USA Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
April 23, 2024

Sommario

USA Cloud Volumes ONTAP

Gestione delle licenze

Gestione delle licenze basate sulla capacità

Gestisci le tue licenze basate sulla capacità dal portafoglio digitale BlueXP per assicurarti che il tuo account NetApp disponga di capacità sufficiente per i tuoi sistemi Cloud Volumes ONTAP.

Le *licenze basate sulla capacità* consentono di pagare Cloud Volumes ONTAP per TIB di capacità.

Il *portafoglio digitale BlueXP* consente di gestire le licenze per Cloud Volumes ONTAP da un'unica postazione. È possibile aggiungere nuove licenze e aggiornare quelle esistenti.

> Mentre l'utilizzo e la misurazione effettivi per i prodotti e i servizi gestiti in BlueXP sono sempre calcolati in GiB e TiB, i termini GB/GiB e TB/TiB vengono utilizzati in modo intercambiabile. Ciò si riflette negli elenchi di Cloud Marketplace, nelle quotazioni, nelle descrizioni degli elenchi e in altra documentazione di supporto

"Scopri di più sulle licenze Cloud Volumes ONTAP".

Modalità di aggiunta delle licenze al portafoglio digitale BlueXP

Dopo aver acquistato una licenza dal rappresentante commerciale NetApp, NetApp invierà un'e-mail con il numero di serie e ulteriori dettagli sulla licenza.

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

Se BlueXP non riesce ad aggiungere la licenza, sarà necessario aggiungerla manualmente al portafoglio digitale. Ad esempio, se il connettore è installato in una posizione che non dispone di accesso a Internet, sarà necessario aggiungere le licenze autonomamente. Scopri come aggiungere le licenze acquistate al tuo account.

Visualizzare la capacità consumata nell'account

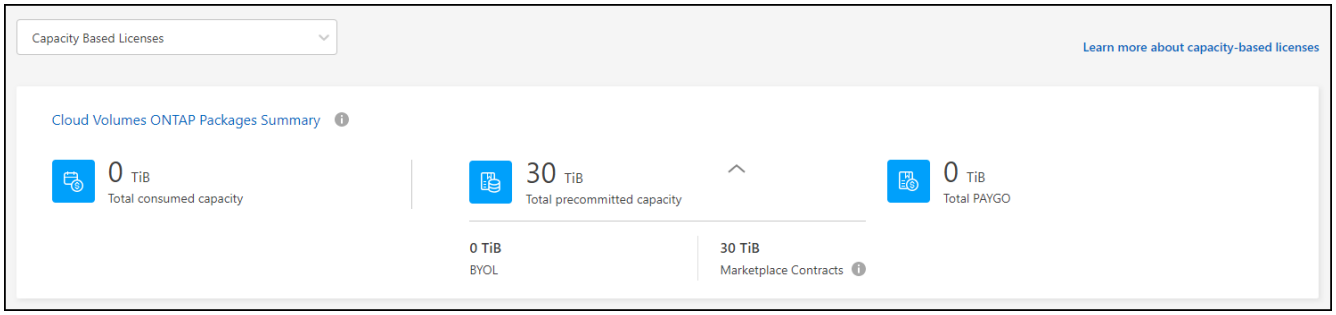
Il portafoglio digitale BlueXP mostra la capacità totale consumata nell'account e la capacità consumata dal pacchetto di licenze. Questo può aiutarti a capire come ti stai addebitando e se hai bisogno di acquistare capacità aggiuntiva.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, mantenere selezionata l'opzione **licenze basate sulla capacità**.
3. Visualizza il riepilogo dei pacchetti, che mostra la capacità consumata, la capacità preimpegnata totale e la capacità PAYGO totale.
    - *Capacità totale consumata* è la capacità totale di provisioning di tutti i sistemi Cloud Volumes ONTAP del tuo account NetApp. La ricarica si basa sulle dimensioni fornite da ciascun volume, indipendentemente dallo spazio locale, utilizzato, memorizzato o effettivo all'interno del volume.

- *Capacità totale preassegnata* è la capacità totale concessa in licenza (BYOL o Marketplace Contract) acquistata da NetApp.
- *Total PAYGO* è la capacità totale fornita con gli abbonamenti al cloud marketplace. L'addebito tramite PAYGO viene utilizzato solo se la capacità consumata è superiore alla capacità concessa in licenza o se non è disponibile alcuna licenza BYOL nel portafoglio digitale BlueXP.

  Ecco un esempio di riepilogo dei pacchetti Cloud Volumes ONTAP nel portafoglio digitale BlueXP:



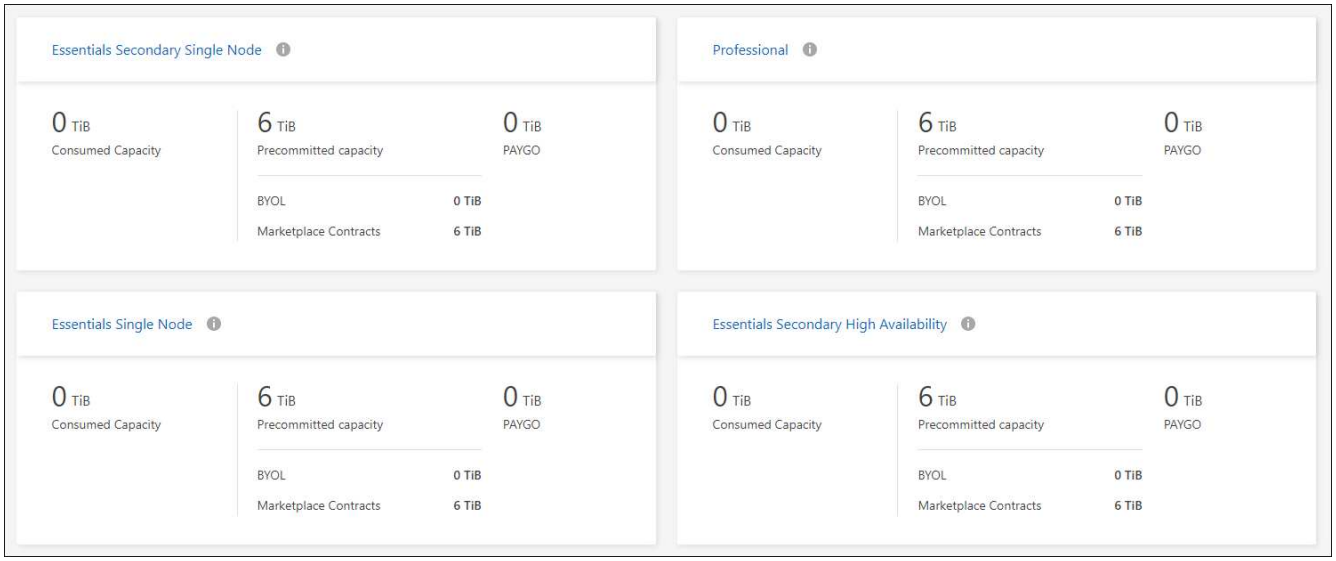
4. Sotto il riepilogo, visualizzare la capacità consumata per ciascun pacchetto di licenze.

   - *Capacità consumata* mostra la capacità dei volumi per quel pacchetto. Per ulteriori informazioni su un pacchetto specifico, passare il mouse sulla descrizione del comando.

     Per comprendere meglio le capacità visualizzate per il pacchetto Essentials, è necessario conoscere il funzionamento della ricarica. "Scopri come ricaricare il pacchetto Essentials".

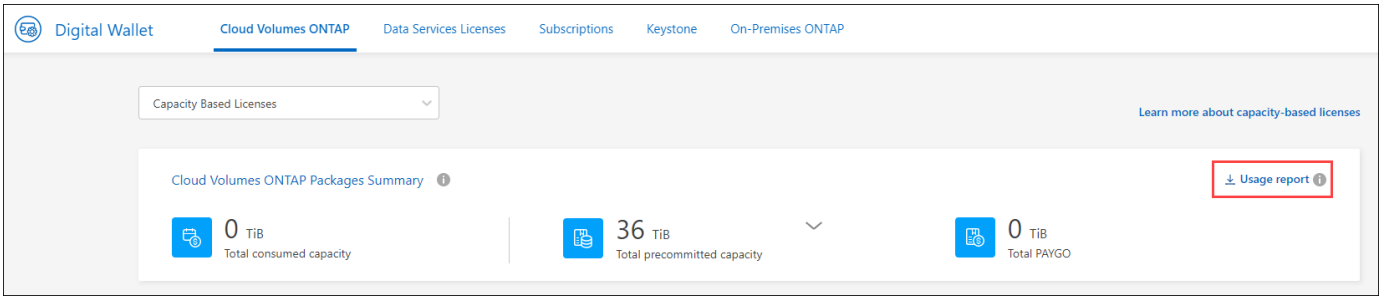
   - *Capacità consigliata* è la capacità concessa in licenza (BYOL o Marketplace Contract) acquistata da NetApp.
     - *BYOL* mostra la capacità concessa in licenza acquistata da NetApp per questo tipo di pacchetto.
     - *Contratti Marketplace* Mostra la capacità concessa in licenza acquistata con un contratto Marketplace per questo tipo di pacchetto.
   - *PAYGO* mostra la capacità consumata in base al modello di consumo delle licenze.

     Ecco un esempio per un account che dispone di diversi pacchetti di licenza:



Scarica i report sull'utilizzo

Gli amministratori degli account possono scaricare quattro report sull'utilizzo dal portafoglio digitale in BlueXP. Questi report sull'utilizzo forniscono i dettagli relativi alla capacità delle sottoscrizioni e indicano come vengono addebitate le risorse nelle sottoscrizioni Cloud Volumes ONTAP. I report scaricabili acquisiscono i dati in un momento specifico e possono essere facilmente condivisi con altri.



I seguenti report sono disponibili per il download. I valori di capacità mostrati sono in TIB.

- **Utilizzo di alto livello**: Questo report mostra esattamente ciò che è contenuto nella scheda "Riepilogo pacchetti Cloud Volumes ONTAP" nel portafoglio digitale. Include le seguenti informazioni:
  - Capacità totale consumata
  - Capacità totale preimpegnata
  - Capacità BYOL totale
  - Capacità totale dei contratti Marketplace
  - Capacità PAYGO totale
- **Utilizzo del pacchetto Cloud Volumes ONTAP**: Questo report mostra esattamente ciò che è riportato sulle schede delle confezioni nel portafoglio digitale. Include le seguenti informazioni per ciascun pacchetto, ad eccezione del pacchetto i/o ottimizzato:
  - Capacità totale consumata
  - Capacità totale preimpegnata
  - Capacità BYOL totale
  - Capacità totale dei contratti Marketplace
  - Capacità PAYGO totale
- **Utilizzo delle VM di storage**: Questo report mostra come viene suddivisa la capacità di carico tra i sistemi Cloud Volumes ONTAP e le macchine virtuali di storage (SVM). Queste informazioni non sono disponibili su nessuna schermata del portafoglio digitale. Include le seguenti informazioni:
  - ID e nome dell'ambiente di lavoro (visualizzato come UUID)
  - Cloud
  - ID account NetApp
  - Configurazione dell'ambiente di lavoro
  - Nome SVM
  - Capacità fornita
  - Roundup di capacità caricata
  - Termine di fatturazione per il mercato

    - Pacchetto o funzione Cloud Volumes ONTAP
    - Addebito del nome dell'abbonamento a SaaS Marketplace
    - Addebito dell'ID di abbonamento SaaS Marketplace
    - Tipo di carico di lavoro
- **Utilizzo dei volumi**: Questo report mostra come la capacità caricata viene suddivisa per volumi in un ambiente di lavoro. Queste informazioni non sono disponibili su nessuna schermata del portafoglio digitale. Include le seguenti informazioni:
    - ID e nome dell'ambiente di lavoro (visualizzato come UUID)
    - Nome SVN
    - ID volume
    - Tipo di volume
    - Capacità di provisioning del volume

> I volumi FlexClone non sono inclusi in questo report perché questi tipi di volumi non comportano costi.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, mantenere selezionata l'opzione **licenze basate sulla capacità** e fare clic su **rapporto di utilizzo**.

   Il report di utilizzo viene scaricato.

3. Aprire il file scaricato per accedere ai report.

Aggiungere le licenze acquistate all'account

Se le licenze acquistate non vengono visualizzate nel portafoglio digitale BlueXP, è necessario aggiungerle a BlueXP in modo che la capacità sia disponibile per Cloud Volumes ONTAP.

Di cosa hai bisogno

- È necessario fornire a BlueXP il numero di serie della licenza o del file di licenza.
- Se si desidera inserire il numero di serie, è necessario prima "Aggiungi il tuo account NetApp Support Site a BlueXP". Si tratta dell'account NetApp Support Site autorizzato ad accedere al numero di serie.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, mantenere selezionata l'opzione **licenze basate sulla capacità** e fare clic su **Aggiungi licenza**.
3. Inserire il numero di serie della licenza basata sulla capacità o caricare il file di licenza.

   Se hai inserito un numero di serie, devi anche selezionare l'account NetApp Support Site autorizzato ad accedere al numero di serie.

4. Fare clic su **Aggiungi licenza**.

Aggiornare una licenza basata sulla capacità

Se hai acquistato capacità aggiuntiva o hai esteso il periodo di validità della licenza, BlueXP aggiorna automaticamente la licenza nel portafoglio digitale. Non c'è niente da fare.

Tuttavia, se BlueXP è stato implementato in una posizione che non dispone di accesso a Internet, sarà necessario aggiornare manualmente la licenza in BlueXP.

Di cosa hai bisogno

Il file di licenza (o *files* se si dispone di una coppia ha).

> Per ulteriori informazioni su come ottenere un file di licenza, vedere "Ottenere un file di licenza di sistema".

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, fare clic sul menu delle azioni accanto alla licenza e selezionare **Aggiorna licenza**.
3. Caricare il file di licenza.
4. Fare clic su **carica licenza**.

Modificare i metodi di ricarica

Le licenze basate sulla capacità sono disponibili sotto forma di *pacchetto*. Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, è possibile scegliere tra diversi pacchetti di licenze in base alle proprie esigenze aziendali. Se le proprie esigenze cambiano dopo aver creato l'ambiente di lavoro, è possibile modificare il pacchetto in qualsiasi momento. Ad esempio, è possibile passare dal pacchetto Essentials al pacchetto Professional.

"Scopri di più sui pacchetti di licenza basati sulla capacità".

A proposito di questa attività

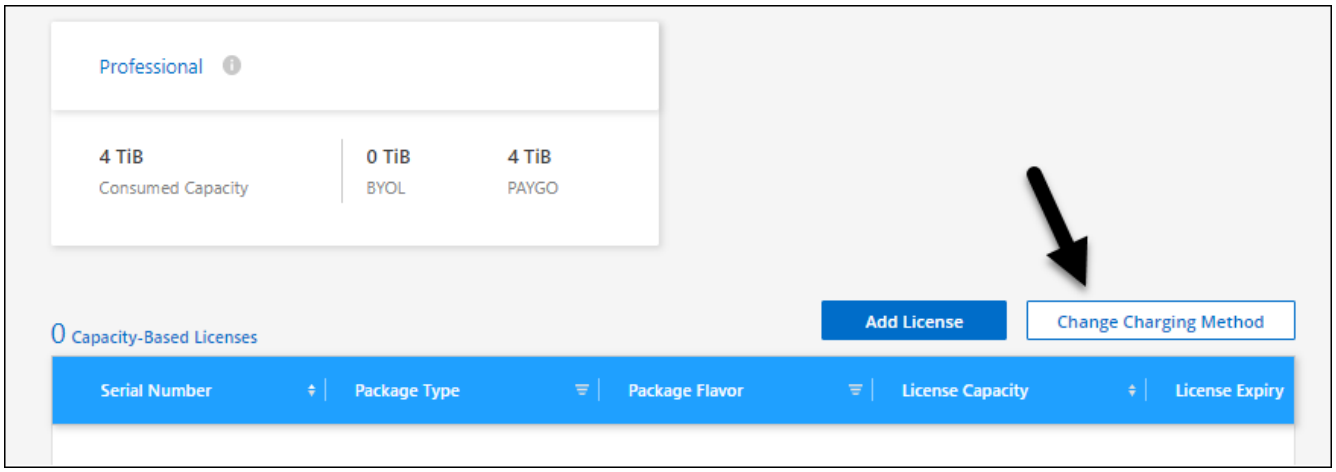
- La modifica del metodo di addebito non influisce sul costo di una licenza acquistata da NetApp (BYOL) o sul mercato del cloud provider (pagamento a consumo).

  BlueXP tenta sempre di addebitare prima i costi di una licenza. Se una licenza non è disponibile, viene applicata una tariffa per un abbonamento al mercato. Non è richiesta alcuna "conversione" per l'abbonamento BYOL al marketplace o viceversa.

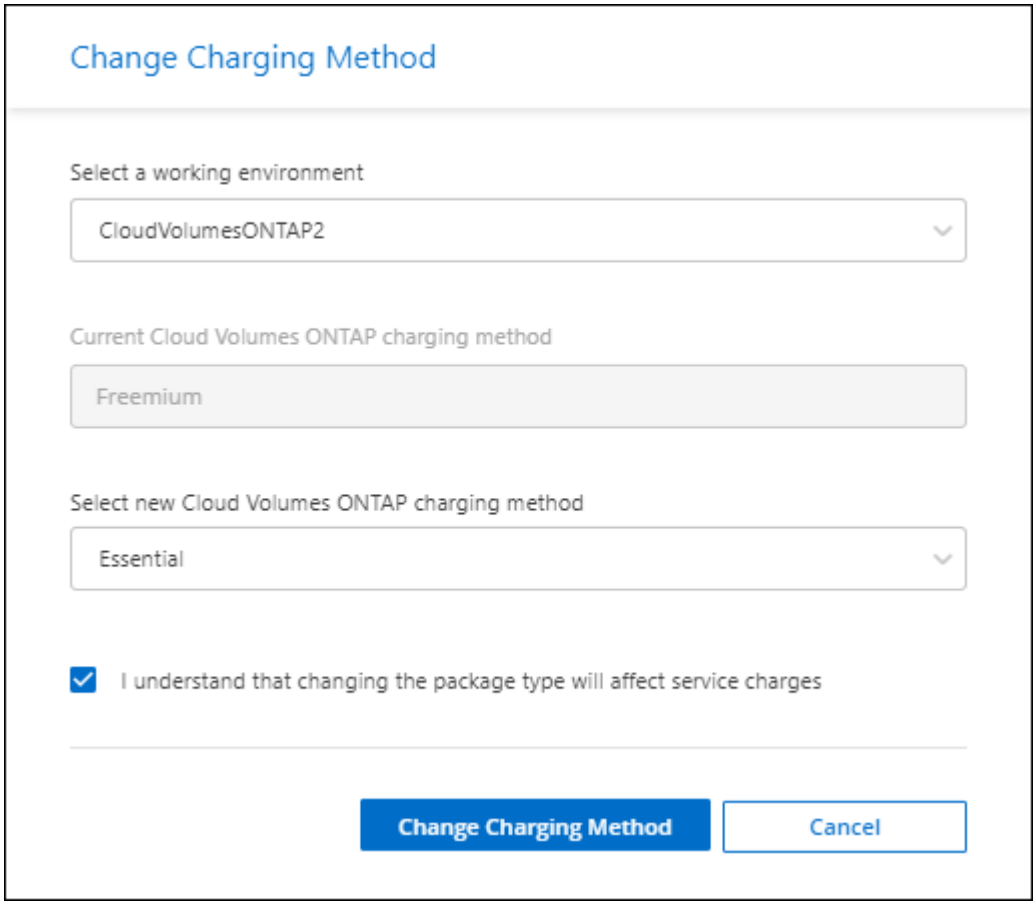
- Se disponi di un'offerta o di un contratto privato sul mercato del tuo cloud provider, il passaggio a un metodo di addebito non incluso nel contratto comporterà l'addebito di BYOL (se hai acquistato una licenza da NetApp) o PAYGO.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, fare clic su **Modifica metodo di ricarica**.



3. Selezionare un ambiente di lavoro, scegliere il nuovo metodo di ricarica, quindi confermare che la modifica del tipo di pacchetto influirà sui costi di servizio.



4. Fare clic su **Modifica metodo di ricarica**.

Risultato

BlueXP modifica il metodo di ricarica per il sistema Cloud Volumes ONTAP.

Potresti anche notare che il portafoglio digitale BlueXP aggiorna la capacità consumata per ciascun tipo di pacchetto per tenere conto della modifica appena apportata.

Rimuovere una licenza basata sulla capacità

Se una licenza basata sulla capacità è scaduta e non è più in uso, è possibile rimuoverla in qualsiasi momento.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, fare clic sul menu delle azioni accanto alla licenza e selezionare **Rimuovi licenza**.
3. Fare clic su **Remove** (Rimuovi) per confermare.

Gestire gli abbonamenti Keystone

Gestisci le tue iscrizioni Keystone dal Digital Wallet di BlueXP abilitando le iscrizioni per l'utilizzo con Cloud Volumes ONTAP e richiedendo modifiche alla capacità sottoposta a commit per i livelli di servizio della tua iscrizione. La richiesta di capacità aggiuntiva per un livello di servizio offre più storage per i cluster ONTAP on-premise o per i sistemi Cloud Volumes ONTAP.

NetApp Keystone è un servizio flessibile basato su abbonamento pay-as-you-grow che offre un'esperienza di cloud ibrido per i clienti che preferiscono OPEX a CAPEX o leasing.

"Scopri di più su Keystone"

Autorizzare l'account

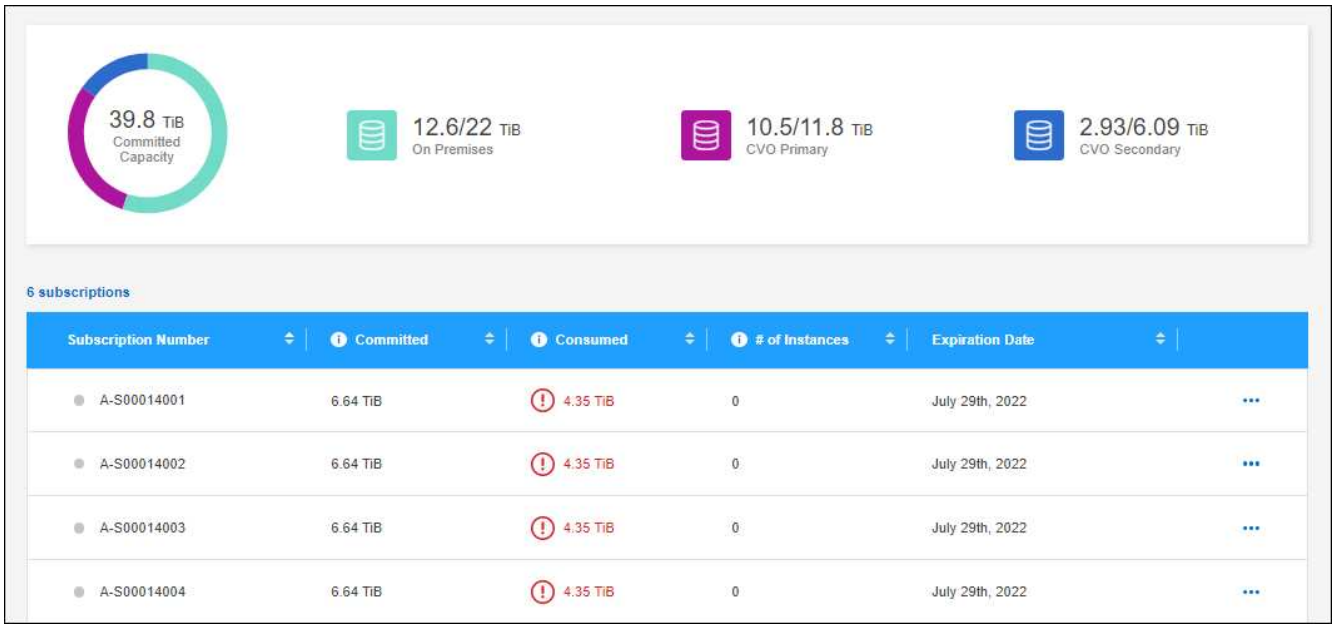
Prima di poter utilizzare e gestire le iscrizioni Keystone in BlueXP, devi contattare NetApp per autorizzare il tuo account utente BlueXP alle iscrizioni Keystone.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare **Keystone**.
3. Se viene visualizzata la pagina **Benvenuti in NetApp Keystone**, inviare un'e-mail all'indirizzo indicato nella pagina.

   Un rappresentante NetApp elaborerà la tua richiesta autorizzando il tuo account utente ad accedere alle sottoscrizioni.

4. Torna all'abbonamento **Keystone** per visualizzare i tuoi abbonamenti.

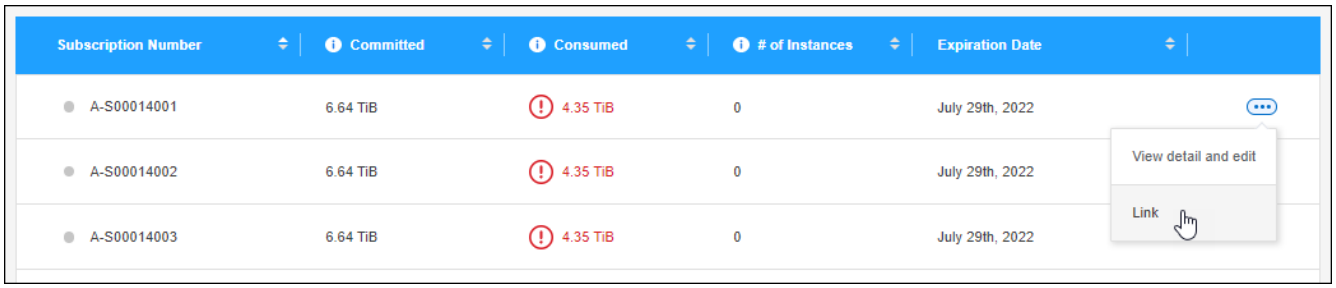


Collegare un abbonamento

Dopo che NetApp ha autorizzato il tuo account, puoi collegare le iscrizioni Keystone per l'utilizzo con Cloud Volumes ONTAP. Questa azione consente agli utenti di selezionare l'abbonamento come metodo di addebito per i nuovi sistemi Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare **Keystone**.
3. Per l'abbonamento che si desidera collegare, fare clic su ••• E selezionare **link**.



Risultato

L'abbonamento è ora collegato al tuo account BlueXP e disponibile per la selezione durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP.

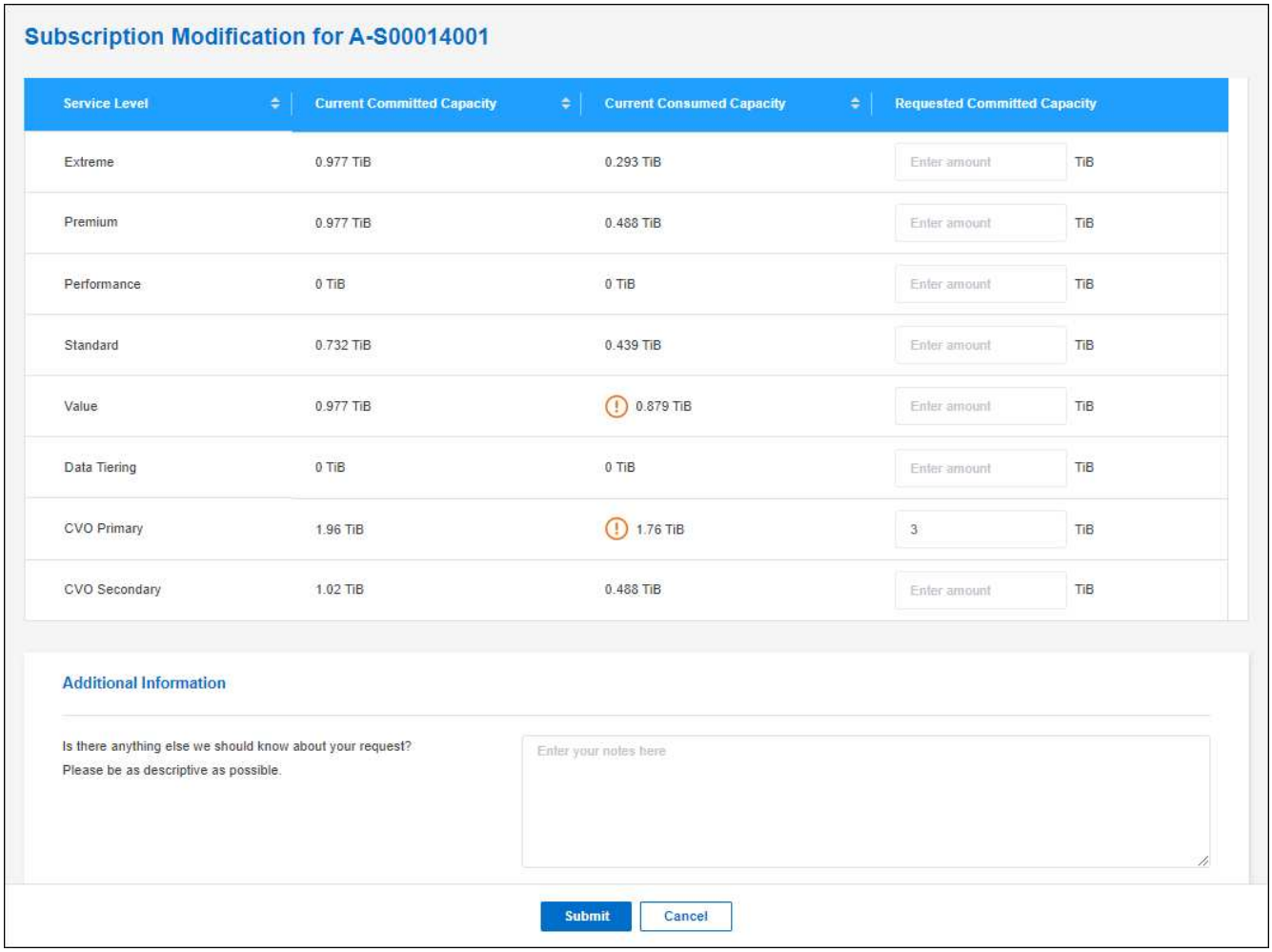
Richiedere una capacità impegnata maggiore o minore

Per modificare la capacità sottoposta a commit per i livelli di servizio della tua iscrizione, puoi inviare una richiesta a NetApp direttamente da BlueXP. La richiesta di capacità aggiuntiva per un livello di servizio offre più storage per i cluster on-premise o per i sistemi Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.

2. Selezionare **Keystone**.
3. Per l'abbonamento che si desidera regolare la capacità, fare clic su ••• E selezionare **Visualizza dettagli e modifica**.
4. Immettere la capacità impegnata richiesta per uno o più abbonamenti.



5. Scorrere verso il basso, inserire eventuali dettagli aggiuntivi per la richiesta, quindi fare clic su **Invia**.

Risultato

La richiesta crea un ticket nel sistema NetApp per l'elaborazione.

Monitoraggio dell'utilizzo

La dashboard del Digital Advisor di BlueXP ti permette di monitorare l'utilizzo dell'abbonamento Keystone e di generare report.

"Ulteriori informazioni sul monitoraggio dell'utilizzo degli abbonamenti"

Scollegare un abbonamento

Se non vuoi più utilizzare un abbonamento Keystone con BlueXP, puoi scollegarlo. Nota: Puoi scollegare solo un abbonamento non allegato a un abbonamento Cloud Volumes ONTAP esistente.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare **Keystone**.
3. Per l'abbonamento che si desidera scollegare, fare clic su ••• E selezionare **Unlink**.

Risultato

L'abbonamento non è collegato all'account BlueXP e non è più disponibile per la selezione durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP.

Gestire le licenze basate su nodo

Gestire le licenze basate su nodo nel portafoglio digitale BlueXP per garantire che ogni sistema Cloud Volumes ONTAP disponga di una licenza valida con la capacità richiesta.

Le *licenze basate su nodo* sono il modello di licenza della generazione precedente (e non sono disponibili per i nuovi clienti):

- Licenze BYOL acquistate da NetApp
- Sottoscrizioni a pagamento orarie (PAYGO) dal mercato del tuo cloud provider

Il *portafoglio digitale BlueXP* consente di gestire le licenze per Cloud Volumes ONTAP da un'unica postazione. È possibile aggiungere nuove licenze e aggiornare quelle esistenti.

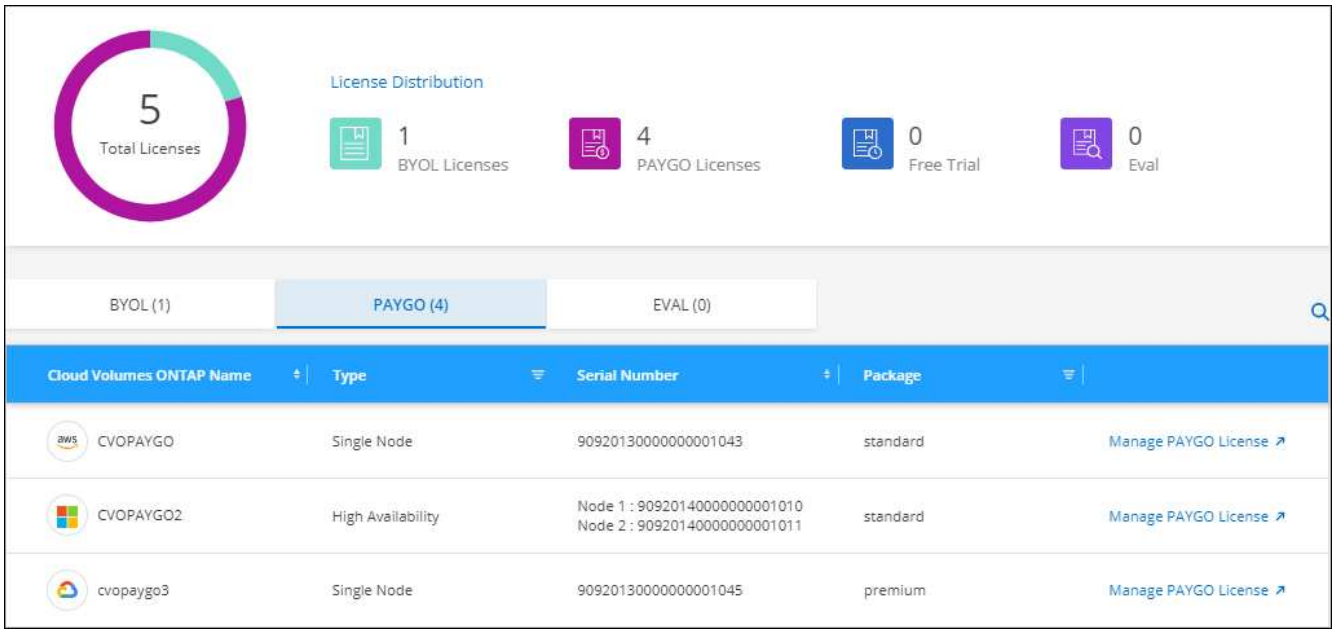
"Scopri di più sulle licenze Cloud Volumes ONTAP".

Gestire le licenze PAYGO

La pagina del portafoglio digitale BlueXP consente di visualizzare i dettagli relativi a ciascun sistema PAYGO Cloud Volumes ONTAP, inclusi il numero di serie e il tipo di licenza PAYGO.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Fare clic su **PAYGO**.
4. Visualizza i dettagli nella tabella di ciascuna licenza PAYGO.



5. Se necessario, fare clic su **Manage PAYGO License** (Gestisci licenza PAYGO) per modificare la licenza PAYGO o il tipo di istanza.

Gestire le licenze BYOL

Gestisci le licenze acquistate direttamente da NetApp aggiungendo e rimuovendo le licenze di sistema e le licenze di capacità extra.

Aggiungere licenze non assegnate

Aggiungere una licenza basata su nodo al portafoglio digitale BlueXP in modo da poter selezionare la licenza quando si crea un nuovo sistema Cloud Volumes ONTAP. Il portafoglio digitale identifica queste licenze come *non assegnate*.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Fare clic su **non assegnato**.
4. Fare clic su **Aggiungi licenze non assegnate**.
5. Inserire il numero di serie della licenza o caricare il file di licenza.

   Se non si dispone ancora del file di licenza, fare riferimento alla sezione seguente.

6. Fare clic su **Aggiungi licenza**.

Risultato

BlueXP aggiunge la licenza al portafoglio digitale. La licenza viene identificata come non assegnata fino a quando non viene associata a un nuovo sistema Cloud Volumes ONTAP. In seguito, la licenza passa alla scheda **BYOL** del portafoglio digitale.

Licenze Exchange basate su nodo non assegnate

Se si dispone di una licenza basata su nodo non assegnata per Cloud Volumes ONTAP che non è stata

utilizzata, è possibile scambiare la licenza convertendola in una licenza di backup e ripristino BlueXP, una licenza di classificazione BlueXP o una licenza di tiering BlueXP.

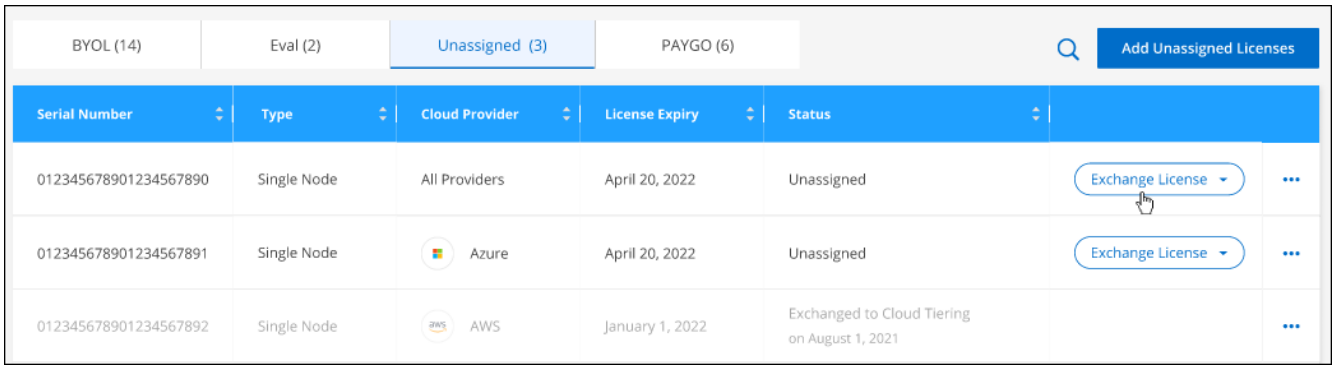
Lo scambio della licenza revoca la licenza Cloud Volumes ONTAP e crea una licenza equivalente al dollaro per il servizio:

- La licenza per una coppia Cloud Volumes ONTAP ha viene convertita in una licenza per servizio dati 51 TIB
- Le licenze per un singolo nodo Cloud Volumes ONTAP vengono convertite in una licenza per servizio dati 32 TIB

La licenza convertita ha la stessa data di scadenza della licenza Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Fare clic su **non assegnato**.
4. Fare clic su **Exchange License**.



5. Selezionare il servizio con cui si desidera scambiare la licenza.
6. Se richiesto, selezionare una licenza aggiuntiva per la coppia ha.
7. Leggere il consenso legale e fare clic su **Accetto**.

Risultato

BlueXP converte la licenza non assegnata nel servizio selezionato. È possibile visualizzare la nuova licenza nella scheda **licenze servizi dati**.

