica sono anche denominate policy di *protezione*, in quanto sono basate sulle tecnologie SnapMirror e SnapVault, che forniscono protezione dal disaster recovery e backup e ripristino disk-to-disk.

La seguente immagine mostra la relazione tra le copie Snapshot e i criteri di replica:




**Tipi di policy di replica**

Esistono tre tipi di policy di replica:

- Un criterio *Mirror* replica le nuove copie Snapshot create in un volume di destinazione.

  È possibile utilizzare queste copie Snapshot per proteggere il volume di origine in preparazione al disaster recovery o alla replica dei dati una tantum. È possibile attivare il volume di destinazione per l'accesso ai dati in qualsiasi momento.

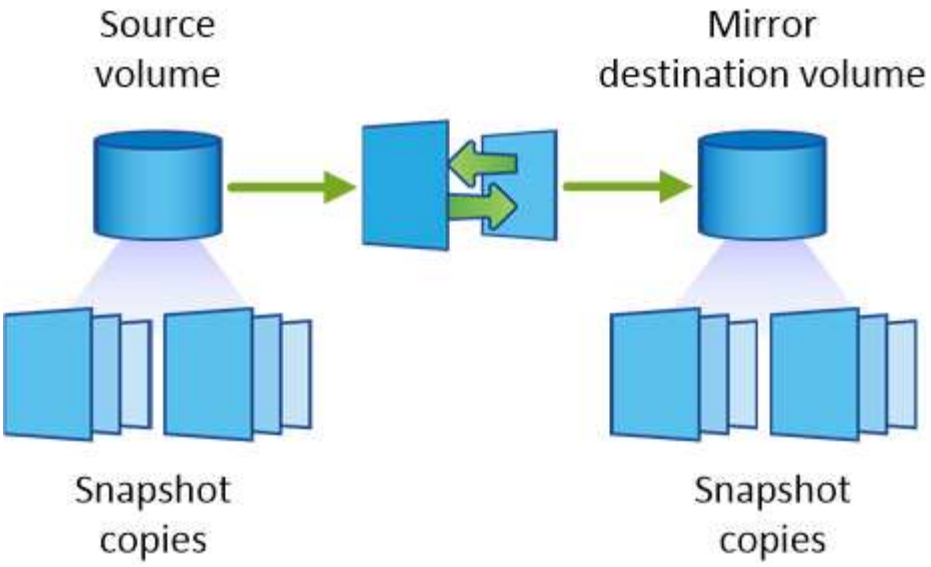
- Un criterio *Backup* replica copie Snapshot specifiche in un volume di destinazione e le conserva per un periodo di tempo più lungo rispetto al volume di origine.

  È possibile ripristinare i dati da queste copie Snapshot quando i dati vengono danneggiati o persi e conservarli per la conformità agli standard e altri scopi correlati alla governance.

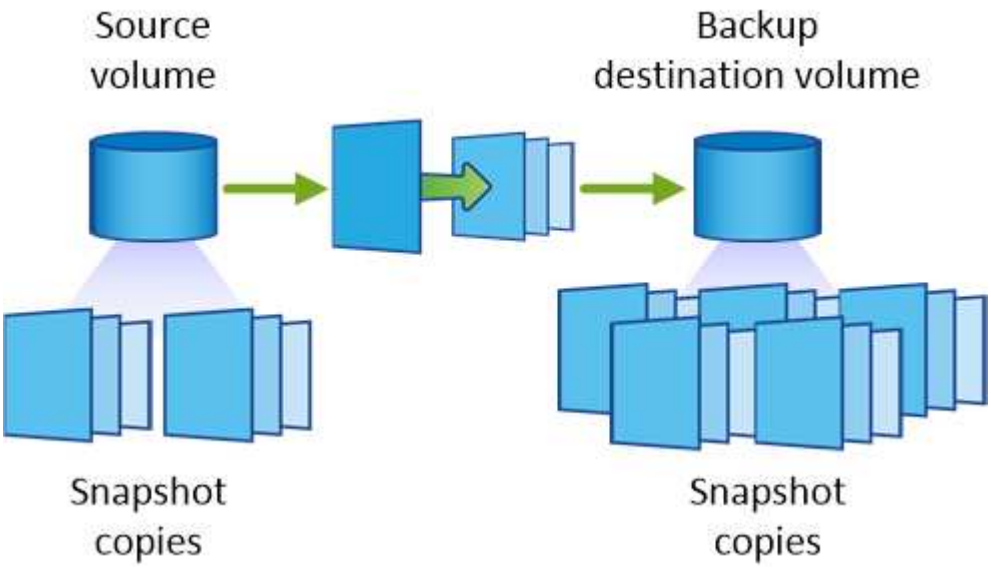
- Una policy di *Mirror e Backup* fornisce sia il disaster recovery che la conservazione a lungo termine.

  Ogni sistema include una policy di backup e mirroring predefinita, che funziona bene per molte situazioni. Se hai bisogno di policy personalizzate, puoi crearle usando System Manager.

Le seguenti immagini mostrano la differenza tra i criteri Mirror e Backup. Un criterio Mirror esegue il mirroring delle copie Snapshot disponibili sul volume di origine.




Una policy di backup conserva in genere le copie Snapshot più a lungo di quanto non vengano conservate nel volume di origine:




### Come funzionano le policy di backup

A differenza dei criteri di mirroring, i criteri di backup (SnapVault) replicano copie Snapshot specifiche in un volume di destinazione. È importante comprendere il funzionamento dei criteri di backup se si desidera utilizzare i propri criteri invece dei criteri predefiniti.

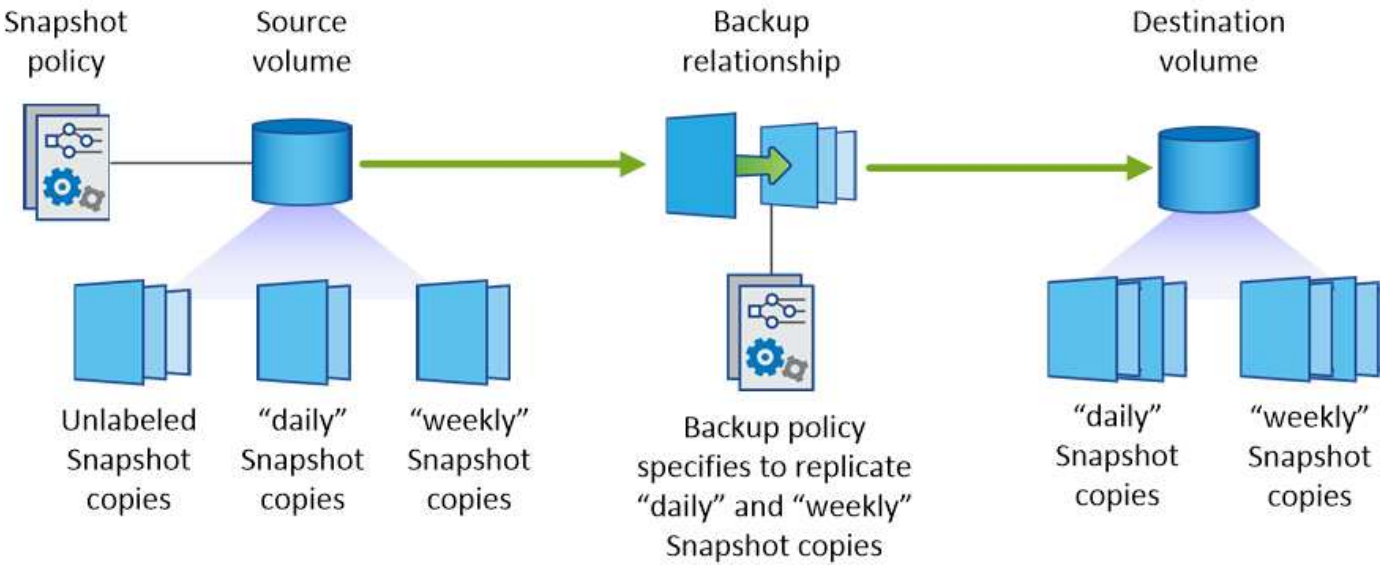
#### Comprensione della relazione tra le etichette delle copie Snapshot e le policy di backup

Una policy Snapshot definisce il modo in cui il sistema crea le copie Snapshot dei volumi. Il criterio specifica quando creare le copie Snapshot, quante copie conservare e come etichettarle. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti ed etichettarle "ogni giorno".

Un criterio di backup include regole che specificano le copie Snapshot etichettate da replicare in un volume di destinazione e il numero di copie da conservare. Le etichette definite in un criterio di backup devono corrispondere a una o più etichette definite in un criterio Snapshot. In caso contrario, il sistema non può

replicare alcuna copia Snapshot.

Ad esempio, una policy di backup che include le etichette "giornaliere" e "settimanali" produce la replica delle copie Snapshot che includono solo quelle etichette. Non vengono replicate altre copie Snapshot, come mostrato nell'immagine seguente:




**Policy predefinite e policy personalizzate**

La policy Snapshot predefinita crea copie Snapshot orarie, giornaliere e settimanali, conservando sei copie Snapshot orarie, due giornaliere e due copie Snapshot settimanali.

È possibile utilizzare facilmente un criterio di backup predefinito con il criterio Snapshot predefinito. Le policy di backup predefinite replicano copie Snapshot giornaliere e settimanali, conservando sette copie Snapshot giornaliere e 52 copie Snapshot settimanali.

Se si creano criteri personalizzati, le etichette definite da tali criteri devono corrispondere. È possibile creare policy personalizzate utilizzando System Manager.

### Replica dei dati da NetApp HCI a Cloud Volumes ONTAP

Se si tenta di replicare i dati da NetApp HCI a Cloud Volumes ONTAP, è possibile farlo su un sistema NetApp HCI che esegue il software NetApp Element utilizzando SnapMirror. In alternativa, è possibile replicare i dati sui volumi creati su un sistema ONTAP Select in esecuzione come guest virtuale in una soluzione NetApp HCI su Cloud Volumes ONTAP.

Per ulteriori informazioni, fare riferimento ai seguenti report tecnici:

- "Report tecnico 4641: Protezione dei dati NetApp HCI"
- "Report tecnico 4651: Architettura e configurazione di NetApp SolidFire SnapMirror"

# Monitorare le performance

### Scopri di più sul servizio di monitoraggio

Sfruttando "Servizio NetApp Cloud Insights", Cloud Manager ti offre informazioni sullo

stato di salute e sulle performance delle tue istanze di Cloud Volumes ONTAP e ti aiuta a risolvere i problemi e ottimizzare le performance del tuo ambiente di cloud storage.

**Caratteristiche**

- Monitorare automaticamente tutti i volumi
- Visualizza i dati sulle performance dei volumi in termini di IOPS, throughput e latenza
- Identifica i problemi di performance per ridurre al minimo l'impatto su utenti e applicazioni

**Cloud provider supportati**

Il servizio di monitoraggio è supportato con Cloud Volumes ONTAP per AWS.

**Costo**

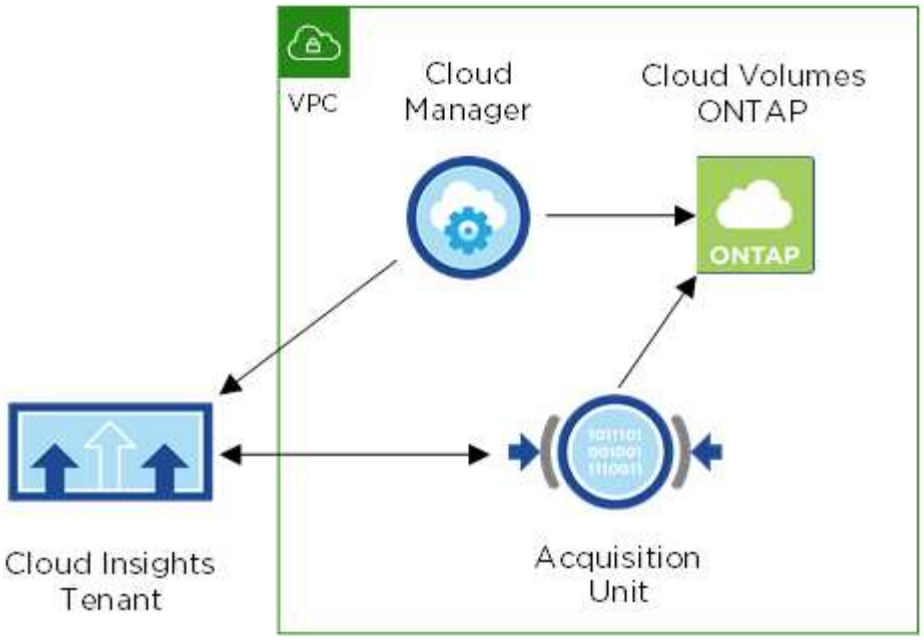
Il monitoraggio è attualmente disponibile come anteprima. L'attivazione è gratuita, ma Cloud Manager lancia una macchina virtuale nel VPC per facilitare il monitoraggio. Questa macchina virtuale comporta costi da parte del tuo cloud provider.

