Documentazione Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
August 19, 2025

This PDF was generated from https://docs.netapp.com/it-it/bluexp-cloud-volumes-ontap/index.html on August 19, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione Cloud Volumes ONTAP . . . 1
Note di rilascio . . . 2
Novità di Cloud Volumes ONTAP . . . 2
11 agosto 2025 . . . 2
14 luglio 2025 . . . 2
25 giugno 2025 . . . 2
29 maggio 2025 . . . 3
12 maggio 2025 . . . 3
16 aprile 2025 . . . 3
14 aprile 2025 . . . 3
3 aprile 2025 . . . 4
28 marzo 2025 . . . 4
12 marzo 2025 . . . 4
10 marzo 2025 . . . 4
6 marzo 2025 . . . 5
03 marzo 2025 . . . 5
18 febbraio 2025 . . . 5
10 febbraio 2025 . . . 5
9 dicembre 2024 . . . 6
11 novembre 2024 . . . 6
25 ottobre 2024 . . . 7
7 ottobre 2024 . . . 8
9 settembre 2024 . . . 8
23 agosto 2024 . . . 8
22 agosto 2024 . . . 9
8 agosto 2024 . . . 9
10 giugno 2024 . . . 9
17 maggio 2024 . . . 9
23 aprile 2024 . . . 10
8 marzo 2024 . . . 10
5 marzo 2024 . . . 10
2 febbraio 2024 . . . 11
16 gennaio 2024 . . . 11
8 gennaio 2024 . . . 11
6 dicembre 2023 . . . 11
5 dicembre 2023 . . . 12
10 novembre 2023 . . . 12
8 novembre 2023 . . . 13
1 novembre 2023 . . . 13
23 ottobre 2023 . . . 13
6 ottobre 2023 . . . 13
10 settembre 2023 . . . 14
30 luglio 2023 . . . 14

26 luglio 2023 . . . 15
2 luglio 2023 . . . 15
26 giugno 2023 . . . 15
4 giugno 2023 . . . 15
7 maggio 2023 . . . 16
4 aprile 2023 . . . 16
3 aprile 2023 . . . 17
13 marzo 2023 . . . 18
5 marzo 2023 . . . 18
5 febbraio 2023 . . . 19
1 gennaio 2023 . . . 20
15 dicembre 2022 . . . 20
8 dicembre 2022 . . . 20
4 dicembre 2022 . . . 21
15 novembre 2022 . . . 21
6 novembre 2022 . . . 21
18 settembre 2022 . . . 22
31 luglio 2022 . . . 23
18 luglio 2022 . . . 24
3 luglio 2022 . . . 24
7 giugno 2022 . . . 25
2 maggio 2022 . . . 27
3 aprile 2022 . . . 29
27 febbraio 2022 . . . 29
9 febbraio 2022 . . . 29
6 febbraio 2022 . . . 30
30 gennaio 2022 . . . 30
2 gennaio 2022 . . . 30
28 novembre 2021 . . . 32
4 ottobre 2021 . . . 33
2 settembre 2021 . . . 33
7 luglio 2021 . . . 34
30 maggio 2021 . . . 36
24 maggio 2021 . . . 37
11 Apr 2021 . . . 37
8 marzo 2021 . . . 37
4 gennaio 2021 . . . 38
3 novembre 2020 . . . 40
Limitazioni note . . . 40
BlueXP non supporta la creazione di volumi FlexGroup . . . 40
BlueXP non supporta S3 con Cloud Volumes ONTAP . . . 40
BlueXP non supporta il disaster recovery per le VM di storage . . . 40
Note di rilascio di Cloud Volumes ONTAP . . . 41
Inizia subito . . . 42
Scopri di più su Cloud Volumes ONTAP . . . 42

Versioni di ONTAP supportate per le implementazioni Cloud Volumes ONTAP . . . 43
AWS . . . 43
Azure . . . 44
Google Cloud . . . 45
Inizia con Amazon Web Services . . . 46
Avvio rapido di Cloud Volumes ONTAP in AWS . . . 46
Pianificare la configurazione di Cloud Volumes ONTAP in AWS . . . 47
Configurare la rete . . . 51
Configura Cloud Volumes ONTAP per l'utilizzo di una chiave gestita dal cliente in AWS . . . 76
Configurare ruoli AWS IAM per i nodi Cloud Volumes ONTAP . . . 79
Impostare la licenza per Cloud Volumes ONTAP in AWS . . . 88
Avviare Cloud Volumes ONTAP in AWS . . . 95
Implementa Cloud Volumes ONTAP in AWS Secret Cloud o AWS Top Secret Cloud . . . 109
Inizia a utilizzare Microsoft Azure . . . 125
Scopri le opzioni di implementazione di Cloud Volumes ONTAP in Azure . . . 125
Inizia subito a BlueXP . . . 126
Implementa Cloud Volumes ONTAP dal marketplace di Azure . . . 178
Inizia a utilizzare Google Cloud . . . 181
Guida rapida per Cloud Volumes ONTAP in Google Cloud . . . 181
Pianificare la configurazione di Cloud Volumes ONTAP in Google Cloud . . . 183
Configura il networking di Google Cloud per Cloud Volumes ONTAP . . . 186
Configura i controlli del servizio VPC per implementare Cloud Volumes ONTAP in Google Cloud . . . 198
Creare un account di servizio Google Cloud per Cloud Volumes ONTAP . . . 200
Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP . . . 203
Impostare la licenza per Cloud Volumes ONTAP in Google Cloud . . . 204
Avviare Cloud Volumes ONTAP in Google Cloud . . . 209
Verifica dell'immagine della piattaforma Google Cloud . . . 222
USA Cloud Volumes ONTAP . . . 234
Gestione delle licenze . . . 234
Gestisci le licenze basate sulla capacità per Cloud Volumes ONTAP . . . 234
Gestione delle iscrizioni a Keystone tramite BlueXP . . . 240
Gestisci la licenza basata su nodi per Cloud Volumes ONTAP . . . 243
Amministrazione di volumi e LUN . . . 248
Creare un FlexVol volume su un sistema Cloud Volumes ONTAP . . . 248
Gestire i volumi su sistemi Cloud Volumes ONTAP . . . 255
Esegui il tiering dei dati Cloud Volumes ONTAP inattivi in uno storage a oggetti a basso costo . . . 265
Connettersi a un LUN su Cloud Volumes ONTAP dal sistema host . . . 272
Accelera l'accesso ai dati con i volumi FlexCache su un sistema Cloud Volumes ONTAP . . . 273
Amministrazione degli aggregati . . . 275
Crea un aggregato per i sistemi Cloud Volumes ONTAP . . . 275
Gestione degli aggregati per i cluster Cloud Volumes ONTAP . . . 277
Gestire la capacità aggregata Cloud Volumes ONTAP su un connettore . . . 278
Amministrazione delle macchine virtuali dello storage . . . 280
Gestione delle macchine virtuali di storage per Cloud Volumes ONTAP . . . 280
Gestisci le macchine virtuali dello storage di distribuzione dei dati per Cloud Volumes ONTAP in AWS 281

Gestisci le macchine virtuali dello storage di distribuzione dei dati per Cloud Volumes ONTAP in Azure 289
Gestisci le macchine virtuali dello storage di data-service per Cloud Volumes ONTAP in Google Cloud 292
Configurare il disaster recovery delle Storage VM per Cloud Volumes ONTAP . . . 295
Sicurezza e crittografia dei dati . . . 295
Crittografa i volumi su Cloud Volumes ONTAP con le soluzioni per la crittografia NetApp . . . 295
Gestisci le chiavi di crittografia Cloud Volumes ONTAP con il servizio di gestione delle chiavi AWS . . . 295
Gestisci le chiavi di crittografia Cloud Volumes ONTAP con il vault delle chiavi di Azure . . . 296
Gestire le chiavi di crittografia Cloud Volumes ONTAP con il servizio KMS di Google Cloud . . . 304
Abilita le soluzioni di protezione dal ransomware NetApp per Cloud Volumes ONTAP . . . 306
Crea copie Snapshot a prova di manomissione dei file WORM su Cloud Volumes ONTAP . . . 309
Amministrazione del sistema . . . 310
Aggiornare il software Cloud Volumes ONTAP . . . 310
Registrare sistemi Cloud Volumes ONTAP pay-as-you-go . . . 319
Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità . . . 321
Avviare e arrestare un sistema Cloud Volumes ONTAP . . . 323
Sincronizzare l’ora del sistema Cloud Volumes ONTAP utilizzando il server NTP . . . 326
Modificare la velocità di scrittura del sistema . . . 326
Modificare la password di amministrazione del cluster Cloud Volumes ONTAP . . . 328
Aggiungere, rimuovere o eliminare sistemi . . . 329
Amministrazione di AWS . . . 333
Amministrazione di Azure . . . 336
Amministrazione di Google Cloud . . . 348
Amministrare Cloud Volumes ONTAP utilizzando Gestione di sistema . . . 349
Amministrare Cloud Volumes ONTAP dalla CLI . . . 352
Stato ed eventi del sistema . . . 352
Verificare la configurazione di AutoSupport per Cloud Volumes ONTAP . . . 353
Configurare EMS per i sistemi Cloud Volumes ONTAP . . . 356
Concetti . . . 357
Licensing . . . 357
Licensing per Cloud Volumes ONTAP . . . 357
Scopri di più sulle licenze basate sulla capacità per Cloud Volumes ONTAP . . . 361
Storage . . . 365
Protocolli client supportati per Cloud Volumes ONTAP . . . 365
Dischi e aggregati utilizzati per i cluster Cloud Volumes ONTAP . . . 366
Scopri di più sul supporto per volumi elastici AWS con Cloud Volumes ONTAP . . . 369
Scopri di più sul tiering dei dati con Cloud Volumes ONTAP in AWS, Azure o Google Cloud . . . 375
Gestione dello storage Cloud Volumes ONTAP . . . 380
Velocità di scrittura . . . 382
Flash cache . . . 385
Scopri lo storage WORM su Cloud Volumes ONTAP . . . 386
Coppie ad alta disponibilità . . . 388
Scopri di più sulle coppie ha di Cloud Volumes ONTAP in AWS . . . 388
Scopri di più sulle coppie ha di Cloud Volumes ONTAP in Azure . . . 395
Scopri di più sulle coppie ha di Cloud Volumes ONTAP in Google Cloud . . . 401
Operazioni non disponibili quando un nodo nella coppia ha Cloud Volumes ONTAP è offline . . . 406

Scopri la crittografia dei dati e la protezione dal ransomware di Cloud Volumes ONTAP . . . 407
Crittografia dei dati inattivi . . . 407
Scansione virus ONTAP . . . 409
Protezione ransomware . . . 409
Scopri il monitoraggio delle performance per i workload Cloud Volumes ONTAP . . . 410
Report tecnici sulle performance . . . 410
Performance della CPU . . . 410
Gestione delle licenze per BYOL basato su nodo . . . 410
Licenze di sistema BYOL . . . 410
Gestione delle licenze per un nuovo sistema . . . 411
Scadenza della licenza . . . 411
Rinnovo della licenza . . . 412
Trasferimento della licenza a un nuovo sistema . . . 412
Scopri in che modo AutoSupport e Digital Advisor vengono utilizzati per Cloud Volumes ONTAP . . . 413
Configurazioni predefinite supportate per Cloud Volumes ONTAP . . . 414
Impostazione predefinita . . . 414
Dischi interni per i dati di sistema . . . 415
Conoscenza e supporto . . . 419
Registrati per ricevere assistenza . . . 419
Panoramica sulla registrazione del supporto . . . 419
Registrare BlueXP per ricevere assistenza NetApp . . . 419
Associare le credenziali NSS per il supporto Cloud Volumes ONTAP . . . 422
Richiedi assistenza . . . 423
Ottieni supporto per un file service del cloud provider . . . 423
Utilizzare le opzioni di supporto automatico . . . 424
Crea un caso con il supporto NetApp . . . 424
Gestire i casi di supporto (anteprima) . . . 426
Note legali . . . 429
Copyright . . . 429
Marchi . . . 429
Brevetti . . . 429
Direttiva sulla privacy . . . 429
Open source . . . 429

Documentazione Cloud Volumes ONTAP

Note di rilascio

Novità di Cloud Volumes ONTAP

Scopri le novità della gestione Cloud Volumes ONTAP in BlueXP.

I miglioramenti descritti in questa pagina sono specifici delle funzionalità di BlueXP che consentono la gestione di Cloud Volumes ONTAP. Per scoprire le novità del software Cloud Volumes ONTAP, "Vai alle Note di rilascio di Cloud Volumes ONTAP".

11 agosto 2025

Fine della disponibilità delle licenze ottimizzate

A partire dall'11 agosto 2025, la licenza Cloud Volumes ONTAP Optimized sarà deprecata e non sarà più disponibile per l'acquisto o il rinnovo nei marketplace di Azure e Google Cloud per gli abbonamenti con pagamento in base al consumo (PAYGO). Se hai un contratto annuale con una licenza Optimized, puoi continuare a utilizzare la licenza fino alla scadenza del contratto. Quando la licenza Optimized scade, puoi optare per le licenze Cloud Volumes ONTAP Essentials o Professional in BlueXP.

Tuttavia, la possibilità di aggiungere o rinnovare le licenze ottimizzate sarà disponibile tramite le API.

Per informazioni sui pacchetti di licenza, fare riferimento a "Licensing per Cloud Volumes ONTAP" .

Per informazioni sul passaggio a un metodo di ricarica diverso, fare riferimento a "Gestire le licenze basate sulla capacità" .

14 luglio 2025

Supporto per proxy trasparente

BlueXP ora supporta server proxy trasparenti oltre alle connessioni proxy esplicite esistenti. Durante la creazione o la modifica del connettore BlueXP , è possibile configurare un server proxy trasparente per gestire in modo sicuro il traffico di rete da e verso Cloud Volumes ONTAP.

Per ulteriori informazioni sull'utilizzo dei server proxy in Cloud Volumes ONTAP, fare riferimento a:

- "Configurazioni di rete per supportare il proxy del connettore in AWS"
- "Configurazioni di rete per supportare il proxy del connettore in Azure"
- "Configurazioni di rete per supportare il proxy del connettore in Google Cloud"

Nuovo tipo di VM supportato per Cloud Volumes ONTAP in Azure

A partire da Cloud Volumes ONTAP 9.13.1, L8s_v3 è supportato come tipo di VM nelle zone di disponibilità singole e multiple di Azure, sia per le distribuzioni di coppie ad alta disponibilità (HA) nuove che esistenti.

Per ulteriori informazioni, fare riferimento a "Configurazioni supportate in Azure".

25 giugno 2025

Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP

A partire dal 25 giugno 2025, NetApp ha limitato il modello di licenza Bring Your Own License (BYOL) per Cloud Volumes ONTAP. La restrizione si applica a tutti i clienti e a tutte le distribuzioni Cloud Volumes ONTAP in AWS, Azure e Google Cloud. Le uniche eccezioni riguardano i clienti del settore pubblico statunitense e le distribuzioni nella regione Cina.

Il supporto e i servizi NetApp continueranno fino alla scadenza del contratto BYOL, ma le licenze scadute non verranno rinnovate né estese. Alla scadenza delle licenze BYOL, è necessario sostituirle con licenze basate sulla capacità acquistate tramite gli abbonamenti al marketplace cloud. Un modello di licenza basato sulla capacità, tramite i marketplace hyperscaler, semplifica l'esperienza di gestione delle licenze e offre maggiori vantaggi aziendali. Contatta il team Account NetApp o i rappresentanti del Customer Success per discutere le opzioni di conversione.

Per ulteriori informazioni, fare riferimento a questo comunicato clienti: "CPC-00661: Modifiche alla politica BYOL Cloud Volumes ONTAP" .

29 maggio 2025

Implementazioni in modalità privata abilitate per Cloud Volumes ONTAP 9.15.1

Ora puoi implementare Cloud Volumes ONTAP 9.15.1 in modalità privata in AWS, Azure e Google Cloud. La modalità privata è abilitata per implementazioni a nodo singolo e high Availability (ha) di Cloud Volumes ONTAP 9.15.1.

Per ulteriori informazioni sulle implementazioni in modalità privata, fare riferimento a "Scopri le modalità di implementazione di BlueXP".

12 maggio 2025

Rilevamento delle implementazioni effettuate attraverso il marketplace Azure in BlueXP

BlueXP ora dispone della capacità di rilevare i sistemi Cloud Volumes ONTAP implementati direttamente attraverso il marketplace di Azure. Questo significa che ora puoi aggiungere e gestire questi sistemi come ambienti di lavoro in BlueXP , proprio come qualsiasi altro sistema Cloud Volumes ONTAP.

"Implementa Cloud Volumes ONTAP dal marketplace di Azure"

16 aprile 2025

Nuove regioni supportate in Azure

Ora puoi implementare Cloud Volumes ONTAP 9.12.1 GA e versioni successive in zone di disponibilità singole e multiple in Azure nelle seguenti regioni. Supporto per implementazioni a nodo singolo e high Availability (ha).

- Spagna Centrale
- Messico Centrale

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

14 aprile 2025

Creazione automatizzata di macchine virtuali di storage tramite le API in Google Cloud

Ora puoi utilizzare le API BlueXP per automatizzare la creazione della macchina virtuale per lo storage in Google Cloud. Hai utilizzato questa funzionalità nelle configurazioni ad alta disponibilità (ha) di Cloud Volumes ONTAP, che è possibile utilizzare anche in implementazioni a nodo singolo. Utilizzando le API BlueXP , puoi creare, rinominare ed eliminare con facilità macchine virtuali storage di altri servizi dati nel tuo ambiente Google Cloud, senza dover configurare manualmente le interfacce di rete, le LIF e le LIF di gestione richieste. Questa automazione semplifica il processo di gestione delle macchine virtuali storage.

"Gestisci le macchine virtuali dello storage di data-service per Cloud Volumes ONTAP in Google Cloud"

3 aprile 2025

Supporto per le regioni della Cina per Cloud Volumes ONTAP 9.13.1 in AWS

Ora puoi implementare Cloud Volumes ONTAP 9.13.1 in AWS nelle aree geografiche Cina. Supporto per implementazioni a nodo singolo e high Availability (ha). Dopo aver distribuito Cloud Volumes ONTAP 9.13.1, è possibile aggiornarlo alle versioni successive. Sono supportate solo le licenze acquistate direttamente da NetApp.

Per la disponibilità regionale, fare riferimento alla "Mappe delle regioni globali per Cloud Volumes ONTAP" .

28 marzo 2025

Implementazioni in modalità privata abilitate per Cloud Volumes ONTAP 9.14.1

Ora puoi implementare Cloud Volumes ONTAP 9.14.1 in modalità privata in AWS, Azure e Google Cloud. La modalità privata è abilitata per implementazioni a nodo singolo e high Availability (ha) di Cloud Volumes ONTAP 9.14.1.

Per ulteriori informazioni sulle implementazioni in modalità privata, fare riferimento a "Scopri le modalità di implementazione di BlueXP".

12 marzo 2025

Nuove regioni supportate per le implementazioni di zone di disponibilità multiple in Azure

Le seguenti regioni ora supportano le implementazioni ha di zone di disponibilità multiple in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Stati Uniti centrali
- US Gov Virginia (Regione del Governo degli Stati Uniti - Virginia)

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

10 marzo 2025

Creazione di macchine virtuali di storage automatizzata tramite le API in Azure

Ora puoi utilizzare le API di BlueXP per creare, rinominare ed eliminare macchine virtuali storage di servizi dati aggiuntivi per Cloud Volumes ONTAP in Azure. L'utilizzo delle API automatizza il processo di creazione della VM di storage, includendo la configurazione delle interfacce di rete richieste, delle LIF e di una LIF di gestione, se devi utilizzare una VM di storage per scopi di gestione.

"Gestisci le macchine virtuali dello storage di distribuzione dei dati per Cloud Volumes ONTAP in Azure"

6 marzo 2025

Cloud Volumes ONTAP 9.16.1 GA

Ora puoi utilizzare BlueXP per implementare e gestire la release della disponibilità generale di Cloud Volumes ONTAP 9.16.1 in Azure e Google Cloud. Tuttavia, questa versione non è disponibile per l'implementazione e l'aggiornamento in AWS.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

03 marzo 2025

Supporto della regione del Nord della Nuova Zelanda in Azure

La regione del Nord della Nuova Zelanda è ora supportata in Azure per configurazioni a nodo singolo e ad alta disponibilità (ha) di Cloud Volumes ONTAP 9.12.1 GA e versioni successive. Si noti che il tipo di istanza Lsv3 non è supportato in questa regione.

Per un elenco di tutte le regioni supportate, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

18 febbraio 2025

Presentazione dell'implementazione diretta del marketplace di Azure

Ora puoi sfruttare l'implementazione diretta del marketplace di Azure per implementare in modo semplice e rapido Cloud Volumes ONTAP direttamente dal marketplace di Azure. Utilizzando questo metodo ottimizzato, puoi esplorare le caratteristiche e le funzionalità principali di Cloud Volumes ONTAP nel tuo ambiente senza dover configurare BlueXP Connector o soddisfare altri criteri di onboarding richiesti per la distribuzione di Cloud Volumes ONTAP tramite BlueXP .

- "Scopri le opzioni di implementazione di Cloud Volumes ONTAP in Azure"
- "Implementa Cloud Volumes ONTAP dal marketplace di Azure"

10 febbraio 2025

Autenticazione utente abilitata per l'accesso a Gestione sistema da BlueXP

In qualità di amministratore BlueXP , è ora possibile attivare l'autenticazione per gli utenti ONTAP che accedono a Gestione sistema ONTAP da BlueXP . È possibile attivare questa opzione modificando le impostazioni del connettore BlueXP . Questa opzione è disponibile per le modalità standard e privata.

"Amministrare Cloud Volumes ONTAP utilizzando Gestione di sistema".

Visualizzazione avanzata BlueXP rinominata in Gestione sistema

L'opzione per la gestione avanzata di Cloud Volumes ONTAP da BlueXP tramite Gestione di sistema di ONTAP è stata rinominata da **visualizzazione avanzata** a **Gestione di sistema**.

"Amministrare Cloud Volumes ONTAP utilizzando Gestione di sistema".

Ecco un modo più semplice per gestire le licenze con il portafoglio digitale di BlueXP

Ora puoi usufruire di una gestione semplificata delle licenze Cloud Volumes ONTAP utilizzando punti di navigazione migliorati all'interno del Digital Wallet di BlueXP :

- Accedi facilmente alle informazioni sulla tua licenza Cloud Volumes ONTAP tramite le schede **Governance > Digital Wallet > Panoramica/licenze dirette**.
- Fare clic su **Visualizza** nel pannello ONTAP volume cloud nella scheda **Panoramica** per ottenere una conoscenza completa delle licenze basate sulla capacità. Questa visualizzazione avanzata offre informazioni dettagliate su licenze e abbonamenti.
- Se si preferisce l'interfaccia precedente, è possibile fare clic sul pulsante **passa alla visualizzazione precedente** per visualizzare i dettagli della licenza in base al tipo e modificare i metodi di addebito per le licenze.

"Gestione delle licenze basate sulla capacità".

9 dicembre 2024

Elenco delle VM supportate aggiornate per Azure per allinearle alle Best practice

Le famiglie di macchine DS_v2 ed es_v3 non sono più disponibili per la selezione in BlueXP quando si distribuiscono nuove istanze di Cloud Volumes ONTAP in Azure. Queste famiglie verranno conservate e supportate solo nei sistemi esistenti più vecchi. Le nuove implementazioni di Cloud Volumes ONTAP sono supportate in Azure solo a partire dalla release 9.12.1. Si consiglia di passare a es_v4 o a qualsiasi altra serie compatibile con Cloud Volumes ONTAP 9.12.1 e versioni successive. Le macchine delle serie DS_v2 ed es_v3, tuttavia, saranno disponibili per le nuove implementazioni effettuate tramite l'API.

"Configurazioni supportate in Azure"

11 novembre 2024

Fine della disponibilità per le licenze basate su nodi

NetApp ha pianificato la fine della disponibilità (EOA) e la fine del supporto (EOS) della licenza basata su nodi Cloud Volumes ONTAP. A partire dal 11 novembre 2024, la disponibilità limitata delle licenze basate su nodi è stata interrotta. Il supporto per le licenze basate su nodi termina il 31 dicembre 2024. Dopo la fine delle licenze basate su nodi, è necessario passare alla licenza basata sulla capacità utilizzando il tool di conversione delle licenze BlueXP .

Per gli impegni annuali o a lungo termine, NetApp consiglia di contattare il rappresentante NetApp prima della data di fine disponibilità o della data di scadenza della licenza, per verificare che siano in essere i prerequisiti per la transizione. Se non disponi di un contratto a lungo termine per un nodo Cloud Volumes ONTAP ed esegui il sistema su un abbonamento PAY-as-you-go (PAYGO) on-demand, è importante pianificare la conversione prima della data dell'EOS. Sia per i contratti a lungo termine che per gli abbonamenti a PAYGO, è possibile utilizzare lo strumento di conversione delle licenze BlueXP per una conversione perfetta.

"Fine della disponibilità delle licenze basate su nodi" "Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità"

Rimozione di implementazioni basate su nodi da BlueXP

L'opzione di implementare i sistemi Cloud Volumes ONTAP utilizzando licenze basate su nodi è obsoleta in BlueXP . Ad eccezione di alcuni casi speciali, non puoi utilizzare le licenze basate su nodi per le

implementazioni Cloud Volumes ONTAP per qualsiasi cloud provider.

NetApp riconosce i seguenti requisiti di licenza esclusivi in conformità con obblighi contrattuali e esigenze operative e continuerà a supportare le licenze basate su nodi in queste situazioni:

- Clienti USA del settore pubblico
- Implementazioni in modalità privata
- Implementazioni nella regione cinese di Cloud Volumes ONTAP in AWS
- Se disponi di una BYOL (Bring Your Own License) valida e non scaduta

"Fine della disponibilità delle licenze basate su nodi"

Aggiunta di un Tier cold per i dati Cloud Volumes ONTAP nello storage BLOB di Azure

BlueXP ora ti permette di selezionare un Tier cold per archiviare i dati del Tier di capacità inattivi nell'storage BLOB di Azure. Aggiungendo il Tier cold ai Tier hot e cool esistenti potrai usufruire di un'opzione di storage più conveniente e di una maggiore efficienza dei costi.

"Tiering dei dati in Azure"

Possibilità di limitare l'accesso pubblico all'account di storage per Azure

Ora puoi limitare l'accesso pubblico al tuo account di storage per i sistemi Cloud Volumes ONTAP in Azure. Disattivando l'accesso, è possibile proteggere l'indirizzo IP privato dall'esposizione anche all'interno dello stesso VNET, qualora fosse necessario conformarsi ai criteri di protezione dell'organizzazione. Questa opzione consente inoltre di disabilitare il tiering dei dati per i sistemi Cloud Volumes ONTAP ed è applicabile sia alle coppie a nodo singolo che a quelle ad alta disponibilità.

"Regole del gruppo di sicurezza".

Abilitazione WORM dopo l'implementazione di Cloud Volumes ONTAP

Ora puoi attivare lo storage WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP esistente utilizzando BlueXP . Questa funzionalità offre la flessibilità di abilitare IL WORM in un ambiente di lavoro, anche se IL WORM non è stato attivato durante la sua creazione. Una volta attivato, non è possibile disattivare IL WORM.

"Abilitazione DI WORM in un ambiente di lavoro Cloud Volumes ONTAP"

25 ottobre 2024

Elenco delle VM supportate aggiornate per Google Cloud per allinearle alle Best practice

Le macchine della serie n1 non sono più disponibili per la selezione in BlueXP quando implementano nuove istanze di Cloud Volumes ONTAP in Google Cloud. Le macchine della serie n1 verranno conservate e supportate solo nei sistemi esistenti meno recenti. Le nuove implementazioni di Cloud Volumes ONTAP sono supportate in Google Cloud solo a partire dalla release 9,8. Si consiglia di passare ai tipi di macchine della serie n2 compatibili con Cloud Volumes ONTAP 9,8 e versioni successive. Le macchine della serie n1, tuttavia, saranno disponibili per le nuove implementazioni eseguite tramite l'API.

"Configurazioni supportate in Google Cloud".

Le zone locali supportano Amazon Web Services in modalità privata

Ora BlueXP supporta le zone locali di AWS per le implementazioni di alta disponibilità (ha) Cloud Volumes ONTAP in modalità privata. Il supporto che in precedenza era limitato solo alla modalità standard è stato ora esteso per includere la modalità privata.

Le zone locali di AWS non sono supportate quando si utilizza BlueXP in modalità limitata.

Per ulteriori informazioni sulle zone locali di AWS con implementazioni ha, fare riferimento a. "Zone locali di AWS".

7 ottobre 2024

Esperienza utente migliorata nella selezione delle versioni per l'aggiornamento

A partire da questa versione, quando si tenta di aggiornare Cloud Volumes ONTAP utilizzando la notifica BlueXP , si riceveranno indicazioni sulle versioni predefinite, più recenti e compatibili da utilizzare. Inoltre, ora è possibile selezionare l'ultima patch o la versione principale compatibile con l'istanza di Cloud Volumes ONTAP, oppure immettere manualmente una versione per l'aggiornamento.

"Aggiornare il software Cloud Volumes ONTAP"

9 settembre 2024

Le funzionalità WORM e ARP non sono più addebitabili

Le funzionalità di sicurezza e data Protection integrate di WORM (Write Once Read Many) e ARP (protezione autonoma dal ransomware) saranno offerte con le licenze Cloud Volumes ONTAP senza costi aggiuntivi. Il nuovo modello di prezzi si applica alle iscrizioni BYOL e PAYGO/Marketplace nuove ed esistenti di AWS, Azure e Google Cloud. Le licenze basate sulla capacità e su nodi conterranno ARP e WORM per tutte le configurazioni, incluse coppie ha (single node e high Availability), senza costi aggiuntivi.

Il prezzo semplificato offre i seguenti vantaggi:

- Gli account che attualmente includono WORM e ARP non saranno più addebitati per queste funzioni. In futuro, la fatturazione comporterà solo addebiti per l'utilizzo della capacità, come avveniva prima di questa modifica. WORM e ARP non saranno più inclusi nelle fatture future.
- Se i vostri conti correnti non includono queste caratteristiche, potete ora optare per il WORM e l'ARP senza costi aggiuntivi.
- Tutte le offerte Cloud Volumes ONTAP per ogni nuovo account escluderanno gli addebiti per WORM e ARP.

Ulteriori informazioni sulle seguenti funzioni:

- "Abilita le soluzioni di protezione dal ransomware NetApp per Cloud Volumes ONTAP"
- "Storage WORM"

23 agosto 2024

Regione del Canada occidentale ora supportata in AWS

La regione del Canada occidentale è ora supportata in AWS per Cloud Volumes ONTAP 9.12.1 GA e versioni

successive.

Per un elenco di tutte le regioni, vedere "Mappa delle regioni globali sotto AWS".

22 agosto 2024

Cloud Volumes ONTAP 9.15.1 GA

BlueXP può ora implementare e gestire la release General Availability di Cloud Volumes ONTAP 9.15.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

8 agosto 2024

Pacchetti di licenze Edge cache obsoleti

I pacchetti di licenza basati sulla capacità di Edge cache non saranno più disponibili per implementazioni future di Cloud Volumes ONTAP. Tuttavia, è possibile utilizzare l'API per utilizzare questa funzionalità.

Supporto minimo delle versioni per Flash cache in Azure

La versione minima di Cloud Volumes ONTAP richiesta per la configurazione di Flash cache in Azure è 9.13.1 GA. Puoi utilizzare ONTAP 9.13.1 GA e versioni successive solo per la distribuzione di Flash cache su sistemi Cloud Volumes ONTAP in Azure.

Per le configurazioni supportate, vedere "Configurazioni supportate in Azure".

Versioni di prova gratuite per gli abbonamenti al mercato obsolete

La licenza di prova automatica gratuita di 30 giorni o la licenza di valutazione per gli abbonamenti pay-as-you-go nel marketplace del cloud provider non sarà più disponibile in Cloud Volumes ONTAP. L'addebito per qualsiasi tipo di abbonamento al mercato (PAYGO o contratto annuale) sarà attivato dal primo utilizzo, senza alcun periodo di prova gratuito.

10 giugno 2024

Cloud Volumes ONTAP 9.15.0

BlueXP ora può implementare e gestire Cloud Volumes ONTAP 9.15.0 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

17 maggio 2024

Supporto per le zone locali di Amazon Web Services

Il supporto per le zone locali di AWS è ora disponibile per le implementazioni ha di Cloud Volumes ONTAP. Le zone locali di AWS sono un'implementazione dell'infrastruttura in cui storage, calcolo, database e altri servizi AWS selezionati sono situati vicino a grandi città e aree del settore.

Le zone locali di AWS sono supportate quando si utilizza BlueXP in modalità standard. Al momento, i zone locali di AWS non sono supportati quando si utilizza BlueXP in modalità limitata o privata.

Per ulteriori informazioni sulle zone locali di AWS con implementazioni ha, fare riferimento a. "Zone locali di AWS".

23 aprile 2024

Nuove regioni supportate per le implementazioni di zone di disponibilità multiple in Azure

Le seguenti regioni ora supportano le implementazioni ha di zone di disponibilità multiple in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Germania Centro Ovest
- Polonia centrale
- US 3 ovest
- Israele Centrale
- Italia Nord
- Canada centrale

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

Regione di Johannesburg ora supportata in Google Cloud

La regione di Johannesburg (`africa-south1` Regionale) è ora supportato in Google Cloud per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali in Google Cloud" .

Tag e modelli di volume non più supportati

Non è più possibile creare un volume da un modello o modificare i tag di un volume. Queste azioni sono state associate al servizio di correzione di BlueXP, che non è più disponibile.

8 marzo 2024

Supporto di Amazon Instant Metadata Service v2

In AWS, Cloud Volumes ONTAP, il mediatore e il connettore supportano ora Amazon Instant Metadata Service v2 (IMDSv2) per tutte le funzioni. IMDSv2 fornisce una maggiore protezione contro le vulnerabilità. In precedenza era supportato solo IMDSv1.

Se richiesto dai criteri di protezione, è possibile configurare le istanze EC2 in modo che utilizzino IMDSv2. Per istruzioni, fare riferimento a. "Documentazione di configurazione e amministrazione di BlueXP per la gestione dei connettori esistenti".

5 marzo 2024

Cloud Volumes ONTAP 9.14.1 GA

BlueXP può ora implementare e gestire la release General Availability di Cloud Volumes ONTAP 9.14.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

2 febbraio 2024

Supporto di macchine virtuali serie Edv5 in Azure

Cloud Volumes ONTAP ora supporta le seguenti macchine virtuali della serie Edv5 a partire dalla release 9.14.1.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Configurazioni supportate in Azure"

16 gennaio 2024

Release di patch in BlueXP

Le release delle patch sono disponibili in BlueXP solo per le tre versioni più recenti di Cloud Volumes ONTAP.

"Aggiornare Cloud Volumes ONTAP"

8 gennaio 2024

Nuove macchine virtuali per più zone di disponibilità di Azure

A partire da Cloud Volumes ONTAP 9.13.1, i seguenti tipi di macchine virtuali supportano le zone di disponibilità multiple Azure per le implementazioni di coppia ad alta disponibilità nuove ed esistenti:

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Configurazioni supportate in Azure"

6 dicembre 2023

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP ora può implementare e gestire Cloud Volumes ONTAP 9.14.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Limite massimo volume FlexVol 300 TiB

Ora puoi creare un volume FlexVol fino alle dimensioni massime di 300 TiB con System Manager e l'interfaccia a riga di comando di ONTAP a partire da Cloud Volumes ONTAP 9.12.1 P2 e 9.13.0 P2 e in BlueXP a partire da Cloud Volumes ONTAP 9.13.1.

- "Limiti di storage in AWS"
- "Limiti di storage in Azure"
- "Limiti di storage in Google Cloud"

5 dicembre 2023

Sono state introdotte le seguenti modifiche.

Nuovo supporto di regione in Azure

Supporto per regione a zona di disponibilità singola

Le seguenti regioni supportano ora implementazioni a zona di disponibilità singola altamente disponibili in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Tel Aviv
- Milano

Supporto di aree di disponibilità multiple

Le seguenti regioni ora supportano implementazioni a più zone di disponibilità altamente disponibili in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- India Centrale
- Norvegia Est
- Svizzera Nord
- Sud Africa, Nord
- Emirati Arabi Uniti Nord

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

10 novembre 2023

La seguente modifica è stata introdotta con la versione 3.9.35 del connettore.

La regione di Berlino ora è supportata in Google Cloud

La regione di Berlino è ora supportata in Google Cloud per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali in Google Cloud" .

8 novembre 2023

La seguente modifica è stata introdotta con la versione 3.9.35 del connettore.

La regione di Tel Aviv è ora supportata in AWS

La regione di Tel Aviv è ora supportata in AWS per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali sotto AWS" .

1 novembre 2023

La seguente modifica è stata introdotta con la versione 3.9.34 del connettore.

Regione dell'Arabia Saudita ora supportata in Google Cloud

La regione dell'Arabia Saudita è ora supportata in Google Cloud per Cloud Volumes ONTAP e nel connettore per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento alla "Mappa delle regioni globali in Google Cloud" .

23 ottobre 2023

La seguente modifica è stata introdotta con la versione 3.9.34 del connettore.

Nuove regioni supportate per le implementazioni ha a zone di disponibilità multiple in Azure

Le seguenti regioni in Azure ora supportano implementazioni a più zone di disponibilità altamente disponibili per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Australia Est
- Asia orientale
- Francia centrale
- Nord Europa
- Qatar Central
- Svezia centrale
- Europa occidentale
- Stati Uniti occidentali 2

Per un elenco di tutte le regioni che supportano più zone di disponibilità, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

6 ottobre 2023

La seguente modifica è stata introdotta con la versione 3.9.34 del connettore.

Cloud Volumes ONTAP 9.14.0

BlueXP può ora implementare e gestire la release di disponibilità generale di Cloud Volumes ONTAP 9.14.0 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

10 settembre 2023

La seguente modifica è stata introdotta con la versione 3.9.33 del connettore.

Supporto di macchine virtuali serie Lsv3 in Azure

I tipi di istanze L48s_v3 e L64s_v3 sono ora supportati con Cloud Volumes ONTAP in Azure per implementazioni a nodo singolo e coppia ad alta disponibilità con dischi gestiti condivisi in zone di disponibilità singole e multiple, a partire dalla release 9.13.1. Questi tipi di istanze supportano Flash cache.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in Azure"
"Visualizza i limiti di storage per Cloud Volumes ONTAP in Azure"

30 luglio 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.32 del connettore.

Flash cache e supporto ad alta velocità di scrittura in Google Cloud

Flash cache e alta velocità di scrittura possono essere attivate separatamente in Google Cloud per Cloud Volumes ONTAP 9.13.1 e versioni successive. È disponibile un'elevata velocità di scrittura su tutti i tipi di istanze supportati. Flash cache è supportata nei seguenti tipi di istanze:

- n2-standard-16
- n2-standard-32
- n2-standard-48
- n2-standard-64

È possibile utilizzare queste funzionalità separatamente o insieme nelle implementazioni a singolo nodo e a coppia ad alta disponibilità.

"Avviare Cloud Volumes ONTAP in Google Cloud"

Miglioramenti dei report sull'utilizzo

Sono ora disponibili diversi miglioramenti alle informazioni visualizzate nei report di utilizzo. Di seguito sono riportati i miglioramenti apportati ai report sull'utilizzo:

- L'unità TIB è ora inclusa nel nome delle colonne.
- È ora incluso un nuovo campo "nodi" per i numeri di serie.
- Una nuova colonna "tipo di carico di lavoro" è ora inclusa nel report sull'utilizzo delle VM di storage.
- I nomi degli ambienti di lavoro sono ora inclusi nei report sull'utilizzo delle VM di storage e dei volumi.
- Il tipo di volume "file" è ora denominato "Primary (Read/Write)" (primario (lettura/scrittura).
- Il tipo di volume "secondario" è ora denominato "secondario (DP)".

Per ulteriori informazioni sui rapporti sull'utilizzo, fare riferimento a "Scarica i report sull'utilizzo".

26 luglio 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.31 del connettore.

Cloud Volumes ONTAP 9.13.1 GA

BlueXP è ora in grado di implementare e gestire la release di disponibilità generale di Cloud Volumes ONTAP 9.13.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

2 luglio 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.31 del connettore.

Supporto per implementazioni di zone a disponibilità multipla in ha in Azure

La centrale giapponese orientale e coreana di Azure ora supporta implementazioni di zone ad alta disponibilità per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni che supportano più zone di disponibilità, fare riferimento alla "Mappa delle regioni globali sotto Azure" .

Supporto autonomo per la protezione ransomware

La protezione ransomware autonoma (ARP) è ora supportata su Cloud Volumes ONTAP. Il supporto ARP è disponibile su Cloud Volumes ONTAP versione 9.12.1 e successive.

Per ulteriori informazioni su ARP con Cloud Volumes ONTAP, fare riferimento a "Protezione ransomware autonoma".

26 giugno 2023

La seguente modifica è stata introdotta con la versione 3.9.30 del connettore.

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.13.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

4 giugno 2023

La seguente modifica è stata introdotta con la versione 3.9.30 del connettore.

Aggiornamento del selettore della versione di aggiornamento di Cloud Volumes ONTAP

Dalla pagina Upgrade Cloud Volumes ONTAP (aggiornamento versione), è possibile scegliere di eseguire l'aggiornamento alla versione più recente disponibile di Cloud Volumes ONTAP o a una versione precedente.

Per ulteriori informazioni sull'aggiornamento di Cloud Volumes ONTAP tramite BlueXP , consultare "Aggiornare Cloud Volumes ONTAP" .

7 maggio 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.29 del connettore.

Regione del Qatar ora supportata in Google Cloud

La regione del Qatar è ora supportata in Google Cloud per Cloud Volumes ONTAP e nel connettore per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Regione centrale della Svezia ora supportata in Azure

La regione centrale svedese è ora supportata in Azure per Cloud Volumes ONTAP e nel connettore per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Supporto per implementazioni di zone ad alta disponibilità multiple in Azure Australia East

La regione orientale australiana di Azure ora supporta implementazioni di zone ad alta disponibilità per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Guasto nell'utilizzo della carica

Ora puoi scoprire cosa ti verrà addebitato quando sei iscritto a licenze basate sulla capacità. I seguenti tipi di report sull'utilizzo sono disponibili per il download dal portafoglio digitale in BlueXP. I 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 possono essere facilmente condivisi con altri.

- Utilizzo del pacchetto Cloud Volumes ONTAP
- Utilizzo di alto livello
- Utilizzo delle VM di storage
- Utilizzo dei volumi

Per ulteriori informazioni, fare riferimento a "Gestione delle licenze basate sulla capacità".

Viene ora visualizzata una notifica quando si accede a BlueXP senza un abbonamento al marketplace

Viene visualizzata una notifica ogni volta che si accede a Cloud Volumes ONTAP in BlueXP senza un abbonamento al marketplace. La notifica indica "è necessario un abbonamento al mercato per questo ambiente di lavoro per essere conforme ai termini e alle condizioni di Cloud Volumes ONTAP".

4 aprile 2023

Supporto per le regioni in Cina per AWS

A partire da Cloud Volumes ONTAP 9.12.1 GA, le regioni della Cina sono ora supportate in AWS come segue.

- Sono supportati i sistemi a nodo singolo.
- Sono supportate le licenze acquistate direttamente da NetApp.

Per la disponibilità regionale, fare riferimento alla "Mappe delle regioni globali per Cloud Volumes ONTAP".

3 aprile 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.28 del connettore.

Regione di Torino ora supportata in Google Cloud

La regione di Torino è ora supportata in Google Cloud per Cloud Volumes ONTAP e nel connettore per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Ottimizzazione del portafoglio digitale BlueXP

Il portafoglio digitale BlueXP ora mostra la capacità concessa in licenza acquistata con le offerte private Marketplace.

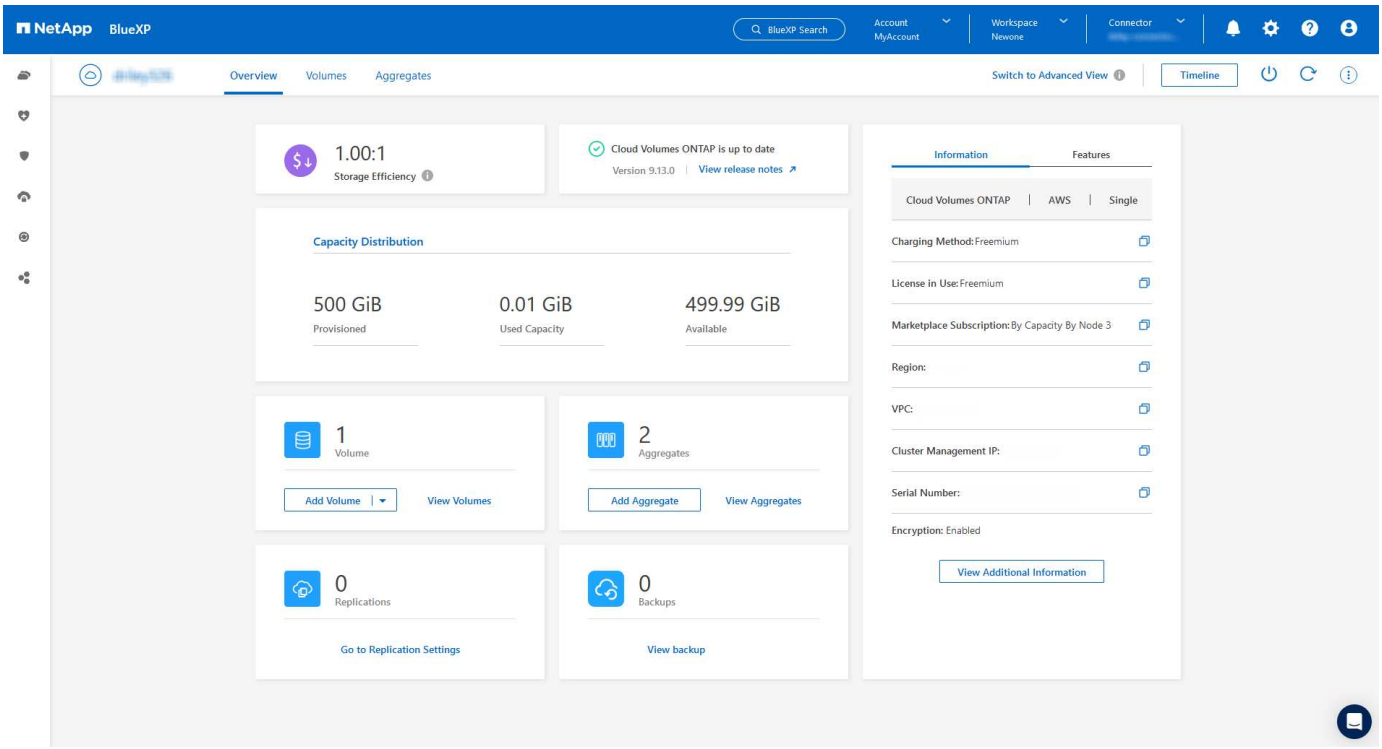
"Scopri come visualizzare la capacità consumata nel tuo account".

Supporto per i commenti durante la creazione del volume

Questa versione consente di creare commenti durante la creazione di un volume Cloud Volumes ONTAP FlexGroup o FlexVol quando si utilizza l'API.

Riprogettazione dell'interfaccia utente di BlueXP per le pagine Panoramica, volumi e aggregati di Cloud Volumes ONTAP

BlueXP dispone ora di un'interfaccia utente riprogettata per le pagine Panoramica, volumi e aggregati di Cloud Volumes ONTAP. Il design basato su sezioni presenta informazioni più complete in ogni sezione per una migliore esperienza utente.

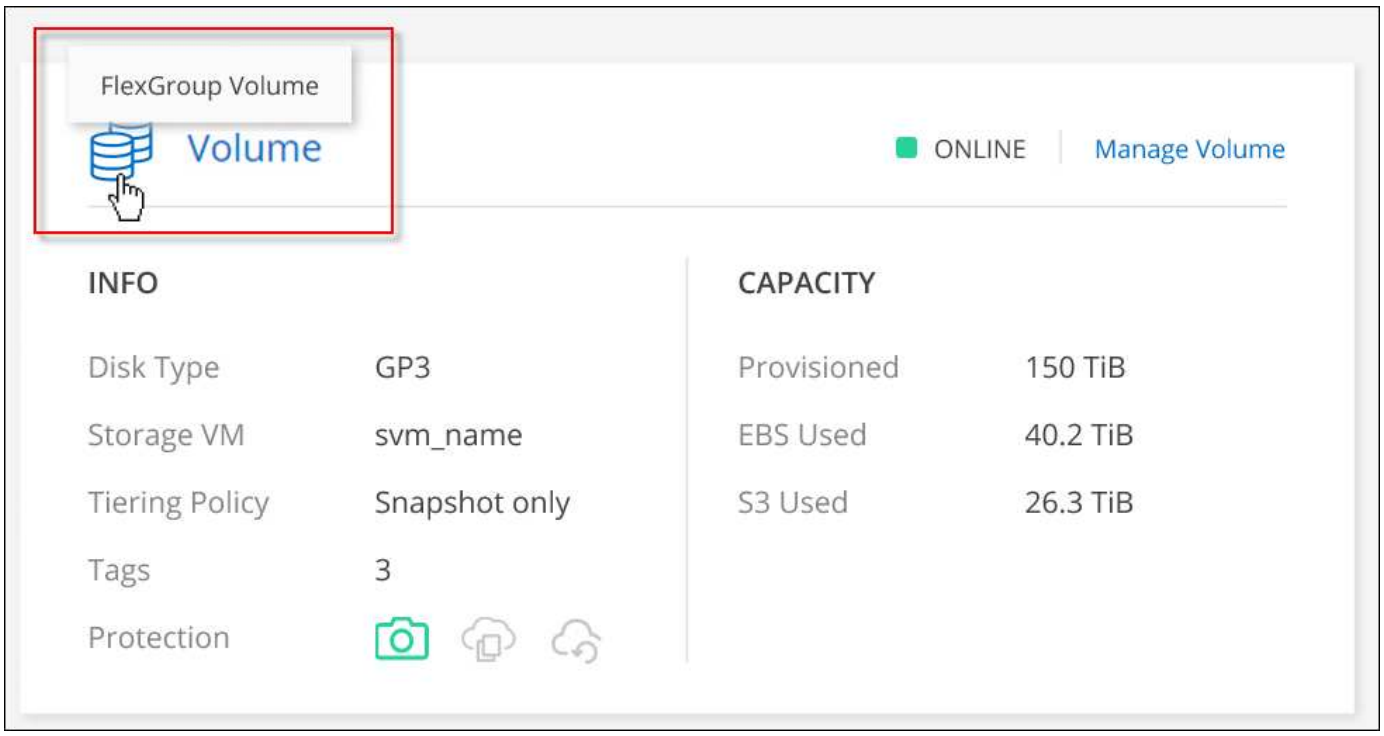


Volumi FlexGroup visualizzabili tramite Cloud Volumes ONTAP

I volumi FlexGroup creati tramite ONTAP System Manager o la CLI di ONTAP sono ora visualizzabili tramite il riquadro dei volumi riprogettati in BlueXP . Identico alle informazioni fornite per i volumi FlexVol, BlueXP

fornisce informazioni dettagliate per i volumi FlexGroup creati attraverso una sezione dedicata ai volumi.

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.



"Scopri di più sulla visualizzazione dei volumi FlexGroup creati."

13 marzo 2023

Supporto per le regioni della Cina in Azure

Cina l'area nord-3 è ora supportata per le implementazioni a nodo singolo di Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA in Azure. In queste regioni sono supportate solo le licenze acquistate direttamente da NetApp (licenze BYOL).

Le nuove implementazioni di Cloud Volumes ONTAP nelle regioni cinesi sono supportate solo in 9.12.1 GA e 9.13.0 GA. È possibile aggiornare queste versioni a patch e release successive di Cloud Volumes ONTAP. Se si desidera distribuire versioni Cloud Volumes ONTAP successive nelle aree geografiche della Cina, contattare il supporto NetApp.