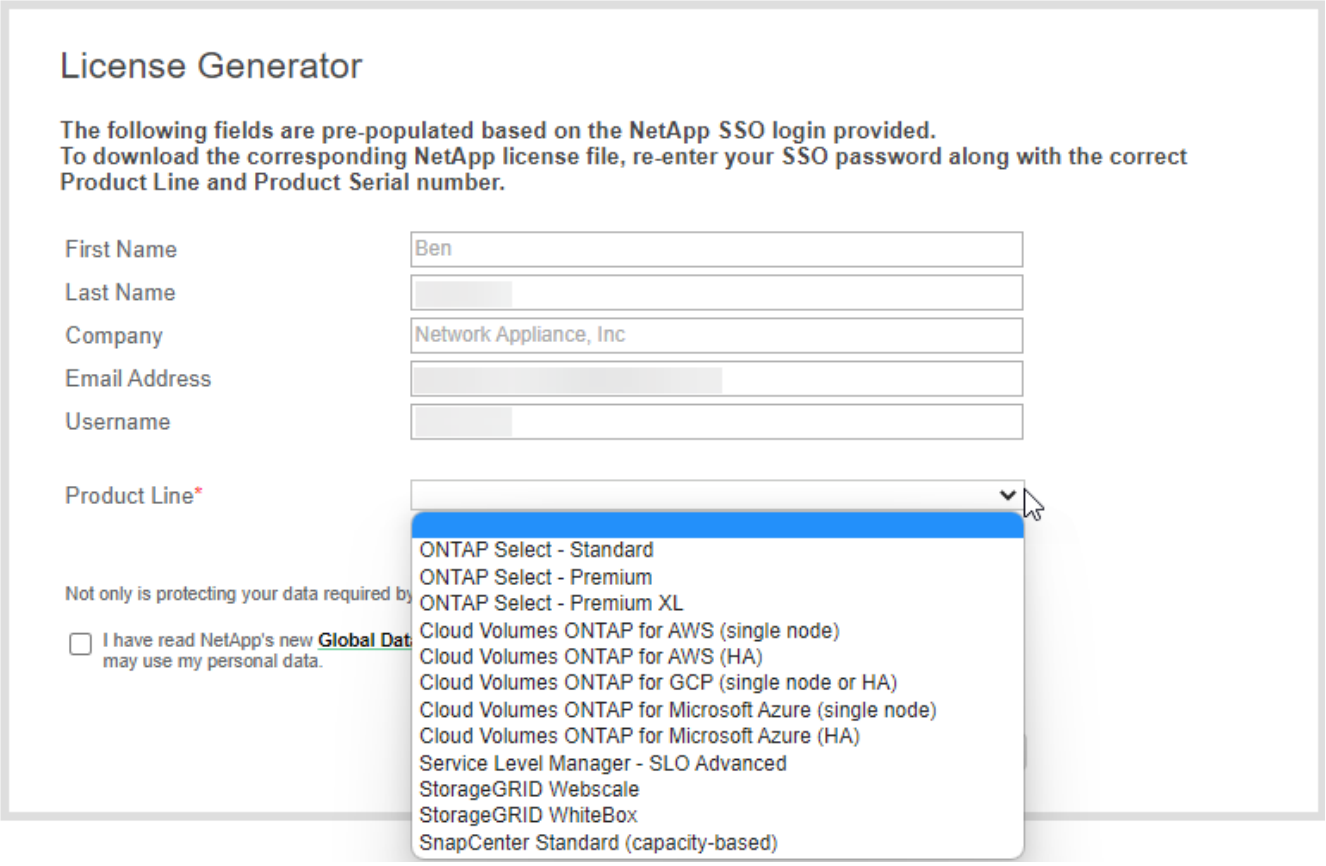
Ottenere un file di licenza di sistema

Nella maggior parte dei casi, BlueXP 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.

Aggiornare una licenza di sistema

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

Se BlueXP non riesce ad accedere al file di licenza tramite una connessione Internet sicura, è possibile ottenere il file da soli e caricarlo manualmente su BlueXP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
4. Fare clic sul menu delle azioni accanto alla licenza di sistema e selezionare **Aggiorna licenza**.
5. Caricare il file di licenza (o i file se si dispone di una coppia ha).
6. Fare clic su **Update License** (Aggiorna licenza).

Risultato

BlueXP aggiorna la licenza sul sistema Cloud Volumes ONTAP.

Gestire licenze di capacità extra

È possibile acquistare licenze di capacità extra per un sistema Cloud Volumes ONTAP BYOL per allocare più di 368 TIB di capacità forniti con una licenza di sistema BYOL. Ad esempio, è possibile acquistare una capacità di licenza aggiuntiva per allocare fino a 736 TIB di capacità a Cloud Volumes ONTAP. Oppure puoi

acquistare tre licenze di capacità extra per ottenere fino a 1.4 PIB.

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

Aggiungere licenze di capacità

Acquistare una licenza di capacità aggiuntiva contattandoci tramite l'icona della chat in basso a destra in BlueXP. Una volta acquistata la licenza, è possibile applicarla a un sistema Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
4. Fare clic su **Add Capacity License**.
5. Inserire il numero di serie o caricare il file di licenza (o i file se si dispone di una coppia ha).
6. Fare clic su **Add Capacity License**.

Aggiornare le licenze di capacità

Se si estende il termine di una licenza con capacità extra, sarà necessario aggiornare la licenza in BlueXP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
4. Fare clic sul menu delle azioni accanto alla licenza di capacità e selezionare **Aggiorna licenza**.
5. Caricare il file di licenza (o i file se si dispone di una coppia ha).
6. Fare clic su **Update License** (Aggiorna licenza).

Rimuovere le licenze di capacità

Se una licenza di capacità extra è scaduta e non è più in uso, è possibile rimuoverla in qualsiasi momento.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
4. Fare clic sul menu delle azioni accanto alla licenza di capacità e selezionare **Remove License** (Rimuovi licenza).
5. Fare clic su **Rimuovi**.

Convertire una licenza di valutazione in una BYOL

Una licenza di valutazione è valida per 30 giorni. È possibile applicare una nuova licenza BYOL alla licenza di valutazione per un aggiornamento in-place.

Quando si converte una licenza di valutazione in una BYOL, BlueXP riavvia il sistema Cloud Volumes ONTAP.

- Per un sistema a nodo singolo, il riavvio provoca un'interruzione i/o durante il processo di riavvio.
- Per una coppia ha, il riavvio avvia il takeover e il giveback per continuare a fornire i/o ai client.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Cloud Volumes ONTAP**, selezionare **licenze basate su nodo** dall'elenco a discesa.
3. Fare clic su **valutazione**.
4. Nella tabella, fare clic su **Converti in licenza BYOL** per un sistema Cloud Volumes ONTAP.
5. Inserire il numero di serie o caricare il file di licenza.
6. Fare clic su **Converti licenza**.

Risultato

BlueXP avvia il processo di conversione. Cloud Volumes ONTAP viene riavviato automaticamente durante questo processo. Quando viene eseguita la copia di backup, le informazioni sulla licenza rispecchieranno la nuova licenza.

Passaggio da PAYGO a BYOL

La conversione di un sistema da UNA licenza PAYGO per nodo a una licenza BYOL per nodo (e viceversa) non è supportata. Se si desidera passare da un abbonamento pay-as-you-go a un abbonamento BYOL, 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.
2. Impostare una replica dei dati una tantum tra i sistemi per ciascun volume da replicare.

   "Scopri come replicare i dati tra sistemi"

3. Terminare il sistema Cloud Volumes ONTAP non più necessario eliminando l'ambiente di lavoro originale.

   "Scopri come eliminare un ambiente di lavoro Cloud Volumes ONTAP".

Amministrazione di volumi e LUN

Creare volumi FlexVol

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

BlueXP offre diversi modi per creare un nuovo volume:

- Specifica i dettagli di un nuovo volume e lascia che BlueXP gestisca gli aggregati di dati sottostanti per te. Scopri di più
- Crea un volume su un aggregato di dati a tua scelta. Scopri di più
- Creare un volume sul secondo nodo in una configurazione ha. Scopri di più

Prima di iniziare

Alcune note sul provisioning dei volumi:

- Quando si crea un volume iSCSI, BlueXP crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".
- È possibile creare ulteriori LUN da System Manager o dall'interfaccia CLI.
- 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".
- Se la configurazione di Cloud Volumes ONTAP supporta la funzione Amazon EBS Elastic Volumes (volumi elastici EBS Amazon), potrebbe essere necessario "scopri di più su cosa accade quando crei un volume".

Creare un volume

Il metodo più comune per creare un volume consiste nel specificare il tipo di volume necessario e quindi BlueXP gestisce l'allocazione del disco. Tuttavia, è possibile scegliere l'aggregato specifico su cui si desidera creare il volume.

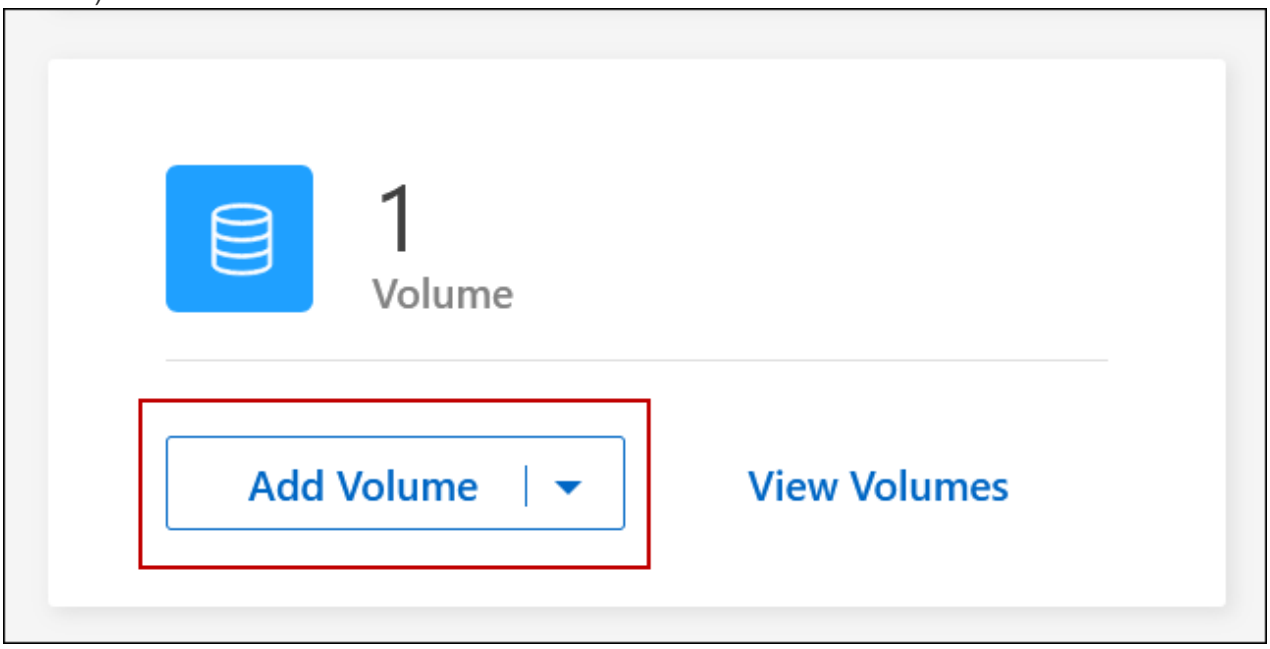
Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera eseguire il provisioning di un volume FlexVol.
3. Creare un nuovo volume consentendo a BlueXP di gestire l'allocazione del disco o di scegliere un aggregato specifico per il volume.

   La scelta di un aggregato specifico è consigliata solo se si dispone di una buona conoscenza degli aggregati di dati nel sistema Cloud Volumes ONTAP.

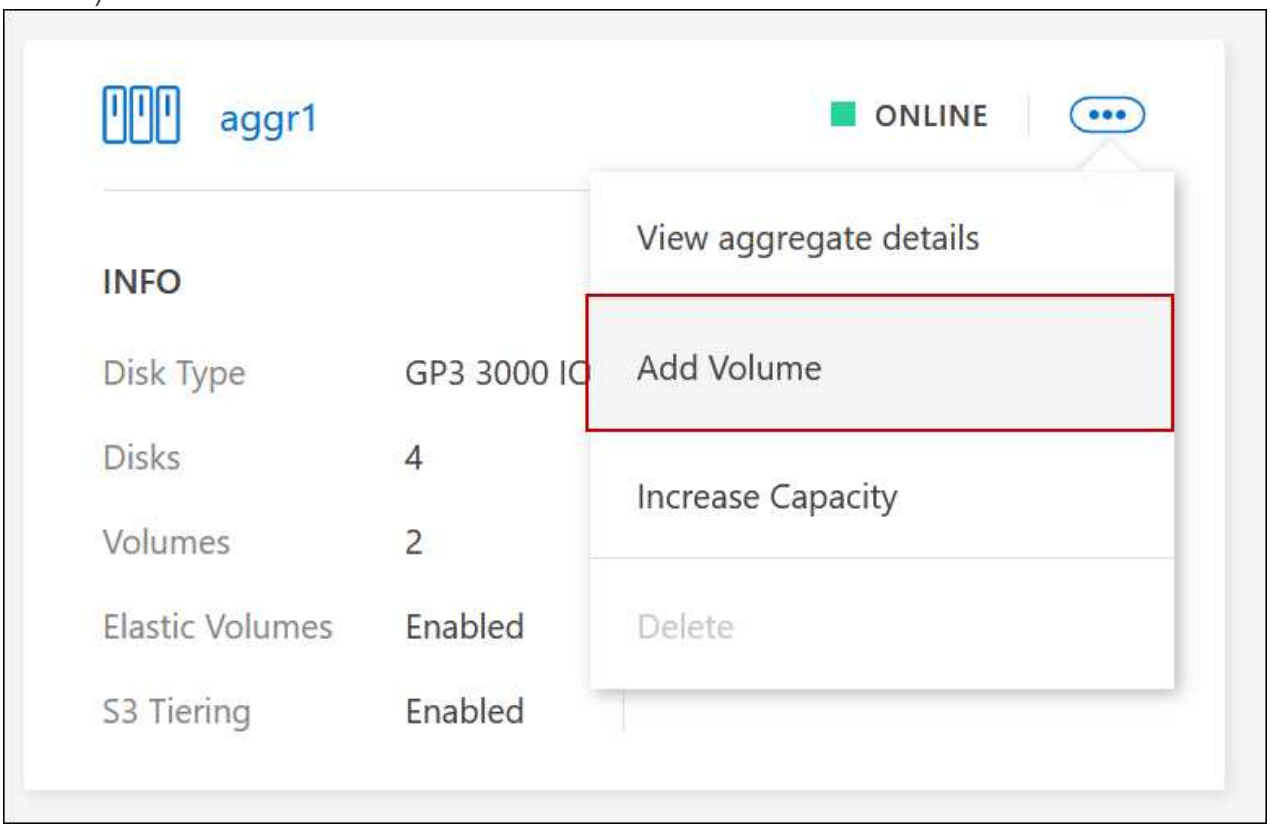
Qualsiasi aggregato

Nella scheda Overview (Panoramica), accedere alla sezione Volumes (volumi) e fare clic su **Add Volume** (Aggiungi
volume).



Aggregato specifico

Nella scheda aggregati, passare alla sezione aggregata desiderata. Fare clic sull'icona del menu, quindi su **Add Volume** (Aggiungi
volume).



4. Seguire i passaggi della procedura guidata per creare il volume.

   a. **Dettagli, protezione e Tag**: Immettere i dettagli di base sul volume e selezionare un criterio Snapshot.

      Alcuni dei campi di questa pagina sono esplicativi. Il seguente elenco descrive i campi per i quali potrebbe essere necessario fornire assistenza:

Campo	Descrizione
Volume Name (Nome volume)	Il nome identificabile che è possibile inserire per il nuovo volume.
Volume Size (dimensione volume)	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.
Storage VM (SVM)	Una VM di storage è una macchina virtuale in esecuzione in ONTAP che fornisce servizi di storage e dati ai client. Questo potrebbe essere conosciuto come SVM o vserver. Cloud Volumes ONTAP è configurato con una VM di storage per impostazione predefinita, ma alcune configurazioni supportano altre VM di storage. È possibile specificare la Storage VM per il nuovo volume.
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.

   b. **Protocol** (protocollo): Scegliere un protocollo per il volume (NFS, CIFS o iSCSI) e fornire le informazioni richieste.

      Se si seleziona CIFS e un server non è configurato, BlueXP richiede di impostare la connettività CIFS dopo aver fatto clic su **Avanti**.

      "Scopri le versioni e i protocolli client supportati".

      Le sezioni seguenti descrivono i campi per i quali potrebbe essere necessario fornire assistenza. Le descrizioni sono organizzate in base al protocollo.

NFS

Controllo degli accessi

Scegliere un criterio di esportazione personalizzato per rendere il volume disponibile ai client.

Policy di esportazione

Definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, BlueXP inserisce un valore che fornisce l'accesso a tutte le istanze della subnet.

CIFS

Permessi e utenti/gruppi

Consente di controllare il livello di accesso a una condivisione SMB 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.

Indirizzo IP primario e secondario DNS

Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.

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

Dominio Active Directory da unire

L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.

Credenziali autorizzate per l'accesso al dominio

Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.

Nome NetBIOS del server CIFS

Un nome server CIFS univoco nel dominio ad.

Unità organizzativa

L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer.

- Per configurare AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.
- 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"^]
- Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=cloud** in questo campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentazione Google Cloud: Unità organizzative in Google Managed Microsoft ad"^]

Dominio DNS

Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.

Server NTP

Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Documenti sull'automazione BlueXP" per ulteriori informazioni.

Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

ISCSI

LUN

Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. Quando si crea un volume iSCSI, BlueXP crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è prevista alcuna gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

Gruppo iniziatore

i gruppi di iniziatori (igroups) specificano quali host possono accedere a LUN specifiche sul sistema di storage

Iniziatore host (IQN)

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).

a. **Disk Type** (tipo di disco): Scegliere un tipo di disco sottostante per il volume in base alle esigenze di performance e ai requisiti di costo.
   - "Dimensionamento del sistema in AWS"
     - "Dimensionamento del sistema in Azure"
     - "Dimensionamento del sistema in Google Cloud"

5. **Profilo di utilizzo e policy di tiering**: Scegliere se attivare o disattivare le funzionalità di efficienza dello storage sul volume, quindi selezionare un "policy di tiering dei volumi".

   ONTAP include diverse funzionalità di efficienza dello storage che consentono di ridurre la quantità totale di storage necessaria. 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.

6. **Revisione**: Esaminare i dettagli relativi al volume, quindi fare clic su **Aggiungi**.

Risultato

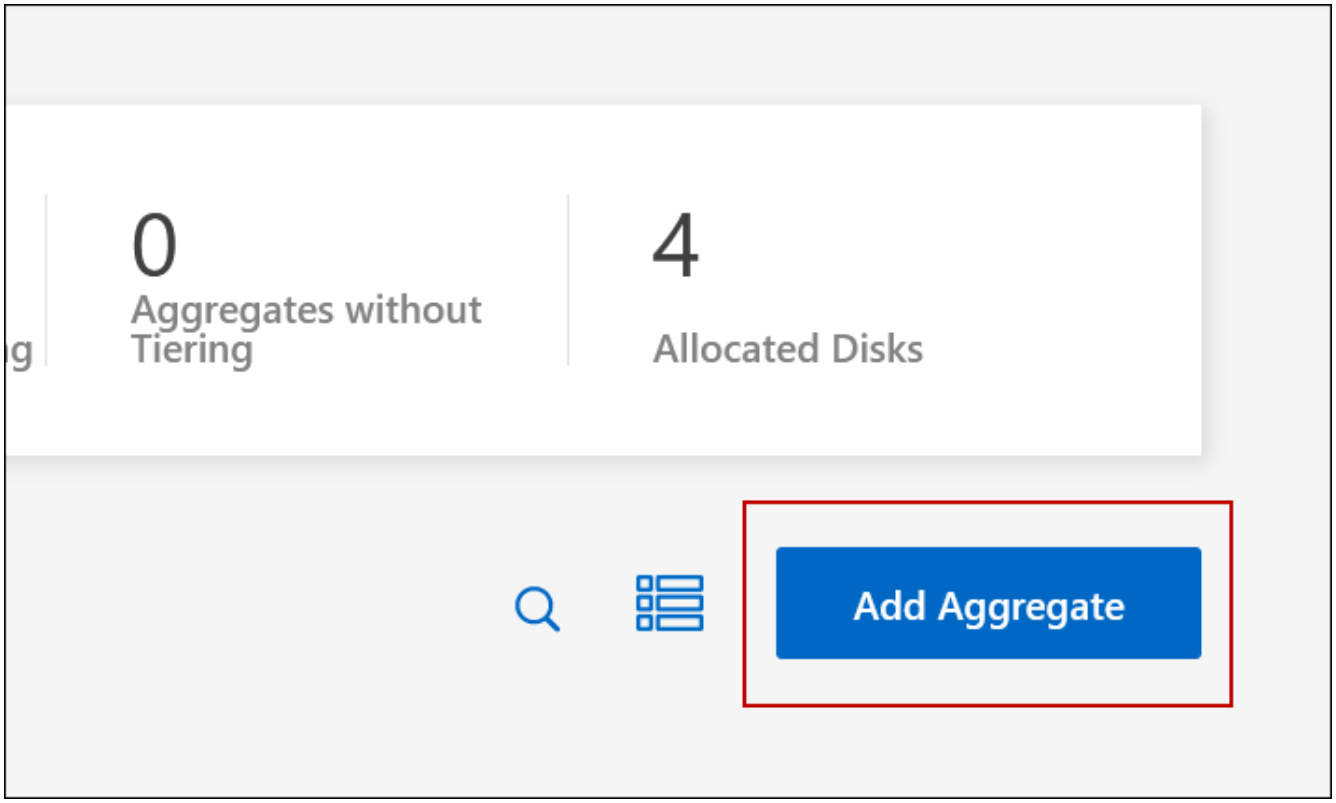
BlueXP crea il volume sul sistema Cloud Volumes ONTAP.

Creare un volume sul secondo nodo in una configurazione ha

Per impostazione predefinita, BlueXP 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. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sul nome dell'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
3. Nella scheda aggregati, fare clic su **Aggiungi aggregato**.
4. Dalla schermata *Add aggregate*, creare l'aggregato.



5. Per nodo principale, scegliere il secondo nodo della coppia ha.
6. Una volta creato l'aggregato, selezionarlo e fare clic su **Create volume** (Crea volume).
7. Inserire i dettagli del nuovo volume, quindi fare clic su **Create** (Crea).

Risultato

BlueXP crea il volume sul secondo nodo della coppia ha.

> 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.

Dopo aver creato un volume

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.

Gestire i volumi esistenti

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

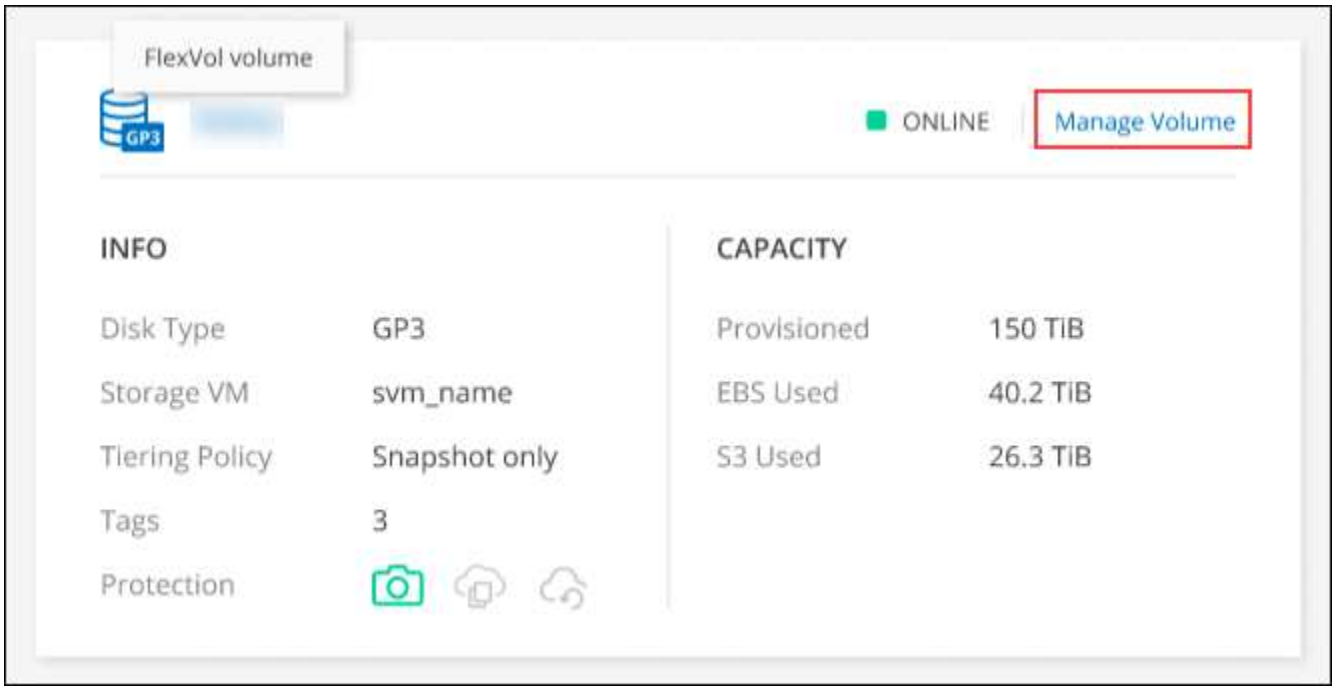
Puoi gestire i volumi in BlueXP Standard View o Advanced View. La visualizzazione standard fornisce un insieme limitato di opzioni per modificare i volumi. La vista avanzata offre un livello di gestione avanzato, come cloning, ridimensionamento, modifica delle impostazioni per anti-ransomware, analytics, protezione e tracciamento delle attività e spostamento dei volumi tra Tier. Vedere "Amministrare Cloud Volumes ONTAP utilizzando la visualizzazione avanzata".

Gestire i volumi

Utilizzando la vista standard di BlueXP, puoi gestire i volumi in base alle tue esigenze di storage. È possibile visualizzare, modificare, clonare, ripristinare ed eliminare i volumi.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire i volumi.
3. Nell'ambiente di lavoro, fare clic sulla scheda **Volumes** (volumi).



4. Nella scheda Volumes (volumi), selezionare il titolo del volume desiderato, quindi fare clic su **Manage volume** (Gestisci volume) per accedere al pannello di destra Manage Volumes (Gestisci volumi).

Attività	Azione
Consente di visualizzare informazioni su un volume	In azioni volume nel pannello Manage Volumes (Gestisci volumi), fare clic su **View volume details** (Visualizza dettagli volume).
Scarica il comando NFS mount	a. In azioni volume nel pannello Manage Volumes (Gestisci volumi), fare clic su **Mount Command** (comando di montaggio). b. Fare clic su **Copy** (Copia).
Clonare un volume	a. In azioni volume nel pannello Manage Volumes (Gestisci volumi), fare clic su **Clone the volume** (Clona volume). b. Modificare il nome del clone secondo necessità, quindi fare clic su **Clone**. 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. Per ulteriori informazioni sui volumi FlexClone, vedere "Guida alla gestione dello storage logico di ONTAP 9".

Attività	Azione
Modifica di un volume (solo volumi di lettura/scrittura)	a. In azioni volume nel pannello Manage Volumes (Gestisci volumi), fare clic su **Edit volume settings** (Modifica impostazioni volume) b. Modificare la policy Snapshot del volume, la versione del protocollo NFS, l'elenco di controllo degli accessi NFS (policy di esportazione) o le autorizzazioni di condivisione, quindi fare clic su **Apply** (Applica). Se sono necessarie policy Snapshot personalizzate, è possibile crearle utilizzando System Manager.
Eliminare un volume	a. In azioni volume nel pannello Manage Volumes (Gestisci volumi), fare clic su **Delete the volume** (Elimina volume). b. Nella finestra Delete Volume (Elimina volume), immettere il nome del volume che si desidera eliminare. c. Fare nuovamente clic su **Delete** per confermare.
Crea una copia Snapshot on-demand	a. In azioni di protezione nel pannello Manage Volumes (Gestisci volumi), fare clic su **Create a Snapshot copy** (Crea una copia Snapshot). b. Modificare il nome, se necessario, quindi fare clic su **Crea**.
Ripristinare i dati da una copia Snapshot a un nuovo volume	a. In azioni di protezione nel pannello Gestisci volumi, fare clic su **Ripristina da copia Snapshot**. b. Selezionare una copia Snapshot, immettere un nome per il nuovo volume, quindi fare clic su **Restore** (Ripristina).
Modificare il tipo di disco sottostante	a. In azioni avanzate nel pannello Gestisci volumi, fare clic su **Cambia tipo di disco**. b. Selezionare il tipo di disco, quindi fare clic su **Cambia**. BlueXP 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. In azioni avanzate nel pannello Gestisci volumi, fare clic su **Modifica policy di tiering**. b. Selezionare un altro criterio e fare clic su **Cambia**. BlueXP 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.

Attività	Azione
Eliminare un volume	a. Selezionare un volume, quindi fare clic su **Delete** (Elimina). b. Digitare il nome del volume nella finestra di dialogo. c. Fare nuovamente clic su **Delete** per confermare.

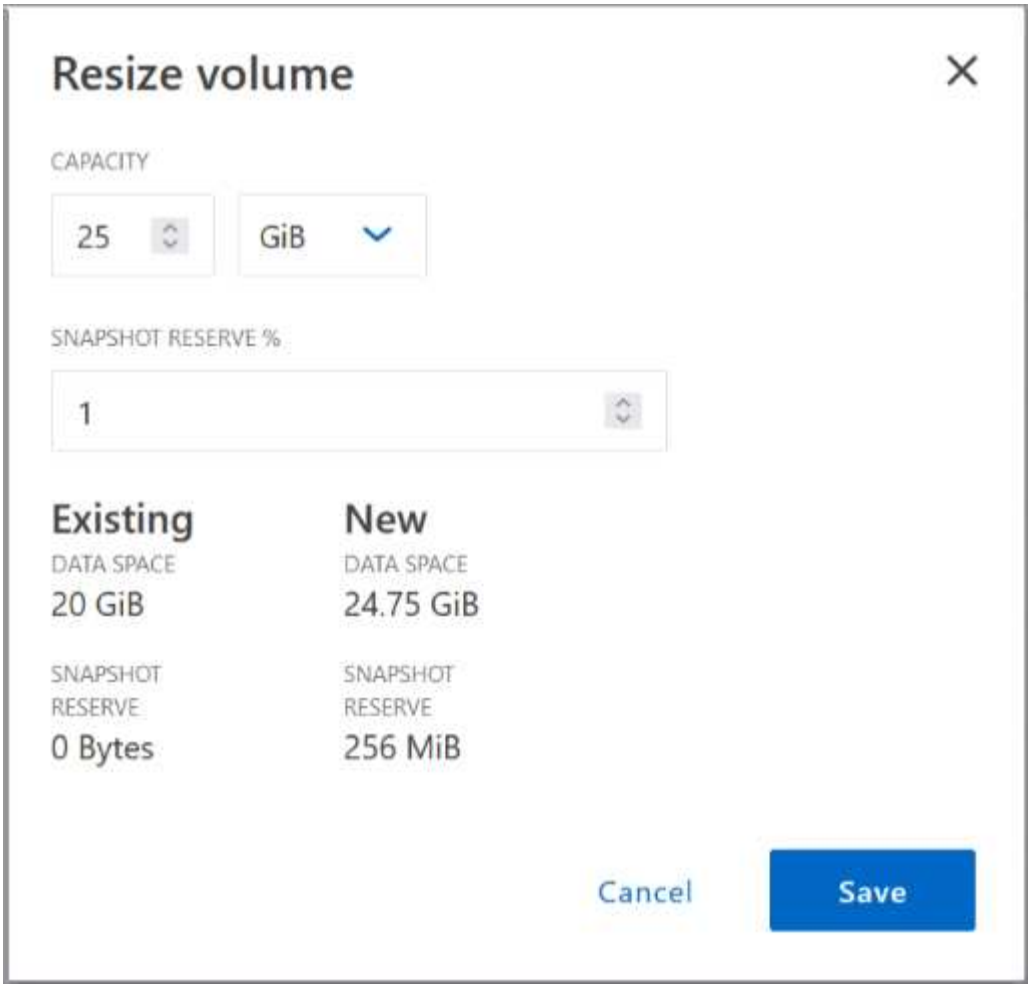
Ridimensionare un volume

Per impostazione predefinita, un volume aumenta automaticamente fino a raggiungere le dimensioni massime quando lo spazio è esaurito. Il valore predefinito è 1.000, il che significa che il volume può aumentare di 11 volte le sue dimensioni. Questo valore è configurabile nelle impostazioni del connettore.

Se devi ridimensionare il volume, puoi farlo dalla vista avanzata di BlueXP.

Fasi

1. Aprire la visualizzazione avanzata per ridimensionare un volume tramite System Manager. Vedere "Come iniziare".
2. Dal menu di navigazione a sinistra, selezionare **Storage > Volumes** (archiviazione > volumi*).
3. Dall'elenco dei volumi, identificare quello da ridimensionare.
4. Fare clic sull'icona delle opzioni ⋮.
5. Selezionare **Ridimensiona**.
6. Nella schermata **Ridimensiona volume**, modificare la capacità e la percentuale di riserva istantanea come richiesto. È possibile confrontare lo spazio disponibile esistente con la capacità modificata.
7. Fare clic su **Save** (Salva).



Durante il ridimensionamento dei volumi, tenere in considerazione i limiti di capacità del sistema. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" per ulteriori dettagli.

Modificare il 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. Dalla scheda Panoramica dell'ambiente di lavoro, fare clic sulla scheda funzionalità nel pannello a destra.
2. Nel campo CIFS Setup (Configurazione CIFS), fare clic sull'icona **matita** per visualizzare la finestra CIFS Setup (Configurazione CIFS).
3. Specificare le impostazioni per il server CIFS:

Attività	Azione
Selezionare Storage VM (SVM)	Selezionando la SVM (Storage Virtual Machine) Cloud Volume ONTAP vengono visualizzate le informazioni CIFS configurate.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.

Attività	Azione
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.
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. Ifdef::gcp[] se si sta configurando Google Managed Active Directory, ad è accessibile per impostazione predefinita con l'indirizzo IP 169.254.169.254. endif::gcp[]
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.
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 AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo. • Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo."Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure" • Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=cloud** in questo campo."Documentazione Google Cloud: Unità organizzative in Google Managed Microsoft ad"

4. Fare clic su **Set** (Imposta).

Risultato

Cloud Volumes ONTAP aggiorna il server CIFS con le modifiche.

Spostare 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".

Spostare un volume quando BlueXP visualizza un messaggio Action Required (azione richiesta)

BlueXP 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 è necessario correggere il problema da soli. In questo caso, è necessario identificare come correggere il problema e spostare uno o più volumi.

> BlueXP visualizza questi messaggi Action Required (azione richiesta) quando un aggregato ha raggiunto il 90% della capacità utilizzata. Se il tiering dei dati è attivato, i messaggi vengono visualizzati quando un aggregato ha raggiunto il 80% della capacità utilizzata. Per impostazione predefinita, il 10% di spazio libero è riservato al tiering dei dati. "Scopri di più sul rapporto di spazio libero per il tiering dei dati".

Fasi

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

Identificare come correggere i problemi di capacità

Se BlueXP 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 dello 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.

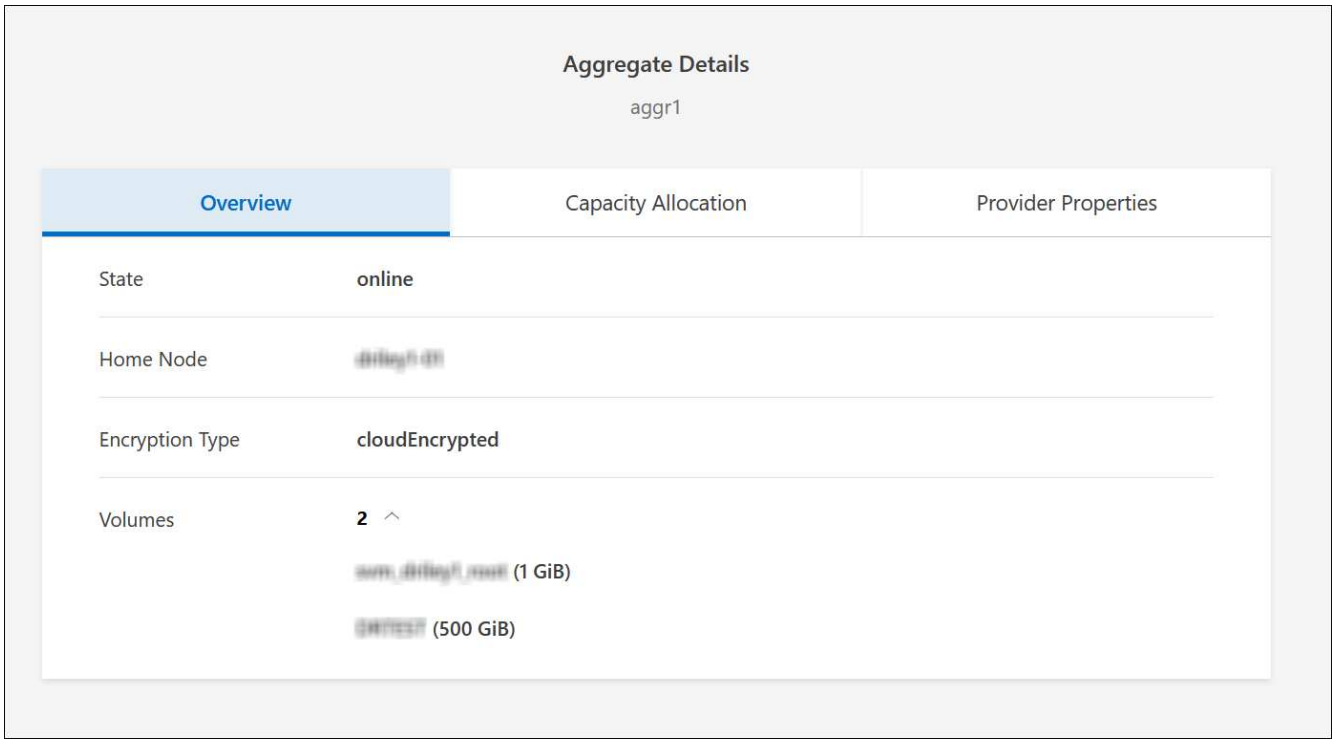
2. Identificare uno o più volumi da spostare fuori dall'aggregato:

   a. Nell'ambiente di lavoro, fare clic sulla scheda **aggregati**.

   b. Selezionare la sezione aggregata desiderata, quindi fare clic sul pulsante **… (Icona ellisse) > Visualizza dettagli aggregati**.

   c. Nella scheda Overview (Panoramica) della schermata aggregate Details (Dettagli aggregato), 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 Spostare i 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 Spostare i 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 Spostare i volumi in un altro aggregato per evitare problemi di capacità.

Spostare i 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):

> Lo spostamento di un volume è necessario per evitare problemi di capacità; tuttavia, BlueXP non può eseguire questa azione perché il sistema ha raggiunto il limite di dischi.

Fasi

1. Identificare un sistema Cloud Volumes ONTAP con capacità disponibile o implementare un nuovo sistema.
2. 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".

3. 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".

4. 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".

5. Eliminare il volume originale.

   Per ulteriori informazioni, vedere "Gestire i volumi".

Spostare i 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.

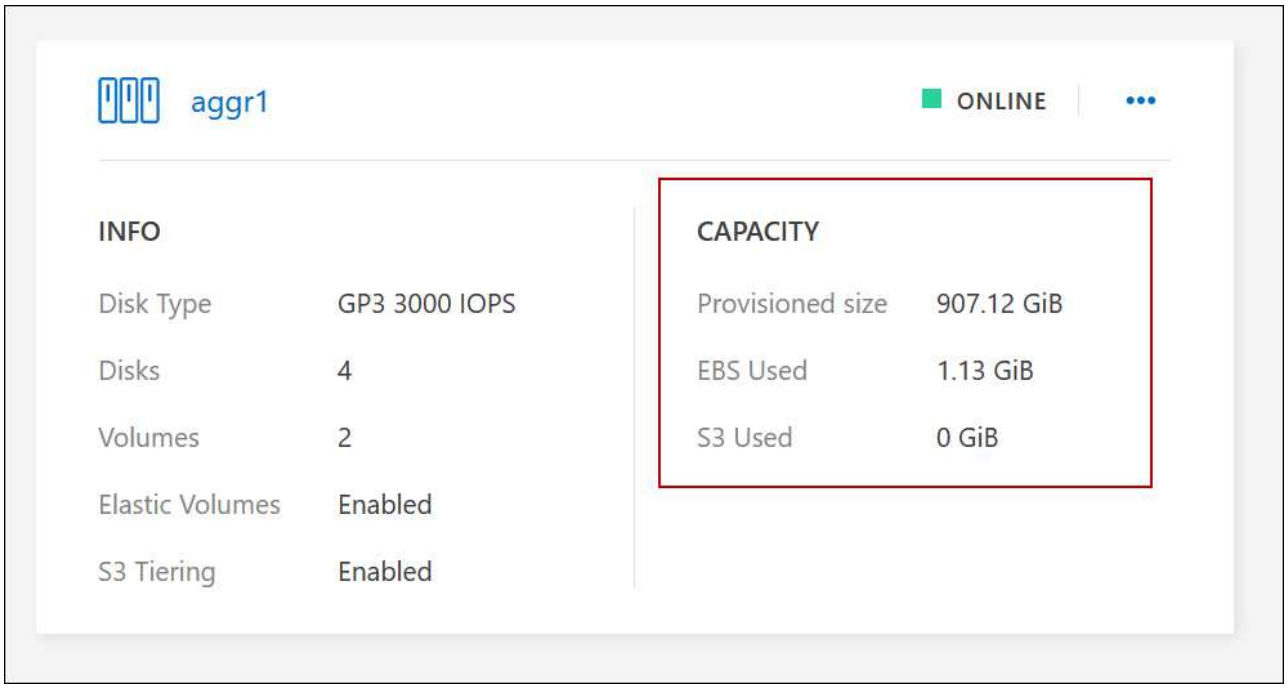
A proposito di questa attività

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

> Lo spostamento di due o più volumi è necessario per evitare problemi di capacità; tuttavia, BlueXP non può eseguire questa azione per te.