**Come funziona Cloud Insights con Cloud Manager**

Ad alto livello, l'integrazione di Cloud Insights con Cloud Manager funziona come segue:

1. Il servizio di monitoraggio viene attivato su Cloud Volumes ONTAP.
2. Cloud Manager configura il tuo ambiente. Esegue le seguenti operazioni:
    a. Crea un tenant Cloud Insights (chiamato anche *ambiente*) e associa tutti gli utenti del tuo account Cloud Central al tenant.
    b. Consente una versione di prova gratuita di 30 giorni di Cloud Insights.
    c. Implementa una macchina virtuale nel VPC chiamata unità di acquisizione, che facilita il monitoraggio dei volumi (si tratta della macchina virtuale menzionata nella sezione dei costi sopra).
    d. Collega l'unità di acquisizione a Cloud Volumes ONTAP e al tenant Cloud Insights.
3. In Cloud Manager, fai clic su Monitoring (monitoraggio) e utilizza i dati delle performance per risolvere i problemi e ottimizzare le performance.

La seguente immagine mostra la relazione tra questi componenti:




#### L'unità di acquisizione

Quando si attiva il monitoraggio, Cloud Manager implementa un'unità di acquisizione nella stessa sottorete del connettore.

Un' *unità di acquisizione* raccoglie i dati delle performance da Cloud Volumes ONTAP e li invia al tenant Cloud Insights. Cloud Manager interroga i dati e li presenta.

Tenere presente quanto segue sull'istanza dell'unità di acquisizione:

- L'unità di acquisizione viene eseguita su un'istanza t3.xlarge con un volume GP2 da 100 GB.
- L'istanza è denominata *AcquisitionUnit* con un hash generato (UUID) concatenato ad essa. Ad esempio: *AcquisitionUnit-FAN7FqeH*
- Per ogni connettore viene implementata una sola unità di acquisizione.
- L'istanza deve essere in esecuzione per accedere alle informazioni sulle prestazioni nella scheda Monitoring (monitoraggio).

#### Tenant Cloud Insights

Cloud Manager imposta un *tenant* per te quando abiliti il monitoraggio. Un tenant Cloud Insights consente di accedere ai dati sulle prestazioni raccolti dall'unità di acquisizione. Il tenant è una partizione di dati sicura all'interno del servizio NetApp Cloud Insights.

#### Interfaccia web di Cloud Insights

La scheda Monitoring (monitoraggio) di Cloud Manager fornisce dati di base sulle performance dei volumi. È possibile accedere all'interfaccia Web di Cloud Insights dal browser per eseguire un monitoraggio più approfondito e configurare gli avvisi per i sistemi Cloud Volumes ONTAP.

#### Prova gratuita e abbonamento

Cloud Manager offre una versione di prova gratuita di 30 giorni di Cloud Insights per fornire dati sulle performance all'interno di Cloud Manager e per consentirti di esplorare le funzionalità offerte dall'edizione standard di Cloud Insights.

Devi iscriverti entro la fine della prova gratuita, altrimenti il tenant Cloud Insights verrà cancellato. Puoi iscriverti all'edizione Basic, Standard o Premium per continuare a utilizzare la funzionalità Monitoring di Cloud Manager.

"Scopri come iscriverti a Cloud Insights".

## Monitoraggio di Cloud Volumes ONTAP in AWS

Completa alcuni passaggi per iniziare a monitorare le performance di Cloud Volumes ONTAP.

### Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

**Verificare il supporto per la configurazione**

È necessaria una nuova installazione di Cloud Manager 3.8.4 o successiva in AWS, Cloud Volumes ONTAP in AWS e devi essere un nuovo cliente Cloud Insights.

**Abilitare il monitoraggio sul sistema nuovo o esistente**

- Nuovi ambienti di lavoro: Assicurarsi di mantenere attivato il monitoraggio quando si crea l'ambiente di lavoro (attivato per impostazione predefinita).
- Ambienti di lavoro esistenti: Selezionare un ambiente di lavoro e fare clic su **Avvia monitoraggio**.

**Visualizzare i dati sulle performance**

Fare clic su **Monitoring** (monitoraggio) e visualizzare i dati delle performance dei volumi.

**Iscriviti a Cloud Insights**

Iscriviti prima della fine della prova gratuita di 30 giorni per continuare a visualizzare i dati sulle performance in Cloud Manager e Cloud Insights. "Scopri come iscriverti".

### Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata.

**Versioni supportate di Cloud Manager**

È necessaria una nuova installazione di Cloud Manager 3.8.4 o successiva. È necessaria una nuova installazione perché è necessaria una nuova infrastruttura per abilitare il servizio di monitoraggio. Questa infrastruttura è disponibile a partire dalle nuove installazioni di Cloud Manager 3.8.4.

**Versioni di Cloud Volumes ONTAP supportate**

Qualsiasi versione di Cloud Volumes ONTAP in AWS.

**Requisito Cloud Insights**

Devi essere un nuovo cliente Cloud Insights. Il monitoraggio non è supportato se si dispone già di un tenant Cloud Insights.

**Indirizzo e-mail per Cloud Central**

L'indirizzo e-mail dell'account utente Cloud Central deve essere l'indirizzo e-mail aziendale. I domini email gratuiti come gmail e hotmail non sono supportati quando si crea un tenant Cloud Insights.

**Collegamento in rete per l'unità di acquisizione**

L'unità di acquisizione utilizza l'autenticazione reciproca/bidirezionale per connettersi al server Cloud Insights. Il certificato client deve essere passato al server Cloud Insights per essere autenticato. A tale scopo, il proxy deve essere impostato per inoltrare la richiesta http al server Cloud Insights senza decifrare i dati.

L'unità di acquisizione utilizza i seguenti due endpoint per comunicare con Cloud Insights. Se si dispone di un firewall tra il server dell'unità di acquisizione e Cloud Insights, sono necessari questi endpoint durante la configurazione delle regole del firewall:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Ad esempio:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contattaci tramite la chat in-product se hai bisogno di aiuto per identificare il tuo dominio Cloud Insights e l'ID tenant.

**Collegamento in rete per il connettore**

Analogamente all'unità di acquisizione, il connettore deve essere collegato in uscita al tenant Cloud Insights. Tuttavia, l'endpoint a cui il connettore entra in contatto è leggermente diverso. Contatta l'URL host del tenant utilizzando l'ID tenant abbreviato:

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Ad esempio:
```

```
 https://abcd12345.c01.cloudinsights.netapp.com
Se hai bisogno di aiuto per identificare l'URL host del tenant, puoi
contattarci tramite la chat del prodotto.
```

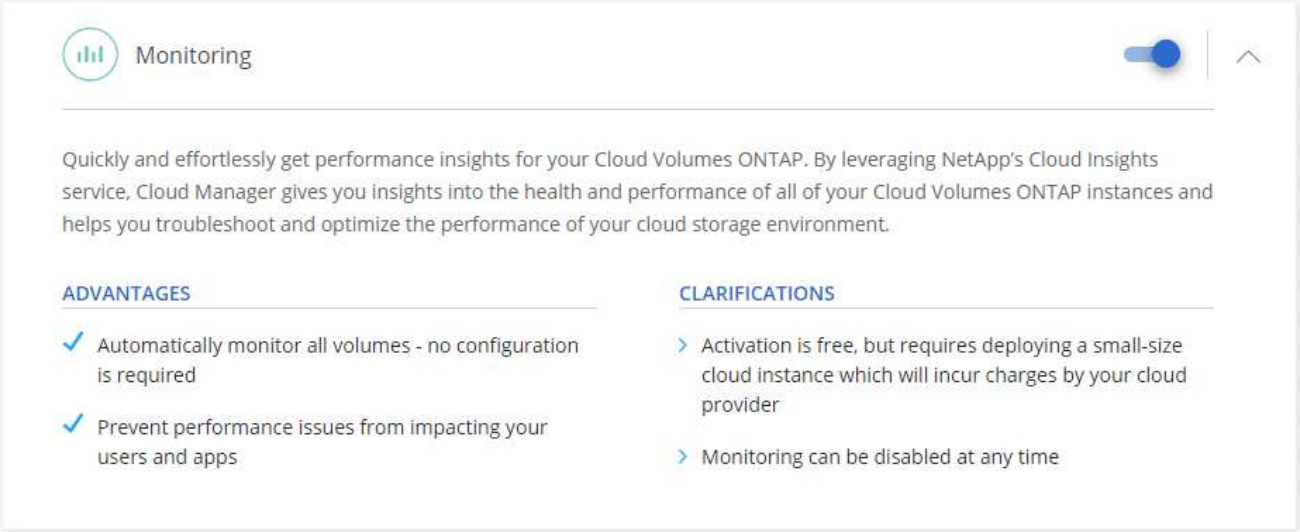
**Abilitazione del monitoraggio su un nuovo sistema**

Il servizio di monitoraggio viene attivato per impostazione predefinita nella procedura guidata dell'ambiente di

lavoro. Assicurarsi di mantenere l'opzione attivata.

**Fasi**

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina servizi, lasciare attivato il servizio e fare clic su **continua**.

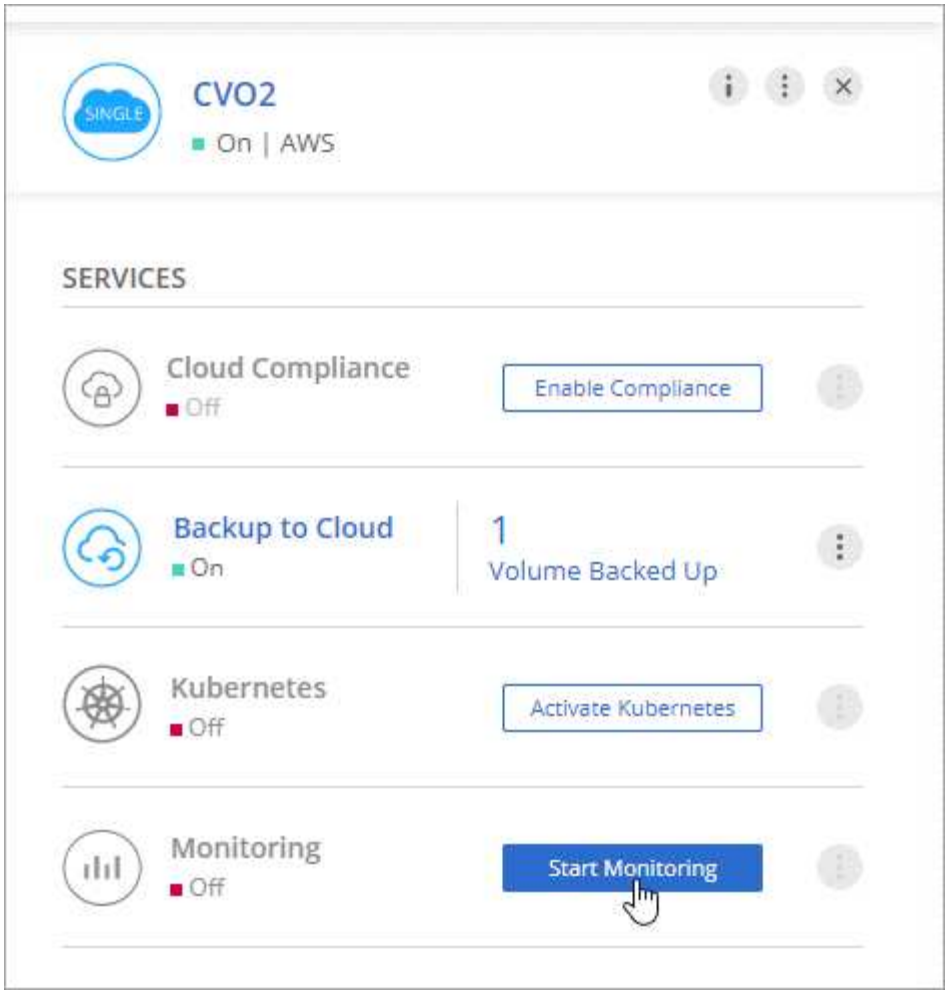



### Abilitazione del monitoraggio su un sistema esistente

Consentire il monitoraggio in qualsiasi momento dall'ambiente di lavoro.

**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare un ambiente di lavoro.
3. Nel riquadro a destra, fare clic su **Avvia monitoraggio**.



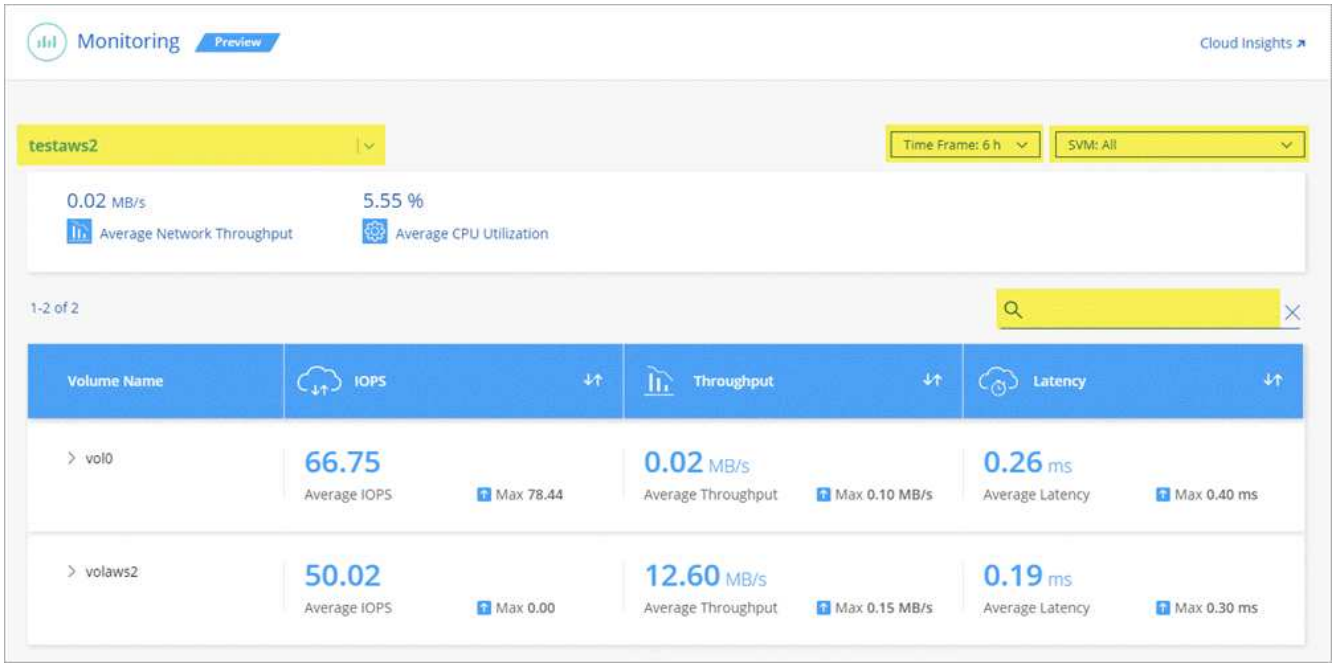

**Monitoraggio dei volumi**

Monitorate le performance visualizzando IOPS, throughput e latenza per ciascuno dei vostri volumi.

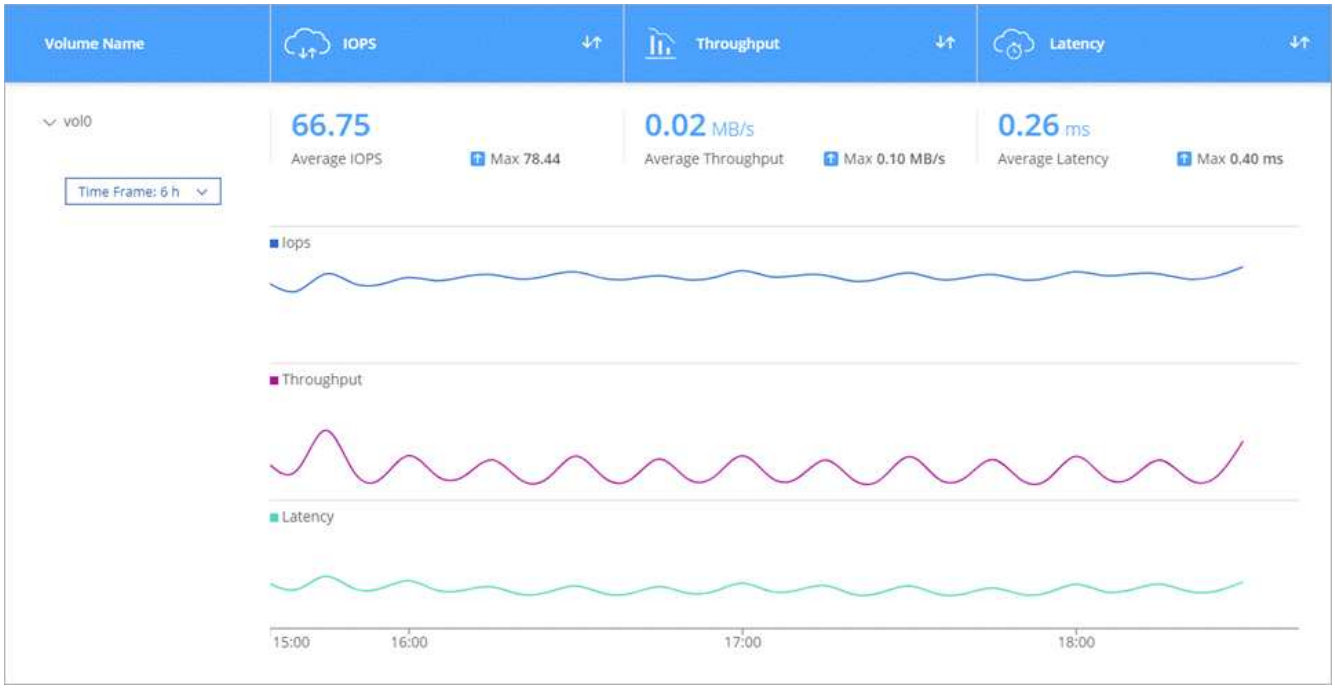
**Fasi**

1. Nella parte superiore di Cloud Manager, fare clic su **Monitoring** (monitoraggio).
2. Filtrare il contenuto della dashboard per ottenere le informazioni necessarie.
    - Selezionare un ambiente di lavoro specifico.
    - Selezionare un intervallo di tempo diverso.
    - Selezionare una SVM specifica.
    - Cercare un volume specifico.

      La seguente immagine evidenzia ciascuna di queste opzioni:




3. Fare clic su un volume nella tabella per espandere la riga e visualizzare una timeline per IOPS, throughput e latenza.




4. Utilizza i dati per identificare i problemi di performance e ridurre al minimo l'impatto su utenti e applicazioni.

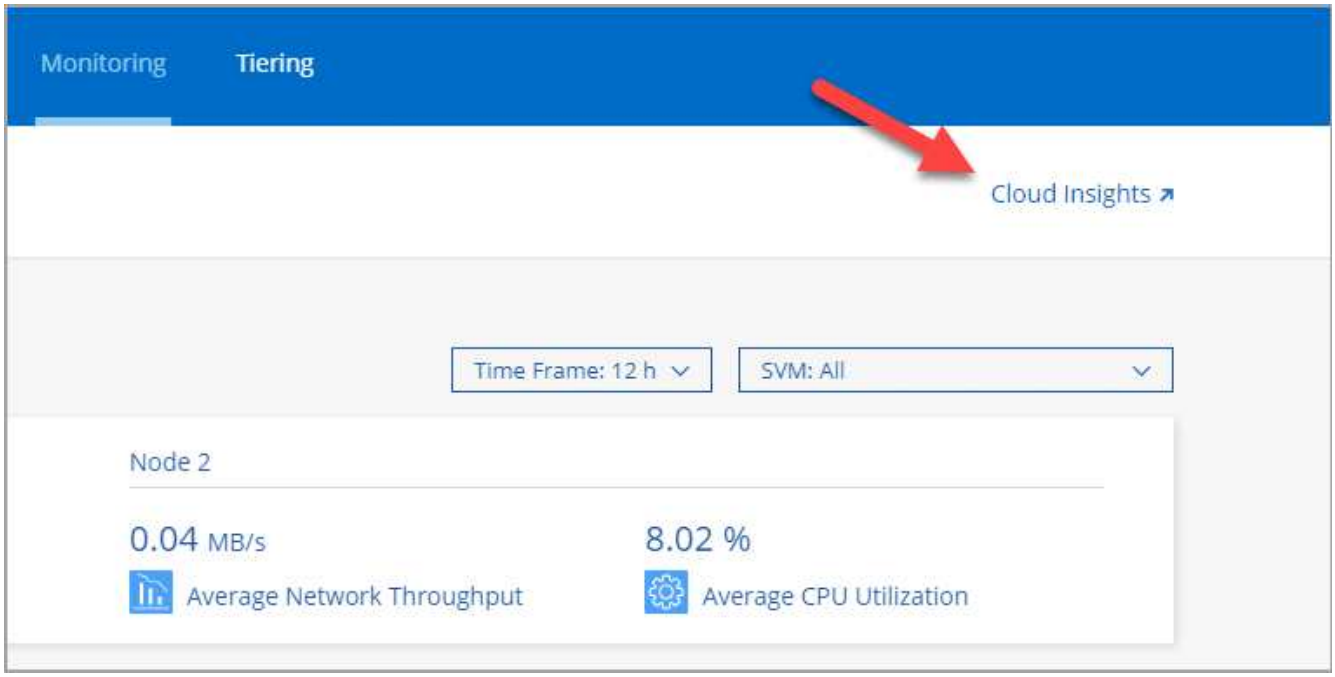
### Ottenere ulteriori informazioni da Cloud Insights

La scheda Monitoring (monitoraggio) di Cloud Manager fornisce dati di base sulle performance dei volumi. È possibile accedere all'interfaccia Web di Cloud Insights dal browser per eseguire un monitoraggio più approfondito e configurare gli avvisi per i sistemi Cloud Volumes ONTAP.

#### Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Monitoring** (monitoraggio).

2. Fare clic sul collegamento **Cloud Insights**.




**Risultato**

Cloud Insights si apre in una nuova scheda del browser. Per ulteriori informazioni, consultare la sezione "Documentazione Cloud Insights".

**Disattivazione del monitoraggio**

Se non si desidera più monitorare Cloud Volumes ONTAP, è possibile disattivare il servizio in qualsiasi momento.

Se si disattiva il monitoraggio da ciascuno degli ambienti di lavoro, sarà necessario eliminare l'istanza EC2 da soli. L'istanza è denominata *AcquisitionUnit* con un hash generato (UUID) concatenato ad essa. Ad esempio: *AcquisitionUnit-FAN7FqeH*

**Fasi**

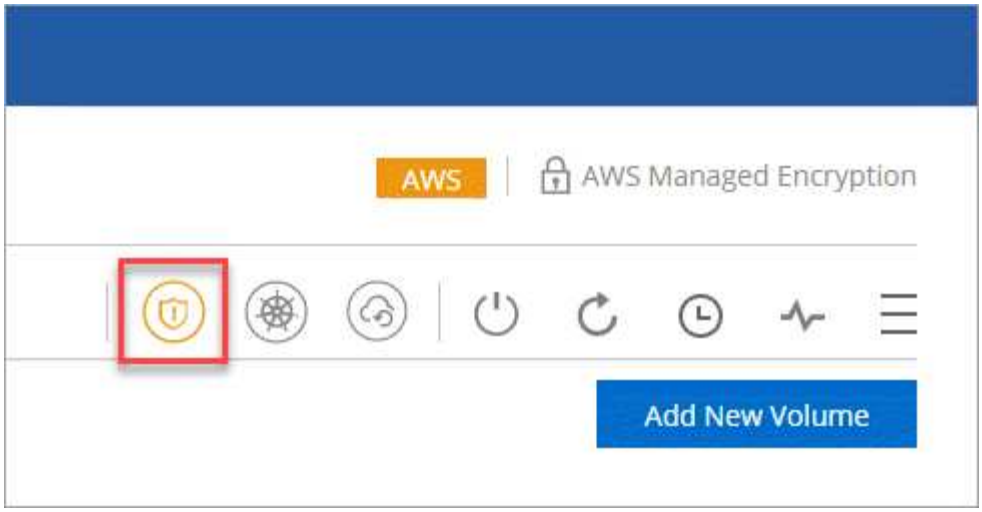
1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare un ambiente di lavoro.
3. Nel riquadro a destra, fare clic su E selezionare **Disattiva scansione**.

# Miglioramento della protezione contro ransomware

Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. Cloud Manager consente di implementare la soluzione NetApp per ransomware, che fornisce strumenti efficaci per visibilità, rilevamento e risoluzione dei problemi.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona **ransomware**.

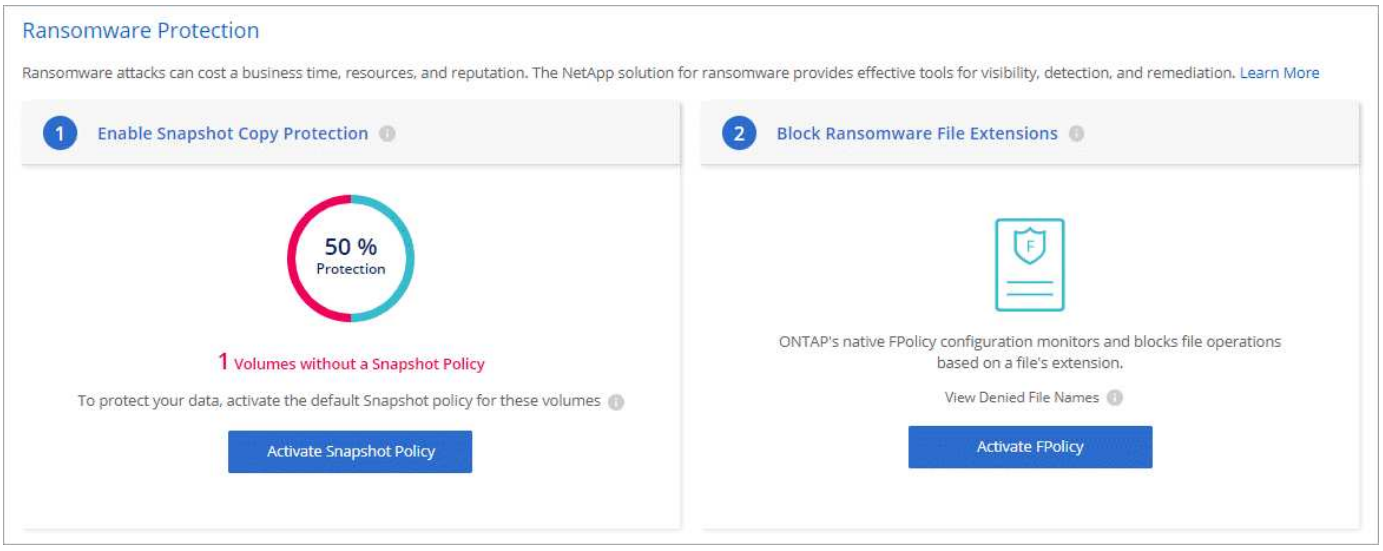



2. Implementare la soluzione NetApp per ransomware:
   a. Fare clic su **Activate Snapshot Policy** (attiva policy Snapshot) se si dispone di volumi che non hanno una policy Snapshot attivata.

      La tecnologia Snapshot di NetApp offre la migliore soluzione del settore per la risoluzione dei problemi ransomware. La chiave per un ripristino corretto è il ripristino da backup non infetti. Le copie Snapshot sono di sola lettura, impedendo la corruzione del ransomware. Possono inoltre offrire la granularità necessaria per creare immagini di una singola copia di file o di una soluzione completa di disaster recovery.

   b. Fare clic su **Activate FPolicy** (attiva FPolicy) per attivare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione di un file.

      Questa soluzione preventiva migliora la protezione dagli attacchi ransomware bloccando i tipi di file ransomware più comuni.




# Amministrare

## Registrazione di sistemi pay-as-you-go

Il supporto NetApp è incluso nei sistemi Cloud Volumes ONTAP Explore, Standard e Premium, ma è necessario prima attivare il supporto registrando i sistemi con NetApp.

**Fasi**

1. Se non hai ancora aggiunto il tuo account NetApp Support Site a Cloud Manager, vai a **Impostazioni account** e aggiungilo ora.

   "Scopri come aggiungere account NetApp Support Site".

2. Nella pagina ambienti di lavoro, fare doppio clic sul nome del sistema che si desidera registrare.
3. Fare clic sull'icona del menu, quindi su **registrazione supporto**:

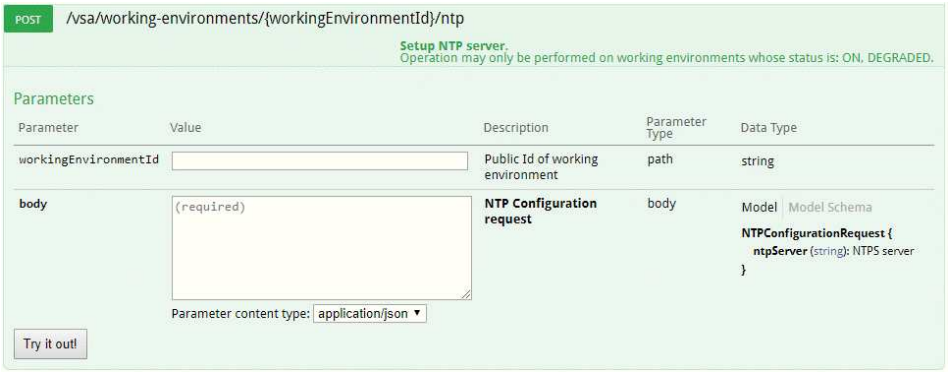

4. Selezionare un account NetApp Support Site e fare clic su **Register**.

**Risultato**

Cloud Manager registra il sistema con NetApp.

## Configurazione di Cloud Volumes ONTAP

Dopo aver implementato Cloud Volumes ONTAP, è possibile configurarlo sincronizzando l'ora del sistema utilizzando NTP ed eseguendo alcune attività facoltative da Gestore di sistema o CLI.

| Attività | Descrizione |
| --- | --- |
| Sincronizzare l'ora del sistema utilizzando NTP | La specifica di un server NTP sincronizza l'ora tra i sistemi della rete, evitando così problemi dovuti a differenze di tempo.<br><br>Specificare un server NTP utilizzando l'API Cloud Manager o dall'interfaccia utente quando si imposta un server CIFS.<br><br>• "Modifica del server CIFS"<br>• "Guida per sviluppatori API di Cloud Manager"<br><br>Ad esempio, ecco l'API per un sistema a nodo singolo in AWS:<br><br>  |
| Facoltativo: Configurare AutoSupport | AutoSupport monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp per impostazione predefinita. Se l'amministratore dell'account ha aggiunto un server proxy a Cloud Manager prima di avviare l'istanza, Cloud Volumes ONTAP viene configurato per utilizzare tale server proxy per i messaggi AutoSupport. Verificare che AutoSupport sia in grado di inviare messaggi. Per istruzioni, consultare la Guida in linea di System Manager o il "Guida di riferimento per l'amministrazione del sistema ONTAP 9". |
| Facoltativo: Configurare Cloud Manager come proxy AutoSupport | Se il tuo ambiente richiede un server proxy per inviare messaggi AutoSupport, puoi configurare Cloud Manager per agire come proxy. Non è richiesta alcuna configurazione per Cloud Manager, ad eccezione dell'accesso a Internet. È sufficiente accedere alla CLI per Cloud Volumes ONTAP ed eseguire il seguente comando:<br><br>`system node autosupport modify -proxy-url <cloud-manager-ip-address>` |