Per la disponibilità regionale, fare riferimento alla "Mappe delle regioni globali per Cloud Volumes ONTAP".

5 marzo 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.27 del connettore.

Cloud Volumes ONTAP 9.13.0

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.13.0 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Supporto di 16 TIB e 32 Tib in Azure

Cloud Volumes ONTAP ora supporta dimensioni dei dischi 16 TiB e 32 TiB per le implementazioni ad alta disponibilità in esecuzione su dischi gestiti in Azure.

Scopri di più "Dimensioni dei dischi supportate in Azure".

Licenza MTEKM

La licenza di gestione delle chiavi di crittografia multi-tenant (MTEKM) è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti con versione 9.12.1 GA o successiva.

La gestione delle chiavi esterne multi-tenant consente alle singole macchine virtuali di storage (SVM) di mantenere le proprie chiavi attraverso un server KMIP quando si utilizza NetApp Volume Encryption.

"Scopri come crittografare i volumi con le soluzioni di crittografia NetApp".

Supporto per ambienti senza Internet

Cloud Volumes ONTAP è ora supportato in qualsiasi ambiente cloud con isolamento completo da Internet. In questi ambienti è supportata solo la licenza basata su nodo (BYOL). Le licenze basate sulla capacità non sono supportate. Per iniziare, installare manualmente il software Connector, accedere alla console BlueXP in esecuzione sul connettore, aggiungere la licenza BYOL al portafoglio digitale BlueXP, quindi implementare Cloud Volumes ONTAP.

- "Installare il connettore in una posizione senza accesso a Internet"
- "Accedere alla console BlueXP sul connettore"
- "Aggiungere una licenza non assegnata"

Flash cache e alta velocità di scrittura in Google Cloud

Il supporto per Flash cache, alta velocità di scrittura e un'unità di trasmissione massima (MTU) elevata di 8,896 byte è ora disponibile per alcune istanze con Cloud Volumes ONTAP 9.13.0.

Scopri di più "Configurazioni supportate da licenza per Google Cloud".

5 febbraio 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.26 del connettore.

Creazione di un gruppo di posizionamento in AWS

È ora disponibile una nuova impostazione di configurazione per la creazione di gruppi di posizionamento con implementazioni AWS ha Single Availability zone (AZ). Ora puoi scegliere di ignorare le creazioni di gruppi di posizionamento non riuscite e consentire il completamento delle implementazioni di AWS ha singolo AZ.

Per informazioni dettagliate su come configurare l'impostazione di creazione del gruppo di posizionamento, fare riferimento alla "Configurare la creazione di gruppi di posizionamento per AWS ha Single AZ".

Aggiornamento della configurazione della zona DNS privata

È ora disponibile una nuova impostazione di configurazione che consente di evitare di creare un collegamento tra una zona DNS privata e una rete virtuale quando si utilizzano i collegamenti privati di Azure. La creazione è attivata per impostazione predefinita.

"Fornisci a BlueXP i dettagli sul tuo Azure Private DNS"

Storage WORM e tiering dei dati

È ora possibile abilitare sia il tiering dei dati che lo storage WORM insieme quando si crea un sistema Cloud Volumes ONTAP 9.8 o successivo. L'abilitazione del tiering dei dati con lo storage WORM consente di eseguire il tiering dei dati in un archivio di oggetti nel cloud.

"Scopri di più sullo storage WORM."

1 gennaio 2023

Le seguenti modifiche sono state introdotte con la versione 3.9.25 del connettore.

Pacchetti di licenza disponibili in Google Cloud

I pacchetti di licenza ottimizzati e basati sulla capacità di Edge cache sono disponibili per Cloud Volumes ONTAP nel Google Cloud Marketplace come offerta pay-as-you-go o come contratto annuale.

Fare riferimento alla "Licenze Cloud Volumes ONTAP".

Configurazione predefinita per Cloud Volumes ONTAP

La licenza di gestione delle chiavi di crittografia multi-tenant (MTEKM) non è più inclusa nelle nuove implementazioni di Cloud Volumes ONTAP.

Per ulteriori informazioni sulle licenze della funzione ONTAP installate automaticamente con Cloud Volumes ONTAP, fare riferimento a "Configurazione predefinita per Cloud Volumes ONTAP".

15 dicembre 2022

Cloud Volumes ONTAP 9.12.0

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.12.0 in AWS e Google Cloud.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

8 dicembre 2022

Cloud Volumes ONTAP 9.12.1

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.12.1, che include il supporto per nuove funzionalità e aree di cloud provider aggiuntive.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP"

4 dicembre 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.24 del connettore.

BACKUP WORM + cloud ora disponibile durante la creazione di Cloud Volumes ONTAP

La possibilità di attivare sia le funzionalità di backup write once, Read Many (WORM) che cloud è ora disponibile durante il processo di creazione di Cloud Volumes ONTAP.

Regione di Israele ora supportata in Google Cloud

La regione di Israele è ora supportata in Google Cloud per Cloud Volumes ONTAP e nel connettore per Cloud Volumes ONTAP 9.11.1 P3 e versioni successive.

15 novembre 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.23 del connettore.

Licenza ONTAP S3 in Google Cloud

Una licenza ONTAP S3 è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.12.1 o successiva nella piattaforma Google Cloud.

"Documentazione di ONTAP: Scopri come configurare e gestire i servizi di storage a oggetti S3"

6 novembre 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.23 del connettore.

Spostamento dei gruppi di risorse in Azure

È ora 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.

Per ulteriori informazioni, fare riferimento a "Spostamento dei gruppi di risorse".

Certificazione NDMP-copy

NDMP-copy è ora certificato per l'utilizzo con Cloud Volume ONTAP.

Per informazioni sulla configurazione e l'utilizzo di NDMP, fare riferimento alla "Documentazione ONTAP: Panoramica sulla configurazione di NDMP" .

Supporto della crittografia dei dischi gestita per Azure

È stata aggiunta una nuova autorizzazione Azure che consente di crittografare tutti i dischi gestiti al momento della creazione.

Per ulteriori informazioni su questa nuova funzionalità, fare riferimento a "Impostare Cloud Volumes ONTAP in modo che utilizzi una chiave gestita dal cliente in Azure".

18 settembre 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.22 del connettore.

Miglioramenti del portafoglio digitale

- Il portafoglio digitale mostra ora un riepilogo del pacchetto di licenze i/o ottimizzato e della capacità WORM fornita per i sistemi Cloud Volumes ONTAP nell'intero account.

  Questi dettagli possono aiutarti a capire meglio come ti vengono addebitati i costi e se hai bisogno di acquistare capacità aggiuntiva.

  "Scopri come visualizzare la capacità consumata nel tuo account".

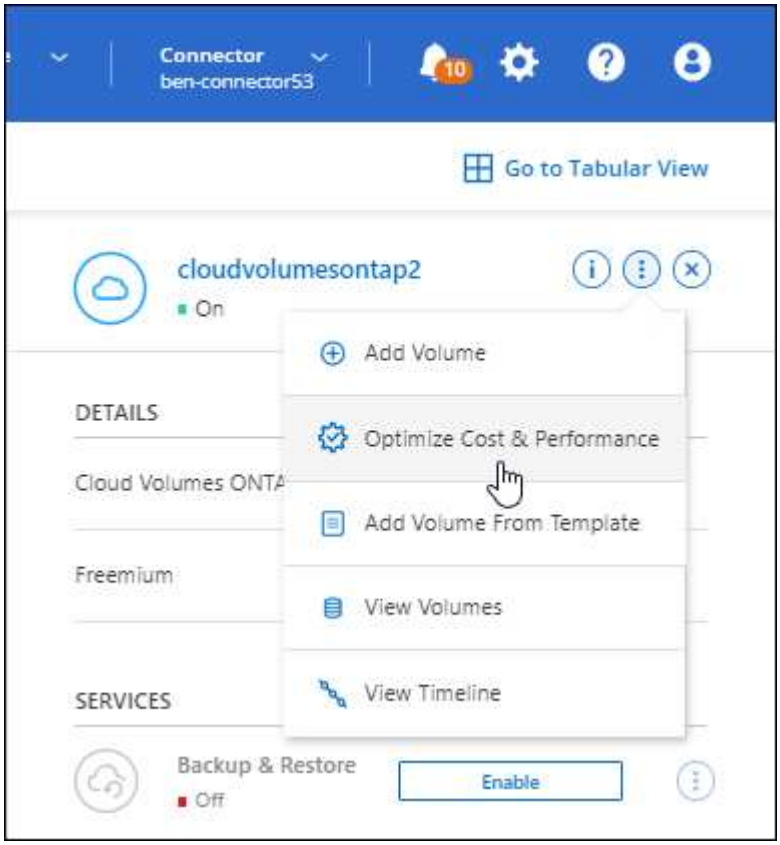
- È ora possibile passare da un metodo di ricarica a un metodo di ricarica ottimizzato.

  "Scopri come modificare i metodi di ricarica".

Ottimizza costi e performance

Ora puoi ottimizzare i costi e le performance di un sistema Cloud Volumes ONTAP direttamente da Canvas.

Dopo aver selezionato un ambiente di lavoro, è possibile scegliere l'opzione **Ottimizza costi e performance** per modificare il tipo di istanza per Cloud Volumes ONTAP. La scelta di un'istanza di dimensioni più piccole può aiutarti a ridurre i costi, mentre il passaggio a un'istanza di dimensioni più grandi può aiutarti a ottimizzare le performance.



Notifiche AutoSupport

BlueXP genererà ora una notifica se un sistema Cloud Volumes ONTAP non è in grado di inviare messaggi AutoSupport. La notifica include un collegamento alle istruzioni che è possibile utilizzare per risolvere i problemi di rete.

31 luglio 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.21 del connettore.

Licenza MTEKM

La licenza per la gestione delle chiavi di crittografia multi-tenant (MTEKM) è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti con versione 9.11.1 o successiva.

La gestione delle chiavi esterne multi-tenant consente alle singole macchine virtuali di storage (SVM) di mantenere le proprie chiavi attraverso un server KMIP quando si utilizza NetApp Volume Encryption.

"Scopri come crittografare i volumi con le soluzioni di crittografia NetApp".

Server proxy

BlueXP configura automaticamente i sistemi Cloud Volumes ONTAP per l'utilizzo del connettore come server proxy, se non è disponibile una connessione Internet in uscita per l'invio di messaggi AutoSupport.

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

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.

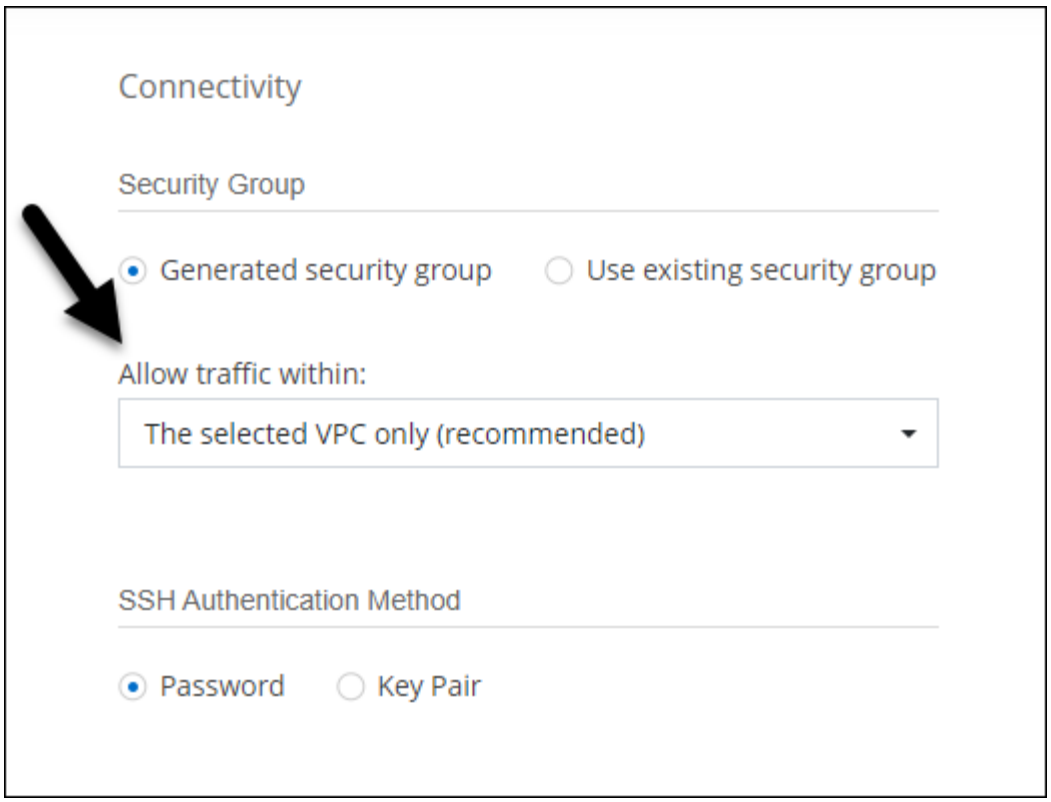
Modificare il metodo di ricarica

È ora possibile modificare il metodo di addebito per un sistema Cloud Volumes ONTAP che utilizza licenze basate sulla capacità. Ad esempio, se hai implementato un sistema Cloud Volumes ONTAP con il pacchetto Essentials, puoi cambiarlo nel pacchetto Professional se le tue esigenze di business sono cambiate. Questa funzione è disponibile nel Digital Wallet.

"Scopri come modificare i metodi di ricarica".

Miglioramento del gruppo di sicurezza

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, l'interfaccia utente consente ora di scegliere se si desidera che il gruppo di protezione predefinito consenta il traffico solo all'interno della rete selezionata (scelta consigliata) o di tutte le reti.



18 luglio 2022

Nuovi pacchetti di licenze in Azure

Due nuovi pacchetti di licenze basati sulla capacità sono disponibili per Cloud Volumes ONTAP in Azure quando paghi tramite un abbonamento a Azure Marketplace:

- **Ottimizzato**: Paga separatamente per le operazioni di i/o e capacità fornite
- **Edge cache**: Licenza per "Cloud Volumes Edge cache"

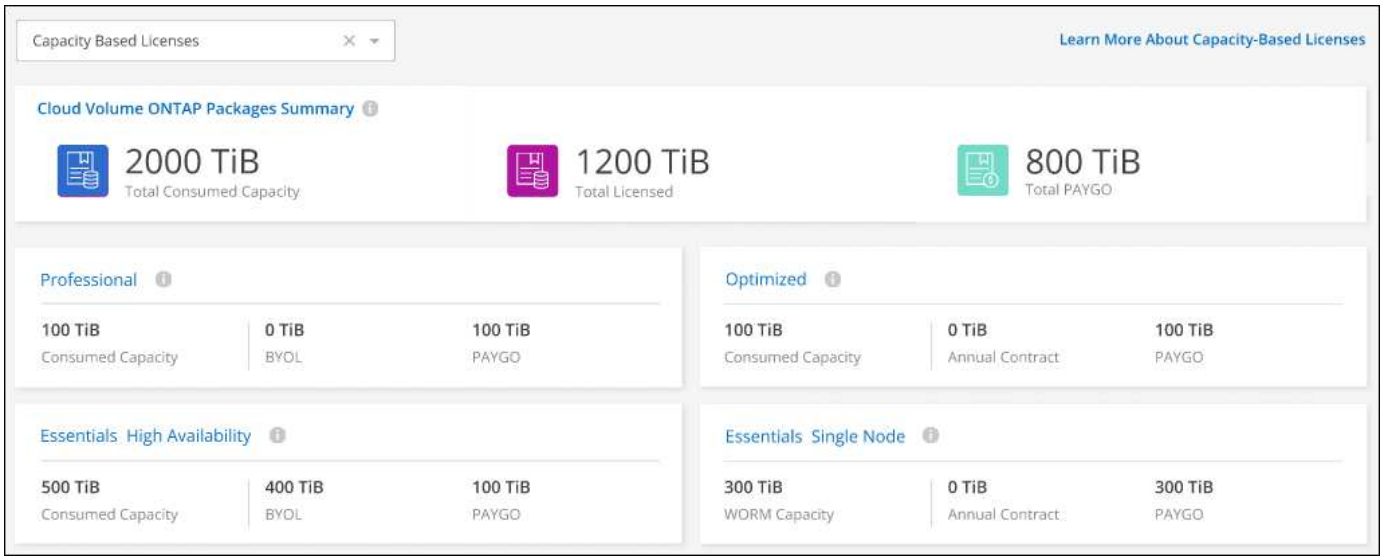
"Scopri di più su questi pacchetti di licenza".

3 luglio 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.20 del connettore.

Portafoglio digitale

Il portafoglio digitale mostra ora 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.



Potenziamento dei volumi elastici

BlueXP ora supporta la funzione EBS di Amazon Elastic Volumes durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP dall'interfaccia utente. La funzione Elastic Volumes (volumi elastici) è attivata per impostazione predefinita quando si utilizzano dischi gp3 o io1. Puoi scegliere la capacità iniziale in base alle tue esigenze di storage e rivederla dopo l'implementazione di Cloud Volumes ONTAP.

"Scopri di più sul supporto per volumi elastici in AWS".

Licenza ONTAP S3 in AWS

Una licenza ONTAP S3 è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.11.0 o successiva in AWS.

"Documentazione di ONTAP: Scopri come configurare e gestire i servizi di storage a oggetti S3"

Nuovo supporto per la regione di Azure Cloud

A partire dalla versione 9.10.1, Cloud Volumes ONTAP è ora supportato nella regione Azure West US 3.

"Visualizza l'elenco completo delle regioni supportate per Cloud Volumes ONTAP"

Licenza ONTAP S3 in Azure

Una licenza ONTAP S3 è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.9.1 o successiva in Azure.

"Documentazione di ONTAP: Scopri come configurare e gestire i servizi di storage a oggetti S3"

7 giugno 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.19 del connettore.

Cloud Volumes ONTAP 9.11.1

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.11.1, che include il supporto per nuove funzionalità e aree di cloud provider aggiuntive.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP"

Nuova 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.

Questa visualizzazione avanzata è disponibile come anteprima con Cloud Volumes ONTAP 9.10.0 e versioni successive. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

"Scopri di più sulla visualizzazione avanzata".

Supporto per Amazon EBS Elastic Volumes

Il supporto per la funzionalità dei volumi elastici di Amazon EBS con un aggregato Cloud Volumes ONTAP offre performance migliori e capacità aggiuntiva, consentendo a BlueXP di aumentare automaticamente la capacità del disco sottostante in base alle necessità.

Il supporto per i volumi elastici è disponibile a partire dai *nuovi* sistemi Cloud Volumes ONTAP 9.11.0 e con i tipi di dischi gp3 e io1 EBS.

"Scopri di più sul supporto per volumi elastici".

Si noti che il supporto per i volumi elastici richiede nuove autorizzazioni AWS per il connettore:

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

Assicurarsi di fornire queste autorizzazioni a ciascun set di credenziali AWS aggiunto a BlueXP. "Visualizza la policy di connessione più recente per AWS".

Supporto per l'implementazione di coppie ha in subnet AWS condivise

Cloud Volumes ONTAP 9.11.1 include il supporto per la condivisione di VPC AWS. Questa versione del connettore consente di implementare una coppia ha in una subnet condivisa AWS quando si utilizza l'API.

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

Accesso limitato alla rete quando si utilizzano endpoint di servizio

BlueXP ora limita l'accesso alla rete quando si utilizza un endpoint del servizio VNET per le connessioni tra Cloud Volumes ONTAP e gli account di storage. BlueXP utilizza un endpoint del servizio se si disattivano le connessioni Azure Private link.

"Scopri di più su Azure Private link Connections con Cloud Volumes ONTAP".

Supporto per la creazione di macchine virtuali storage in Google Cloud

Cloud Volumes ONTAP supporta più VM di storage in Google Cloud, a partire dalla release 9.11.1. A partire da questa versione del connettore, BlueXP consente di creare macchine virtuali di storage su coppie Cloud

Volumes ONTAP ha in Google Cloud utilizzando l'API.

Il supporto per la creazione di macchine virtuali storage richiede nuove autorizzazioni Google Cloud per il connettore:

```
- compute.instanceGroups.get
- compute.addresses.get
```

Tenere presente che per creare una VM di storage su un sistema a nodo singolo è necessario utilizzare la CLI o il Gestore di sistema di ONTAP.

- "Scopri di più sui limiti delle macchine virtuali per lo storage in Google Cloud"
- "Scopri come creare macchine virtuali storage per il data-service per Cloud Volumes ONTAP in Google Cloud"

2 maggio 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.18 del connettore.

Cloud Volumes ONTAP 9.11.0

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.11.0.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Miglioramento degli aggiornamenti dei mediatori

Quando BlueXP aggiorna il mediatore per una coppia ha, ora convalida la disponibilità di una nuova immagine del mediatore prima di eliminare il disco di avvio. Questa modifica garantisce che il mediatore possa continuare a funzionare correttamente in caso di esito negativo del processo di aggiornamento.

La scheda K8s è stata rimossa

La scheda K8s era obsoleta in una versione precedente ed è stata rimossa.

Contratto annuale in Azure

I pacchetti Essentials e Professional sono ora disponibili in Azure attraverso un contratto annuale. Puoi contattare il tuo commerciale NetApp per acquistare un contratto annuale. Il contratto è disponibile come offerta privata in Azure Marketplace.

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

"Scopri di più sulle licenze".

Recupero istantaneo di S3 Glacier

Ora puoi memorizzare i dati a più livelli nella classe di storage Amazon S3 Glacier Instant Retrieval.

"Scopri come cambiare la classe di storage per i dati a più livelli".

Nuove autorizzazioni AWS richieste per il connettore

Le seguenti autorizzazioni sono ora necessarie per creare un gruppo di posizionamento AWS Spread quando si implementa una coppia ha in una singola zona di disponibilità (AZ):

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Queste autorizzazioni sono ora necessarie per ottimizzare il modo in cui BlueXP crea il gruppo di posizionamento.

Assicurarsi di fornire queste autorizzazioni a ciascun set di credenziali AWS aggiunto a BlueXP. "Visualizza la policy di connessione più recente per AWS".

Nuovo supporto per la regione di Google Cloud

Cloud Volumes ONTAP è ora supportato nelle seguenti aree di Google Cloud a partire dalla versione 9.10.1:

- Delhi (asia-Sud 2)
- Melbourne (australia-sud-est 2)
- Milano (europa-West8) - solo nodo singolo
- Santiago (southamerica-West1) - solo nodo singolo

"Visualizza l'elenco completo delle regioni supportate per Cloud Volumes ONTAP"

Supporto per n2-standard-16 in Google Cloud

Il tipo di computer n2-standard-16 è ora supportato con Cloud Volumes ONTAP in Google Cloud, a partire dalla release 9.10.1.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in Google Cloud"

Miglioramenti alle policy firewall di Google Cloud

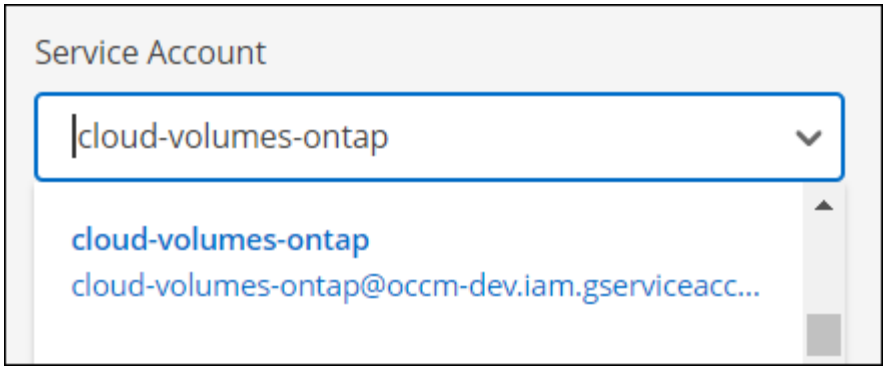
- Quando si crea una coppia Cloud Volumes ONTAP ha in Google Cloud, BlueXP visualizza ora tutte le policy firewall esistenti in un VPC.

  In precedenza, BlueXP non visualizzava alcun criterio in VPC-1, VPC-2 o VPC-3 che non disponeva di un tag di destinazione.

- Quando si crea un sistema a nodo singolo Cloud Volumes ONTAP in Google Cloud, è ora possibile scegliere se si desidera che il criterio firewall predefinito consenta il traffico solo all'interno del VPC selezionato (consigliato) o di tutti i VPC.

Miglioramento degli account dei servizi Google Cloud

Quando si seleziona l'account del servizio Google Cloud da utilizzare con Cloud Volumes ONTAP, BlueXP visualizza ora l'indirizzo e-mail associato a ciascun account del servizio. La visualizzazione dell'indirizzo di posta elettronica consente di distinguere più facilmente gli account di servizio che condividono lo stesso nome.



3 aprile 2022

Il collegamento di System Manager è stato rimosso

Abbiamo rimosso il link di Gestione sistema precedentemente disponibile da un ambiente di lavoro Cloud Volumes ONTAP.

È comunque possibile connettersi a Gestore di sistema immettendo l'indirizzo IP di gestione del cluster in un browser Web che dispone di una connessione al sistema Cloud Volumes ONTAP. "Scopri di più sulla connessione a System Manager".

Addebito per lo storage WORM

Una volta scaduta la tariffa speciale introduttiva, verrà addebitato l'utilizzo dello storage WORM. La carica viene addebitata ogni ora, in base alla capacità totale dei volumi WORM. Questo vale per i sistemi Cloud Volumes ONTAP nuovi ed esistenti.

"Scopri i prezzi dello storage WORM".

27 febbraio 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.16 del connettore.

Creazione guidata volume riprogettata

La creazione guidata di un nuovo volume introdotta di recente è ora disponibile quando si crea un volume su un aggregato specifico dall'opzione **allocazione avanzata**.

"Scopri come creare volumi su un aggregato specifico".

9 febbraio 2022

Aggiornamenti del marketplace

- Il pacchetto Essentials e il pacchetto Professional sono ora disponibili in tutti i mercati dei cloud provider.

  Questi metodi di addebito in base alla capacità ti consentono di pagare entro l'ora o di acquistare un contratto annuale direttamente dal tuo cloud provider. È comunque possibile acquistare una licenza per capacità direttamente da NetApp.

  Se disponi già di un abbonamento a un cloud marketplace, sarai automaticamente iscritto a queste nuove offerte. È possibile scegliere la ricarica in base alla capacità quando si implementa un nuovo ambiente di

lavoro Cloud Volumes ONTAP.

Se sei un nuovo cliente, BlueXP ti chiederà di iscriverti quando crei un nuovo ambiente di lavoro.

- Le licenze per nodo da tutti i mercati dei cloud provider sono obsolete e non sono più disponibili per i nuovi abbonati. Sono inclusi i contratti annuali e gli abbonamenti orari (Explore, Standard e Premium).

  Questo metodo di addebito è ancora disponibile per i clienti esistenti che dispongono di un abbonamento attivo.

"Scopri di più sulle opzioni di licenza per Cloud Volumes ONTAP".

6 febbraio 2022

Licenze Exchange non assegnate

Se si dispone di una licenza non assegnata basata su nodo per Cloud Volumes ONTAP che non è stata utilizzata, è possibile sostituire la licenza convertendola in una licenza di backup cloud, una licenza di rilevamento dati cloud o una licenza di tiering cloud.

Questa azione revoca la licenza Cloud Volumes ONTAP e crea una licenza equivalente al dollaro per il servizio con la stessa data di scadenza.

"Scopri come scambiare licenze basate su nodo non assegnate".

30 gennaio 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.15 del connettore.

Nuova selezione delle licenze

Abbiamo riprogettato la schermata di selezione delle licenze quando creiamo un nuovo ambiente di lavoro Cloud Volumes ONTAP. I cambiamenti evidenziano i metodi di addebito in base alla capacità introdotti nel luglio 2021 e supportano le offerte future attraverso i mercati dei cloud provider.

Aggiornamento del portafoglio digitale

Abbiamo aggiornato il **portafoglio digitale** consolidando le licenze Cloud Volumes ONTAP in un'unica scheda.

2 gennaio 2022

Le seguenti modifiche sono state introdotte con la versione 3.9.14 del connettore.

Supporto per altri tipi di macchine virtuali Azure

Cloud Volumes ONTAP è ora supportato con i seguenti tipi di macchine virtuali in Microsoft Azure, a partire dalla versione 9.10.1:

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

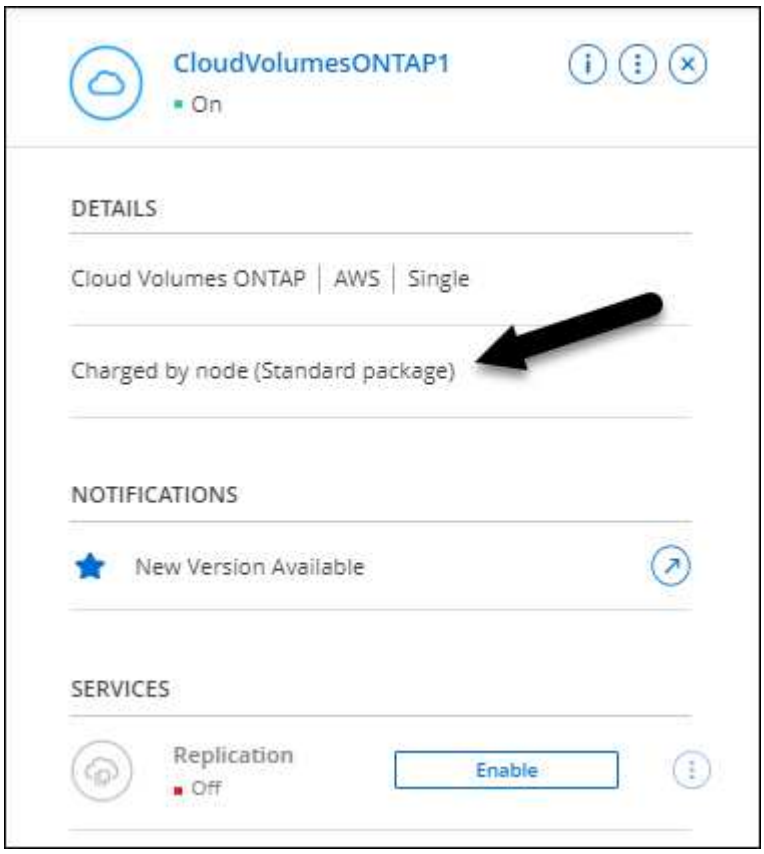
Accedere alla "Note di rilascio di Cloud Volumes ONTAP" per ulteriori informazioni sulle configurazioni supportate.

Aggiornamento della ricarica FlexClone

Se si utilizza un "licenza basata sulla capacità" Per Cloud Volumes ONTAP, la capacità utilizzata dai volumi FlexClone non viene più addebitata.

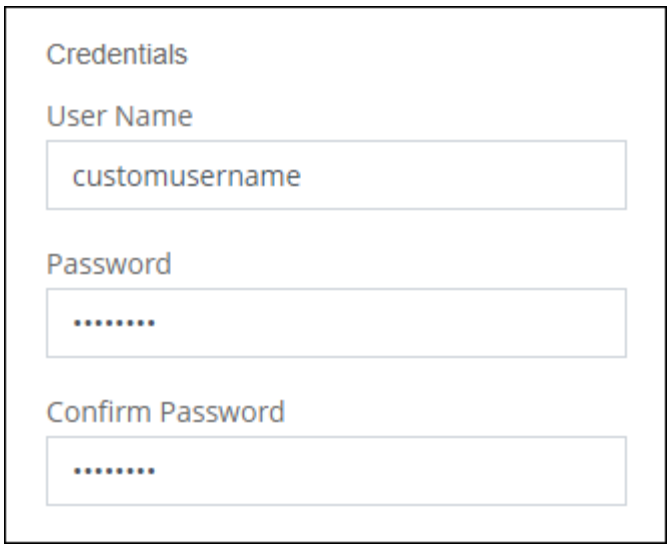
Viene visualizzato il metodo di ricarica

BlueXP mostra ora il metodo di addebito per ogni ambiente di lavoro Cloud Volumes ONTAP nel pannello di destra di Canvas.



Scegliere il nome utente

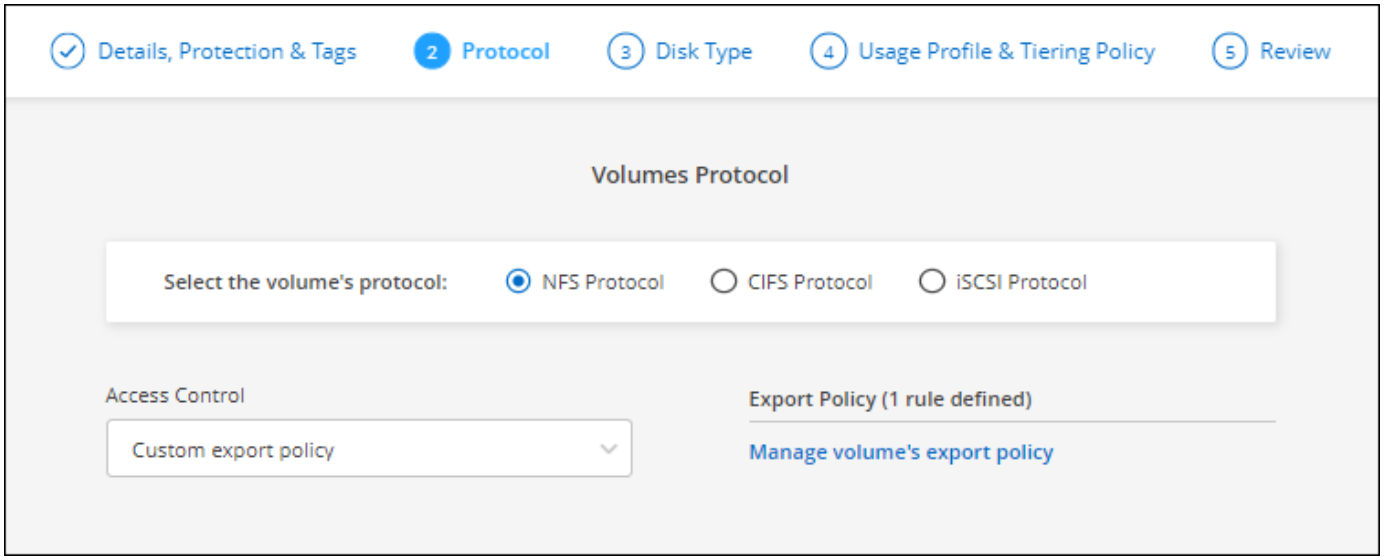
Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, è ora possibile inserire il nome utente preferito, invece del nome utente admin predefinito.



Miglioramenti alla creazione di volumi

Abbiamo apportato alcuni miglioramenti alla creazione di volumi:

- Abbiamo riprogettato la creazione guidata del volume per una maggiore facilità di utilizzo.
- È ora possibile scegliere una policy di esportazione personalizzata per NFS.



28 novembre 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.13 del connettore.

Cloud Volumes ONTAP 9.10.1

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.10.1.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Abbonamenti NetApp Keystone

Ora puoi utilizzare gli abbonamenti Keystone per pagare le coppie Cloud Volumes ONTAP ha.

Un abbonamento Keystone è un servizio basato su abbonamento pay-as-you-grow che offre un'esperienza di cloud ibrido perfetta per coloro che preferiscono i modelli di consumo OpEx a CapEx o al leasing anticipati.

Un abbonamento Keystone è supportato con tutte le nuove versioni di Cloud Volumes ONTAP che è possibile implementare da BlueXP.

- "Scopri di più sugli abbonamenti NetApp Keystone".
- "Scopri come iniziare a utilizzare gli abbonamenti Keystone in BlueXP".

Nuovo supporto regione AWS

Cloud Volumes ONTAP è ora supportato nella regione AWS Asia-Pacifico (Osaka) (ap-Northeast-3).

Riduzione delle porte

Le porte 8023 e 49000 non sono più aperte sui sistemi Cloud Volumes ONTAP in Azure sia per i sistemi a nodo singolo che per le coppie ha.

Questa modifica si applica ai *nuovi* sistemi Cloud Volumes ONTAP a partire dalla release 3.9.13 del connettore.

4 ottobre 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.11 del connettore.

Cloud Volumes ONTAP 9.10.0

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.10.0.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Riduzione dei tempi di implementazione

Abbiamo ridotto il tempo necessario per implementare un ambiente di lavoro Cloud Volumes ONTAP in Microsoft Azure o in Google Cloud quando è attivata la normale velocità di scrittura. Il tempo di implementazione è ora in media inferiore di 3-4 minuti.

2 settembre 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.10 del connettore.

Chiave di crittografia gestita dal cliente in Azure

I dati vengono automaticamente crittografati in Cloud Volumes ONTAP in Azure utilizzando una chiave gestita da "Azure Storage Service Encryption" Microsoft. Tuttavia, ora è possibile utilizzare la propria chiave di crittografia gestita dal cliente completando i seguenti passaggi:

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

"Scopri di più su questi passaggi".

7 luglio 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.8 del connettore.

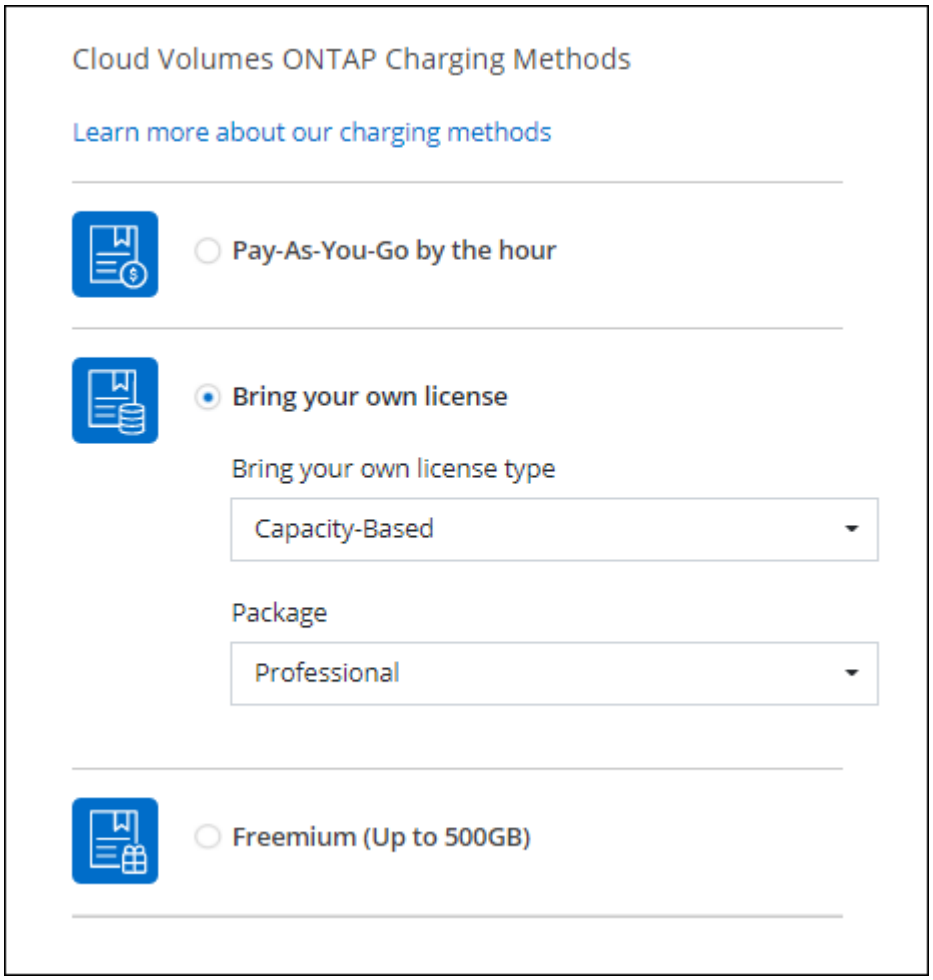
Nuovi metodi di ricarica

Sono disponibili nuovi metodi di ricarica per Cloud Volumes ONTAP.

- **BYOL basato sulla capacità**: Una licenza basata sulla capacità consente di pagare Cloud Volumes ONTAP per TIB di capacità. La licenza è associata al tuo account NetApp e ti consente di creare come sistemi Cloud Volumes ONTAP multipli, purché sia disponibile una capacità sufficiente attraverso la licenza. Le licenze basate sulla capacità sono disponibili sotto forma di pacchetto, *Essentials* o *Professional*.
- **Offerta Freemium**: Freemium ti consente di utilizzare tutte le funzionalità Cloud Volumes ONTAP gratuitamente da NetApp (i costi dei cloud provider sono ancora a carico). Hai un limite di 500 GiB di capacità fornita per sistema e non c'è alcun contratto di supporto. Puoi avere fino a 10 sistemi Freemium.

  "Scopri di più su queste opzioni di licenza".

  Ecco un esempio dei metodi di ricarica tra cui scegliere:



Storage WORM disponibile per uso generico

Lo storage WORM (Write Once, Read Many) non è più disponibile nell'anteprima ed è ora disponibile per l'uso generico con Cloud Volumes ONTAP. "Scopri di più sullo storage WORM".

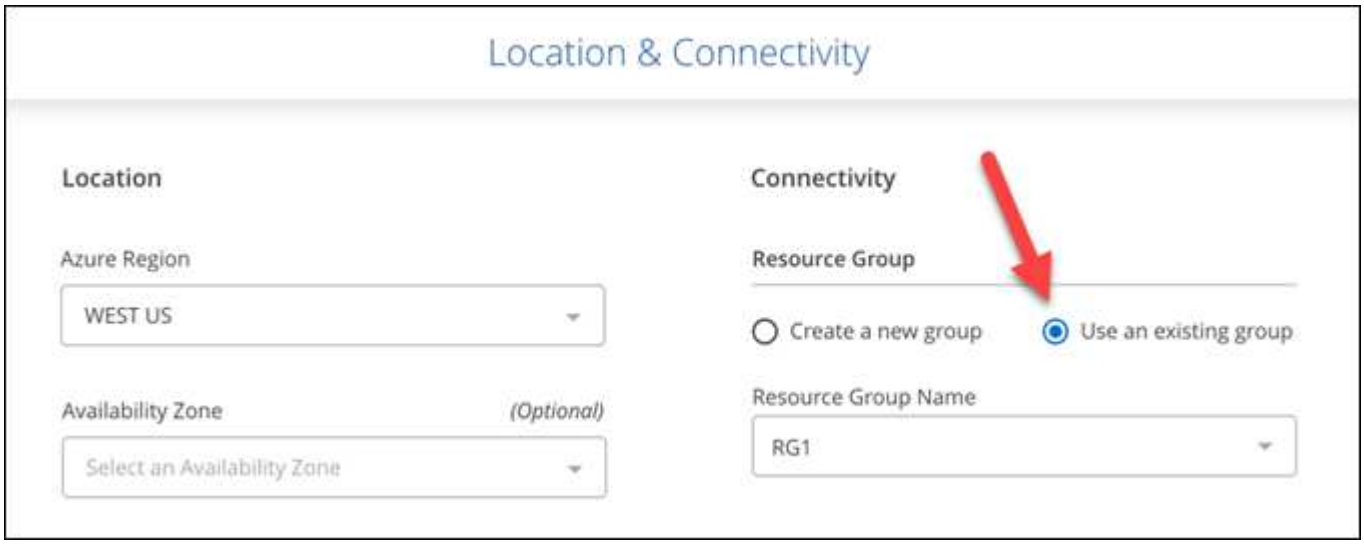
Supporto per m5dn.24xlarge in AWS

A partire dalla versione 9.9.1, Cloud Volumes ONTAP ora supporta il tipo di istanza m5dn.24xlarge con i seguenti metodi di addebito: PAYGO Premium, Bring Your Own License (BYOL) e Freemium.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in AWS".

Selezionare i gruppi di risorse Azure esistenti

Quando si crea un sistema Cloud Volumes ONTAP in Azure, è ora possibile selezionare un gruppo di risorse esistente per la macchina virtuale e le risorse associate.



Le seguenti autorizzazioni consentono a BlueXP di rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione:

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

Assicurarsi di fornire queste autorizzazioni a ciascun set di credenziali Azure aggiunto a BlueXP. "Visualizza la policy di connessione più recente per Azure".

Accesso pubblico BLOB ora disattivato in Azure

Come miglioramento della sicurezza, BlueXP disattiva **Blob public access** quando si crea un account storage per Cloud Volumes ONTAP.

Miglioramento di Azure Private link

Per impostazione predefinita, BlueXP attiva ora una connessione Azure Private link sull'account di storage per la diagnostica di avvio per i nuovi sistemi Cloud Volumes ONTAP.

Ciò significa che gli account di storage per Cloud Volumes ONTAP utilizzeranno ora un collegamento privato.

"Scopri di più sull'utilizzo di un collegamento privato Azure con Cloud Volumes ONTAP".

Dischi persistenti bilanciati in Google Cloud

A partire dalla versione 9.9.1, Cloud Volumes ONTAP ora supporta dischi persistenti bilanciati (pd-Balanced).

Questi SSD bilanciano le performance e i costi fornendo IOPS inferiori per GiB.

Custom-4-16384 non più supportato in Google Cloud

Il tipo di macchina custom-4-16384 non è più supportato dai nuovi sistemi Cloud Volumes ONTAP.

Se si dispone di un sistema esistente in esecuzione su questo tipo di macchina, è possibile continuare a utilizzarlo, ma si consiglia di passare al tipo di macchina n2-standard-4.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in GCP".

30 maggio 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.7 del connettore.

Nuovo Professional Package in AWS

Un nuovo pacchetto professionale consente di raggruppare Cloud Volumes ONTAP e Cloud Backup Service utilizzando un contratto annuale di AWS Marketplace. Il pagamento avviene per TiB. Questo abbonamento non consente di eseguire il backup dei dati in locale.

Scegliendo questa opzione di pagamento, è possibile eseguire il provisioning di un massimo di 2 PIB per sistema Cloud Volumes ONTAP tramite dischi EBS e tiering allo storage a oggetti S3 (nodo singolo o ha).

Accedere alla "Pagina AWS Marketplace" per visualizzare i dettagli sui prezzi e accedere alla "Note di rilascio di Cloud Volumes ONTAP" per ulteriori informazioni su questa opzione di licenza.

Tag sui volumi EBS in AWS

BlueXP ora aggiunge tag ai volumi EBS quando crea un nuovo ambiente di lavoro Cloud Volumes ONTAP. I tag sono stati creati in precedenza dopo l'implementazione di Cloud Volumes ONTAP.

Questa modifica può essere utile se l'organizzazione utilizza i criteri di controllo dei servizi (SCP) per gestire le autorizzazioni.

Periodo minimo di raffreddamento per policy di tiering automatico

Se è stato attivato il tiering dei dati su un volume utilizzando il criterio di tiering *auto*, è ora possibile regolare il periodo di raffreddamento minimo utilizzando l'API.

"Scopri come regolare il periodo di raffreddamento minimo."

Miglioramento delle policy di esportazione personalizzate

Quando si crea un nuovo volume NFS, BlueXP ora visualizza i criteri di esportazione personalizzati in ordine crescente, semplificando la ricerca dei criteri di esportazione necessari.

Eliminazione di vecchie snapshot cloud

BlueXP ora elimina le vecchie snapshot cloud dei dischi root e di boot creati quando viene implementato un sistema Cloud Volumes ONTAP e ogni volta che viene spento. Vengono conservati solo i due snapshot più recenti per i volumi root e boot.

Questo miglioramento aiuta a ridurre i costi dei cloud provider rimuovendo le snapshot non più necessarie.

Si noti che un connettore richiede una nuova autorizzazione per eliminare le snapshot di Azure. "Visualizza la policy di connessione più recente per Azure".

```
"Microsoft.Compute/snapshots/delete"
```

24 maggio 2021

Cloud Volumes ONTAP 9.9.1

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.9.1.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

11 Apr 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.5 del connettore.

Reporting dello spazio logico

BlueXP consente ora il reporting dello spazio logico sulla VM di storage iniziale creata per Cloud Volumes ONTAP.

Quando lo spazio viene segnalato logicamente, ONTAP riporta lo spazio del volume in modo che tutto lo spazio fisico salvato dalle funzionalità di efficienza dello storage venga riportato come utilizzato.

Supporto per dischi gp3 in AWS

Cloud Volumes ONTAP ora supporta i dischi *gp3 (General Purpose SSD)*, a partire dalla release 9.7. i dischi gp3 sono gli SSD più economici che bilanciano costi e performance per un'ampia gamma di carichi di lavoro.

"Scopri di più sull'utilizzo dei dischi gp3 con Cloud Volumes ONTAP".

I dischi rigidi Cold non sono più supportati in AWS

Cloud Volumes ONTAP non supporta più dischi rigidi a freddo (sc1).

TLS 1.2 per gli account di storage Azure

Quando BlueXP crea account di storage in Azure per Cloud Volumes ONTAP, la versione TLS dell'account di storage è la 1.2.

8 marzo 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.4 del connettore.

Cloud Volumes ONTAP 9.9.0

BlueXP è ora in grado di implementare e gestire Cloud Volumes ONTAP 9.9.0.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Supporto per l'ambiente AWS C2S

È ora possibile implementare Cloud Volumes ONTAP 9.8 nell'ambiente dei servizi cloud commerciali AWS (C2S).

"Scopri come iniziare a utilizzare C2S".

Crittografia AWS con CMK gestiti dal cliente

BlueXP ti ha sempre consentito di crittografare i dati Cloud Volumes ONTAP utilizzando il servizio di gestione delle chiavi AWS (KMS). A partire da Cloud Volumes ONTAP 9.9.0, i dati sui dischi EBS e i dati a livelli S3 vengono crittografati se si seleziona un CMK gestito dal cliente. In precedenza, solo i dati EBS sarebbero stati crittografati.

Tenere presente che è necessario fornire al ruolo IAM Cloud Volumes ONTAP l'accesso per utilizzare il CMK.

"Scopri di più sulla configurazione di AWS KMS con Cloud Volumes ONTAP".

Supporto per Azure DoD

È ora possibile implementare Cloud Volumes ONTAP 9.8 nel dipartimento della difesa di Azure (DOD) Impact Level 6 (IL6).

Riduzione dell'indirizzo IP in Google Cloud

Abbiamo ridotto il numero di indirizzi IP richiesti per Cloud Volumes ONTAP 9.8 e versioni successive in Google Cloud. Per impostazione predefinita, è richiesto un indirizzo IP in meno (abbiamo unificato la LIF di intercluster con la LIF di gestione dei nodi). È inoltre possibile saltare la creazione della LIF di gestione SVM quando si utilizza l'API, riducendo la necessità di un indirizzo IP aggiuntivo.

"Scopri di più sui requisiti degli indirizzi IP in Google Cloud".

Supporto VPC condiviso in Google Cloud

Quando si implementa una coppia Cloud Volumes ONTAP ha in Google Cloud, è ora possibile scegliere VPC condivisi per VPC-1, VPC-2 e VPC-3. In precedenza, solo VPC-0 poteva essere un VPC condiviso. Questa modifica è supportata con Cloud Volumes ONTAP 9.8 e versioni successive.

"Scopri di più sui requisiti di rete di Google Cloud".

4 gennaio 2021

Le seguenti modifiche sono state introdotte con la versione 3.9.2 del connettore.

AWS outpost

Alcuni mesi fa, abbiamo annunciato che Cloud Volumes ONTAP aveva ottenuto la designazione di Amazon Web Services (AWS) Outposts Ready. Oggi siamo lieti di annunciare che abbiamo validato BlueXP e Cloud Volumes ONTAP con gli outpost AWS.