Fasi

1. Verificare se un aggregato esistente dispone di capacità disponibile per i volumi da spostare:
   a. Nell'ambiente di lavoro, fare clic sulla scheda **aggregati**.
   b. Selezionare la sezione aggregata desiderata, quindi fare clic sul pulsante **… (Icona ellisse) > Visualizza dettagli aggregati**.
   c. Nella sezione aggregato, visualizzare la capacità disponibile (dimensione fornita meno capacità aggregata utilizzata).



2. Se necessario, aggiungere dischi a un aggregato esistente:
   a. Selezionare l'aggregato, quindi fare clic sul pulsante **… (Icona ellisse) > Add Disks** (Aggiungi dischi).
   b. Selezionare il numero di dischi da aggiungere, quindi fare clic su **Aggiungi**.
3. Se nessun aggregato dispone di capacità, creare un nuovo aggregato.

   Per ulteriori informazioni, vedere "Creazione di aggregati".

4. Utilizzare System Manager o CLI per spostare i volumi nell'aggregato.
5. 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.
- Uno degli aggregati utilizza uno schema di denominazione precedente per gli oggetti. Entrambi gli aggregati devono utilizzare lo stesso formato dei nomi.

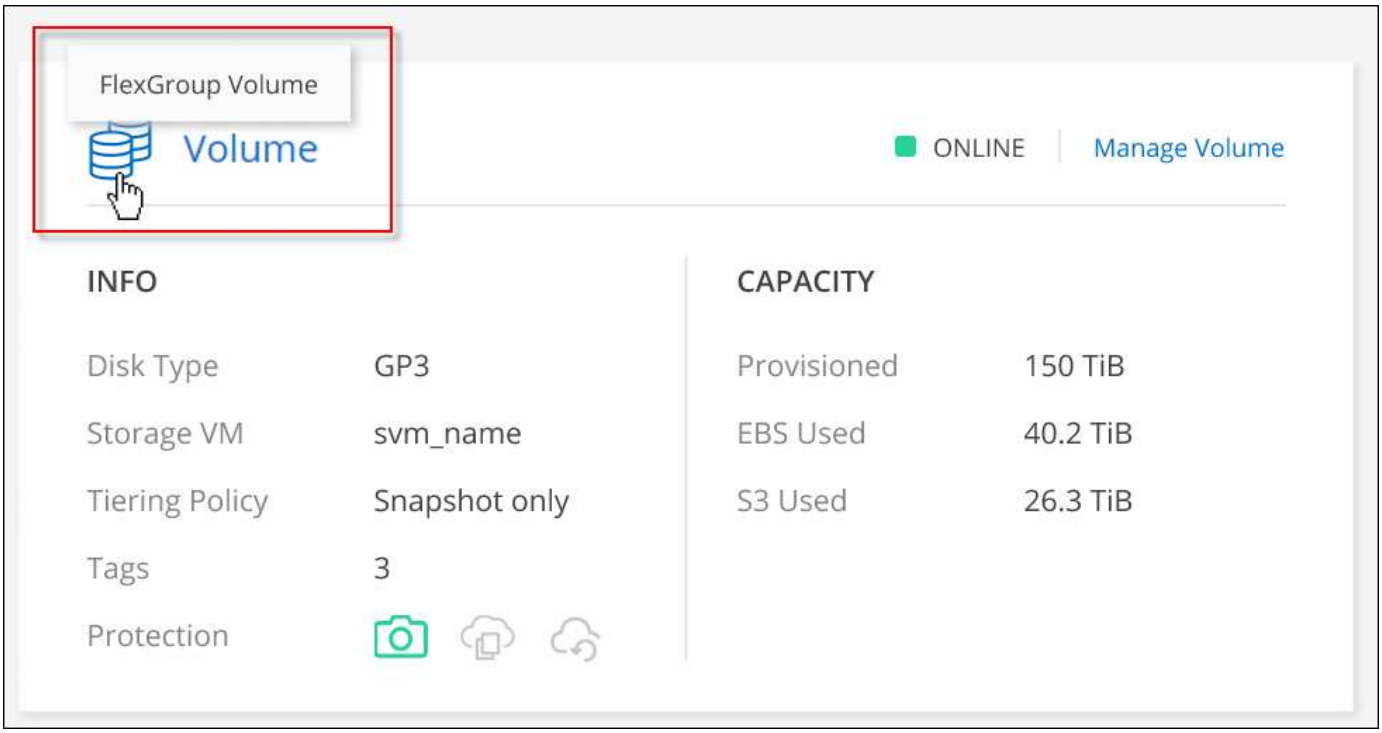
  Viene utilizzato uno schema di denominazione precedente se il tiering dei dati è stato attivato su un aggregato nella versione 9.4 o precedente.

- 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.

Visualizza volumi FlexGroup

È possibile visualizzare i volumi FlexGroup creati tramite CLI o Gestore di sistema direttamente attraverso la scheda Volumes (volumi) di BlueXP. Identico alle informazioni fornite per i volumi FlexVol, BlueXP fornisce informazioni dettagliate per i volumi FleGroup creati attraverso una sezione dedicata ai volumi. Nella sezione Volumes (volumi), è possibile identificare ciascun gruppo di volumi FlexGroup tramite il testo dell'icona. Inoltre, è possibile identificare e ordinare i volumi FlexGroup nella vista elenco volumi attraverso la colonna stile volume.



Attualmente, in BlueXP è possibile visualizzare solo i volumi FlexGroup esistenti. La possibilità di creare volumi FlexGroup in BlueXP non è disponibile, ma è prevista per una release futura.

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. Il tiering dei dati è basato sulla tecnologia FabricPool. Per una panoramica generale, vedere "Panoramica sul tiering dei dati".

Per impostare il tiering dei dati, è necessario effettuare le seguenti operazioni:

1. **Scegliere una configurazione supportata**

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

2 **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 sarà necessario eseguire alcuna operazione se BlueXP dispone delle autorizzazioni necessarie. Scopri di più.
- Per Google Cloud, è necessario configurare la subnet per Private Google Access e impostare un account di servizio. Scopri di più.

3 **Assicurarsi di disporre di un aggregato con il tiering attivato**

Il tiering dei dati deve essere attivato su un aggregato per consentire il tiering dei dati su un volume. È necessario conoscere i requisiti per i nuovi volumi e per i volumi esistenti. Scopri di più.

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

BlueXP richiede di scegliere un criterio 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 un archivio di oggetti per il Tier di capacità. BlueXP fa questo per te.
> - Non è necessario abilitare il tiering dei dati a livello di sistema.
>
> BlueXP crea un archivio di oggetti per i dati cold quando il sistema viene creato, a condizione che non vi siano problemi di connettività o permessi. In seguito, è sufficiente attivare il tiering dei dati sui volumi (e in alcuni casi, sugli aggregati).

Configurazioni che supportano il tiering dei dati

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

Supporto in AWS

- Il tiering dei dati è supportato in AWS a partire da Cloud Volumes ONTAP 9.2.
- Il livello di performance può essere SSD General Purpose (gp3 o gp2) o SSD IOPS con provisioning (io1).

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

Supporto in Azure

- Il tiering dei dati è supportato in Azure come segue:
  - Versione 9.4 in con sistemi a nodo singolo

    - Versione 9.6 in con coppie ha
- Il Tier di performance può essere costituito da dischi gestiti da SSD Premium, dischi gestiti da SSD Standard o dischi gestiti da HDD Standard.

Supporto in Google Cloud

- Il tiering dei dati è supportato in Google Cloud a partire da Cloud Volumes ONTAP 9.6.
- Il Tier di performance può essere costituito da dischi persistenti SSD, dischi persistenti bilanciati o dischi persistenti standard.

Interoperabilità delle funzionalità

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

Requisiti

A seconda del provider di cloud, è necessario impostare alcune connessioni e autorizzazioni in modo che Cloud Volumes ONTAP possa eseguire il Tier dei dati cold sullo storage a oggetti.

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 impostare una connessione tra il Tier di performance e il Tier di capacità, purché BlueXP disponga delle autorizzazioni necessarie. BlueXP abilita un endpoint del servizio VNET se il ruolo personalizzato per il connettore dispone delle seguenti autorizzazioni:

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

Per impostazione predefinita, le autorizzazioni sono incluse nel ruolo personalizzato. "Visualizzare l'autorizzazione Azure per il connettore"

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 allegare un account di servizio a Cloud Volumes ONTAP.

  "Scopri come configurare questo account di servizio".

  Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, viene richiesto di selezionare questo account di servizio.

  Se non si seleziona un account di servizio durante l'implementazione, è necessario chiudere Cloud Volumes ONTAP, accedere alla console di Google Cloud, quindi collegare l'account di servizio alle istanze di Cloud Volumes ONTAP. È quindi possibile attivare il tiering dei dati come descritto nella sezione successiva.

- Per crittografare il bucket con chiavi di crittografia gestite dal cliente, abilitare il bucket di storage Google Cloud per l'utilizzo della chiave.

  "Scopri come utilizzare le chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP".

Abilitazione del tiering dei dati dopo l'implementazione dei requisiti

BlueXP crea un archivio di oggetti per i dati cold quando viene creato il sistema, a condizione che non vi siano problemi di connettività o permessi. Se i requisiti elencati sopra non sono stati implementati fino a quando non è stato creato il sistema, sarà necessario attivare manualmente il tiering tramite l'API o System Manager, che crea l'archivio di oggetti.

> La possibilità di abilitare il tiering tramite l'interfaccia utente di BlueXP sarà disponibile in una release futura di Cloud Volumes ONTAP.

Garantire che il tiering sia abilitato sugli aggregati

Il tiering dei dati deve essere attivato su un aggregato per consentire il tiering dei dati su un volume. È necessario conoscere i requisiti per i nuovi volumi e per i volumi esistenti.

- **Nuovi volumi**

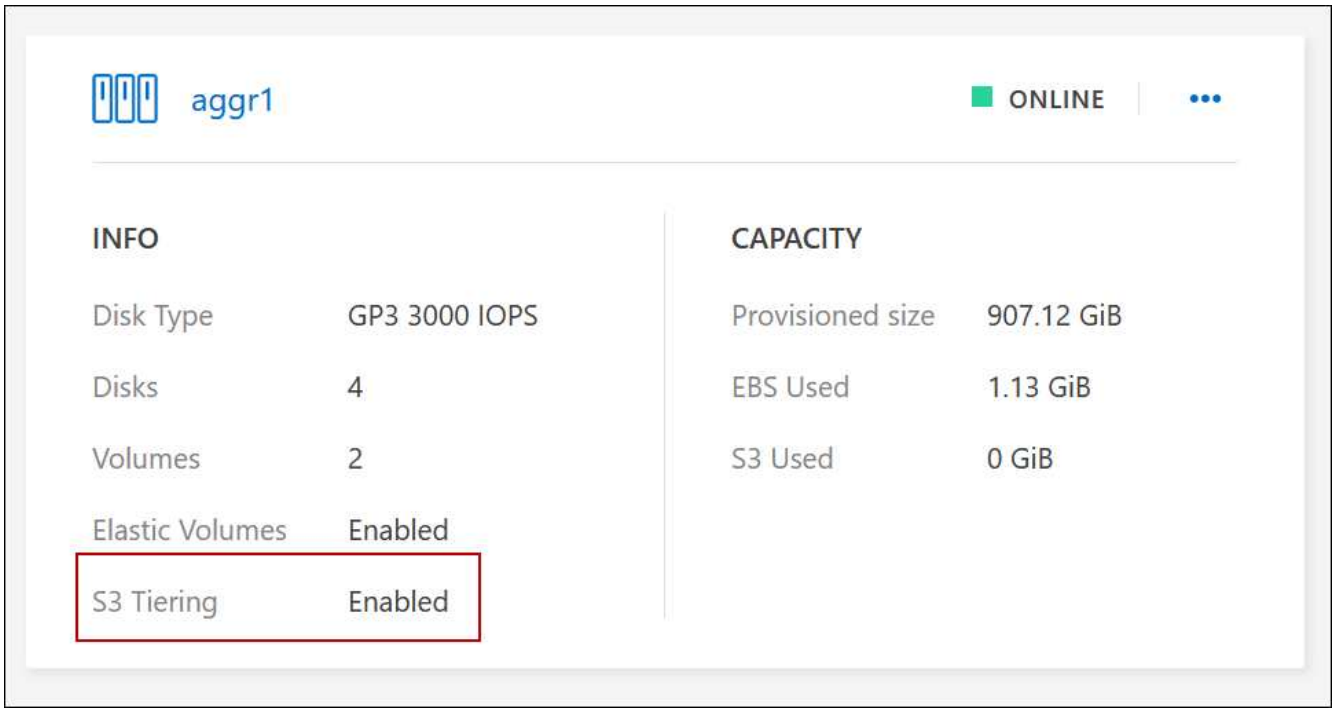
  Se abiliti il tiering dei dati su un nuovo volume, non dovrai preoccuparti di abilitare il tiering dei dati su un aggregato. BlueXP crea il volume su un aggregato esistente che ha attivato il tiering oppure crea un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering dei dati.

- **Volumi esistenti**

  Se si desidera attivare il tiering dei dati su un volume esistente, è necessario assicurarsi che il tiering dei dati sia attivato sull'aggregato sottostante. Se il tiering dei dati non è abilitato sull'aggregato esistente, sarà necessario utilizzare System Manager per associare un aggregato esistente all'archivio di oggetti.

Procedura per confermare se il tiering è attivato su un aggregato

1. Aprire l'ambiente di lavoro in BlueXP.
2. Fare clic sulla scheda aggregati.
3. Selezionare la sezione desiderata e verificare se il tiering è attivato o disattivato sull'aggregato.



Passaggi per abilitare il tiering su un aggregato

1. In System Manager, fare clic su **Storage > Tier**.
2. Fare clic sul menu delle azioni dell'aggregato e selezionare **Attach Cloud Tier**.
3. Selezionare il livello cloud da allegare e fare clic su **Save** (Salva).

Quali sono le prossime novità?

È ora possibile abilitare il tiering dei dati su volumi nuovi ed esistenti, come spiegato nella sezione successiva.

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

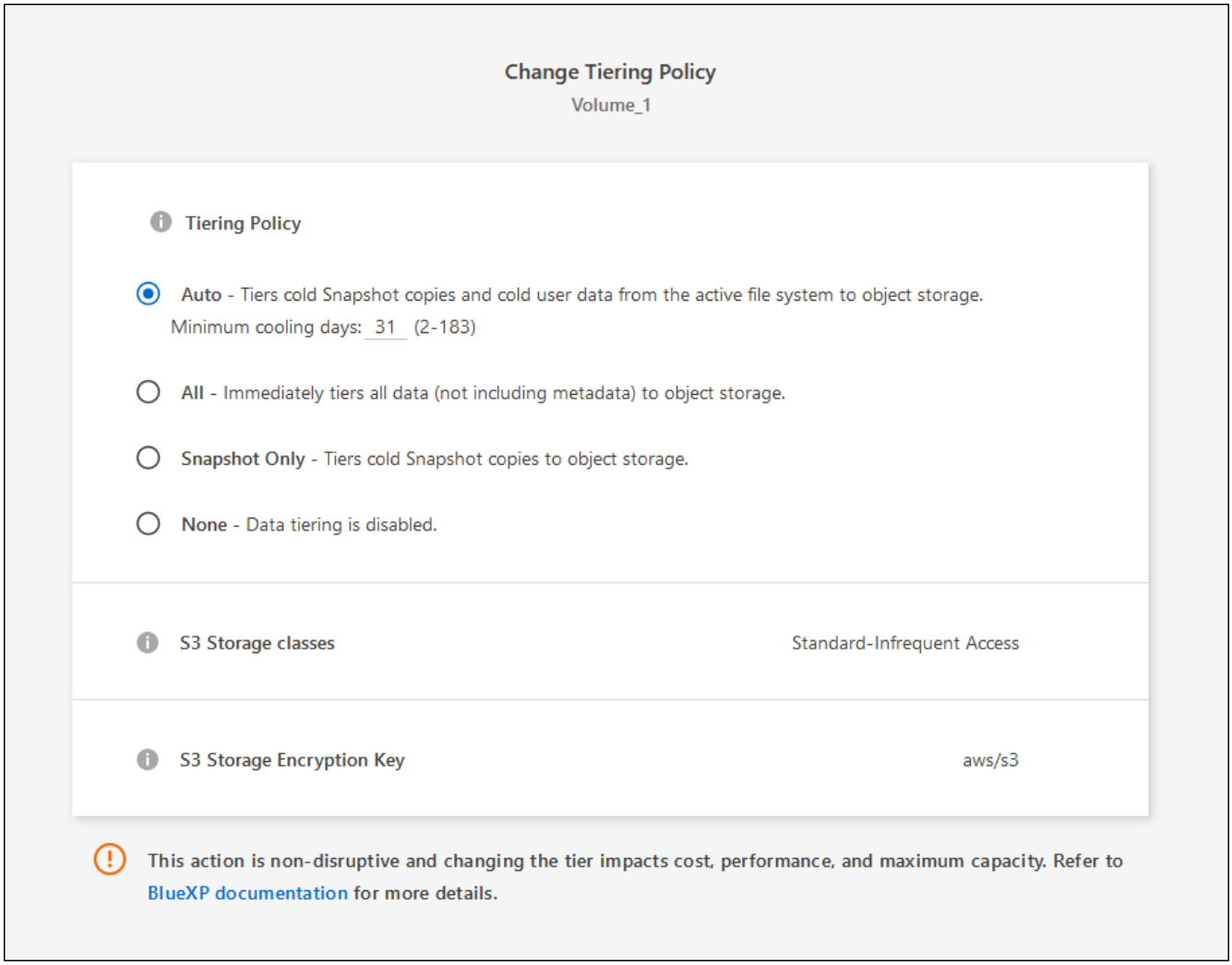
1. Nella scheda Volumes (volumi) dell'ambiente di lavoro, creare un nuovo volume o modificare il livello di un volume esistente:

Attività	Azione
Creare un nuovo volume	Fare clic su **Add New Volume** (Aggiungi nuovo volume).
Modificare un volume esistente	Selezionare il riquadro del volume desiderato, fare clic su **Manage volume** (Gestisci volume) per accedere al pannello a destra Manage Volumes (Gestisci volumi), quindi fare clic su **Advanced Actions** (azioni avanzate) e **Change Tiering policy** (Modifica policy di tiering) nel pannello a destra.

2. Selezionare una policy di tiering.

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

Esempio



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

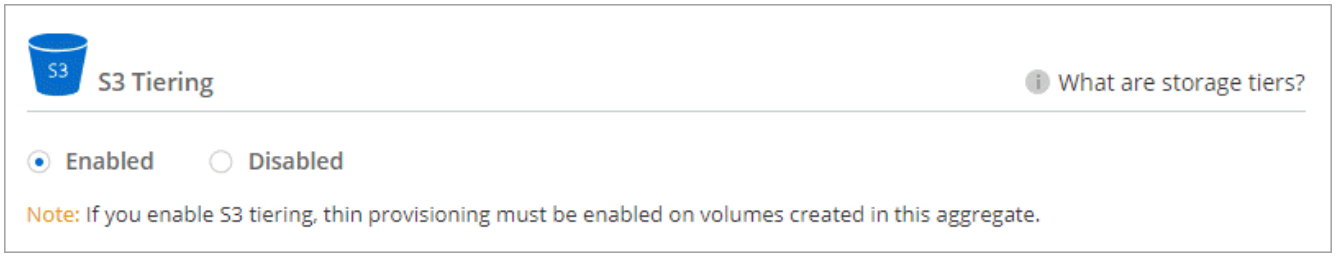
Tiering dei dati dai volumi di protezione dei dati

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. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume.
3. 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).

Modifica del rapporto di spazio libero per il tiering dei dati

Il rapporto di spazio libero per il tiering dei dati definisce la quantità di spazio libero richiesta su SSD/HDD Cloud Volumes ONTAP durante il tiering dei dati sullo storage a oggetti. L'impostazione predefinita è 10% di spazio libero, ma è possibile modificare l'impostazione in base ai requisiti.

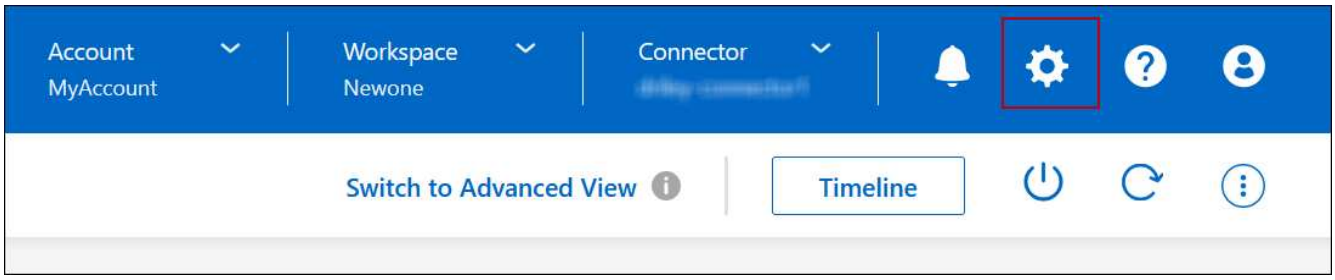
Ad esempio, è possibile scegliere meno del 10% di spazio libero per assicurarsi di utilizzare la capacità acquistata. BlueXP può quindi acquistare dischi aggiuntivi quando è richiesta capacità aggiuntiva (fino a raggiungere il limite di dischi per l'aggregato).

> Se lo spazio non è sufficiente, Cloud Volumes ONTAP non riesce a spostare i dati e potrebbe verificarsi un peggioramento delle performance. Qualsiasi modifica deve essere eseguita con cautela. In caso di dubbi, contatta il supporto NetApp per ricevere assistenza.

Il rapporto è importante per gli scenari di disaster recovery perché, man mano che i dati vengono letti dall'archivio a oggetti, Cloud Volumes ONTAP sposta i dati su SSD/HDD per offrire performance migliori. Se lo spazio non è sufficiente, Cloud Volumes ONTAP non può spostare i dati. Prenditi in considerazione questo aspetto quando modifichi il rapporto in modo da poter soddisfare i tuoi requisiti di business.

Fasi

1. Nella parte superiore destra della console BlueXP, fai clic sull'icona **Impostazioni** e seleziona **Impostazioni Cloud Volumes ONTAP**.



2. In **Capacity**, fare clic su **aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.
3. Modificare il rapporto dello spazio libero in base alle proprie esigenze e fare clic su **Save** (Salva).

Modifica del periodo di raffreddamento per la policy di tiering automatico

Se è stato attivato il tiering dei dati su un volume Cloud Volumes ONTAP utilizzando la policy di tiering *auto*, è possibile regolare il periodo di raffreddamento predefinito in base alle esigenze aziendali. Questa azione è supportata solo tramite API e CLI.

Il periodo di raffreddamento è il numero di giorni in cui i dati utente di un volume devono rimanere inattivi prima che vengano considerati "freddi" e spostati nello storage a oggetti.

Il periodo di raffreddamento predefinito per il criterio di tiering automatico è di 31 giorni. È possibile modificare il periodo di raffreddamento come segue:

- 9.8 o successivo: da 2 giorni a 183 giorni
- 9.7 o precedente: da 2 giorni a 63 giorni

Fase

1. Utilizzare il parametro *minimumCoolingDays* con la richiesta API durante la creazione di un volume o la modifica di un volume esistente.

Collegare un LUN a un host

Quando si crea un volume iSCSI, BlueXP crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, utilizzare IQN per connettersi al LUN dagli host.

Tenere presente quanto segue:

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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire i volumi.
3. Nell'ambiente di lavoro, fare clic sulla scheda **Volumes** (volumi).
4. Nella scheda Volumes (volumi), selezionare il titolo del volume desiderato, quindi fare clic su **Manage volume** (Gestisci volume) per accedere al pannello di destra Manage Volumes (Gestisci volumi).

5. Fare clic su **Target IQN**.
6. Fare clic su **Copy** (Copia) per copiare il nome IQN.
7. 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"
    - "Configurazione dell'host SAN ONTAP"

Accelera l'accesso ai dati con FlexCache Volumes

Un volume FlexCache è un volume di storage che memorizza nella cache i dati in lettura SMB e NFS da un volume di origine (o 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.

BlueXP offre gestione dei volumi FlexCache con a. "Caching del volume BlueXP" servizio.

Puoi anche utilizzare l'interfaccia a riga di comando di ONTAP o ONTAP System Manager 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"

BlueXP genera una licenza FlexCache per tutti i nuovi sistemi Cloud Volumes ONTAP. La licenza include un limite di utilizzo di 500 GiB.

Amministrazione degli aggregati

Creare aggregati

È possibile creare aggregati o lasciare che BlueXP 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.

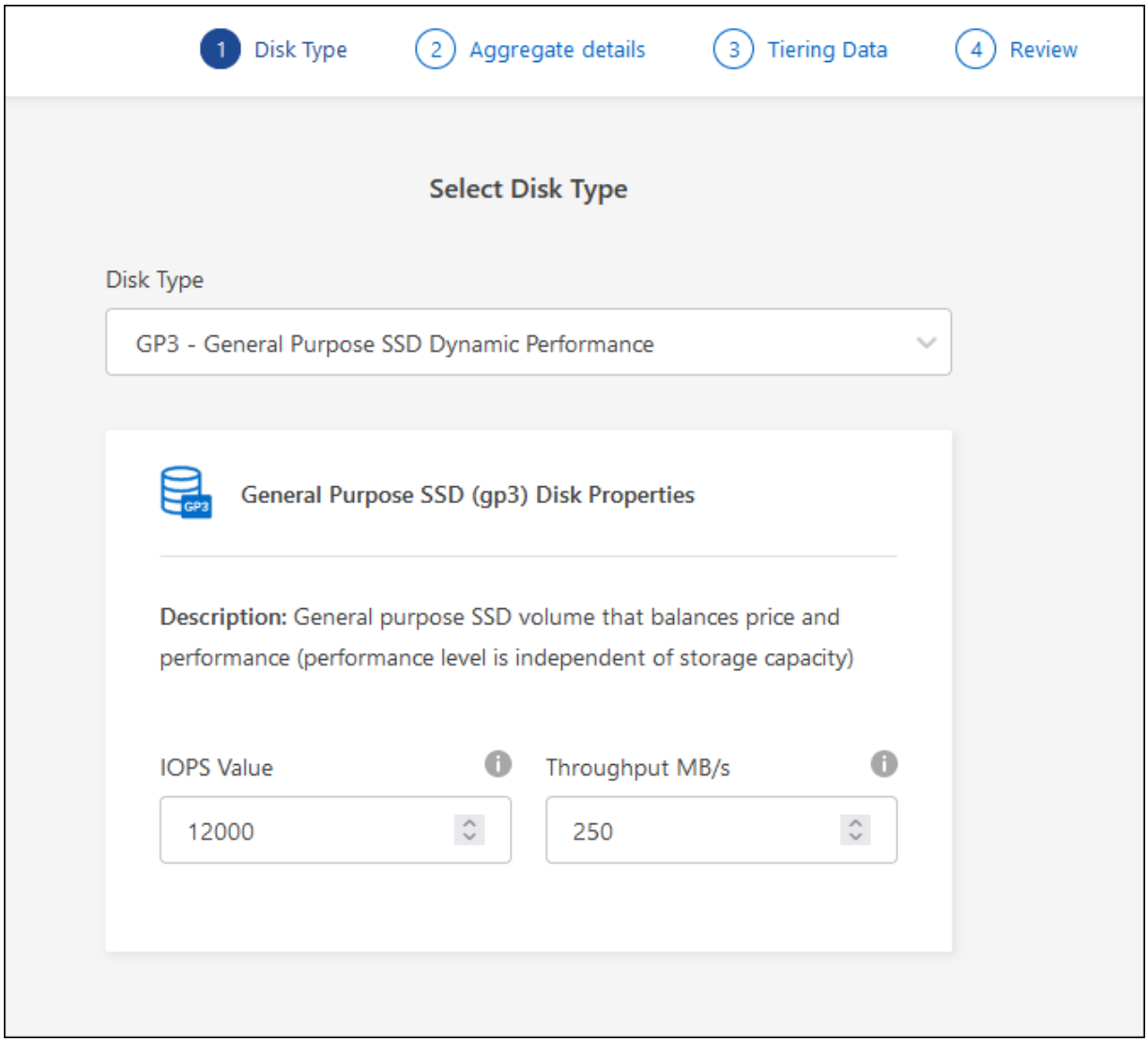
> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da BlueXP. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sul nome dell'istanza di Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
3. Nella scheda aggregati, fare clic su **Aggiungi aggregato**, quindi specificare i dettagli per l'aggregato.

AWS

- Se viene richiesto di scegliere un tipo di disco e una dimensione del disco, fare riferimento a. "Pianificare la configurazione di Cloud Volumes ONTAP in AWS".
- Se ti viene richiesto di inserire le dimensioni della capacità dell'aggregato, stai creando un aggregato su una configurazione che supporta la funzione Amazon EBS Elastic Volumes. La seguente schermata mostra un esempio di un nuovo aggregato composto da dischi gp3.



"Scopri di più sul supporto per volumi elastici".

Azure

Per informazioni sul tipo di disco e sulle dimensioni del disco, fare riferimento a. "Pianificare la configurazione di Cloud Volumes ONTAP in Azure".

Google Cloud

Per informazioni sul tipo di disco e sulle dimensioni del disco, fare riferimento a. "Pianificare la configurazione di Cloud Volumes ONTAP in Google Cloud".

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

Gestire gli aggregati

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

> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da BlueXP. 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.

Prima di iniziare

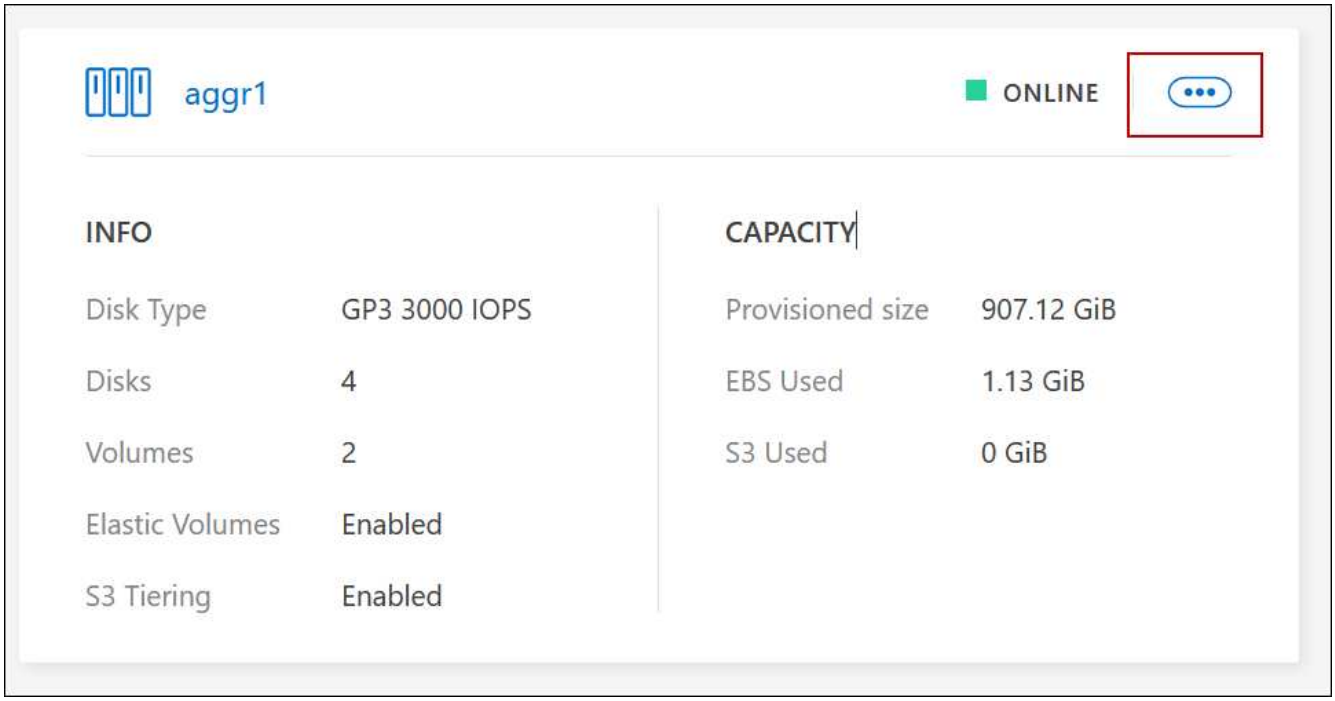
Se si desidera eliminare un aggregato, è necessario prima eliminare i volumi nell'aggregato.

A proposito di questa attività

Se un aggregato sta esaurendo lo spazio, è possibile spostare i volumi in un altro aggregato utilizzando System Manager.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
3. Nell'ambiente di lavoro, fare clic sulla scheda **aggregati**.
4. Nella scheda aggregati, selezionare il titolo desiderato e fare clic sul pulsante **… (icona ellisse)**.



5. Gestisci i tuoi aggregati:

Attività	Azione
Visualizzare informazioni su un aggregato	Sotto il … (Icona ellisse), fare clic su **View aggregate details** (Visualizza dettagli aggregati).

Attività	Azione
Creare un volume su un aggregato specifico	Sotto il … (Icona ellisse), fare clic su **Add volume** (Aggiungi volume).
Aggiungere dischi a un aggregato	a. Sotto il … (Icona ellisse), fare clic su **Aggiungi dischi**. b. Selezionare il numero di dischi che si desidera aggiungere e fare clic su **Aggiungi**. Tutti i dischi di un aggregato devono avere le stesse dimensioni.
Aumenta la capacità di un aggregato che supporta i volumi elastici di Amazon EBS	a. Sotto il … (Icona ellisse), fare clic su **aumenta capacità**. b. Immettere la capacità aggiuntiva che si desidera aggiungere, quindi fare clic su **aumento**. Si noti che è necessario aumentare la capacità dell'aggregato di un minimo di 256 GiB o del 10% delle dimensioni dell'aggregato. Ad esempio, se si dispone di un aggregato 1.77 TIB, il 10% corrisponde a 181 GiB. Si tratta di un valore inferiore a 256 GiB, pertanto le dimensioni dell'aggregato devono aumentare di almeno 256 GiB.
Eliminare un aggregato	a. Selezionare una sezione aggregata che non contiene volumi. Fare clic sul pulsante **… (Icona ellisse) > Elimina**. b. Fare nuovamente clic su **Delete** per confermare.

Gestire le impostazioni di capacità su un connettore

Ogni connettore dispone di impostazioni che determinano il modo in cui gestisce la capacità aggregata per Cloud Volumes ONTAP.

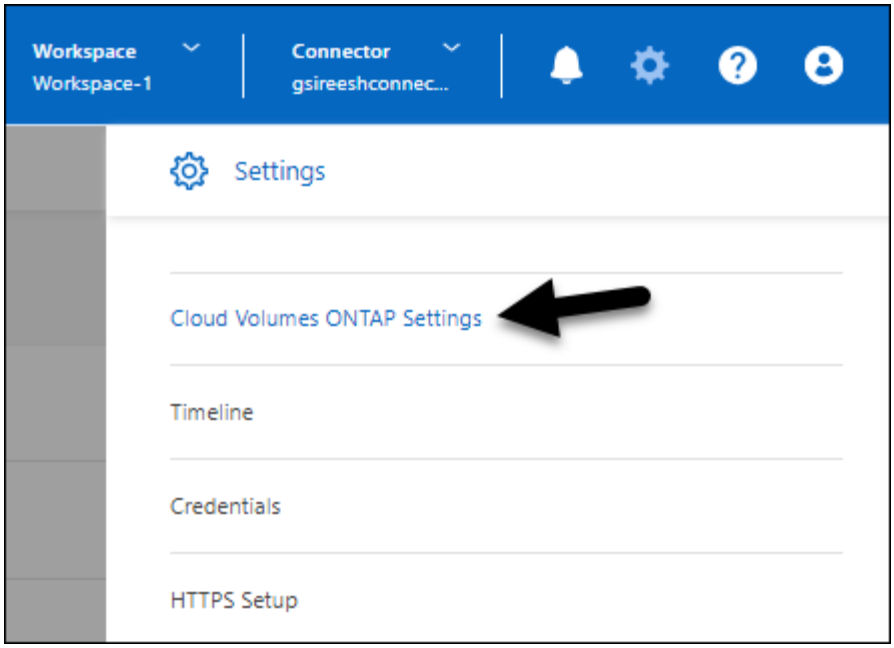
Queste impostazioni influiscono su tutti i sistemi Cloud Volumes ONTAP gestiti da un connettore. Se si dispone di un altro connettore, è possibile configurarlo in modo diverso.

Autorizzazioni richieste

Per modificare le impostazioni di Cloud Volumes ONTAP sono necessari i privilegi di amministratore dell'account.

Fasi

1. Nella parte superiore destra della console BlueXP, fai clic sull'icona Impostazioni e seleziona **Impostazioni Cloud Volumes ONTAP**.



2. In **capacità**, modificare una delle seguenti impostazioni:

Modalità di gestione della capacità

Scegli se BlueXP ti notifica le decisioni relative alla capacità dello storage o se BlueXP gestisce automaticamente i requisiti di capacità per te.

"Scopri come funziona la modalità di gestione della capacità".

Soglia capacità aggregata - rapporto spazio libero

Questo rapporto è un parametro chiave nelle decisioni di gestione della capacità e la comprensione del suo impatto è essenziale indipendentemente dal fatto che ci si trovi in una modalità di gestione della capacità automatica o manuale. Si consiglia di impostare questa soglia tenendo in considerazione le proprie esigenze di storage specifiche e la crescita prevista per mantenere un equilibrio tra utilizzo delle risorse e costi.

In modalità manuale, se il rapporto di spazio libero su un aggregato scende al di sotto della soglia specificata, viene attivata una notifica che avvisa l'utente che è necessario intraprendere azioni per risolvere il rapporto di spazio libero basso. È importante monitorare queste notifiche e gestire manualmente la capacità aggregata per evitare interruzioni del servizio e garantire performance ottimali.

Il rapporto di spazio libero viene calcolato come segue:
(capacità aggregata - capacità totale utilizzata sull'aggregato) / capacità aggregata

Vedere "Gestione automatica della capacità" Per apprendere ora la capacità viene gestita automaticamente in Cloud Volumes ONTAP.

Soglie di capacità aggregate - rapporto spazio libero per il tiering dei dati

Definisce la quantità di spazio libero richiesta sul Tier di performance (dischi) quando si tierano i dati su un Tier di capacità (storage a oggetti).

Il rapporto è importante per gli scenari di disaster recovery. Man mano che i dati vengono letti dal Tier di capacità, Cloud Volumes ONTAP sposta i dati nel Tier di performance per offrire performance migliori. Se lo spazio non è sufficiente, Cloud Volumes ONTAP non può spostare i dati.

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

Amministrazione delle macchine virtuali dello storage

Gestire le VM di storage in BlueXP

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.

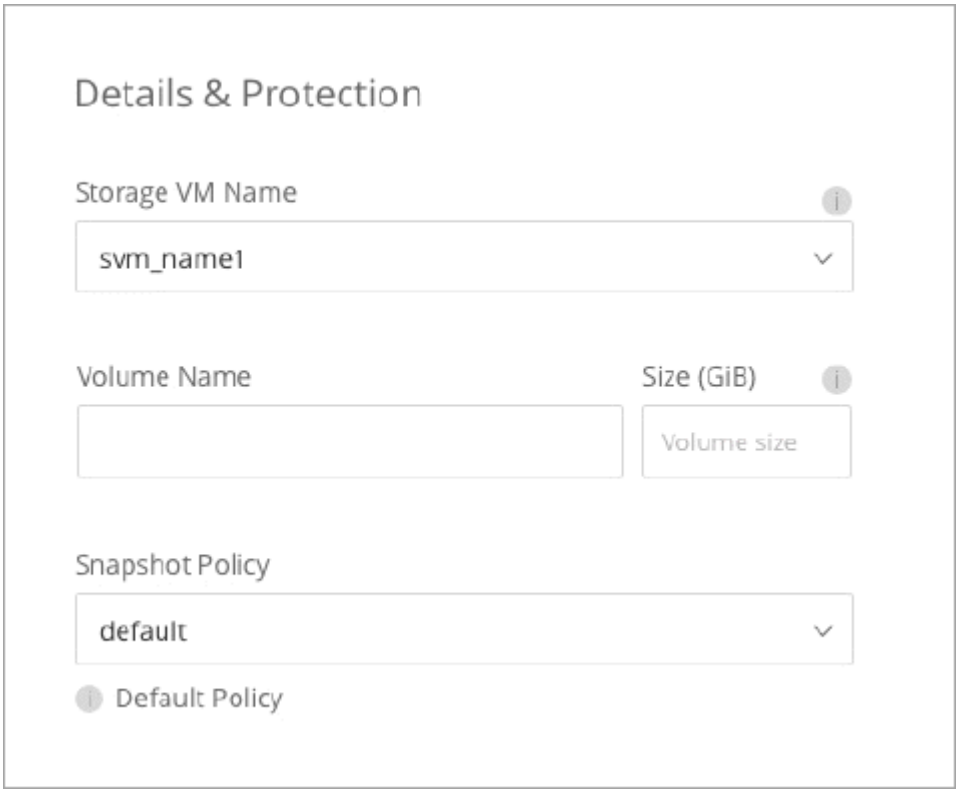
Numero di VM storage supportate

Alcune configurazioni supportano più VM di storage. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" Per verificare il numero di VM storage supportate per la versione di Cloud Volumes ONTAP in uso.