| Opzionale: Configurare EMS | Il sistema di gestione degli eventi (EMS) raccoglie e visualizza informazioni sugli eventi che si verificano nei sistemi Cloud Volumes ONTAP. Per ricevere le notifiche degli eventi, è possibile impostare le destinazioni degli eventi (indirizzi e-mail, host di trap SNMP o server syslog) e i percorsi degli eventi per una particolare gravità degli eventi. È possibile configurare EMS utilizzando la CLI. Per istruzioni, consultare "Guida rapida alla configurazione EMS di ONTAP 9". |

| Attività | Descrizione |
| --- | --- |
| Opzionale: Creare un'interfaccia di rete di gestione SVM (LIF) per i sistemi ha in più zone di disponibilità AWS | Se si desidera utilizzare SnapCenter o SnapDrive per Windows con una coppia ha, è necessaria un'interfaccia di rete per la gestione delle macchine virtuali storage (SVM). La LIF di gestione SVM deve utilizzare un indirizzo IP *mobile* quando si utilizza una coppia ha in più zone di disponibilità AWS.<br><br>Cloud Manager richiede di specificare l'indirizzo IP mobile quando si avvia la coppia ha. Se non è stato specificato l'indirizzo IP, è possibile creare autonomamente la LIF di gestione SVM da System Manager o dalla CLI. Nell'esempio seguente viene illustrato come creare la LIF dalla CLI:<br><br>`network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt` |
| Facoltativo: Modificare la posizione di backup dei file di configurazione | Cloud Volumes ONTAP crea automaticamente file di backup della configurazione contenenti informazioni sulle opzioni configurabili necessarie per il corretto funzionamento. Per impostazione predefinita, Cloud Volumes ONTAP esegue il backup dei file sull'host del connettore ogni otto ore. Se si desidera inviare i backup a una posizione alternativa, è possibile modificare la posizione in un server FTP o HTTP nel data center o in AWS. Ad esempio, è possibile che si disponga già di una posizione di backup per i sistemi di storage FAS. È possibile modificare la posizione di backup utilizzando l'interfaccia CLI. Vedere "Guida di riferimento per l'amministrazione del sistema ONTAP 9". |

## Gestione delle licenze BYOL per Cloud Volumes ONTAP

Aggiungere una licenza di sistema Cloud Volumes ONTAP BYOL per aggiungere capacità aggiuntiva, aggiornare una licenza di sistema esistente e gestire le licenze BYOL per il backup nel cloud.

### Gestione delle licenze di sistema

È possibile acquistare più licenze per un sistema Cloud Volumes ONTAP BYOL per allocare più di 368 TB di capacità. Ad esempio, è possibile acquistare due licenze per allocare fino a 736 TB di capacità a Cloud Volumes ONTAP. Oppure puoi acquistare quattro licenze per ottenere fino a 1.4 PB.

Il numero di licenze che è possibile acquistare per un sistema a nodo singolo o una coppia ha è illimitato.

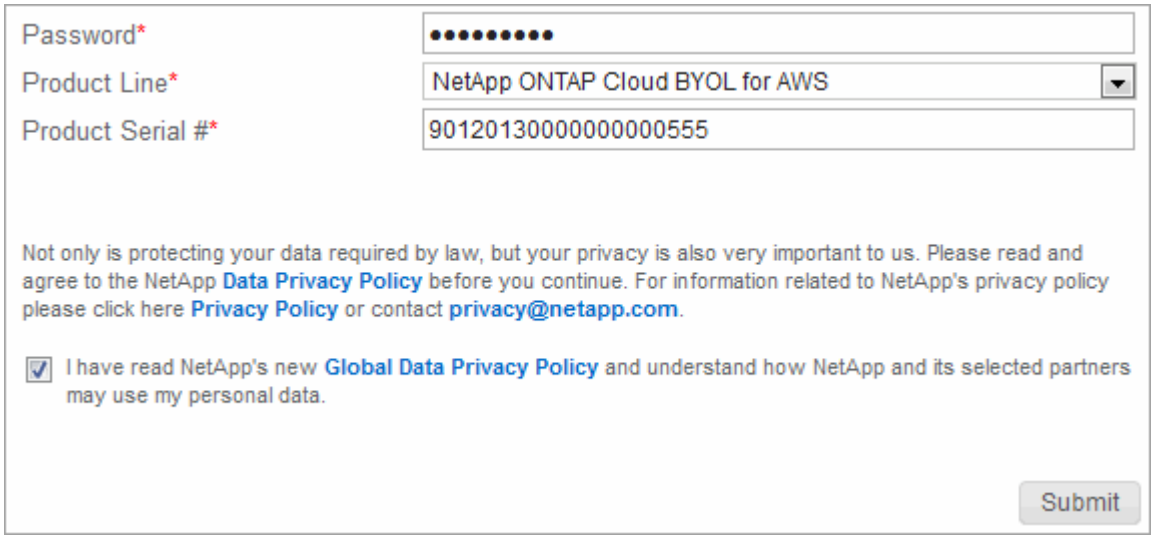
#### Ottenere un file di licenza di sistema

Nella maggior parte dei casi, Cloud Manager può ottenere automaticamente il file di licenza utilizzando l'account NetApp Support Site. In caso contrario, sarà necessario caricare manualmente il file di licenza. Se non si dispone del file di licenza, è possibile ottenerlo da netapp.com.

**Fasi**

1. Accedere alla "NetApp License file Generator" Ed effettua l'accesso utilizzando le credenziali del sito di supporto NetApp.
2. Inserire la password, scegliere il prodotto, inserire il numero di serie, confermare di aver letto e accettato l'informativa sulla privacy, quindi fare clic su **Invia**.

   **Esempio**



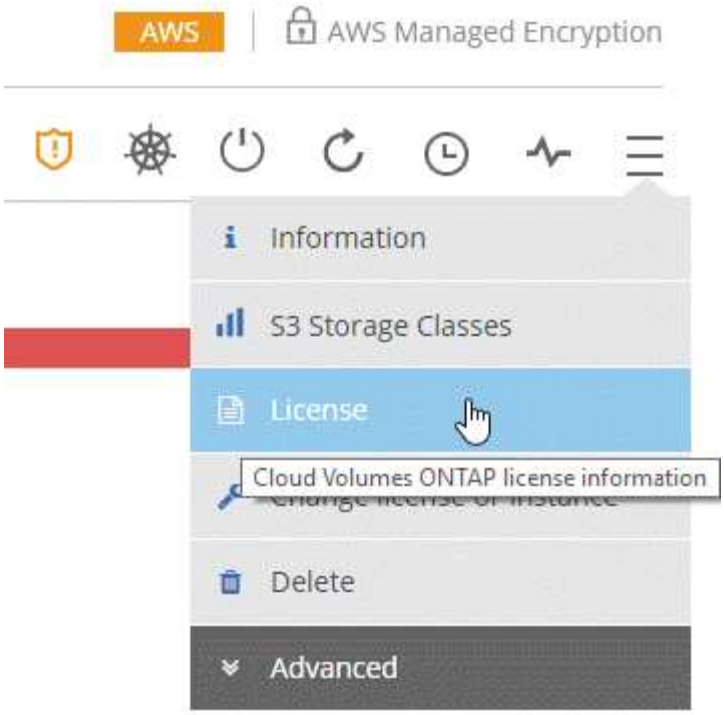

3. Scegliere se si desidera ricevere il file serialnumber.NLF JSON tramite e-mail o download diretto.

#### Aggiunta di una nuova licenza di sistema

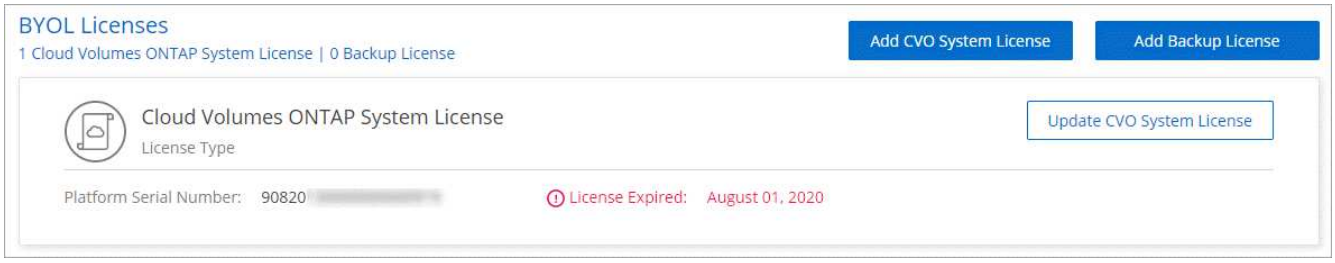
Aggiungi una nuova licenza di sistema BYOL in qualsiasi momento per allocare altri 368 TB di capacità al tuo sistema BYOL Cloud Volumes ONTAP.

**Fasi**

1. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
2. Fare clic sull'icona del menu, quindi su **licenza**.




3. Fare clic su **Add CVO System License** (Aggiungi licenza di sistema CVO).




4. Scegliere di inserire il numero di serie o di caricare il file di licenza.
5. Fare clic su **Aggiungi licenza**.

**Risultato**

Cloud Manager installa il nuovo file di licenza sul sistema Cloud Volumes ONTAP.

#### Aggiornamento di una licenza di sistema

Quando rinnovi un abbonamento BYOL contattando un rappresentante NetApp, Cloud Manager ottiene automaticamente la nuova licenza da NetApp e la installa sul sistema Cloud Volumes ONTAP.

Se Cloud Manager non riesce ad accedere al file di licenza tramite la connessione Internet sicura, è possibile ottenere il file da solo e caricarlo manualmente in Cloud Manager.

**Fasi**

1. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
2. Fare clic sull'icona del menu, quindi su **licenza**.
3. Fare clic su **Update CVO System License** (Aggiorna licenza di sistema CVO).


4. Fare clic su **Upload file** (carica file) e selezionare il file di licenza.
5. Fare clic su **Update License** (Aggiorna licenza).

**Risultato**

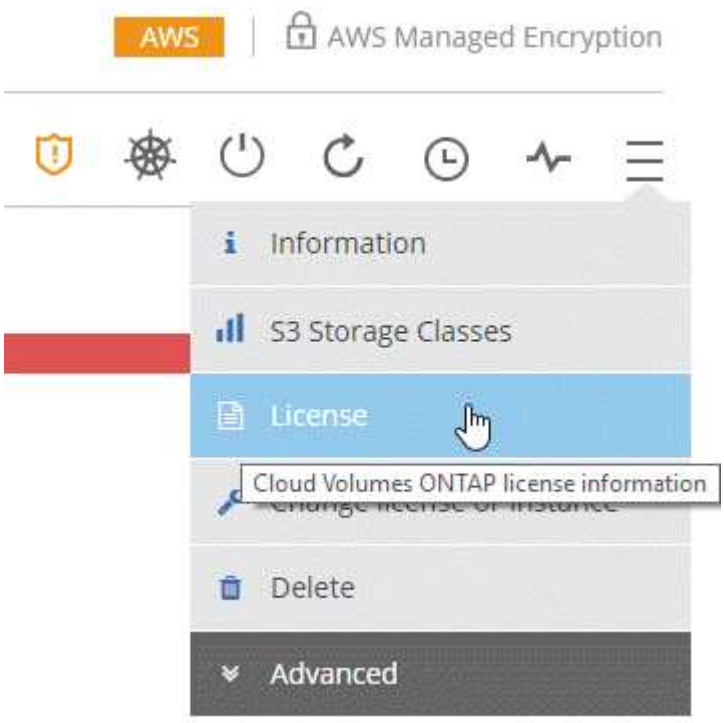
Cloud Manager aggiorna la licenza sul sistema Cloud Volumes ONTAP.

### Aggiunta e aggiornamento della licenza BYOL di backup

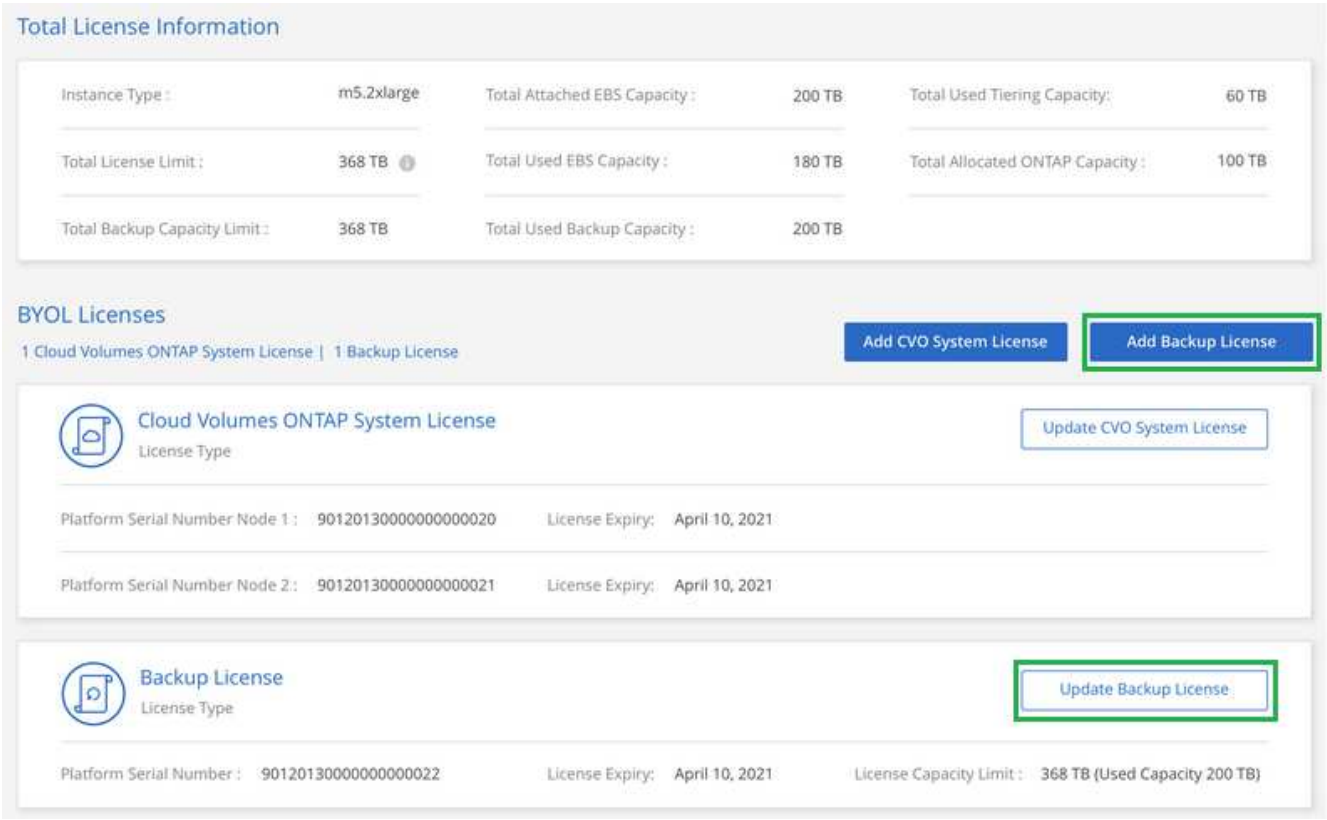
Utilizzare la pagina BYOL Licenses (licenze BYOL) per aggiungere o aggiornare la licenza BYOL di backup.

**Fasi**

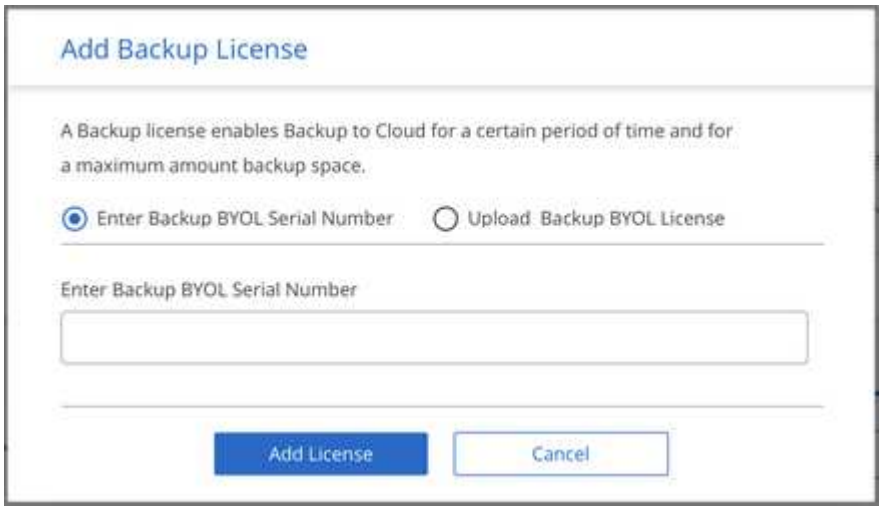
1. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
2. Fare clic sull'icona del menu, quindi su **licenza**.




3. Fare clic su **Add Backup License** (Aggiungi licenza di backup) o **Update Backup License** (Aggiorna licenza di backup) a seconda che si stia aggiungendo una nuova licenza o aggiornando una licenza esistente.




4. Inserire le informazioni sulla licenza e fare clic su **Add License** (Aggiungi licenza):
   - Se si dispone del numero di serie, selezionare l'opzione **inserire il numero di serie BYOL di backup** e immettere il numero di serie.
   - Se si dispone del file di licenza di backup, selezionare l'opzione **Upload Backup BYOL License** (carica licenza BYOL di backup) e seguire le istruzioni visualizzate per allegare il file.




**Risultato**

Cloud Manager aggiunge o aggiorna la licenza in modo che il servizio Backup to Cloud sia attivo.

## Aggiornamento del software Cloud Volumes ONTAP

Cloud Manager include diverse opzioni che è possibile utilizzare per eseguire

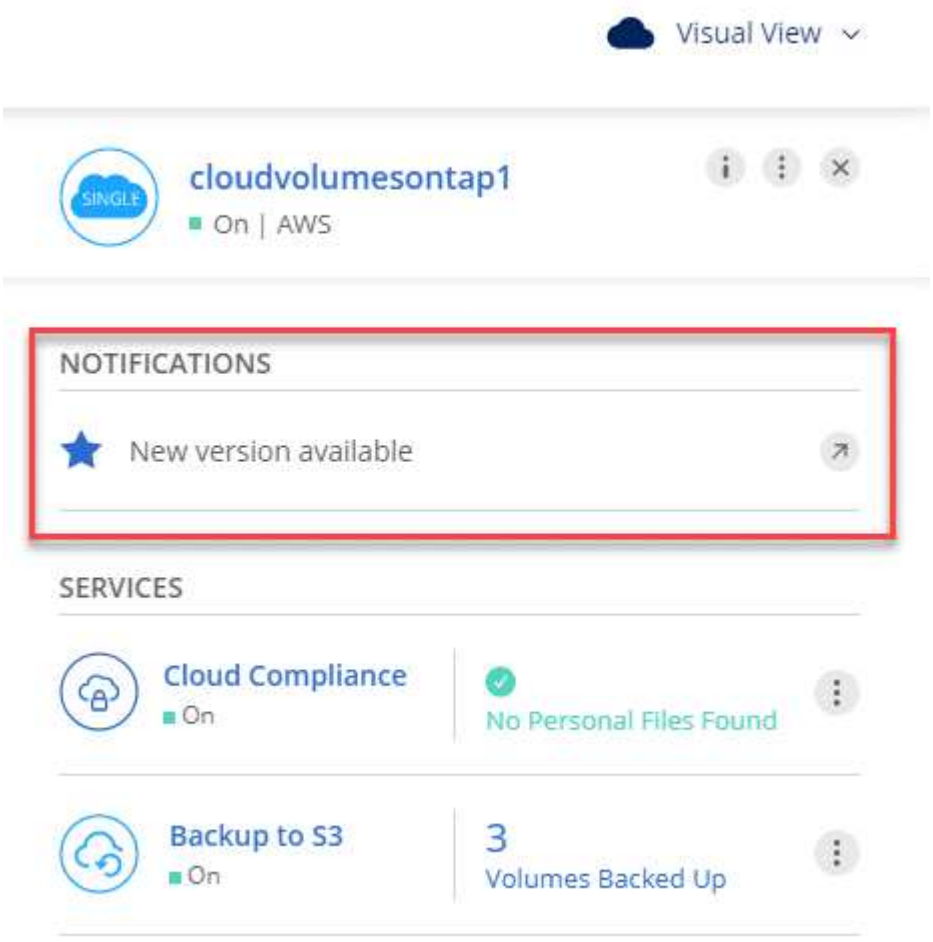