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

Vi sono alcune limitazioni da sottolineare:

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

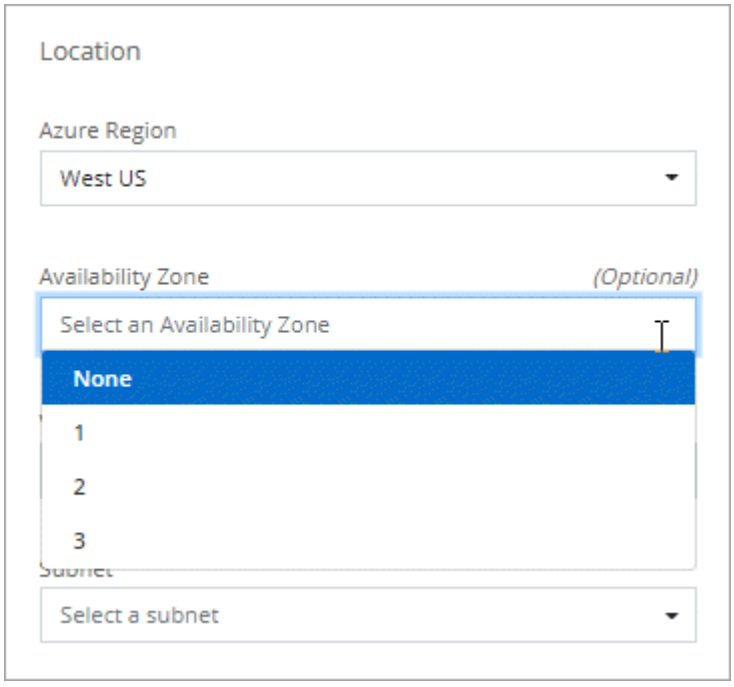
Ultra SSD VNVRAM nelle regioni Azure supportate

Cloud Volumes ONTAP può ora utilizzare un Ultra SSD come VNVRAM quando si utilizza il tipo di macchina virtuale E32s_v3 con un sistema a nodo singolo "In qualsiasi regione Azure supportata".

La VNVRAM offre migliori prestazioni di scrittura.

Scegli una zona di disponibilità in Azure

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



Dischi più grandi in Google Cloud

Cloud Volumes ONTAP ora supporta dischi da 64 TB in GCP.

La capacità massima del sistema con i soli dischi rimane a 256 TB a causa dei limiti GCP.

Nuovi tipi di computer in Google Cloud

Cloud Volumes ONTAP ora supporta i seguenti tipi di computer:

- n2-standard-4 con la licenza Explore e con BYOL
- n2-standard-8 con licenza Standard e con BYOL
- n2-standard-32 con licenza Premium e con BYOL

3 novembre 2020

Le seguenti modifiche sono state introdotte con la versione 3.9.0 del connettore.

Collegamento privato Azure per Cloud Volumes ONTAP

Per impostazione predefinita, BlueXP attiva ora una connessione Azure Private link tra Cloud Volumes ONTAP e gli account di storage associati. Un collegamento privato protegge le connessioni tra gli endpoint in Azure.

- "Scopri di più sui link privati di Azure"
- "Scopri di più sull'utilizzo di un collegamento privato Azure con Cloud Volumes ONTAP"

Limitazioni note

Le limitazioni note identificano piattaforme, dispositivi o funzioni non supportate da questa versione del prodotto o che non interagiscono correttamente con esso. Esaminare attentamente queste limitazioni.

Queste limitazioni sono specifiche per la gestione di Cloud Volumes ONTAP in BlueXP. Per visualizzare le limitazioni del software Cloud Volumes ONTAP, "Vai alle Note di rilascio di Cloud Volumes ONTAP"

BlueXP non supporta la creazione di volumi FlexGroup

Sebbene Cloud Volumes ONTAP supporti i volumi FlexGroup, attualmente BlueXP non supporta la creazione di volumi FlexGroup. Se si crea un volume FlexGroup da Gestione di sistema di ONTAP o dalla CLI di ONTAP, è necessario impostare la modalità Gestione capacità di BlueXP su Manuale. La modalità automatica potrebbe non funzionare correttamente con i volumi FlexGroup.

La possibilità di creare volumi FlexGroup in BlueXP è prevista per una release futura.

BlueXP non supporta S3 con Cloud Volumes ONTAP

Sebbene Cloud Volumes ONTAP supporti S3 come opzione per lo storage scale-out, BlueXP non fornisce alcuna funzionalità di gestione per questa funzionalità. L'utilizzo della CLI è la procedura consigliata per configurare l'accesso al client S3 da Cloud Volumes ONTAP. Per ulteriori informazioni, fare riferimento a. "Guida all'alimentazione per la configurazione S3".

"Scopri di più sul supporto Cloud Volumes ONTAP per S3 e altri protocolli client".

BlueXP non supporta il disaster recovery per le VM di storage

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

"Scopri di più sul disaster recovery delle SVM".

Note di rilascio di Cloud Volumes ONTAP

Le Note di rilascio per Cloud Volumes ONTAP forniscono informazioni specifiche sulla release. Novità della release, configurazioni supportate, limiti di storage e qualsiasi limitazione o problema noto che possa influire sulla funzionalità del prodotto.

"Vai alle Note di rilascio di Cloud Volumes ONTAP"

Inizia subito

Scopri di più su Cloud Volumes ONTAP

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

Cloud Volumes ONTAP è un'appliance di storage solo software che esegue il software di gestione dei dati ONTAP nel cloud. Offre storage di livello Enterprise con le seguenti funzionalità principali:

- Efficienza dello storage

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

- Alta disponibilità

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

- Protezione dei dati

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

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

  "Scopri di più sul backup e ripristino BlueXP"

- Tiering dei dati

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

- Coerenza applicativa

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

  "Scopri di più su SnapCenter"

- Sicurezza dei dati

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

- Controlli di conformità alla privacy

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

  "Scopri di più sulla classificazione BlueXP"

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

"Visualizza le configurazioni Cloud Volumes ONTAP supportate"

"Scopri di più su Cloud Volumes ONTAP"

Versioni di ONTAP supportate per le implementazioni Cloud Volumes ONTAP

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

Le versioni di Cloud Volumes ONTAP diverse da quelle elencate non sono disponibili per le nuove implementazioni. Per informazioni sull'aggiornamento, fare riferimento alla "Percorsi di upgrade supportati".

AWS

Nodo singolo

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Coppia HA

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1

- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

Nodo singolo

- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

Coppia HA

- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3

- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

Nodo singolo

- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

Coppia HA

- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Inizia con Amazon Web Services

Avvio rapido di Cloud Volumes ONTAP in AWS

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

1 Creare un connettore

Se non si dispone ancora di un "Connettore", è necessario crearne uno. "Scopri come creare un connettore in AWS"

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

2 Pianificare la configurazione

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

3 Configurare la rete

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

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

3. Impostare un endpoint VPC sul servizio S3.

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

"Scopri di più sui requisiti di rete".

4 Configurare AWS KMS

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

5 Avviare Cloud Volumes ONTAP utilizzando BlueXP

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

Link correlati

- "Crea un connettore in AWS da BlueXP"
- "Creare un connettore da AWS Marketplace"
- "Installazione e configurazione di un connettore on-premise"
- "Autorizzazioni AWS per il connettore"

Pianificare la configurazione di Cloud Volumes ONTAP in AWS

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

Scegliere una licenza Cloud Volumes ONTAP

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

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

Scegliere una regione supportata

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

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

Scegliere una zona locale supportata

La selezione di una zona locale è facoltativa. Cloud Volumes ONTAP è supportato in alcune zone locali di AWS, inclusa Singapore. Cloud Volumes ONTAP in AWS supporta solo la modalità ha (High Availability) in una singola zona di disponibilità. Le implementazioni a nodo singolo non sono supportate.

> Cloud Volumes ONTAP non dispone del supporto per il tiering dei dati e il tiering cloud nelle zone locali di AWS. Inoltre, le zone locali con istanze non qualificate per Cloud Volumes ONTAP non sono supportate. Un esempio è Miami, che non è disponibile come zona locale, perché ha solo Gen6 istanze non supportate e non qualificate.

"Documentazione AWS: visualizza l'elenco completo delle zone locali" . Le zone locali devono essere abilitate prima di poter creare e gestire risorse in tali zone.

"Documentazione AWS: Introduzione alle zone locali AWS" .

Scegliere un'istanza supportata

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

"Configurazioni supportate per Cloud Volumes ONTAP in AWS"

Comprendere i limiti dello storage

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

"Limiti di storage per Cloud Volumes ONTAP in AWS"

Dimensionare il sistema in AWS

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

Tipo di istanza

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

Tipo di disco EBS

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

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

  Quando si seleziona un disco gp3, BlueXP inserisce i valori IOPS e di throughput predefiniti che garantiscono prestazioni equivalenti a quelle di un disco gp2 in base alle dimensioni del disco selezionato. È possibile aumentare i valori per ottenere prestazioni migliori a un costo maggiore, ma non supportiamo valori inferiori perché potrebbero comportare prestazioni inferiori. In breve, mantenete i valori predefiniti oppure aumentateli. Non abbassarli. "Documentazione AWS: Scopri di più sui dischi gp3 e sulle loro prestazioni" .

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

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

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

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

Il tiering dei dati in AWS S3 non è disponibile nelle zone locali di AWS a causa della mancanza di connettività.

Dimensione del disco EBS

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

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Le prestazioni dei dischi EBS sono legate alle dimensioni dei dischi. La dimensione determina gli IOPS di riferimento e la durata massima del burst per i dischi SSD e il throughput di base e burst per i dischi HDD.
- In definitiva, è necessario scegliere le dimensioni del disco che offrono le *prestazioni sostenute* necessarie.
- Anche se si scelgono dischi più grandi (ad esempio, sei dischi 4 TIB), è possibile che non si ottengano tutti gli IOPS perché l'istanza EC2 può raggiungere il limite di larghezza di banda.

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

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

Visualizzare i dischi di sistema predefiniti

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

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

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

Prepararsi a implementare Cloud Volumes ONTAP in un Outpost AWS

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

Vi sono alcune limitazioni da sottolineare:

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

Raccogliere informazioni di rete

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

Nodo singolo o coppia ha in un singolo AZ

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

Coppia HA in AZS multipli

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

Scegliere una velocità di scrittura

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

scrittura".

Scegliere un profilo di utilizzo del volume

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

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

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

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

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

Configurare la rete

Configura il networking AWS per Cloud Volumes ONTAP

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

Requisiti generali

Verifica di aver soddisfatto i seguenti requisiti in AWS.

Accesso a Internet in uscita per nodi Cloud Volumes ONTAP

I sistemi Cloud Volumes ONTAP richiedono l'accesso a Internet outbound per l'accesso a endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con severi requisiti di sicurezza.

BlueXP Connector contatta anche diversi endpoint per le operazioni quotidiane e la console basata sul Web di BlueXP . Per informazioni sugli endpoint BlueXP , fare riferimento a "Visualizzare gli endpoint contattati dal connettore" e "Preparazione del networking per l'utilizzo della console BlueXP".

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Endpoint	Applicabile per	Scopo	Modalità di implementazione di BlueXP	Impatto se l'endpoint non è disponibile
https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione BlueXP .	Modalità standard e limitata.	L'autenticazione dell'utente non riesce e i seguenti servizi rimangono non disponibili: • I servizi di Cloud Volumes ONTAP • Servizi ONTAP • E servizi proxy
https://cloudmanager.cloud.netapp.com/tenancy	Locazione	Utilizzato per recuperare le risorse Cloud Volumes ONTAP dalla tenancy BlueXP per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
https://support.NetApp.com/aods/asuppmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Utilizzato per inviare dati telemetrici AutoSupport al supporto NetApp.	Modalità standard e limitata.	Le informazioni AutoSupport rimangono non trasmesse.
L'endpoint commerciale esatto per il servizio AWS (con suffisso `amazonaws.com`) dipende dalla regione AWS in uso. Fare riferimento alla "Per conoscere i dettagli, consultare la documentazione AWS".	• CloudFormation • Elastic Compute Cloud (EC2) • Gestione delle identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • S3 (Simple Storage Service)	Comunicazione con i servizi AWS.	Modalità standard e privata.	Cloud Volumes ONTAP non può comunicare con il servizio AWS per eseguire operazioni BlueXP specifiche in AWS.

Endpoint	Applicabile per	Scopo	Modalità di implementazione di BlueXP	Impatto se l'endpoint non è disponibile
L'endpoint governativo esatto per il servizio AWS dipende dalla regione AWS utilizzata. Gli endpoint sono suffissi con `amazonaws.com` E `c2s.ic.gov` . Fare riferimento a "SDK AWS" E "Documentazione AWS" per maggiori informazioni.	• CloudFormation • Elastic Compute Cloud (EC2) • Gestione delle identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • S3 (Simple Storage Service)	Comunicazione con i servizi AWS.	Modalità limitata.	Cloud Volumes ONTAP non può comunicare con il servizio AWS per eseguire operazioni BlueXP specifiche in AWS.

Accesso a Internet in uscita per il mediatore ha

L'istanza di ha mediator deve disporre di una connessione in uscita al servizio AWS EC2 in modo che possa fornire assistenza per il failover dello storage. Per fornire la connessione, è possibile aggiungere un indirizzo IP pubblico, specificare un server proxy o utilizzare un'opzione manuale.

L'opzione manuale può essere un gateway NAT o un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2. Per ulteriori informazioni sugli endpoint VPC, fare riferimento alla "Documentazione AWS: Endpoint VPC di interfaccia (AWS PrivateLink)" .

Configurazioni di rete per supportare il proxy del connettore

È possibile utilizzare i server proxy configurati per BlueXP Connector per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. BlueXP supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy del connettore. L'amministratore del connettore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato nell'ambiente di lavoro Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP attraverso il proxy del connettore. Quando si configura un proxy trasparente, l'amministratore del connettore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurarsi di ottenere e caricare lo stesso certificato CA radice nell'ambiente di lavoro Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy per BlueXP Connector, fare riferimento a "Configurare un connettore per l'utilizzo di un server proxy" .

Indirizzi IP privati

BlueXP assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi IP privati.

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

Indirizzi IP per un sistema a nodo singolo

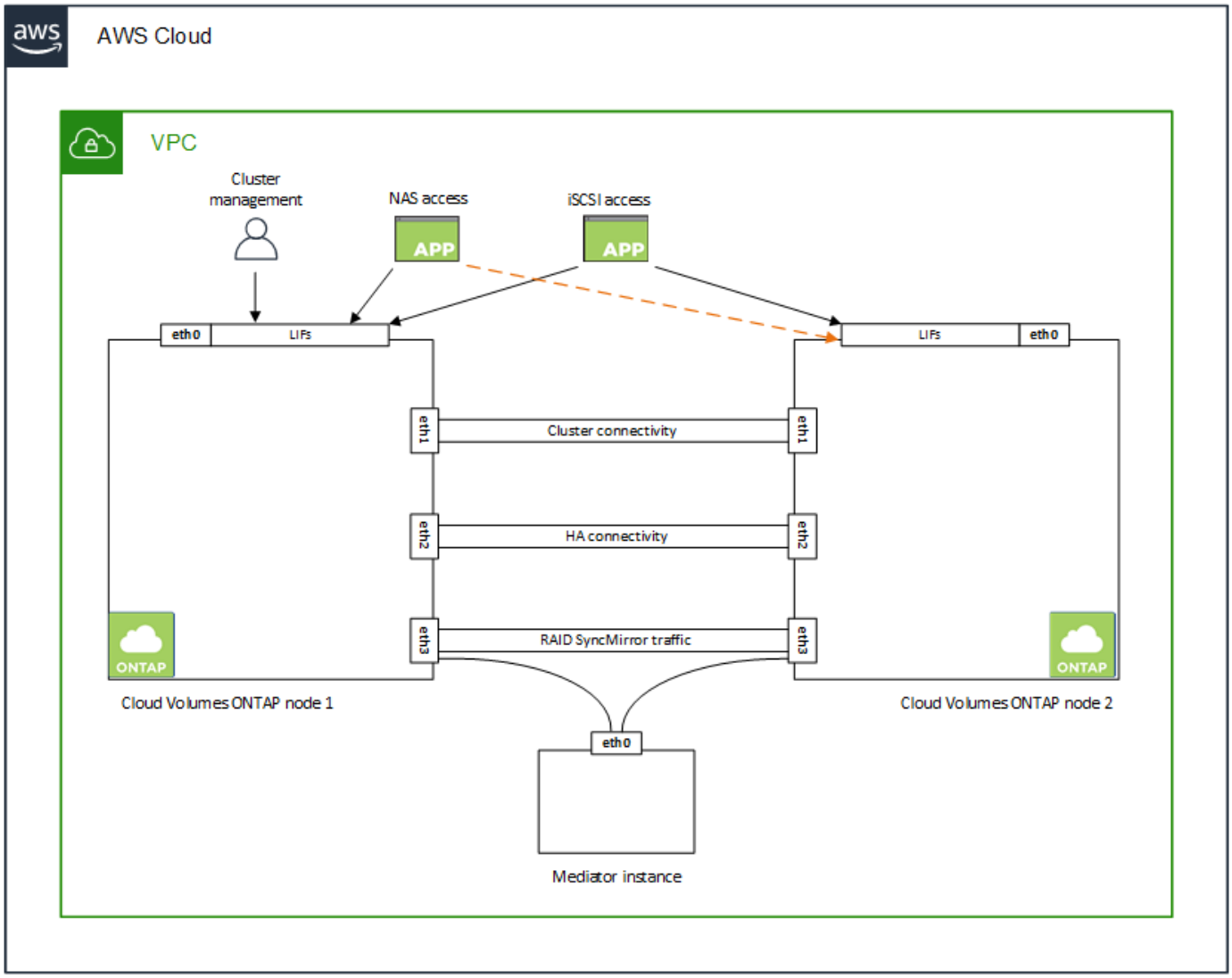
BlueXP assegna 6 indirizzi IP a un sistema a nodo singolo.

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

LIF	Scopo
Gestione del cluster	Gestione amministrativa dell'intero cluster (coppia ha).
Gestione dei nodi	Gestione amministrativa di un nodo.
Intercluster	Comunicazione tra cluster, backup e replica.
Dati NAS	Accesso client tramite protocolli NAS.
Dati iSCSI	Accesso del client tramite il protocollo iSCSI. Utilizzato anche dal sistema per altri importanti flussi di lavoro di rete. Questa LIF è obbligatoria e non deve essere eliminata.
Gestione delle macchine virtuali dello storage	Una LIF di gestione delle macchine virtuali dello storage viene utilizzata con strumenti di gestione come SnapCenter.

Indirizzi IP per coppie ha

Le coppie HA richiedono più indirizzi IP rispetto a un sistema a nodo singolo. Questi indirizzi IP sono distribuiti su diverse interfacce ethernet, come mostrato nell'immagine seguente:



Il numero di indirizzi IP privati richiesti per una coppia ha dipende dal modello di implementazione scelto. Una coppia ha implementata in una *singola* AWS Availability zone (AZ) richiede 15 indirizzi IP privati, mentre una coppia ha implementata in *multiple* AZS richiede 13 indirizzi IP privati.

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

LIF	Interfaccia	Nodo	Scopo
Gestione del cluster	eth0	nodo 1	Gestione amministrativa dell'intero cluster (coppia ha).
Gestione dei nodi	eth0	nodo 1 e nodo 2	Gestione amministrativa di un nodo.
Intercluster	eth0	nodo 1 e nodo 2	Comunicazione tra cluster, backup e replica.
Dati NAS	eth0	nodo 1	Accesso client tramite protocolli NAS.
Dati iSCSI	eth0	nodo 1 e nodo 2	Accesso del client tramite il protocollo iSCSI. Utilizzato anche dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere cancellati.

LIF	Interfaccia	Nodo	Scopo
Connettività del cluster	eth1	nodo 1 e nodo 2	Consente ai nodi di comunicare tra loro e di spostare i dati all'interno del cluster.
Connettività HA	eth2	nodo 1 e nodo 2	Comunicazione tra i due nodi in caso di failover.
Traffico iSCSI RSM	eth3	nodo 1 e nodo 2	Traffico iSCSI RAID SyncMirror, nonché comunicazione tra i due nodi Cloud Volumes ONTAP e il mediatore.
Mediatore	eth0	Mediatore	Un canale di comunicazione tra i nodi e il mediatore per assistere nei processi di acquisizione e giveback dello storage.

LIF	Interfaccia	Nodo	Scopo
Gestione dei nodi	eth0	nodo 1 e nodo 2	Gestione amministrativa di un nodo.
Intercluster	eth0	nodo 1 e nodo 2	Comunicazione tra cluster, backup e replica.
Dati iSCSI	eth0	nodo 1 e nodo 2	Accesso del client tramite il protocollo iSCSI. Queste LIF gestiscono anche la migrazione di indirizzi IP mobili tra nodi. Questi LIF sono obbligatori e non devono essere cancellati.
Connettività del cluster	eth1	nodo 1 e nodo 2	Consente ai nodi di comunicare tra loro e di spostare i dati all'interno del cluster.
Connettività HA	eth2	nodo 1 e nodo 2	Comunicazione tra i due nodi in caso di failover.
Traffico iSCSI RSM	eth3	nodo 1 e nodo 2	Traffico iSCSI RAID SyncMirror, nonché comunicazione tra i due nodi Cloud Volumes ONTAP e il mediatore.
Mediatore	eth0	Mediatore	Un canale di comunicazione tra i nodi e il mediatore per assistere nei processi di acquisizione e giveback dello storage.

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

Gruppi di sicurezza

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

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

Connessione per il tiering dei dati

Se si desidera utilizzare EBS come Tier di performance e AWS S3 come Tier di capacità, è necessario assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione consiste nella creazione di un endpoint VPC per il servizio S3. Per istruzioni, fare riferimento alla "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, consultare la "AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"

Connessioni ai sistemi ONTAP

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

DNS e Active Directory per CIFS

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

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

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

Condivisione VPC

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

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

Requisiti per coppie ha in più AZS

Ulteriori requisiti di rete AWS si applicano alle configurazioni Cloud Volumes ONTAP ha che utilizzano zone di disponibilità multiple (AZS). Prima di avviare una coppia ha, è necessario esaminare questi requisiti perché è necessario inserire i dettagli di rete in BlueXP quando si crea l'ambiente di lavoro.

Per informazioni sul funzionamento delle coppie ha, fare riferimento alla "Coppie ad alta disponibilità".

Zone di disponibilità

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

In ciascuna zona di disponibilità dovrebbe essere disponibile una subnet.

Indirizzi IP mobili per dati NAS e gestione cluster/SVM

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

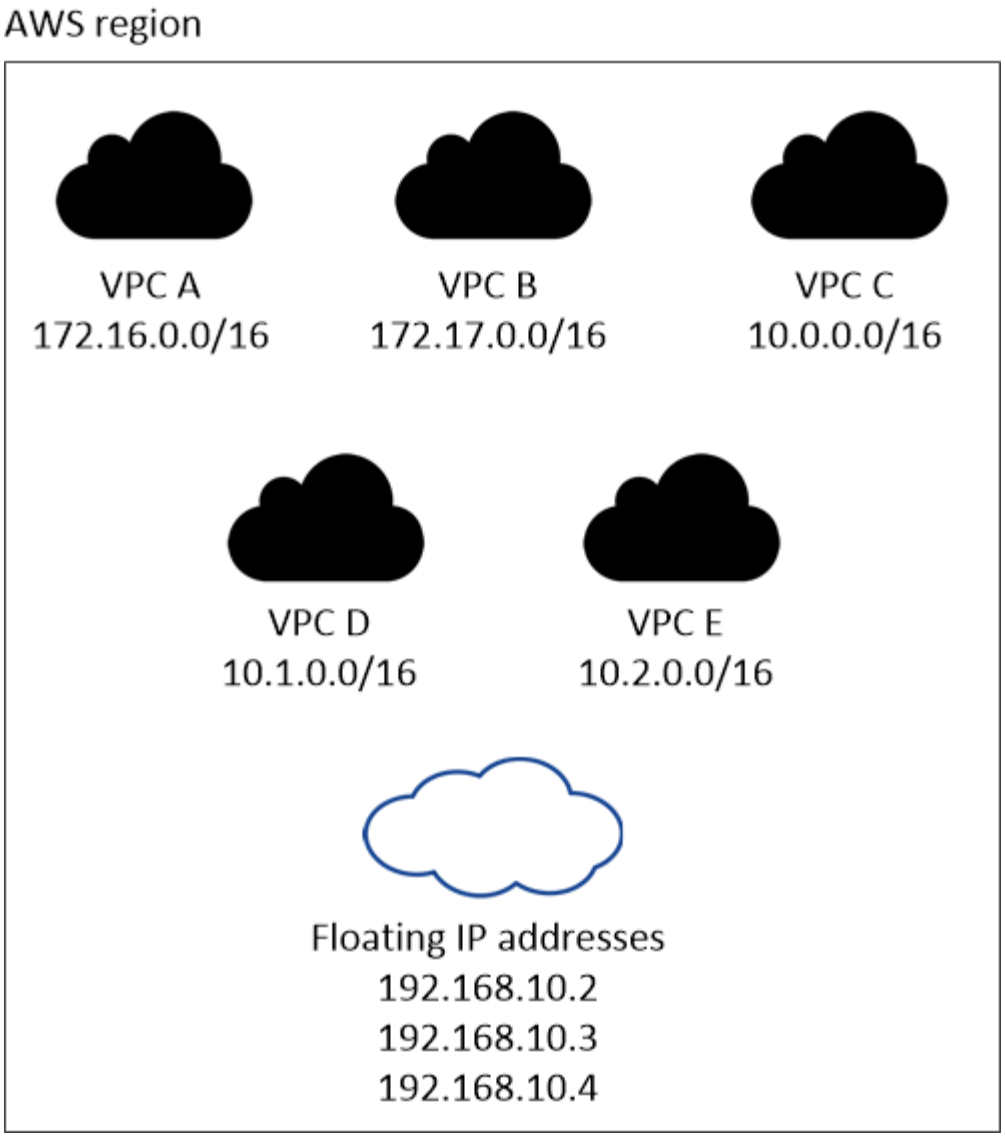
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

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

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

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

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



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

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

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

Tabelle di percorso

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

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

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

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

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

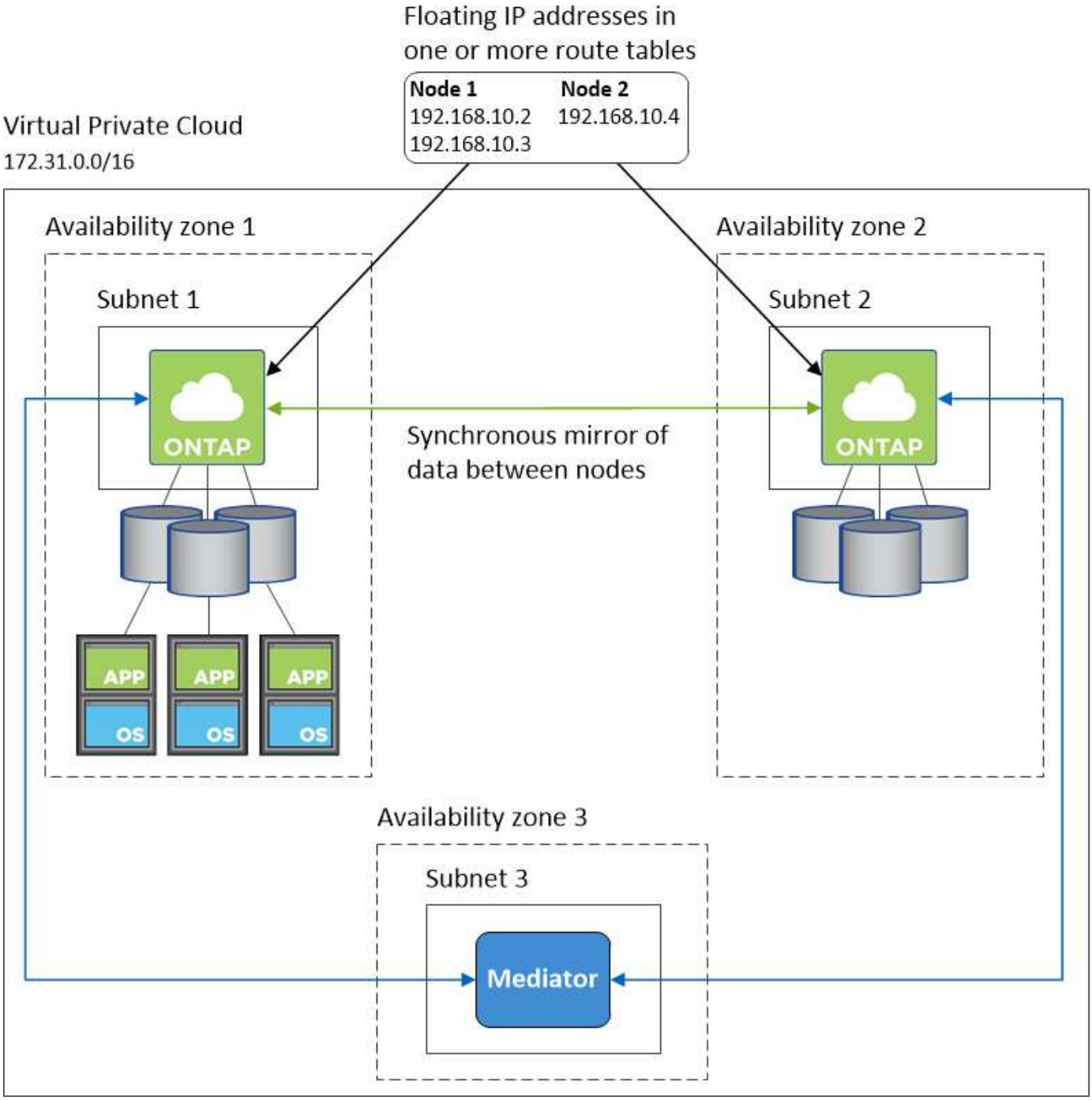
Connessione ai tool di gestione NetApp

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

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

Esempio di configurazione ha

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



Requisiti per il connettore

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

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

Argomenti correlati

- "Verificare la configurazione di AutoSupport per Cloud Volumes ONTAP"
- "Informazioni sulle porte interne di ONTAP".

Configurare un gateway di transito AWS per le coppie ha Cloud Volumes ONTAP

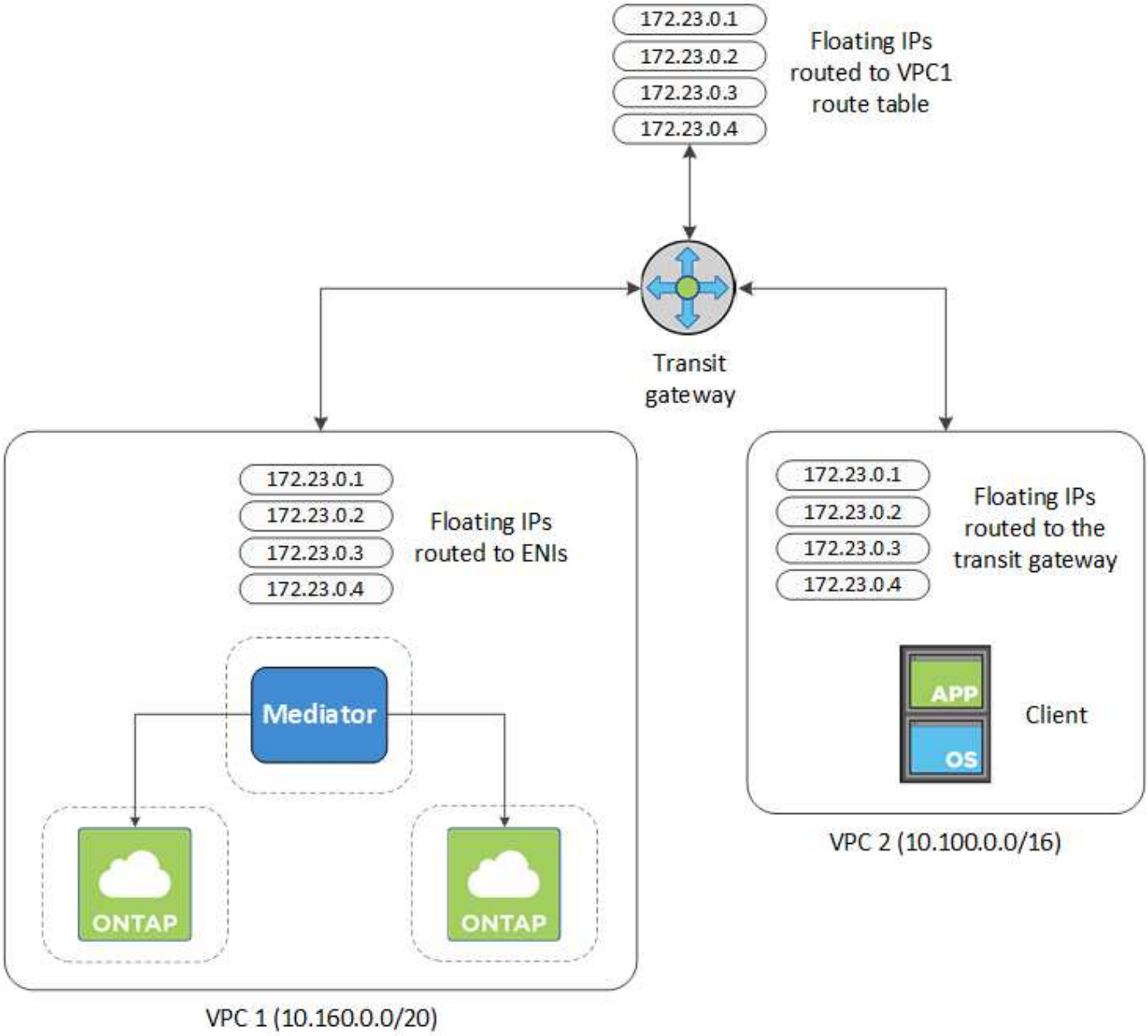
Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha "Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

Quando una configurazione Cloud Volumes ONTAP ha viene distribuita in più zone di disponibilità AWS, sono richiesti indirizzi IP mobili per l'accesso ai dati NAS dall'interno del VPC. Questi indirizzi IP mobili possono migrare tra i nodi in caso di guasti, ma non sono accessibili in modo nativo dall'esterno del VPC. Gli indirizzi IP privati separati forniscono l'accesso ai dati dall'esterno del VPC, ma non forniscono il failover automatico.

Gli indirizzi IP mobili sono richiesti anche per l'interfaccia di gestione del cluster e per la LIF di gestione SVM opzionale.

Se si imposta un gateway di transito AWS, si abilita l'accesso agli indirizzi IP mobili dall'esterno del VPC in cui risiede la coppia ha. Ciò significa che i client NAS e gli strumenti di gestione NetApp esterni al VPC possono accedere agli IP mobili.

Ecco un esempio che mostra due VPC connessi da un gateway di transito. Un sistema ha risiede in un VPC, mentre un client risiede nell'altro. È quindi possibile montare un volume NAS sul client utilizzando l'indirizzo IP mobile.

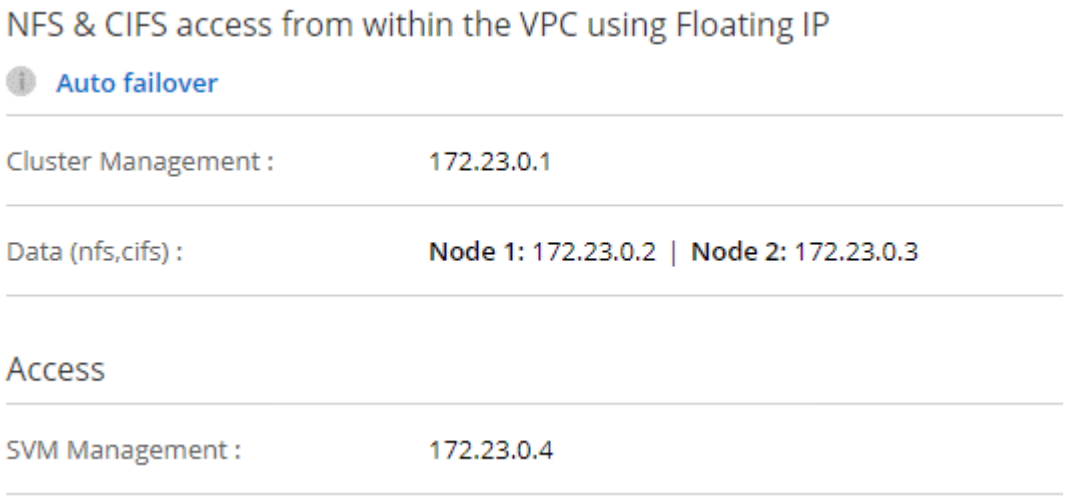


La seguente procedura illustra come configurare una configurazione simile.

Fasi

1. "Creare un gateway di transito e collegare i VPC al gateway".
2. Associare i VPC alla tabella di routing del gateway di transito.
   a. Nel servizio **VPC**, fare clic su **Transit Gateway Route Table**.
   b. Selezionare la tabella dei percorsi.
   c. Fare clic su **Associazioni**, quindi selezionare **Crea associazione**.
   d. Scegliere gli allegati (i VPC) da associare, quindi fare clic su **Crea associazione**.
3. Creare le route nella tabella delle route del gateway di transito specificando gli indirizzi IP mobili della coppia ha.

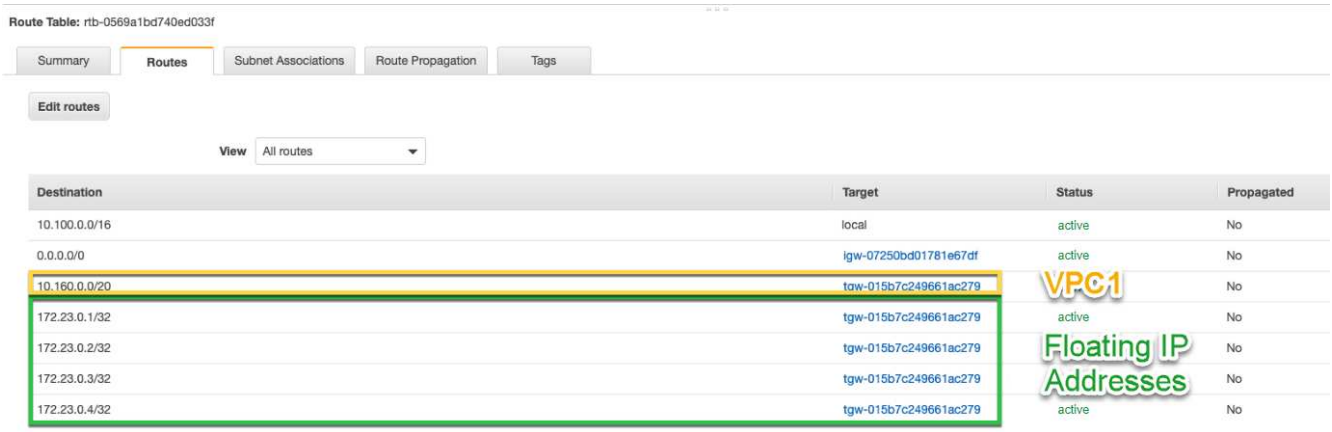
   Gli indirizzi IP mobili sono disponibili nella pagina Working Environment Information (informazioni sull'ambiente di lavoro) di BlueXP. Ecco un esempio:



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

4. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.
   a. Aggiungere voci di routing agli indirizzi IP mobili.
   b. Aggiungere una voce di percorso al blocco CIDR del VPC in cui risiede la coppia ha.

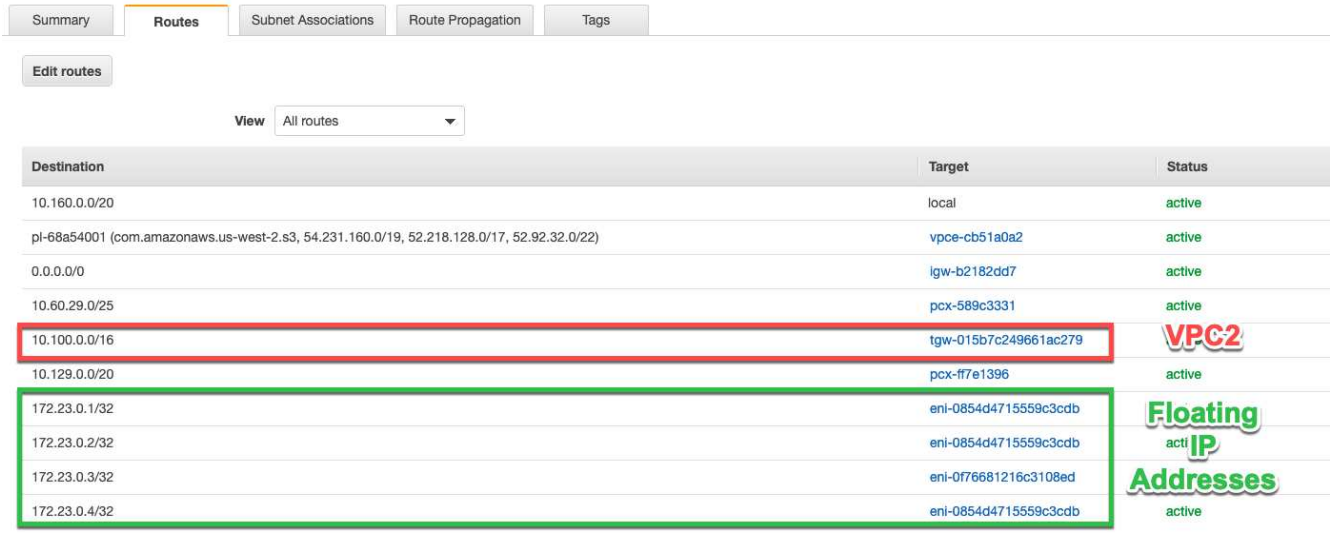
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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

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

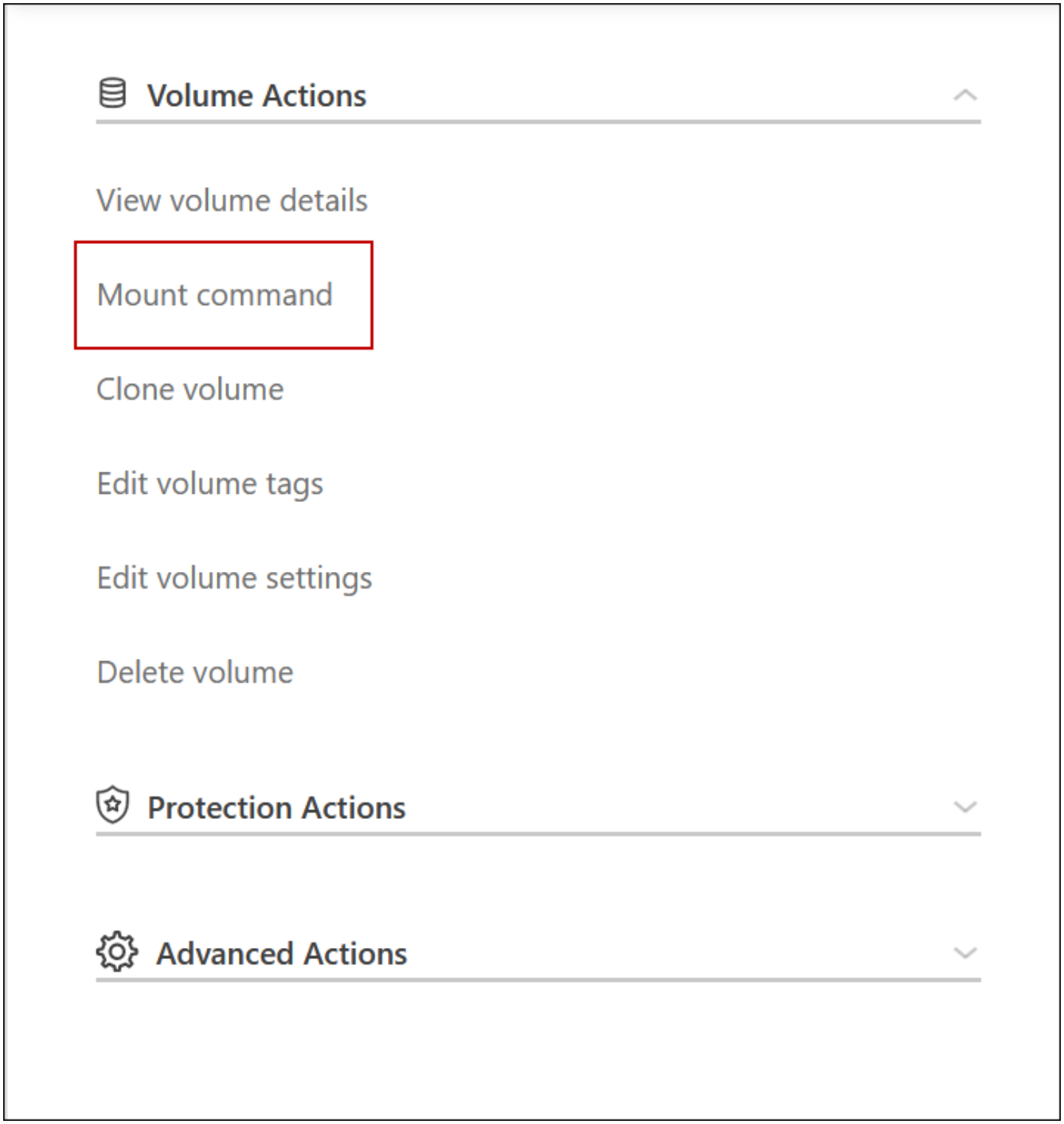
   L'immagine di esempio seguente mostra la tabella di percorso per VPC 1. Include un routing agli indirizzi IP mobili e a VPC 2, che è dove risiede un client. BlueXP ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha implementato la coppia ha.



6. Aggiornare le impostazioni dei gruppi di protezione a tutto il traffico per il VPC.
   a. In Virtual Private Cloud, fare clic su **subnet**.
   b. Fare clic sulla scheda **Tabella di instradamento**, selezionare l'ambiente desiderato per uno degli indirizzi IP mobili per una coppia ha.
   c. Fare clic su **gruppi di sicurezza**.
   d. Selezionare **Modifica regole in entrata**.
   e. Fare clic su **Aggiungi regola**.
   f. In tipo, selezionare **tutto il traffico**, quindi selezionare l'indirizzo IP VPC.
   g. Fare clic su **Salva regole** per applicare le modifiche.
7. Montare i volumi sui client utilizzando l'indirizzo IP mobile.

   È possibile trovare l'indirizzo IP corretto in BlueXP tramite l'opzione **Mount Command** nel pannello

Manage Volumes (Gestisci volumi) di BlueXP.



8. Se si sta montando un volume NFS, configurare il criterio di esportazione in modo che corrisponda alla subnet del VPC client.

   "Scopri come modificare un volume".

Link correlati

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

Implementa le coppie ha Cloud Volumes ONTAP in una subnet condivisa AWS

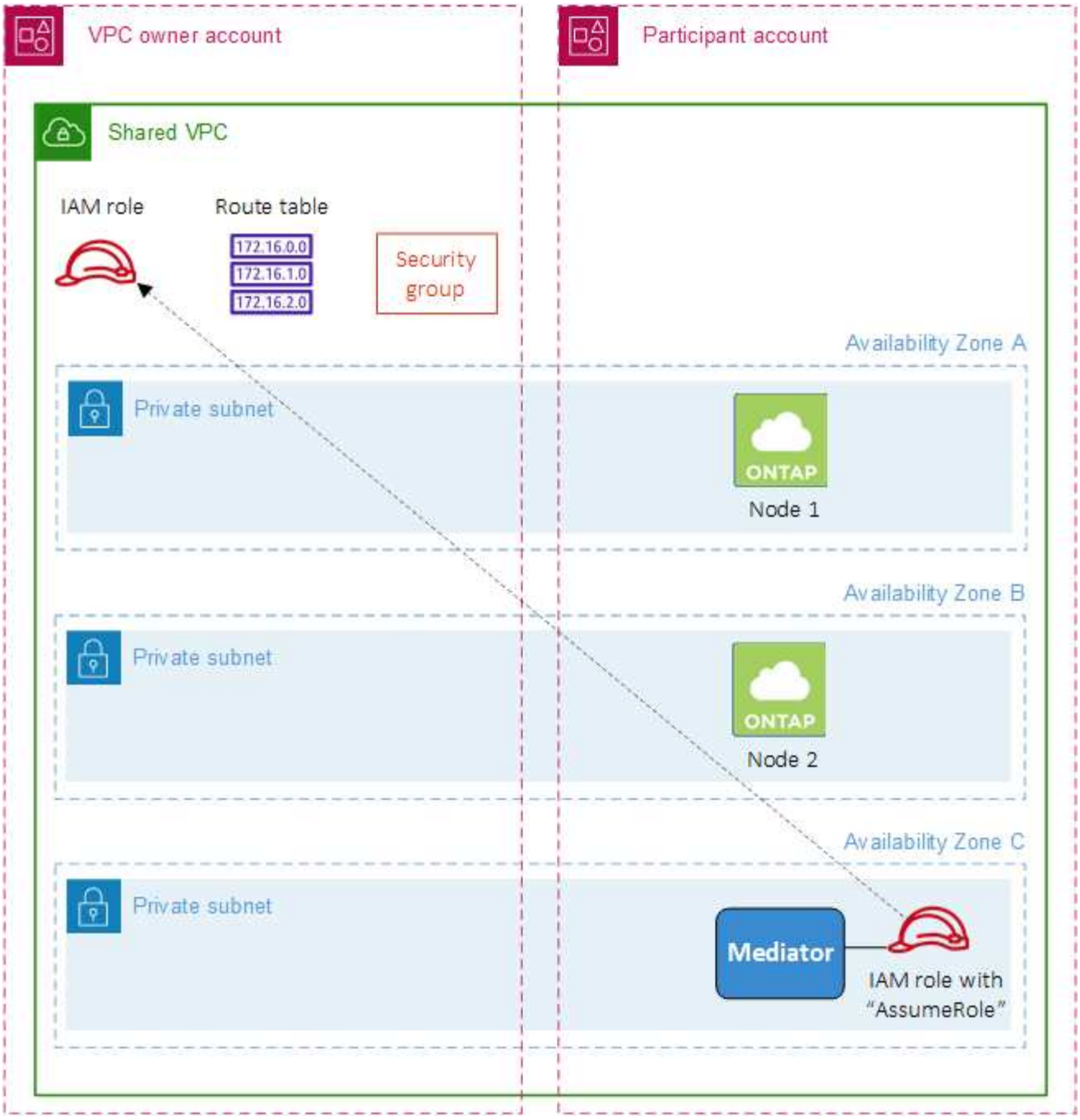
A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP ha sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere le subnet con altri account AWS. Per utilizzare questa configurazione, è necessario configurare l'ambiente AWS e implementare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

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

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

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

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



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

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

Fasi

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

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

   "Documentazione AWS: Consente di condividere una subnet"

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

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

3. Nell'account proprietario del VPC, creare un ruolo IAM che includa le seguenti autorizzazioni:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Utilizzare l'API BlueXP per creare un nuovo ambiente di lavoro Cloud Volumes ONTAP.

   Si noti che è necessario specificare i seguenti campi:

   - "SecurityGroupId"

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

   - "AssumeRoleArn" nell'oggetto "haParams"

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

     Ad esempio:

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

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

Configurare la creazione di gruppi di posizionamento per le coppie ha Cloud Volumes ONTAP in AWS single AZS

In caso di errore della creazione del gruppo di posizionamento, le implementazioni ad alta disponibilità (ha) di Cloud Volumes ONTAP in AWS Single Availability zone (AZ) possono eseguire il failback. Anche la creazione del gruppo di posizionamento non riesce e la distribuzione torna indietro se il nodo Cloud Volumes ONTAP e l'istanza del

mediatore non sono disponibili. Per evitare questo problema, è possibile modificare la configurazione per consentire il completamento della distribuzione anche se la creazione del gruppo di posizionamento non riesce.

Quando si ignora il processo di rollback, il processo di distribuzione di Cloud Volumes ONTAP viene completato correttamente e viene notificato che la creazione del gruppo di posizionamento è incompleta.

Fasi

1. Utilizzare SSH per connettersi all'host del connettore e accedere.
2. Passare a `/opt/application/netapp/cloudmanager/docker_occm/data`.
3. Modificare `app.conf` cambiando il valore del `rollback-on-placement-group-failure` parametro in `false`. Il valore predefinito di questo parametro è `true`.

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Salvare il file e disconnettersi dal connettore. Non è necessario riavviare il connettore.

Regole in entrata e in uscita del gruppo di sicurezza AWS per Cloud Volumes ONTAP

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

Regole per Cloud Volumes ONTAP

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

Regole in entrata

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

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

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione cluster
HTTPS	443	Connettività con il connettore e accesso HTTPS alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita

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

Regole di base in uscita

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

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

Regole avanzate in uscita

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

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

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

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

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

Regole per il gruppo di sicurezza esterno del mediatore ha

Il gruppo di sicurezza esterno predefinito per il mediatore Cloud Volumes ONTAP ha include le seguenti regole in entrata e in uscita.