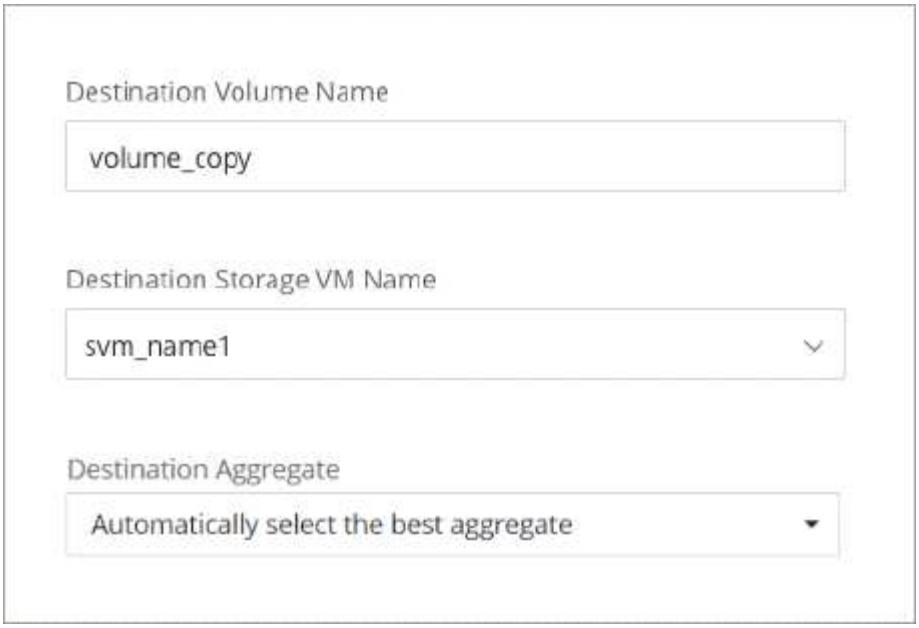
Lavorare con più macchine virtuali storage

BlueXP supporta tutte le VM 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.



Modificare il nome della VM di storage predefinita

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

Creazione di macchine virtuali storage per il data-service per Cloud Volumes ONTAP in AWS

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.

Per creare ulteriori VM di storage che servono i dati, è necessario allocare gli indirizzi IP in AWS ed eseguire i comandi ONTAP in base alla configurazione Cloud Volumes ONTAP.

Numero di VM storage supportate

Sono supportate più macchine virtuali storage con configurazioni Cloud Volumes ONTAP specifiche a partire dalla release 9.7. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" Per verificare il numero di VM storage supportate per la versione di Cloud Volumes ONTAP in uso.

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.

Verificare i limiti della configurazione

Ogni istanza EC2 supporta un numero massimo di indirizzi IPv4 privati per interfaccia di rete. È necessario verificare il limite prima di allocare gli indirizzi IP in AWS per la nuova VM di storage.

Fasi

1. Vai a. "Sezione limiti di storage nelle Note di release di Cloud Volumes ONTAP".
2. Identificare il numero massimo di indirizzi IP per interfaccia per il tipo di istanza.
3. Prendere nota di questo numero perché sarà necessario nella sezione successiva quando si assegnano gli indirizzi IP in AWS.

Allocare gli indirizzi IP in AWS

Gli indirizzi IPv4 privati devono essere assegnati alla porta e0a in AWS prima di creare LIF per la nuova VM di storage.

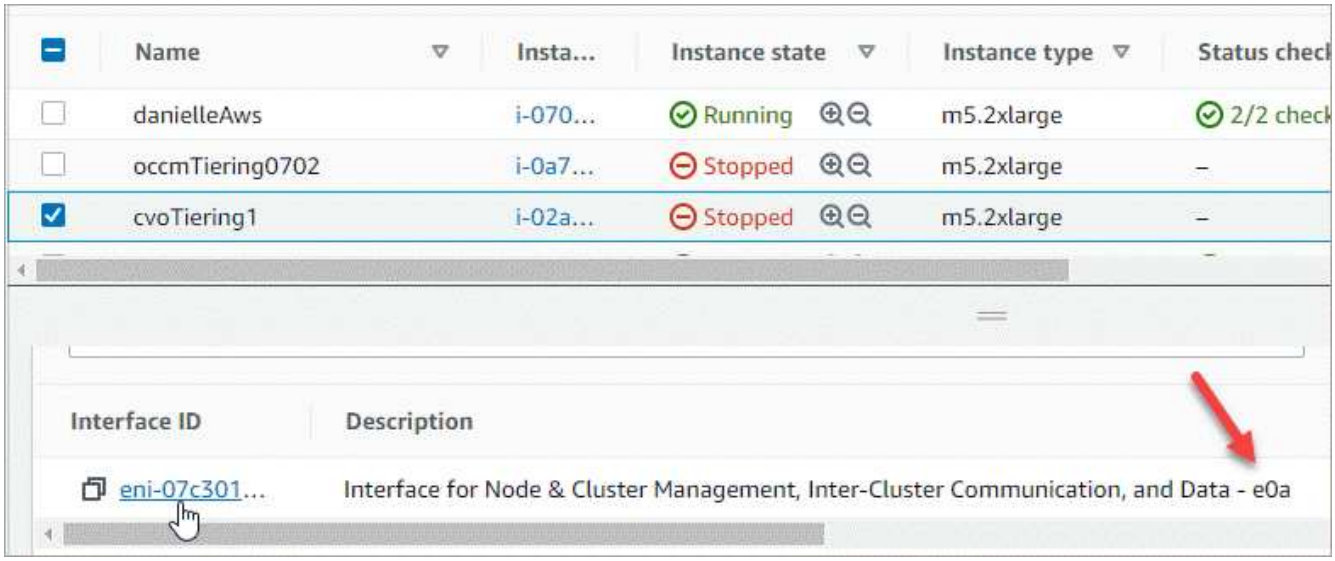
Si noti che una LIF di gestione opzionale per una VM di storage richiede un indirizzo IP privato su un sistema a nodo singolo e su una coppia ha in un singolo AZ. Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

Fasi

1. Accedere ad AWS e aprire il servizio EC2.
2. Selezionare l'istanza di Cloud Volumes ONTAP e fare clic su **rete**.

   Se si sta creando una VM di storage su una coppia ha, selezionare il nodo 1.

3. Scorrere fino a **Network interfaces** (interfacce di rete) e fare clic su **Interface ID** (ID interfaccia) per la porta e0a.



4. Selezionare l'interfaccia di rete e fare clic su **azioni > Gestisci indirizzi IP**.
5. Espandere l'elenco degli indirizzi IP per e0a.
6. Verificare gli indirizzi IP:
   a. Contare il numero di indirizzi IP allocati per confermare che la porta dispone di spazio per ulteriori indirizzi IP.

      Nella sezione precedente di questa pagina dovrebbe essere stato identificato il numero massimo di indirizzi IP supportati per interfaccia.

   b. Facoltativo: Accedere alla CLI per Cloud Volumes ONTAP ed eseguire **Network Interface show** per verificare che ciascuno di questi indirizzi IP sia in uso.

Se un indirizzo IP non è in uso, è possibile utilizzarlo con la nuova VM di storage.

7. Nella console AWS, fare clic su **Assign new IP address** (Assegna nuovo indirizzo IP) per assegnare ulteriori indirizzi IP in base alla quantità necessaria per la nuova VM di storage.
   - Sistema a nodo singolo: È necessario un IP privato secondario inutilizzato.

     Se si desidera creare una LIF di gestione sulla VM di storage, è necessario un IP privato secondario opzionale.

   - Coppia HA in un singolo AZ: Un IP privato secondario inutilizzato è richiesto sul nodo 1.

     Se si desidera creare una LIF di gestione sulla VM di storage, è necessario un IP privato secondario opzionale.

   - COPPIA HA in AZS multipli: Un IP privato secondario inutilizzato è richiesto su ciascun nodo.
8. Se si sta allocando l'indirizzo IP su una coppia ha in un singolo AZ, abilitare **Consenti la riassegnazione degli indirizzi IPv4 privati secondari**.
9. Fare clic su **Save** (Salva).
10. Se si dispone di una coppia ha in più AZS, è necessario ripetere questi passaggi per il nodo 2.

Creare una VM di storage su un sistema a nodo singolo

Questi passaggi creano una nuova VM di storage su un sistema a nodo singolo. Per creare un LIF NAS è necessario un indirizzo IP privato e un altro indirizzo IP privato opzionale per creare un LIF di gestione.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

   ```
   vserver create -rootvolume-security-style unix -rootvolume root_svm_2
   -snapshot-policy default -vserver svm_2 -aggregate aggr1
   ```

   ```
   network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
   subnet_gateway
   ```

2. Creare una LIF NAS.

   ```
   network interface create -auto-revert true -vserver svm_2 -service
   -policy default-data-files -home-port e0a -address private_ip_x -netmask
   node1Mask -lif ip_nas_2 -home-node cvo-node
   ```

   Dove *private_ip_x* è un IP privato secondario non utilizzato su e0a.

3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Dove *private_ip_y* è un altro IP privato secondario non utilizzato su e0a.

4. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

Creare una VM di storage su una coppia ha in un singolo AZ

Questi passaggi creano una nuova VM di storage su una coppia ha in un singolo AZ. Per creare un LIF NAS è necessario un indirizzo IP privato e un altro indirizzo IP privato opzionale per creare un LIF di gestione.

Entrambe queste LIF vengono allocate sul nodo 1. In caso di guasti, gli indirizzi IP privati possono spostarsi tra i nodi.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Creare un LIF NAS sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Dove *private_ip_x* è un IP privato secondario non utilizzato su e0a di cvo-node1. Questo indirizzo IP può essere ricollocato in e0a di cvo-node2 in caso di takeover perché i file di dati predefiniti della policy di servizio indicano che gli IP possono migrare nel nodo partner.

3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Dove *private_ip_y* è un altro IP privato secondario non utilizzato su e0a.

4. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

5. Se si utilizza Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare le policy dei servizi di rete per la VM di storage.

La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare la LIF iSCSI per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Creare una VM di storage su una coppia ha in più AZS

Questi passaggi creano una nuova VM di storage su una coppia ha in più AZS.

Un indirizzo IP *floating* è richiesto per un LIF NAS ed è opzionale per un LIF di gestione. Questi indirizzi IP mobili non richiedono l'allocazione di IP privati in AWS. Invece, gli IP mobili vengono configurati automaticamente nella tabella di routing AWS per puntare all'ENI di un nodo specifico nello stesso VPC.

Affinché gli IP mobili funzionino con ONTAP, è necessario configurare un indirizzo IP privato su ogni VM di storage su ciascun nodo. Ciò si riflette nei passaggi seguenti in cui viene creata una LIF iSCSI sul nodo 1 e sul nodo 2.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Creare un LIF NAS sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - L'indirizzo IP mobile deve essere esterno ai blocchi CIDR per tutti i VPC nella regione AWS in cui si implementa la configurazione ha. 192.168.209.27 è un esempio di indirizzo IP mobile. "Scopri di più sulla scelta di un indirizzo IP mobile".
   - `-service-policy default-data-files` Indica che gli IP possono migrare nel nodo partner.
3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Creare una LIF iSCSI sul nodo 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - Questa LIF iSCSI è necessaria per supportare la migrazione LIF degli IP mobili nella VM di storage. Non deve essere un LIF iSCSI, ma non può essere configurato per la migrazione tra nodi.
   - `-service-policy default-data-block` Indica che un indirizzo IP non esegue la migrazione tra i nodi.
   - *Private_ip* è un indirizzo IP privato secondario non utilizzato su eth0 (e0a) di cvo_node1.
5. Creare una LIF iSCSI sul nodo 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- Questa LIF iSCSI è necessaria per supportare la migrazione LIF degli IP mobili nella VM di storage. Non deve essere un LIF iSCSI, ma non può essere configurato per la migrazione tra nodi.
- `-service-policy default-data-block` Indica che un indirizzo IP non esegue la migrazione tra i nodi.
- *Private_ip* è un indirizzo IP privato secondario non utilizzato su eth0 (e0a) di cvo_node2.

6. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

7. Se si utilizza Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare le policy dei servizi di rete per la VM di storage.

   La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare la LIF iSCSI per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Creare macchine virtuali storage per il data-service per Cloud Volumes ONTAP in Azure

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 sono supportate VM di storage aggiuntive quando si esegue Cloud Volumes ONTAP in Azure.

Per creare ulteriori VM di storage che servono i dati, è necessario allocare gli indirizzi IP in Azure ed eseguire i comandi ONTAP per creare le VM di storage e le LIF dei dati.

Per eseguire ulteriori attività relative alle schede NIC, è possibile assegnare un ruolo di contributore della rete o un ruolo personalizzato con le autorizzazioni appropriate in Azure. Per ulteriori informazioni su queste autorizzazioni relative alla scheda NIC, consultare la "Documentazione di Microsoft Azure".

Numero di VM storage supportate

Sono supportate più macchine virtuali storage con configurazioni Cloud Volumes ONTAP specifiche a partire dalla release 9.9.0. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" Per verificare il numero di VM storage supportate per la versione di Cloud Volumes ONTAP in uso.

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.

Allocare gli indirizzi IP in Azure

È necessario allocare gli indirizzi IP in Azure prima di creare una VM di storage e allocare le LIF.

Sistema a nodo singolo

Gli indirizzi IP devono essere assegnati a nic0 in Azure prima di creare una VM di storage e allocare i LIF.

È necessario creare un indirizzo IP per l'accesso ai dati LIF e un altro indirizzo IP opzionale per una LIF di gestione delle macchine virtuali di storage (SVM). Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

Fasi

1. Accedere al portale Azure e aprire il servizio **macchina virtuale**.
2. Fare clic sul nome della macchina virtuale Cloud Volumes ONTAP.
3. Fare clic su **rete**.
4. Fare clic sul nome dell'interfaccia di rete per nic0.
5. In **Impostazioni**, fare clic su **configurazioni IP**.
6. Fare clic su **Aggiungi**.
7. Immettere un nome per la configurazione IP, selezionare **Dynamic**, quindi fare clic su **OK**.
8. Fare clic sul nome della configurazione IP appena creata, modificare l'opzione **Assignment** (assegnazione) in **Static** (statico) e fare clic su **Save** (Salva).

   Si consiglia di utilizzare un indirizzo IP statico perché un indirizzo IP statico garantisce che l'indirizzo IP non venga modificato, il che può aiutare a prevenire inutili interruzioni dell'applicazione.

Se si desidera creare una LIF di gestione SVM, ripetere questa procedura per creare un indirizzo IP aggiuntivo.

Al termine

Copiare gli indirizzi IP privati appena creati. Quando si creano i file LIF per la nuova VM di storage, è necessario specificare tali indirizzi IP.

Coppia HA

La modalità di allocazione degli indirizzi IP per una coppia ha dipende dal protocollo di storage utilizzato.

ISCSI

Gli indirizzi IP iSCSI devono essere assegnati a nic0 in Azure prima di creare una VM di storage e allocare i LIF. Gli IPS per iSCSI sono assegnati a nic0 e non al bilanciamento del carico, perché iSCSI utilizza ALUA per il failover.

È necessario creare i seguenti indirizzi IP:

- Un indirizzo IP per l'accesso LIF ai dati iSCSI dal nodo 1
- Un indirizzo IP per l'accesso LIF ai dati iSCSI dal nodo 2
- Un indirizzo IP opzionale per una LIF di gestione delle macchine virtuali di storage (SVM)

  Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

Fasi

1. Accedere al portale Azure e aprire il servizio **macchina virtuale**.
2. Fare clic sul nome della macchina virtuale Cloud Volumes ONTAP per il nodo 1.
3. Fare clic su **rete**.
4. Fare clic sul nome dell'interfaccia di rete per nic0.
5. In **Impostazioni**, fare clic su **configurazioni IP**.
6. Fare clic su **Aggiungi**.
7. Immettere un nome per la configurazione IP, selezionare **Dynamic**, quindi fare clic su **OK**.
8. Fare clic sul nome della configurazione IP appena creata, modificare l'opzione **Assignment** (assegnazione) in **Static** (statico) e fare clic su **Save** (Salva).

   Si consiglia di utilizzare un indirizzo IP statico perché un indirizzo IP statico garantisce che l'indirizzo IP non venga modificato, il che può aiutare a prevenire inutili interruzioni dell'applicazione.

9. Ripetere questi passaggi sul nodo 2.
10. Se si desidera creare una LIF di gestione SVM, ripetere questi passaggi sul nodo 1.

NFS

Gli indirizzi IP utilizzati per NFS vengono allocati nel bilanciamento del carico in modo che gli indirizzi IP possano migrare verso l'altro nodo in caso di eventi di failover.

È necessario creare i seguenti indirizzi IP:

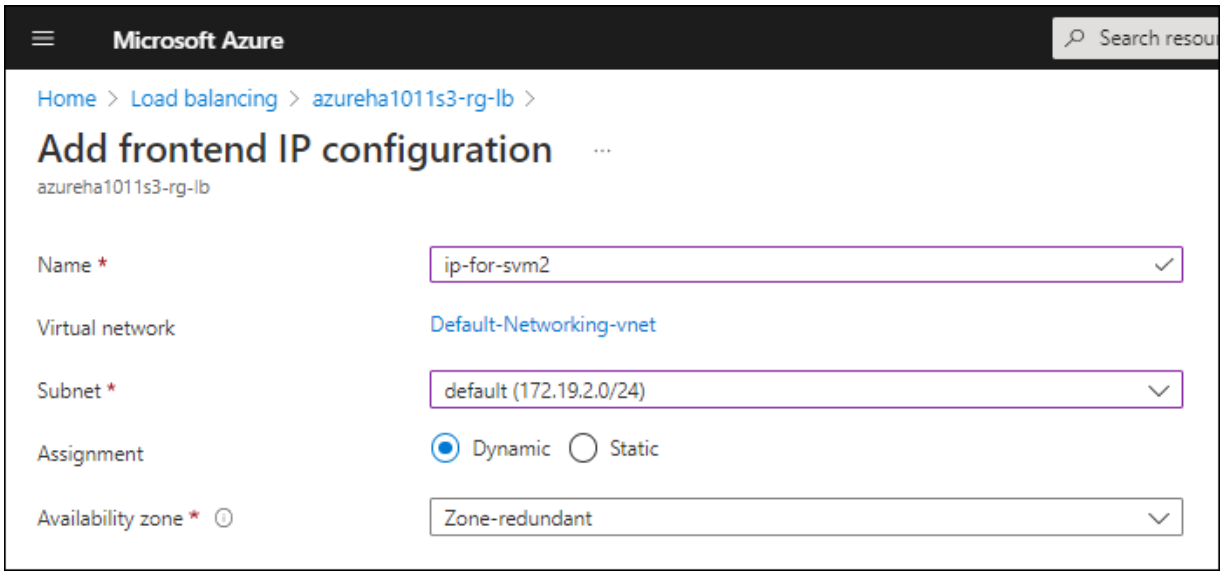
- Un indirizzo IP per l'accesso LIF dei dati NAS dal nodo 1
- Un indirizzo IP per l'accesso LIF dei dati NAS dal nodo 2
- Un indirizzo IP opzionale per una LIF di gestione delle macchine virtuali di storage (SVM)

  Le LIF iSCSI sono necessarie per la comunicazione DNS. A questo scopo viene utilizzato un LIF iSCSI perché non esegue la migrazione in caso di failover.

  Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

Fasi

1. Nel portale Azure, aprire il servizio **Load Balancer**.
2. Fare clic sul nome del bilanciamento del carico per la coppia ha.
3. Creare una configurazione IP front-end per l'accesso LIF dei dati dal nodo 1, un'altra per l'accesso LIF dei dati dal nodo 2 e un altro IP front-end opzionale per una LIF di gestione delle macchine virtuali storage (SVM).
   a. In **Settings** (Impostazioni), fare clic su **Frontend IP Configuration** (Configurazione IP front-end).
   b. Fare clic su **Aggiungi**.
   c. Inserire un nome per l'IP front-end, selezionare la subnet per la coppia Cloud Volumes ONTAP ha, lasciare selezionata l'opzione **dinamica** e, nelle regioni con zone di disponibilità, lasciare selezionata l'opzione **zona-ridondante** per garantire che l'indirizzo IP rimanga disponibile in caso di guasto di una zona.

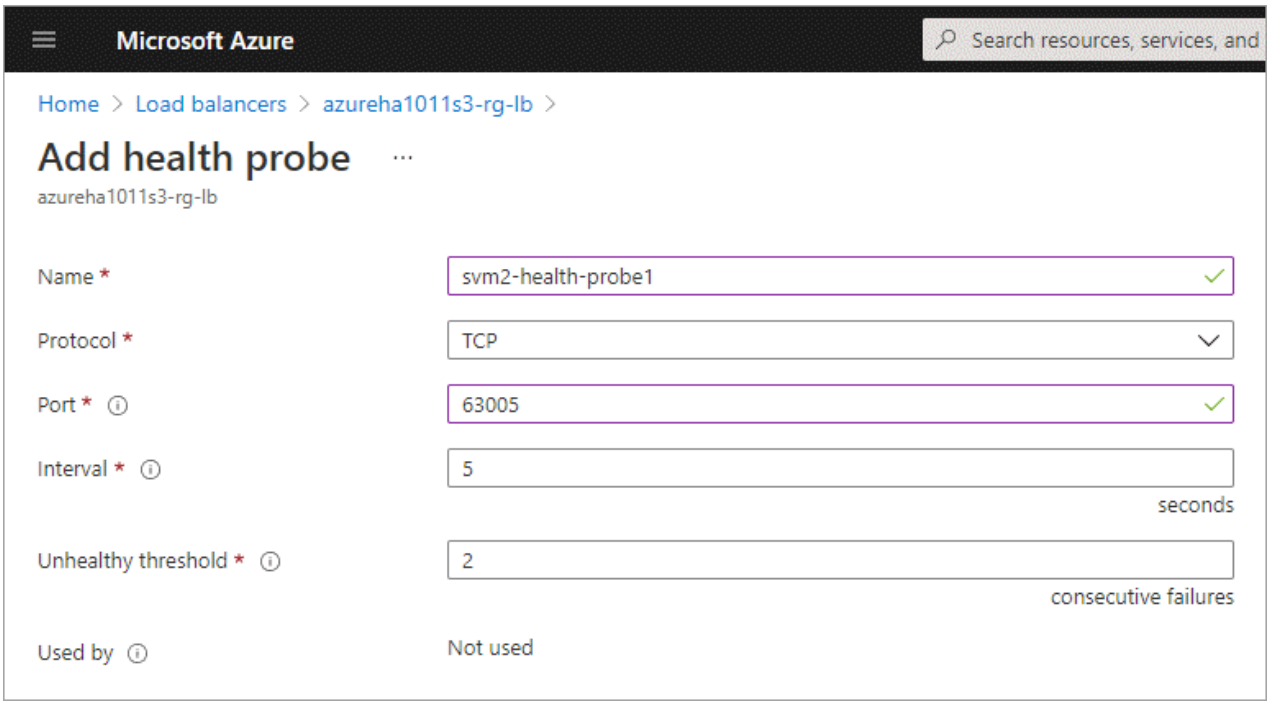


   d. Fare clic sul nome della configurazione IP front-end appena creata, impostare **Assignment** su **Static** e fare clic su **Save**.

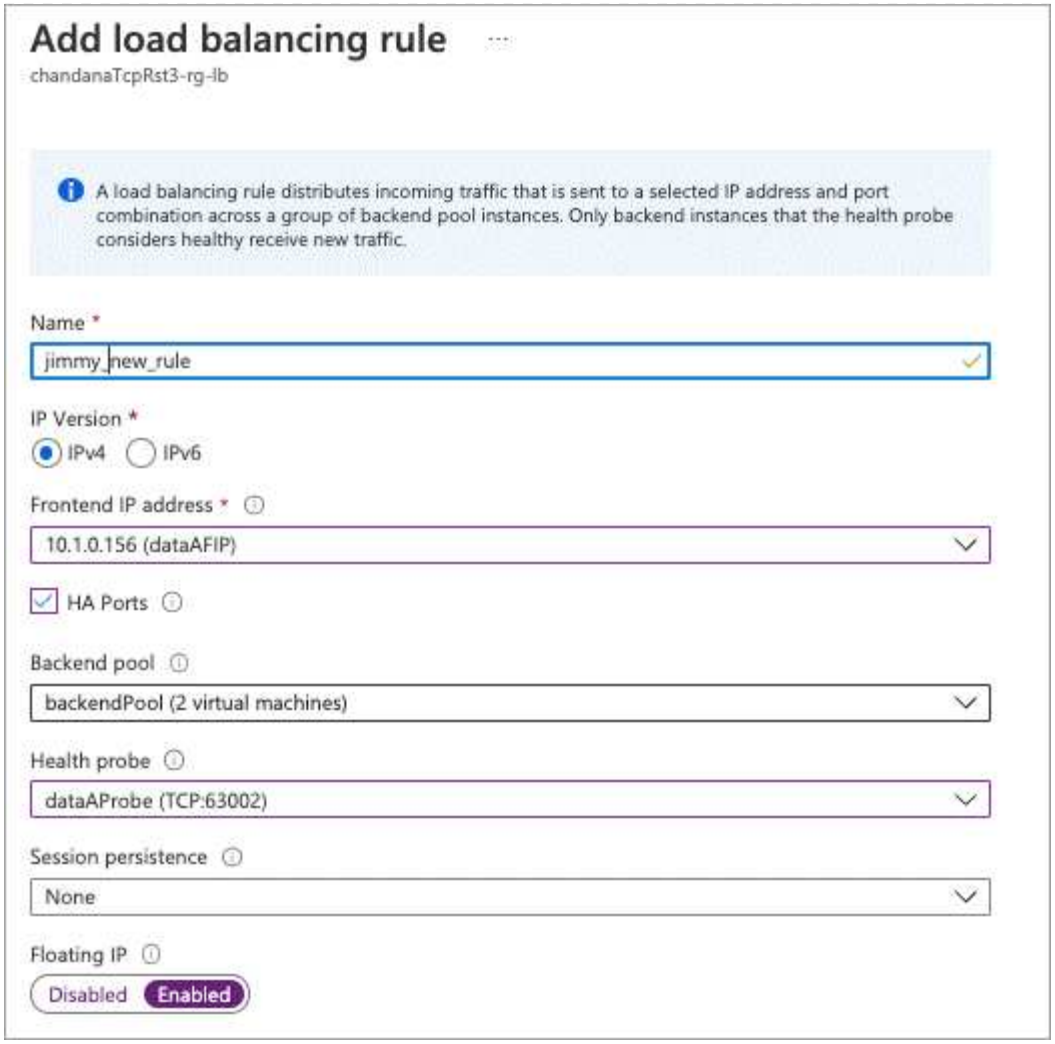
      Si consiglia di utilizzare un indirizzo IP statico perché un indirizzo IP statico garantisce che l'indirizzo IP non venga modificato, il che può aiutare a prevenire inutili interruzioni dell'applicazione.

4. Aggiungi una sonda di stato per ogni IP di frontend appena creato.
   a. Sotto **Settings** (Impostazioni) del bilanciamento del carico, fare clic su **Health probe**.
   b. Fare clic su **Aggiungi**.
   c. Immettere un nome per la sonda sanitaria e un numero di porta compreso tra 63005 e 65000. Mantenere i valori predefiniti per gli altri campi.

      È importante che il numero della porta sia compreso tra 63005 e 65000. Ad esempio, se si creano tre sonde di integrità, è possibile inserire le sonde che utilizzano i numeri di porta 63005, 63006 e 63007.



5. Creare nuove regole di bilanciamento del carico per ciascun IP front-end.
   a. Sotto le **Impostazioni** del bilanciamento del carico, fare clic su **regole di bilanciamento del carico**.
   b. Fare clic su **Add** (Aggiungi) e inserire le informazioni richieste:
      - **Nome**: Immettere un nome per la regola.
      - **IP Version** (versione IP): Selezionare **IPv4**.
      - **Indirizzo IP front-end**: Selezionare uno degli indirizzi IP front-end appena creati.
      - **Ha Ports**: Attivare questa opzione.
      - **Pool di backend**: Mantenere il pool di backend predefinito già selezionato.
      - **Health probe**: Selezionare la sonda sanitaria creata per l'IP front-end selezionato.
      - **Persistenza della sessione**: Selezionare **Nessuno**.
      - **Floating IP** (IP mobile): Selezionare **Enabled** (abilitato).



6. Assicurarsi che le regole del gruppo di sicurezza di rete per Cloud Volumes ONTAP consentano al bilanciamento del carico di inviare le sonde TCP per le sonde di stato create al punto 4 precedente. Si noti che questa opzione è consentita per impostazione predefinita.

PMI

Gli indirizzi IP utilizzati per i dati SMB vengono allocati nel bilanciamento del carico in modo che gli indirizzi IP possano migrare verso l'altro nodo in caso di eventi di failover.

È necessario creare i seguenti indirizzi IP nel bilanciamento del carico:

- Un indirizzo IP per l'accesso LIF dei dati NAS dal nodo 1
- Un indirizzo IP per l'accesso LIF dei dati NAS dal nodo 2
- Un indirizzo IP per una LIF iSCSI sul nodo 1 in ciascuna NIC0 della VM
- Un indirizzo IP per una LIF iSCSI sul nodo 2

  Le LIF iSCSI sono necessarie per le comunicazioni DNS e SMB. A questo scopo viene utilizzato un LIF iSCSI perché non esegue la migrazione in caso di failover.

- Un indirizzo IP opzionale per una LIF di gestione delle macchine virtuali di storage (SVM)

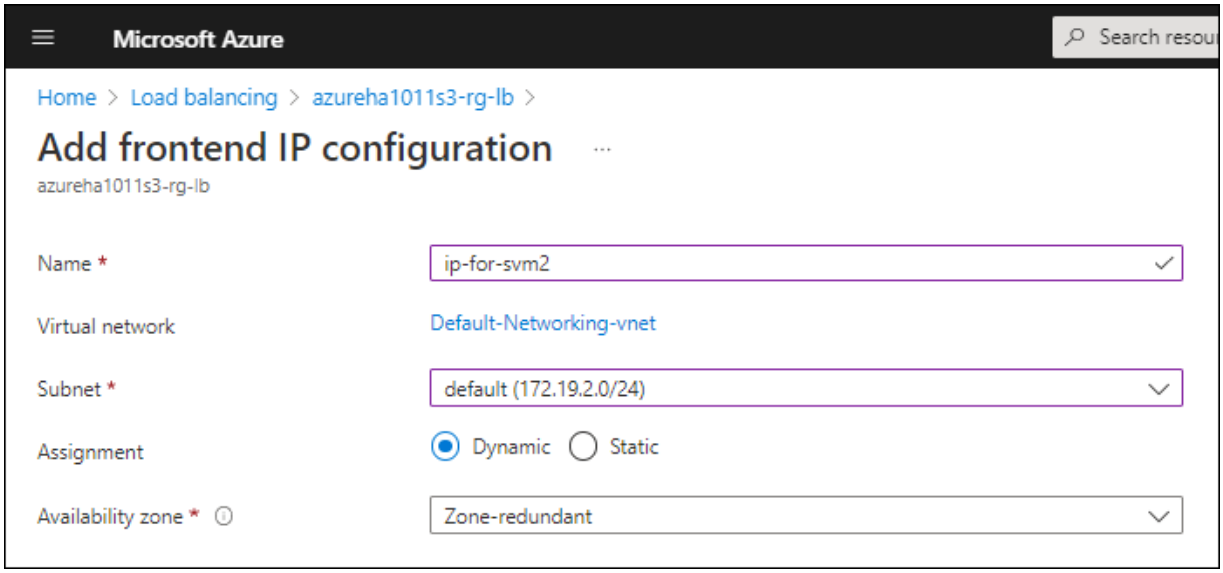
  Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

Fasi

1. Nel portale Azure, aprire il servizio **Load Balancer**.
2. Fare clic sul nome del bilanciamento del carico per la coppia ha.
3. Creare il numero richiesto di configurazioni IP front-end solo per i LIF di dati e SVM:

> Un IP front-end deve essere creato solo sotto NIC0 per ogni SVM corrispondente. Per ulteriori informazioni su come aggiungere l'indirizzo IP a SVM NIC0, vedere "Passo 7 [hyperlink]"

   a. In **Settings** (Impostazioni), fare clic su **Frontend IP Configuration** (Configurazione IP front-end).
   b. Fare clic su **Aggiungi**.
   c. Inserire un nome per l'IP front-end, selezionare la subnet per la coppia Cloud Volumes ONTAP ha, lasciare selezionata l'opzione **dinamica** e, nelle regioni con zone di disponibilità, lasciare selezionata l'opzione **zona-ridondante** per garantire che l'indirizzo IP rimanga disponibile in caso di guasto di una zona.



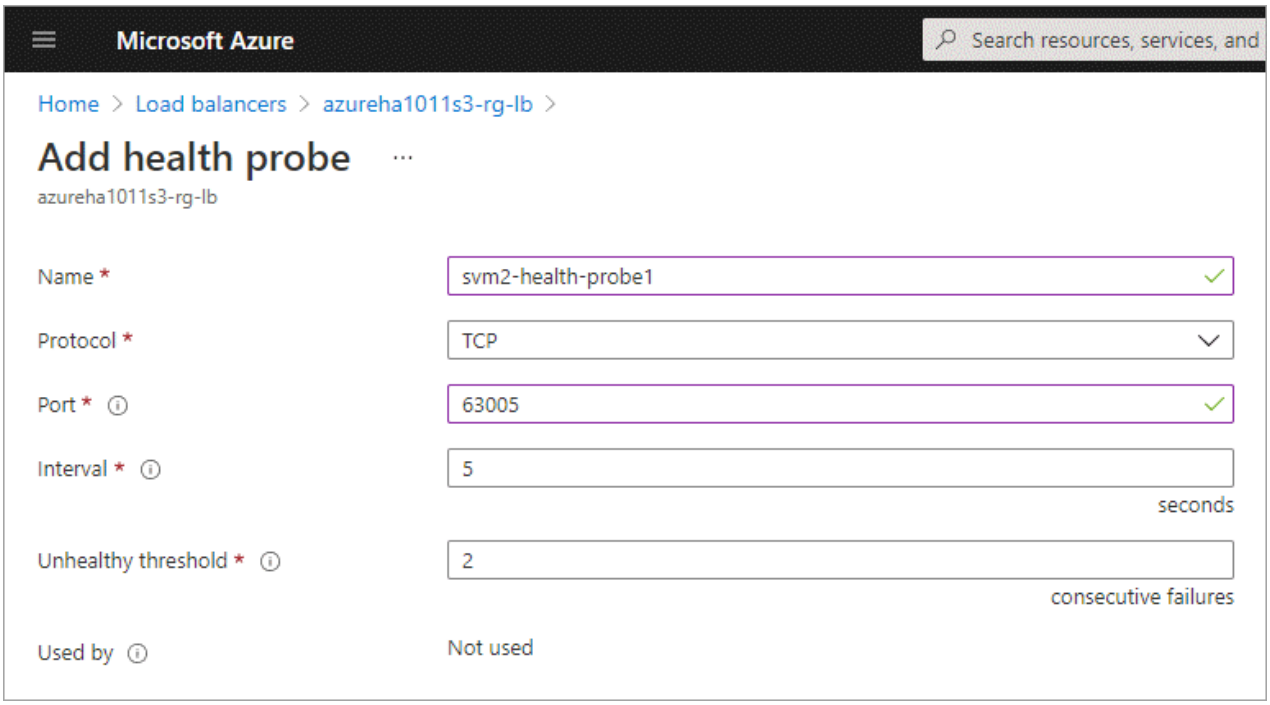
   d. Fare clic sul nome della configurazione IP front-end appena creata, impostare **Assignment** su **Static** e fare clic su **Save**.

      Si consiglia di utilizzare un indirizzo IP statico perché un indirizzo IP statico garantisce che l'indirizzo IP non venga modificato, il che può aiutare a prevenire inutili interruzioni dell'applicazione.

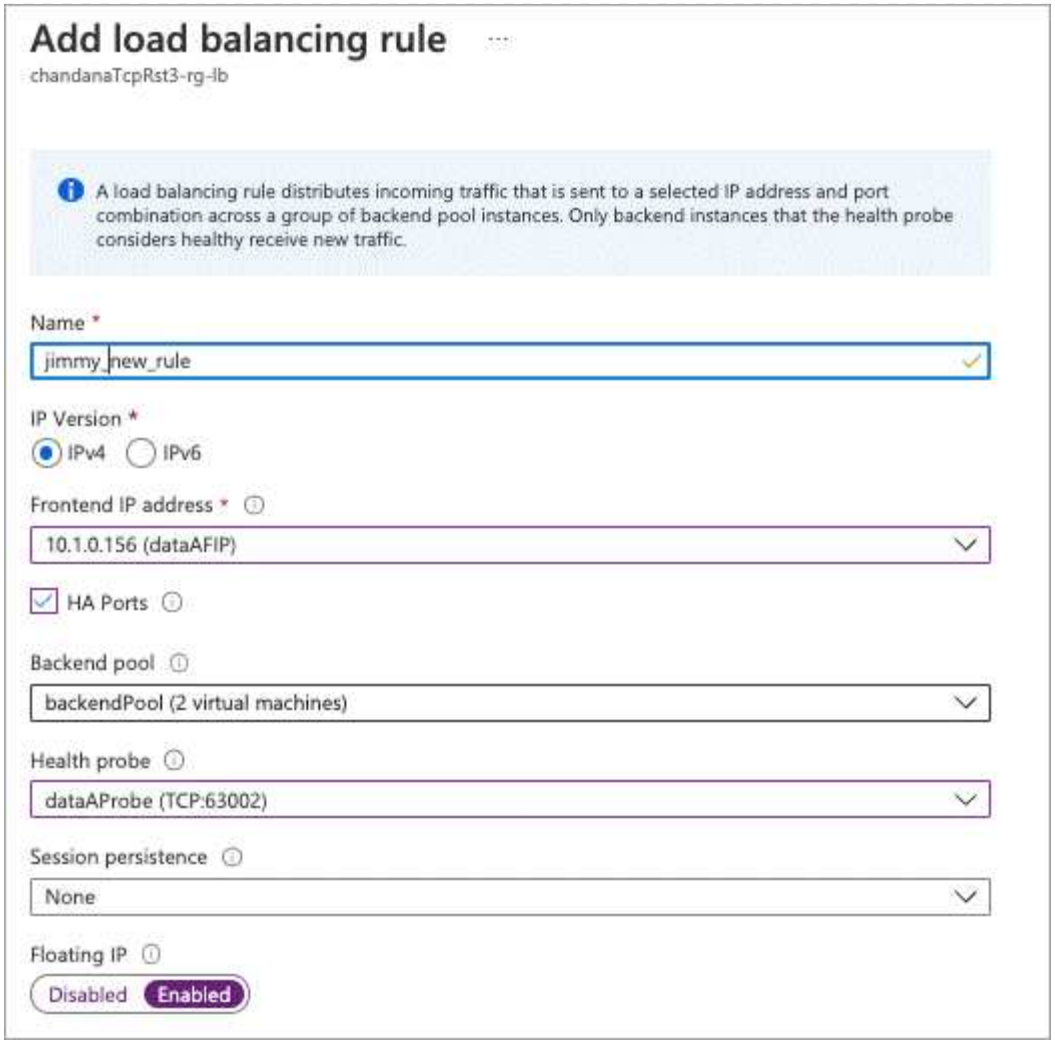
4. Aggiungi una sonda di stato per ogni IP di frontend appena creato.

   a. Sotto **Settings** (Impostazioni) del bilanciamento del carico, fare clic su **Health probe**.
   b. Fare clic su **Aggiungi**.
   c. Immettere un nome per la sonda sanitaria e un numero di porta compreso tra 63005 e 65000. Mantenere i valori predefiniti per gli altri campi.