l'aggiornamento alla release corrente di Cloud Volumes ONTAP o per eseguire il downgrade di Cloud Volumes ONTAP a una release precedente. È necessario preparare i sistemi Cloud Volumes ONTAP prima di aggiornare o eseguire il downgrade del software.

### Gli aggiornamenti software devono essere completati da Cloud Manager

Gli aggiornamenti di Cloud Volumes ONTAP devono essere completati da Cloud Manager. Non aggiornare Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI. In questo modo si può influire sulla stabilità del sistema.

### Metodi per aggiornare Cloud Volumes ONTAP

Cloud Manager visualizza una notifica negli ambienti di lavoro Cloud Volumes ONTAP quando è disponibile una nuova versione di Cloud Volumes ONTAP:




È possibile avviare il processo di aggiornamento da questa notifica, che automatizza il processo ottenendo l'immagine software da un bucket S3, installando l'immagine e riavviando il sistema. Per ulteriori informazioni, vedere Aggiornamento di Cloud Volumes ONTAP dalle notifiche di Cloud Manager.

Per i sistemi ha in AWS, Cloud Manager potrebbe aggiornare il mediatore ha come parte del processo di aggiornamento.

#### Opzioni avanzate per gli aggiornamenti software

Cloud Manager offre inoltre le seguenti opzioni avanzate per l'aggiornamento del software Cloud Volumes ONTAP:

- Aggiornamenti software utilizzando un'immagine su un URL esterno

  Questa opzione è utile se Cloud Manager non riesce ad accedere al bucket S3 per aggiornare il software, se è stata fornita una patch o se si desidera eseguire il downgrade del software a una versione specifica.

  Per ulteriori informazioni, vedere Aggiornamento o downgrade di Cloud Volumes ONTAP utilizzando un server HTTP o FTP.

- Aggiornamenti software utilizzando l'immagine alternativa sul sistema

  È possibile utilizzare questa opzione per eseguire il downgrade alla versione precedente, rendendo l'immagine software alternativa l'immagine predefinita. Questa opzione non è disponibile per le coppie ha.

  Per ulteriori informazioni, vedere Downgrade di Cloud Volumes ONTAP utilizzando un'immagine locale.

### Preparazione all'aggiornamento del software Cloud Volumes ONTAP

Prima di eseguire un upgrade o un downgrade, è necessario verificare che i sistemi siano pronti ed eseguire le modifiche di configurazione richieste.

- Pianificazione del downtime
- Revisione dei requisiti di versione
- Verificare che il giveback automatico sia ancora attivato
- Sospensione dei trasferimenti SnapMirror
- Verificare che gli aggregati siano online

#### Pianificazione del downtime

Quando si aggiorna un sistema a nodo singolo, il processo di aggiornamento porta il sistema offline per un massimo di 25 minuti, durante i quali l'i/o viene interrotto.

L'aggiornamento di una coppia ha è senza interruzioni e l'i/o è ininterrotto. Durante questo processo di aggiornamento senza interruzioni, ogni nodo viene aggiornato in tandem per continuare a fornire i/o ai client.

#### Revisione dei requisiti di versione

La versione di ONTAP che è possibile aggiornare o eseguire il downgrade varia in base alla versione di ONTAP attualmente in esecuzione nel sistema.

Per informazioni sui requisiti di versione, fare riferimento a. "Documentazione di ONTAP 9: Requisiti per l'aggiornamento del cluster".

#### Verificare che il giveback automatico sia ancora attivato

Il giveback automatico deve essere attivato su una coppia Cloud Volumes ONTAP ha (impostazione predefinita). In caso contrario, l'operazione avrà esito negativo.

"Documentazione di ONTAP 9: Comandi per la configurazione del giveback automatico"

#### Sospensione dei trasferimenti SnapMirror

Se un sistema Cloud Volumes ONTAP dispone di relazioni SnapMirror attive, si consiglia di sospendere i trasferimenti prima di aggiornare il software Cloud Volumes ONTAP. La sospensione dei trasferimenti impedisce gli errori di SnapMirror. È necessario sospendere i trasferimenti dal sistema di destinazione.

**A proposito di questa attività**

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

**Fasi**

1. "Accedere a System Manager" dal sistema di destinazione.
2. Fare clic su **protezione > Relazioni**.
3. Selezionare la relazione e fare clic su **operazioni > Quiesce**.

#### Verificare che gli aggregati siano online

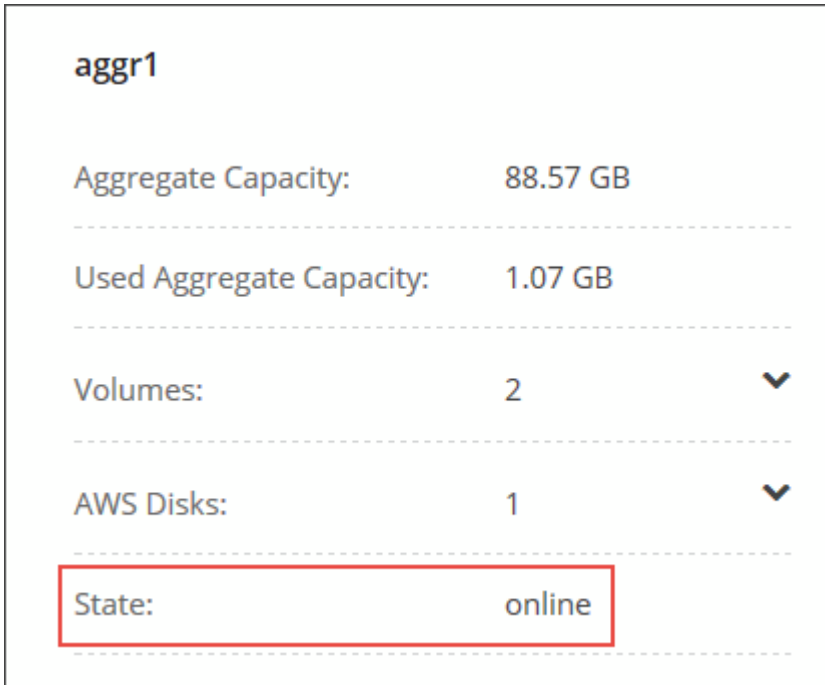
Gli aggregati per Cloud Volumes ONTAP devono essere online prima di aggiornare il software. Gli aggregati devono essere online nella maggior parte delle configurazioni, ma in caso contrario, è necessario portarli online.

**A proposito di questa attività**

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

**Fasi**

1. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
2. Selezionare un aggregato, fare clic su **Info**, quindi verificare che lo stato sia online.




3. Se l'aggregato non è in linea, utilizzare System Manager per portare l'aggregato online:
   a. "Accedere a System Manager".
   b. Fare clic su **Storage > Aggregates & Disks > Aggregates**.

c. Selezionare l'aggregato, quindi fare clic su **altre azioni > Stato > Online**.

### Aggiornamento di Cloud Volumes ONTAP dalle notifiche di Cloud Manager

Cloud Manager ti avvisa quando è disponibile una nuova versione di Cloud Volumes ONTAP. Fare clic sulla notifica per avviare il processo di aggiornamento.

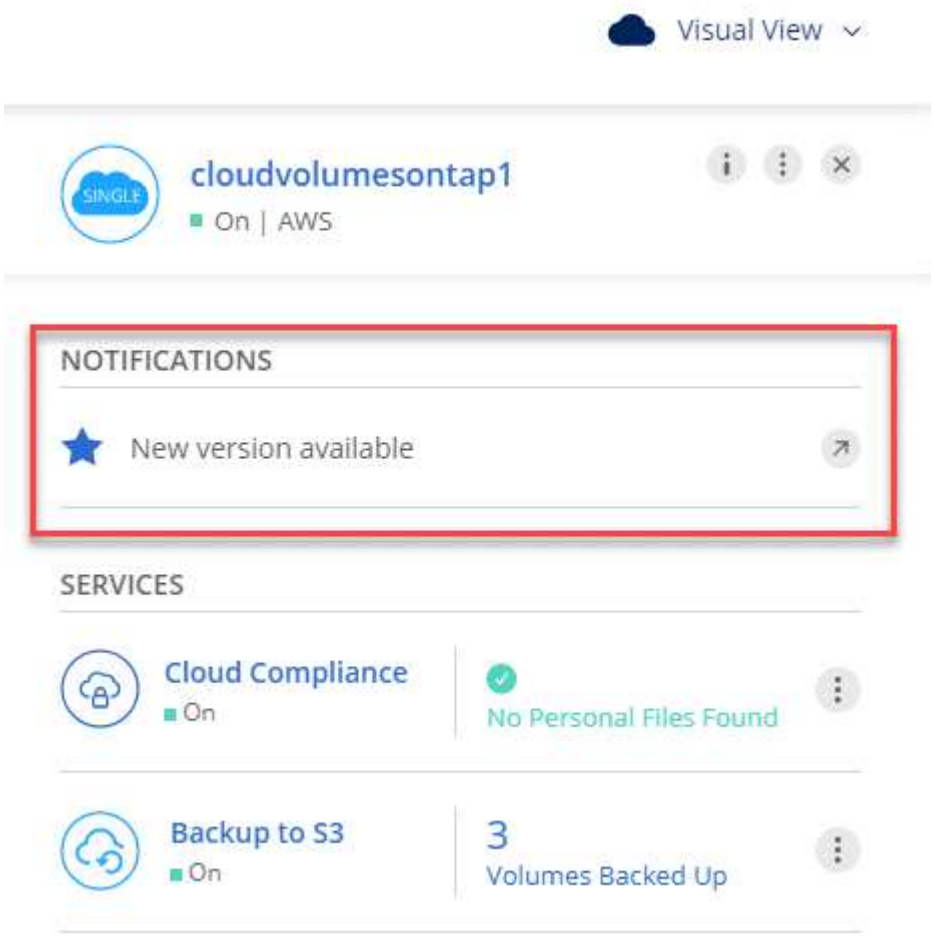
#### Prima di iniziare

Le operazioni di Cloud Manager, come la creazione di volumi o aggregati, non devono essere in corso per il sistema Cloud Volumes ONTAP.

#### Fasi

1. Fare clic su **ambienti di lavoro**.
2. Selezionare un ambiente di lavoro.

   Se è disponibile una nuova versione, nel riquadro di destra viene visualizzata una notifica:




3. Se è disponibile una nuova versione, fare clic su **Upgrade** (Aggiorna).
4. Nella pagina Release Information (informazioni sulla release), fare clic sul collegamento per leggere le Note sulla release per la versione specificata, quindi selezionare la casella di controllo **ho letto…**.
5. Nella pagina del Contratto di licenza con l'utente finale (EULA), leggere il Contratto e selezionare **i Read and Approve the EULA** (Leggi e approva il Contratto di licenza con l'utente finale).

6. Nella pagina Review and Approve (esamina e approva), leggere le note importanti, selezionare **i cape…**, quindi fare clic su **Go**.

**Risultato**

Cloud Manager avvia l'aggiornamento del software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

**Al termine**

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

### Aggiornamento o downgrade di Cloud Volumes ONTAP utilizzando un server HTTP o FTP

È possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP o FTP e avviare l'aggiornamento software da Cloud Manager. È possibile utilizzare questa opzione se Cloud Manager non riesce ad accedere al bucket S3 per aggiornare il software o se si desidera eseguire il downgrade del software.