Regole in entrata

Il gruppo di sicurezza predefinito per il mediatore ha include la seguente regola inbound.

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

Regole in uscita

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

Regole di base in uscita

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

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

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita dal mediatore ha.

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

Anziché aprire le porte 443 e 53, è possibile creare un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2.

Regole per il gruppo di sicurezza interno della configurazione ha

Il gruppo di protezione interno predefinito per una configurazione Cloud Volumes ONTAP ha include le seguenti regole. Questo gruppo di sicurezza consente la comunicazione tra i nodi ha e tra il mediatore e i nodi.

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

Regole in entrata

Il gruppo di sicurezza predefinito include le seguenti regole in entrata.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

Regole in uscita

Il gruppo di protezione predefinito include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

Regole per il connettore

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

Configura Cloud Volumes ONTAP per l'utilizzo di una chiave gestita dal cliente in AWS

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

Fasi

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

   Il CMK può essere un CMK gestito da AWS o un CMK gestito dal cliente. Può trovarsi nello stesso account

AWS di BlueXP e Cloud Volumes ONTAP o in un altro account AWS.

"Documentazione AWS: Customer Master Keys (CMK)"

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

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

   "Documentazione AWS: Modifica delle chiavi"

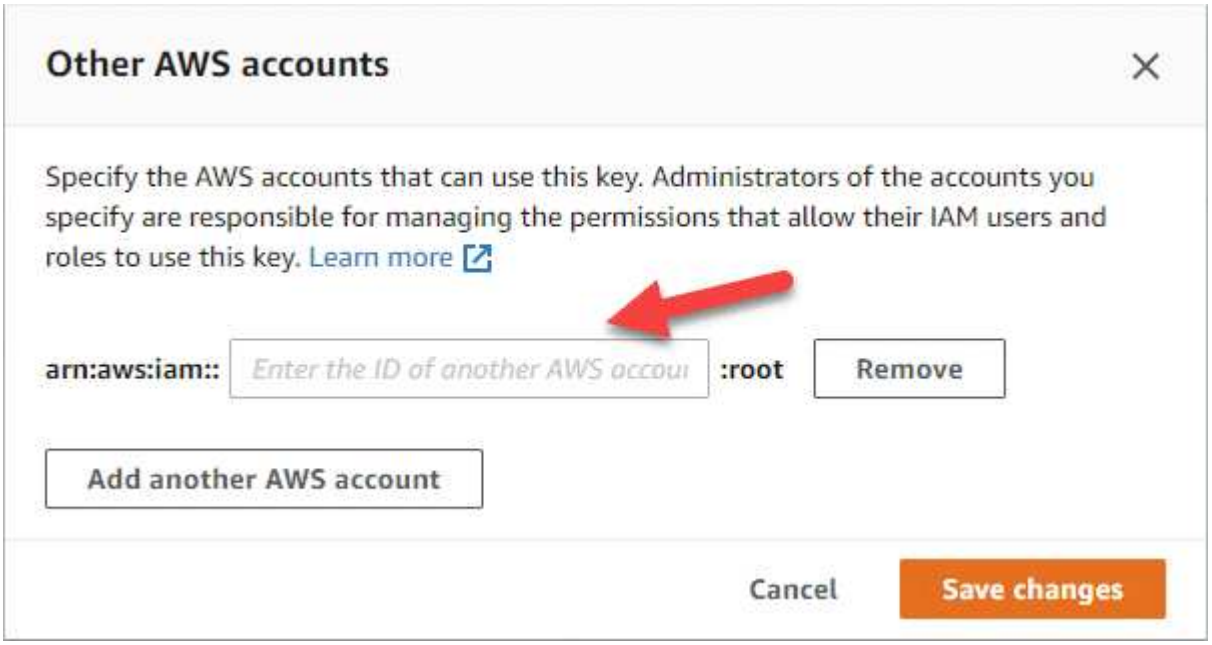
3. Se il CMK si trova in un account AWS diverso, completare la seguente procedura:

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

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

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

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



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

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

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

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

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

+
Per ulteriori informazioni su questo processo, fare riferimento alla "Documentazione AWS: Consente agli utenti di altri account di utilizzare una chiave KMS" .

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

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

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

   "Documentazione AWS: Modifica delle chiavi"

Configurare ruoli AWS IAM per i nodi Cloud Volumes ONTAP

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

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

Nel cloud segreto di AWS è necessario fornire il tuo ruolo IAM. "Scopri come implementare Cloud Volumes ONTAP in C2S".

Fasi

1. Accedere alla console AWS IAM.
2. Creare policy IAM che includano le seguenti autorizzazioni:

   - Policy di base per nodi Cloud Volumes ONTAP

Regioni standard

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

Regioni di GovCloud (USA)

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

Regioni più segrete

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

Regioni segrete

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

- Policy di backup per nodi Cloud Volumes ONTAP

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

Regioni standard

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

Regioni di GovCloud (USA)

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

Regioni più segrete

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

Regioni segrete

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

- MEDIATORE HA

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

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

Risultato

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

Ulteriori informazioni

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

Impostare la licenza per Cloud Volumes ONTAP in AWS

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

Freemium

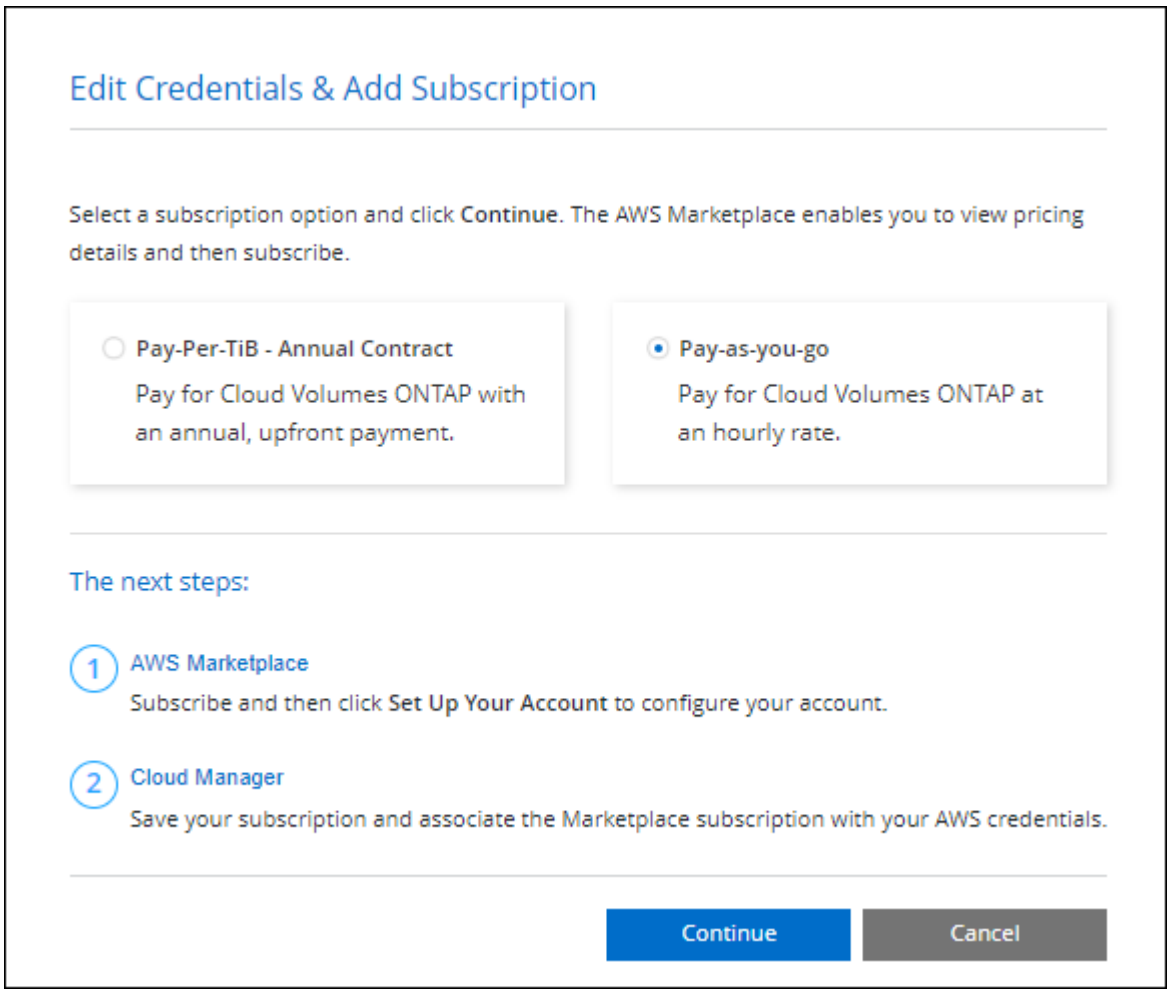
Scegli l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con un massimo di 500 GB di capacità fornita. "Scopri di più sull'offerta Freemium".

Fasi

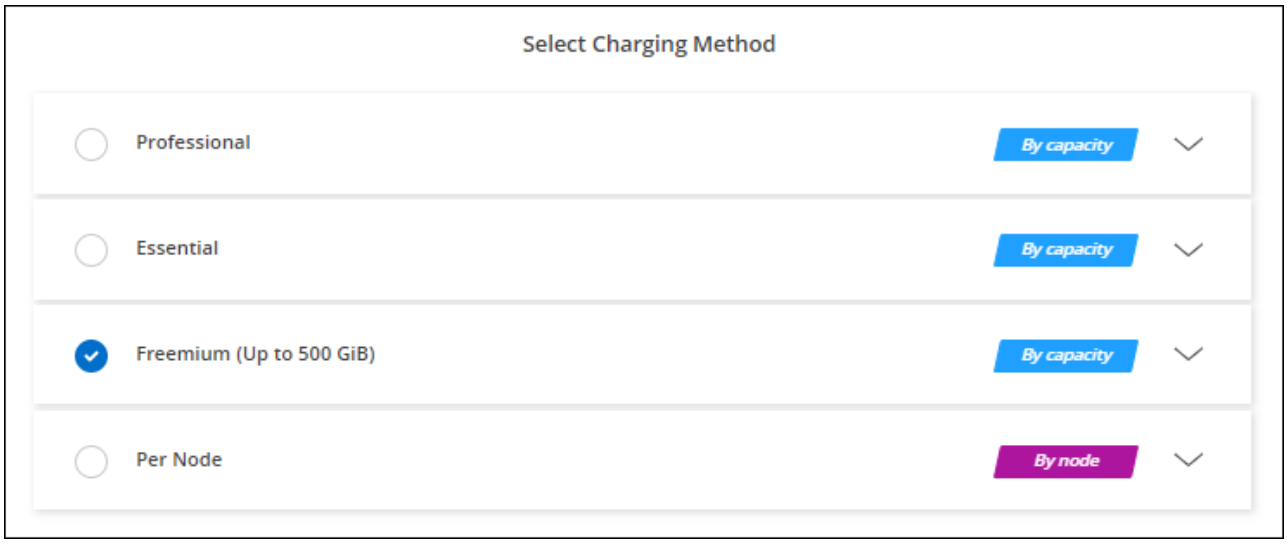
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

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

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



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



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

Licenza basata sulla capacità

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

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

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

"Scopri di più sulle licenze basate sulla capacità".

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

BYOL

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

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Fasi

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

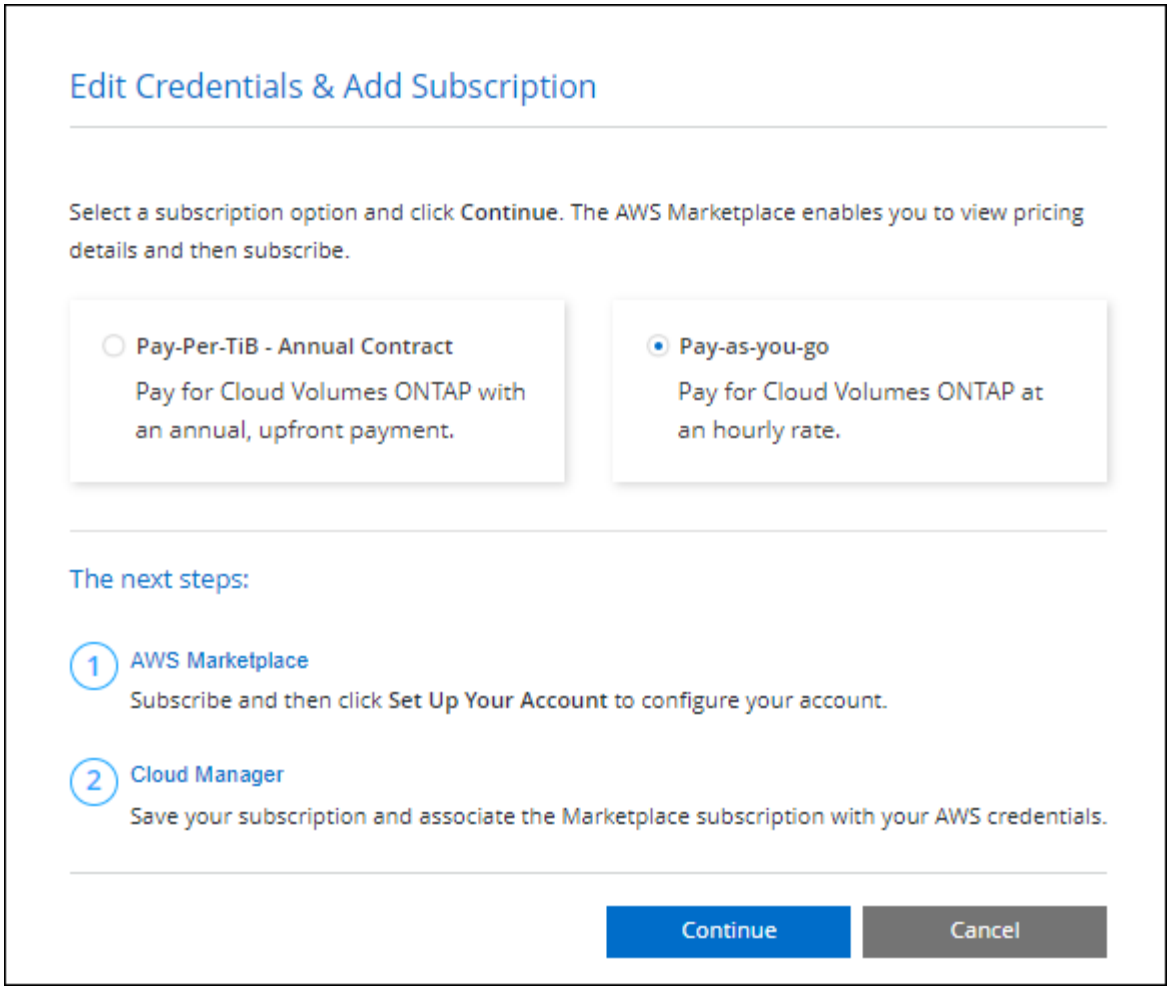
   BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

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

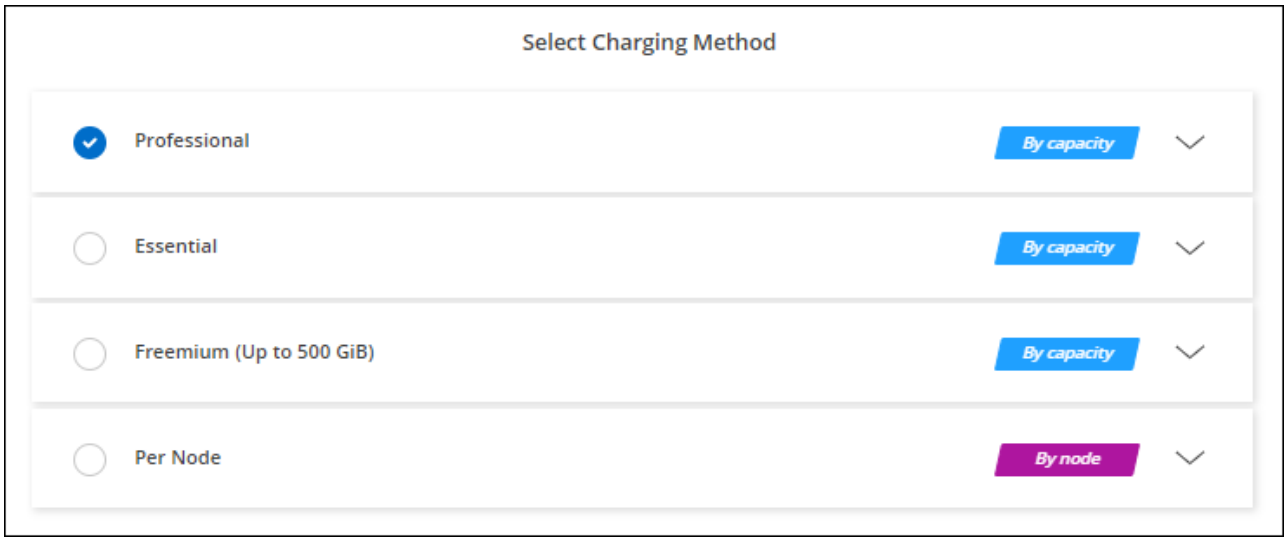
3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

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

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



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



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

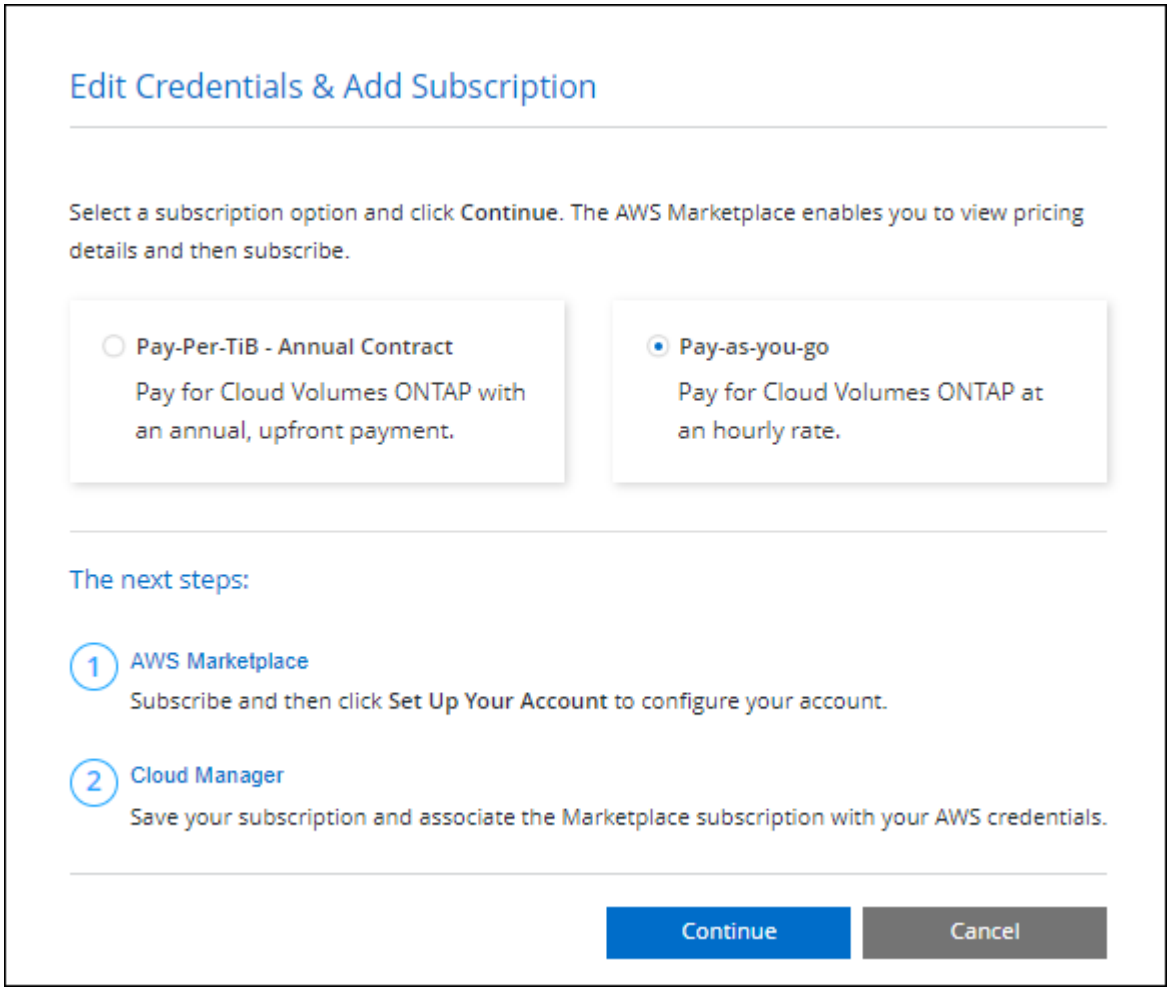
Abbonamento PAYGO

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

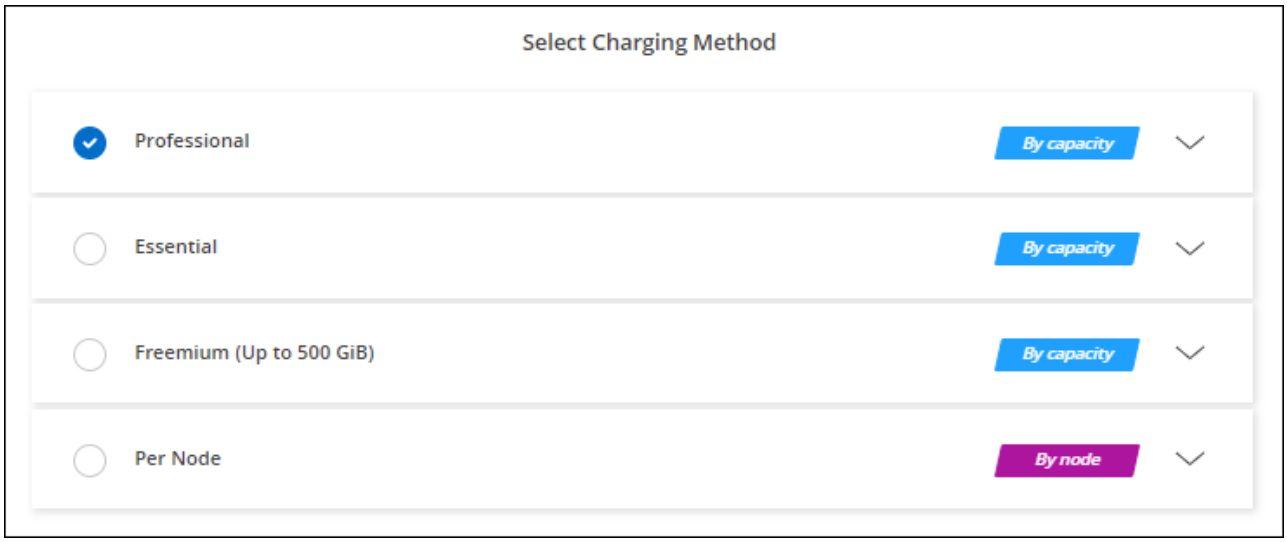
Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, BlueXP richiede di sottoscrivere il contratto disponibile nel marketplace AWS. Tale abbonamento viene quindi associato all'ambiente di lavoro per la ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

Fasi

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



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



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

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

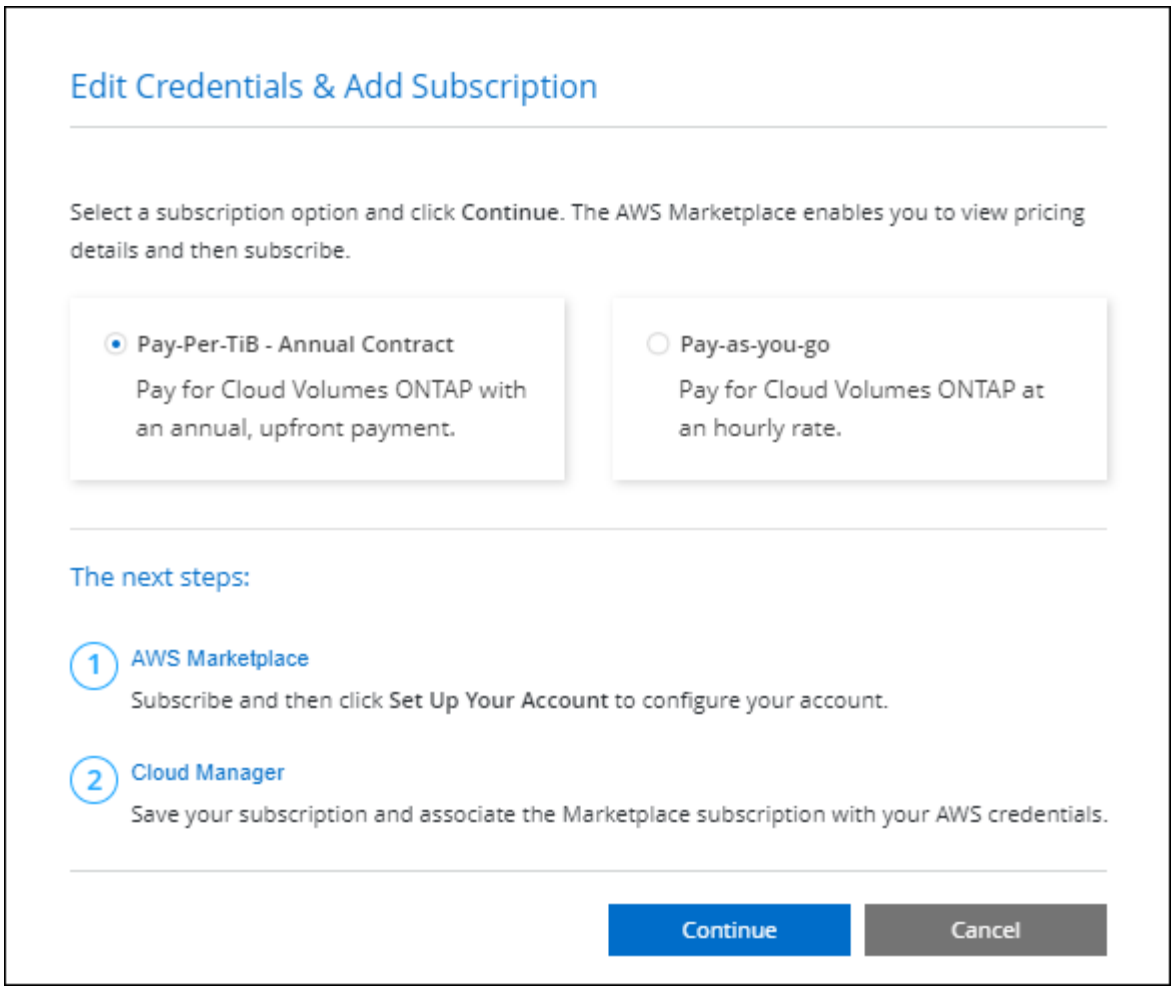
Contratto annuale

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

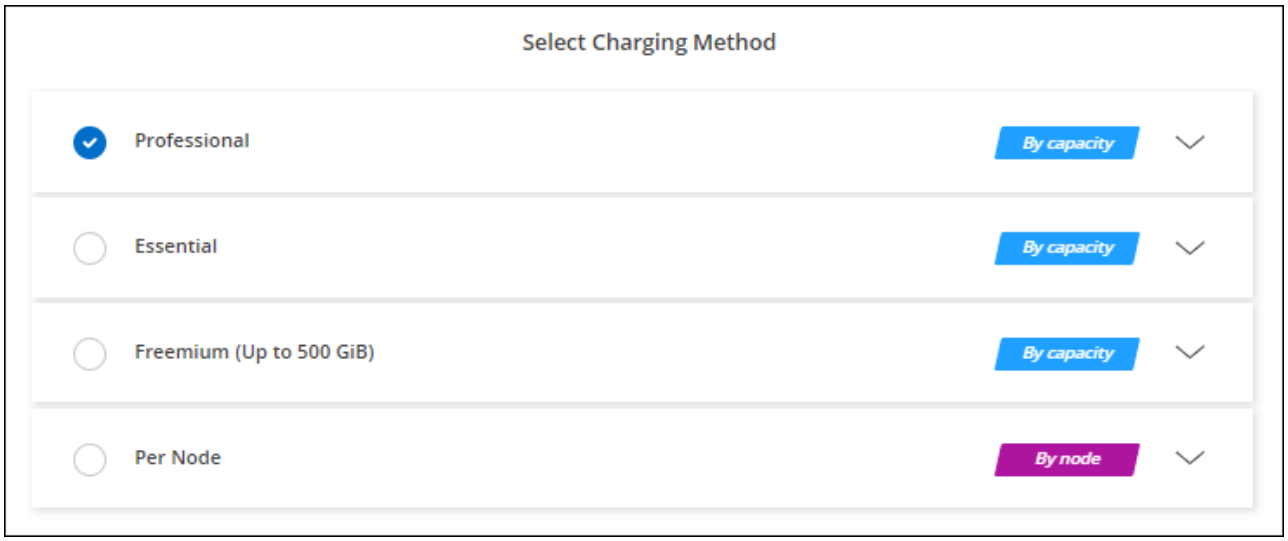
Analogamente a un abbonamento orario, BlueXP richiede di sottoscrivere il contratto annuale disponibile in AWS Marketplace.

Fasi

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



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



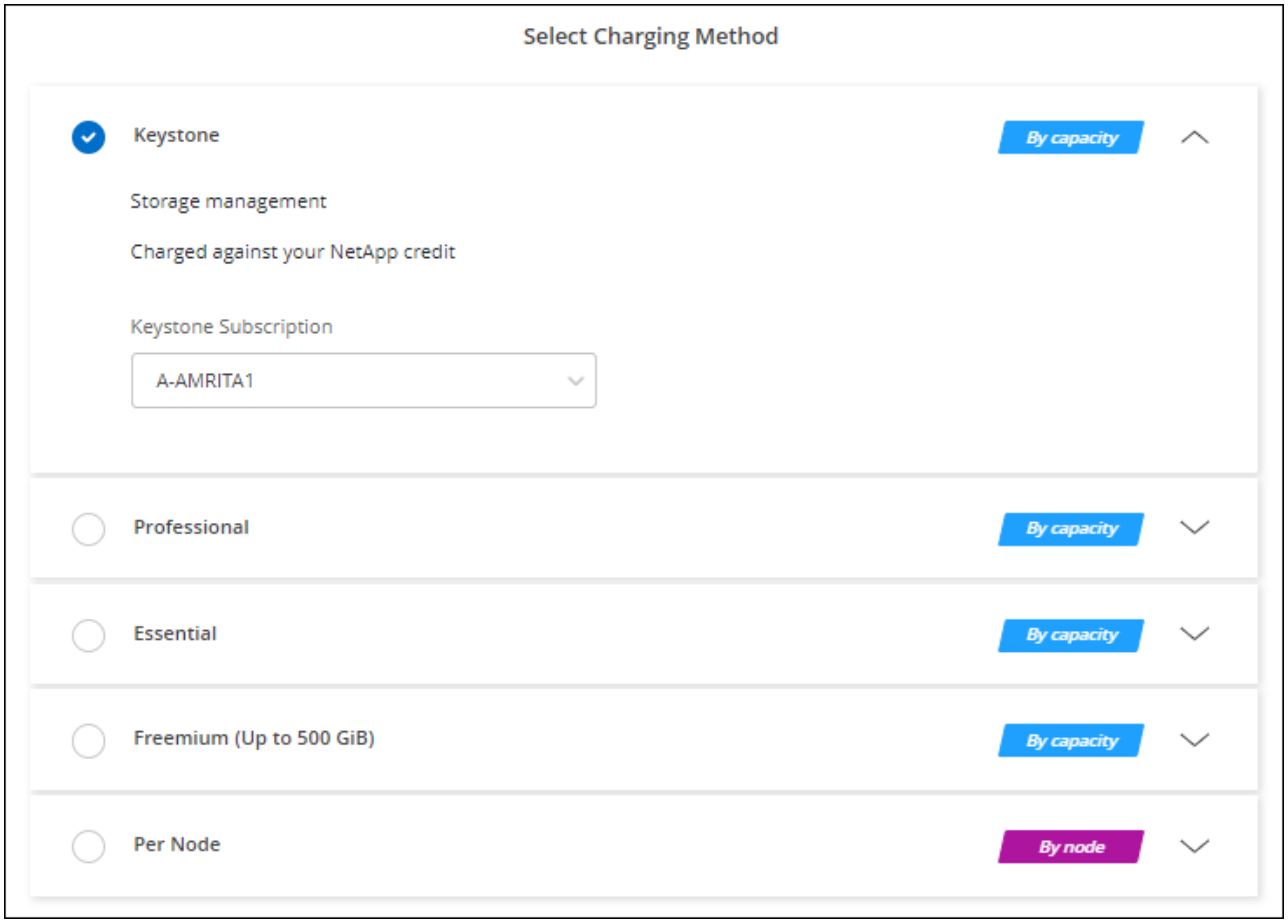
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

Iscrizione Keystone

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

Fasi

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



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

Avviare Cloud Volumes ONTAP in AWS

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

Prima di iniziare

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

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

  Si dovrebbe aver preparato scegliendo una configurazione e ottenendo le informazioni di rete AWS dall'amministratore. Per ulteriori informazioni, fare riferimento alla "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Comprensione di ciò che è necessario per impostare le licenze per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze".
- Configurazioni DNS e Active Directory per CIFS.

  Per ulteriori informazioni, fare riferimento alla "Requisiti di rete per Cloud Volumes ONTAP in AWS".

Lancia un sistema Cloud Volumes ONTAP a nodo singolo in AWS

Per lanciare Cloud Volumes ONTAP in AWS, devi creare un nuovo ambiente di lavoro in BlueXP .

A proposito di questa attività

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

Fasi

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

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

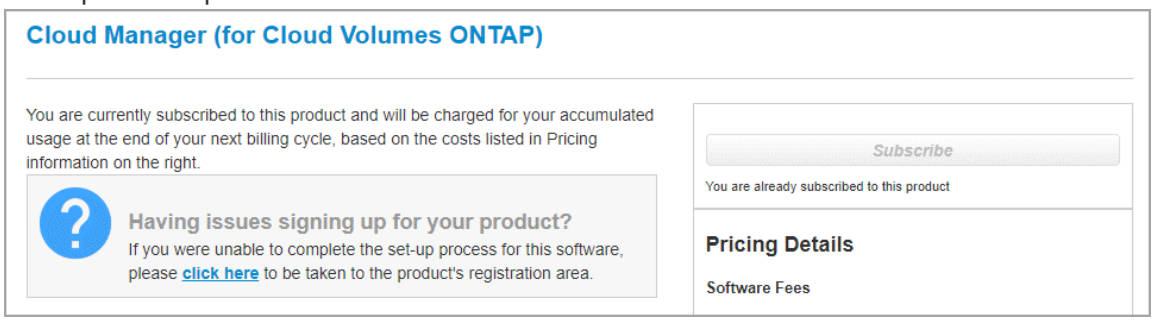
Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.

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

Il seguente video mostra come associare un abbonamento al marketplace con pagamento a consumo alle tue credenziali AWS:

Iscriviti a BlueXP dal marketplace AWS

Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo che il primo utente si è iscritto, il marketplace AWS informa gli utenti successivi che sono già iscritti, come mostrato nell'immagine qui sotto. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi a tale abbonamento. Se vedi il messaggio mostrato di seguito, clicca sul link **clicca qui** per accedere al sito web di BlueXP e completare la procedura.



6. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla classificazione BlueXP"
   - "Scopri di più sul backup e ripristino BlueXP"

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

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

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

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

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

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

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

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

   "Scopri di più sulle tecnologie di crittografia supportate".

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

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

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

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

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

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

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

    > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 è disponibile. L'aggiornamento non viene eseguito da una versione all'altra, ad esempio da 9,13 a 9,14.

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

    Tenere presente quanto segue:

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

      "Scopri come funziona il tiering dei dati".

15. **Velocità di scrittura e WORM**:

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

       "Scopri di più sulla velocità di scrittura".

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

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

    "Scopri di più sullo storage WORM".

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

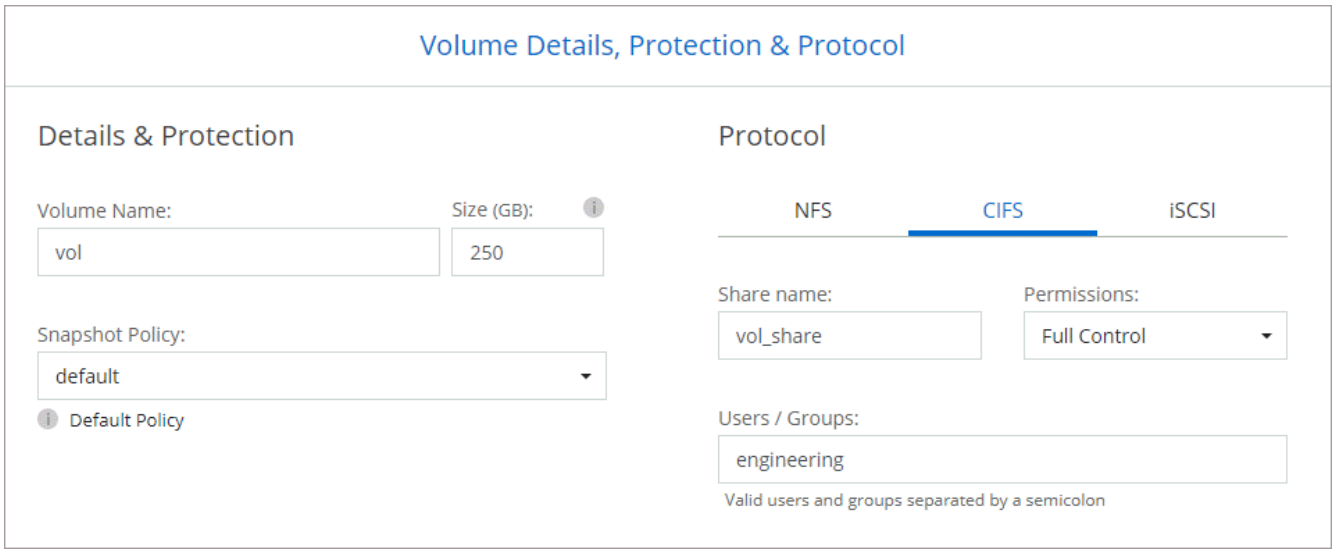
16. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    "Scopri le versioni e i protocolli client supportati".

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

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

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



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

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

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

    Per ulteriori informazioni, fare riferimento a "Comprensione dei profili di utilizzo dei volumi", , "Panoramica sul tiering dei dati"e. "KB: Quali funzionalità di efficienza dello storage inline sono supportate in CVO?"

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

Risultato

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

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

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

Al termine

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

  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.

Lancia una coppia ha Cloud Volumes ONTAP in AWS

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

Limitazione

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

A proposito di questa attività

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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP ha**.

   Sono disponibili alcune zone AWS Local.

   Prima di poter utilizzare AWS Local Zones, è necessario abilitare Local Zones (zone locali) e creare una subnet nella Local zone (zona locale) del proprio account AWS. Segui i passaggi **Opt in to an AWS Local zone** e **Extend your Amazon VPC to the Local zone** nella "Tutorial AWS: Inizia a implementare le applicazioni a bassa latenza con le zone locali AWS".

Se utilizzi una versione di connettore 3.9.36 o precedente, devi aggiungere il seguente permesso al ruolo di connettore AWS nella console AWS EC2: DescribeAvailabilityZones.

4. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e l'abbonamento AWS, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

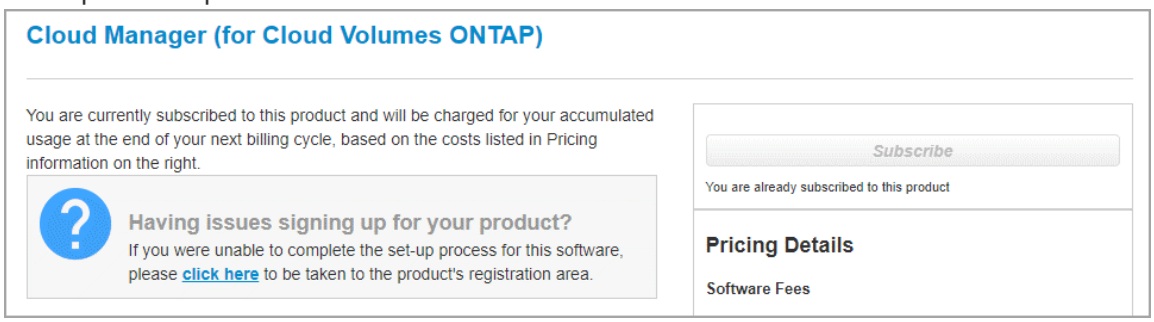
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

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

Il seguente video mostra come associare un abbonamento al marketplace con pagamento a consumo alle tue credenziali AWS:

Iscriviti a BlueXP dal marketplace AWS

Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo che il primo utente si è iscritto, il marketplace AWS informa gli utenti successivi che sono già iscritti, come mostrato nell'immagine qui sotto. Mentre è in vigore un abbonamento per l'*account* AWS, ciascun utente IAM deve associarsi a tale abbonamento. Se vedi il messaggio mostrato di seguito, clicca sul link **clicca qui** per accedere al sito web di BlueXP e completare la procedura.



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

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

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

   Per una panoramica dei modelli di distribuzione, fare riferimento alla "Cloud Volumes ONTAP ha per AWS".

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

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

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

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

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

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

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

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

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

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

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

    "Scopri di più sulle tecnologie di crittografia supportate".

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

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

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

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

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

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

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

Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 è disponibile. L'aggiornamento non viene eseguito da una versione all'altra, ad esempio da 9,13 a 9,14.

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

    Tenere presente quanto segue:

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

      "Scopri come funziona il tiering dei dati".

18. **Velocità di scrittura e WORM**:

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

       "Scopri di più sulla velocità di scrittura".

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

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

    "Scopri di più sullo storage WORM".

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

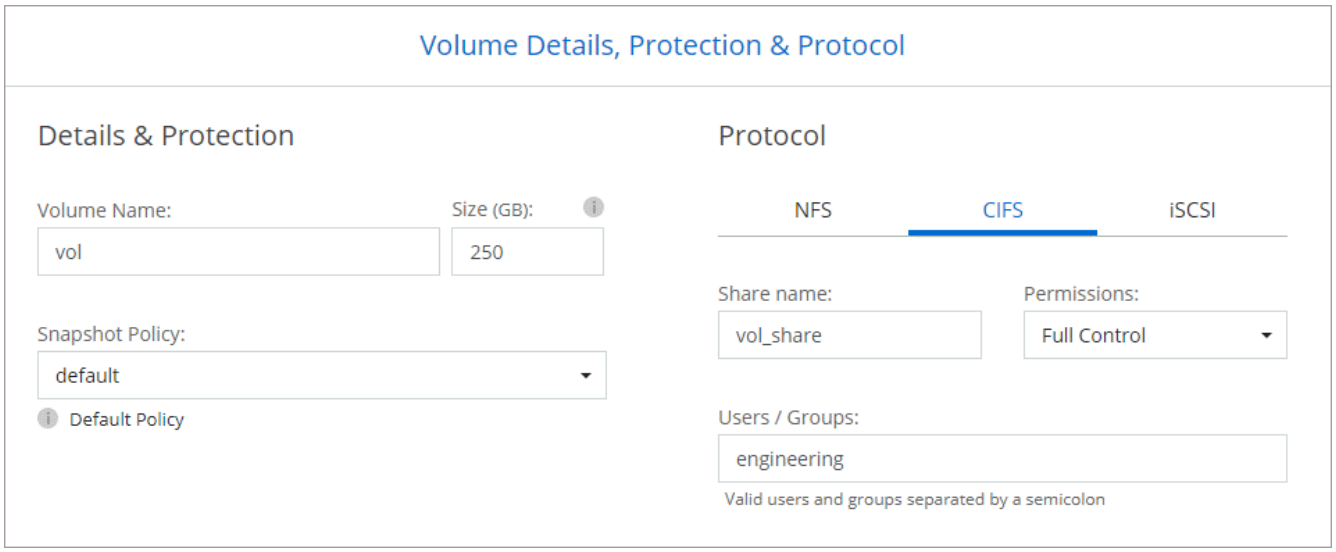
19. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    "Scopri le versioni e i protocolli client supportati".

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

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

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



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

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

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

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

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

Risultato

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

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

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

Al termine

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

  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.

Implementa Cloud Volumes ONTAP in AWS Secret Cloud o AWS Top Secret Cloud

Simile a una regione AWS standard, puoi utilizzare BlueXP in "Cloud segreto AWS" e in "Cloud AWS top secret" Per implementare Cloud Volumes ONTAP, che offre funzionalità Enterprise per il tuo cloud storage. AWS Secret Cloud e Top Secret Cloud sono regioni chiuse specifiche degli Stati Uniti Intelligence Community; le istruzioni in questa pagina si applicano solo agli utenti delle regioni Cloud segreto e Cloud segreto.

Prima di iniziare

Prima di iniziare, esamina le versioni supportate in AWS Secret Cloud e Top Secret Cloud e scopri la modalità privata di BlueXP.

- Consulta le seguenti versioni supportate in AWS Secret Cloud e Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Versione 3.9.32 del connettore

    Il connettore è un software necessario per implementare e gestire Cloud Volumes ONTAP in AWS. Potrai accedere a BlueXP dal software installato sull'istanza del connettore. Il sito web SaaS per BlueXP non è supportato da AWS Secret Cloud e Top Secret Cloud.
- Informazioni sulla modalità privata

  In AWS Secret Cloud e Top Secret Cloud, BlueXP opera in *modalità privata*. In modalità privata, non è disponibile alcuna connettività al livello SaaS di BlueXP. Gli utenti accedono a BlueXP localmente dalla console basata su web disponibile da Connector, non dal layer SaaS.

  Per ulteriori informazioni sul funzionamento della modalità privata, fare riferimento a. "Modalità di implementazione privata di BlueXP".

Fase 1: Configurare il collegamento in rete

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

Fasi

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

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

Passaggio 2: Impostare le autorizzazioni

Impostare policy e ruoli IAM che forniscono a Connector e Cloud Volumes ONTAP le autorizzazioni necessarie per eseguire le azioni nel cloud segreto AWS o nel cloud segreto principale.

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

- L'istanza del connettore
- Istanze di Cloud Volumes ONTAP
- Per coppie ha, l'istanza Cloud Volumes ONTAP ha mediator (se si desidera implementare coppie ha)

Fasi

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

> Crei queste policy per supportare i bucket S3 nel tuo ambiente AWS. Durante la creazione dei bucket in un secondo momento, assicurarsi che i nomi dei bucket siano preceduti da `fabric-pool-`. Questo requisito si applica a entrambe le regioni: Cloud segreto e cloud top secret.

Regioni segrete

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

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

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

Regioni più segrete

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Creare un criterio per Cloud Volumes ONTAP.

Regioni segrete

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

Regioni più segrete

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

Per le coppie ha, se intendi implementare una coppia ha Cloud Volumes ONTAP, crea una policy per il mediatore ha.

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

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

   Creare il ruolo:

   Analogamente ai criteri, è necessario avere un ruolo IAM per il connettore e uno per i nodi Cloud Volumes ONTAP.
   Per coppie ha: Simili alle policy, occorre un ruolo IAM per il connettore, uno per i nodi Cloud Volumes ONTAP e uno per il mediatore ha (se si desidera implementare coppie ha).

   Selezionare il ruolo:

   Quando si avvia l'istanza di Connector, è necessario selezionare il ruolo di Connector IAM. Puoi selezionare i ruoli IAM per Cloud Volumes ONTAP quando crei un ambiente di lavoro Cloud Volumes ONTAP da BlueXP.
   Per le coppie ha, puoi selezionare i ruoli IAM per Cloud Volumes ONTAP e ha mediator quando crei un ambiente di lavoro Cloud Volumes ONTAP da BlueXP.

Fase 3: Configurare il KMS AWS

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

Fasi

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

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

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

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

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

   In questo modo, vengono assegnate autorizzazioni BlueXP per utilizzare CMK con Cloud Volumes ONTAP.

Fase 4: Installare il connettore e configurare BlueXP

Prima di iniziare a usare BlueXP per implementare Cloud Volumes ONTAP in AWS, devi installare e configurare BlueXP Connector. Il connettore consente a BlueXP di gestire risorse e processi all'interno dell'ambiente di cloud pubblico (incluso Cloud Volumes ONTAP).

Fasi

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

   > Per le aree di AWS Secret Cloud, è necessario caricare `NSS Root CA 2` E per il Cloud Top Secret, il `Amazon Root CA 4` certificate (certificato). Assicurarsi di caricare solo questi certificati e non l'intera catena. Il file per la catena di certificati è di grandi dimensioni e il caricamento potrebbe non riuscire. Se si dispone di certificati aggiuntivi, è possibile caricarli in un secondo momento, come descritto nel passaggio successivo.

   Durante il processo di configurazione, è necessario caricare il certificato. BlueXP utilizza il certificato attendibile per inviare richieste ad AWS su HTTPS.

2. Avviare l'istanza di Connector:
   a. Consulta la pagina del marketplace della community dell'intelligenza AWS per BlueXP.
   b. Nella scheda Custom Launch (Avvio personalizzato), scegliere l'opzione per avviare l'istanza dalla console EC2.
   c. Seguire le istruzioni per configurare l'istanza.

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

      - Si consiglia di utilizzare t3.xlarge.
      - È necessario scegliere il ruolo IAM creato quando si impostano le autorizzazioni.
      - È necessario mantenere le opzioni di storage predefinite.
      - I metodi di connessione richiesti per il connettore sono i seguenti: SSH, HTTP e HTTPS.
3. Configurare BlueXP da un host che ha una connessione all'istanza del connettore:
   a. Aprire un browser Web e immettere https://ipaddress Dove ipaddress è l’indirizzo IP dell’host Linux in cui è stato installato il connettore.
   b. Specificare un server proxy per la connettività ai servizi AWS.
   c. Caricare il certificato ottenuto al punto 1.
   d. Selezionare **Set Up New BlueXP** (Configura nuovo BlueXP*) e seguire le istruzioni per configurare il sistema.
      - **Dettagli sistema**: Inserire un nome per il connettore e il nome della società.
      - **Create Admin User** (Crea utente amministratore): Consente di creare l'utente amministratore per il sistema.

Questo account utente viene eseguito localmente sul sistema. Non esiste alcuna connessione al servizio auth0 disponibile tramite BlueXP.

- **Revisione**: Esaminare i dettagli, accettare il contratto di licenza, quindi selezionare **Configurazione**.

e. Per completare l'installazione del certificato firmato dalla CA, riavviare l'istanza del connettore dalla console EC2.

4. Una volta riavviato il connettore, accedere utilizzando l'account utente amministratore creato nell'installazione guidata.

Passaggio 5: (Facoltativo) installare un certificato in modalità privata

Questo passaggio è opzionale per le regioni Cloud segreto AWS e Cloud segreto superiore ed è necessario solo se si dispone di certificati aggiuntivi oltre ai certificati di origine installati nel passaggio precedente.