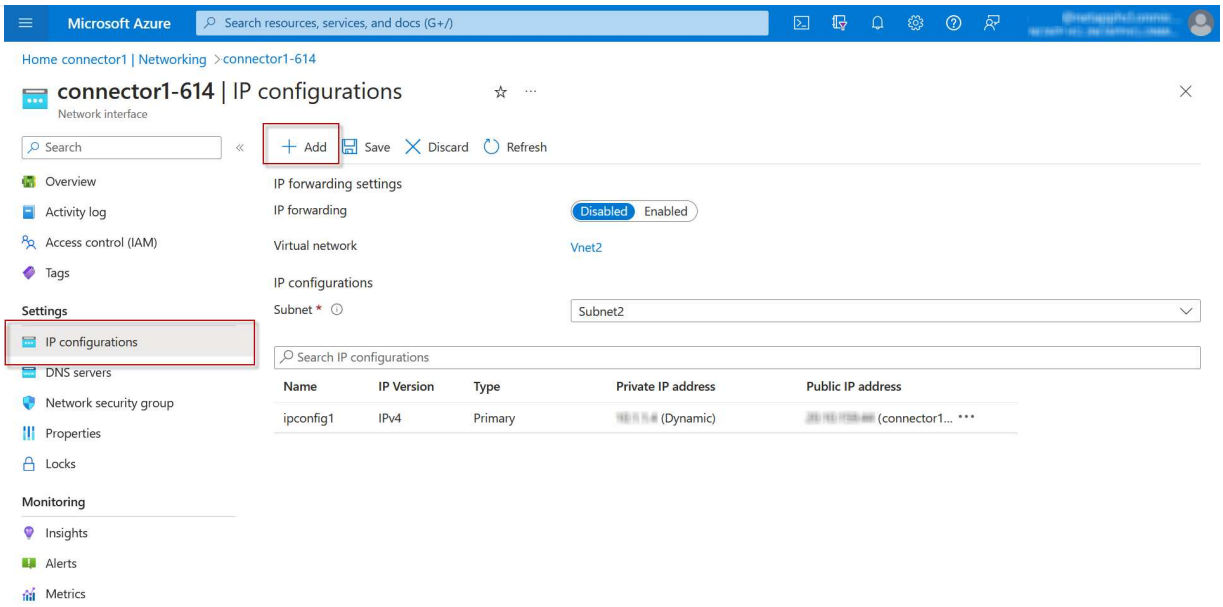
      È importante che il numero della porta sia compreso tra 63005 e 65000. Ad esempio, se si creano tre sonde di integrità, è possibile inserire le sonde che utilizzano i numeri di porta 63005, 63006 e 63007.



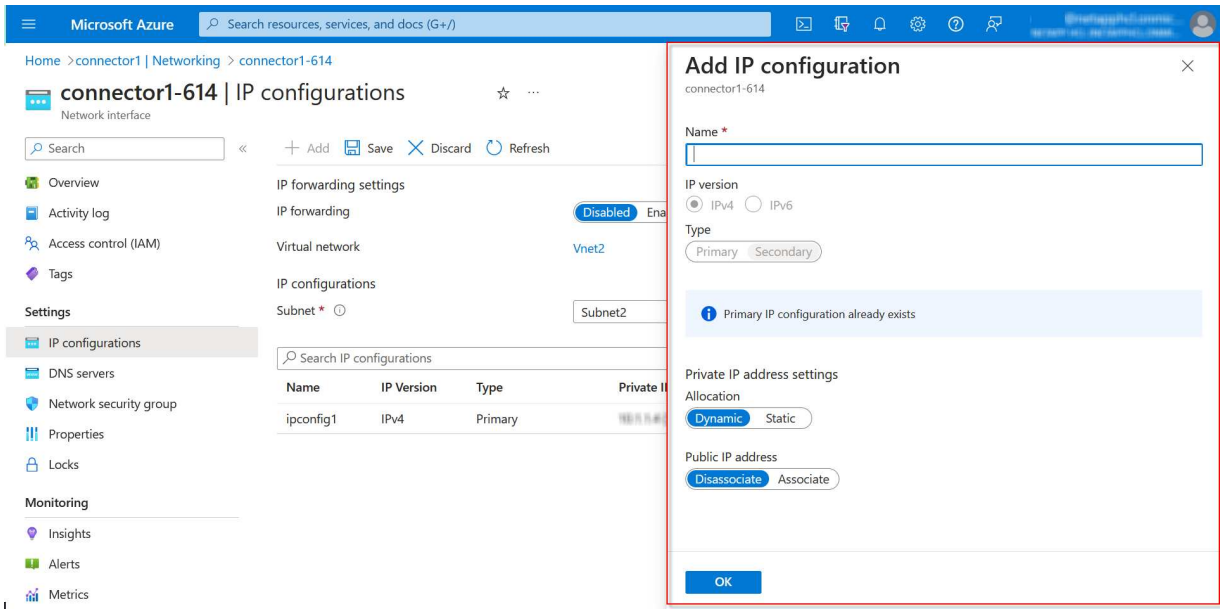
5. Creare nuove regole di bilanciamento del carico per ciascun IP front-end.
   a. Sotto le **Impostazioni** del bilanciamento del carico, fare clic su **regole di bilanciamento del carico**.
   b. Fare clic su **Add** (Aggiungi) e inserire le informazioni richieste:
      - **Nome**: Immettere un nome per la regola.
      - **IP Version** (versione IP): Selezionare **IPv4**.
      - **Indirizzo IP front-end**: Selezionare uno degli indirizzi IP front-end appena creati.
      - **Ha Ports**: Attivare questa opzione.
      - **Pool di backend**: Mantenere il pool di backend predefinito già selezionato.
      - **Health probe**: Selezionare la sonda sanitaria creata per l'IP front-end selezionato.
      - **Persistenza della sessione**: Selezionare **Nessuno**.
      - **Floating IP** (IP mobile): Selezionare **Enabled** (abilitato).



6. Assicurarsi che le regole del gruppo di sicurezza di rete per Cloud Volumes ONTAP consentano al bilanciamento del carico di inviare le sonde TCP per le sonde di stato create al punto 4 precedente. Si noti che questa opzione è consentita per impostazione predefinita.
7. Per le LIF iSCSI, aggiungere l'indirizzo IP per NIC0.
   a. Fare clic sul nome della macchina virtuale Cloud Volumes ONTAP.
   b. Fare clic su **rete**.
   c. Fare clic sul nome dell'interfaccia di rete per nic0.
   d. In Impostazioni, fare clic su **configurazioni IP**.
   e. Fare clic su **Aggiungi**.



f. Immettere un nome per la configurazione IP, selezionare Dynamic (dinamica), quindi fare clic su **OK**.



g. Fare clic sul nome della configurazione IP appena creata, impostare l'assegnazione su Static (statico) e fare clic su **Save** (Salva).

> Si consiglia di utilizzare un indirizzo IP statico perché un indirizzo IP statico garantisce che l'indirizzo IP non venga modificato, il che può aiutare a prevenire inutili interruzioni dell'applicazione.

Al termine

Copiare gli indirizzi IP privati appena creati. Quando si creano i file LIF per la nuova VM di storage, è necessario specificare tali indirizzi IP.

Creazione di una VM di storage e di LIF

Dopo aver allocato gli indirizzi IP in Azure, è possibile creare una nuova VM di storage su un sistema a nodo singolo o su una coppia ha.

Sistema a nodo singolo

Il modo in cui crei una VM di storage e dei LIF su un sistema a nodo singolo dipende dal protocollo di storage in uso.

ISCSI

Seguire questi passaggi per creare una nuova VM di storage, insieme ai LIF richiesti.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Creare una LIF dati:

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>
-home-node <name-of-node1> -data-protocol iscsi
```

3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

NFS

Seguire questi passaggi per creare una nuova VM di storage, insieme ai LIF richiesti.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Creare una LIF dati:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

PMI

Seguire questi passaggi per creare una nuova VM di storage, insieme ai LIF richiesti.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Creare una LIF dati:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

Coppia HA

Il modo in cui si crea una VM di storage e una LIF su una coppia ha dipende dal protocollo di storage in uso.

ISCSI

Seguire questi passaggi per creare una nuova VM di storage, insieme ai LIF richiesti.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Creazione di LIF dei dati:
   a. Utilizzare il seguente comando per creare una LIF iSCSI sul nodo 1.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. Utilizzare il seguente comando per creare una LIF iSCSI sul nodo 2.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage sul nodo 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

   Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

4. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un

aggregato prima di poter creare volumi sulla VM di storage.

5. Se si utilizza Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare le policy dei servizi di rete per la VM di storage.

   a. Immettere il seguente comando per accedere alla modalità avanzata.

   ```
   ::> set adv -con off
   ```

   La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare la LIF iSCSI per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

Seguire questi passaggi per creare una nuova VM di storage, insieme ai LIF richiesti.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Creazione di LIF dei dati:
   a. Utilizzare il seguente comando per creare un LIF NAS sul nodo 1.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. Utilizzare il seguente comando per creare un LIF NAS sul nodo 2.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. Creazione di LIF iSCSI per la comunicazione DNS:
   a. Utilizzare il seguente comando per creare una LIF iSCSI sul nodo 1.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. Utilizzare il seguente comando per creare una LIF iSCSI sul nodo 2.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage sul nodo 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

   Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

5. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage sul nodo 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

   Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

6. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

7. Se si utilizza Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare le policy dei servizi di rete per la VM di storage.

   a. Immettere il seguente comando per accedere alla modalità avanzata.

```
::> set adv -con off
```

      La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare la LIF iSCSI per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

PMI

Seguire questi passaggi per creare una nuova VM di storage, insieme ai LIF richiesti.

Fasi

1. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Creazione di LIF dati NAS:
   a. Utilizzare il seguente comando per creare un LIF NAS sul nodo 1.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. Utilizzare il seguente comando per creare un LIF NAS sul nodo 2.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. Creazione di LIF iSCSI per la comunicazione DNS:
   a. Utilizzare il seguente comando per creare una LIF iSCSI sul nodo 1.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. Utilizzare il seguente comando per creare una LIF iSCSI sul nodo 2.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. Opzionale: Creare una LIF di gestione delle macchine virtuali dello storage sul nodo 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

5. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

6. Se si utilizza Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare le policy dei servizi di rete per la VM di storage.

   a. Immettere il seguente comando per accedere alla modalità avanzata.

   ```
   ::> set adv -con off
   ```

   La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare la LIF iSCSI per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

Quali sono le prossime novità?

Dopo aver creato una VM di storage su una coppia ha, si consiglia di attendere 12 ore prima di eseguire il provisioning dello storage su tale SVM. A partire da Cloud Volumes ONTAP 9.10.1, BlueXP esegue la scansione delle impostazioni per il bilanciamento del carico di una coppia ha a un intervallo di 12 ore. Se sono presenti nuove SVM, BlueXP abilita un'impostazione che fornisce un failover non pianificato più breve.

Creare macchine virtuali storage per il data-service per Cloud Volumes ONTAP in Google Cloud

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

A partire dalla versione 9.11.1, sono supportate più macchine virtuali storage con configurazioni Cloud Volumes ONTAP specifiche in Google Cloud. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" Per verificare il numero di VM storage supportate per la versione di Cloud Volumes ONTAP in uso.

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.

Creare una VM di storage

Se supportato dalla licenza, è possibile creare più VM di storage su un sistema a nodo singolo o su una coppia ha. Tenere presente che è necessario utilizzare l'API BlueXP per creare una VM di storage su una coppia ha, mentre è possibile utilizzare CLI o System Manager per creare una VM di storage su un sistema a nodo singolo.

Sistema a nodo singolo

Questa procedura consente di creare una nuova VM di storage su un sistema a nodo singolo utilizzando la CLI. Per creare una LIF dati è necessario un indirizzo IP privato e un altro indirizzo IP privato opzionale per creare una LIF di gestione.

Fasi

1. In Google Cloud, accedere all'istanza di Cloud Volumes ONTAP e aggiungere un indirizzo IP a nic0 per ogni LIF.

Se si desidera creare una LIF di gestione sulla VM di storage, è necessario un indirizzo IP per una LIF dati e un altro indirizzo IP opzionale.

"Documentazione di Google Cloud: Aggiunta di intervalli IP alias a un'istanza esistente"

2. Creare la VM di storage e un percorso verso la VM di storage.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-
volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway
<ip-of-gateway-server>
```

3. Creare una LIF dati specificando l'indirizzo IP aggiunto in Google Cloud.

ISCSI

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data
-protocol iscsi
```

NFS o SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

4. Facoltativo: Creare una LIF di gestione delle macchine virtuali dello storage specificando l'indirizzo IP aggiunto in Google Cloud.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length
<length> -home-node <name-of-node1> -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false
-failover-group Default
```

5. Assegnare uno o più aggregati alla VM di storage.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

Questo passaggio è necessario perché la nuova VM di storage deve accedere ad almeno un aggregato prima di poter creare volumi sulla VM di storage.

Coppia HA

È necessario utilizzare l'API BlueXP per creare una VM di storage su un sistema Cloud Volumes ONTAP in Google Cloud. L'utilizzo dell'API (e non di System Manager o CLI) è necessario perché BlueXP configura la VM di storage con i servizi LIF richiesti, oltre a un LIF iSCSI necessario per le comunicazioni SMB/CIFS in uscita.

Si noti che BlueXP assegna gli indirizzi IP richiesti in Google Cloud e crea la VM di storage con una LIF dati per l'accesso SMB/NFS e una LIF iSCSI per le comunicazioni SMB in uscita.

Autorizzazioni richieste per Google Cloud

Il connettore richiede autorizzazioni specifiche per la creazione e la gestione di macchine virtuali storage per le coppie Cloud Volumes ONTAP ha. Le autorizzazioni richieste sono incluse in "Le policy fornite da NetApp".

Fasi

1. Utilizzare la seguente chiamata API per creare una VM di storage:

   ```
   POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
   ```

   L'ente di richiesta deve includere quanto segue:

   ```
   { "svmName": "myNewSvm1" }
   ```

Gestire le VM di storage su coppie ha

L'API BlueXP supporta anche la ridenominazione e l'eliminazione delle macchine virtuali di storage sulle coppie ha.

Rinominare una VM di storage

Se necessario, è possibile modificare il nome di una VM di storage in qualsiasi momento.

Fasi

1. Utilizzare la seguente chiamata API per rinominare una VM di storage:

   ```
   PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
   ```

   L'ente di richiesta deve includere quanto segue:

   ```
   {
   "svmNewName": "newSvmName",
   "svmName": "oldSvmName"
   }
   ```

Eliminare una VM di storage

Se non hai più bisogno di una VM di storage, puoi eliminarla da Cloud Volumes ONTAP.

Fasi

1. Utilizzare la seguente chiamata API per eliminare una VM di storage:

   ```
   DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
   ```

Configurare il disaster recovery delle SVM

BlueXP non fornisce supporto di setup o orchestrazione per il disaster recovery delle Storage VM (SVM). È necessario utilizzare System Manager o la CLI.

Se configuri la replica SVM di SnapMirror tra due sistemi Cloud Volumes ONTAP, la replica deve essere eseguita tra due sistemi ha Pair o due sistemi a nodo singolo. Non è possibile configurare la replica SVM SnapMirror tra una coppia ha e un sistema a nodo singolo.

Fare riferimento ai seguenti documenti per le istruzioni CLI.

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

Sicurezza e crittografia dei dati

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). NVE e NAE sono soluzioni software che consentono la crittografia dei volumi a riposo dei dati conforme a FIPS 140-2. "Scopri di più su queste soluzioni di crittografia".

NVE e NAE sono supportati con un gestore di chiavi esterno.

Gestione delle chiavi con AWS Key Management Service

È possibile utilizzare "KMS (Key Management Service) di AWS" Per proteggere le chiavi di crittografia ONTAP in un'applicazione implementata da AWS.

La gestione delle chiavi con AWS KMS può essere abilitata con l'interfaccia CLI o l'API REST ONTAP.

Quando si utilizza il KMS, tenere presente che per impostazione predefinita viene utilizzata la LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi del cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione di AWS. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.12.0 o successiva
- È necessario aver installato la licenza Volume Encryption (VE) e.
- È necessario aver installato la licenza MTEKM (Multi-tenant Encryption Key Management).
- Devi essere un amministratore del cluster o di SVM
- È necessario disporre di un abbonamento AWS attivo

> È possibile configurare le chiavi solo per una SVM dati.

Configurazione

AWS

1. È necessario creare un "concedi" Per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     Per creare una sovvenzione, fare riferimento a. "Documentazione AWS".

2. "Aggiungere un criterio al ruolo IAM appropriato." La policy dovrebbe supportare `DescribeKey`, `Encrypt`, e. `Decrypt` operazioni.

Cloud Volumes ONTAP

1. Passa all'ambiente Cloud Volumes ONTAP.
2. Passare al livello di privilegio avanzato:
   `set -privilege advanced`
3. Abilitare il gestore delle chiavi AWS:
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando richiesto, inserire la chiave segreta.
5. Verificare che AWS KMS sia stato configurato correttamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Gestisci le chiavi con Azure Key Vault

È possibile utilizzare "Azure Key Vault (AKV)" Per proteggere le chiavi di crittografia ONTAP in un'applicazione implementata da Azure.

AKV può essere utilizzato per proteggere "Chiavi NetApp Volume Encryption (NVE)" Solo per SVM di dati.

La gestione delle chiavi con AKV può essere abilitata con la CLI o l'API REST ONTAP.

Quando si utilizza AKV, tenere presente che per impostazione predefinita viene utilizzata una LIF SVM di dati per comunicare con l'endpoint di gestione delle chiavi cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.10.1 o successiva
- Licenza di crittografia dei volumi (VE) installata (la licenza di crittografia dei volumi NetApp viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp)
- È necessario disporre di una licenza per la gestione delle chiavi di crittografia multi-tenant (MT_EK_MGMT)
- Devi essere un amministratore del cluster o di SVM
- Un abbonamento Active Azure

Limitazioni

- AKV può essere configurato solo su una SVM dati
- NAE non può essere usato con AKV. NAE richiede un server KMIP supportato dall'esterno.

Processo di configurazione

I passaggi descritti spiegano come registrare la configurazione di Cloud Volumes ONTAP con Azure e come creare un archivio chiavi Azure. Se la procedura è già stata completata, assicurarsi di disporre delle impostazioni di configurazione corrette, in particolare nella sezione Creare un vault Azure Key, quindi passare a. Configurazione di Cloud Volumes ONTAP.

- Registrazione dell'applicazione Azure
- Creare un segreto per il client Azure
- Creare un vault Azure Key
- Creare una chiave di crittografia
- Creazione di un endpoint Azure Active Directory (solo ha)
- Configurazione di Cloud Volumes ONTAP

Registrazione dell'applicazione Azure

1. È necessario prima registrare l'applicazione nell'abbonamento Azure che si desidera utilizzare per accedere al vault delle chiavi Cloud Volumes ONTAP. All'interno del portale Azure, selezionare **registrazioni app**.
2. Selezionare **Nuova registrazione**.
3. Fornire un nome per l'applicazione e selezionare un tipo di applicazione supportato. Il tenant singolo predefinito è sufficiente per l'utilizzo di Azure Key Vault. Selezionare **Registra**.
4. Nella finestra Panoramica di Azure, selezionare l'applicazione registrata. Copiare l'ID **applicazione (client)** e l'ID **directory (tenant)** in una posizione sicura. Saranno richiesti più avanti nel processo di registrazione.

Creare un segreto per il client Azure

1. Nel portale Azure per la registrazione dell'applicazione Azure Key Vault, seleziona il pannello **certificati e segreti**.
2. Selezionare **nuovo segreto client**. Immettere un nome significativo per il client secret. NetApp consiglia un periodo di scadenza di 24 mesi; tuttavia, le policy di governance del cloud specifiche potrebbero richiedere un'impostazione diversa.
3. Fare clic su **Aggiungi** per creare il segreto del client. Copiare la stringa segreta elencata nella colonna **valore** e memorizzarla in una posizione sicura per utilizzarla successivamente in Configurazione di Cloud Volumes ONTAP. Il valore segreto non viene visualizzato di nuovo dopo aver allontanato la pagina.

Creare un vault Azure Key

1. Se si dispone già di un vault delle chiavi Azure, è possibile collegarlo alla configurazione di Cloud Volumes ONTAP; tuttavia, è necessario adattare i criteri di accesso alle impostazioni in questo processo.
2. Nel portale Azure, accedere alla sezione **Vaults chiave**.
3. Fare clic su **+Crea** e inserire le informazioni richieste, tra cui gruppo di risorse, regione e livello di prezzo. Inoltre, immettere il numero di giorni per conservare i vault cancellati e selezionare **Enable purge Protection** (attiva protezione di eliminazione) nel vault delle chiavi.
4. Selezionare **Avanti** per scegliere una policy di accesso.
5. Selezionare le seguenti opzioni:
   a. In **Configurazione Access**, selezionare **criterio di accesso al vault**.
   b. In **accesso alle risorse**, selezionare **crittografia disco Azure per la crittografia del volume**.
6. Selezionare **+Crea** per aggiungere una policy di accesso.
7. In **Configura da un modello**, fare clic sul menu a discesa, quindi selezionare il modello **Gestione chiavi, segreti e certificati**.
8. Scegliere ciascuno dei menu a discesa delle autorizzazioni (chiave, segreto, certificato), quindi **Seleziona tutto** nella parte superiore dell'elenco dei menu per selezionare tutte le autorizzazioni disponibili. Dovresti avere:

- **Permessi chiave**: 20 selezionato
- **Permessi segreti**: 8 selezionati
- **Permessi del certificato**: 16 selezionato

Create an access policy

1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Cryptographic Operations

- [x] Select all
- [x] Decrypt
- [x] Encrypt
- [x] Unwrap Key
- [x] Wrap Key
- [x] Verify
- [x] Sign

Privileged Key Operations

- [x] Select all
- [x] Purge
- [x] Release

Rotation Policy Operations

- [x] Select all
- [x] Rotate
- [x] Get Rotation Policy
- [x] Set Rotation Policy

Secret permissions

Secret Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Set
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Privileged Secret Operations

- [x] Select all
- [x] Purge

Certificate permissions

Certificate Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore
- [x] Manage Contacts
- [x] Manage Certificate Authorities
- [x] Get Certificate Authorities
- [x] List Certificate Authorities
- [x] Set Certificate Authorities
- [x] Delete Certificate Authorities

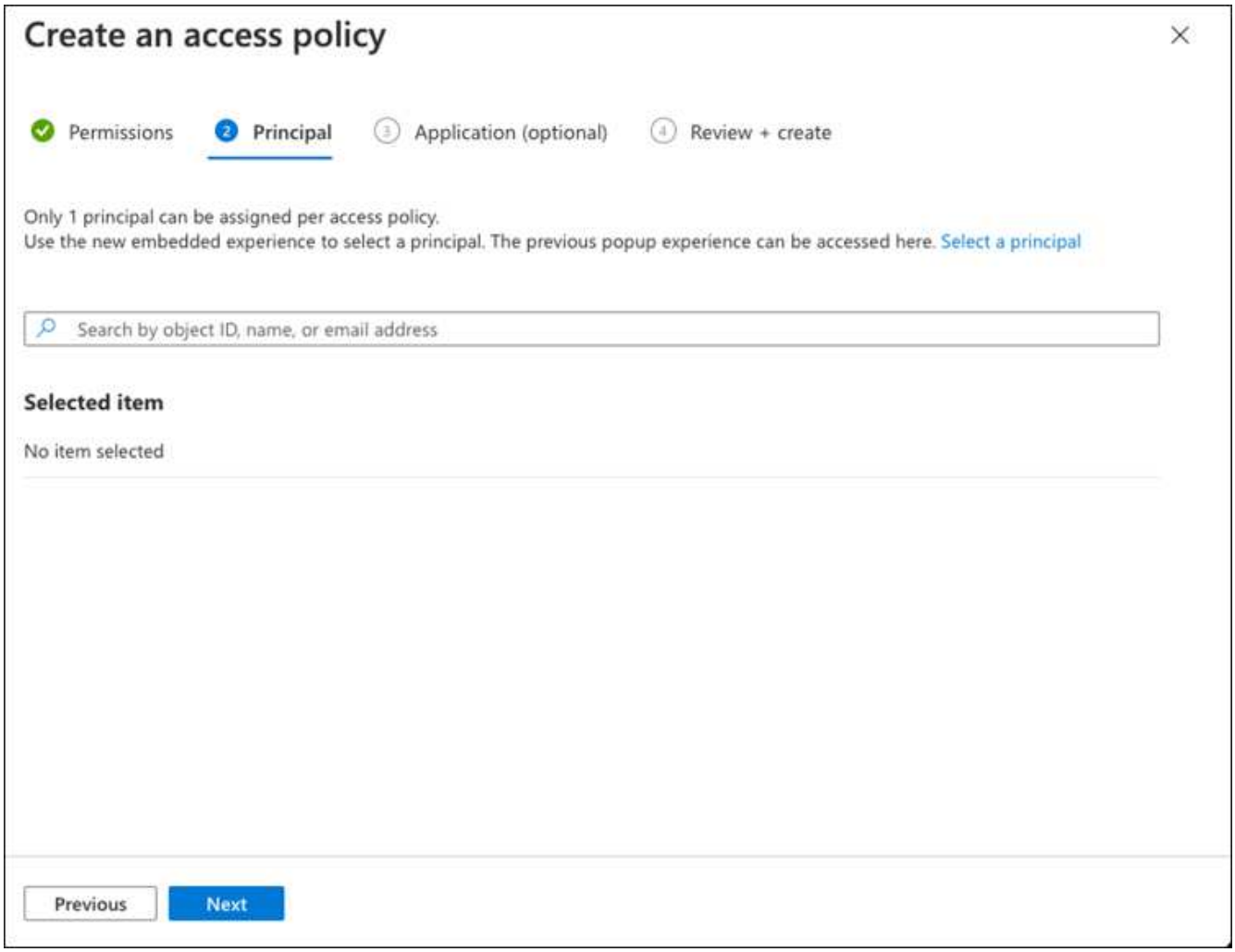
Privileged Certificate Operations

- [x] Select all
- [x] Purge

Previous Next

9. Fare clic su **Avanti** per selezionare l'applicazione registrata **Principal** Azure in cui è stata creata Registrazione dell'applicazione Azure. Selezionare **Avanti**.

È possibile assegnare un solo principal per policy.



10. Fare clic su **Avanti** due volte fino a visualizzare **Rivedi e crea**. Quindi, fare clic su **Crea**.
11. Selezionare **Avanti** per passare alle opzioni **rete**.
12. Scegliere il metodo di accesso alla rete appropriato o selezionare **tutte le reti** e **Rivedi + Crea** per creare il vault delle chiavi. (Il metodo di accesso alla rete può essere prescritto da una policy di governance o dal tuo team di sicurezza del cloud aziendale).
13. Registrare l'URI del vault delle chiavi: Nel vault delle chiavi creato, accedere al menu Overview (Panoramica) e copiare l'URI del vault** dalla colonna di destra. Questo è necessario per un passaggio successivo.

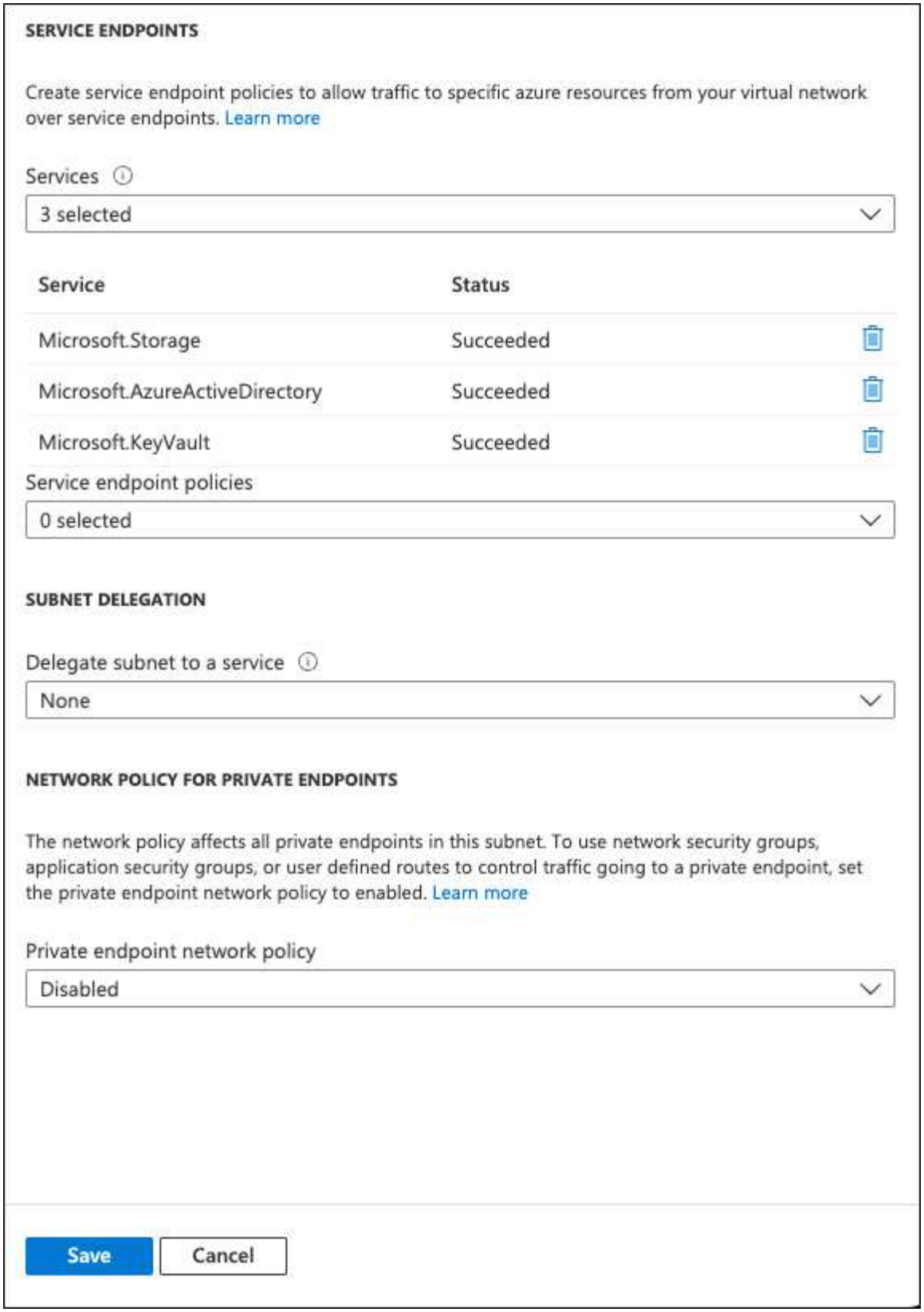
Creare una chiave di crittografia

1. Nel menu del vault delle chiavi creato per Cloud Volumes ONTAP, selezionare l'opzione **chiavi**.
2. Selezionare **genera/importa** per creare una nuova chiave.
3. Lasciare l'opzione predefinita impostata su **genera**.
4. Fornire le seguenti informazioni:

    - Nome della chiave di crittografia
    - Tipo di chiave: RSA
    - Dimensione chiave RSA: 2048
    - Abilitato: Sì
5. Selezionare **Crea** per creare la chiave di crittografia.
6. Tornare al menu **tasti** e selezionare la chiave appena creata.
7. Selezionare l'ID della chiave in **versione corrente** per visualizzare le proprietà della chiave.
8. Individuare il campo **Key Identifier**. Copiare l'URI fino alla stringa esadecimale, ma non inclusa.

Creazione di un endpoint Azure Active Directory (solo ha)

1. Questo processo è necessario solo se si configura Azure Key Vault per un ambiente di lavoro ha Cloud Volumes ONTAP.
2. Nel portale Azure, accedere a **reti virtuali**.
3. Selezionare la rete virtuale in cui è stato implementato l'ambiente di lavoro Cloud Volumes ONTAP e selezionare il menu **subnet** sul lato sinistro della pagina.
4. Selezionare dall'elenco il nome della subnet per la distribuzione Cloud Volumes ONTAP.
5. Passare all'intestazione **endpoint del servizio**. Nel menu a discesa, selezionare:
    - **Microsoft.AzureActiveDirectory**
    - **Microsoft.KeyVault**
    - **Microsoft.Storage** (opzionale)



6. Selezionare **Salva** per acquisire le impostazioni.

Configurazione di Cloud Volumes ONTAP

1. Connettersi alla LIF di gestione del cluster con il client SSH preferito.
2. Accedere alla modalità avanzata dei privilegi in ONTAP:

```
set advanced -con off
```

3. Identificare i dati SVM desiderati e verificarne la configurazione DNS:
   `vserver services name-service dns show`
   a. Se esiste una voce DNS per i dati SVM desiderati e contiene una voce per il DNS di Azure, non è richiesta alcuna azione. In caso contrario, aggiungere una voce del server DNS per la SVM dei dati che punta al DNS Azure, al DNS privato o al server on-premise. Questo deve corrispondere alla voce per l'amministratore del cluster SVM:
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`
   b. Verificare che il servizio DNS sia stato creato per i dati SVM:
      `vserver services name-service dns show`
4. Abilitare Azure Key Vault utilizzando l'ID client e l'ID tenant salvati dopo la registrazione dell'applicazione:
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > Il `_full_key_URI` il valore deve utilizzare `<https:// <key vault host name>/keys/<key label>` formato.

5. Dopo aver attivato con successo il vault delle chiavi di Azure, immettere il `client secret value` quando richiesto.
6. Controllare lo stato del gestore delle chiavi:
   `security key-manager external azure check`L'output sarà simile a:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Se il `service_reachability` lo stato non è `OK`, SVM non può raggiungere il servizio Azure Key Vault con tutte le autorizzazioni e la connettività richieste. Assicurati che le policy di rete e il routing di Azure non blocchino il tuo VNET privato dal raggiungere l'endpoint pubblico di Azure KeyVault. In caso affermativo, prendere in considerazione l'utilizzo di un endpoint Azure Private per accedere al vault delle chiavi

dall'interno di VNET. Per risolvere l'indirizzo IP privato dell'endpoint, potrebbe essere necessario aggiungere una voce di host statici sulla SVM.

Il `kms_wrapped_key_status` verrà segnalato `UNKNOWN` alla configurazione iniziale. Il suo stato cambierà in `OK` dopo la crittografia del primo volume.

7. FACOLTATIVO: Creare un volume di test per verificare la funzionalità di NVE.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   Se configurato correttamente, Cloud Volumes ONTAP crea automaticamente il volume e attiva la crittografia del volume.

8. Verificare che il volume sia stato creato e crittografato correttamente. In tal caso, il `-is-encrypted` il parametro viene visualizzato come `true`.
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```

Gestisci le chiavi con il Cloud Key Management Service di Google

È possibile utilizzare "Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)" Per proteggere le chiavi di crittografia ONTAP in un'applicazione implementata dalla piattaforma cloud Google.

La gestione delle chiavi con Cloud KMS può essere abilitata con la CLI o l'API REST di ONTAP.

Quando si utilizza Cloud KMS, tenere presente che per impostazione predefinita viene utilizzata la LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi del cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (oauth2.googleapis.com). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.10.1 o successiva
- Licenza VE (Volume Encryption) installata
- Licenza di gestione delle chiavi di crittografia multi-tenant (MTEKM) installata, a partire da Cloud Volumes ONTAP 9.12.1 GA.
- Devi essere un amministratore del cluster o di SVM
- Un abbonamento attivo a Google Cloud Platform

Limitazioni

- Cloud KMS può essere configurato solo su una SVM dati

Configurazione

Google Cloud

1. Nel tuo ambiente Google Cloud, "Creare un anello e una chiave GCP simmetrici".
2. Creare un ruolo personalizzato per l'account del servizio Cloud Volumes ONTAP.

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. Assegnare il ruolo personalizzato alla chiave KMS cloud e all'account del servizio Cloud Volumes ONTAP:
   `gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`
4. Scarica la chiave JSON dell'account di servizio:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Connettersi alla LIF di gestione del cluster con il client SSH preferito.
2. Passare al livello di privilegio avanzato:
   `set -privilege advanced`
3. Creare un DNS per i dati SVM.
   `dns create -domains c.`*`<project>`*`.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
4. Crea voce CMEK:
   `security key-manager external gcp enable -vserver` *`SVM_name`* `-project-id` *`project`* `-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
5. Quando richiesto, inserire la chiave JSON dell'account di servizio dal proprio account GCP.
6. Confermare che il processo di abilitazione è riuscito:
   `security key-manager external gcp check -vserver` *`svm_name`*
7. FACOLTATIVO: Creare un volume per verificare la crittografia `vol create` *`volume_name`* `-aggregate` *`aggregate`* `-vserver` *`vserver_name`* `-size 10G`

Risolvere i problemi

Se è necessario risolvere il problema, è possibile eseguire il tail dei log REST API raw nei due passaggi precedenti:

1. `set d`
2. `systemshell -node` *`node`* `-command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Miglioramento della protezione contro ransomware

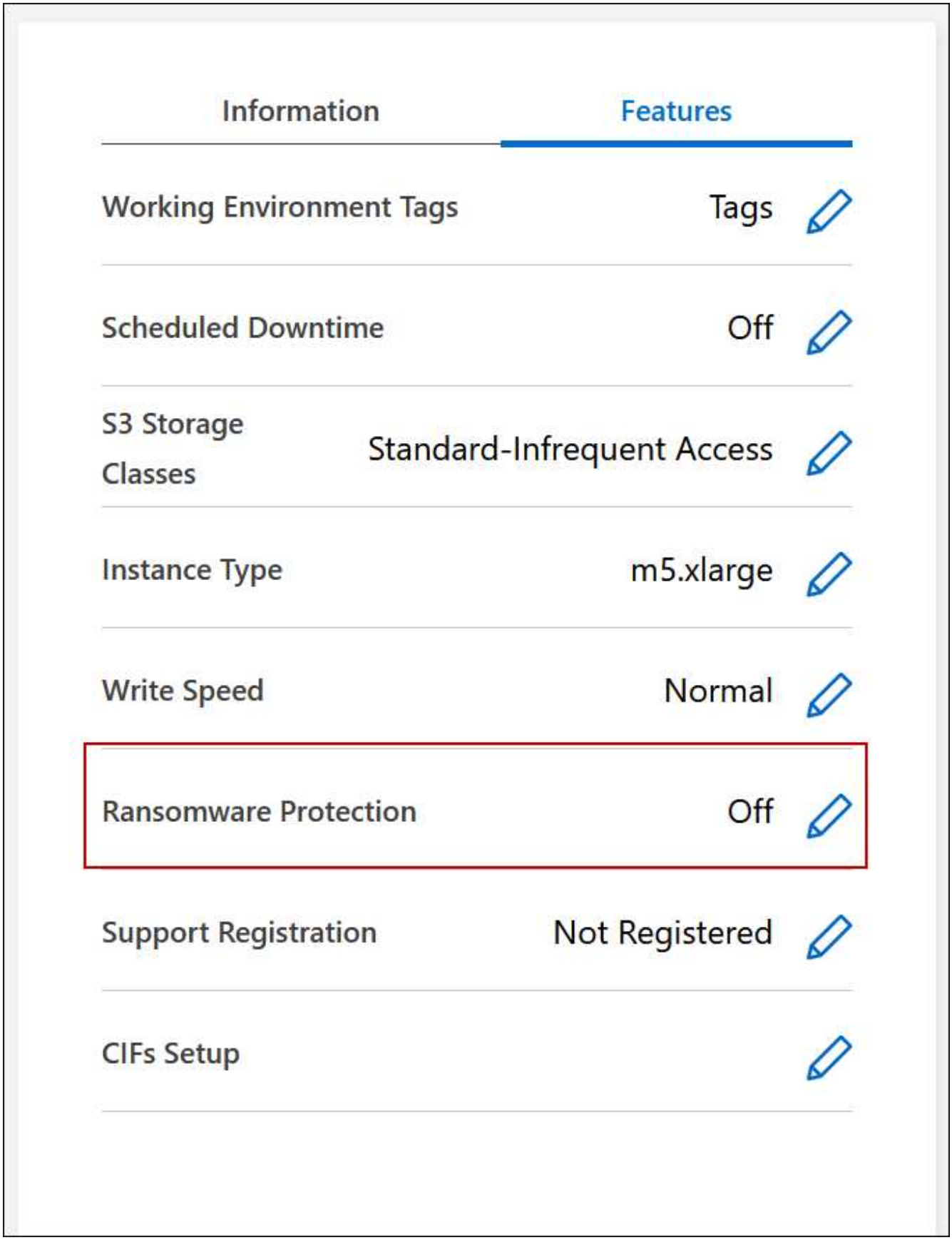
Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. BlueXP ti permette di implementare due soluzioni NetApp per il ransomware: Protezione dalle comuni estensioni di file ransomware e protezione autonoma dal ransomware (ARP). Queste soluzioni forniscono strumenti efficaci per visibilità, rilevamento e correzione.