**Fasi**

1. Configurare un server HTTP o FTP in grado di ospitare l'immagine del software Cloud Volumes ONTAP.
2. Se si dispone di una connessione VPN alla rete virtuale, è possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP o FTP nella propria rete. In caso contrario, è necessario posizionare il file su un server HTTP o FTP nel cloud.
3. Se si utilizza il proprio gruppo di protezione per Cloud Volumes ONTAP, assicurarsi che le regole in uscita consentano connessioni HTTP o FTP in modo che Cloud Volumes ONTAP possa accedere all'immagine software.

   Per impostazione predefinita, il gruppo di protezione Cloud Volumes ONTAP predefinito consente le connessioni HTTP e FTP in uscita.

4. Ottenere l'immagine software da "Il sito di supporto NetApp".
5. Copiare l'immagine del software nella directory del server HTTP o FTP da cui verrà servito il file.
6. Dall'ambiente di lavoro in Cloud Manager, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Aggiorna Cloud Volumes ONTAP**.
7. Nella pagina di aggiornamento del software, scegliere **selezionare un'immagine disponibile da un URL**, immettere l'URL, quindi fare clic su **Cambia immagine**.
8. Fare clic su **Procedi** per confermare.

**Risultato**

Cloud Manager avvia l'aggiornamento software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

**Al termine**

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

### Downgrade di Cloud Volumes ONTAP utilizzando un'immagine locale

La transizione di Cloud Volumes ONTAP a una release precedente nella stessa famiglia di release (ad esempio, da 9.5 a 9.4) viene definita downgrade. È possibile eseguire il downgrade senza assistenza durante il downgrade di cluster nuovi o di test, ma è necessario contattare il supporto tecnico se si desidera eseguire il downgrade di un cluster di produzione.

Ogni sistema Cloud Volumes ONTAP può contenere due immagini software: L'immagine corrente in esecuzione e un'immagine alternativa che è possibile avviare. Cloud Manager può modificare l'immagine alternativa in modo che sia l'immagine predefinita. È possibile utilizzare questa opzione per eseguire il downgrade alla versione precedente di Cloud Volumes ONTAP, in caso di problemi con l'immagine corrente.

#### A proposito di questa attività

Questo processo di downgrade è disponibile solo per sistemi Cloud Volumes ONTAP singoli. Non è disponibile per le coppie ha.

#### Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Aggiorna Cloud Volumes ONTAP**.
2. Nella pagina di aggiornamento del software, selezionare l'immagine alternativa, quindi fare clic su **Cambia immagine**.
3. Fare clic su **Procedi** per confermare.

#### Risultato

Cloud Manager avvia l'aggiornamento software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

#### Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

## Modifica dei sistemi Cloud Volumes ONTAP

Potrebbe essere necessario modificare la configurazione dei sistemi Cloud Volumes ONTAP in base alle esigenze di storage. Ad esempio, è possibile passare da una configurazione pay-as-you-go all'altra, modificare l'istanza o il tipo di macchina virtuale e molto altro ancora.

### Modifica dell'istanza o del tipo di macchina per Cloud Volumes ONTAP

Quando si avvia Cloud Volumes ONTAP in AWS, Azure o GCP, è possibile scegliere tra diversi tipi di istanze o computer. È possibile modificare l'istanza o il tipo di macchina in qualsiasi momento se si determina che è sottodimensionato o sovradimensionato per le proprie esigenze.

#### A proposito di questa attività

- Il giveback automatico deve essere attivato su una coppia Cloud Volumes ONTAP ha (impostazione predefinita). In caso contrario, l'operazione avrà esito negativo.

  "Documentazione di ONTAP 9: Comandi per la configurazione del giveback automatico"

- La modifica dell'istanza o del tipo di macchina influisce sui costi di servizio del provider di cloud.
- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

Cloud Manager modifica correttamente un nodo alla volta avviando il Takeover e attendendo il give back. Il team di QA di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha rilevato alcun problema sul lato client. Con la modifica delle connessioni, abbiamo visto tentativi a livello di i/o, ma il livello applicativo ha superato questi brevi "re-wire" delle connessioni NFS/CIFS.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS, **Change License or VM** for Azure o **Change License or machine** for GCP.
2. Se si utilizza una configurazione pay-as-you-go, è possibile scegliere una licenza diversa.
3. Selezionare un'istanza o un tipo di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **OK**.

**Risultato**

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

### Passaggio da una configurazione pay-as-you-go all'altra

Dopo aver lanciato i sistemi Cloud Volumes ONTAP pay-as-you-go, è possibile passare da una configurazione Explore a una configurazione standard e a una configurazione Premium in qualsiasi momento modificando la licenza. La modifica della licenza aumenta o diminuisce il limite di capacità raw e consente di scegliere tra diversi tipi di istanze AWS o tipi di macchine virtuali Azure.

In GCP, è disponibile un singolo tipo di macchina per ogni configurazione pay-as-you-go. Non è possibile scegliere tra diversi tipi di computer.

**A proposito di questa attività**

Tenere presente quanto segue circa il passaggio da una licenza pay-as-you-go all'altra:

- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

- La modifica dell'istanza o del tipo di macchina influisce sui costi di servizio del provider di cloud.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS, **Change License or VM** for Azure o **Change License or machine** for GCP.
2. Selezionare un tipo di licenza e un tipo di istanza o di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **OK**.

**Risultato**

Cloud Volumes ONTAP si riavvia con la nuova licenza, il tipo di istanza o il tipo di macchina o entrambi.

### Passaggio a una configurazione Cloud Volumes ONTAP alternativa

Se si desidera passare da un abbonamento pay-as-you-go a un abbonamento BYOL o tra un singolo sistema Cloud Volumes ONTAP e una coppia ha, è necessario implementare un nuovo sistema e replicare i dati dal sistema esistente al nuovo sistema.

**Fasi**

1. Creare un nuovo ambiente di lavoro Cloud Volumes ONTAP.

   "Avvio di Cloud Volumes ONTAP in AWS"
   "Lancio di Cloud Volumes ONTAP in Azure"
   "Avvio di Cloud Volumes ONTAP in GCP"