Fasi

1. Elencare i certificati installati esistenti.
   a. Per raccogliere l'id occm Container docker (nome identificato "ds-occm-1"), eseguire il seguente comando:

```
docker ps
```

   b. Per entrare nel contenitore occm, eseguire il comando seguente:

```
docker exec -it <docker-id> /bin/sh
```

   c. Per raccogliere la password dalla variabile di ambiente "TRUST_STORE_PASSWORD", eseguire il seguente comando:

```
env
```

   d. Per elencare tutti i certificati installati in truststore, eseguire il comando seguente e utilizzare la password raccolta nel passaggio precedente:

```
keytool -list -v -keystore occm.truststore
```

2. Aggiunta di un certificato.
   a. Per raccogliere l'id occm Container docker (nome identificato "ds-occm-1"), eseguire il seguente comando:

```
docker ps
```

   b. Per entrare nel contenitore occm, eseguire il comando seguente:

```
docker exec -it <docker-id> /bin/sh
```

Salvare il nuovo file di certificato.

c. Per raccogliere la password dalla variabile di ambiente "TRUST_STORE_PASSWORD", eseguire il seguente comando:

```
env
```

d. Per aggiungere il certificato al truststore, eseguire il comando seguente e utilizzare la password del passaggio precedente:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. Per verificare che il certificato sia installato, eseguire il comando seguente:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. Per uscire dal contenitore occm, eseguire il comando seguente:

```
exit
```

g. Per ripristinare occm container, eseguire il comando seguente:

```
docker restart <docker-id>
```

Fase 6: Aggiunta di una licenza al Digital Wallet di BlueXP

Se hai acquistato una licenza da NetApp, devi aggiungerla al Digital Wallet di BlueXP in modo da poterla selezionare quando crei un nuovo sistema Cloud Volumes ONTAP. Il portafoglio digitale identifica le 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.
6. Se non si dispone ancora del file di licenza, è necessario caricare manualmente il file di licenza da netapp.com.

a. Accedere alla "NetApp License file Generator" Ed effettua l'accesso utilizzando le credenziali del sito di supporto NetApp.

b. 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**.

c. Scegliere se si desidera ricevere il file serialnumber.NLF JSON tramite e-mail o download diretto.

7. 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. Quindi, la licenza passa alla scheda BYOL del portafoglio digitale.

Fase 7: Avviare Cloud Volumes ONTAP da BlueXP

È possibile avviare le istanze Cloud Volumes ONTAP nel cloud segreto e nel cloud segreto principale di AWS creando nuovi ambienti di lavoro in BlueXP.

Prima di iniziare

Per le coppie ha, è necessaria una coppia di chiavi per abilitare l'autenticazione SSH basata su chiave al mediatore ha.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro**.
2. In **Crea**, selezionare Cloud Volumes ONTAP.

   Per ha: In **Crea**, selezionare Cloud Volumes ONTAP o Cloud Volumes ONTAP ha.

3. Completare la procedura guidata per avviare il sistema Cloud Volumes ONTAP.

> Durante le selezioni effettuate mediante la procedura guidata, non selezionare **Data Sense & Compliance** e **Backup su cloud** in **servizi**. In **pacchetti preconfigurati**, seleziona **Cambia solo configurazione** e assicurati di non aver selezionato altre opzioni. I pacchetti preconfigurati non sono supportati nelle regioni Cloud Secret e Cloud Top Secret e, se selezionati, l'implementazione non avrà esito positivo.

Note per l'implementazione di ha Cloud Volumes ONTAP in più zone di disponibilità

Segui quanto segue al termine della procedura guidata per le coppie ha.

- È necessario configurare un gateway di transito quando si implementa Cloud Volumes ONTAP ha in più zone di disponibilità (AZS). Per istruzioni, fare riferimento alla "Configurare un gateway di transito AWS".
- Implementa la configurazione come segue, perché al momento della pubblicazione erano disponibili solo due zone di disponibilità nell'AWS Top Secret Cloud:
  - Nodo 1: Zona di disponibilità A.
  - Nodo 2: Zona di disponibilità B
  - Mediatore: Zona di disponibilità A o B.

Note per l'implementazione di Cloud Volumes ONTAP nei singoli nodi e nei nodi ha

Al termine della procedura guidata, tenere presente quanto segue:

- Lasciare l'opzione predefinita per utilizzare un gruppo di protezione generato.

  Il gruppo di protezione predefinito include le regole necessarie per il corretto funzionamento di Cloud Volumes ONTAP. Se hai un requisito per utilizzare il tuo, puoi fare riferimento alla sezione relativa al gruppo di sicurezza riportata di seguito.

- È necessario scegliere il ruolo IAM creato durante la preparazione dell'ambiente AWS.
- Il tipo di disco AWS sottostante è per il volume Cloud Volumes ONTAP iniziale.

  È possibile scegliere un tipo di disco diverso per i volumi successivi.

- Le prestazioni dei dischi AWS sono legate alle dimensioni dei dischi.

  È necessario scegliere le dimensioni del disco in grado di garantire le prestazioni costanti necessarie. Fare riferimento alla documentazione AWS per ulteriori dettagli sulle prestazioni EBS.

- La dimensione del disco è la dimensione predefinita per tutti i dischi del sistema.

> Se in un secondo momento è necessaria una dimensione diversa, è possibile utilizzare l'opzione Advanced allocation (allocazione avanzata) per creare un aggregato che utilizza dischi di una dimensione specifica.

Risultato

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

Passaggio 8: Installazione dei certificati di protezione per il tiering dei dati

Devi installare manualmente i certificati di sicurezza per abilitare il tiering dei dati nelle regioni di AWS Secret Cloud e Top Secret Cloud.

Prima di iniziare

1. Creare bucket S3.

> Assicurarsi che i nomi dei bucket siano preceduti da `fabric-pool-`. Ad esempio `fabric-pool-testbucket`.

2. Conservare i certificati di origine installati in `step 4` comodo.

Fasi

1. Copiare il testo dai certificati di origine installati in `step 4`.
2. Connettersi in modo sicuro al sistema Cloud Volumes ONTAP utilizzando la CLI.
3. Installare i certificati di origine. Potrebbe essere necessario premere il `ENTER` tasti più volte:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. Quando richiesto, immettere l'intero testo copiato, inclusi e da `----- BEGIN CERTIFICATE -----` a. `----- END CERTIFICATE -----`.

5. Conservare una copia del certificato digitale firmato dalla CA per riferimenti futuri.
6. Conservare il nome della CA e il numero di serie del certificato.
7. Configurare l'archivio di oggetti per il cloud segreto AWS e le aree del cloud top secret: `set -privilege advanced -confirmations off`
8. Eseguire questo comando per configurare l'archivio oggetti.

> Tutti i nomi delle risorse Amazon (Arns) devono essere contrassegnati con il suffisso `-iso-b`, ad esempio `arn:aws-iso-b`. Ad esempio, se una risorsa richiede un ARN con una regione, per Top Secret Cloud, utilizzare la convenzione di denominazione come `us-iso-b` per `-server` allarme. Per AWS Secret Cloud, utilizza `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Verificare che l'archivio oggetti sia stato creato correttamente: `storage aggregate object-store show -instance`
10. Collegare l'archivio di oggetti all'aggregato. Questo deve essere ripetuto per ogni nuovo aggregato: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Inizia a utilizzare Microsoft Azure

Scopri le opzioni di implementazione di Cloud Volumes ONTAP in Azure

NetApp offre due opzioni per implementare Cloud Volumes ONTAP in Azure. Cloud Volumes ONTAP si affida tradizionalmente a BlueXP per l'implementazione e l'orchestrazione. A partire da Cloud Volumes ONTAP 9.16.1, puoi sfruttare l'implementazione diretta di Azure Marketplace, un processo ottimizzato che fornisce l'accesso a un set limitato ma comunque potente di funzionalità e opzioni Cloud Volumes ONTAP.

Quando implementi Cloud Volumes ONTAP direttamente dal marketplace di Azure, non ti viene richiesto di configurare BlueXP Connector o di soddisfare altri criteri di sicurezza e onboarding richiesti per la distribuzione di Cloud Volumes ONTAP tramite BlueXP . Dal marketplace di Azure, puoi implementare rapidamente Cloud Volumes ONTAP in pochi clic ed esplorarne le caratteristiche e le funzionalità principali nel tuo ambiente.

Una volta completata l'implementazione nel marketplace di Azure, è possibile rilevare questi sistemi in BlueXP . Dopo la Discovery, sarà possibile gestirli come ambienti di lavoro e sfruttare tutte le funzionalità di BlueXP . Fare riferimento alla "Scopri i sistemi implementati in BlueXP ".

Di seguito viene riportato il confronto delle funzioni tra le due opzioni. Si noti che le funzionalità di un'istanza standalone implementata attraverso il marketplace di Azure cambiano quando viene rilevata in BlueXP .

	Marketplace Azure	BlueXP
Onboarding	Più breve e semplice, preparazione minima necessaria per l'implementazione diretta	Processo di inserimento più lungo, inclusa l'installazione del connettore BlueXP
Tipi di macchine virtuali supportati	Tipi di istanza EDS_v5 e LS_v3	Gamma completa di tipi di VM. "Configurazioni supportate in Azure"
Licenza	Licenza gratuita	Qualsiasi licenza basata sulla capacità. "Licenze Cloud Volumes ONTAP"
Supporto NetApp	Non incluso	Disponibile, in base al tipo di licenza
Capacità	Fino a 500 GiB	Espandibile per configurazione
Modello di distribuzione	Implementazione in modalità ad alta disponibilità (ha) in una singola zona di disponibilità (AZ)	Tutte le configurazioni supportate, incluse le modalità ha e a nodo singolo, le implementazioni AZ singole e multiple
Tipo di disco supportato	SSD Premium, v2 dischi gestiti	Supporto più ampio. "Configurazione predefinita per Cloud Volumes ONTAP"
Velocità di scrittura (modalità di scrittura veloce)	Non supportato	Supportato, in base alla configurazione. "Scopri le velocità di scrittura in Cloud Volumes ONTAP".
Capacità di orchestrazione	Non disponibile	Disponibile tramite BlueXP , in base al tipo di licenza
Numero di VM di storage supportate	Uno per implementazione	Macchine virtuali storage multiple in base alla tua configurazione. "Numero di VM storage supportate"
Modifica del tipo di istanza	Non supportato	Supportato
Tiering FabricPool	Non supportato	Supportato

Link correlati

- Implementazione diretta del marketplace Azure: "Implementa Cloud Volumes ONTAP dal marketplace di Azure"
- Distribuzione BlueXP : "Avvio rapido di Cloud Volumes ONTAP in Azure"
- "Documentazione BlueXP"

Inizia subito a BlueXP

Avvio rapido di Cloud Volumes ONTAP in Azure

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

1 Creare un connettore

Se non si dispone ancora di un "Connettore", è necessario crearne uno. "Scopri come creare un connettore in Azure"

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

2 Pianificare la configurazione

BlueXP offre pacchetti preconfigurati che soddisfano i requisiti del carico di lavoro, oppure è possibile creare una configurazione personalizzata. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. Per informazioni, fare riferimento alla "Pianificare la configurazione di Cloud Volumes ONTAP in Azure".

3 Configurare la rete

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

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

"Scopri di più sui requisiti di rete".

4 Avviare Cloud Volumes ONTAP utilizzando BlueXP

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

Link correlati

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

Pianificare la configurazione di Cloud Volumes ONTAP in Azure

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

Scegliere una licenza Cloud Volumes ONTAP

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

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

Scegliere una regione supportata

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

Scegliere un tipo di macchina virtuale supportato

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

"Configurazioni supportate per Cloud Volumes ONTAP in Azure"

Comprendere i limiti dello storage

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

"Limiti di storage per Cloud Volumes ONTAP in Azure"

Dimensionare il sistema in Azure

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

Tipo di macchina virtuale

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

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

Tipo di disco Azure con sistemi a nodo singolo

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

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

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- *Dischi gestiti Premium SSD da v2 GB* offrono prestazioni più elevate con latenza inferiore a un costo inferiore rispetto ai dischi gestiti Premium SSD.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.

- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

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

Tipo di disco Azure con coppie ha

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

Dimensioni del disco Azure

Quando si avviano le istanze di Cloud Volumes ONTAP, è necessario scegliere la dimensione predefinita del disco per gli aggregati. BlueXP utilizza questa dimensione del disco per l'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa da quella predefinita di "utilizzando l'opzione di allocazione avanzata".

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

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

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

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

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

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

Visualizzare i dischi di sistema predefiniti

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

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

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

Raccogliere informazioni di rete

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

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

Scegliere una velocità di scrittura

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

Scegliere un profilo di utilizzo del volume

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

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

Thin provisioning

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

Deduplica

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

Compressione

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

Configura il networking Azure per Cloud Volumes ONTAP

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

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti di rete devono essere soddisfatti in Azure.

Accesso a Internet in uscita

I sistemi Cloud Volumes ONTAP richiedono l'accesso a Internet outbound per l'accesso a endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con severi requisiti di sicurezza.

BlueXP Connector contatta anche diversi endpoint per le operazioni quotidiane e la console basata sul Web di BlueXP . Per informazioni sugli endpoint BlueXP , fare riferimento a "Visualizzare gli endpoint contattati dal connettore" e "Preparazione del networking per l'utilizzo della console BlueXP".

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Endpoint	Applicabile per	Scopo	Modalità di implementazione di BlueXP	Impatto se non disponibile
https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione BlueXP .	Modalità standard e limitata.	L'autenticazione dell'utente non riesce e i seguenti servizi rimangono non disponibili: • I servizi di Cloud Volumes ONTAP • Servizi ONTAP • E servizi proxy
https://vault.azure.net	Vault delle chiavi	Utilizzato per recuperare le chiavi segrete client da Azure Key Vault quando si utilizzano chiavi gestite dal cliente (CMK).	Modalità standard, limitata e privata.	I servizi Cloud Volumes ONTAP non sono disponibili.
https://cloudmanager.cloud.netapp.com/tenancy	Locazione	Utilizzato per recuperare le risorse Cloud Volumes ONTAP dalla tenancy BlueXP per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
https://support.NetApp.com/aods/asuppmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Utilizzato per inviare dati telemetrici AutoSupport al supporto NetApp.	Modalità standard e limitata.	Le informazioni AutoSupport rimangono non trasmesse.
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Regioni pubbliche	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non può comunicare con il servizio Azure per eseguire operazioni BlueXP specifiche in Azure.

Endpoint	Applicabile per	Scopo	Modalità di implementazione di BlueXP	Impatto se non disponibile
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Cina	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non può comunicare con il servizio Azure per eseguire operazioni BlueXP specifiche in Azure.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Germania	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non può comunicare con il servizio Azure per eseguire operazioni BlueXP specifiche in Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Degli Stati Uniti	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non può comunicare con il servizio Azure per eseguire operazioni BlueXP specifiche in Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Regioni DoD del governo	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non può comunicare con il servizio Azure per eseguire operazioni BlueXP specifiche in Azure.

Configurazioni di rete per supportare il proxy del connettore

È possibile utilizzare i server proxy configurati per BlueXP Connector per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. BlueXP supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy del connettore. L'amministratore del connettore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato nell'ambiente di lavoro Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP attraverso il proxy del connettore. Quando si configura un proxy trasparente,

l'amministratore del connettore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurarsi di ottenere e caricare lo stesso certificato CA radice nell'ambiente di lavoro Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy per BlueXP Connector, fare riferimento a "Configurare un connettore per l'utilizzo di un server proxy" .

Indirizzi IP

BlueXP assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Azure. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi IP privati.

Il numero di LIF allocati da BlueXP per Cloud Volumes ONTAP dipende dalla distribuzione di un sistema a nodo singolo o di una coppia ha. LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

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

Indirizzi IP per un sistema a nodo singolo

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

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

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

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

Indirizzi IP per coppie ha

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

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

NIC0

- IP di gestione dei nodi
- IP intercluster
- IP iSCSI

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

NIC1

- IP della rete del cluster

NIC2

- Cluster Interconnect IP (IC ha)

NIC3

- IP NIC Pageblob (accesso al disco)

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

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

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

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

Connessioni sicure ai servizi Azure

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

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

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

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

Connessioni ad altri sistemi ONTAP

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

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

Porta per l'interconnessione ha

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

Per impostazione predefinita, la comunicazione tra le LIF di interconnessione ha è aperta e non esistono regole di gruppo di sicurezza per questa porta. Tuttavia, se si crea un firewall tra le LIF di interconnessione ha, è necessario assicurarsi che il traffico TCP sia aperto per la porta 10006 in modo che la coppia ha possa funzionare correttamente.

Solo una coppia ha in un gruppo di risorse Azure

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

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

Regole del gruppo di sicurezza

BlueXP crea gruppi di sicurezza di Azure che includono le regole in ingresso e in uscita affinché Cloud Volumes ONTAP funzioni correttamente. "Visualizzare le regole del gruppo di protezione per il connettore" .

I gruppi di sicurezza di Azure per Cloud Volumes ONTAP richiedono che le porte appropriate siano aperte per la comunicazione interna tra i nodi. "Informazioni sulle porte interne di ONTAP" .

Si sconsiglia di modificare i gruppi di sicurezza predefiniti o di utilizzare gruppi di sicurezza personalizzati. Tuttavia, se necessario, si noti che il processo di distribuzione richiede che il sistema Cloud Volumes ONTAP abbia accesso completo alla propria subnet. Al termine della distribuzione, se si decide di modificare il gruppo di sicurezza di rete, assicurarsi di mantenere aperte le porte del cluster e le porte di rete HA. Ciò garantisce una comunicazione fluida all'interno del cluster Cloud Volumes ONTAP (comunicazione any-to-any tra i nodi).

Regole in entrata per sistemi a nodo singolo

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

- **Solo VNET selezionato**: L'origine del traffico in entrata è l'intervallo di sottorete del VNET per il sistema Cloud Volumes ONTAP e l'intervallo di sottorete del VNET in cui risiede il connettore. Questa è l'opzione consigliata.
- **All VNets**: La fonte del traffico in entrata è l'intervallo IP 0,0.0.0/0.
- **Disabilitato**: Questa opzione limita l'accesso alla rete pubblica all'account di storage e disattiva il tiering dei dati per i sistemi Cloud Volumes ONTAP. Questa è un'opzione consigliata se gli indirizzi IP privati non devono essere esposti anche all'interno dello stesso VNET a causa di norme e criteri di sicurezza.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1001 inbound_http	80 TCP	Qualsiasi a qualsiasi	Accesso HTTP alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione cluster
1002 inbound_111_tcp	111 TCP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1003 inbound_111_udp	111 UDP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1004 inbound_139	139 TCP	Qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1006 inbound_161-162 _udp	161-162 UDP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1007 inbound_443	443 TCP	Qualsiasi a qualsiasi	Connettività con il connettore e accesso HTTPS alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione del cluster
1008 inbound_445	445 TCP	Qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con frame NetBIOS
1009 inbound_635_tcp	635 TCP	Qualsiasi a qualsiasi	Montaggio NFS
1010 inbound_635_udp	635 UDP	Qualsiasi a qualsiasi	Montaggio NFS
1011 inbound_749	749 TCP	Qualsiasi a qualsiasi	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualsiasi a qualsiasi	Daemon del server NFS
1013 inbound_2049_udp	2049 UDP	Qualsiasi a qualsiasi	Daemon del server NFS
1014 inbound_3260	3260 TCP	Qualsiasi a qualsiasi	Accesso iSCSI tramite LIF dei dati iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1017 inbound_10000	10000 TCP	Qualsiasi a qualsiasi	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualsiasi a qualsiasi	Trasferimento dei dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Qualsiasi a qualsiasi	Blocca tutto il traffico TCP in entrata

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Qualsiasi a qualsiasi	Blocca tutto il traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

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

- **Solo VNET selezionato**: L'origine del traffico in entrata è l'intervallo di sottorete del VNET per il sistema Cloud Volumes ONTAP e l'intervallo di sottorete del VNET in cui risiede il connettore. Questa è l'opzione consigliata.
- **All VNets**: La fonte del traffico in entrata è l'intervallo IP 0,0.0.0/0.

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

- **Disabilitato**: Questa opzione limita l'accesso alla rete pubblica all'account di storage e disattiva il tiering dei dati per i sistemi Cloud Volumes ONTAP. Questa è un'opzione consigliata se gli indirizzi IP privati non devono essere esposti anche all'interno dello stesso VNET a causa di norme e criteri di sicurezza.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 inbound_443	443 qualsiasi protocollo	Qualsiasi a qualsiasi	Connettività con il connettore e accesso HTTPS alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione del cluster
101 inbound_111_tcp	111 qualsiasi protocollo	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
102 inbound_2049_tcp	2049 qualsiasi protocollo	Qualsiasi a qualsiasi	Daemon del server NFS
111 inbound_ssh	22 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121 inbound_53	53 qualsiasi protocollo	Qualsiasi a qualsiasi	DNS e CIFS

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in uscita

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

Regole di base in uscita

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

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

Regole avanzate in uscita

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

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

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

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
AutoSupport	HTTPS	443	LIF di gestione dei nodi	support.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	LIF di gestione dei nodi	support.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	LIF di gestione dei nodi	Connettore	Invio di messaggi AutoSupport tramite un server proxy sul connettore, se non è disponibile una connessione Internet in uscita
Backup della configurazione	HTTP	80	LIF di gestione dei nodi	Http://<connector-IP-address>/occm/offboxconfig	Inviare i backup della configurazione al connettore. "Documentazione ONTAP".
DHCP	68	UDP	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	67	UDP	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	53	UDP	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	25	TCP	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	161	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	161	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	11104	TCP	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	11105	TCP	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	514	UDP	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Requisiti per il connettore

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

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

Argomenti correlati

- "Verificare la configurazione di AutoSupport per Cloud Volumes ONTAP"
- "Informazioni sulle porte interne di ONTAP".

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

I dati vengono crittografati automaticamente su Cloud Volumes ONTAP in Azure utilizzando la crittografia del servizio di storage Azure con una chiave gestita da Microsoft. Tuttavia, è possibile utilizzare la propria chiave di crittografia seguendo la procedura riportata in questa pagina.

Panoramica sulla crittografia dei dati

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

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

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

Modalità di crittografia dei dati

BlueXP utilizza un set di crittografia del disco, che consente la gestione delle chiavi di crittografia con dischi gestiti e non con blob di pagine. Anche i nuovi dischi dati utilizzano lo stesso set di crittografia del disco. Le versioni più basse utilizzeranno la chiave gestita da Microsoft, invece della chiave gestita dal cliente.

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

Configurazione di Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Nodo singolo	• Avvio • Core • NVRAM	• Radice • Dati
Singola zona di disponibilità di Azure ha con BLOB di pagina	• Avvio • Core • NVRAM	Nessuno

Configurazione di Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Singola zona di disponibilità di Azure ha con dischi gestiti condivisi	• Avvio • Core • NVRAM	• Radice • Dati
Ha di Azure diverse zone di disponibilità con dischi gestiti condivisi	• Avvio • Core • NVRAM	• Radice • Dati

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

Rotazione della chiave in Cloud Volumes ONTAP

Quando si configurano le chiavi di crittografia, è necessario utilizzare il portale di Azure per impostare e abilitare la rotazione automatica delle chiavi. La creazione e l'abilitazione di una nuova versione delle chiavi di crittografia garantisce che Cloud Volumes ONTAP possa rilevare e utilizzare automaticamente la versione più recente della chiave per la crittografia, garantendo la sicurezza dei dati senza la necessità di interventi manuali.

Per informazioni sulla configurazione dei tasti e sull'impostazione della rotazione dei tasti, fare riferimento ai seguenti argomenti della documentazione di Microsoft Azure:

- "Configurare la rotazione automatica della chiave crittografica in Azure Key Vault"
- "Azure PowerShell: Abilitare le chiavi gestite dal cliente"

> Dopo aver configurato le chiavi, assicurati di aver selezionato "*Abilita rotazione automatica*" , in modo che Cloud Volumes ONTAP possa utilizzare le nuove chiavi alla scadenza di quelle precedenti. Se non si abilita questa opzione nel portale di Azure, Cloud Volumes ONTAP non sarà in grado di rilevare automaticamente le nuove chiavi, il che potrebbe causare problemi con il provisioning dello storage.

Creare un'identità gestita assegnata dall'utente

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

La risorsa ha il seguente ID: `userassignedidentity`.

Fasi

1. In Azure, accedere a servizi Azure e selezionare **identità gestite**.
2. Fare clic su **Create** (Crea).

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

Creare un vault delle chiavi e generare una chiave

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

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

Fasi

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

   Tenere presente i seguenti requisiti per il vault delle chiavi:

   - Il vault delle chiavi deve risiedere nella stessa regione del sistema Cloud Volumes ONTAP.
   - Devono essere attivate le seguenti opzioni:
     - **Soft-delete** (questa opzione è attivata per impostazione predefinita, ma deve *non* essere disattivata)
     - **Protezione da spurgo**
     - **Azure Disk Encryption per la crittografia dei volumi** (per sistemi a nodo singolo, coppie ha in zone multiple e implementazioni ha Single AZ)

       L'utilizzo delle chiavi di crittografia Azure gestite dal cliente dipende dall'attivazione della crittografia del disco di Azure per il vault delle chiavi.

   - Se è stata creata un'identità gestita assegnata dall'utente, deve essere attivata la seguente opzione:
     - **Policy di accesso al vault**
2. Se è stata selezionata la policy di accesso al vault, fare clic su Create (Crea) per creare una policy di accesso per il vault delle chiavi. In caso contrario, passare alla fase 3.
   a. Selezionare le seguenti autorizzazioni:
      - ottieni
      - elenco
      - decrittare
      - crittografare
      - tasto di savvolgimento
      - tasto di avvolgimento
      - verificare

        - segnale
    b. Selezionare l'identità gestita (risorsa) assegnata dall'utente come principale.
    c. Esaminare e creare la policy di accesso.
3. "Generare una chiave nell'archivio chiavi".

    Tenere presente i seguenti requisiti per la chiave:

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

Creare un ambiente di lavoro che utilizzi la chiave di crittografia

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

Autorizzazioni richieste

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

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

"Visualizzare l'elenco più recente delle autorizzazioni"

Fasi

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

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

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

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

    "Scopri di più su questa chiamata API".

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

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

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

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

vault).

"Scopri di più su questa chiamata API".

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

   a. Per una coppia ha:

      `POST /azure/ha/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

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

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

      "Scopri di più su questa chiamata API".

   b. Per un sistema a nodo singolo:

      `POST /azure/vsa/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

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

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

"Scopri di più su questa chiamata API".

Risultato

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

Impostare la licenza per Cloud Volumes ONTAP in Azure

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

Freemium

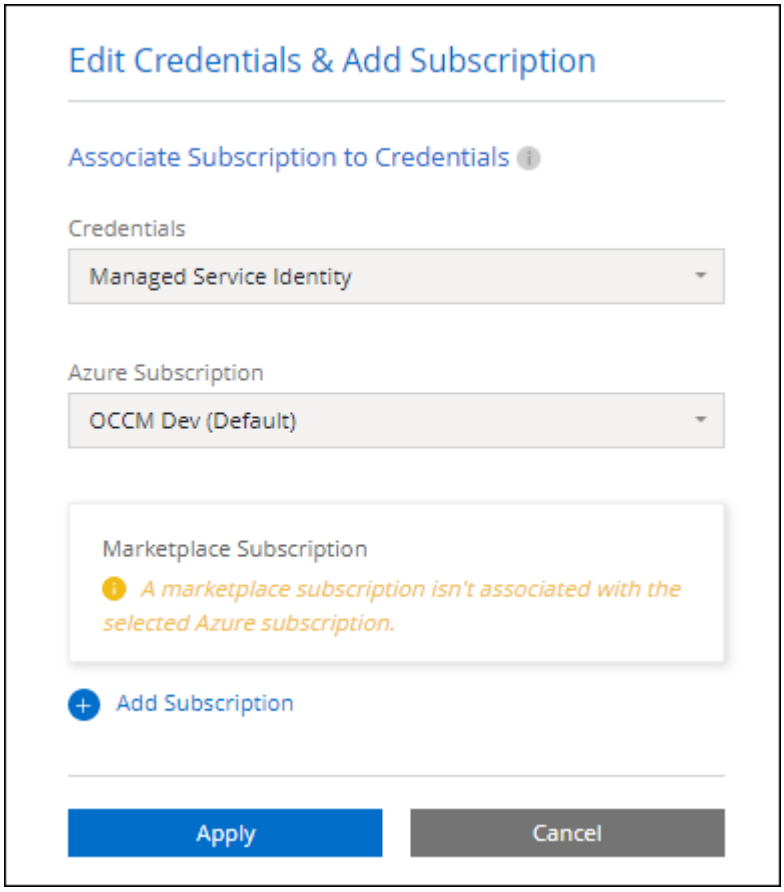
Scegli l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con un massimo di 500 GB di capacità fornita. "Scopri di più sull'offerta Freemium".

Fasi

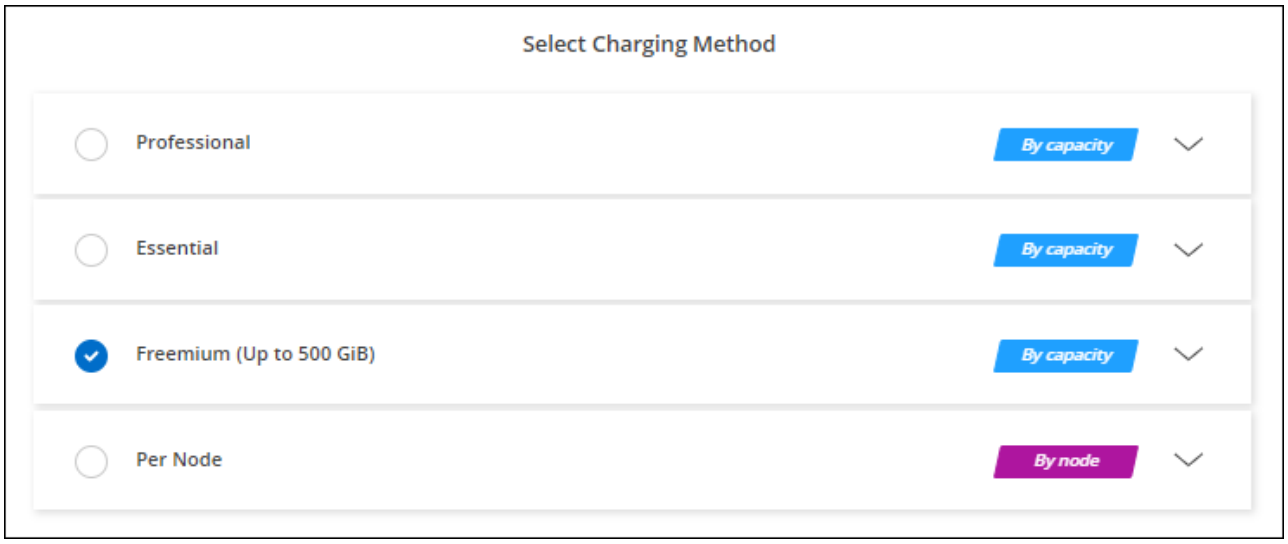
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

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

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



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



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

Licenza basata sulla capacità

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

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

- Una licenza acquistata da NetApp (Bring Your Own License, BYOL)
- Un abbonamento oraria a pagamento (PAYGO) da Azure Marketplace
- Un contratto annuale

"Scopri di più sulle licenze basate sulla capacità".

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

BYOL

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

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Fasi

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

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

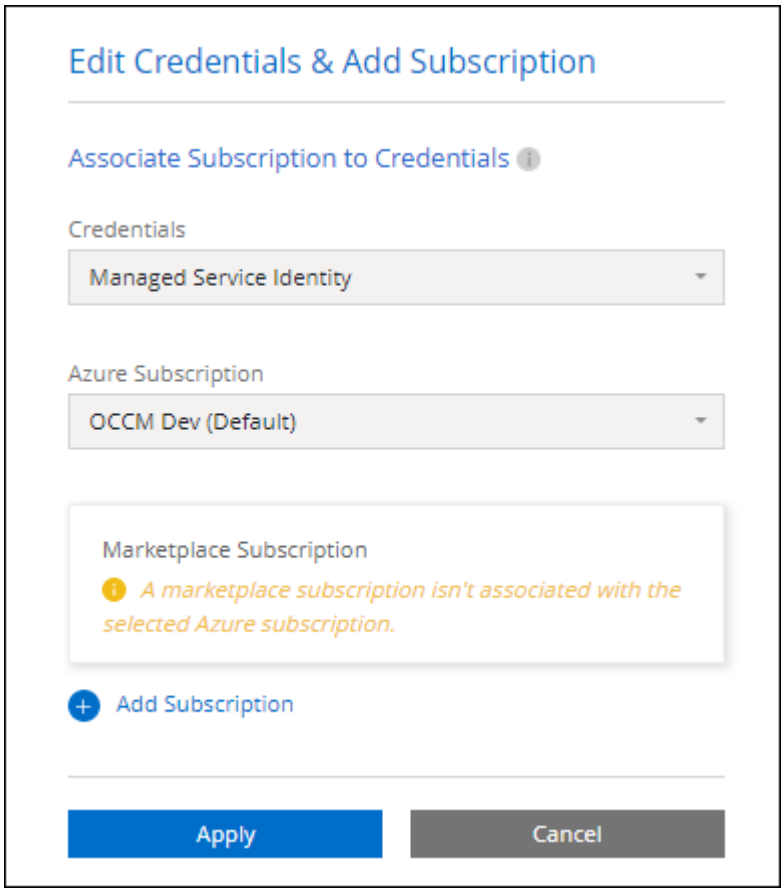
   La licenza deve essere disponibile sul portafoglio digitale BlueXP prima di poter essere utilizzata con

Cloud Volumes ONTAP. Se necessario, è possibile "Aggiungere manualmente la licenza al portafoglio digitale BlueXP".

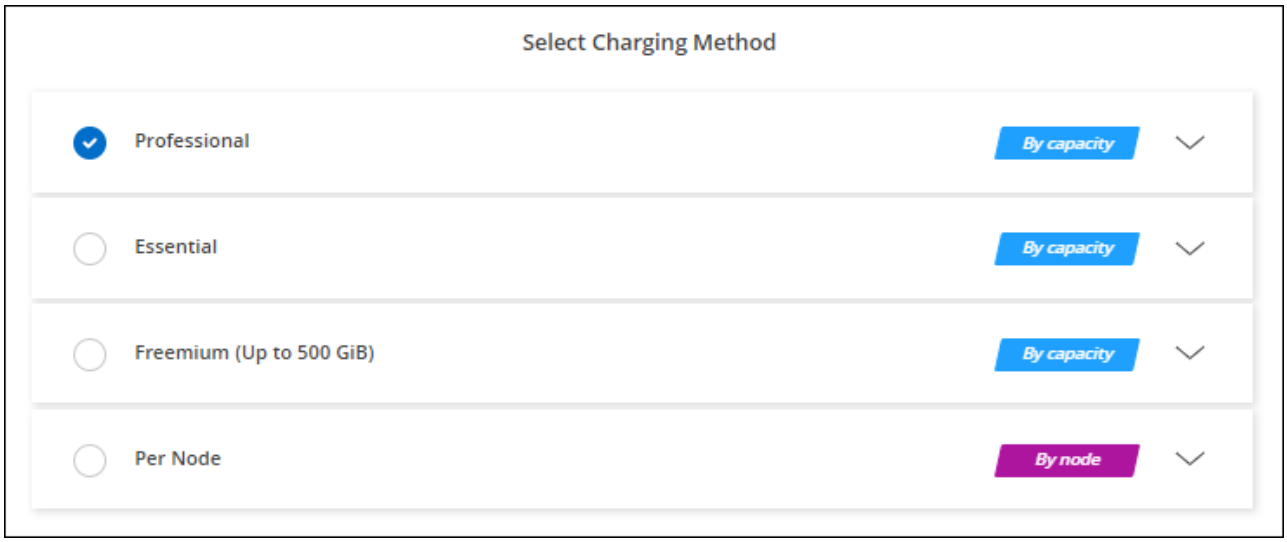
3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

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

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



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



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

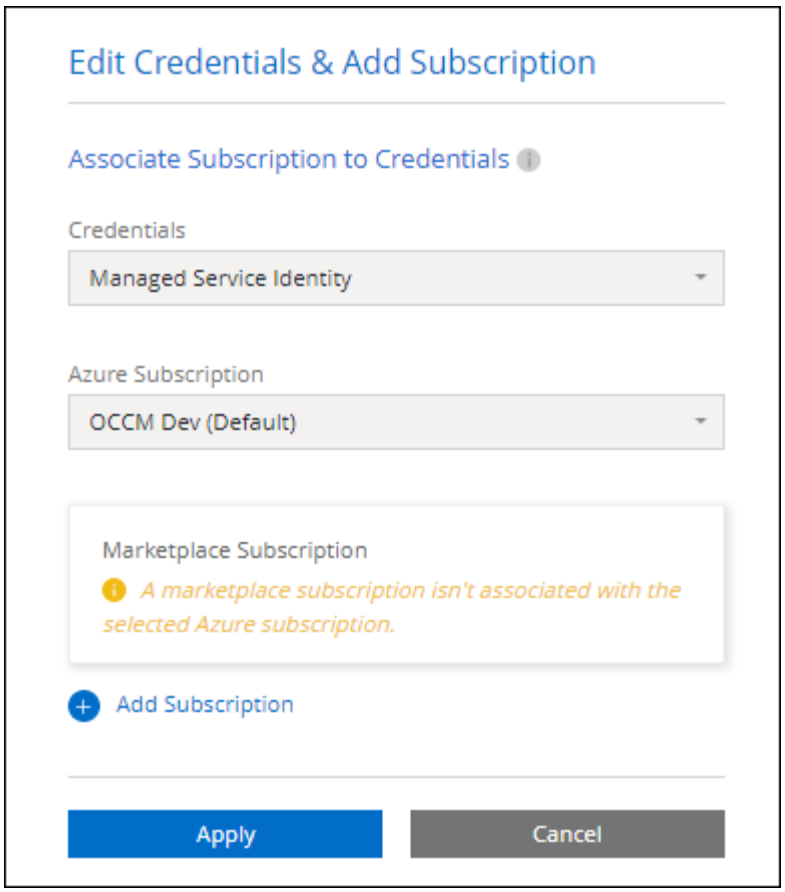
Abbonamento PAYGO

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

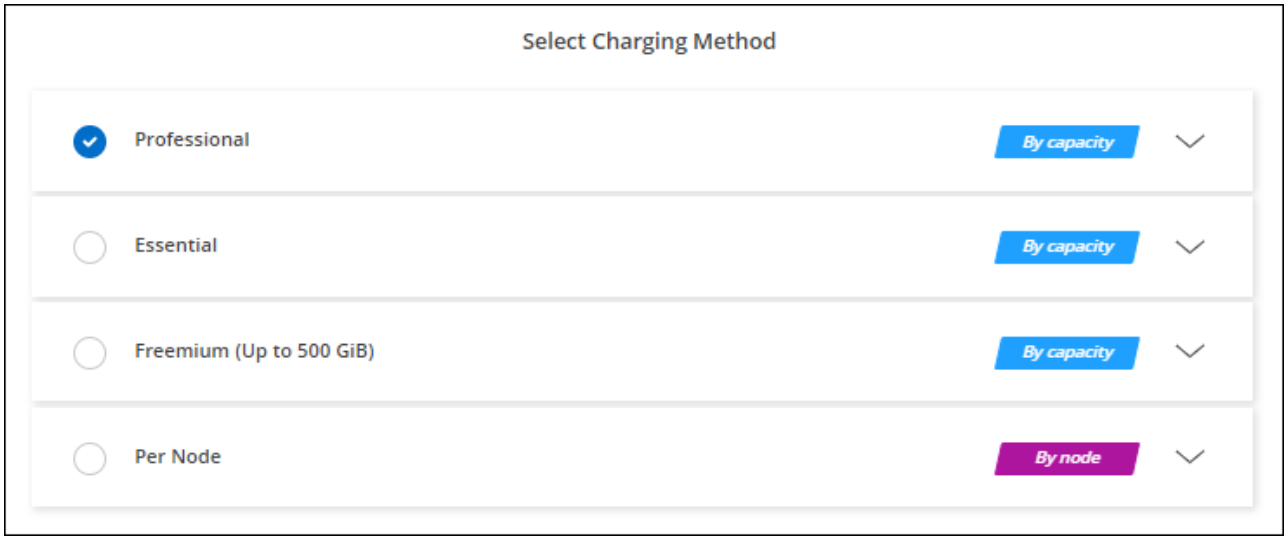
Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, BlueXP richiede di sottoscrivere il contratto disponibile in Azure Marketplace. Tale abbonamento viene quindi associato all'ambiente di lavoro per la ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

Fasi

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



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



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

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

Contratto annuale

Paga Cloud Volumes ONTAP ogni anno acquistando un contratto annuale.

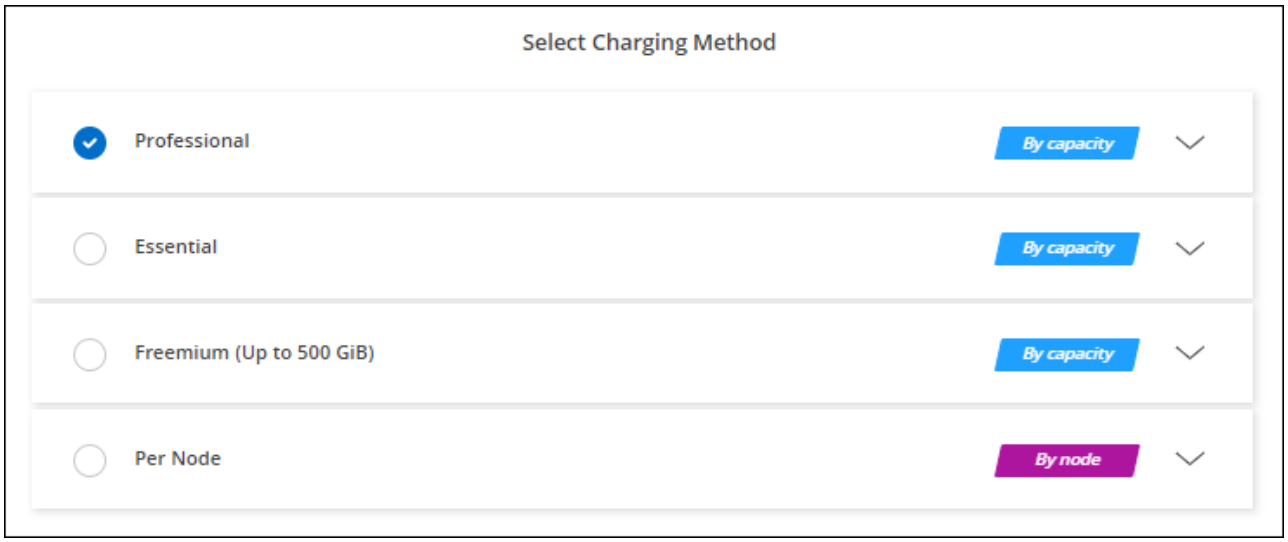
Fasi

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

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

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

2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento > continua**.
   b. Nel portale Azure, seleziona il piano annuale condiviso con il tuo account Azure, quindi fai clic su **Iscriviti**.
   c. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



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

Iscrizione Keystone

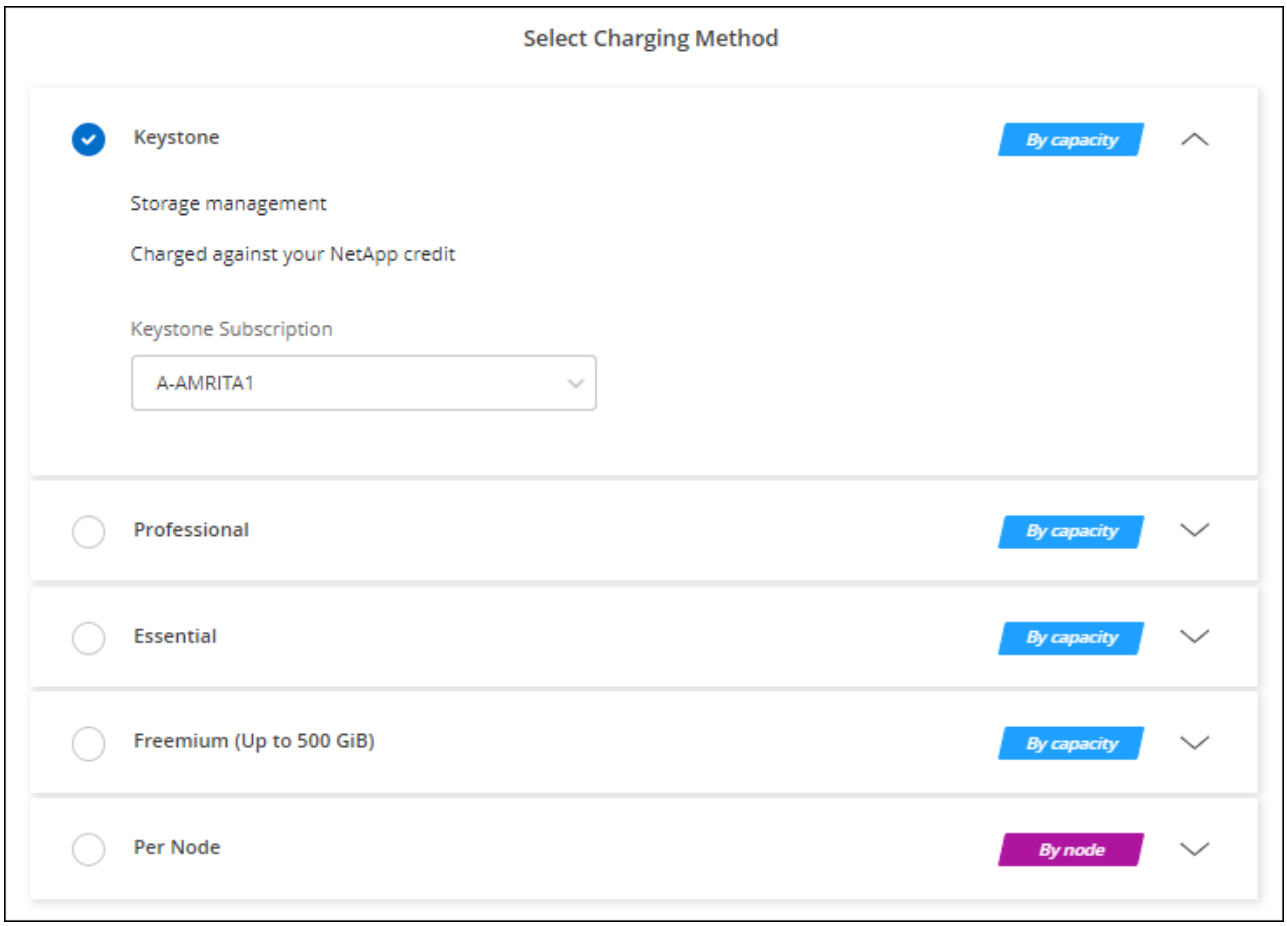
Un abbonamento Keystone è un servizio basato su abbonamento pay-as-you-grow. "Scopri di più sugli abbonamenti NetApp Keystone".

Fasi

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

procedura in BlueXP.

a. Quando richiesto, selezionare il metodo di ricarica per l'abbonamento Keystone.



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

Abilita la modalità high Availability in Azure

La modalità ad alta disponibilità (ha) di Microsoft Azure deve essere abilitata per ridurre i tempi di failover non pianificati e per consentire il supporto NFSv4 ore su 24, 7 giorni su 7 per Cloud Volumes ONTAP. In questa modalità, i nodi ha Cloud Volumes ONTAP possono raggiungere un recovery time objective (RTO) basso (60 secondi) durante i failover non pianificati sui client CIFS e NFSv4.

A partire da Cloud Volumes ONTAP 9.10.1, abbiamo ridotto il tempo di failover non pianificato per le coppie ha Cloud Volumes ONTAP in esecuzione in Microsoft Azure e abbiamo aggiunto il supporto per NFSv4. Per rendere disponibili questi miglioramenti per Cloud Volumes ONTAP, devi abilitare la funzionalità di alta disponibilità nella tua iscrizione ad Azure.

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

Tenere presente quanto segue:

- Non ci sono problemi con l'alta disponibilità della tua coppia Cloud Volumes ONTAP ha. Questa funzionalità di Azure funziona in collaborazione con ONTAP per ridurre il tempo di interruzione

dell'applicazione osservato dal client per i protocolli NFS che derivano da eventi di failover non pianificati.

- L'attivazione di questa funzione non comporta interruzioni per le coppie Cloud Volumes ONTAP ha.
- L'attivazione di questa funzione sull'abbonamento ad Azure non causa problemi ad altre macchine virtuali.
- Cloud Volumes ONTAP utilizza un bilanciatore di carico Azure interno durante il failover di interfacce LIF di gestione cluster e SVM su client CIFS e NFS.
- Quando la modalità ha è abilitata, BlueXP esegue una scansione del sistema ogni 12 ore per aggiornare le regole interne del bilanciamento del carico di Azure.

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

Fasi

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

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

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

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

Azure CLI dovrebbe restituire un risultato simile a quanto segue:

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

Attiva VMOrchestratorZonalMultiFD per Cloud Volumes ONTAP in Azure

Per la distribuzione di istanze VM in zone di disponibilità singola (AZ) LRS (Local Redundant Storage), è necessario attivare la funzione Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` per gli abbonamenti. In una modalità ad alta disponibilità (ha), questa funzionalità facilita l'implementazione dei nodi

in domini di errore separati nella stessa zona di disponibilità.

A meno che non si attivi questa funzione, la distribuzione zonale non si verifica e la precedente distribuzione non zonale LRS diventa effettiva.

Per informazioni sull'implementazione della VM in una singola zona di disponibilità, fare riferimento alla "Coppie ad alta disponibilità in Azure".