Protezione dalle comuni estensioni di file ransomware

Disponibile tramite BlueXP, l'impostazione di protezione ransomware consente di utilizzare la funzionalità FPolicy di ONTAP per proteggersi dai comuni tipi di estensione di file ransomware.

Fasi

1. Nella pagina Canvas, fare doppio clic sul nome del sistema configurato per la protezione ransomware.
2. Nella scheda Overview (Panoramica), fare clic sul pannello Features (funzionalità), quindi sull'icona a forma di matita accanto a **ransomware Protection**.



3. 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.

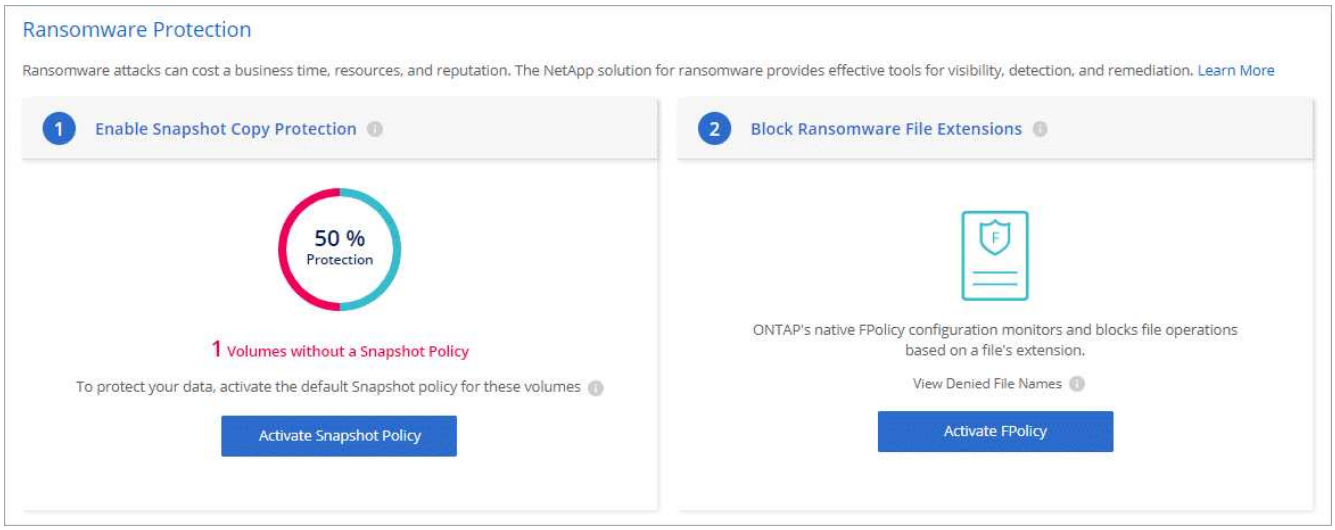
b. Fare clic su **Activate FPolicy** (attiva FPolicy) per attivare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione di un file.

   Questa soluzione preventiva migliora la protezione dagli attacchi ransomware bloccando i tipi di file ransomware più comuni.

   L'ambito FPolicy predefinito blocca i file con le seguenti estensioni:

   micro, crittografato, bloccato, criptato, criptato, Crinf, r5a, XRNT, XTBL, R16M01D05, PzDC, Good, LOL!, OMG!, RDM, RRK, encodedRS, crjoker, encifered, LeChiffre

   BlueXP crea questo ambito quando si attiva FPolicy su Cloud Volumes ONTAP. L'elenco si basa su tipi di file ransomware comuni. È possibile personalizzare le estensioni dei file bloccati utilizzando i comandi *vserver fpolicy scope* della CLI di Cloud Volumes ONTAP.



Protezione ransomware autonoma

Cloud Volumes ONTAP supporta la funzionalità di protezione ransomware autonoma (ARP), che esegue analisi sui carichi di lavoro per rilevare e avvisare in modo proattivo in caso di attività anomale che potrebbero indicare un attacco ransomware.

Separare dalle protezioni di estensione file fornite attraverso "impostazione di protezione dal ransomware", La funzione ARP utilizza l'analisi del carico di lavoro per avvisare l'utente in caso di potenziali attacchi in base a "attività anomala" rilevata. Sia l'impostazione di protezione dal ransomware che la funzione ARP possono essere utilizzate insieme per una protezione completa dal ransomware.

La funzione ARP è disponibile solo con le licenze BYOL (da 1 a 36 mesi) sia sui modelli di licenza basati sulla capacità che su nodi. Per acquistare una nuova licenza aggiuntiva separata da utilizzare con la funzionalità ARP di Cloud Volumes ONTAP, è necessario contattare il rappresentante commerciale NetApp.

La licenza ARP è considerata una licenza "mobile", il che significa che non è legata a una singola istanza Cloud Volumes ONTAP e può essere applicata a più ambienti Cloud Volumes ONTAP.

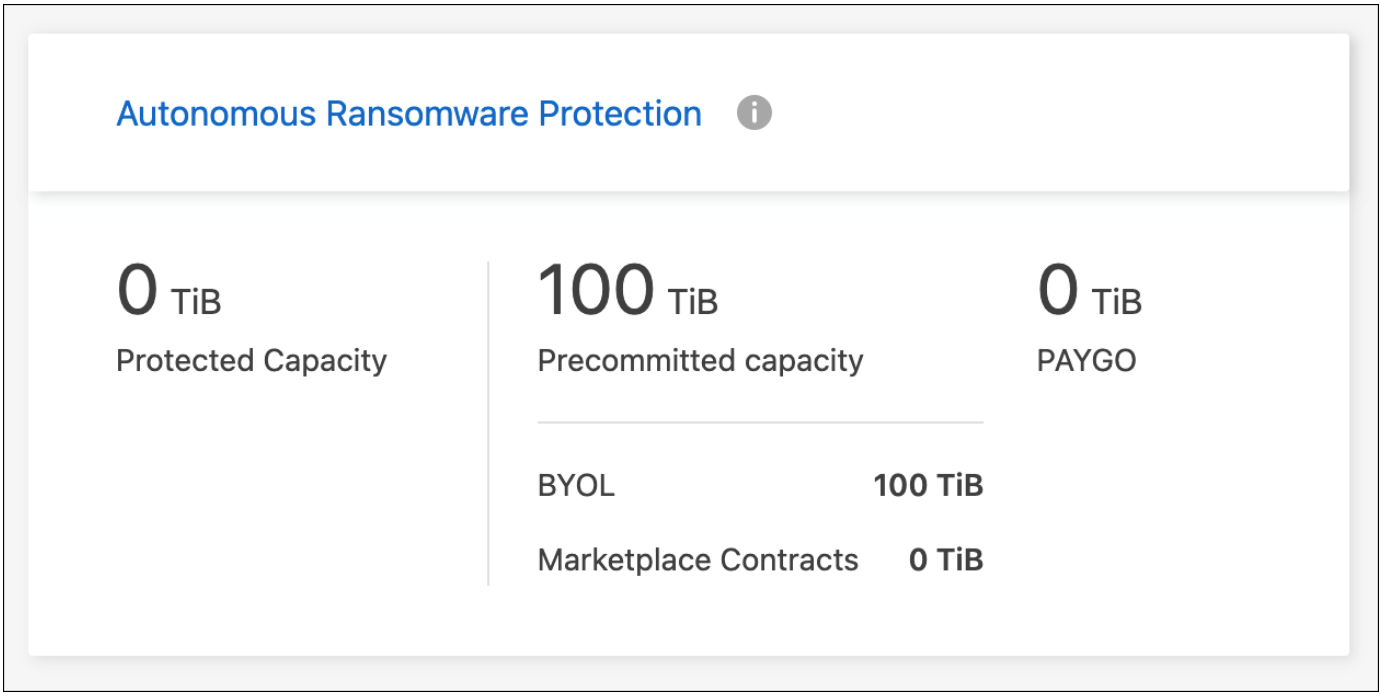
> L'utilizzo della funzione ARP con le licenze Cloud Volumes ONTAP basate su nodi non è attualmente presente nel Digital Wallet. La possibilità di visualizzare l'utilizzo dell'ARP basato su nodi sarà disponibile in Digital Wallet in una versione futura.

Acquistando una licenza add-on e aggiungendola al portafoglio digitale, puoi abilitare ARP per volume con Cloud Volumes ONTAP. La ricarica per ARP viene misurata a un livello di volume, in base alla capacità totale dei volumi con la funzione ARP abilitata. La capacità minima di licenza è di 1TB TB. Tuttavia, non è prevista una ricarica della capacità minima per la funzione ARP.

I volumi abilitati per ARP hanno lo stato designato "modalità di apprendimento" o "attivo". Qualsiasi volume con stato ARP "Disabilitato" è escluso dalla ricarica. Ad esempio, un ambiente Cloud Volumes ONTAP con 30 TiB di capacità sottoposta a provisioning può scegliere di avere solo un sottoinsieme di volumi TIB 15 con ARP attivato.

La configurazione di ARP per i volumi viene eseguita tramite Gestore di sistema di ONTAP e CLI di ONTAP.

Per ulteriori informazioni su come attivare ARP con Gestione di sistema e CLI di ONTAP, vedere "Attiva la protezione ransomware autonoma".



> Il supporto non è disponibile per l'uso di funzioni con licenza senza licenza.

Amministrazione del sistema

Aggiornare il software Cloud Volumes ONTAP

Aggiorna Cloud Volumes ONTAP da BlueXP per accedere alle nuove funzionalità e ai miglioramenti più recenti. Preparare i sistemi Cloud Volumes ONTAP prima di aggiornare il software.

Panoramica sull'aggiornamento

Prima di avviare il processo di aggiornamento di Cloud Volumes ONTAP, tenere presente quanto segue.

Aggiornamento solo da BlueXP

Gli aggiornamenti di Cloud Volumes ONTAP devono essere completati da BlueXP. Non aggiornare Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI. In questo modo si può influire sulla stabilità del sistema.

Come eseguire l'upgrade

BlueXP offre due modi per aggiornare Cloud Volumes ONTAP:

- Seguendo le notifiche di aggiornamento visualizzate nell'ambiente di lavoro
- Posizionando l'immagine di aggiornamento in una posizione HTTPS e fornendo a BlueXP l'URL

Percorsi di upgrade supportati

La versione di Cloud Volumes ONTAP a cui è possibile eseguire l'aggiornamento dipende dalla versione di Cloud Volumes ONTAP attualmente in esecuzione.

Versione corrente	Versioni a cui è possibile eseguire direttamente l'aggiornamento
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7

Versione corrente	Versioni a cui è possibile eseguire direttamente l'aggiornamento
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Tenere presente quanto segue:

- I percorsi di aggiornamento supportati per Cloud Volumes ONTAP sono diversi da quelli per un cluster ONTAP on-premise.
- Se si esegue l'aggiornamento seguendo le notifiche di aggiornamento visualizzate in un ambiente di lavoro, BlueXP richiederà di eseguire l'aggiornamento a una release che segue questi percorsi di aggiornamento supportati.
- Se si esegue l'aggiornamento posizionando un'immagine di aggiornamento in una posizione HTTPS, assicurarsi di seguire questi percorsi di aggiornamento supportati.
- In alcuni casi, potrebbe essere necessario eseguire l'aggiornamento alcune volte per raggiungere la release di destinazione.

  Ad esempio, se si utilizza la versione 9.8 e si desidera eseguire l'aggiornamento alla versione 9.10.1, è necessario prima eseguire l'aggiornamento alla versione 9.9.1 e poi alla versione 9.10.1.

Rilascio delle patch

A partire da gennaio 2024, gli aggiornamenti delle patch sono disponibili in BlueXP solo se rappresentano una release di patch per le tre ultime versioni di Cloud Volumes ONTAP. Utilizziamo l'ultima release di GA per determinare le tre versioni più recenti da visualizzare in BlueXP. Ad esempio, se la release corrente di GA è 9.13.1, le patch per 9.11.1-9.13.1 vengono visualizzate in BlueXP. Se si desidera eseguire l'aggiornamento a una versione di patch per le versioni 9.11.1 o precedenti, sarà necessario utilizzare la procedura di aggiornamento manuale Download dell'immagine ONTAP in corso.

Come regola generale per le release di patch (P), è possibile eseguire l'aggiornamento da una versione a qualsiasi versione P-release della versione corrente in esecuzione o della versione successiva.

Ecco alcuni esempi:

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

Ripristino o downgrade

Il ripristino o il downgrade di Cloud Volumes ONTAP a una release precedente non è supportato.

Registrazione del supporto

Cloud Volumes ONTAP deve essere registrato presso il supporto NetApp per poter aggiornare il software utilizzando uno dei metodi descritti in questa pagina. Ciò vale sia PER PAYGO che per BYOL. È necessario "Registrare manualmente i sistemi PAYGO", Mentre i sistemi BYOL sono registrati per impostazione predefinita.

> Un sistema che non è registrato per il supporto riceverà comunque le notifiche di aggiornamento software che vengono visualizzate in BlueXP quando è disponibile una nuova versione. Tuttavia, è necessario registrare il sistema prima di poter aggiornare il software.

Aggiornamenti del mediatore ha

BlueXP aggiorna inoltre l'istanza del mediatore secondo necessità durante il processo di aggiornamento di Cloud Volumes ONTAP.

Upgrade in AWS con tipi di istanze C4, M4 e R4 EC2

Cloud Volumes ONTAP non supporta più i tipi di istanze C4, M4 e R4 EC2. Con questi tipi di istanza è possibile aggiornare le distribuzioni esistenti a Cloud Volumes ONTAP versioni 9,8-9.12.1. Prima di eseguire l'aggiornamento, si consiglia di farlo modificare il tipo di istanza. Se non è possibile modificare il tipo di istanza, è necessario abilita il networking avanzato prima di eseguire l'aggiornamento. Per ulteriori informazioni sulla modifica del tipo di istanza e sull'attivazione di una rete avanzata, consultare le sezioni seguenti.

In Cloud Volumes ONTAP con versioni 9.13.0 e successive, non è possibile eseguire l'aggiornamento con i tipi di istanza C4, M4 e R4 EC2. In questo caso, è necessario ridurre il numero di dischi e. modificare il tipo di istanza In alternativa, puoi implementare una nuova configurazione ha-Pair con i tipi di istanza C5, M5 e R5 EC2 e migrare i dati.

Modificare il tipo di istanza

I tipi di istanze C4, M4 e R4 EC2 consentono un maggior numero di dischi per nodo rispetto ai tipi di istanze C5, M5 e R5 EC2. Se il numero di dischi per nodo per l'istanza C4, M4 o R4 EC2 che si sta eseguendo è inferiore al limite massimo di dischi per nodo per le istanze C5, M5 e R5, è possibile modificare il tipo di istanza EC2 in C5, M5 o R5.

"Verifica dei limiti di dischi e tiering in base all'istanza EC2"
"Modificare il tipo di istanza EC2 per Cloud Volumes ONTAP"

Se non è possibile modificare il tipo di istanza, attenersi alla procedura descritta in Abilita il networking avanzato.

Abilita il networking avanzato

Per eseguire l'aggiornamento alle versioni 9,8 e successive di Cloud Volumes ONTAP, è necessario attivare *Enhanced Networking* nel cluster che esegue il tipo di istanza C4, M4 o R4. Per abilitare ENA, fare riferimento all'articolo della Knowledge base "Come abilitare funzionalità di rete avanzate come SR-IOV o ENA sulle istanze di AWS Cloud Volumes ONTAP".

Preparatevi all'aggiornamento

Prima di eseguire un aggiornamento, è necessario verificare che i sistemi siano pronti e apportare le modifiche necessarie alla configurazione.

- Pianificare il downtime
- Verificare che il giveback automatico sia ancora attivato
- Sospendere i trasferimenti SnapMirror
- Verificare che gli aggregati siano online
- Verifica che tutte le LIF siano sulle porte home

Pianificare il 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.

In molti casi, 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.

I protocolli orientati alla sessione potrebbero causare effetti negativi su client e applicazioni in determinate aree durante gli aggiornamenti. Per ulteriori informazioni, "Fare riferimento alla documentazione di ONTAP"

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"

Sospendere i 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.

> Anche se il backup e ripristino di BlueXP utilizza un'implementazione di SnapMirror per creare file di backup (chiamata SnapMirror Cloud), non è necessario sospendere i backup quando viene aggiornato un sistema.

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.

   È possibile accedere a System Manager puntando il browser Web all'indirizzo IP della LIF di gestione del cluster. L'indirizzo IP è disponibile nell'ambiente di lavoro Cloud Volumes ONTAP.

   > Il computer da cui si accede a BlueXP deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario effettuare l'accesso a BlueXP da un host jump presente nella rete del provider di servizi cloud.

2. Fare clic su **protezione > Relazioni**.
3. Selezionare la relazione e fare clic su **operazioni > Quiesce**.

Verificare che gli aggregati siano online

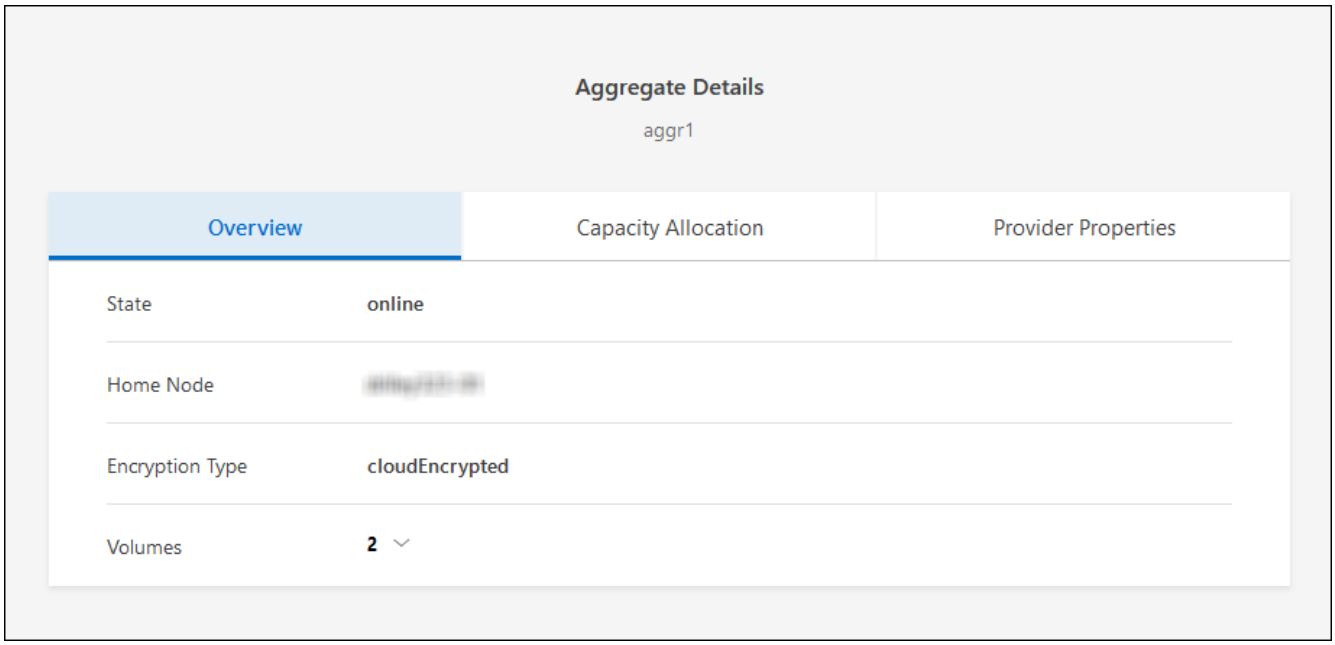
Gli aggregati per Cloud Volumes ONTAP devono essere online prima di aggiornare il software. Gli aggregati devono essere online nella maggior parte delle configurazioni, ma in caso contrario, è necessario portarli online.

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 sulla scheda **aggregati**.
2. Sotto il titolo dell'aggregato, fare clic sul pulsante ellisse, quindi selezionare **Visualizza dettagli dell'aggregato**.



3. Se l'aggregato non è in linea, utilizzare System Manager per portare l'aggregato online:
   a. Fare clic su **Storage > Aggregates & Disks > Aggregates**.
   b. Selezionare l'aggregato, quindi fare clic su **altre azioni > Stato > Online**.

Verifica che tutte le LIF siano sulle porte home

Prima di eseguire l'upgrade, tutte le LIF devono trovarsi sulle porte home. Fare riferimento alla documentazione di ONTAP a. "Verifica che tutte le LIF siano sulle porte home".

Se si verifica un errore di aggiornamento, fare riferimento alla "Articolo della Knowledge base "aggiornamento Cloud Volumes ONTAP non riuscito"".

Aggiornare Cloud Volumes ONTAP

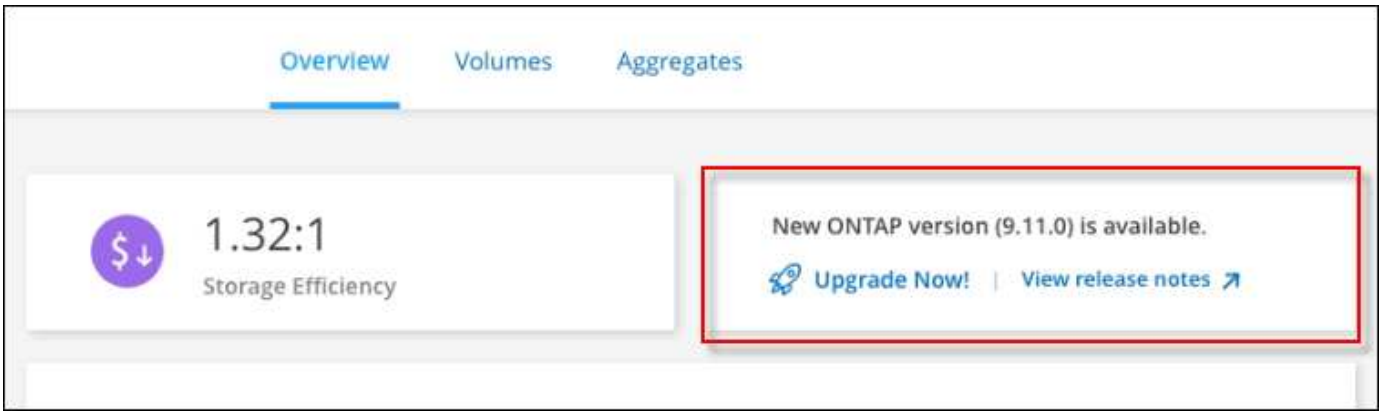
BlueXP informa l'utente quando è disponibile una nuova versione per l'aggiornamento. È possibile avviare il processo di aggiornamento da questa notifica. Per ulteriori informazioni, vedere Aggiornamento dalle notifiche BlueXP.

Un altro metodo per eseguire aggiornamenti software utilizzando un'immagine su un URL esterno. Questa opzione è utile se BlueXP non riesce ad accedere al bucket S3 per aggiornare il software o se è stata fornita

una patch. Per ulteriori informazioni, vedere Aggiornamento da un'immagine disponibile su un URL.

Aggiornamento dalle notifiche BlueXP

BlueXP 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.

Prima di iniziare

Le operazioni BlueXP, come la creazione di volumi o aggregati, non devono essere in corso sul sistema Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Selezionare un ambiente di lavoro.

   Se è disponibile una nuova versione, nella scheda Panoramica viene visualizzata una notifica:

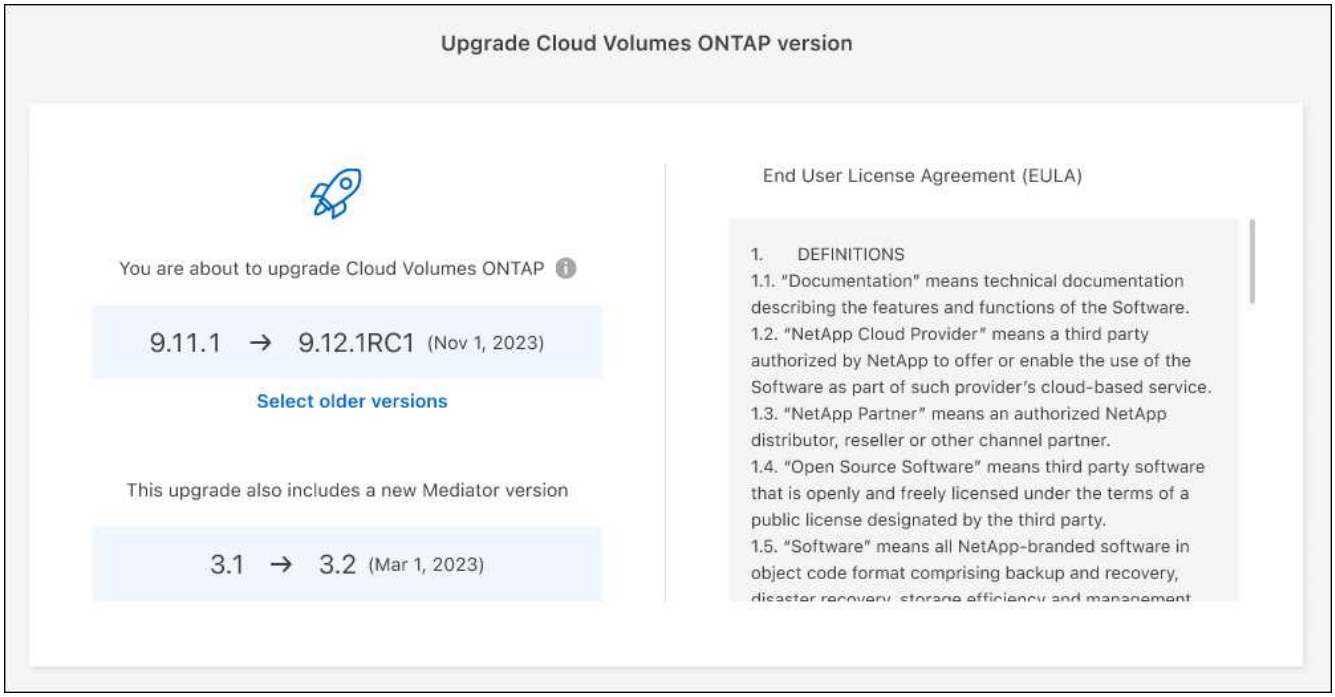
3. Se è disponibile una nuova versione, fare clic su **Aggiorna ora!**

   > Prima di poter aggiornare Cloud Volumes ONTAP tramite la notifica BlueXP, è necessario disporre di un account per il sito di supporto NetApp.

4. Nella pagina Upgrade Cloud Volumes ONTAP (Contratto di licenza con l'utente finale), leggere l'EULA, quindi selezionare **i Read and Approve the EULA** (Leggi e approva l'EULA).

5. Fare clic su **Upgrade** (Aggiorna).

> Per impostazione predefinita, la pagina Upgrade Cloud Volumes ONTAP (aggiornamento versione Cloud Volumes ONTAP) seleziona l'ultima versione disponibile per l'aggiornamento. Se disponibili, è possibile selezionare le versioni precedenti di Cloud Volumes ONTAP per l'aggiornamento facendo clic su **Seleziona versioni precedenti**. Fare riferimento a. "Elenco dei percorsi di upgrade supportati" Per il percorso di aggiornamento appropriato in base alla versione corrente di Cloud Volumes ONTAP.



6. Per verificare lo stato dell'aggiornamento, fare clic sull'icona Impostazioni e selezionare **Timeline**.

Risultato

BlueXP 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 da un'immagine disponibile su un URL

È possibile posizionare l'immagine del software Cloud Volumes ONTAP sul connettore o su un server HTTP e avviare l'aggiornamento del software da BlueXP. È possibile utilizzare questa opzione se BlueXP non riesce ad accedere al bucket S3 per aggiornare il software.

Prima di iniziare

- Le operazioni BlueXP, come la creazione di volumi o aggregati, non devono essere in corso sul sistema Cloud Volumes ONTAP.
- Se si utilizza HTTPS per ospitare immagini ONTAP, l'aggiornamento potrebbe non riuscire a causa di problemi di autenticazione SSL, causati dalla mancanza di certificati. La soluzione è generare e installare un certificato firmato dalla CA da utilizzare per l'autenticazione tra ONTAP e BlueXP.

  Consulta la Knowledge base di NetApp per visualizzare istruzioni dettagliate:

"KB di NetApp: Come configurare BlueXP come server HTTPS per ospitare le immagini di aggiornamento"

Fasi

1. Facoltativo: Configurare un server HTTP in grado di ospitare l'immagine del software Cloud Volumes ONTAP.

   Se si dispone di una connessione VPN alla rete virtuale, è possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP nella propria rete. In caso contrario, è necessario posizionare il file su un server HTTP nel cloud.

2. Se si utilizza il proprio gruppo di protezione per Cloud Volumes ONTAP, assicurarsi che le regole in uscita consentano connessioni HTTP 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 in uscita.

3. Ottenere l'immagine software da "Il sito di supporto NetApp".
4. Copiare l'immagine del software in una directory sul connettore o su un server HTTP da cui verrà fornito il file.

   Sono disponibili due percorsi. Il percorso corretto dipende dalla versione del connettore.

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`

5. Dall'ambiente di lavoro in BlueXP, fare clic sul pulsante **… (Icona ellisse)**, quindi fare clic su **Aggiorna Cloud Volumes ONTAP**.
6. Nella pagina Aggiorna versione Cloud Volumes ONTAP, immettere l'URL, quindi fare clic su **Cambia immagine**.

   Se l'immagine software è stata copiata nel connettore nel percorso indicato sopra, immettere il seguente URL:

   Http://<Connector-private-IP-address>/ontap/images/<image-file-name>

   Nell'URL, **nome-file-immagine** deve seguire il formato "cot.image.9.13.1P2.tgz".

7. Fare clic su **Procedi** per confermare.

Risultato

BlueXP 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.

Correggere gli errori di download quando si utilizza un gateway NAT Google Cloud

Il connettore scarica automaticamente gli aggiornamenti software per Cloud Volumes ONTAP. Il download potrebbe non riuscire se la configurazione utilizza un gateway Google Cloud NAT. È possibile correggere questo problema limitando il numero di parti in cui è divisa l'immagine software. Questa fase deve essere

completata utilizzando l'API BlueXP.

Fase

1. Inviare una richiesta PUT a /occm/config con il seguente JSON come corpo:

```
{
  "maxDownloadSessions": 32
}
```

Il valore per *maxDownloadSessions* può essere 1 o qualsiasi numero intero maggiore di 1. Se il valore è 1, l'immagine scaricata non verrà divisa.

Si noti che 32 è un valore di esempio. Il valore da utilizzare dipende dalla configurazione NAT e dal numero di sessioni che è possibile avere contemporaneamente.

"Scopri di più sulla chiamata API /occm/config".

Registrazione di sistemi pay-as-you-go

Il supporto di NetApp è incluso nei sistemi PAYGO di Cloud Volumes ONTAP, ma è necessario prima attivare il supporto registrando i sistemi con NetApp.

La registrazione di un sistema PAYGO con NetApp è necessaria per aggiornare il software ONTAP utilizzando uno qualsiasi dei metodi "descritto in questa pagina".

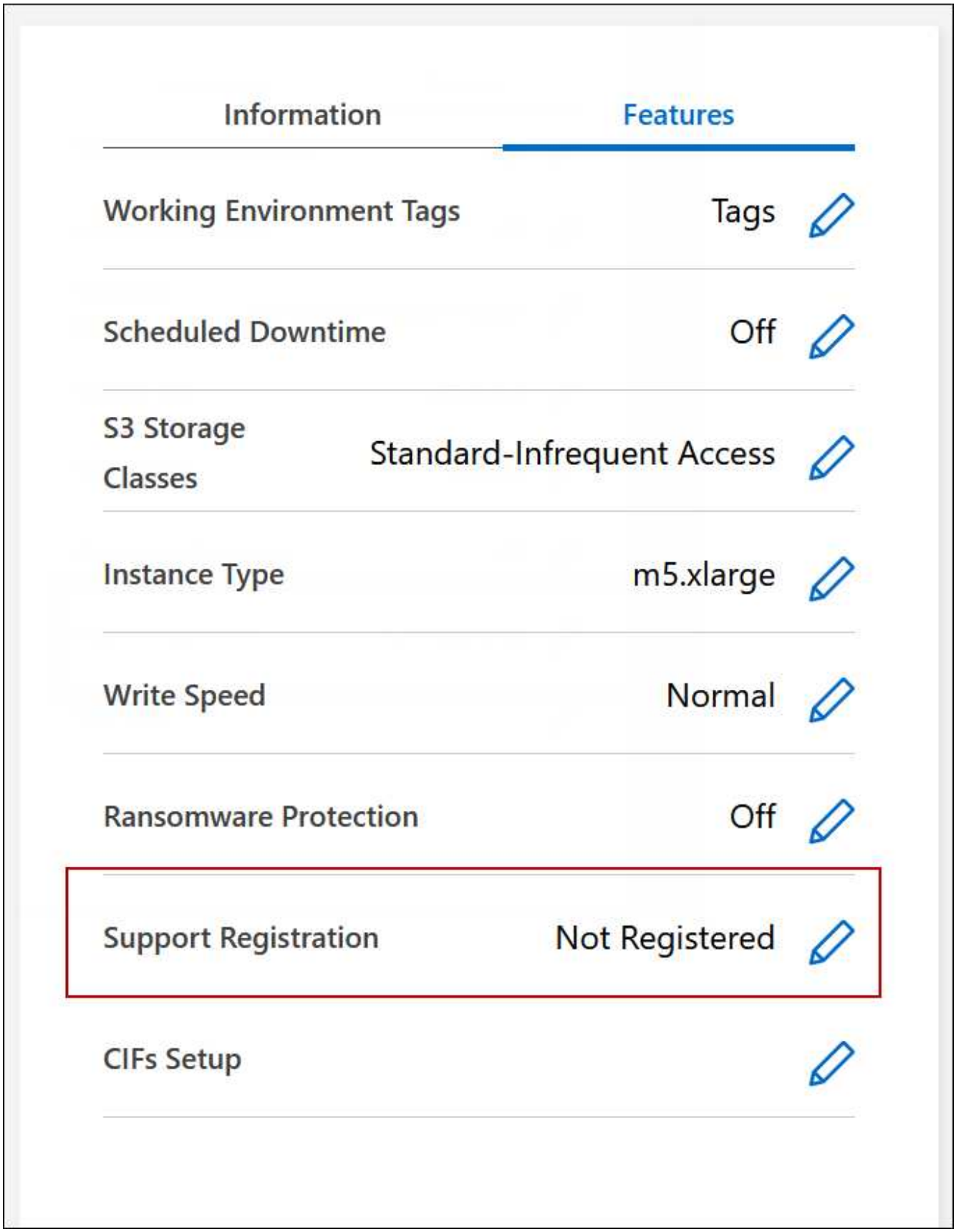
> Un sistema che non è registrato per il supporto riceverà comunque le notifiche di aggiornamento software che vengono visualizzate in BlueXP quando è disponibile una nuova versione. Tuttavia, è necessario registrare il sistema prima di poter aggiornare il software.

Fasi

1. Se non hai ancora aggiunto il tuo account NetApp Support Site a BlueXP, vai a **Impostazioni account** e aggiungilo ora.

   "Scopri come aggiungere account NetApp Support Site".

2. Nella pagina Canvas, fare doppio clic sul nome del sistema che si desidera registrare.
3. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi fare clic sull'icona a forma di matita accanto a **registrazione supporto**.



4. Selezionare un account NetApp Support Site e fare clic su **Register**.

Risultato

BlueXP registra il sistema con NetApp.

Gestione dello stato di Cloud Volumes ONTAP

Puoi arrestare e avviare Cloud Volumes ONTAP da BlueXP 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 BlueXP in modo che si spenga e riavvii automaticamente i sistemi in determinati momenti.

A proposito di questa attività

- Quando si pianifica un arresto automatico del sistema Cloud Volumes ONTAP, BlueXP posticipa l'arresto se è in corso un trasferimento di dati attivo.

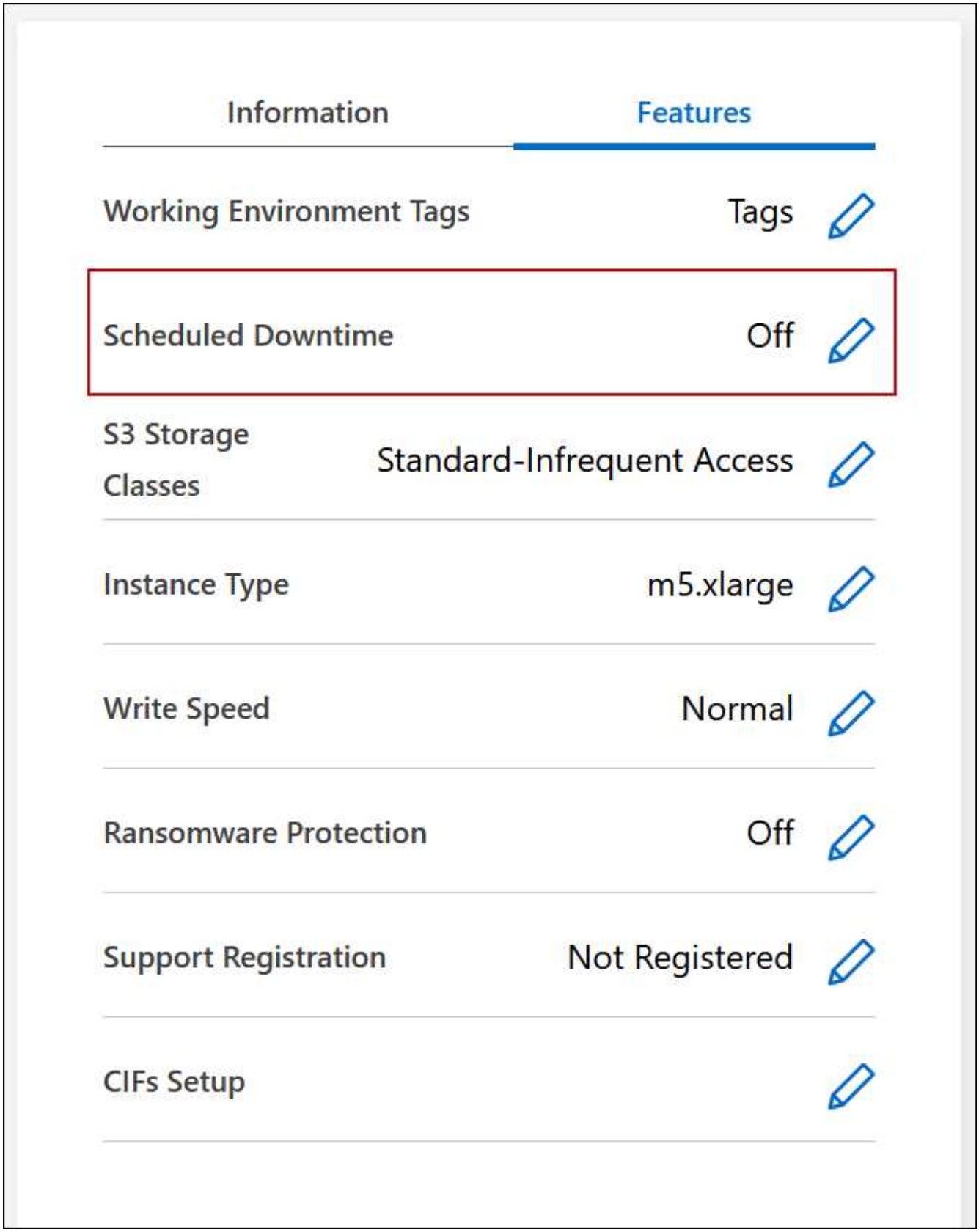
  BlueXP arresta il sistema al termine del trasferimento.

- Questa attività pianifica gli arresti automatici di entrambi i nodi in una coppia ha.
- Le snapshot dei dischi di boot e root non vengono create quando si disattiva Cloud Volumes ONTAP attraverso arresti pianificati.

  Le snapshot vengono create automaticamente solo quando si esegue un arresto manuale, come descritto nella sezione successiva.

Fasi

1. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro desiderato.
2. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi fare clic sull'icona a forma di matita accanto a **downtime pianificato**.