2. "Configurare la replica dei dati una tantum" tra i sistemi per ciascun volume da replicare.
3. Terminare il sistema Cloud Volumes ONTAP di cui non si ha più bisogno "eliminazione dell'ambiente di lavoro originale".

### Modifica della velocità di scrittura su normale o alta

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. La velocità di scrittura predefinita è normale. È possibile passare a un'elevata velocità di scrittura se sono richieste prestazioni di scrittura rapide per il carico di lavoro. Prima di modificare la velocità di scrittura, è necessario "comprendere le differenze tra le impostazioni normali e quelle alte".

**A proposito di questa attività**

- Assicurarsi che operazioni come la creazione di volumi o aggregati non siano in corso.
- Tenere presente che questa modifica riavvia Cloud Volumes ONTAP, il che significa che l'i/o viene interrotto.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > Writing Speed** (Avanzate > velocità di scrittura).
2. Selezionare **normale** o **alta**.

   Se scegli High, allora devi leggere il messaggio "capisco…" e confermare selezionando la casella.

3. Fare clic su **Save** (Salva), controllare il messaggio di conferma, quindi fare clic su **Proceed** (Procedi).

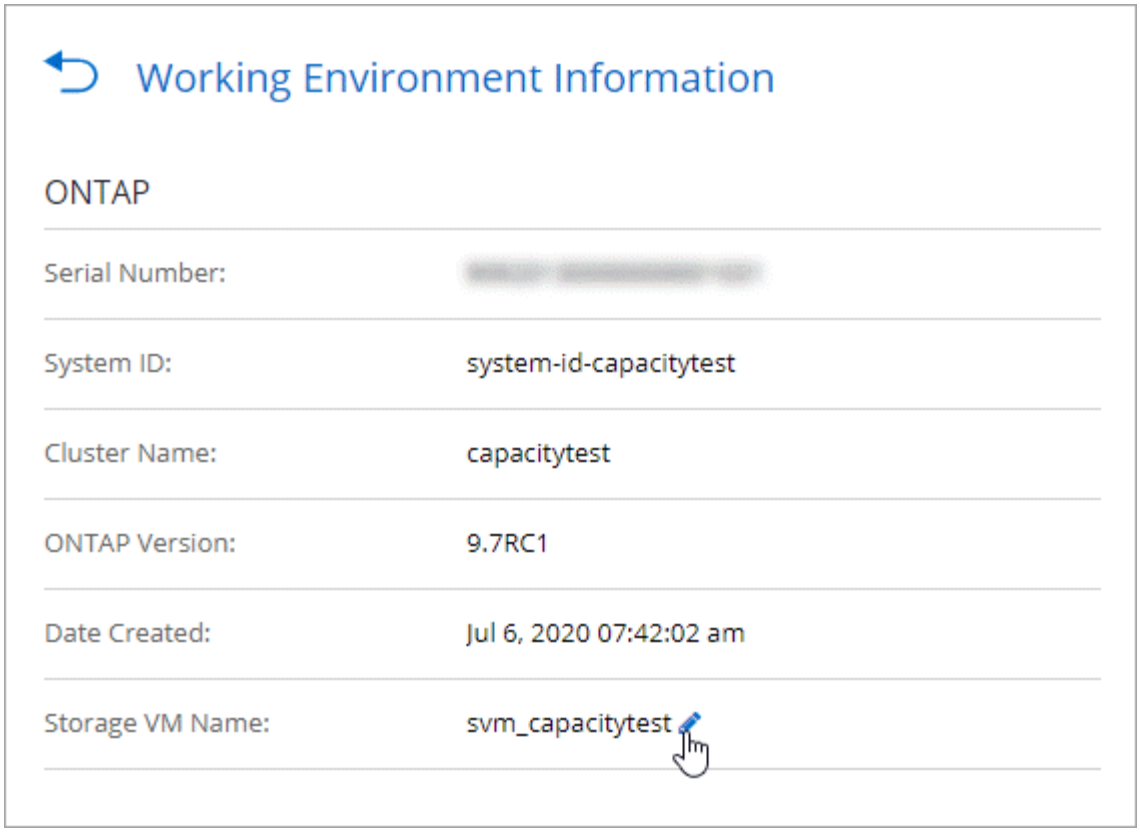
### Modifica del nome della VM di storage

Cloud Manager assegna automaticamente un nome alla singola VM di storage creata per Cloud Volumes ONTAP. È possibile modificare il nome della SVM se si dispone di standard di denominazione rigorosi. Ad esempio, è possibile che il nome corrisponda a quello delle SVM per i cluster ONTAP.

Tuttavia, se hai creato altre SVM per Cloud Volumes ONTAP, non puoi rinominare le SVM da Cloud Manager. È necessario eseguire questa operazione direttamente da Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **informazioni**.
2. Fare clic sull'icona di modifica a destra del nome della VM di storage.




3. Nella finestra di dialogo Modify SVM Name (Modifica nome SVM), modificare il nome, quindi fare clic su **Save** (Salva).

### Modifica della password per Cloud Volumes ONTAP

Cloud Volumes ONTAP include un account di amministrazione del cluster. Se necessario, puoi modificare la password per questo account da Cloud Manager.

> Non modificare la password per l'account admin tramite System Manager o CLI. La password non verrà riflessa in Cloud Manager. Di conseguenza, Cloud Manager non è in grado di monitorare correttamente l'istanza.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Imposta password**.
2. Inserire due volte la nuova password, quindi fare clic su **Save** (Salva).

   La nuova password deve essere diversa da una delle ultime sei password utilizzate.

### Modifica della MTU di rete per istanze di grandi dimensioni c4.4x4 e c4.8x

Per impostazione predefinita, Cloud Volumes ONTAP è configurato per l'utilizzo di 9,000 MTU (detti anche frame jumbo) quando si sceglie l'istanza c4.4xlarge o l'istanza c4.8xlarge in AWS. È possibile modificare l'MTU di rete a 1,500 byte, se più appropriato per la configurazione di rete.

**A proposito di questa attività**

Un'unità MTU (Network Maximum Transmission Unit) di 9,000 byte può fornire il massimo throughput di rete possibile per configurazioni specifiche.

9,000 MTU è una buona scelta se i client nello stesso VPC comunicano con il sistema Cloud Volumes ONTAP e alcuni o tutti questi client supportano anche 9,000 MTU. Se il traffico lascia il VPC, può verificarsi la frammentazione dei pacchetti, che peggiora le performance.

Una MTU di rete di 1,500 byte è una buona scelta se client o sistemi esterni al VPC comunicano con il sistema Cloud Volumes ONTAP.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > Network Utilization** (Avanzate > utilizzo rete).
2. Selezionare **Standard** o **Jumbo Frame**.
3. Fare clic su **Cambia**.

#### Modifica delle tabelle di percorso associate alle coppie ha in più AWS AZS

È possibile modificare le tabelle di routing AWS che includono i percorsi verso gli indirizzi IP mobili per una coppia ha. È possibile eseguire questa operazione se i nuovi client NFS o CIFS devono accedere a una coppia ha in AWS.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **informazioni**.
2. Fare clic su **Route Tables**.
3. Modificare l'elenco delle tabelle di percorso selezionate, quindi fare clic su **Save** (Salva).

**Risultato**

Cloud Manager invia una richiesta AWS per modificare le tabelle di routing.

## Gestione dello stato di Cloud Volumes ONTAP

Puoi arrestare e avviare Cloud Volumes ONTAP da Cloud Manager per gestire i costi di calcolo del cloud.

#### Pianificazione degli arresti automatici di Cloud Volumes ONTAP

Per ridurre i costi di calcolo, potrebbe essere necessario arrestare Cloud Volumes ONTAP durante intervalli di tempo specifici. Invece di eseguire questa operazione manualmente, è possibile configurare Cloud Manager in modo che arresti e riavvii automaticamente i sistemi in orari specifici.

**A proposito di questa attività**

Quando si pianifica un arresto automatico del sistema Cloud Volumes ONTAP, Cloud Manager posticipa l'arresto se è in corso un trasferimento di dati attivo. Cloud Manager arresta il sistema al termine del trasferimento.

Questa attività pianifica gli arresti automatici di entrambi i nodi in una coppia ha.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona dell'orologio:

2. Specificare il programma di arresto:

   a. Scegliere se si desidera spegnere il sistema ogni giorno, ogni giorno feriale, ogni fine settimana o qualsiasi combinazione delle tre opzioni.

   b. Specificare quando si desidera spegnere il sistema e per quanto tempo si desidera disattivarlo.

      **Esempio**

      La seguente immagine mostra un programma che indica a Cloud Manager di spegnere il sistema ogni sabato alle 12:00 per 48 ore. Cloud Manager riavvia il sistema ogni lunedì alle 12:00


3. Fare clic su **Save** (Salva).

**Risultato**

Cloud Manager salva la pianificazione. L'icona dell'orologio cambia per indicare che è stata impostata una pianificazione: 

### Arresto di Cloud Volumes ONTAP

L'arresto di Cloud Volumes ONTAP consente di risparmiare sui costi di calcolo e di creare snapshot dei dischi root e di boot, che possono essere utili per la risoluzione dei problemi.

**A proposito di questa attività**

Quando si interrompe una coppia ha, Cloud Manager arresta entrambi i nodi.

**Fasi**

1. Dall'ambiente di lavoro, fare clic sull'icona **Spegni**.

2. Mantenere l'opzione per creare snapshot abilitata, in quanto le snapshot possono abilitare il ripristino del sistema.
3. Fare clic su **Spegni**.

   L'arresto del sistema può richiedere fino a qualche minuto. È possibile riavviare i sistemi in un secondo momento dalla pagina ambiente di lavoro.