Eseguire questi passaggi come utente con Privileges "Proprietario":

Fasi

1. Accedi ad Azure Cloud Shell dal portale di Azure. Per informazioni, fare riferimento alla "Documentazione di Microsoft Azure: Introduzione ad Azure Cloud Shell".
2. Effettuare la registrazione `Microsoft.Compute/VMOrchestratorZonalMultiFD` eseguendo questo comando:

   ```
   az account set -s <Azure_subscription_name_or_ID> az Feature Register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Verificare lo stato della registrazione e il campione di output:

   ```
   az Feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/abbonamenti/<ID>/provider/Microsoft.features/provider/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "State": "Registered" }, "type": "Microsoft.features/providers/features" }
   ```

Avviare Cloud Volumes ONTAP in Azure

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

Prima di iniziare

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

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

  È necessario aver scelto una configurazione e ottenuto le informazioni di rete di Azure dall'amministratore. Per informazioni, fare riferimento alla "Pianificazione della configurazione di Cloud Volumes ONTAP".

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

  "Scopri come impostare le licenze".

A proposito di questa attività

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

Potenziale perdita di dati

La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per ciascun sistema Cloud Volumes ONTAP.

L'implementazione di Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente non è consigliata a causa del rischio di perdita di dati. Mentre BlueXP può rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse condiviso in caso di errore di implementazione o di eliminazione, un utente Azure potrebbe accidentalmente eliminare le risorse Cloud Volumes ONTAP da un gruppo di risorse condiviso.

Lancia un sistema Cloud Volumes ONTAP a nodo singolo in Azure

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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una posizione**: Seleziona **Microsoft Azure** e **nodo singolo Cloud Volumes ONTAP**.
4. Se richiesto, "Creare un connettore".
5. **Dettagli e credenziali**: Se necessario, modificare le credenziali e la sottoscrizione di Azure, specificare un nome del cluster, aggiungere tag, quindi specificare le credenziali.

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

Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che alla macchina virtuale Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Tag del gruppo di risorse	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, BlueXP li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento alla "Documentazione di Microsoft Azure: Utilizzo di tag per organizzare le risorse di Azure" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestione di sistema di ONTAP o l'interfaccia a riga di comando di ONTAP. Mantenere il nome utente predefinito *admin* o modificarlo in un nome utente personalizzato.

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

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

Iscriviti a BlueXP da Azure Marketplace

6. **Servizi**: Consente di attivare o disattivare i singoli servizi che si desidera utilizzare o che non si desidera utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla classificazione BlueXP"
   - "Scopri di più sul backup e ripristino BlueXP"

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

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

   Per le regioni in Cina, le implementazioni a nodo singolo sono supportate solo in Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA. È possibile aggiornare queste versioni a patch e release successive di Cloud Volumes ONTAP. Se si desidera distribuire versioni Cloud Volumes ONTAP successive nelle aree geografiche della Cina, contattare il supporto NetApp. Solo le licenze acquistate direttamente da NetApp sono supportate nelle regioni della Cina e gli abbonamenti ai mercati non sono disponibili.

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

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

Campo	Descrizione
Gruppo di risorse	Creare un nuovo gruppo di risorse per Cloud Volumes ONTAP o utilizzare un gruppo di risorse esistente. La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile implementare Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, non è consigliabile a causa del rischio di perdita dei dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. Se l'account Azure in uso dispone di "autorizzazioni richieste", BlueXP rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione.

Campo	Descrizione
Gruppo di sicurezza generato	Se si lascia che BlueXP generi il gruppo di protezione, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VNET Only** (solo VNET selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VNET selezionato e l'intervallo di sottorete del VNET in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VNets**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA esistente	Se si sceglie un gruppo di protezione esistente, questo deve soddisfare i requisiti Cloud Volumes ONTAP. "Visualizzare il gruppo di protezione predefinito".

9. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
10. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

11. **Licenze**: Modificare la versione di Cloud Volumes ONTAP se necessario e selezionare un tipo di macchina virtuale.

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 è disponibile. L'aggiornamento non viene eseguito da una versione all'altra, ad esempio da 9,13 a 9,14.

12. **Iscriviti da Azure Marketplace**: Se BlueXP non è in grado di abilitare le implementazioni programmatiche di Cloud Volumes ONTAP, visualizzerai questa pagina. Seguire i passaggi elencati sullo schermo. "Distribuzione programmatica dei prodotti Marketplace" Per ulteriori informazioni, fare riferimento alla.
13. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

    Tenere presente quanto segue:

    - Se l'accesso pubblico all'account di storage è disabilitato in VNET, non è possibile abilitare il tiering dei dati nel sistema Cloud Volumes ONTAP. Per informazioni, fare riferimento alla "Regole del gruppo di sicurezza".
    - Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.
    - Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP quando si utilizza l'opzione di provisioning semplice. È possibile creare

aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

Per informazioni sulla scelta del tipo e delle dimensioni di un disco, fare riferimento alla sezione "Dimensionamento del sistema in Azure".

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

"Scopri di più sul tiering dei dati".

14. **Velocità di scrittura e WORM**:

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

    "Scopri di più sulla velocità di scrittura".

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

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

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

"Scopri di più sullo storage WORM".

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

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

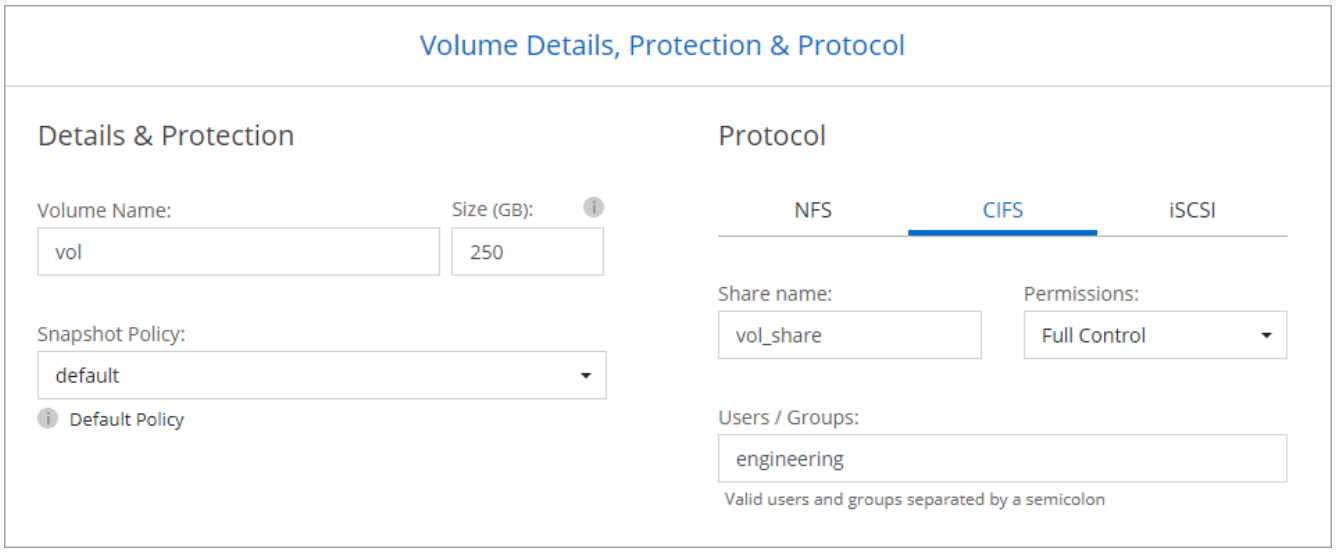
"Scopri le versioni e i protocolli client supportati".

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

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, BlueXP inserisce un valore che fornisce l'accesso a tutte le istanze della subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.

Campo	Descrizione
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, BlueXP crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

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



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

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.

Campo	Descrizione
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Per ulteriori informazioni, fare riferimento alla "Documenti sull'automazione BlueXP" . Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

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

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

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

Risultato

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

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

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

Al termine

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

  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.

Lancia una coppia ha Cloud Volumes ONTAP in Azure

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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. Se richiesto, "Creare un connettore".
4. **Dettagli e credenziali**: Se necessario, modificare le credenziali e la sottoscrizione di Azure, specificare un nome del cluster, aggiungere tag, quindi specificare le credenziali.

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

Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che alla macchina virtuale Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Tag del gruppo di risorse	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, BlueXP li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento alla "Documentazione di Microsoft Azure: Utilizzo di tag per organizzare le risorse di Azure" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestione di sistema di ONTAP o l'interfaccia a riga di comando di ONTAP. Mantenere il nome utente predefinito *admin* o modificarlo in un nome utente personalizzato.
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP. Per implementare un sistema Cloud Volumes ONTAP pay-as-you-go, devi associare un abbonamento Azure Marketplace all'abbonamento Azure selezionato. "Scopri come aggiungere le credenziali".

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

   Iscriviti a BlueXP da Azure Marketplace

5. **Servizi**: Consente di attivare o disattivare i singoli servizi a seconda che si desideri utilizzarli con Cloud Volumes ONTAP.
   - "Scopri di più sulla classificazione BlueXP"
   - "Scopri di più sul backup e ripristino BlueXP"

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

6. **Modelli di implementazione ha**:
   a. Selezionare **Single Availability zone** o **Multiple Availability zone**.
      - Per le singole zone di disponibilità, selezionare un'area Azure, una zona di disponibilità, VNET e una subnet.

        A partire da Cloud Volumes ONTAP 9.15.1, è possibile implementare istanze di macchine virtuali in modalità ha in singole zone di disponibilità (AZS) in Azure. È necessario selezionare una zona e un'area che supportino questa distribuzione. Se la zona o la regione non supporta la distribuzione zonale, viene seguita la precedente modalità di distribuzione non zonale per LRS. Per informazioni sulle configurazioni supportate per i dischi gestiti condivisi, fare riferimento a "Configurazione DI una singola zona di disponibilità HA con dischi gestiti condivisi".

      - Per più zone di disponibilità, selezionare una regione, VNET, subnet, zona per il nodo 1 e zona per il nodo 2.
   b. Selezionare la casella di controllo **ho verificato la connettività di rete…**.
7. **Connettività**: Scegliere un gruppo di risorse nuovo o esistente, quindi scegliere se utilizzare il gruppo di protezione predefinito o il proprio.

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

Campo	Descrizione
Gruppo di risorse	Creare un nuovo gruppo di risorse per Cloud Volumes ONTAP o utilizzare un gruppo di risorse esistente. La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile implementare Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, non è consigliabile a causa del rischio di perdita dei dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. È necessario utilizzare un gruppo di risorse dedicato per ogni coppia di Cloud Volumes ONTAP ha implementata in Azure. In un gruppo di risorse è supportata una sola coppia ha. BlueXP presenta problemi di connessione se si tenta di implementare una seconda coppia Cloud Volumes ONTAP ha in un gruppo di risorse Azure. Se l'account Azure in uso dispone di "autorizzazioni richieste", BlueXP rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione.

Campo	Descrizione
Gruppo di sicurezza generato	Se si lascia che BlueXP generi il gruppo di protezione, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VNET Only** (solo VNET selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VNET selezionato e l'intervallo di sottorete del VNET in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VNets**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA esistente	Se si sceglie un gruppo di protezione esistente, questo deve soddisfare i requisiti Cloud Volumes ONTAP. "Visualizzare il gruppo di protezione predefinito".

8. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Cambia configurazione**.

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

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 è disponibile. L'aggiornamento non viene eseguito da una versione all'altra, ad esempio da 9,13 a 9,14.
11. **Iscriviti al marketplace Azure**: Segui la procedura se BlueXP non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
12. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

    Tenere presente quanto segue:
    - Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

      Per informazioni sulla scelta delle dimensioni del disco, fare riferimento alla sezione "Dimensionare il sistema in Azure".
    - Se l'accesso pubblico all'account di storage è disabilitato in VNET, non è possibile abilitare il tiering dei dati nel sistema Cloud Volumes ONTAP. Per informazioni, fare riferimento alla "Regole del gruppo di

sicurezza".

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

  "Scopri di più sul tiering dei dati".

- A partire da Cloud Volumes ONTAP 9.15.0P1, i blob delle pagine di Azure non sono più supportati per le nuove implementazioni di coppie ad alta disponibilità. Se al momento utilizzi Azure page blob in implementazioni esistenti di coppie ad alta disponibilità, puoi migrare a tipi di istanze di macchine virtuali più recenti nelle macchine virtuali della serie Edsv4 e nelle macchine virtuali della serie Edsv5.

  "Scopri di più sulle configurazioni supportate in Azure".

13. **Velocità di scrittura e WORM**:

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

       "Scopri di più sulla velocità di scrittura".

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

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

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

    "Scopri di più sullo storage WORM".

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

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

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

    "Scopri di più sullo storage WORM".

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

    "Scopri di più sullo storage WORM".

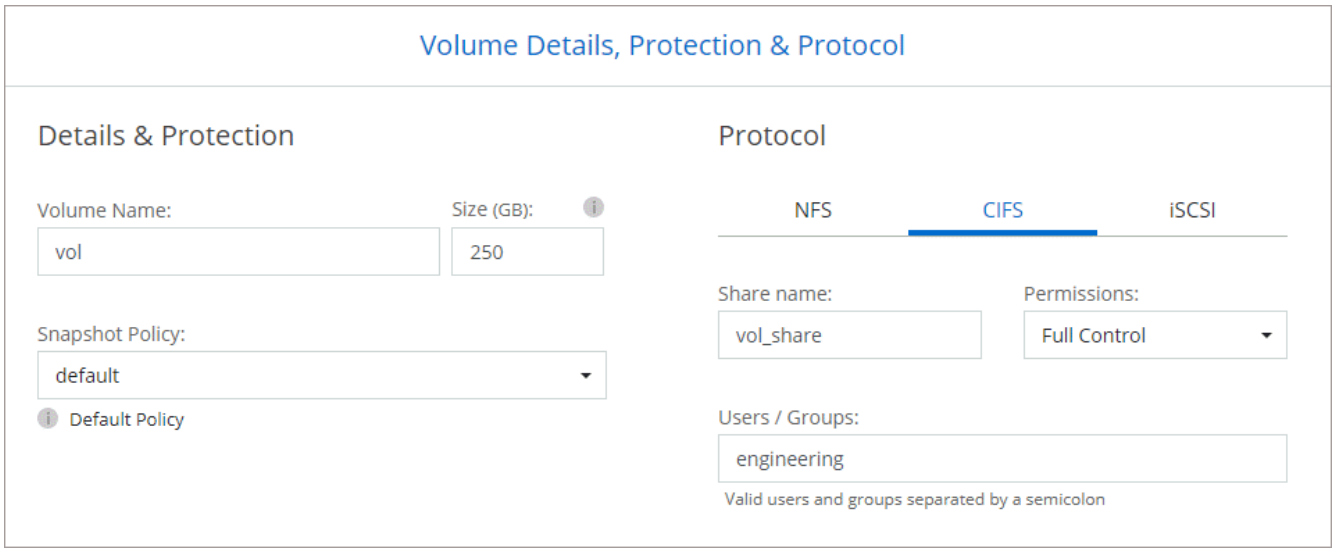
15. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    "Scopri le versioni e i protocolli client supportati".

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

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

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



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

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Per ulteriori informazioni, fare riferimento alla "Documenti sull'automazione BlueXP" . Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

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

    Per ulteriori informazioni, fare riferimento a "Scegliere un profilo di utilizzo del volume", , "Panoramica sul tiering dei dati"e. "KB: Quali funzionalità di efficienza dello storage inline sono supportate in CVO?"

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

Risultato

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

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

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

Al termine

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

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

Verifica l'immagine della piattaforma Azure

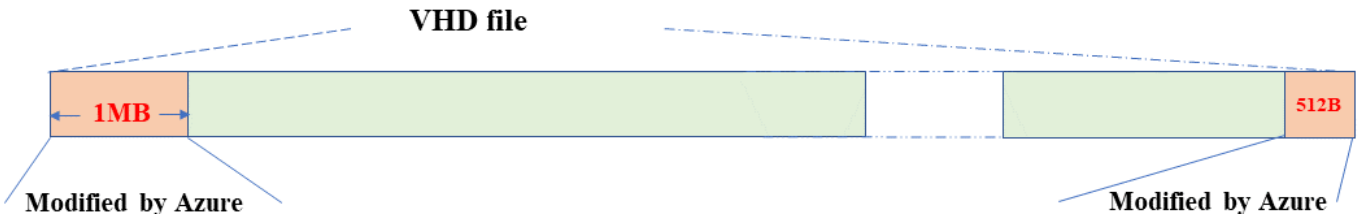
Verifica delle immagini di Azure Marketplace per Cloud Volumes ONTAP

La verifica dell'immagine di Azure è conforme ai requisiti di sicurezza NetApp avanzati. La verifica di un file immagine è un processo semplice. Tuttavia, la verifica della firma dell'immagine di Azure richiede considerazioni specifiche per il file immagine VHD di Azure, poiché viene modificato in Azure Marketplace.

La verifica delle immagini di Azure è supportata su Cloud Volumes ONTAP 9.15.0 e versioni successive.

Modifica di Azure dei file VHD pubblicati

Azure modifica 1 MB (1048576 byte) all'inizio e 512 byte alla fine del file VHD. NetApp firma il file VHD rimanente.



Nell'esempio, il file VHD è di 10 GB. La parte firmata da NetApp è contrassegnata in verde (10 GB - 1 MB - 512 byte).

Link correlati

- "Page Fault Blog: Come firmare e verificare usando OpenSSL"
- "USA l'immagine di Azure Marketplace per creare l'immagine VM per la tua GPU Azure Stack Edge Pro | Microsoft Learn"
- "Esportare/copiare un disco gestito in un account di storage utilizzando l'interfaccia CLI di Azure | Microsoft Learn"
- "Azure Cloud Shell Quickstart - Bash | Microsoft Learn"
- "Come installare la CLI di Azure | Microsoft Learn"
- "Copia BLOB storage az | Microsoft Learn"
- "Accedi con Azure CLI — Login e autenticazione | Microsoft Learn"

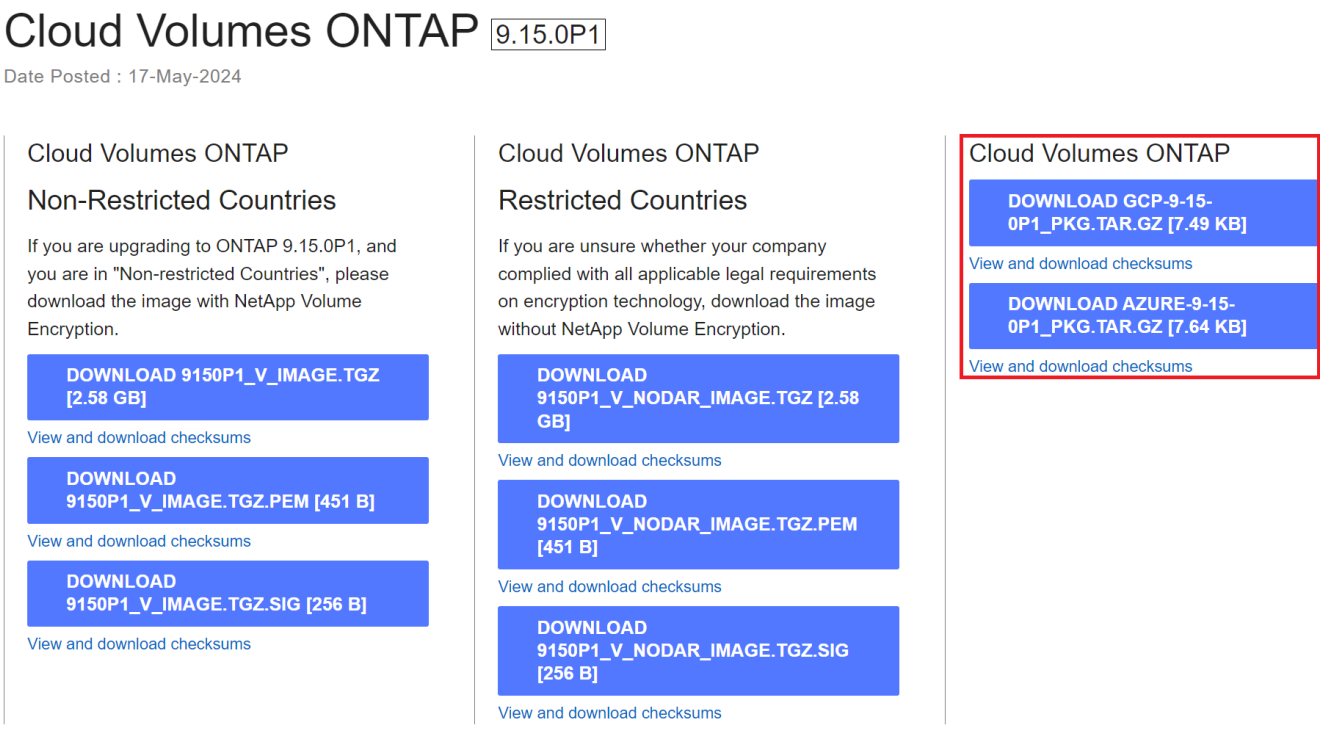
Scarica il file immagine di Azure per Cloud Volumes ONTAP

È possibile scaricare il file immagine di Azure da "Sito di supporto NetApp" .

Il file *tar.gz* contiene i file necessari per la verifica della firma dell'immagine. Insieme al file *tar.gz*, è necessario scaricare anche il file *checksum* per l'immagine. Il file di checksum contiene `md5` E `sha256` checksum del file *tar.gz*.

Fasi

1. Vai al "Pagina del prodotto Cloud Volumes ONTAP sul sito del supporto NetApp" e scaricare la versione software richiesta dalla sezione **Download**.
2. Nella pagina di download di Cloud Volumes ONTAP, fare clic sul file scaricabile per l'immagine di Azure e scaricare il file *tar.gz*.



3. Su Linux, esegui `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Su macOS, esegui `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Verificare che il `md5sum` E `sha256sum` i valori corrispondono a quelli nell'immagine di Azure scaricata.
5. Su Linux e macOS, estrarre il file *tar.gz* utilizzando il comando `tar -xzf` comando.

   Il file *tar.gz* estratto contiene il file digest (*.sig*), il file del certificato della chiave pubblica (*.pem*) e il file del certificato della catena (*.pem*).

   Esempio di output dopo l'estrazione del file tar.gz:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Esporta immagini VHD per Cloud Volumes ONTAP dal marketplace di Azure

Una volta pubblicata sul cloud di Azure, l'immagine VHD non è più gestita da NetApp. Al contrario, l'immagine pubblicata viene posizionata sul marketplace di Azure. Quando l'immagine viene preparata e pubblicata su Azure Marketplace, Azure modifica 1 MB all'inizio e 512 byte alla fine del VHD. Per verificare la firma del file VHD, è necessario esportare l'immagine VHD modificata da Azure da Azure Marketplace.

Prima di iniziare

Assicurarsi che l'interfaccia della riga di comando di Azure sia installata sul sistema o che Azure Cloud Shell sia disponibile tramite il portale di Azure. Per ulteriori informazioni su come installare l'interfaccia della riga di comando di Azure, consultare "Documentazione di Azure: come installare l'interfaccia della riga di comando di Azure" .

Fasi

1. Mappa la versione di Cloud Volumes ONTAP sul tuo sistema alla versione dell'immagine di Azure Marketplace utilizzando il contenuto del file *version_readme*. La versione di Cloud Volumes ONTAP è rappresentata da `buildname` e la versione dell'immagine di Azure Marketplace è rappresentata da `version` nelle mappature delle versioni.

   Nell'esempio seguente, la versione di Cloud Volumes ONTAP `9.15.0P1` è mappato alla versione dell'immagine di Azure Marketplace `9150.01000024.05090105` . Questa versione dell'immagine di Azure Marketplace viene utilizzata in seguito per impostare l'URN dell'immagine.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifica la regione in cui desideri creare le VM. Il nome della regione viene utilizzato come valore per `locName` variabile quando si imposta l'URN dell'immagine del marketplace. Per elencare le regioni disponibili, eseguire questo comando:

   ```
   az account list-locations -o table
   ```

In questa tabella, il nome della regione appare nella `Name` campo.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Esaminare i nomi SKU per le versioni di Cloud Volumes ONTAP e i tipi di distribuzione delle VM corrispondenti nella tabella seguente. Il nome SKU viene utilizzato come valore per `skuName` variabile quando si imposta l'URN dell'immagine del marketplace.

   Ad esempio, tutte le implementazioni a nodo singolo con Cloud Volumes ONTAP 9.15.0 devono utilizzare `ontap_cloud_byol` come nome SKU.

Versione Cloud Volumes ONTAP	Metodo di distribuzione VM	Nome SKU
9.16.1 e versioni successive	Tramite il metodo di distribuzione diretta del mercato	ONTAP_cloud_direct
9.16.1 e versioni successive	Tutte le implementazioni tramite BlueXP	ONTAP_cloud
9.15.1	Tutte le implementazioni tramite BlueXP	ONTAP_cloud
9.15.0	Nodo singolo	cloud_ontap_byol
9.15.0	Alta disponibilità	ontap_cloud_byol_ha

4. Dopo aver mappato la versione di ONTAP e l'immagine di Azure Marketplace, esportare il file VHD da Azure Marketplace tramite Azure Cloud Shell o Azure CLI.

Esportare file VHD utilizzando Azure Cloud Shell su Linux

Da Azure Cloud Shell, esporta l'immagine del marketplace nel file VHD (ad esempio, *9150.01000024.05090105.vhd*) e scaricala sul tuo sistema Linux locale. Segui questi passaggi per ottenere l'immagine VHD da Azure Marketplace.

Fasi

1. Imposta l'URN e altri parametri dell'immagine del marketplace. , puoi elencare le immagini del marketplace NetApp per confermare la versione corretta dell'immagine.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Crea un nuovo disco gestito dall'immagine del marketplace con la versione dell'immagine corrispondente:

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Esportare il file VHD dal disco gestito ad Archiviazione di Azure. Creare un contenitore con il livello di accesso appropriato. In questo esempio, abbiamo utilizzato un contenitore denominato `vm-images` con `Container` Livello di accesso. Ottieni la chiave di accesso dell'account di archiviazione dal portale di Azure: **Account di archiviazione > *examplesname* > Chiave di accesso > *key1* > *key* > Mostra > *<copia>***

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Scarica l’immagine generata sul tuo sistema Linux. Usa il `wget` comando per scaricare il file VHD:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

L’URL segue un formato standard. Per l’automazione, è possibile ricavare la stringa URL come mostrato di seguito. In alternativa, è possibile utilizzare l’interfaccia della riga di comando di Azure. `az` Comando per ottenere l’URL. Esempio di URL: https://examplesaname.blob.core.windows.net/vm-images/9150.01000024.05090105.vhd

5. Pulisci il disco gestito

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Esportare file VHD tramite l’interfaccia della riga di comando di Azure su Linux

Esportare l’immagine del marketplace in un file VHD tramite l’interfaccia della riga di comando di Azure da un sistema Linux locale.

Fasi

1. Accedi all’interfaccia della riga di comando di Azure ed elenca le immagini del marketplace:

```
% az login --use-device-code
```

2. Per effettuare l’accesso, utilizzare un browser Web per aprire la pagina https://microsoft.com/devicelogin e inserisci il codice di autenticazione.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Crea un nuovo disco gestito dall'immagine del marketplace con la versione dell'immagine corrispondente.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

Per automatizzare il processo, è necessario estrarre il SAS dall'output standard. Per istruzioni, fare riferimento ai documenti appropriati.

4. Esportare il file VHD dal disco gestito.

   a. Crea un contenitore con il livello di accesso appropriato. In questo esempio, un contenitore denominato `vm-images` con `Container` viene utilizzato il livello di accesso.

   b. Ottieni la chiave di accesso dell'account di archiviazione dal portale di Azure: **Account di archiviazione > *examplesaname* > Chiave di accesso > *key1* > *key* > Mostra > <*copia*>**

      Puoi anche usare il `az` comando per questo passaggio.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Controllare lo stato della copia del BLOB.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxx/abcd?sv=2018-03-28&sr=b&si=xxxxxxxx-
xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Scarica l'immagine generata sul tuo server Linux.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

L'URL segue un formato standard. Per l'automazione, è possibile ricavare la stringa URL come mostrato di seguito. In alternativa, è possibile utilizzare l'interfaccia della riga di comando di Azure. `az` Comando per ottenere l'URL. Esempio di URL: https://examplesaname.blob.core.windows.net/vm-images/9150.01000024.05090105.vhd

7. Pulisci il disco gestito

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

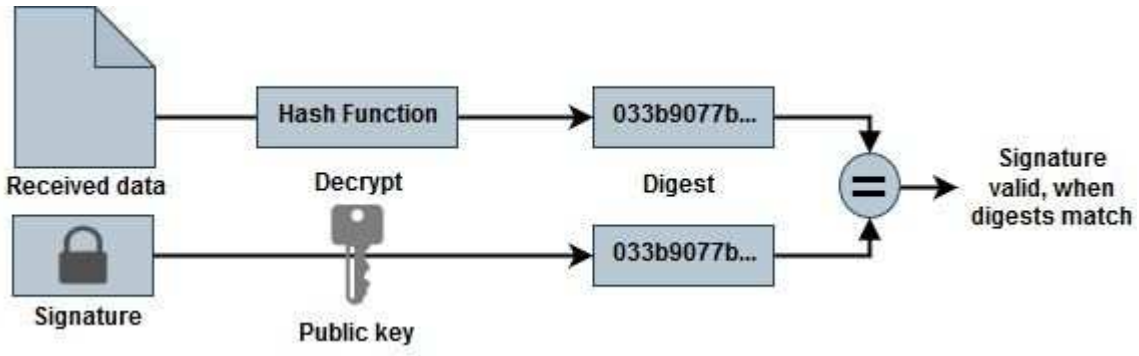
Verifica la firma del file

Verifica della firma dell'immagine del marketplace Azure per Cloud Volumes ONTAP

Il processo di verifica dell'immagine di Azure genera un file digest dal file VHD estraendo 1 MB all'inizio e 512 byte alla fine, quindi applicando una funzione hash. Per far corrispondere la procedura di firma, viene utilizzato *sha256* per l'hashing.

Riepilogo del flusso di lavoro di verifica della firma dei file

Di seguito viene fornita una panoramica del processo del flusso di lavoro di verifica della firma dei file.



- Scaricamento dell'immagine di Azure da "Sito di supporto NetApp" ed estraendo il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem). Per ulteriori informazioni, fare riferimento "Scarica il file digest dell'immagine di Azure" a.
- Verifica della catena di fiducia.
- Estrazione della chiave pubblica (.pub) dal certificato della chiave pubblica (.pem).
- Decifrare il file digest utilizzando la chiave pubblica estratta.
- Confrontando il risultato con un digest appena generato di un file temporaneo creato dal file immagine dopo aver rimosso 1 MB all'inizio e 512 byte alla fine. Questo passaggio viene eseguito utilizzando lo strumento da riga di comando di OpenSSL. Lo strumento da riga di comando di OpenSSL visualizza un messaggio appropriato in caso di esito positivo o negativo della ricerca dei file.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Verificare la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su Linux

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Fasi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Per ulteriori informazioni, fare riferimento "Scarica il file digest dell'immagine di Azure" a.

2. Verificare la catena di trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica.

   Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Pulire lo spazio di lavoro.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su macOS

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Fasi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Per ulteriori informazioni, fare riferimento "Scarica il file digest dell'immagine di Azure" a.

2. Verificare la catena di trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. . Tieni presente che su macOS il comando tail potrebbe richiedere circa dieci minuti per essere completato

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilizza OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file di firma e la chiave pubblica. Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Pulire lo spazio di lavoro.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Implementa Cloud Volumes ONTAP dal marketplace di Azure

Puoi utilizzare l'implementazione diretta del marketplace di Azure per implementare rapidamente e facilmente Cloud Volumes ONTAP. Dal marketplace di Azure, puoi implementare rapidamente Cloud Volumes ONTAP in pochi clic ed esplorarne le caratteristiche e le funzionalità principali nel tuo ambiente.

Per ulteriori informazioni su questa offerta, fare riferimento a "Scopri le offerte Cloud Volumes ONTAP su BlueXP e sul marketplace".

A proposito di questa attività

Il sistema Cloud Volumes ONTAP implementato utilizzando la distribuzione diretta del marketplace di Azure possiede queste proprietà. Si noti che le funzionalità di un'istanza standalone implementata attraverso il marketplace di Azure cambiano quando viene rilevata in BlueXP .

- La versione più recente di Cloud Volumes ONTAP (9.16.1 o successiva).
- Una licenza gratuita per Cloud Volumes ONTAP, limitata a 500 GiB di capacità con provisioning. Questa licenza non include il supporto NetApp e non ha data di scadenza.
- Due nodi configurati in modalità high Availability (ha) in una singola zona di disponibilità (AZ), con numeri di serie predefiniti. Le Storage Virtual Machine (VM di storage) vengono implementate in una "modalità di orchestrazione flessibile".
- Un aggregato per l'istanza creata per impostazione predefinita.
- Un disco gestito SSD Premium v2 con capacità di provisioning di 500 GiB, un disco root e un disco dati.
- Una macchina virtuale per lo storage dei dati implementata con servizi dati NFS, CIFS, iSCSI e NVMe/TCP. Non è possibile aggiungere altre macchine virtuali per lo storage dei dati.
- Licenze installate per NFS, CIFS (SMB), iSCSI, protezione autonoma dal ransomware (ARP), SnapLock e SnapMirror.
- "Efficienza dello storage sensibile alla temperatura (TSSE) ONTAP", crittografia del volume e gestione esterna delle chiavi attivate per impostazione predefinita.
- Queste funzioni non sono supportate:
  - Tiering FabricPool
  - Modifica del tipo di VM di storage
  - Modalità di scrittura rapida

Prima di iniziare

- Assicurati di disporre di un'iscrizione valida al marketplace Azure.
- Assicurati di soddisfare i requisiti di rete di un "Implementazione HA in una singola AZ" in Azure. Fare riferimento alla "Configura il networking Azure per Cloud Volumes ONTAP".
- Per implementare Cloud Volumes ONTAP è necessario assegnare uno di questi ruoli di Azure:

- Il `contributor` ruolo con le autorizzazioni predefinite. Per ulteriori informazioni, fare riferimento alla "Documentazione di Azure: Ruoli integrati di Azure" .
- Un ruolo RBAC personalizzato con le seguenti autorizzazioni. Per ulteriori informazioni, fare riferimento alla "Documentazione di Azure: Ruoli personalizzati di Azure" .

```
"Permissions": [ { "Actions": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/Subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write" Microsoft.Network/virtualNetworks/read"
Microsoft.Compute/disks/write" Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action"
Microsoft.Network/networkSecurityGroups/write"
Microsoft.Compute/virtualMachineScaleSets/write",
"resources/Microsoft.Network/virtualNetworks/write"
Microsoft.Network/networkSecurityGroups/read"
Microsoft.Network/virtualNetworks/subnets/read"",
"resources/Microsoft.Compute/virtualMachines/write"",
"resources/Microsoft.Compute/virtualMachines/extensions/write"",
"resources/Microsoft.Network/networkInterfaces/write""
```

Se hai registrato il provider di risorse "Microsoft.storage" al tuo abbonamento, non hai bisogno dell' `Microsoft.AAD/register/action`autorizzazione. Per ulteriori informazioni, fare riferimento alla "Documentazione di Azure: Autorizzazioni di Azure per lo storage" .

Fasi

1. Nel sito Azure Marketplace, cerca i prodotti NetApp.
2. Selezionare **NetApp Cloud Volumes ONTAP Direct**.
3. Fare clic su **Crea** per avviare la distribuzione guidata.
4. Selezionare un piano. L'elenco **piano** visualizza in genere le ultime versioni di Cloud Volumes ONTAP.
5. Nella scheda **informazioni di base**, fornire i seguenti dettagli:
   - **Abbonamento**: Selezionare un abbonamento. La distribuzione sarà collegata al numero di abbonamento.
   - **Gruppo di risorse**: Utilizzare un gruppo di risorse esistente o crearne uno nuovo. I gruppi di risorse consentono di allocare tutte le risorse, come dischi e macchine virtuali di storage, all'interno di un singolo gruppo per un sistema Cloud Volumes ONTAP.
   - **Regione**: Seleziona un'area che supporta l'implementazione ha di Azure in una singola AZ. Vengono visualizzate solo le regioni disponibili nell'elenco.
   - **Dimensione**: Selezionare una dimensione VM di archiviazione per il disco gestito SSD Premium v2 supportato.
   - **Zona**: Selezionare una zona per la regione selezionata.
   - **Admin Password**: Consente di impostare una password. Questa password amministratore viene utilizzata per accedere al sistema dopo la distribuzione.
   - **Conferma password**: Immettere nuovamente la stessa password per la conferma.
     - Nella scheda **rete**, aggiungere una rete virtuale e una subnet oppure selezionarle dagli elenchi.

Per rispettare le restrizioni di Microsoft Azure, è necessario creare una nuova subnet durante la configurazione di una nuova rete virtuale. Allo stesso modo, se si sceglie una rete esistente, è necessario selezionare una subnet esistente.

- Per selezionare un gruppo di protezione di rete predefinito, selezionare **Sì**. Selezionare **No** per assegnare un gruppo di protezione di rete predefinito di Azure con le regole di traffico necessarie. Per ulteriori informazioni, fare riferimento a "Regole del gruppo di sicurezza per Azure".
- Nella scheda **Avanzate** verificare se le due funzionalità di Azure necessarie per questa distribuzione sono state impostate. Fare riferimento a "Abilita una funzionalità Azure per le implementazioni di Cloud Volumes ONTAP single AZ" e "Abilita la modalità high Availability per Cloud Volumes ONTAP in Azure".
- È possibile definire coppie di nomi e valori per le risorse o i gruppi di risorse nella scheda **Tag**.
- Nella scheda **Rivedi + crea**, esaminare i dettagli e avviare la distribuzione.

Al termine

Selezionare l'icona di notifica per visualizzare l'avanzamento della distribuzione. Dopo l'implementazione di Cloud Volumes ONTAP, è possibile visualizzare l'elenco delle macchine virtuali per lo storage in cui sono riportate le operazioni.

Una volta accessibile, usa il System Manager di ONTAP o l'interfaccia a riga di comando di ONTAP per accedere alla macchina virtuale storage con le credenziali di amministratore impostate. Successivamente, è possibile creare volumi, LUN o condivisioni e iniziare a utilizzare le funzionalità di storage di Cloud Volumes ONTAP.

Risolvere i problemi di implementazione

I sistemi Cloud Volumes ONTAP implementati direttamente attraverso il marketplace di Azure non includono il supporto di NetApp. In caso di problemi durante l'implementazione, puoi eseguire il troubleshooting e risolverli in maniera indipendente.

Fasi

1. Sul sito di Azure Marketplace, andare a **Diagnostica di avvio > Registro seriale**.
2. Scaricare e analizzare i registri seriali.
3. Consultare la documentazione del prodotto e gli articoli della Knowledge base (KB) per la risoluzione dei problemi.
   - "Documentazione del marketplace di Azure"
   - "Documentazione NetApp"
   - "Articoli della KB di NetApp"

Scopri i sistemi implementati in BlueXP

Puoi scoprire i sistemi Cloud Volumes ONTAP implementati utilizzando l'implementazione diretta del marketplace Azure e gestirli come ambienti di lavoro in BlueXP . BlueXP Connector rileva i sistemi, li aggiunge come ambienti di lavoro, applica le licenze BlueXP necessarie e sblocca tutte le funzionalità di BlueXP per questi sistemi. La configurazione ha originale in una singola AZ con dischi gestiti PSSD v2 viene conservata e il sistema viene registrato nello stesso gruppo di risorse e abbonamento di Azure dell'implementazione originale.

A proposito di questa attività

Scoprendo i sistemi Cloud Volumes ONTAP implementati utilizzando la distribuzione diretta del marketplace di

Azure, BlueXP Connector esegue le seguenti attività:

- Sostituisce le licenze gratuite dei sistemi rilevati come regolari basati sulla capacità "Licenze Freemium".
- Mantiene le funzionalità esistenti dei sistemi implementati e aggiunge le funzionalità aggiuntive di BlueXP , come ad esempio data Protection, gestione dei dati e funzionalità di sicurezza.
- Sostituisce le licenze installate sui nodi con nuove licenze ONTAP per NFS, CIFS (SMB), iSCSI, ARP, SnapLock e SnapMirror.
- Converte i numeri di serie dei nodi generici in numeri di serie univoci.
- Assegna nuovi tag di sistema sulle risorse in base alle necessità.
- Converte gli indirizzi IP dinamici dell'istanza in indirizzi IP statici.
- Consente di abilitare le funzionalità dello storage"Tiering FabricPool" , , "AutoSupport"e "write-once-read-many" (WORM) sui sistemi distribuiti. È possibile attivare queste funzioni dalla console BlueXP quando necessario.
- Registra le istanze negli account NSS utilizzati per rilevarle.
- Abilita le funzionalità di gestione della capacità in "modalità automatica e manuale" per i sistemi rilevati.

Prima di iniziare

Assicurati che l'implementazione sia completa sul marketplace di Azure. BlueXP Connector è in grado di rilevare i sistemi solo quando l'implementazione è completa e disponibile per il rilevamento.

Fasi

In BlueXP , seguire la procedura standard per il rilevamento dei sistemi esistenti. Fare riferimento alla "Aggiunta di un sistema Cloud Volumes ONTAP esistente a BlueXP ".

Al termine

Al termine del rilevamento, è possibile visualizzare i sistemi elencati come ambienti di lavoro in BlueXP . È possibile eseguire diverse attività di gestione, quali "espansione dell'aggregato", "aggiunta di volumi", "Provisioning di VM di storage aggiuntive"e "modifica dei tipi di istanza".

Link correlati

Fare riferimento alla documentazione di ONTAP per ulteriori informazioni sulla creazione dello storage:

- "Creare volumi per NFS"
- "Creare LUN per iSCSI"
- "Crea condivisioni per CIFS"

Inizia a utilizzare Google Cloud

Guida rapida per Cloud Volumes ONTAP in Google Cloud

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

1 Creare un connettore

Se non si dispone ancora di un "Connettore", è necessario crearne uno. "Scopri come creare un connettore in Google Cloud"

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

2 Pianificare la configurazione

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

"Scopri di più sulla pianificazione della configurazione".

3 Configurare la rete

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

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

"Scopri di più sui requisiti di rete".

4 Impostare un account di servizio

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

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

"Leggi le istruzioni dettagliate".

5 Abilitare le API di Google Cloud

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

- API di Cloud Deployment Manager V2
- API Cloud Logging
- API Cloud Resource Manager

- API di Compute Engine
- API IAM (Identity and Access Management)

Avviare Cloud Volumes ONTAP utilizzando BlueXP

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

Link correlati

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

Pianificare la configurazione di Cloud Volumes ONTAP in Google Cloud

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

Scegliere una licenza Cloud Volumes ONTAP

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

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

Scegliere una regione supportata

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

Scegliere un tipo di computer supportato

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

"Configurazioni supportate per Cloud Volumes ONTAP in GCP"

Comprendere i limiti dello storage

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

"Limiti di storage per Cloud Volumes ONTAP in GCP"

Dimensionare il sistema in GCP

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di performance e

capacità. Quando si sceglie un tipo di macchina, un tipo di disco e una dimensione del disco, occorre tenere presente alcuni punti chiave:

Tipo di macchina

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

Per ulteriori informazioni, fare riferimento a quanto segue:

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

Tipo di disco GCP

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

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

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

Dimensione del disco GCP

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

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

  Per ulteriori informazioni, fare riferimento a quanto segue:

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

Visualizzare i dischi di sistema predefiniti

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

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

- "Documenti di Google Cloud: Quote delle risorse"

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

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

Raccogliere informazioni di rete

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

Informazioni di rete per un sistema a nodo singolo

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

Informazioni di rete per una coppia ha in più zone

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

Informazioni di rete per una coppia ha in una singola zona

Informazioni GCP	Il tuo valore
Regione	
Zona	

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

Scegliere una velocità di scrittura

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

Scegliere un profilo di utilizzo del volume

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

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

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

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

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

Configura il networking di Google Cloud per Cloud Volumes ONTAP

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

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

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in Google Cloud.

Requisiti specifici per i sistemi a nodo singolo

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

Un VPC

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

Indirizzi IP privati

Per un sistema a nodo singolo in Google Cloud, BlueXP alloca gli indirizzi IP privati per quanto segue:

- Nodo
- Cluster
- VM di storage
- LIF data NAS
- LIF iSCSI dei dati

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

```
skipSvmManagementLif: true
```

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

Requisiti specifici delle coppie ha

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

Una o più zone

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

- Zone multiple (consigliato)

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

- Zona singola

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

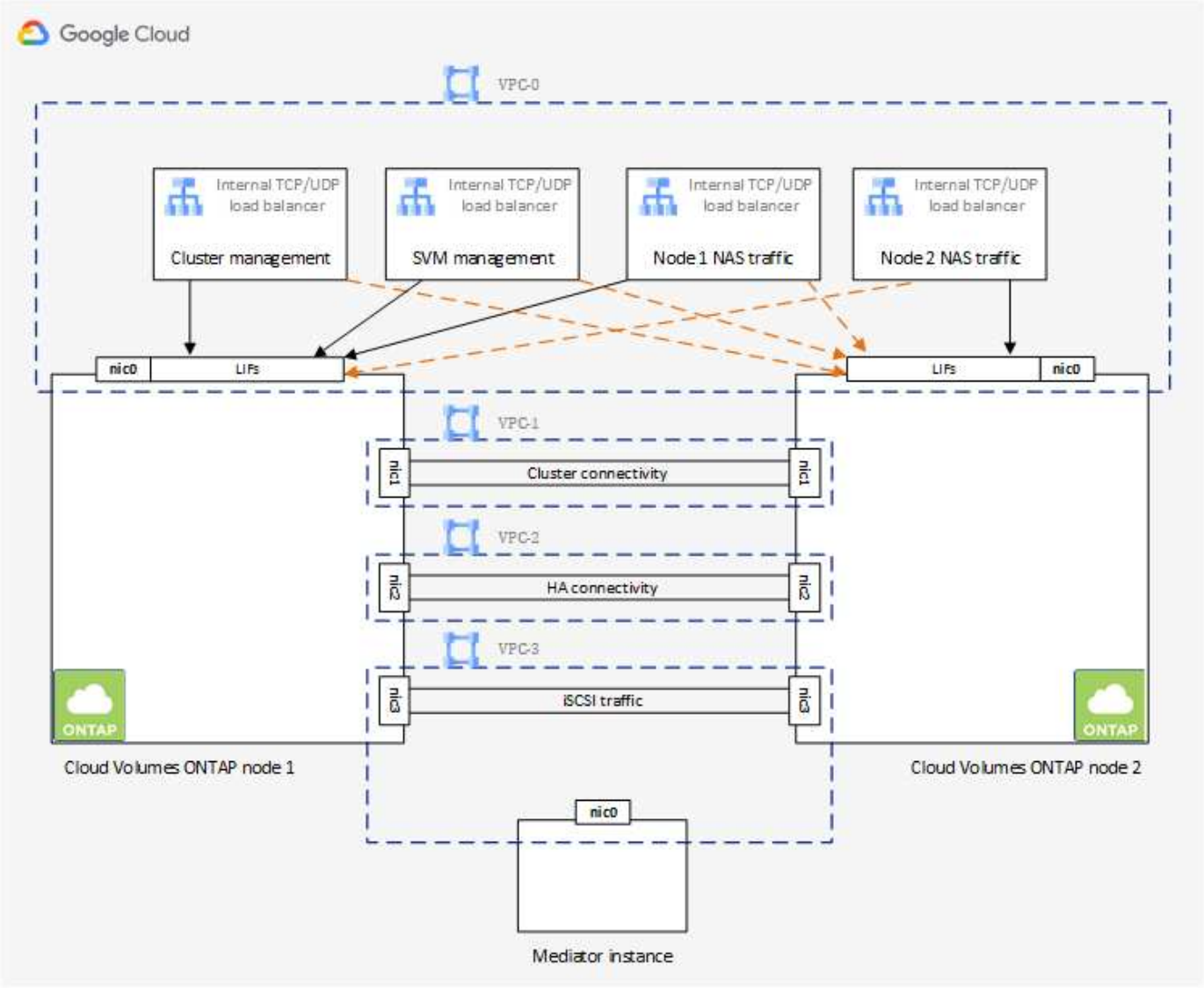
  Questo modello di implementazione riduce i costi perché non sono previsti costi di uscita dei dati tra le zone.

Quattro cloud privati virtuali

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

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

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



Subnet

Per ogni VPC è necessaria una subnet privata.

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

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

Indirizzi IP privati

BlueXP assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Google Cloud. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi privati.

Il numero di LIF allocati da BlueXP per Cloud Volumes ONTAP dipende dalla distribuzione di un sistema a nodo singolo o di una coppia ha. LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

- **Nodo singolo** BlueXP assegna 4 indirizzi IP a un sistema a nodo singolo:
  - LIF di gestione dei nodi
  - LIF gestione cluster
  - LIF dati iSCSI

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

  - LIF NAS

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

```
skipSvmManagementLif: true
```

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

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

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

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