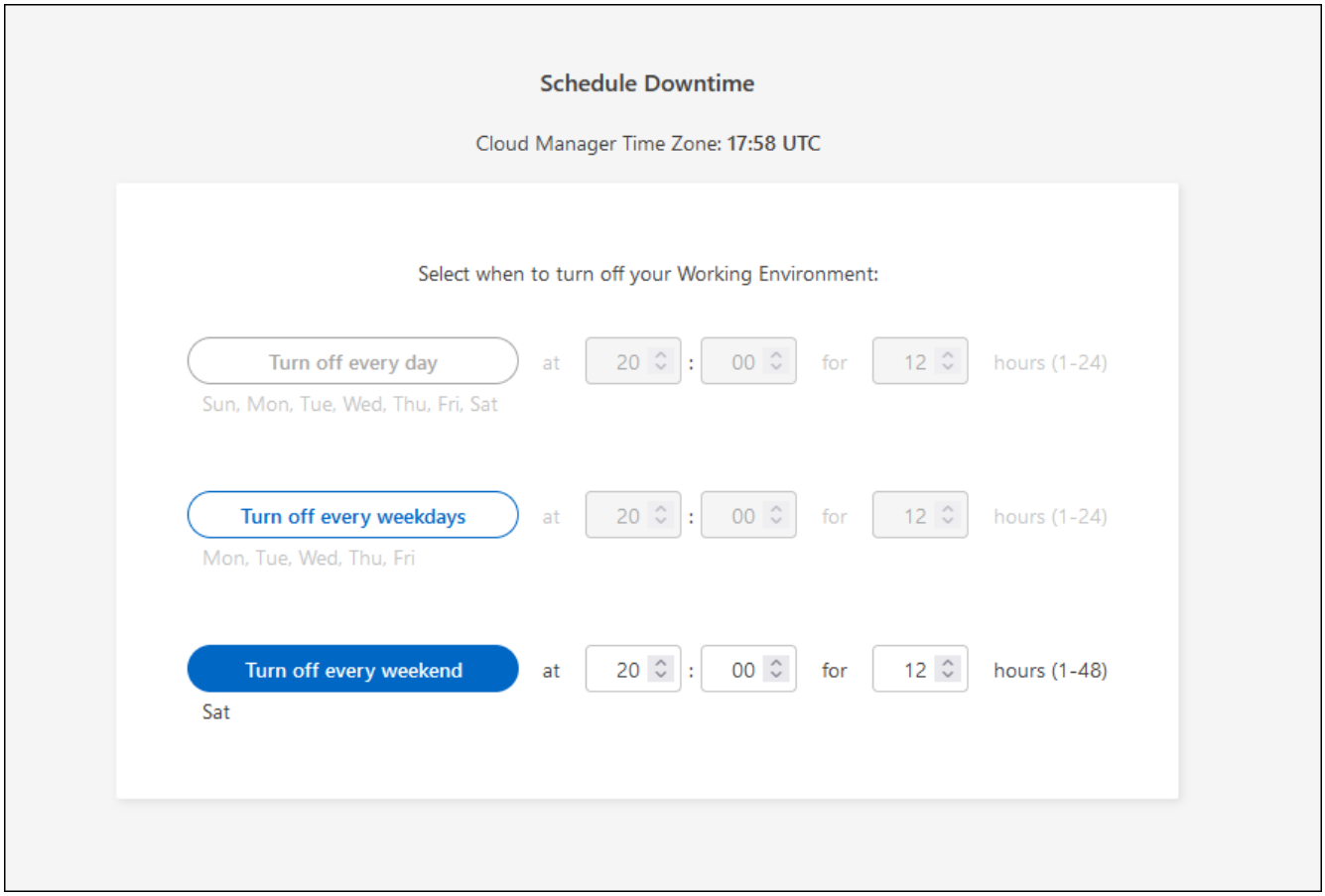
3. Specificare il programma di arresto:

   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 una pianificazione che indica a BlueXP di spegnere il sistema ogni sabato alle 20:00 (20:00) per 12 ore. BlueXP riavvia il sistema ogni lunedì alle 12:00



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

Risultato

BlueXP salva la pianificazione. La voce corrispondente del downtime pianificato sotto il pannello funzioni visualizza "on".

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.

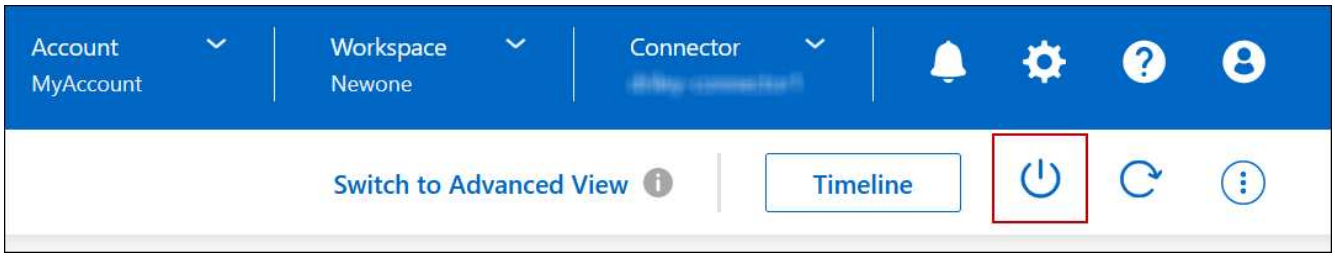
> Per ridurre i costi, BlueXP elimina periodicamente le vecchie snapshot dei dischi root e di boot. Vengono conservati solo i due snapshot più recenti per i dischi root e di boot.

A proposito di questa attività

Quando si interrompe una coppia ha, BlueXP 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.

   Le snapshot vengono create automaticamente al riavvio.

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.

Specificare un server NTP utilizzando "API BlueXP" o dall'interfaccia utente quando si "Creare un server CIFS".

Modificare la velocità di scrittura del sistema

BlueXP consente di scegliere una velocità di scrittura normale o elevata per Cloud Volumes ONTAP. 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.

L'elevata velocità di scrittura è supportata con tutti i tipi di sistemi a nodo singolo e alcune configurazioni di coppia ha. Visualizzare le configurazioni supportate in "Note di rilascio di Cloud Volumes ONTAP"

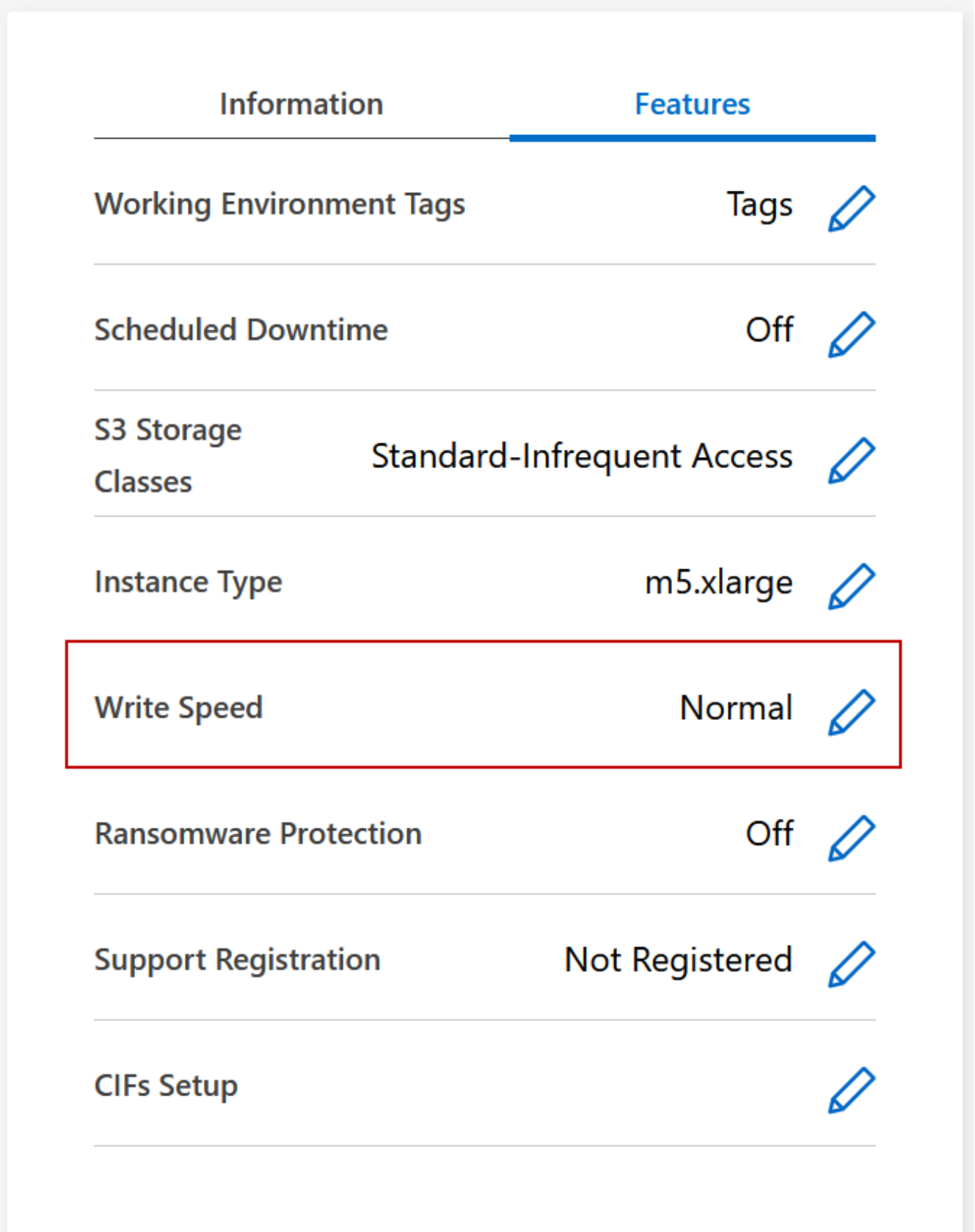
Prima di modificare la velocità di scrittura, è necessario "comprendere le differenze tra le impostazioni normali e quelle alte".

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 il sistema Cloud Volumes ONTAP. Si tratta di un processo di interruzione che richiede downtime per l'intero sistema.

Fasi

1. Nella pagina Canvas, fare doppio clic sul nome del sistema configurato per la velocità di scrittura.
2. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi fare clic sull'icona a forma di matita accanto a **velocità di scrittura**.



3. Selezionare **normale** o **alta**.

   Se scegli High, allora devi leggere il messaggio "capisco…" e confermare selezionando la casella.

L'opzione **High** write speed è supportata con le coppie Cloud Volumes ONTAP ha in Google Cloud a partire dalla versione 9.13.0.

4. Fare clic su **Save** (Salva), rivedere il messaggio di conferma, quindi fare clic su **Approve** (approva).

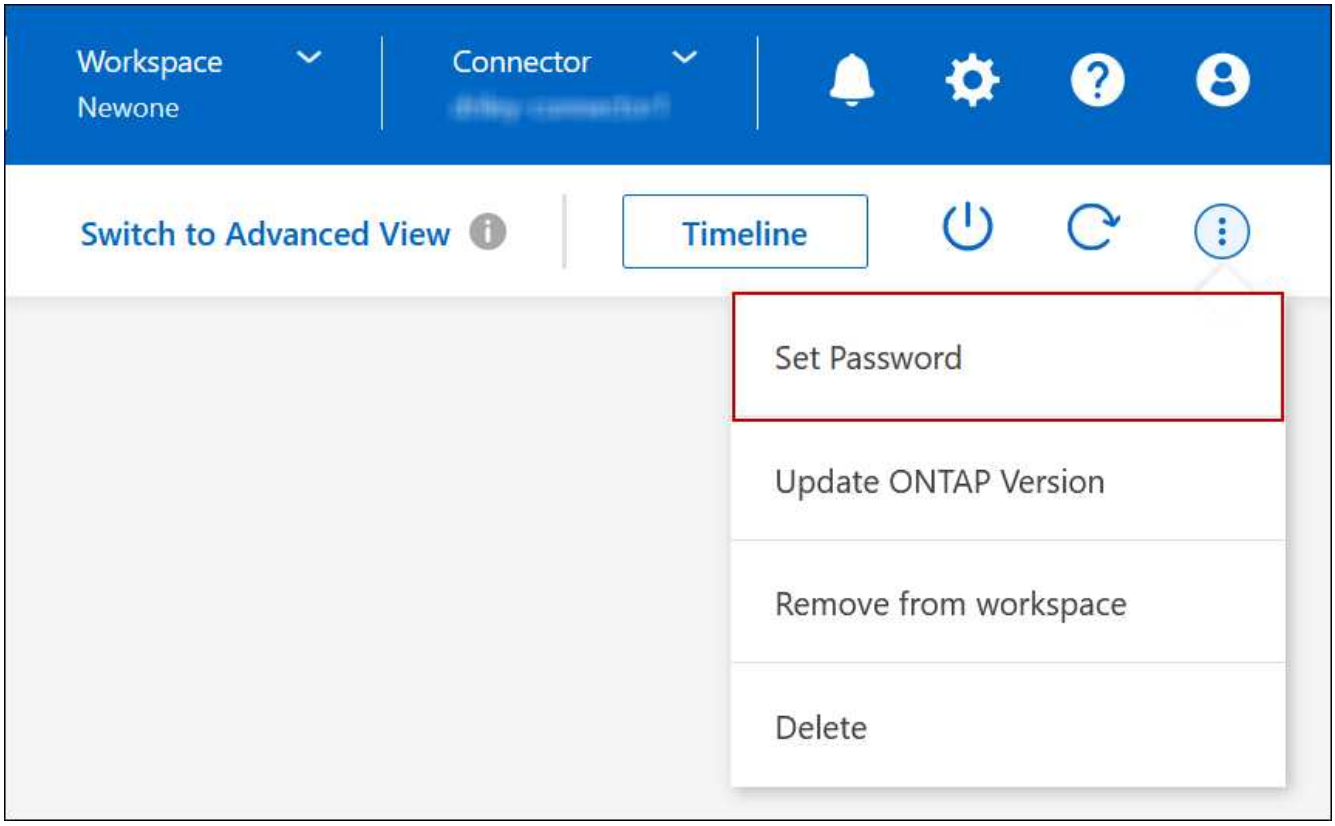
Modificare la password per Cloud Volumes ONTAP

Cloud Volumes ONTAP include un account di amministrazione del cluster. Se necessario, puoi modificare la password per questo account da BlueXP.

Non modificare la password per l'account admin tramite System Manager o CLI. La password non verrà riflessa in BlueXP. Di conseguenza, BlueXP non è in grado di monitorare correttamente l'istanza.

Fasi

1. Nella pagina Canvas, fare doppio clic sul nome dell'ambiente di lavoro Cloud Volumes ONTAP.
2. Nella parte superiore destra della console BlueXP, fare clic sull'icona ellisse e selezionare **Set password** (Imposta password).



La nuova password deve essere diversa da una delle ultime sei password utilizzate.

Aggiungere, rimuovere o eliminare sistemi

Aggiunta di sistemi Cloud Volumes ONTAP esistenti a BlueXP

È possibile individuare e aggiungere sistemi Cloud Volumes ONTAP esistenti a BlueXP. È

possibile eseguire questa operazione se si implementa un nuovo sistema BlueXP.

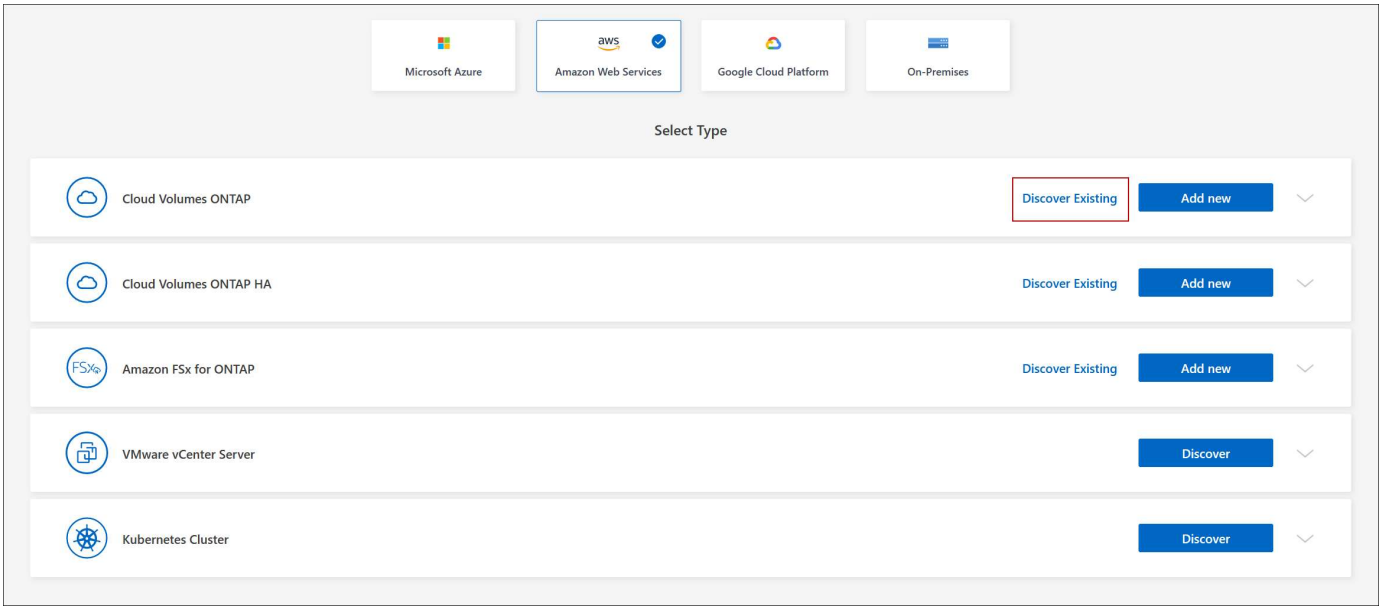
Prima di iniziare

È necessario conoscere la password dell'account utente amministratore di Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
3. Selezionare il provider cloud in cui risiede il sistema.
4. Scegliere il tipo di sistema Cloud Volumes ONTAP.
5. Fare clic sul collegamento per individuare un sistema esistente.

+



1. Nella pagina Area, scegliere l'area in cui sono in esecuzione le istanze, quindi selezionare le istanze.
2. Nella pagina credenziali, immettere la password per l'utente amministratore di Cloud Volumes ONTAP, quindi fare clic su **Go**.

Risultato

BlueXP aggiunge le istanze di Cloud Volumes ONTAP allo spazio di lavoro.

Rimozione degli ambienti di lavoro Cloud Volumes ONTAP

L'amministratore dell'account può rimuovere un ambiente di lavoro Cloud Volumes ONTAP per spostarlo in un altro sistema o per risolvere i problemi di rilevamento.

A proposito di questa attività

La rimozione di un ambiente di lavoro Cloud Volumes ONTAP lo rimuove da BlueXP. Non elimina il sistema Cloud Volumes ONTAP. In seguito, sarà possibile riscoprire l'ambiente di lavoro.

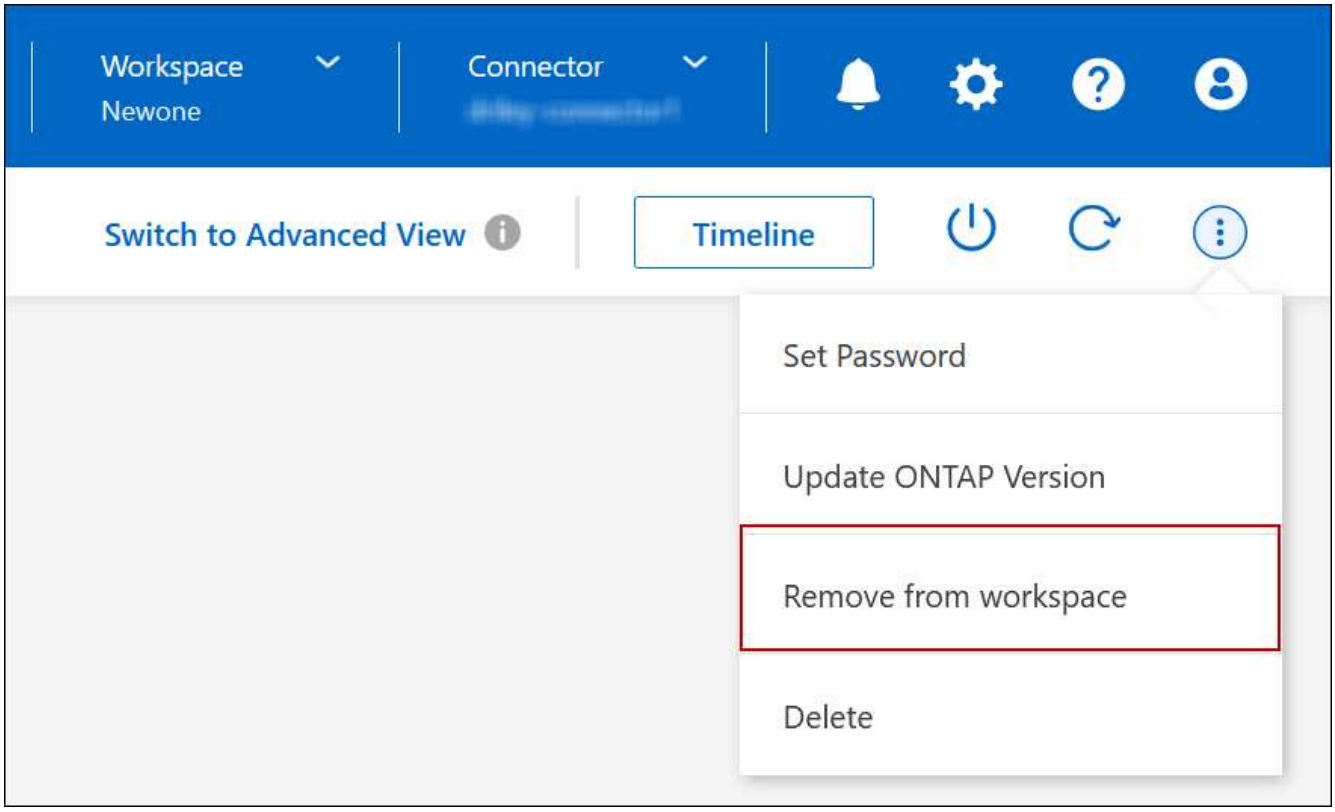
La rimozione di un ambiente di lavoro da BlueXP consente di effettuare le seguenti operazioni:

- Riscoprirla in un altro spazio di lavoro

- Riscoprirla da un altro sistema BlueXP
- Riscoprirla se si sono verificati problemi durante il rilevamento iniziale

Fasi

1. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro che si desidera rimuovere.
2. Nella parte superiore destra della console BlueXP, fare clic sull'icona dell'ellisse e selezionare **Rimuovi dall'area di lavoro**.



3. Nella finestra Review from Workspace (esamina da area di lavoro), fare clic su **Remove** (Rimuovi).

Risultato

BlueXP rimuove l'ambiente di lavoro. Gli utenti possono riscoprire questo ambiente di lavoro dalla pagina Canvas in qualsiasi momento.

Eliminazione di un sistema Cloud Volumes ONTAP

Si consiglia di eliminare sempre i sistemi Cloud Volumes ONTAP da BlueXP, anziché dalla console del provider di servizi cloud. Ad esempio, se si termina un'istanza di Cloud Volumes ONTAP con licenza dal provider cloud, non è possibile utilizzare la chiave di licenza per un'altra istanza. Per rilasciare la licenza, è necessario eliminare l'ambiente di lavoro da BlueXP.

Quando si elimina un ambiente di lavoro, BlueXP termina le istanze di Cloud Volumes ONTAP ed elimina dischi e snapshot.

Le risorse gestite da altri servizi, come i backup per il backup e ripristino BlueXP e le istanze per la classificazione BlueXP, non vengono eliminate quando si elimina un ambiente di lavoro. Dovrai eliminarli manualmente. In caso contrario, continuerai a ricevere i costi per queste risorse.

Quando BlueXP implementa Cloud Volumes ONTAP nel tuo cloud provider, abilita la protezione delle terminazioni sulle istanze. Questa opzione aiuta a prevenire la terminazione accidentale.

Fasi

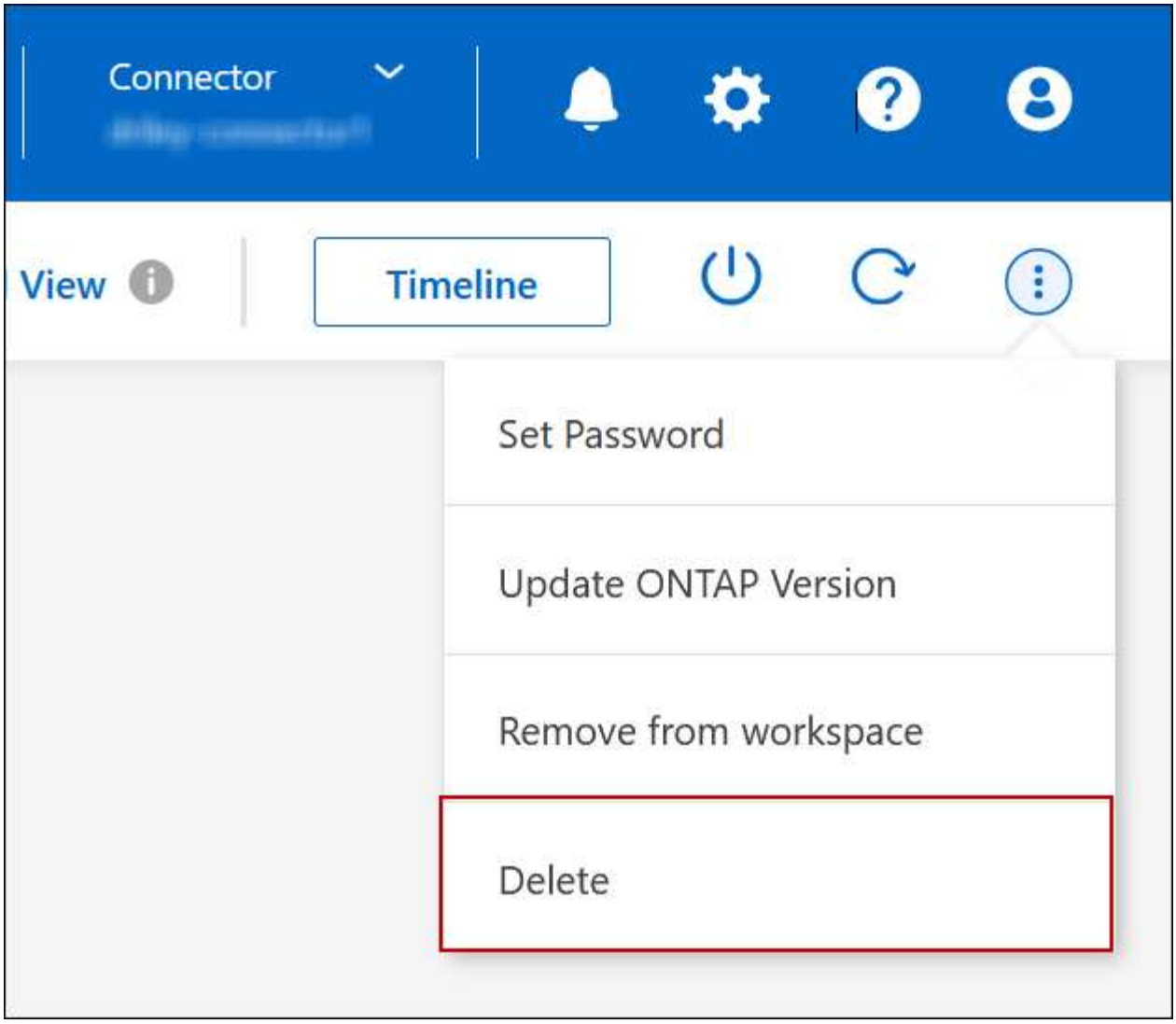
1. Se nell'ambiente di lavoro è stato attivato il backup e il ripristino di BlueXP, determinare se i dati di cui è stato eseguito il backup sono ancora necessari "eliminare i backup, se necessario".

   Il backup e il ripristino di BlueXP sono indipendenti da Cloud Volumes ONTAP per progettazione. Il backup e il ripristino di BlueXP non eliminano automaticamente i backup quando si elimina un sistema Cloud Volumes ONTAP e non esiste attualmente alcun supporto nell'interfaccia utente per eliminare i backup dopo che il sistema è stato eliminato.

2. Se è stata abilitata la classificazione BlueXP su questo ambiente di lavoro e nessun altro ambiente di lavoro utilizza questo servizio, sarà necessario eliminare l'istanza per il servizio.

   "Scopri di più sull'istanza di classificazione BlueXP".

3. Eliminare l'ambiente di lavoro Cloud Volumes ONTAP.
   a. Nella pagina Canvas, fare doppio clic sul nome dell'ambiente di lavoro Cloud Volumes ONTAP che si desidera eliminare.
   b. Nella parte superiore destra della console BlueXP, fare clic sull'icona dell'ellisse e selezionare **Delete** (Elimina).



c. Nella finestra Delete Working Environment (Elimina ambiente di lavoro), 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.

Amministrazione di AWS

Modificare il tipo di istanza EC2 per Cloud Volumes ONTAP

È possibile scegliere tra diversi tipi o istanze quando si avvia Cloud Volumes ONTAP in AWS. È possibile modificare il tipo di istanza 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 del tipo di istanza può influire sui costi del servizio AWS.

- 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.

> BlueXP 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.

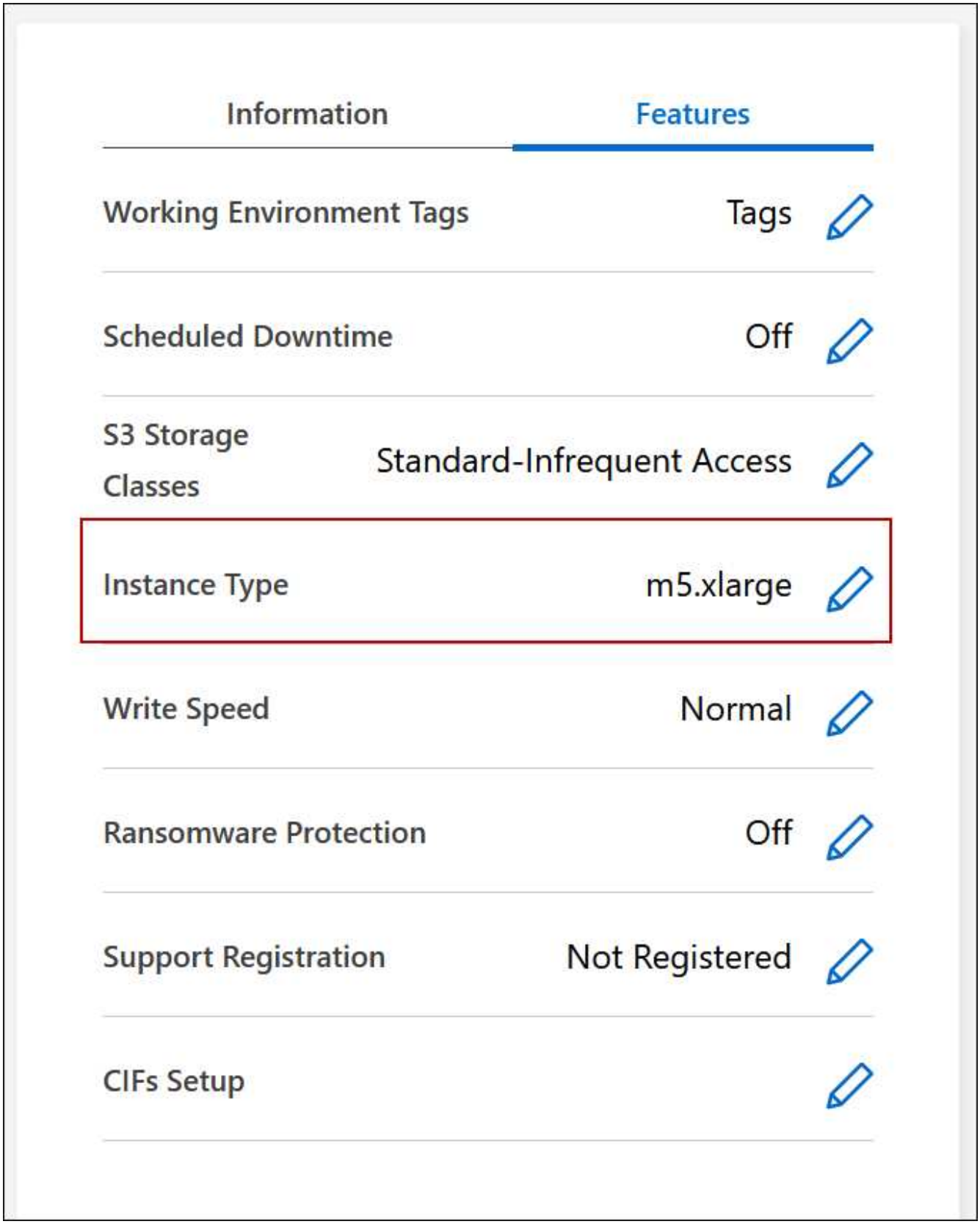
Riferimento

Per un elenco dei tipi di istanza supportati in AWS, vedere "Istanze EC2 supportate".

Se non è possibile modificare il tipo di istanza da istanze C4, M4 o R4, vedere l’articolo della Knowledge base "Impossibile modificare il tipo di istanza da R4 a R5 con errore di conteggio dischi".

Fasi

1. Nella pagina Canvas, selezionare l’ambiente di lavoro.
2. Nella scheda Panoramica, fare clic sul pannello funzionalità, quindi fare clic sull’icona a forma di matita accanto a **tipo di istanza**.



a. Se si utilizza una licenza PAYGO basata su nodo, è possibile scegliere un tipo di licenza e istanza diverso facendo clic sull'icona a forma di matita accanto a **tipo di licenza**.

3. Scegliere un tipo di istanza, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **Cambia**.

Risultato

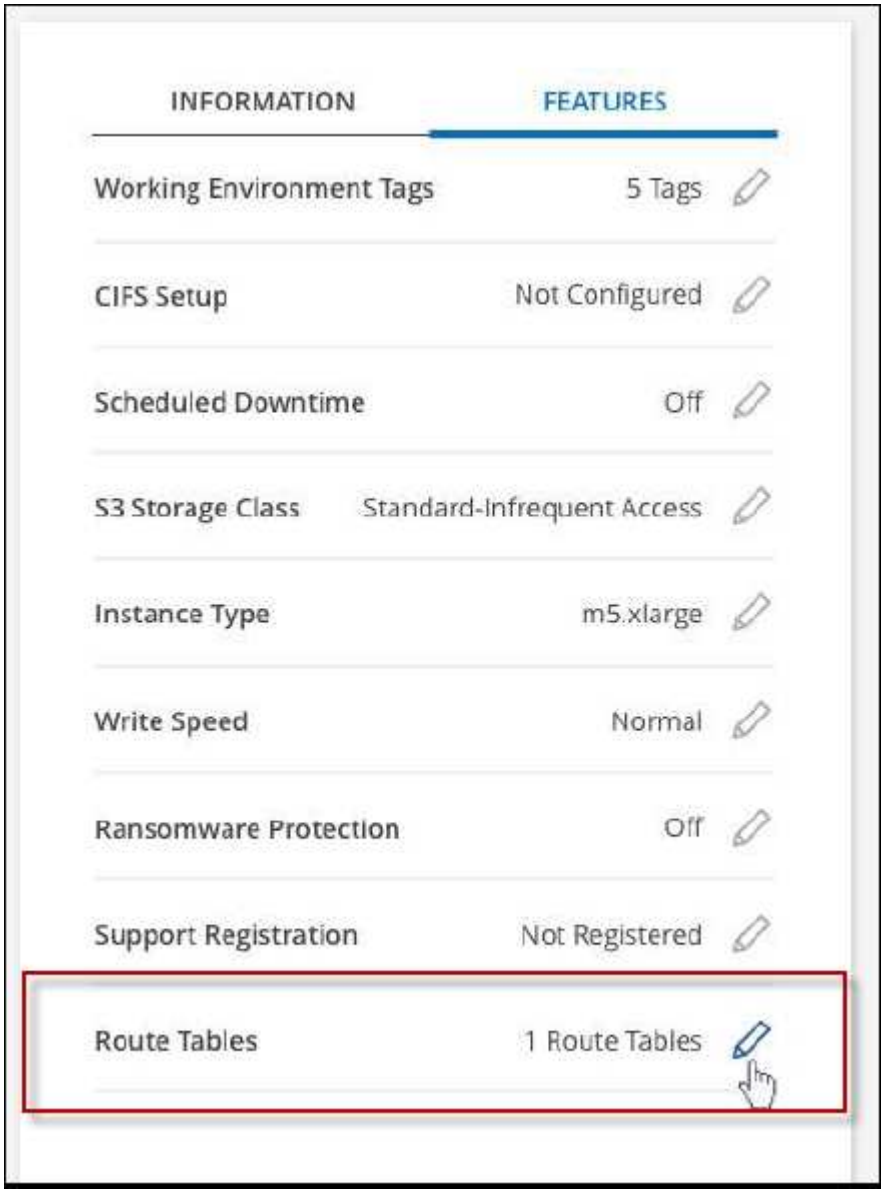
Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Modificare le tabelle di percorso per le coppie ha in più AZS

È possibile modificare le tabelle di routing AWS che includono i percorsi verso gli indirizzi IP mobili per una coppia ha implementata in più AWS Availability Zones (AZS). È possibile eseguire questa operazione se i nuovi client NFS o CIFS devono accedere a una coppia ha in AWS.

Fasi

1. Nella pagina Canvas, selezionare l'ambiente di lavoro.
2. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi fare clic sull'icona a forma di matita accanto a **tabelle di percorso**.



3. Modificare l'elenco delle tabelle di percorso selezionate, quindi fare clic su **Save** (Salva).

Risultato

BlueXP invia una richiesta AWS per modificare le tabelle di routing.

Amministrazione di Azure

Modificare il tipo di Azure VM per Cloud Volumes ONTAP

È possibile scegliere tra diversi tipi di macchine virtuali quando si avvia Cloud Volumes ONTAP in Microsoft Azure. È possibile modificare il tipo di macchina virtuale 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 del tipo di macchina virtuale può influire sui costi del servizio Microsoft Azure.
- L'operazione riavvia Cloud Volumes ONTAP.

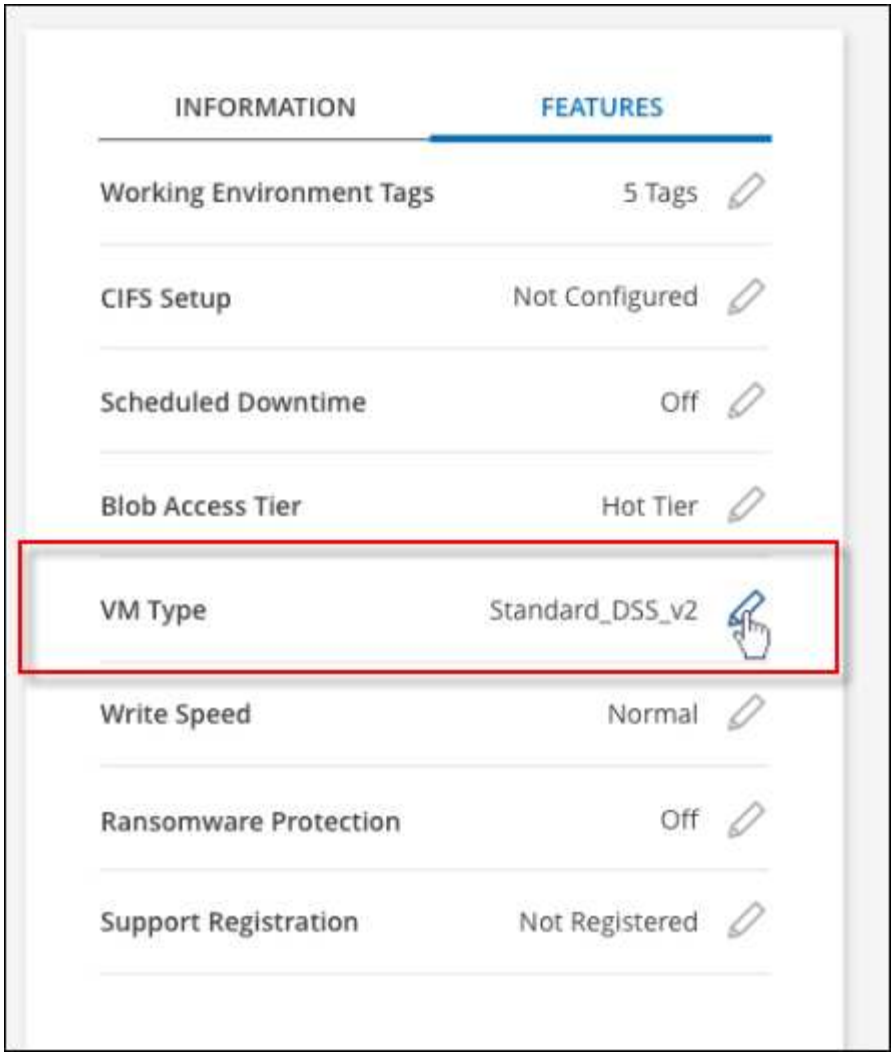
  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

> BlueXP 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. Nella pagina Canvas, selezionare l'ambiente di lavoro.
2. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi sull'icona a forma di matita accanto a **tipo di macchina virtuale**.



a. Se si utilizza una licenza PAYGO basata su nodo, è possibile scegliere una licenza e un tipo di macchina virtuale diversi facendo clic sull'icona a forma di matita accanto a **tipo di licenza**.