## Monitoraggio dei costi delle risorse AWS

Cloud Manager consente di visualizzare i costi delle risorse associati all'esecuzione di Cloud Volumes ONTAP in AWS. Puoi anche vedere quanto denaro hai risparmiato utilizzando le funzionalità di NetApp che possono ridurre i costi di storage.

### A proposito di questa attività

Cloud Manager aggiorna i costi quando aggiorni la pagina. Fare riferimento ad AWS per i dettagli sui costi finali.

### Fase

1. Verificare che Cloud Manager possa ottenere informazioni sui costi da AWS:
   a. Assicurarsi che il criterio IAM che fornisce le autorizzazioni a Cloud Manager includa le seguenti azioni:

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Queste azioni sono incluse nella versione più recente "Policy di Cloud Manager". I nuovi sistemi implementati da NetApp Cloud Central includono automaticamente queste autorizzazioni.

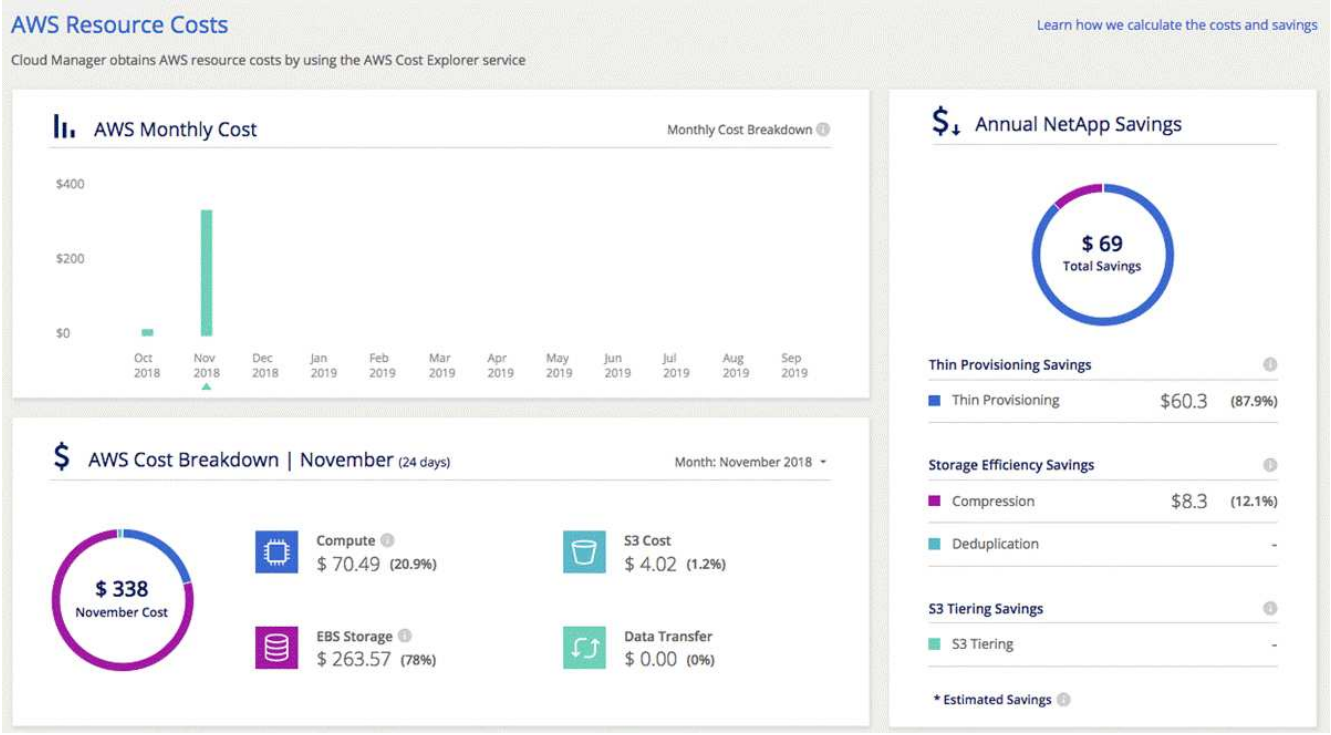
   b. "Attivare il tag **WorkingEnvironmentId**".

      Per tenere traccia dei costi AWS, Cloud Manager assegna un tag di allocazione dei costi alle istanze di Cloud Volumes ONTAP. Dopo aver creato il primo ambiente di lavoro, attivare il tag **WorkingEnvironmentId**. I tag definiti dall'utente non vengono visualizzati nei report di fatturazione AWS finché non vengono attivati nella console di fatturazione e gestione dei costi.

2. Nella pagina Working Environments (ambienti di lavoro), selezionare un ambiente di lavoro Cloud Volumes ONTAP e fare clic su **Cost** (costo).

   La pagina dei costi visualizza i costi per i mesi correnti e precedenti e mostra i risparmi annuali di NetApp, se hai abilitato le funzionalità di risparmio sui volumi di NetApp.

   La seguente immagine mostra una pagina di costo di esempio:




## Connessione a Cloud Volumes ONTAP

Se è necessario eseguire una gestione avanzata di Cloud Volumes ONTAP, è possibile farlo utilizzando Gestione di sistema di OnCommand o l'interfaccia della riga di comando.

### Connessione a System Manager in corso

Potrebbe essere necessario eseguire alcune attività di Cloud Volumes ONTAP da Gestore di sistema, uno strumento di gestione basato su browser che viene eseguito sul sistema Cloud Volumes ONTAP. Ad esempio, se si desidera creare LUN, è necessario utilizzare System Manager.

#### Prima di iniziare

Il computer da cui si accede a Cloud Manager deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario effettuare l'accesso a Cloud Manager da un host jump in AWS o Azure.

> Quando vengono implementate in più zone di disponibilità AWS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

#### Fasi

1. Dalla pagina ambienti di lavoro, fare doppio clic sul sistema Cloud Volumes ONTAP che si desidera gestire con Gestione sistema.
2. Fare clic sull'icona del menu, quindi fare clic su **Advanced > System Manager**.
3. Fare clic su **Avvia**.

   System Manager viene caricato in una nuova scheda del browser.

4. Nella schermata di accesso, inserire **admin** nel campo User Name (Nome utente), immettere la password specificata al momento della creazione dell'ambiente di lavoro, quindi fare clic su **Sign in** (Accedi).

**Risultato**

Viene caricata la console di System Manager. Ora puoi utilizzarlo per gestire Cloud Volumes ONTAP.

### Connessione all'interfaccia utente di Cloud Volumes ONTAP

La CLI di Cloud Volumes ONTAP consente di eseguire tutti i comandi amministrativi ed è una buona scelta per attività avanzate o se si è più comodi nell'utilizzo della CLI. È possibile connettersi all'interfaccia CLI utilizzando Secure Shell (SSH).

**Prima di iniziare**

L'host da cui si utilizza SSH per connettersi a Cloud Volumes ONTAP deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario utilizzare SSH da un host jump in AWS o Azure.

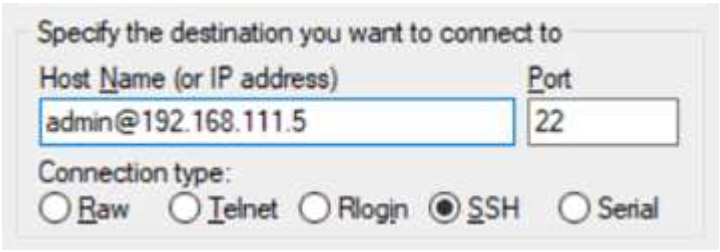
> Quando vengono implementate in più AZS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

**Fasi**

1. In Cloud Manager, identificare l'indirizzo IP dell'interfaccia di gestione del cluster:
   a. Nella pagina ambienti di lavoro, selezionare il sistema Cloud Volumes ONTAP.
   b. Copiare l'indirizzo IP di gestione del cluster visualizzato nel riquadro di destra.
2. Utilizzare SSH per connettersi all'indirizzo IP dell'interfaccia di gestione del cluster utilizzando l'account admin.

   **Esempio**

   L'immagine seguente mostra un esempio di utilizzo di PuTTY:

3. Al prompt di login, inserire la password per l'account admin.

   **Esempio**

   ```
   Password: ********
   COT2::>
   ```

## Aggiunta di sistemi Cloud Volumes ONTAP esistenti a Cloud Manager

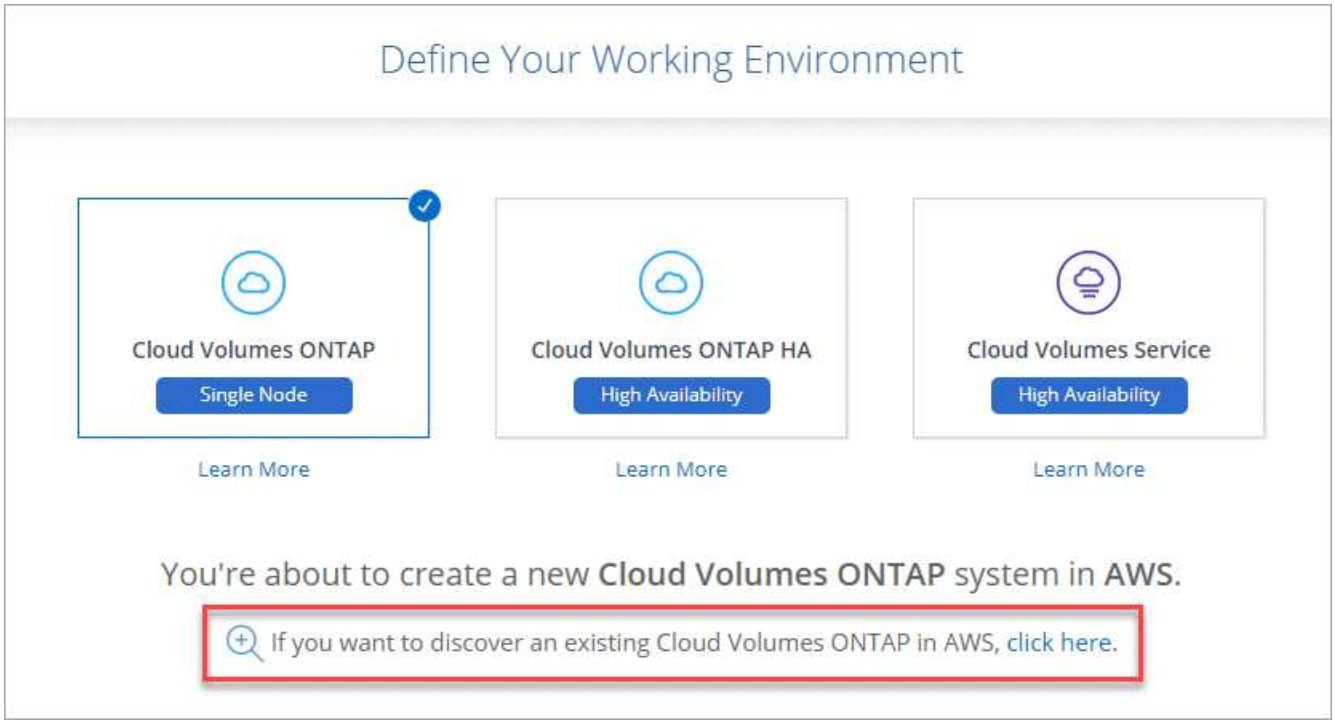
Puoi scoprire e aggiungere sistemi Cloud Volumes ONTAP esistenti a Cloud Manager. Puoi farlo se hai implementato un nuovo sistema Cloud Manager.

**Prima di iniziare**

È necessario conoscere la password dell'account utente amministratore di Cloud Volumes ONTAP.

**Fasi**

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro**.
2. Selezionare il provider cloud in cui risiede il sistema.
3. Scegliere il tipo di sistema Cloud Volumes ONTAP.
4. Fare clic sul collegamento per individuare un sistema esistente.




5. Nella pagina Area, scegliere l'area in cui sono in esecuzione le istanze, quindi selezionare le istanze.
6. Nella pagina credenziali, immettere la password per l'utente amministratore di Cloud Volumes ONTAP, quindi fare clic su **Go**.

**Risultato**

Cloud Manager aggiunge le istanze di Cloud Volumes ONTAP allo spazio di lavoro.

## Eliminazione di un ambiente di lavoro Cloud Volumes ONTAP

Si consiglia di eliminare i sistemi Cloud Volumes ONTAP da Cloud Manager, piuttosto che dalla console del provider di cloud. Ad esempio, se si termina un'istanza di Cloud Volumes ONTAP con licenza da AWS, non è possibile utilizzare la chiave di licenza per un'altra istanza. Per rilasciare la licenza, è necessario eliminare l'ambiente di lavoro da Cloud Manager.

### A proposito di questa attività

Quando si elimina un ambiente di lavoro, Cloud Manager termina le istanze, elimina dischi e snapshot.

> Le istanze di Cloud Volumes ONTAP dispongono di una protezione di terminazione abilitata per prevenire la terminazione accidentale da parte di AWS. Tuttavia, se si interrompe un'istanza di Cloud Volumes ONTAP da AWS, è necessario accedere alla console di AWS CloudFormation ed eliminare lo stack dell'istanza. Il nome dello stack è il nome dell'ambiente di lavoro.

### Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Delete** (Elimina).
2. Digitare il nome dell'ambiente di lavoro, quindi fare clic su **Delete** (Elimina).

   L'eliminazione dell'ambiente di lavoro può richiedere fino a 5 minuti.

## Informazioni sul copyright



## Informazioni sul marchio commerciale