3. Selezionare un tipo di macchina virtuale, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **Cambia**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Esclusione dei blocchi CIFS per le coppie ha Cloud Volumes ONTAP in Azure

L'amministratore dell'account può attivare un'impostazione in BlueXP che impedisce problemi con il giveback dello storage Cloud Volumes ONTAP durante gli eventi di manutenzione di Azure. Quando si attiva questa impostazione, Cloud Volumes ONTAP esegue il veto di CIFS e ripristina le sessioni CIFS attive.

A proposito di questa attività

Microsoft Azure pianifica gli eventi di manutenzione periodica sulle macchine virtuali. Quando si verifica un evento di manutenzione su una coppia Cloud Volumes ONTAP ha, la coppia ha avvia il Takeover dello storage. Se durante questo evento di manutenzione sono presenti sessioni CIFS attive, i blocchi sui file CIFS possono impedire il giveback dello storage.

Se si attiva questa impostazione, Cloud Volumes ONTAP veto i blocchi e ripristina le sessioni CIFS attive. Di conseguenza, la coppia ha può completare il giveback dello storage durante questi eventi di manutenzione.

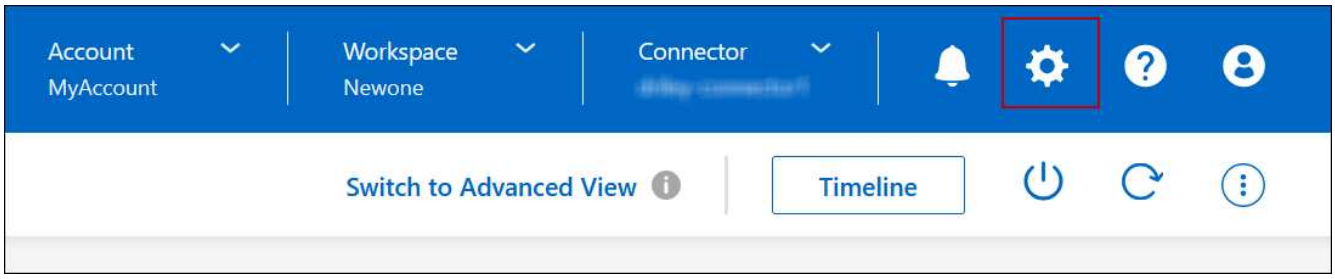
> Questo processo potrebbe interrompere i client CIFS. I dati non impegnati dai client CIFS potrebbero andare persi.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di BlueXP. "Scopri come".

Fasi

1. Nella parte superiore destra della console BlueXP, fai clic sull'icona Impostazioni e seleziona **Impostazioni Cloud Volumes ONTAP**.



2. In **Azure**, fare clic su **Azure CIFS Blocks for Azure ha Working Environments**.
3. Fare clic sulla casella di controllo per attivare la funzione, quindi fare clic su **Save** (Salva).

Utilizzare un collegamento privato Azure o endpoint del servizio

Cloud Volumes ONTAP utilizza un collegamento privato Azure per le connessioni agli account di storage associati. Se necessario, è possibile disattivare Azure Private Links e utilizzare gli endpoint del servizio.

Panoramica

Per impostazione predefinita, BlueXP attiva un collegamento privato Azure per le connessioni tra Cloud Volumes ONTAP e i relativi account di storage associati. Azure Private link protegge le connessioni tra gli endpoint in Azure e offre vantaggi in termini di performance.

Se necessario, è possibile configurare Cloud Volumes ONTAP in modo che utilizzi gli endpoint del servizio invece di un collegamento privato Azure.

Con entrambe le configurazioni, BlueXP limita sempre l'accesso alla rete per le connessioni tra Cloud Volumes ONTAP e gli account di storage. L'accesso alla rete è limitato a VNET in cui viene implementato Cloud Volumes ONTAP e a VNET in cui viene implementato il connettore.

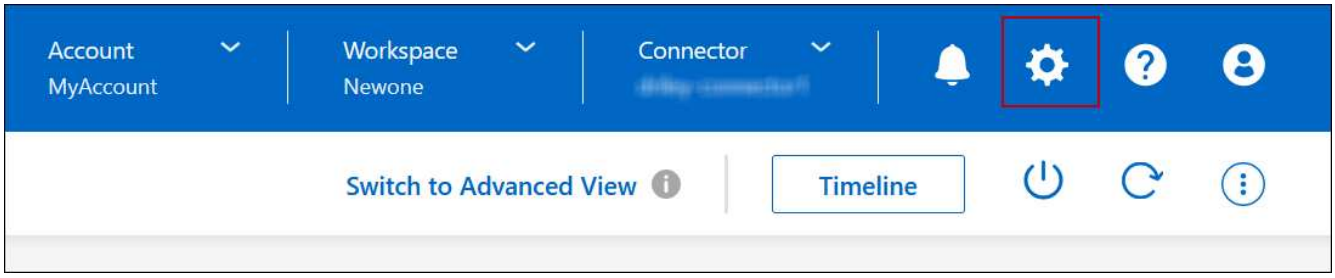
Disattivare Azure Private Links e utilizzare gli endpoint del servizio

Se richiesto dall'azienda, è possibile modificare un'impostazione in BlueXP in modo che configuri Cloud Volumes ONTAP per l'utilizzo degli endpoint del servizio invece di un collegamento privato Azure. La modifica di questa impostazione si applica ai nuovi sistemi Cloud Volumes ONTAP creati. Gli endpoint del servizio sono supportati solo in "Coppie di regioni Azure" Tra il connettore e i VNet Cloud Volumes ONTAP.

Il connettore deve essere implementato nella stessa area Azure dei sistemi Cloud Volumes ONTAP gestiti o in "Coppia di regioni Azure" Per i sistemi Cloud Volumes ONTAP.

Fasi

1. Nella parte superiore destra della console BlueXP, fai clic sull'icona Impostazioni e seleziona **Impostazioni Cloud Volumes ONTAP**.



2. In **Azure**, fare clic su **Use Azure Private link**.
3. Deselezionare **connessione di collegamento privato tra account Cloud Volumes ONTAP e storage**.
4. Fare clic su **Save** (Salva).

Al termine

Se Azure Private Links è stato disattivato e il connettore utilizza un server proxy, è necessario attivare il traffico API diretto.

"Scopri come attivare il traffico API diretto sul connettore"

Lavorare con Azure Private Links

Nella maggior parte dei casi, non c'è nulla da fare per impostare i link privati di Azure con Cloud Volumes ONTAP. BlueXP gestisce Azure Private Links per te. Tuttavia, se si utilizza una zona Azure Private DNS esistente, è necessario modificare un file di configurazione.

Requisito per il DNS personalizzato

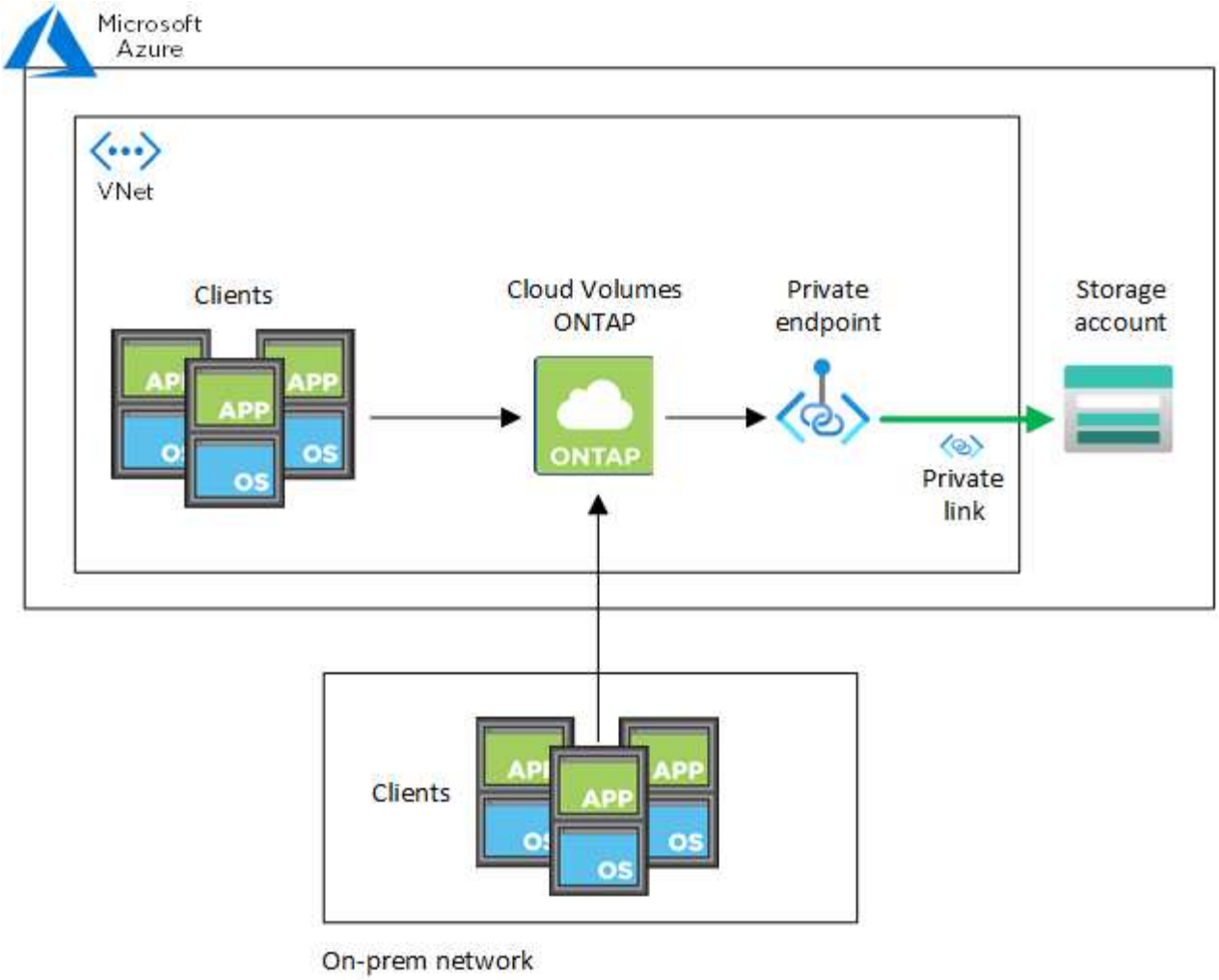
Se si utilizza un DNS personalizzato, è possibile creare un server di inoltro condizionale per la zona DNS privata di Azure dai server DNS personalizzati. Per ulteriori informazioni, fare riferimento a. "Documentazione di Azure sull'utilizzo di un server di inoltro DNS".

Funzionamento delle connessioni di collegamento privato

Quando BlueXP implementa Cloud Volumes ONTAP in Azure, crea un endpoint privato nel gruppo di risorse. L'endpoint privato è associato agli account storage per Cloud Volumes ONTAP. Di conseguenza, l'accesso allo storage Cloud Volumes ONTAP passa attraverso la rete backbone Microsoft.

L'accesso client passa attraverso il collegamento privato quando i client si trovano all'interno della stessa rete virtuale di Cloud Volumes ONTAP, all'interno di reti VPN peered o nella rete on-premise quando si utilizza una connessione privata VPN o ExpressRoute a VNET.

Ecco un esempio che mostra l'accesso del client su un collegamento privato dall'interno dello stesso VNET e da una rete on-premise che dispone di una connessione privata VPN o ExpressRoute.



Se i sistemi Connector e Cloud Volumes ONTAP sono implementati in reti VNet diverse, è necessario impostare il peering VNET tra la rete in cui viene implementato il connettore e la rete in cui vengono implementati i sistemi Cloud Volumes ONTAP.

Fornisci a BlueXP i dettagli sul tuo Azure Private DNS

Se si utilizza "DNS privato Azure", Quindi è necessario modificare un file di configurazione su ciascun connettore. In caso contrario, BlueXP non può attivare la connessione Azure Private link tra Cloud Volumes ONTAP e i relativi account di storage associati.

Il nome DNS deve corrispondere ai requisiti di denominazione DNS di Azure "Come mostrato nella documentazione di Azure".

Fasi

1. SSH all'host del connettore e accedere.
2. Accedere alla seguente directory: /Opt/application/netapp/cloudmanager/docker_occm/data
3. Modificare app.conf aggiungendo il parametro "user-private-dns-zone-settings" con le seguenti coppie parola chiave-valore:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

Il parametro deve essere inserito allo stesso livello di "ID sistema", come mostrato di seguito:

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

Tenere presente che la parola chiave Subscription è richiesta solo se l'Area DNS privata è presente in un abbonamento diverso da quello del connettore.

4. Salvare il file e disconnettersi dal connettore.

   Non è necessario riavviare.

Abilitare il rollback in caso di errori

Se BlueXP non riesce a creare un Azure Private link come parte di azioni specifiche, completa l'azione senza la connessione Azure Private link. Ciò può verificarsi quando si crea un nuovo ambiente di lavoro (nodo singolo o coppia ha) o quando si verificano le seguenti azioni su una coppia ha: Creazione di un nuovo aggregato, aggiunta di dischi a un aggregato esistente o creazione di un nuovo account storage quando si supera 32 TIB.

È possibile modificare questo comportamento predefinito attivando il rollback se BlueXP non riesce a creare Azure Private link. In questo modo è possibile garantire la piena conformità con le normative di sicurezza aziendali.

Se si attiva il rollback, BlueXP interrompe l'azione e riporta tutte le risorse create come parte dell'azione.

È possibile attivare il rollback attraverso l'API o aggiornando il file app.conf.

Attivare il rollback attraverso l'API

Fase

1. Utilizzare `PUT /occm/config` Chiamata API con il seguente corpo della richiesta:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Attiva il rollback aggiornando app.conf

Fasi

1. SSH all'host del connettore e accedere.

2. Accedere alla seguente directory: /Opt/application/netapp/cloudmanager/docker_occm/data
3. Modificare app.conf aggiungendo il seguente parametro e valore:

```
 "rollback-on-private-link-failure": true
. Salvare il file e disconnettersi dal connettore.
```

Non è necessario riavviare.

Spostamento dei gruppi di risorse

Cloud Volumes ONTAP supporta lo spostamento dei gruppi di risorse Azure, ma il flusso di lavoro avviene solo nella console Azure.

È possibile spostare un ambiente di lavoro da un gruppo di risorse a un gruppo di risorse diverso in Azure all'interno della stessa sottoscrizione Azure. Lo spostamento di gruppi di risorse tra diverse sottoscrizioni Azure non è supportato.

Fasi

1. Rimuovere l'ambiente di lavoro da **Canvas**.

   Per informazioni su come rimuovere un ambiente di lavoro, vedere "Rimozione degli ambienti di lavoro Cloud Volumes ONTAP".

2. Eseguire lo spostamento del gruppo di risorse nella console di Azure.

   Per completare lo spostamento, fare riferimento a. "Spostare le risorse in un nuovo gruppo di risorse o in un abbonamento nella documentazione di Microsoft Azure".

3. In **Canvas**, scopri l'ambiente di lavoro.
4. Cercare il nuovo gruppo di risorse nelle informazioni relative all'ambiente di lavoro.

Risultato

L'ambiente di lavoro e le relative risorse (macchine virtuali, dischi, account di storage, interfacce di rete, snapshot) fanno parte del nuovo gruppo di risorse.

Isolamento del traffico SnapMirror in Azure

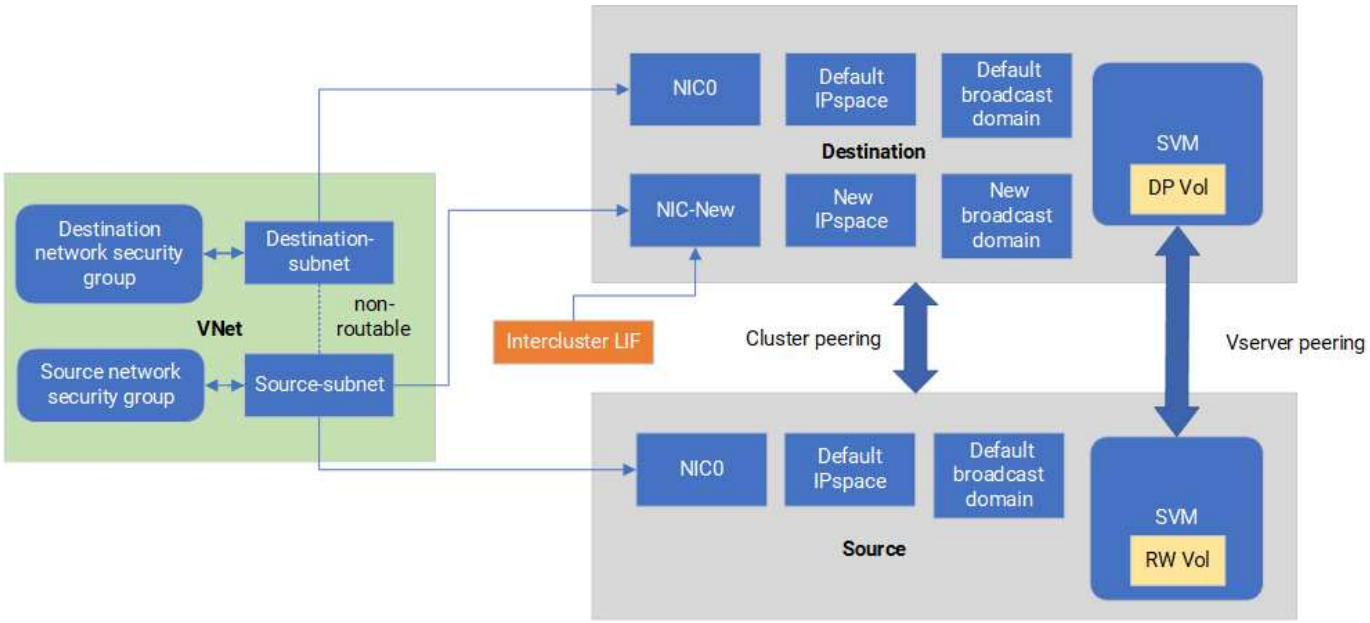
Con Cloud Volumes ONTAP in Azure, puoi separare il traffico di replica SnapMirror dai dati e dal traffico di gestione. Per separare il traffico di replica SnapMirror dal traffico dati, è necessario aggiungere una nuova scheda di interfaccia di rete (NIC), una LIF associata e una subnet non instradabile.

Informazioni sulla segregazione del traffico SnapMirror in Azure

Per impostazione predefinita, BlueXP configura tutti i NIC e le LIF in un'implementazione di Cloud Volumes ONTAP sulla stessa subnet. In tali configurazioni, il traffico di replica di SnapMirror e il traffico di dati e gestione utilizzano la stessa subnet. Il segregazione del traffico SnapMirror sfrutta una subnet aggiuntiva non indirizzabile alla subnet esistente utilizzata per i dati e il traffico di gestione.

Figura 1

I diagrammi seguenti mostrano la segregazione del traffico di replica SnapMirror con una scheda di rete aggiuntiva, una LIF intercluster associata e una subnet non instradabile in un'implementazione a nodo singolo. Un'implementazione ha Pair differisce leggermente.



Prima di iniziare

Fare riferimento alle seguenti considerazioni:

- Puoi aggiungere una sola NIC a un singolo nodo o a un'implementazione ha-Pair (istanza VM) Cloud Volumes ONTAP per la segregazione del traffico SnapMirror.
- Per aggiungere una nuova scheda di rete, il tipo di istanza della macchina virtuale che si implementa deve disporre di una scheda di rete non utilizzata.
- I cluster di origine e di destinazione devono avere accesso alla stessa rete virtuale (VNET). Il cluster di destinazione è un sistema Cloud Volumes ONTAP in Azure. Il cluster di origine può essere un sistema Cloud Volumes ONTAP in Azure o un sistema ONTAP.

Fase 1: Creare una scheda NIC aggiuntiva e collegarla alla macchina virtuale di destinazione

Questa sezione fornisce istruzioni su come creare una scheda NIC aggiuntiva e collegarla alla macchina virtuale di destinazione. La macchina virtuale di destinazione è il nodo singolo o un sistema ha-Pair in Cloud Volumes ONTAP in Azure, in cui si desidera configurare la scheda di interfaccia di rete aggiuntiva.

Fasi

1. Nell'interfaccia CLI di ONTAP, arrestare il nodo.

```
dest::> halt -node <dest_node-vm>
```

2. Nel portale di Azure, verifica che lo stato della VM (nodo) sia arrestato.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Utilizzare l'ambiente Bash in Azure Cloud Shell per arrestare il nodo.
   a. Arrestare il nodo.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

   b. Disallocare il nodo.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-
vm>
```

4. Configurare le regole del gruppo di protezione della rete per rendere le due sottoreti (subnet del cluster di origine e subnet del cluster di destinazione) non instradabili l'una all'altra.
   a. Creare la nuova NIC sulla VM di destinazione.
   b. Cercare l'ID subnet per la subnet del cluster di origine.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet
-name <vnet> --query id
```

   c. Creare la nuova scheda di rete sulla macchina virtuale di destinazione con l'ID della subnet per la subnet del cluster di origine. Immettere il nome della nuova scheda NIC.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>
--subnet <id_from_prev_command> --accelerated-networking true
```

   d. Salvare privateIPAddress. Questo indirizzo IP, <new_added_nic_primary_addr>, viene utilizzato per creare una intercluster LIF in Dominio di broadcast, intercluster LIF per la nuova scheda NIC.
5. Collegare la nuova scheda NIC alla macchina virtuale.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics
<dest_node-vm-nic-new>
```

6. Avviare la VM (nodo).

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Nel portale di Azure, andare su **Networking** e confermare che la nuova NIC, ad esempio nic-new, esiste e la rete accelerata è abilitata.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg
--query "[].{NIC: name, VM: virtualMachine.id}"
```

Per le implementazioni ha-Pair, ripeti i passaggi per il nodo partner.

Fase 2: Creare un nuovo IPSpace, dominio di broadcast e intercluster LIF per la nuova scheda di rete

Un IPSpace separato per intercluster LIF fornisce la separazione logica tra funzionalità di rete per la replica tra cluster.

Utilizzare l'interfaccia CLI di ONTAP per i seguenti passaggi.

Fasi

1. Creare il nuovo IPSpace (new_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Creare un dominio broadcast sul nuovo IPSpace (new_ipspace) e aggiungere la porta nic-new.

```
dest::> network port show
```

3. Per i sistemi a nodo singolo, la porta appena aggiunta è *e0b*. Per le implementazioni ha-Pair con dischi gestiti, la porta appena aggiunta è *e0d*. Per le implementazioni ha-Pair con page blob, la porta appena aggiunta è *e0e*. Utilizzare il nome del nodo e non il nome della VM. Trovare il nome del nodo eseguendo `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Creare una LIF intercluster nella nuova broadcast-domain (new_bd) e nella nuova NIC (nic-new).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Verifica della creazione del nuovo intercluster LIF.

```
dest::> net int show
```

Per le implementazioni ha-Pair, ripeti i passaggi per il nodo partner.

Fase 3: Verificare il peering dei cluster tra i sistemi di origine e di destinazione

Questa sezione fornisce istruzioni su come verificare il peering tra i sistemi di origine e di destinazione.

Utilizzare l'interfaccia CLI di ONTAP per i seguenti passaggi.

Fasi

1. Verificare che la LIF intercluster del cluster di destinazione sia in grado di eseguire il ping intercluster LIF del cluster di origine. Poiché il cluster di destinazione esegue questo comando, l'indirizzo IP di destinazione è l'indirizzo IP intercluster LIF sull'origine.

   ```
   dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
   -destination <10.161.189.6>
   ```

2. Verificare che la LIF intercluster del cluster di origine sia in grado di eseguire il ping della LIF del cluster di destinazione. La destinazione è l'indirizzo IP della nuova scheda NIC creata sulla destinazione.

   ```
   src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
   <10.161.189.18>
   ```

Per le implementazioni ha-Pair, ripeti i passaggi per il nodo partner.

Fase 4: Creare il peering SVM tra il sistema di origine e destinazione

Questa sezione fornisce istruzioni per creare il peering SVM tra il sistema di origine e di destinazione.

Utilizzare l'interfaccia CLI di ONTAP per i seguenti passaggi.

Fasi

1. Creare il peering dei cluster sulla destinazione utilizzando l'indirizzo IP intercluster LIF di origine come `-peer-addrs`. Per le coppie ha, elenca l'indirizzo IP intercluster LIF di origine per entrambi i nodi come `-peer-addrs`.

   ```
   dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
   <new_ipspace>
   ```

2. Immettere e confermare la password.
3. Creare il peering dei cluster sull'origine utilizzando l'indirizzo IP LIF del cluster di destinazione come `peer-addrs`. Per le coppie ha, elenca l'indirizzo IP LIF di destinazione per entrambi i nodi come `-peer-addrs`.

   ```
   src::> cluster peer create -peer-addrs <10.161.189.18>
   ```

4. Immettere e confermare la password.
5. Controllare che il cluster sia stato sottoposto a peering.

```
src::> cluster peer show
```

Il peering riuscito mostra **disponibile** nel campo disponibilità.

6. Creare il peering di SVM sulla destinazione. Sia le SVM di origine che di destinazione devono essere SVM di dati.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Accetta il peering della SVM.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Verificare che la SVM sia stata sottoposta a peed.

```
dest::> vserver peer show
```

Visualizzazione dello stato peer **`peered`** e le applicazioni di peering **`snapmirror`**.

Fase 5: Creare una relazione di replica SnapMirror tra il sistema di origine e quello di destinazione

Questa sezione fornisce istruzioni su come creare una relazione di replica SnapMirror tra il sistema di origine e quello di destinazione.

Per spostare una relazione di replica SnapMirror esistente, è necessario prima interrompere la relazione di replica SnapMirror esistente prima di creare una nuova relazione di replica SnapMirror.

Utilizzare l'interfaccia CLI di ONTAP per i seguenti passaggi.

Fasi

1. Creazione di un volume protetto sui dati nella SVM di destinazione.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Creare una relazione di replica di SnapMirror nella destinazione, che includa il criterio e il programma di replica di SnapMirror.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Inizializzare la relazione di replica SnapMirror sulla destinazione.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. Nella CLI di ONTAP, convalida lo stato della relazione di SnapMirror eseguendo il seguente comando:

```
dest::> snapmirror show
```

   Lo stato della relazione è `Snapmirrored` e la salute del rapporto è `true`.

5. Opzionale: Nell'interfaccia della riga di comando di ONTAP, esegui il seguente comando per visualizzare la cronologia delle azioni per la relazione di SnapMirror.

```
dest::> snapmirror show-history
```

In alternativa, è possibile montare i volumi di origine e di destinazione, scrivere un file nell'origine e verificare che il volume sia in fase di replica sulla destinazione.

Amministrazione di Google Cloud

Modificare il tipo di macchina Google Cloud per Cloud Volumes ONTAP

È possibile scegliere tra diversi tipi di computer quando si avvia Cloud Volumes ONTAP in Google Cloud. 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 del tipo di computer può influire sui costi di servizio di Google Cloud.
- L'operazione riavvia Cloud Volumes ONTAP.

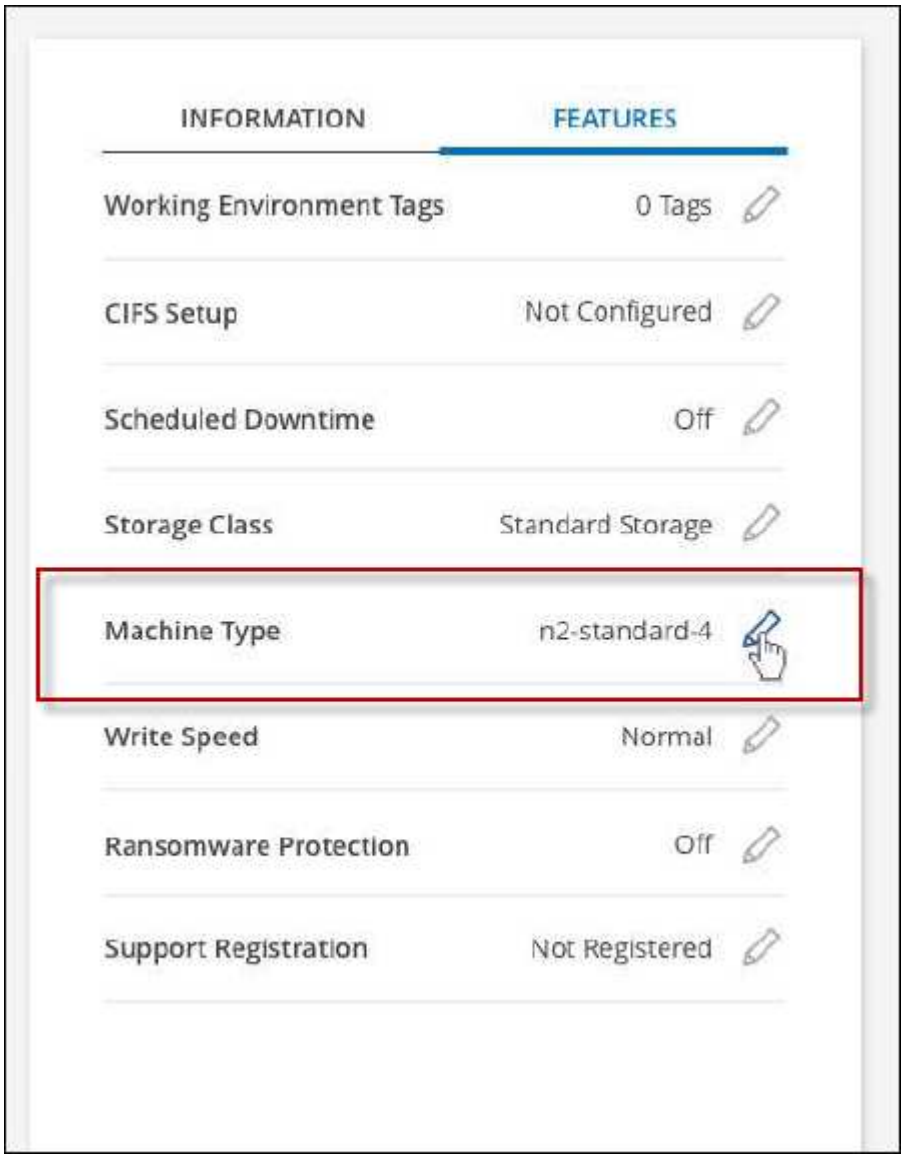
  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

> BlueXP 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. Nella pagina Canvas, selezionare l'ambiente di lavoro.
2. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi fare clic sull'icona a forma di matita accanto a **tipo di macchina**.



   a. Se si utilizza una licenza PAYGO basata su nodo, è possibile scegliere una licenza e un tipo di macchina diversi facendo clic sull'icona a forma di matita accanto a **tipo di licenza**.

3. Scegliere un tipo di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **Cambia**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Amministrare Cloud Volumes ONTAP utilizzando la visualizzazione avanzata

Se è necessario eseguire una gestione avanzata di Cloud Volumes ONTAP, è possibile farlo utilizzando Gestione di sistema di ONTAP, un'interfaccia di gestione fornita con un sistema ONTAP. Abbiamo incluso l'interfaccia di System Manager direttamente in BlueXP,

in modo che non sia necessario lasciare BlueXP per una gestione avanzata.

Caratteristiche

La visualizzazione avanzata di BlueXP consente di accedere a funzionalità di gestione aggiuntive:

- Gestione avanzata dello storage

  Gestione di gruppi di coerenza, condivisioni, qtree, quote e Storage VM.

- Gestione del networking

  Gestione di IPspaces, interfacce di rete, portset e porte ethernet.

- Eventi e lavori

  Visualizza registri eventi, avvisi di sistema, processi e registri di audit.

- Protezione avanzata dei dati

  Protezione di VM di storage, LUN e gruppi di coerenza.

- Gestione degli host

  Configurare I gruppi iniziatori SAN e i client NFS.

Configurazioni supportate

La gestione avanzata tramite Gestione di sistema è supportata con Cloud Volumes ONTAP 9.10.0 e versioni successive nelle aree cloud standard.

L'integrazione di System Manager non è supportata nelle regioni di GovCloud o nelle regioni che non dispongono di accesso a Internet in uscita.

Limitazioni

Alcune funzioni visualizzate nell'interfaccia di Gestione sistema non sono supportate da Cloud Volumes ONTAP:

- Tiering BlueXP

  Il servizio di tiering BlueXP non è supportato con Cloud Volumes ONTAP. Quando si creano volumi, è necessario impostare il tiering dei dati sullo storage a oggetti direttamente dalla vista standard di BlueXP.

- Tier

  La gestione degli aggregati (inclusi Tier locali e Tier cloud) non è supportata da System Manager. È necessario gestire gli aggregati direttamente dalla vista standard di BlueXP.

- Aggiornamenti del firmware

  Gli aggiornamenti automatici del firmware dalla pagina **Cluster > Impostazioni** non sono supportati con Cloud Volumes ONTAP.

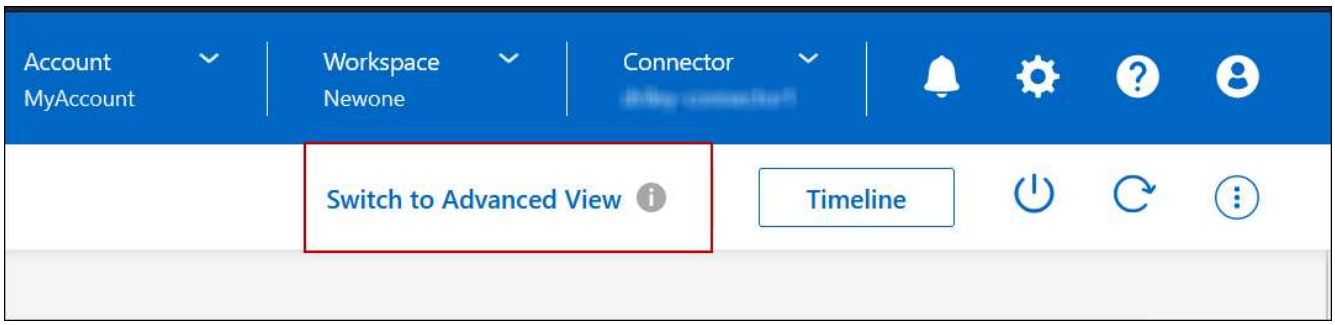
Inoltre, il controllo degli accessi basato sui ruoli da System Manager non è supportato.

Come iniziare

Aprire un ambiente di lavoro Cloud Volumes ONTAP e fare clic sull'opzione visualizzazione avanzata.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare doppio clic sul nome di un sistema Cloud Volumes ONTAP.
3. In alto a destra, fare clic su **passa alla visualizzazione avanzata**.



4. Se viene visualizzato il messaggio di conferma, leggerlo e fare clic su **Chiudi**.
5. Utilizzare Gestione sistema per gestire Cloud Volumes ONTAP.
6. Se necessario, fare clic su **passa alla visualizzazione standard** per tornare alla gestione standard tramite BlueXP.

Guida all'utilizzo di System Manager

Per assistenza sull'utilizzo di Gestione di sistema con Cloud Volumes ONTAP, consultare la sezione "Documentazione ONTAP" per istruzioni dettagliate. Di seguito sono riportati alcuni link utili:

- "Gestione di volumi e LUN"
- "Gestione della rete"
- "Protezione dei dati"

Amministrare Cloud Volumes ONTAP dalla CLI

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 di collegamento nella rete del provider di cloud.

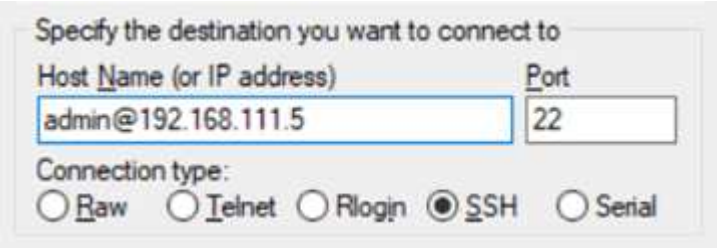
> Quando vengono implementate in più AZS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

Fasi

1. In BlueXP, identificare l'indirizzo IP dell'interfaccia di gestione del cluster:
   a. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
   b. Nella pagina Canvas, selezionare il sistema Cloud Volumes ONTAP.
   c. 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::>
```

Stato ed eventi del sistema

Verificare l'installazione di AutoSupport

AutoSupport monitora in modo proattivo lo stato di salute del sistema e invia messaggi al supporto tecnico NetApp. Per impostazione predefinita, AutoSupport è attivato su ciascun nodo per inviare messaggi al supporto tecnico utilizzando il protocollo di trasporto HTTPS. Si consiglia di verificare che AutoSupport possa inviare questi messaggi.

L'unica fase di configurazione necessaria è garantire che Cloud Volumes ONTAP disponga di connettività Internet in uscita. Per ulteriori informazioni, consulta i requisiti di rete per il tuo cloud provider.

Requisiti AutoSupport

I nodi Cloud Volumes ONTAP richiedono l'accesso a Internet in uscita per NetApp AutoSupport, che monitora in modo proattivo lo stato di salute del sistema e invia messaggi al supporto tecnico NetApp.

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

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

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

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

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

Risolvere i problemi della configurazione AutoSupport

Se non è disponibile una connessione in uscita e BlueXP non è in grado di configurare il sistema Cloud Volumes ONTAP in modo che utilizzi il connettore come server proxy, verrà inviata una notifica da BlueXP intitolata "<working environment name> is unable to send AutoSupport messages" (Impossibile inviare messaggi Microsoft).

Molto probabilmente ricevi questo messaggio a causa di problemi di rete.

Per risolvere il problema, procedere come segue.

Fasi

1. SSH al sistema Cloud Volumes ONTAP in modo da poter amministrare il sistema dalla CLI.

   "Scopri come passare da SSH a Cloud Volumes ONTAP".

2. Visualizzare lo stato dettagliato del sottosistema AutoSupport:

   ```
   autosupport check show-details
   ```

   La risposta deve essere simile a quanto segue:

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

Se lo stato della categoria http-https è "ok" significa che AutoSupport è configurato correttamente e che è possibile inviare messaggi.

3. Se lo stato non è corretto, verificare l'URL del proxy per ciascun nodo Cloud Volumes ONTAP:

   ```
   autosupport show -fields proxy-url
   ```

4. Se il parametro dell'URL del proxy è vuoto, configurare Cloud Volumes ONTAP in modo che utilizzi il connettore come proxy:

   ```
   autosupport modify -proxy-url http://<connector private ip>:3128
   ```

5. Verificare nuovamente lo stato AutoSupport:

   ```
   autosupport check show-details
   ```

6. Se lo stato continua a non essere corretto, verificare la presenza di connettività tra Cloud Volumes ONTAP e il connettore sulla porta 3128.
7. Se l'ID di stato continua a non riuscire dopo aver verificato la presenza di connettività, SSH al connettore.

   "Scopri di più sulla connessione a Linux VM per il connettore"

8. Passare a. `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Aprire il file di configurazione del proxy `squid.conf`

   La struttura di base del file è la seguente:

   ```
   http_port 3128
   acl localnet src 172.31.0.0/16
   acl azure_aws_metadata dst 169.254.169.254

   http_access allow localnet
   http_access deny azure_aws_metadata
   http_access allow localhost
   http_access deny all
   ```

   Il valore src di localnet è il CIDR del sistema Cloud Volumes ONTAP.

10. Se il blocco CIDR del sistema Cloud Volumes ONTAP non rientra nell'intervallo specificato nel file, aggiornare il valore o aggiungere una nuova voce come segue:

    ```
    acl cvonet src <cidr>
    ```

    Se Aggiungi questa nuova voce, non dimenticare di aggiungere anche una voce Consenti:

    ```
    http_access allow cvonet
    ```

    Ecco un esempio:

    ```
    http_port 3128
    acl localnet src 172.31.0.0/16
    acl cvonet src 172.33.0.0/16
    acl azure_aws_metadata dst 169.254.169.254

    http_access allow localnet
    http_access allow cvonet
    http_access deny azure_aws_metadata
    http_access allow localhost
    http_access deny all
    ```

11. Dopo aver modificato il file di configurazione, riavviare il container proxy come sudo:

    ```
    docker restart squid
    ```

12. Tornare all'interfaccia utente di Cloud Volumes ONTAP e verificare che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

    ```
    autosupport check show-details
    ```

Configurare EMS

Il sistema di gestione degli eventi (EMS) raccoglie e visualizza informazioni sugli eventi che si verificano nei sistemi 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, fare riferimento a. "Documenti ONTAP: Panoramica della configurazione EMS".