```
skipSvmManagementLif: true
```

Bilanciatori di carico interni

BlueXP crea automaticamente quattro bilanciatori di carico interni di Google Cloud (TCP/UDP) che gestiscono il traffico in entrata verso la coppia ha di Cloud Volumes ONTAP. Non è richiesta alcuna configurazione Questo

requisito è stato elencato semplicemente per informarti del traffico di rete e per mitigare eventuali problemi di sicurezza.

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

La configurazione per ciascun bilanciamento del carico è la seguente:

- Un indirizzo IP privato condiviso
- Un controllo globale dello stato di salute

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

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

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

VPC condivisi

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

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

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

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

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

Mirroring dei pacchetti in VPC

"Mirroring dei pacchetti" Deve essere disattivato nella subnet Google Cloud in cui si implementa Cloud Volumes ONTAP.

Accesso a Internet in uscita

I sistemi Cloud Volumes ONTAP richiedono l'accesso a Internet outbound per l'accesso a endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con severi requisiti di sicurezza.

BlueXP Connector contatta anche diversi endpoint per le operazioni quotidiane e la console basata sul Web di BlueXP . Per informazioni sugli endpoint BlueXP , fare riferimento a "Visualizzare gli endpoint contattati dal connettore" e "Preparazione del networking per l'utilizzo della console BlueXP".

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Endpoint	Applicabile per	Scopo	Modalità di distribuzione BlueXP	Impatto se l'endpoint non è disponibile
https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione BlueXP .	Modalità standard e limitata.	L'autenticazione dell'utente non riesce e i seguenti servizi rimangono non disponibili: • I servizi di Cloud Volumes ONTAP • Servizi ONTAP • E servizi proxy
https://cloudmanager.cloud.netapp.com/tenancy	Locazione	Utilizzato per recuperare le risorse Cloud Volumes ONTAP dalla tenancy BlueXP per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
https://support.NetApp.com/aods/asupp message https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Utilizzato per inviare dati telemetrici AutoSupport al supporto NetApp.	Modalità standard e limitata.	Le informazioni AutoSupport rimangono non trasmesse.

Endpoint	Applicabile per	Scopo	Modalità di distribuzione BlueXP	Impatto se l'endpoint non è disponibile
https://www.googleapis.com/compute/v1/projects/ https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects https://compute.googleapis.com/compute/v1	Google Cloud (uso commerciale).	Comunicazioni con i servizi Google Cloud.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non può comunicare con il servizio Google Cloud per eseguire specifiche operazioni BlueXP in Google Cloud.

Connessioni a sistemi ONTAP in altre reti

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

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

Regole del firewall

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

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

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

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

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

Regole in entrata

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

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

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

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione cluster
HTTPS	443	Connettività con il connettore e accesso HTTPS alla console web di ONTAP System Manager usando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
TCP	63001-63050	Bilanciamento del carico delle porte delle sonde per determinare quale nodo è integro (richiesto solo per coppie ha)
UDP	111	Chiamata a procedura remota per NFS

Protocollo	Porta	Scopo
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita

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

Regole di base in uscita

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

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

Regole avanzate in uscita

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

La sorgente è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

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

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
AutoSupport	HTTPS	443	LIF di gestione dei nodi	support.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	LIF di gestione dei nodi	support.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	LIF di gestione dei nodi	Connettore	Invio di messaggi AutoSupport tramite un server proxy sul connettore, se non è disponibile una connessione Internet in uscita
Backup della configurazione	HTTP	80	LIF di gestione dei nodi	Http://<connector-IP-address>/occm/offboxconfig	Inviare i backup di configurazione al connettore. "Documentazione ONTAP"
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

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

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

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

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

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

Requisiti per il connettore

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

- "Visualizzare i requisiti di rete per il connettore"
- "Regole del firewall in Google Cloud"

Configurazioni di rete per supportare il proxy del connettore

È possibile utilizzare i server proxy configurati per BlueXP Connector per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. BlueXP supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy del connettore. L'amministratore del connettore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato nell'ambiente di lavoro Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP attraverso il proxy del connettore. Quando si configura un proxy trasparente, l'amministratore del connettore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurarsi di ottenere e caricare lo stesso certificato CA radice nell'ambiente di lavoro Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy per BlueXP Connector, fare riferimento a "Configurare un connettore per l'utilizzo di un server proxy" .

Configurare i tag di rete per Cloud Volumes ONTAP in Google Cloud

Durante la configurazione del proxy trasparente del connettore, l'amministratore del connettore aggiunge un tag di rete per Google Cloud. È necessario ottenere e aggiungere manualmente lo stesso tag di rete per la configurazione Cloud Volumes ONTAP . Questo tag è necessario per il corretto funzionamento del server proxy.

1. Nella console di Google Cloud, individua il tuo ambiente di lavoro Cloud Volumes ONTAP .
2. Vai a **Dettagli > Networking > Tag di rete**.

3. Aggiungere il tag utilizzato per il connettore e salvare la configurazione.

Argomenti correlati

- "Verificare la configurazione di AutoSupport per Cloud Volumes ONTAP"
- "Informazioni sulle porte interne di ONTAP".

Configura i controlli del servizio VPC per implementare Cloud Volumes ONTAP in Google Cloud

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

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

Come i servizi NetApp comunicano con VPC Service Controls

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

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

Immagini

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

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

Implementazione di un connettore

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

Implementazione di Cloud Volumes ONTAP

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

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

Servizio VPC controlla le policy del perimetro

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

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

Regole di ingresso

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

OPPURE

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

OPPURE

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

Regole di uscita

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

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

Creare un account di servizio Google Cloud per Cloud Volumes ONTAP

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

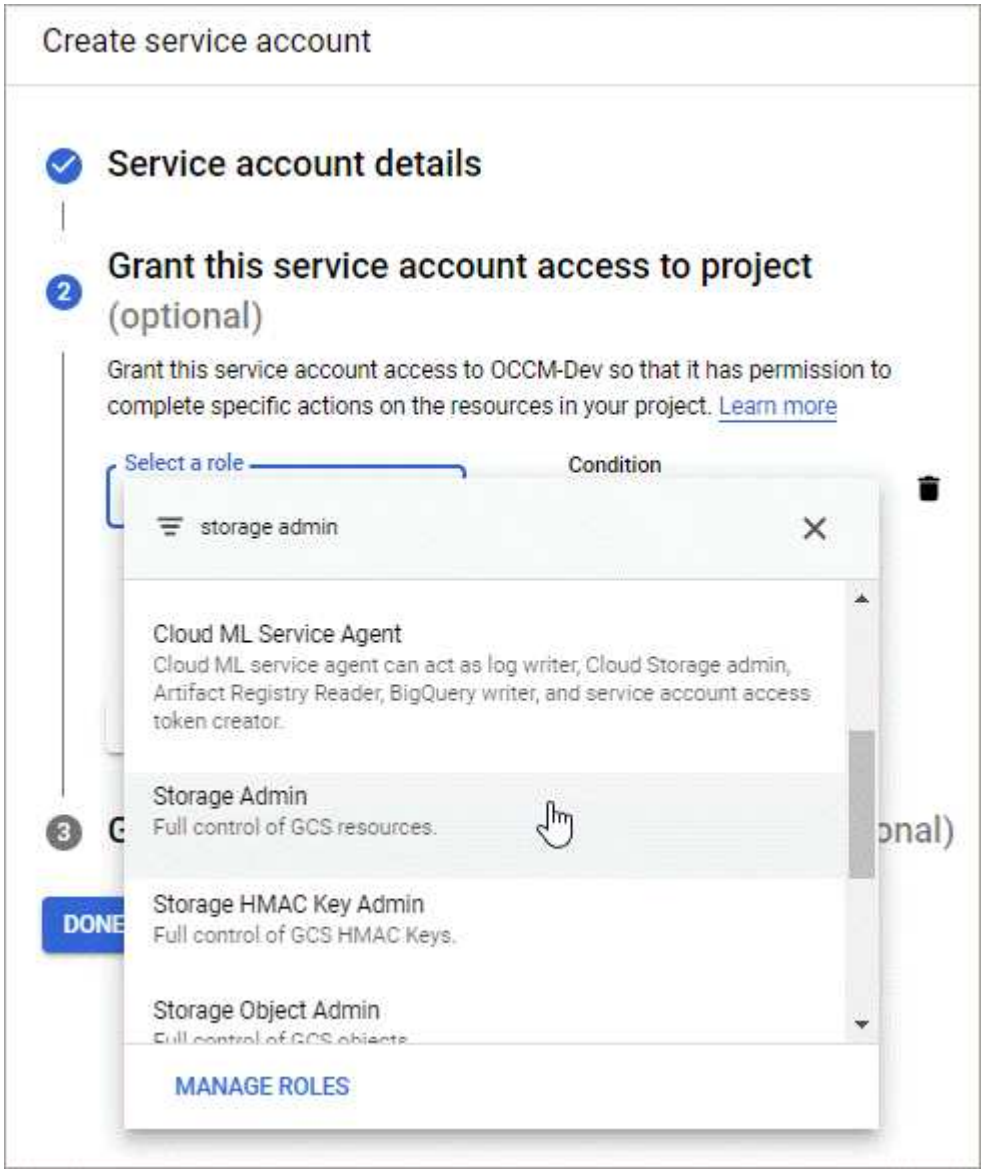
Cloud Volumes ONTAP utilizza l'account di servizio per accedere e gestire un bucket per i dati a più livelli e un altro bucket per i backup.

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

Fasi

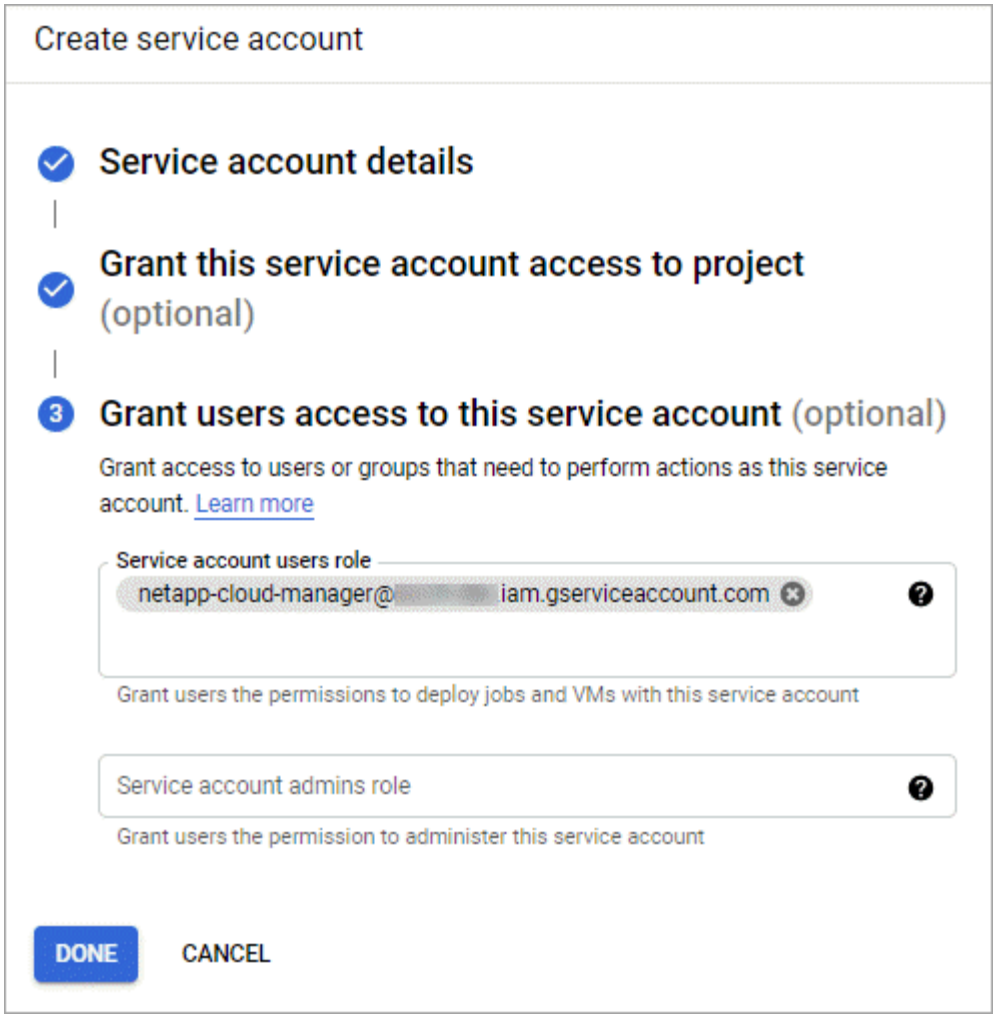
1. Nella console di Google Cloud, "Accedere alla pagina Service accounts (account servizio)".
2. Selezionare il progetto.
3. Fare clic su **Create service account** (Crea account servizio) e fornire le informazioni richieste.

a. **Dettagli account servizio**: Inserire un nome e una descrizione.
b. **Consenti a questo account di servizio l'accesso al progetto**: Selezionare il ruolo **Storage Admin**.



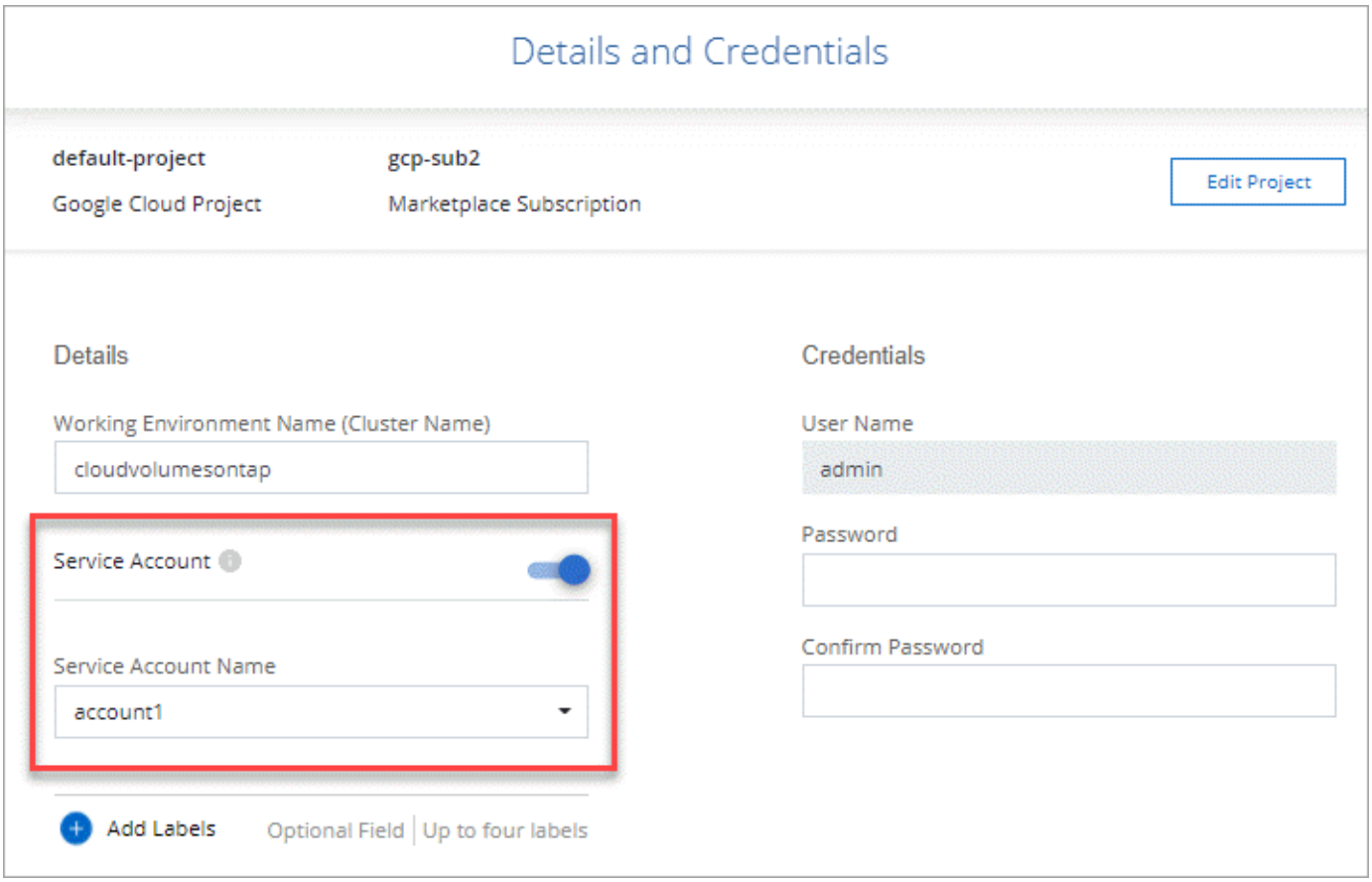
c. **Consenti agli utenti di accedere a questo account del servizio**: Aggiungi l'account del servizio Connector come *utente dell'account del servizio* a questo nuovo account del servizio.

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



Quali sono le prossime novità?

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



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

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

Fasi

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

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

   Le autorizzazioni sono le seguenti:

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

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

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

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

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

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

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

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

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

   Esempio

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

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

Impostare la licenza per Cloud Volumes ONTAP in Google Cloud

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

Freemium

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

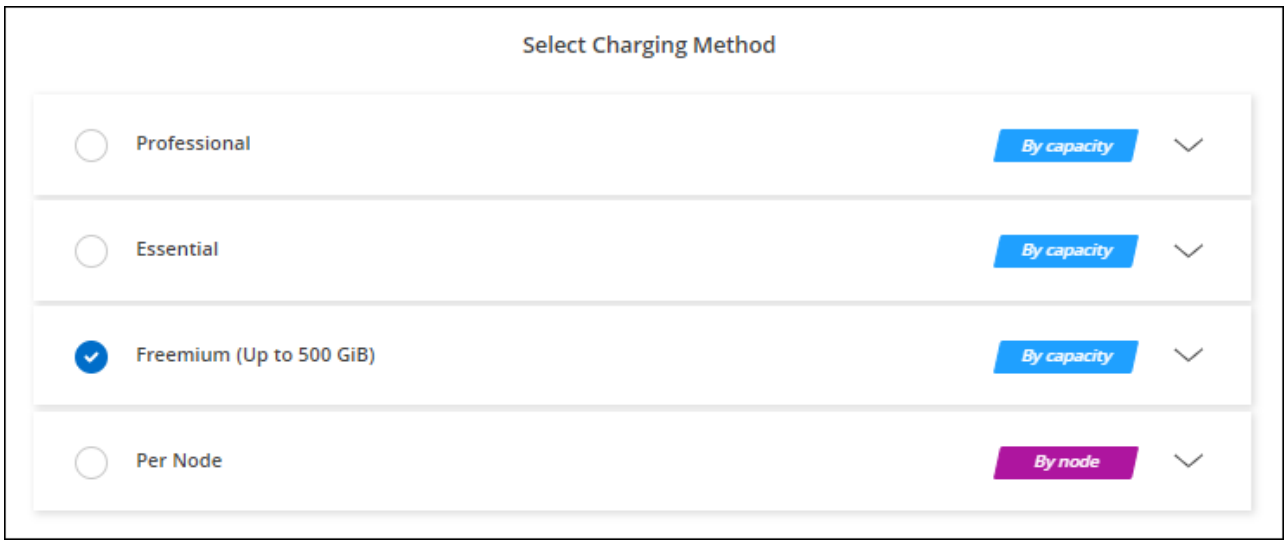
Fasi

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

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

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

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



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

Licenza basata sulla capacità

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

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

- Una licenza acquistata da NetApp (Bring Your Own License, BYOL)
- Un abbonamento oraria a pagamento (PAYGO) da Google Cloud Marketplace
- Un contratto annuale

"Scopri di più sulle licenze basate sulla capacità".

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

BYOL

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

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Fasi

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

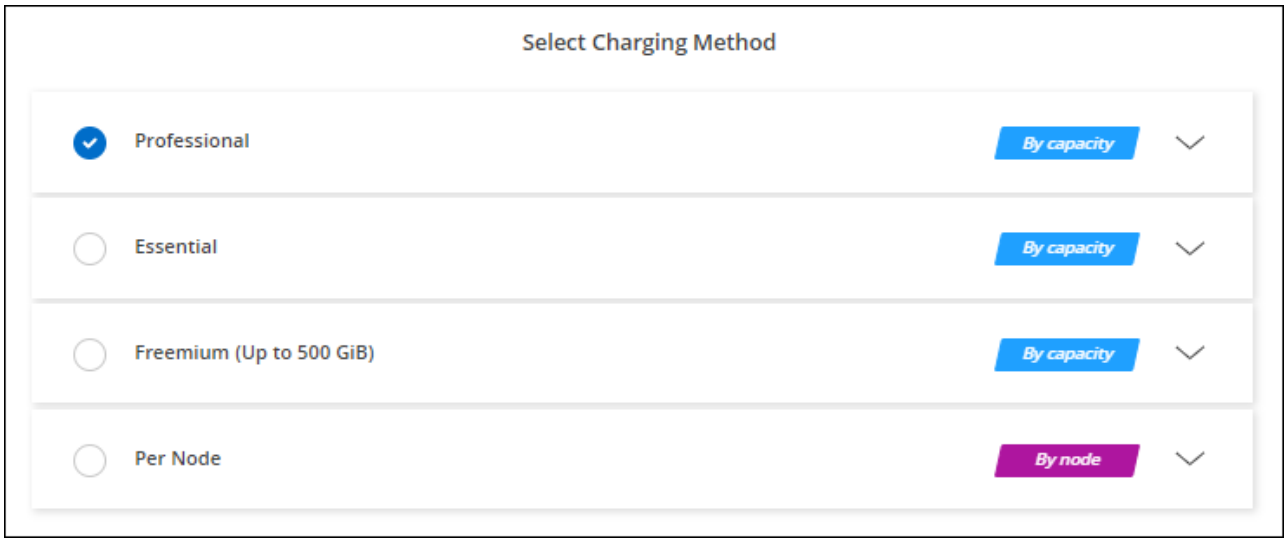
BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

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

3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in Google Cloud Marketplace.

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

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



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

Abbonamento PAYGO

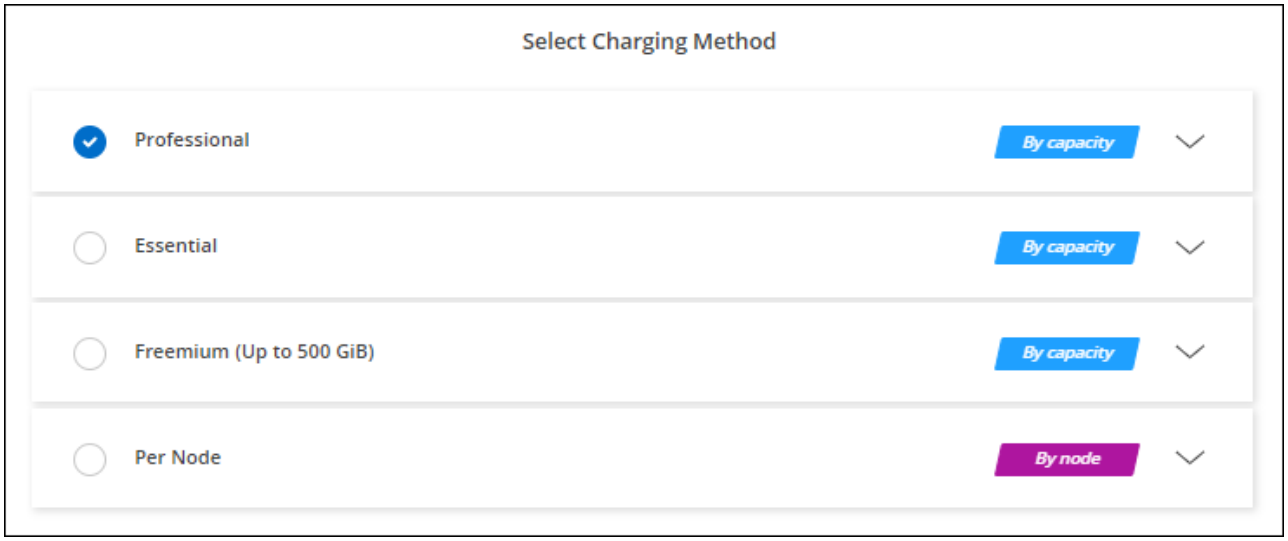
Paga ogni ora sottoscrivendo l'offerta sul mercato del tuo cloud provider.

Quando crei un ambiente di lavoro Cloud Volumes ONTAP, BlueXP ti chiede di sottoscrivere il contratto disponibile in Google Cloud Marketplace. Tale abbonamento viene quindi associato all'ambiente di lavoro per la ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in Google Cloud Marketplace.
   b. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla

pagina dei metodi di ricarica.



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

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

Contratto annuale

Paga Cloud Volumes ONTAP ogni anno acquistando un contratto annuale.

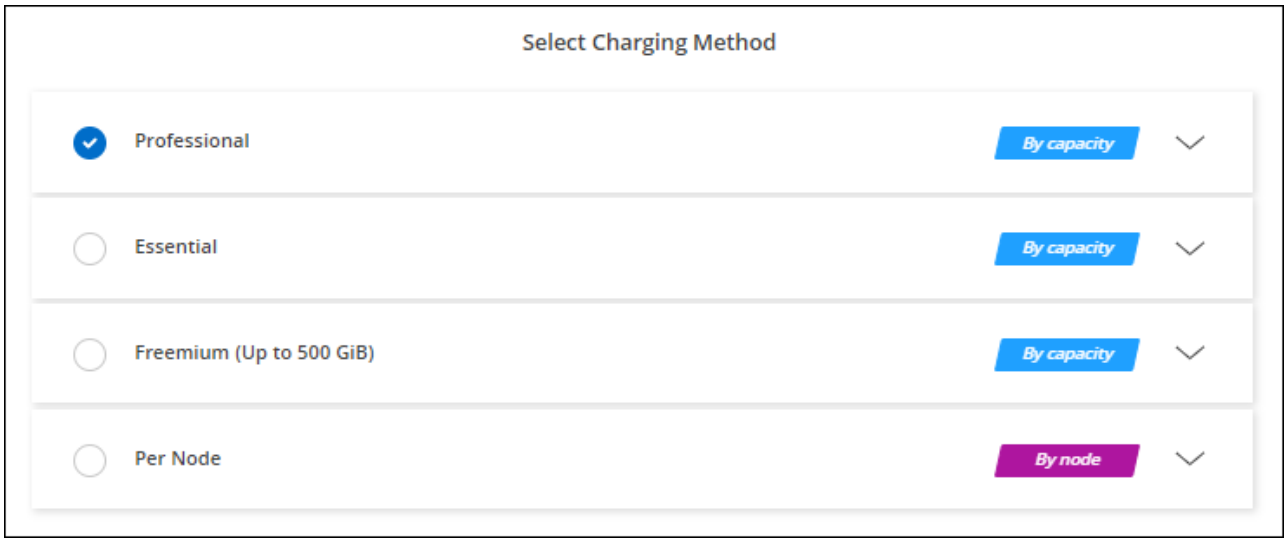
Fasi

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

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

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

2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi al piano annuale in Google Cloud Marketplace.
   b. In Google Cloud, seleziona il piano annuale condiviso con il tuo account, quindi fai clic su **Iscriviti**.
   c. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



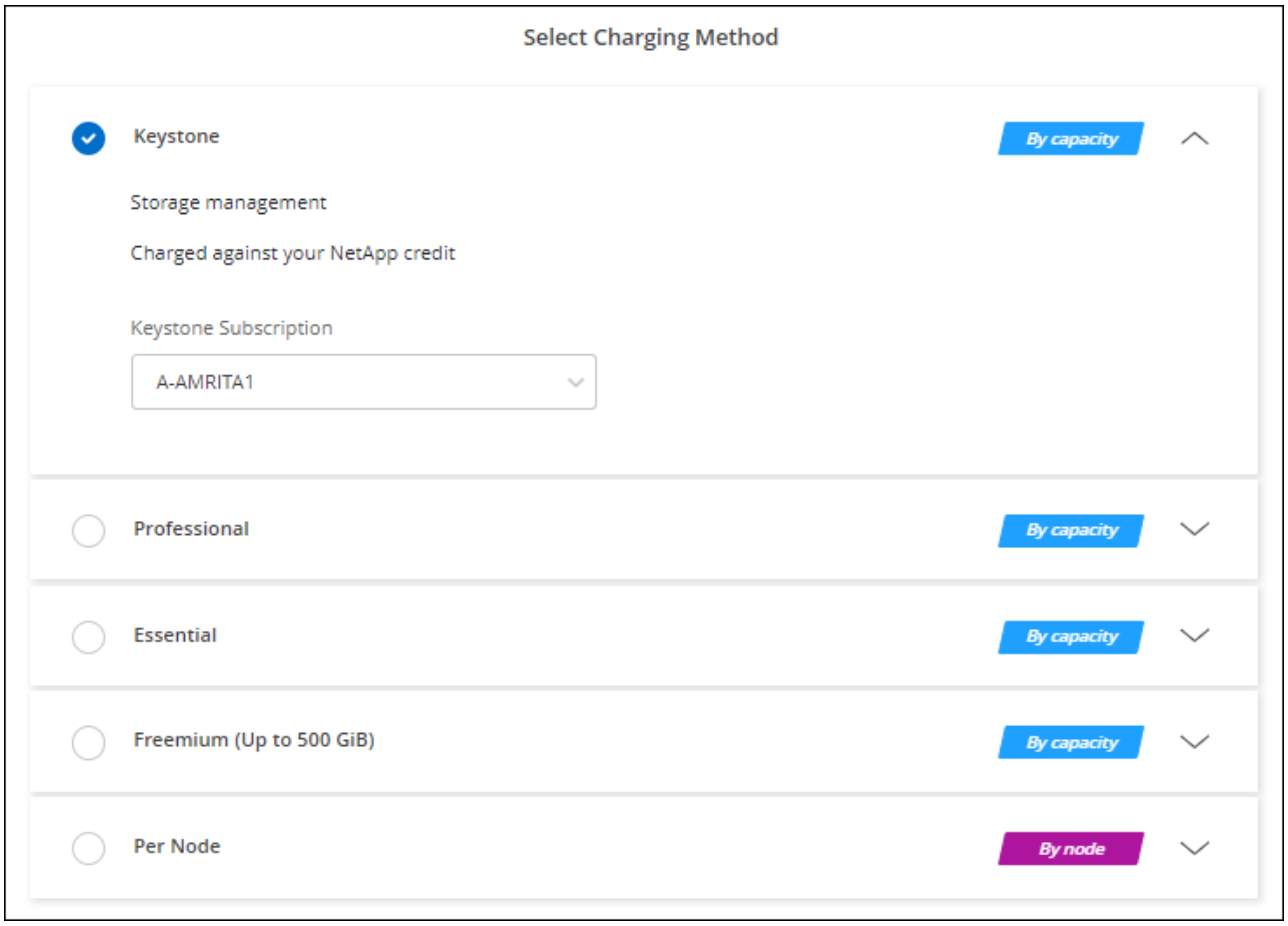
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud".

Iscrizione Keystone

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

Fasi

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



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

Avviare Cloud Volumes ONTAP in Google Cloud

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

Prima di iniziare

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

- Un connettore funzionante.
  - Si dovrebbe avere un "Connettore associato al progetto o all'area di lavoro".
  - "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
  - L'account del servizio associato al connettore "deve disporre delle autorizzazioni necessarie"
- Comprensione della configurazione che si desidera utilizzare.

  Dovresti aver preparato scegliendo una configurazione e ottenendo le informazioni di rete di Google Cloud dal tuo amministratore. Per ulteriori informazioni, fare riferimento alla "Pianificazione della configurazione di Cloud Volumes ONTAP".

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

  "Scopri come impostare le licenze".

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

Lancia un sistema a nodo singolo in Google Cloud

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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una località**: Seleziona **Google Cloud** e **Cloud Volumes ONTAP**.
4. Se richiesto, "Creare un connettore".
5. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, selezionare un account di servizio, aggiungere etichette e specificare le credenziali.

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

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

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

Il seguente video mostra come associare un abbonamento al marketplace a consumo al tuo progetto Google Cloud. In alternativa, segui i passaggi per l'abbonamento indicati nella sezione "Associazione di un abbonamento a Marketplace con le credenziali Google Cloud" sezione.

Iscriviti a BlueXP dal marketplace di Google Cloud

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

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

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

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

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

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

8. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 è disponibile. L'aggiornamento non viene eseguito da una versione all'altra, ad esempio da 9,13 a 9,14.
11. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

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

    Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

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

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

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

"Scopri di più sulla velocità di scrittura".

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

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

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

"Scopri di più sullo storage WORM".

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

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

Tenere presente quanto segue:

- BlueXP imposta l'account del servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Assicurarsi di aggiungere l'account del servizio Connector come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da BlueXP
- Per informazioni sull'aggiunta di un account Google Cloud, fare riferimento alla sezione "Configurazione e aggiunta di account Google Cloud per il tiering dei dati con 9.6".
- Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
- Se si disattiva il tiering dei dati, è possibile attivarlo su aggregati successivi, ma è necessario spegnere il sistema e aggiungere un account di servizio dalla console di Google Cloud.

"Scopri di più sul tiering dei dati".

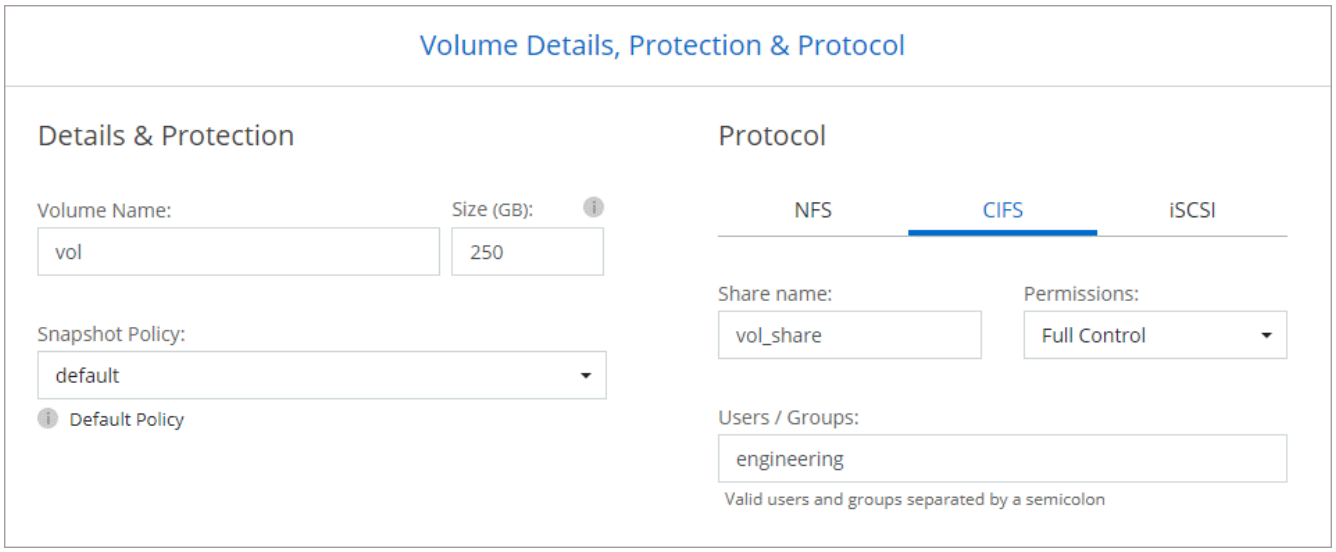
14. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

"Scopri le versioni e i protocolli client supportati".

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

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

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



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

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce. Se si configura Google Managed Active Directory, per impostazione predefinita è possibile accedere ad utilizzando l'indirizzo IP 169.254.169.254.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=cloud** in questo campo.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. Per "Documenti sull'automazione BlueXP" ulteriori informazioni, fare riferimento alla . Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

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

    Per ulteriori informazioni, fare riferimento a "Scegliere un profilo di utilizzo del volume", , "Panoramica sul tiering dei dati"e. "KB: Quali funzionalità di efficienza dello storage inline sono supportate in CVO?"

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

Risultato

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

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

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

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

Al termine

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

  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.

Lancia una coppia ha in Google Cloud

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

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una località**: Seleziona **Google Cloud** e **Cloud Volumes ONTAP ha**.
4. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, selezionare un account di servizio, aggiungere etichette e specificare le credenziali.

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

Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome account servizio	Se si intende utilizzare "Tiering BlueXP" oppure "Backup e ripristino BlueXP" Services (servizi), è necessario attivare lo switch **Service account** (account servizio) e selezionare l'account di servizio che ha il ruolo di amministratore dello storage predefinito.
Aggiungi etichette	Le etichette sono metadati per le risorse Google Cloud. BlueXP aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse di Google Cloud associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro. Per informazioni sulle etichette, fare riferimento a. "Documentazione Google Cloud: Risorse per l'etichettatura".
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestione di sistema di ONTAP o l'interfaccia a riga di comando di ONTAP. Mantenere il nome utente predefinito *admin* o modificarlo in un nome utente personalizzato.

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

Il seguente video mostra come associare un abbonamento al marketplace a consumo al tuo progetto Google Cloud. In alternativa, segui i passaggi per l'abbonamento indicati nella sezione "Associazione di un abbonamento al marketplace alle credenziali di Google Cloud" sezione.

Iscriviti a BlueXP dal marketplace di Google Cloud

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

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

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

   "Scopri di più sui modelli di implementazione ha".

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

   "Scopri di più sui requisiti di rete".

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

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

8. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 è disponibile. L'aggiornamento non viene eseguito da una versione all'altra, ad esempio da 9,13 a 9,14.
11. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

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

    Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

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

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

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

"Scopri di più sulla velocità di scrittura".

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

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

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

"Scopri di più sullo storage WORM".

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

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

Tenere presente quanto segue:

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

"Scopri di più sul tiering dei dati".

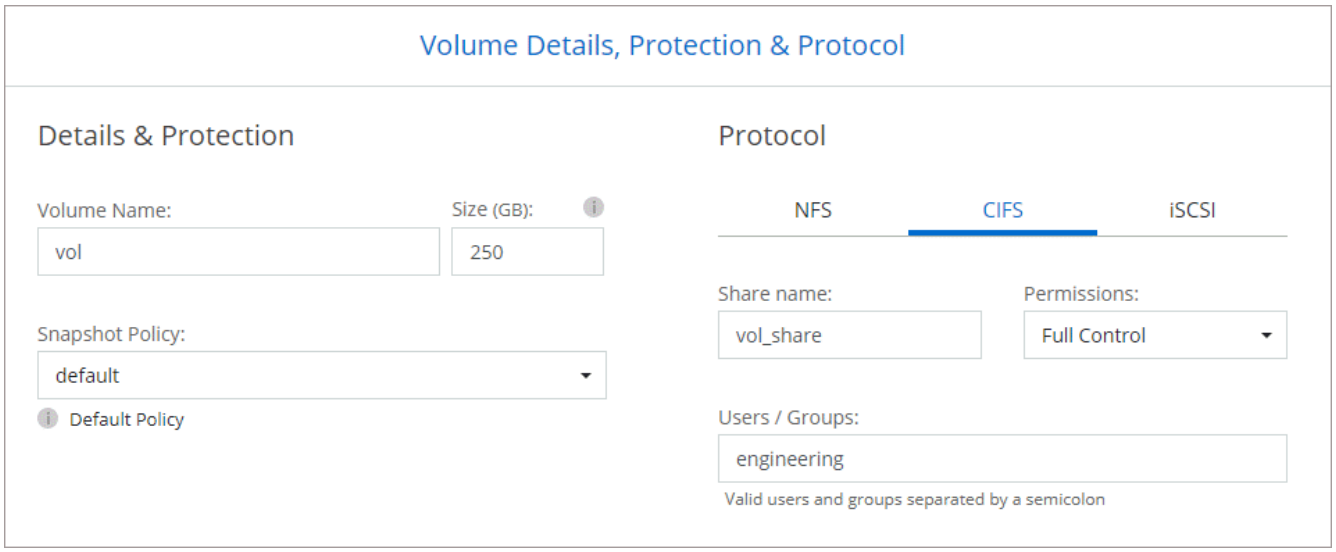
14. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

"Scopri le versioni e i protocolli client supportati".

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

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

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



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

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce. Se si configura Google Managed Active Directory, per impostazione predefinita è possibile accedere ad utilizzando l'indirizzo IP 169.254.169.254.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=cloud** in questo campo.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. Per ulteriori informazioni, fare riferimento alla "Documenti sull'automazione BlueXP" . Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

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

    Per ulteriori informazioni, fare riferimento a "Scegliere un profilo di utilizzo del volume", , "Panoramica sul tiering dei dati"e. "KB: Quali funzionalità di efficienza dello storage inline sono supportate in CVO?"

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

Risultato

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

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

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

Al termine

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

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

Verifica dell'immagine della piattaforma Google Cloud

Scopri come l'immagine di Google Cloud è verificata in Cloud Volumes ONTAP

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

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

Converti immagine Google Cloud in formato RAW per Cloud Volumes ONTAP

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

Perché è necessario questo passaggio?

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

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

- Accesso al bucket di storage Google
- Scrivi al bucket di storage Google
- Creazione di processi di cloud build (utilizzati durante il processo di esportazione)

- Accesso all’immagine desiderata
- Creare attività di esportazione delle immagini

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

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

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

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

Esportare l’immagine di Google Cloud utilizzando gcloud

Fare clic per visualizzare

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

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


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

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

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

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

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

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


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

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

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

Estrarre i file compressi

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

Per ulteriori informazioni su come esportare un'immagine tramite Google Cloud, fare riferimento a "Documento Google Cloud sull'esportazione di un'immagine".

Verifica della firma dell'immagine

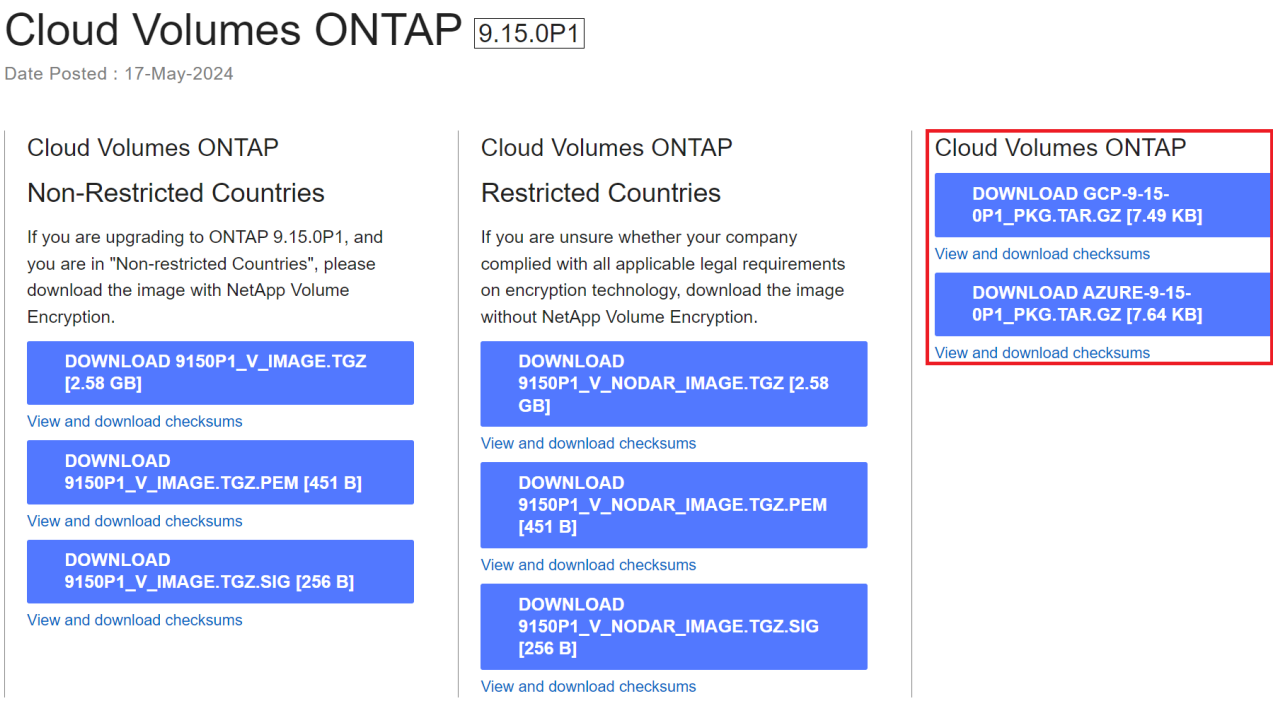
Verifica della firma dell'immagine Google Cloud per Cloud Volumes ONTAP

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

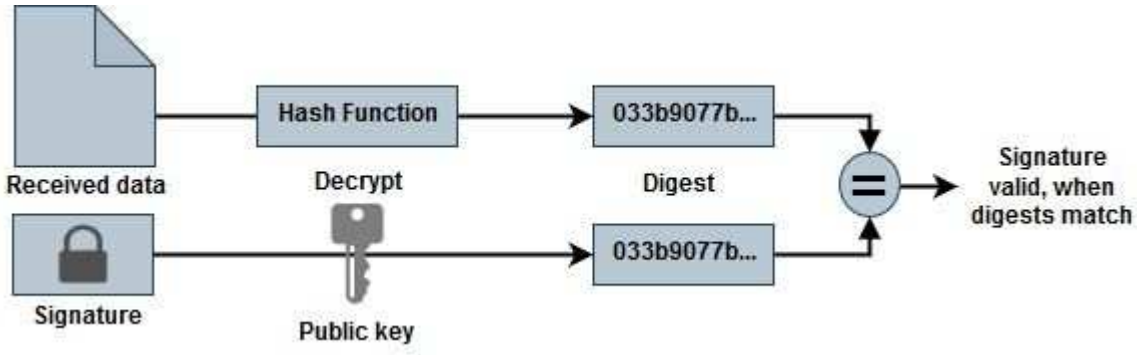
Riepilogo del flusso di lavoro per la verifica dell'immagine firmata

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

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



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



Verificare il file disk.raw dell'immagine di Google Cloud per Cloud Volumes ONTAP utilizzando OpenSSL

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

I comandi OpenSSL per convalidare l'immagine sono compatibili con i computer Linux, macOS e Windows.

Fasi

1. Verificare il certificato utilizzando OpenSSL.

Fare clic per visualizzare

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

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

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

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

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

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

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

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

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

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

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

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

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

Fare clic per visualizzare

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

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

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

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

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

USA Cloud Volumes ONTAP

Gestione delle licenze

Gestisci le licenze basate sulla capacità per Cloud Volumes ONTAP

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.

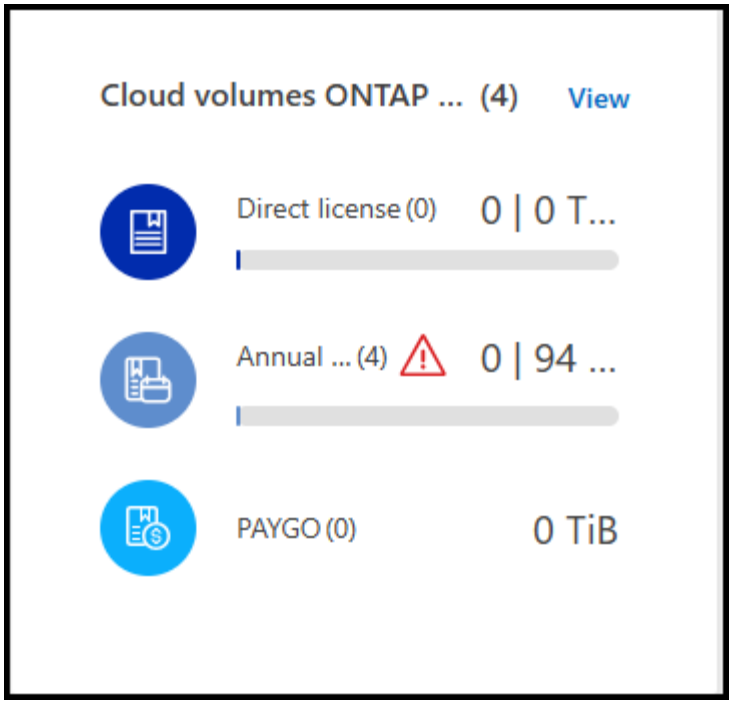
Se BlueXP non riesce ad aggiungere la licenza, sarà necessario aggiungerla manualmente al portafoglio digitale. Ad esempio, se il connettore è installato in una posizione che non dispone di accesso a Internet, sarà necessario aggiungere le licenze. "Scopri come aggiungere le licenze acquistate al tuo 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 **Panoramica**, il riquadro Cloud Volumes ONTAP visualizza la capacità corrente fornita per l'account.



- *Direct License* è la capacità totale fornita di tutti i sistemi Cloud Volumes ONTAP nell'account NetApp. La ricarica si basa sulle dimensioni fornite da ciascun volume, indipendentemente dallo spazio locale, utilizzato, memorizzato o effettivo all'interno del volume.
- *Contratto annuale* è la capacità totale con licenza (Bring Your Own License (BYOL) o contratto di mercato) acquistata da NetApp.
- *PAYGO* è la capacità totale sottoposta a provisioning mediante le iscrizioni al marketplace cloud. 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.

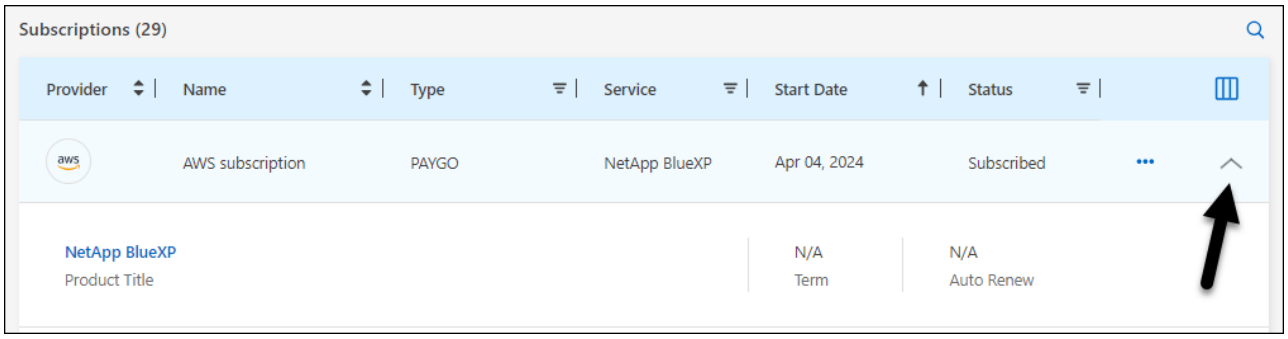
3. Selezionare **Visualizza** per visualizzare la capacità consumata per ciascun pacchetto di licenze.
4. Selezionare la scheda **licenze** per visualizzare i dettagli relativi a ciascuna licenza pacchetto acquistata.

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

5. Selezionare la scheda **Sottoscrizioni** per visualizzare la capacità consumata in base al modello di consumo della licenza. Questa scheda include sia le licenze PAYGO che le licenze contrattuali annuali.

   Verranno visualizzati solo gli abbonamenti associati all'organizzazione attualmente visualizzata.

6. Durante la visualizzazione delle informazioni relative alle sottoscrizioni, è possibile interagire con i dettagli della tabella come segue:
   - Espandere una riga per visualizzare ulteriori dettagli.

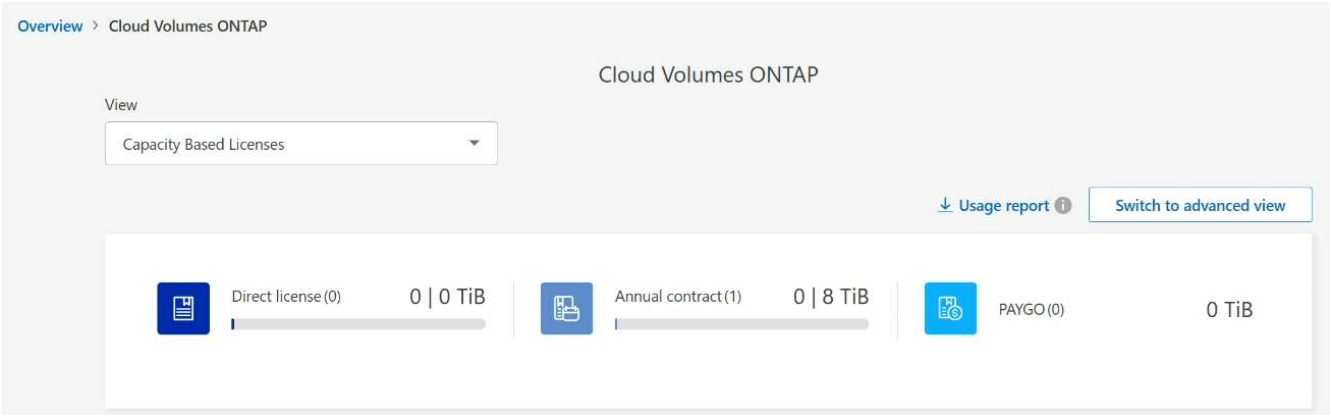


- Selezionare per scegliere le colonne da visualizzare nella tabella. Si noti che le colonne Term (termine) e Auto Renew (Rinnova automaticamente) non vengono visualizzate per impostazione predefinita. La colonna Auto Renew (rinnovo automatico) visualizza le informazioni di rinnovo solo per i contratti Azure.

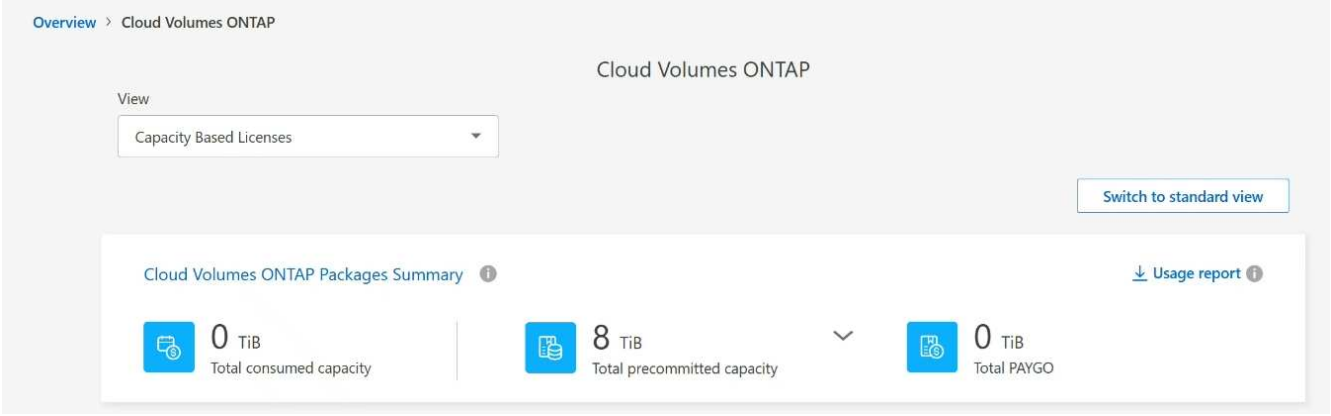
Visualizzazione dei dettagli del pacchetto

È possibile visualizzare i dettagli sulla capacità utilizzata per pacchetto passando alla modalità legacy nella pagina Cloud Volumes ONTAP.

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Nella scheda **Panoramica**, il riquadro Cloud Volumes ONTAP visualizza la capacità corrente fornita per l'account.
3. Selezionare **View** (Visualizza) per visualizzare la capacità fornita per ciascun pacchetto di licenze.
4. Selezionare **passa alla vista avanzata**.



5. Consente di visualizzare i dettagli del pacchetto che si desidera visualizzare.



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

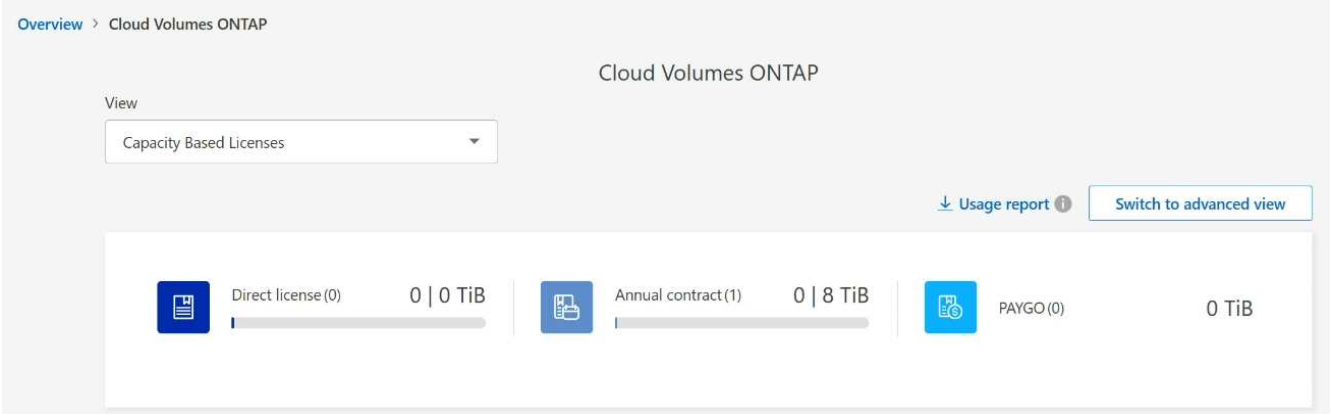
- La modifica del metodo di addebito non influisce sul costo di una licenza acquistata tramite NetApp (BYOL) o sull'abbonamento pay-as-you-go (Marketplace) del cloud provider.

  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.

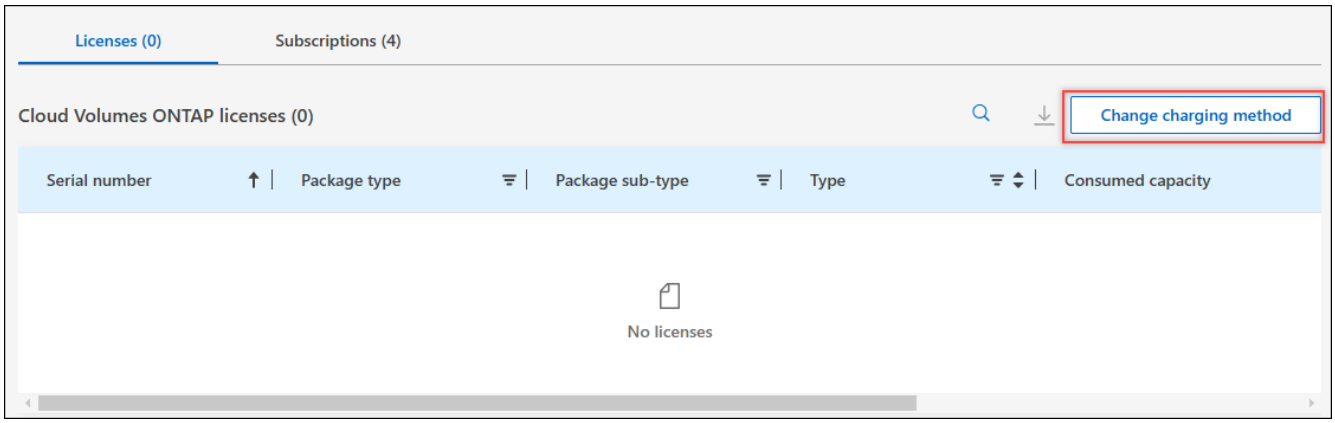
- Se disponi di un'offerta o di un contratto privato sul mercato del tuo cloud provider, il passaggio a un metodo di addebito non incluso nel contratto comporterà l'addebito di BYOL (se hai acquistato una licenza da NetApp) o PAYGO.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **passa alla vista avanzata**.



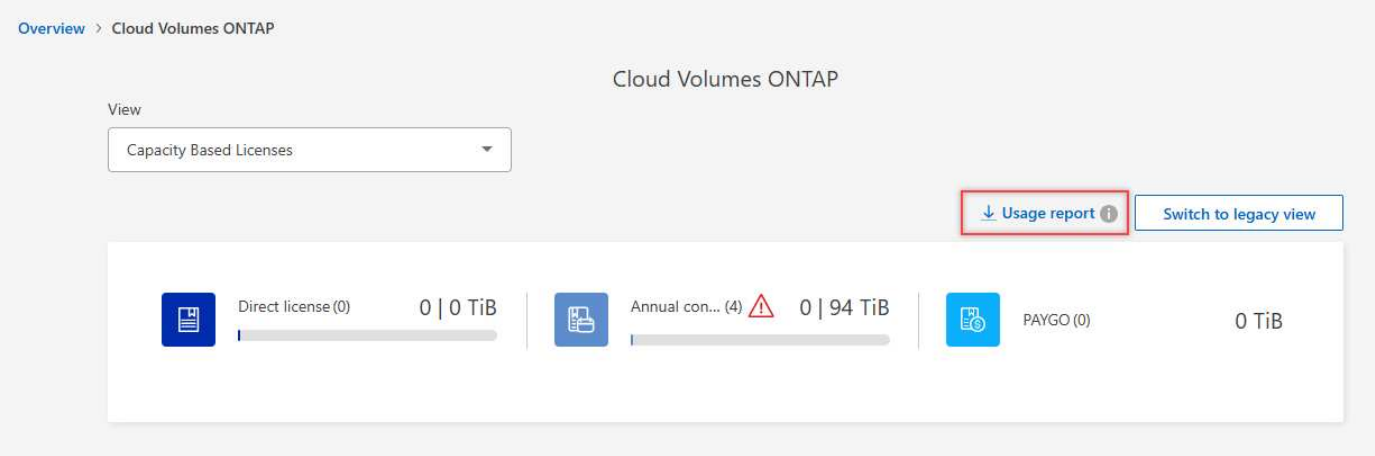
5. Scorrere verso il basso fino alla tabella **licenza basata sulla capacità** e selezionare **Modifica metodo di addebito**.



6. Nella finestra a comparsa **Modifica metodo di ricarica**, selezionare un ambiente di lavoro, scegliere il nuovo metodo di ricarica, quindi confermare che la modifica del tipo di pacchetto influirà sulle spese di assistenza.
7. Selezionare **Modifica metodo di ricarica**.

Scarica i report sull'utilizzo

Puoi scaricare quattro report sull'utilizzo dal Digital Wallet di 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 rapporto 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 include le seguenti informazioni per ciascun pacchetto:
  - 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 sono disponibili solo nel report. Contiene 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 **Panoramica**, selezionare **Visualizza** dal riquadro Cloud Volumes ONTAP.
3. Selezionare **rapporto sull'utilizzo**.

   Il report di utilizzo viene scaricato.

4. Aprire il file scaricato per accedere ai report.

Gestione delle iscrizioni a Keystone tramite BlueXP

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.

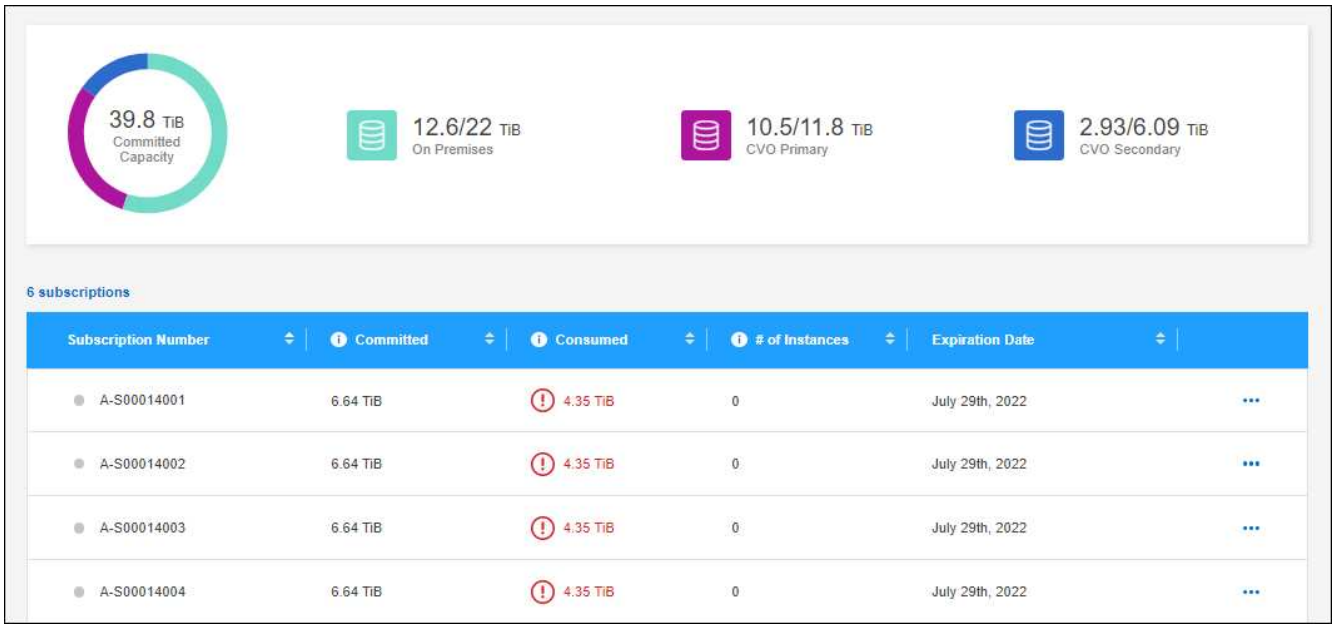
Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare **Iscrizioni 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 alla scheda **Iscrizioni Keystone** per visualizzare le iscrizioni.

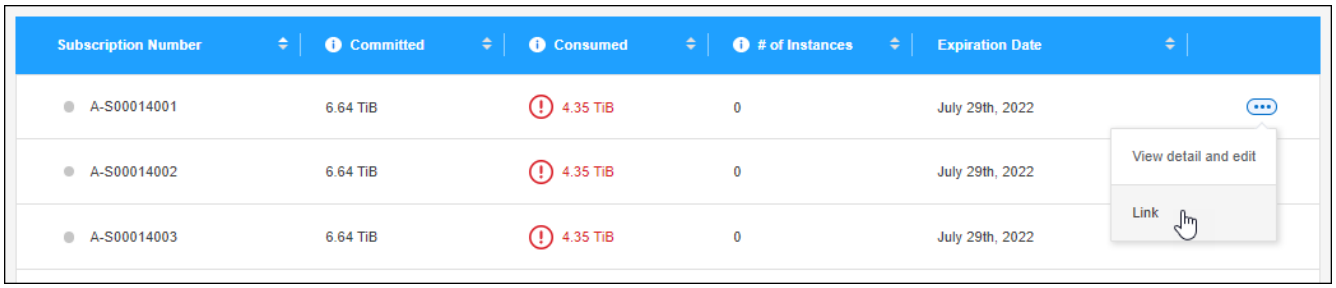


Collegare un abbonamento

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 **Iscrizioni Keystone**.
3. Per l'abbonamento che si desidera collegare, fare clic su ••• E selezionare **link**.



Risultato

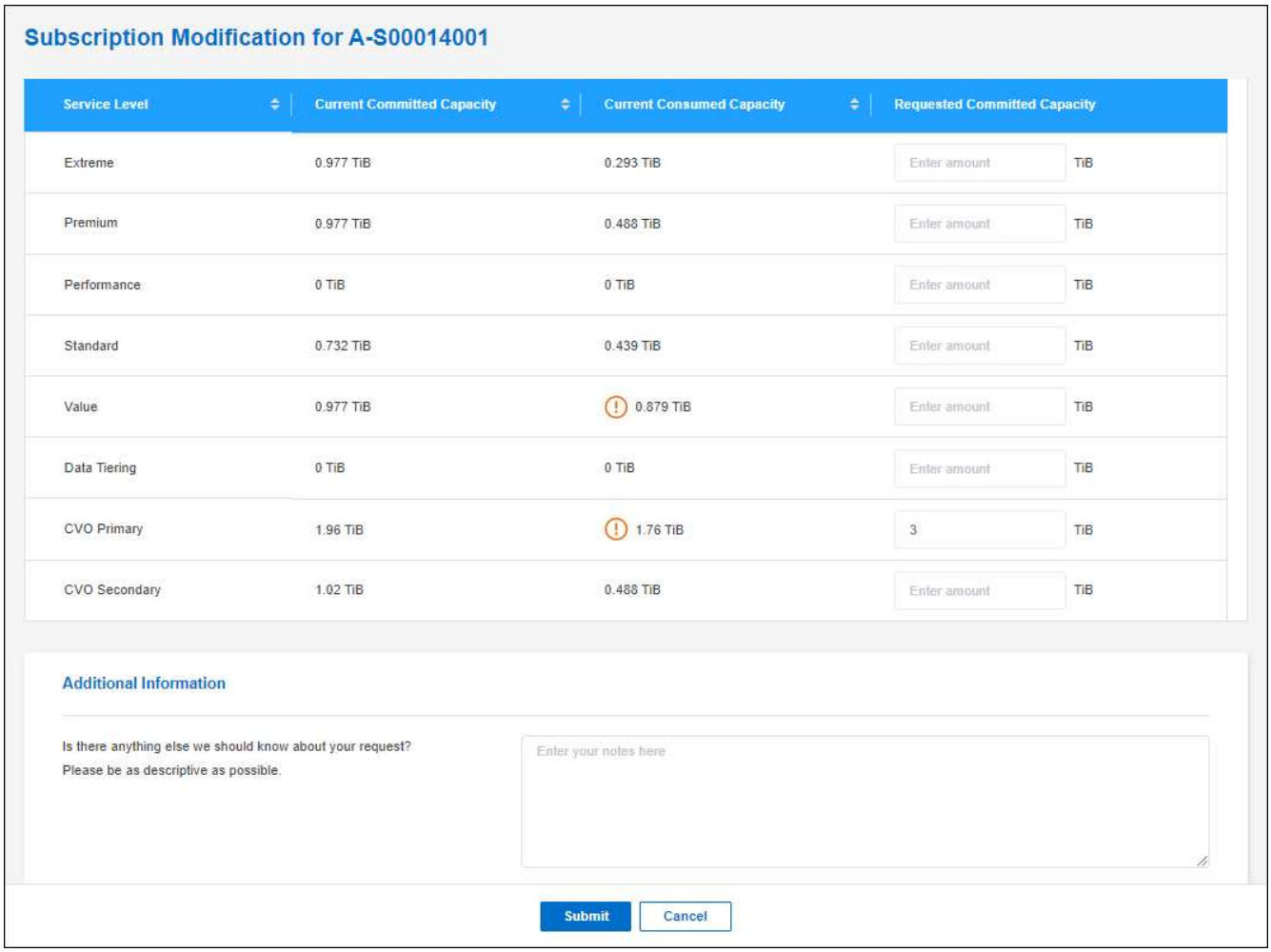
L'abbonamento è ora collegato all'organizzazione o all'account BlueXP e può essere selezionato quando si crea un ambiente di lavoro Cloud Volumes ONTAP.

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 **Iscrizioni 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 desideri 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'organizzazione o all'account BlueXP e non è più disponibile per la selezione durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP.

Gestisci la licenza basata su nodi per Cloud Volumes ONTAP

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):

- BYOL (Bring Your Own License) acquistato 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.

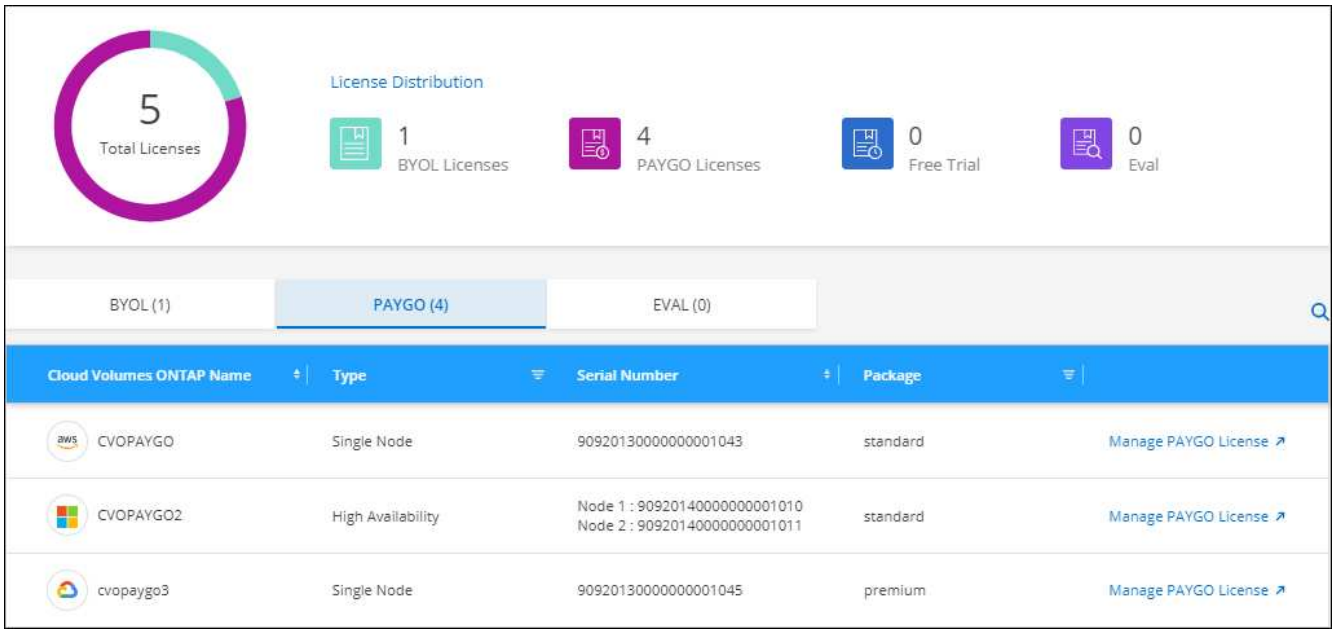
"Scopri di più sulle licenze Cloud Volumes ONTAP".

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. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Fare clic su **PAYGO**.
6. Visualizza i dettagli nella tabella di ciascuna licenza PAYGO.



7. 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.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

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. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Fare clic su **non assegnato**.
6. Fare clic su **Aggiungi licenze non assegnate**.
7. 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.

8. 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:

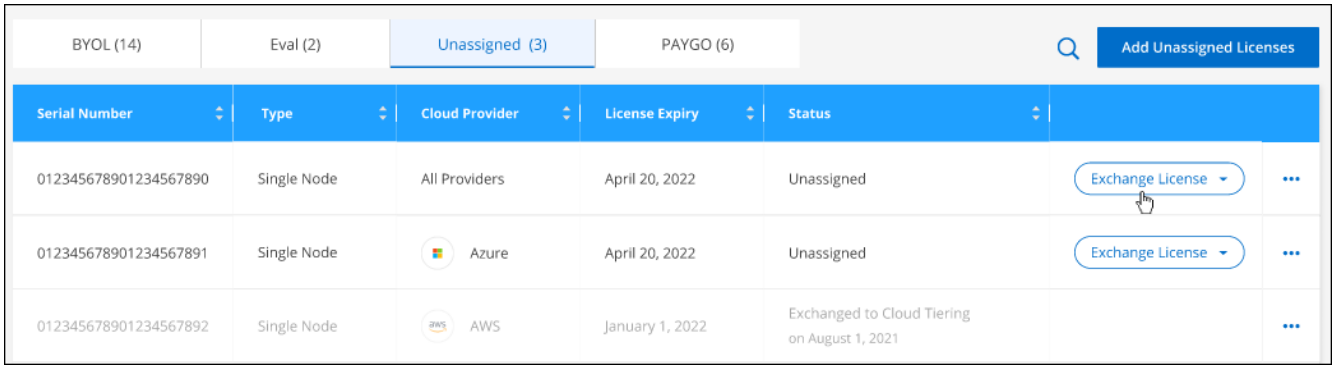
- La licenza per una coppia ha Cloud Volumes ONTAP viene convertita in una licenza diretta da 51 TiB
- La licenza per un singolo nodo Cloud Volumes ONTAP viene convertita in una licenza diretta 32 TiB

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

"Visualizzare la procedura dettagliata per lo scambio di licenze basate su nodi."

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Fare clic su **non assegnato**.
6. Fare clic su **Exchange License**.



7. Selezionare il servizio con cui si desidera scambiare la licenza.
8. Se richiesto, selezionare una licenza aggiuntiva per la coppia ha.
9. 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

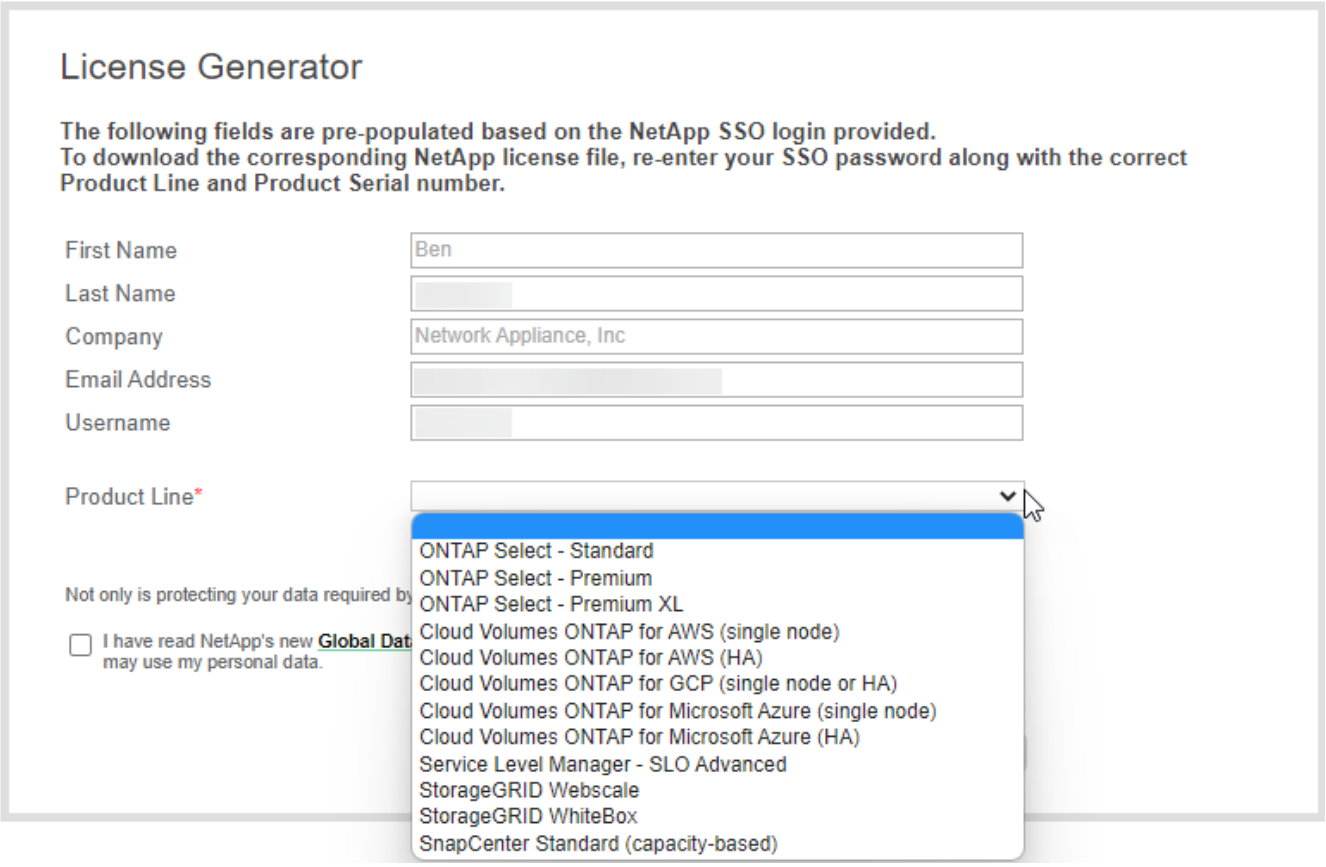
Nella maggior parte dei casi, BlueXP può ottenere automaticamente il file di licenza utilizzando l'account

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 rinnovi 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 la connessione Internet sicura, puoi ottenere il file autonomamente e caricarlo manualmente su BlueXP.

Fasi

1. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.

6. Fare clic sul menu delle azioni accanto alla licenza di sistema e selezionare **Aggiorna licenza**.
7. Caricare il file di licenza (o i file se si dispone di una coppia ha).
8. 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. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
6. Fare clic su **Add Capacity License**.
7. Inserire il numero di serie o caricare il file di licenza (o i file se si dispone di una coppia ha).
8. 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. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
6. Fare clic sul menu delle azioni accanto alla licenza di capacità e selezionare **Aggiorna licenza**.
7. Caricare il file di licenza (o i file se si dispone di una coppia ha).
8. 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. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP, selezionare **Visualizza**.
4. Selezionare **licenze basate su nodo** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli di un sistema Cloud Volumes ONTAP.
6. Fare clic sul menu delle azioni accanto alla licenza di capacità e selezionare **Remove License** (Rimuovi licenza).
7. Fare clic su **Rimuovi**.

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".

Link correlati

collegamento: "Fine della disponibilità delle licenze basate su nodi" "Converti le licenze basate su nodi in base alla capacità"

Amministrazione di volumi e LUN

Creare un FlexVol volume su un sistema Cloud Volumes ONTAP

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 ONTAP System Manager o dall'interfaccia a riga di comando di ONTAP.
- Se si desidera utilizzare CIFS in AWS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, fare riferimento alla "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.

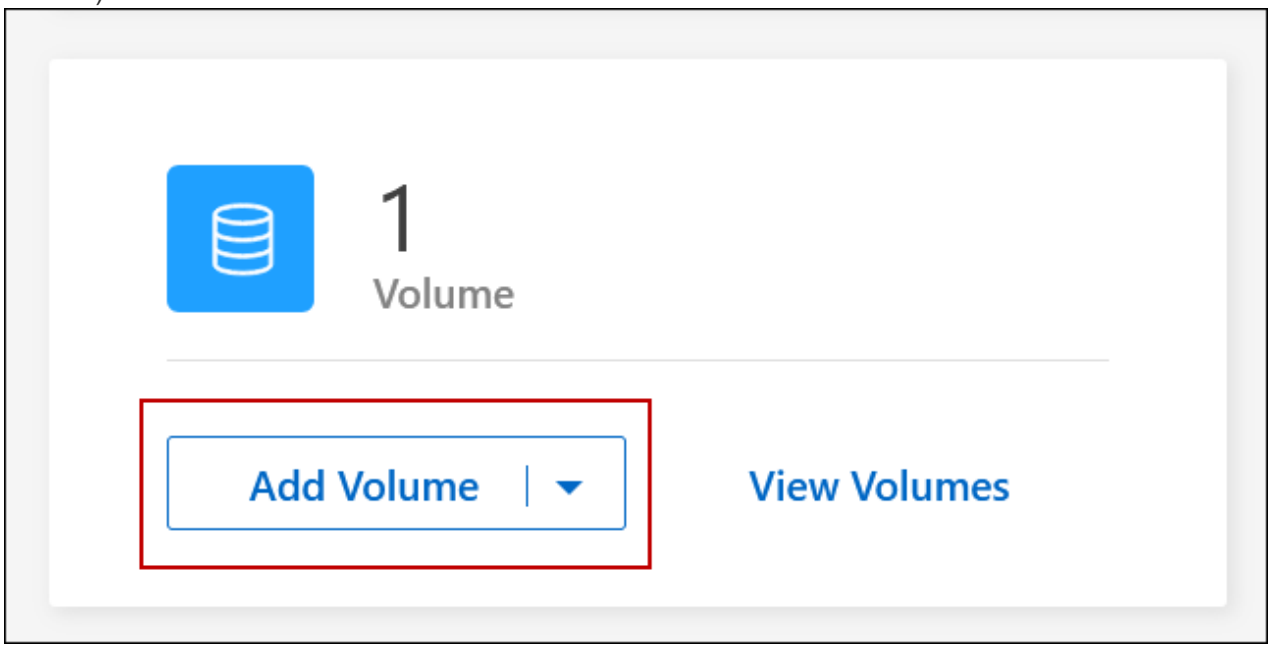
Fasi

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.

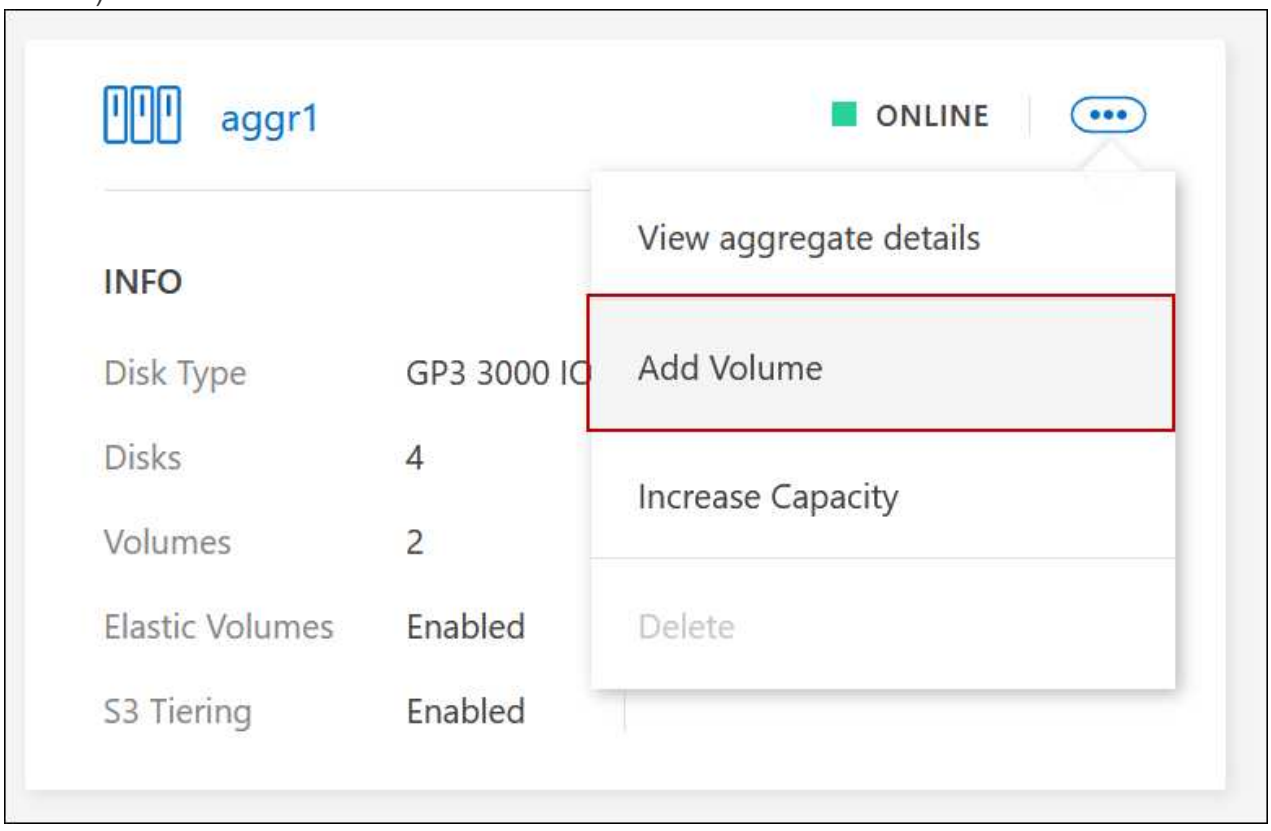
Qualsiasi aggregato

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. Per ulteriori informazioni, fare riferimento alla "Documenti sull'automazione BlueXP" .

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

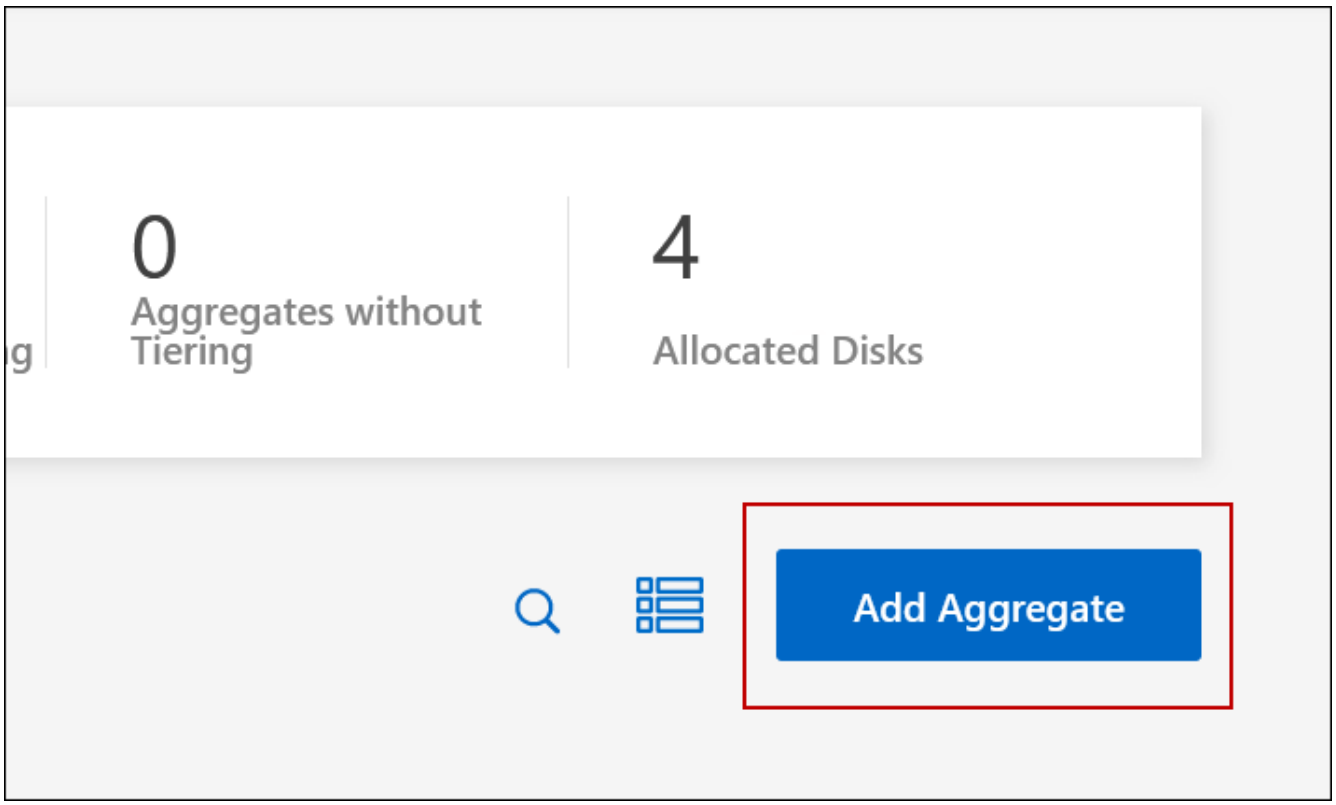
BlueXP crea il volume sul sistema Cloud Volumes ONTAP.

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.

Per applicare quote ai volumi, è necessario utilizzare ONTAP System Manager o l'interfaccia a riga di comando di ONTAP. 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 su sistemi Cloud Volumes ONTAP

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

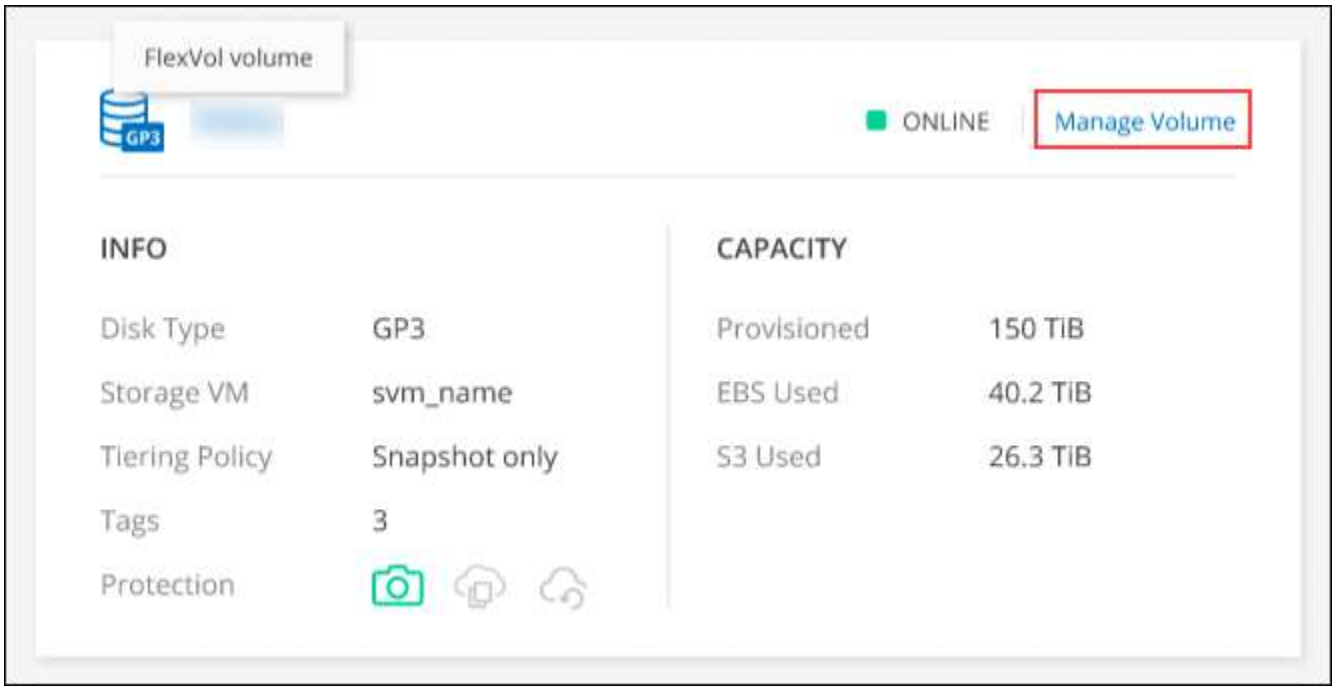
Puoi gestire i volumi nella vista standard di BlueXP o tramite ONTAP System Manager incluso in BlueXP per la gestione avanzata dei volumi. La visualizzazione standard fornisce un insieme limitato di opzioni per modificare i volumi. System Manager offre un livello di gestione avanzato, come cloning, ridimensionamento, modifica delle impostazioni per anti-ransomware, analytics, protezione e monitoraggio delle attività e spostamento dei volumi tra Tier. Per informazioni, fare riferimento alla "Amministrare Cloud Volumes ONTAP utilizzando Gestione di sistema".

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 su FlexClone Volumes, fare riferimento alla "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 necessari criteri Snapshot personalizzati, è possibile crearli utilizzando Gestione sistema di ONTAP.
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.

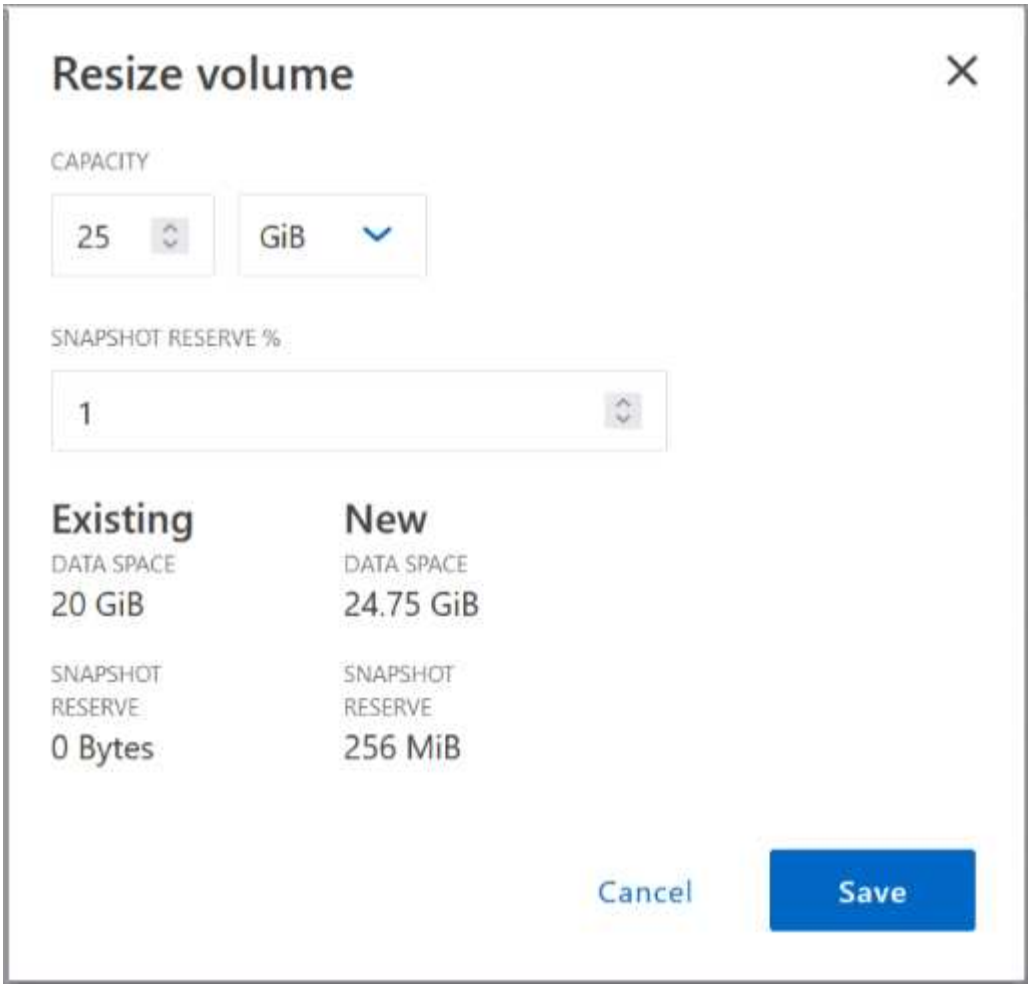
Ridimensionare un volume

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 è necessario ridimensionare il volume, è possibile farlo da Gestione di sistema di ONTAP in BlueXP .

Fasi

1. Fare clic sulla vista Gestione sistema per ridimensionare un volume tramite Gestione sistema di ONTAP. Fare riferimento alla "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. "Note di rilascio di Cloud Volumes ONTAP"Per ulteriori informazioni, consultare la sezione.

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.

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

Fasi

1. Utilizza ONTAP System Manager o la CLI di ONTAP per spostare i volumi nell'aggregato.

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

Per istruzioni, fare riferimento alla "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.

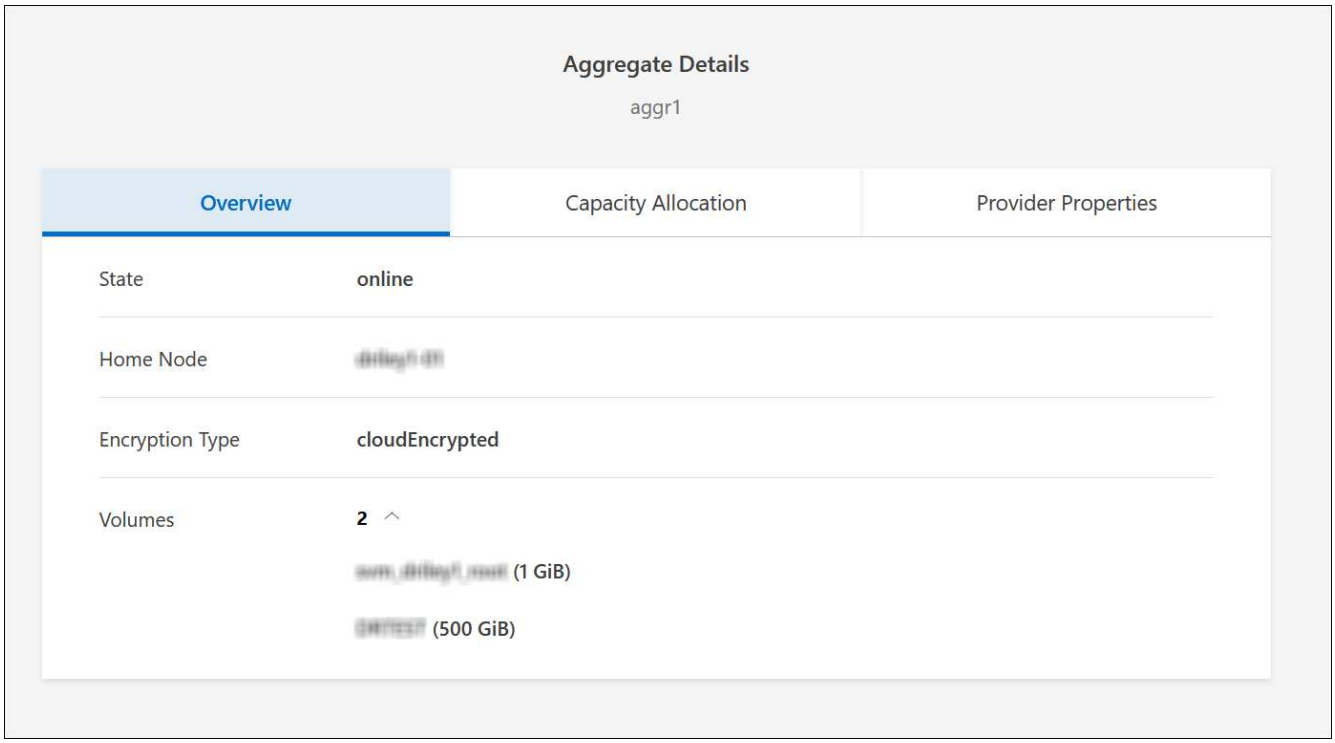
2. Identificare uno o più volumi da spostare fuori dall'aggregato:

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

   b. Passare alla sezione di aggregazione desiderata, quindi fare clic sul pulsante **… (Icona ellissi) > 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 informazioni, fare riferimento alla 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 informazioni, fare riferimento alla 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 informazioni, fare riferimento alla 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 informazioni, fare riferimento alla "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 informazioni, fare riferimento alla "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, fare riferimento alla "Guida rapida per il disaster recovery dei volumi di ONTAP 9".

5. Eliminare il volume originale.

   Per informazioni, fare riferimento alla "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.

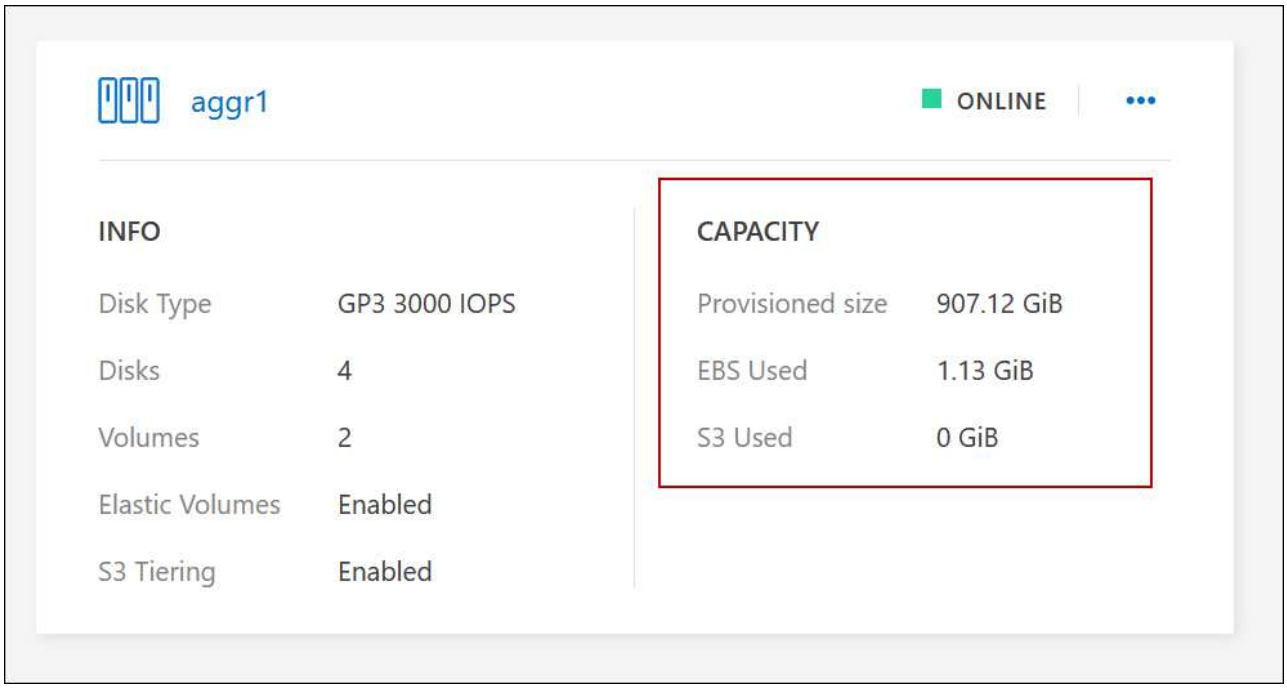
A proposito di questa attività

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. Passare alla sezione di aggregazione desiderata, quindi fare clic sul pulsante **… (Icona ellissi) > 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 ellissi) > 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 informazioni, fare riferimento alla "Creazione di aggregati".
4. Utilizza ONTAP System Manager o la CLI di ONTAP per spostare i volumi nell'aggregato.
5. Nella maggior parte dei casi, è possibile utilizzare System Manager per spostare i volumi.

   Per istruzioni, fare riferimento alla "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:

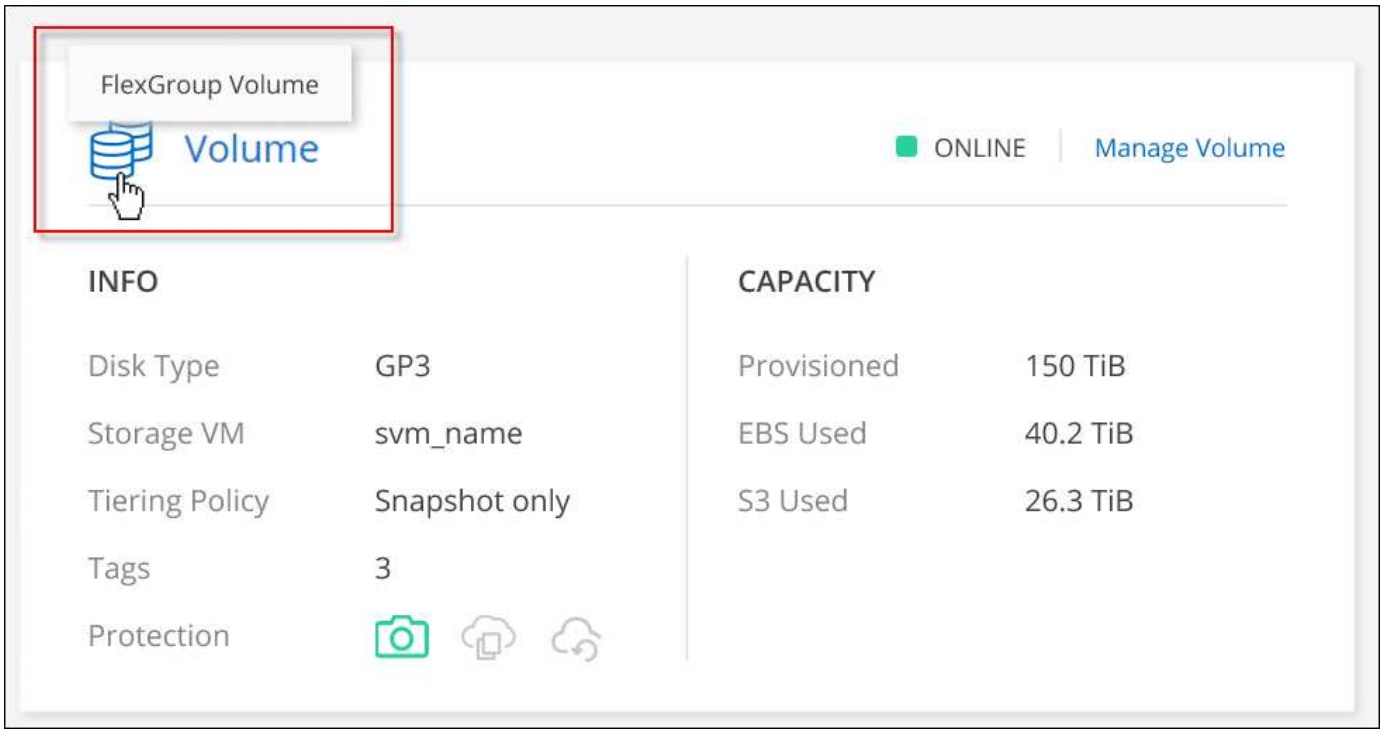
- Il volume è un clone.
- Il volume è il padre di un clone.
- L'aggregato di origine o di destinazione dispone di un disco HDD (st1) ottimizzato per il throughput singolo.
- Uno degli aggregati utilizza uno schema di denominazione precedente per gli oggetti. Entrambi gli aggregati devono utilizzare lo 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

Puoi vedere i volumi FlexGroup creati tramite ONTAP System Manager o la CLI ONTAP direttamente attraverso la scheda Volumes all'interno 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.

Esegui il tiering dei dati Cloud Volumes ONTAP inattivi in uno 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 di alto livello, fare riferimento alla "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 che esegue la versione più recente, è possibile 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

In un aggregato, il tiering dei dati deve essere abilitato per poter essere utilizzato 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.

- "Eseguire il tiering dei dati dai volumi di lettura/scrittura"
- "Eseguire il tiering dei dati dai volumi di data Protection"

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 crea il sistema, a condizione che non vi siano problemi di connettività o permessi. Dopodiché, sarà sufficiente abilitare 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

- La suddivisione in livelli dei dati è supportata 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 suddividere i dati in livelli per l'archiviazione di oggetti quando si utilizzano HDD Throughput Optimized (st1).

- I dati inattivi vengono suddivisi in bucket Amazon S3. Il suddivisione in bucket di altri provider non è supportata.

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.
- I dati inattivi sono suddivisi in livelli in Microsoft Azure Blob. Il suddivisione in livelli in altri provider non è supportata.

Supporto in Google Cloud

- La suddivisione in livelli dei dati è supportata 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.
- I dati inattivi sono gestiti tramite livelli di Google Cloud Storage. Il livello di altri provider non è supportato.

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, fare riferimento alla "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, fare riferimento a "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",
```

Il ruolo personalizzato include le autorizzazioni per impostazione predefinita. "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 sopra elencati non sono stati implementati prima della creazione del sistema, sarà necessario abilitare manualmente il tiering tramite l'API o ONTAP 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.

Verifica 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**

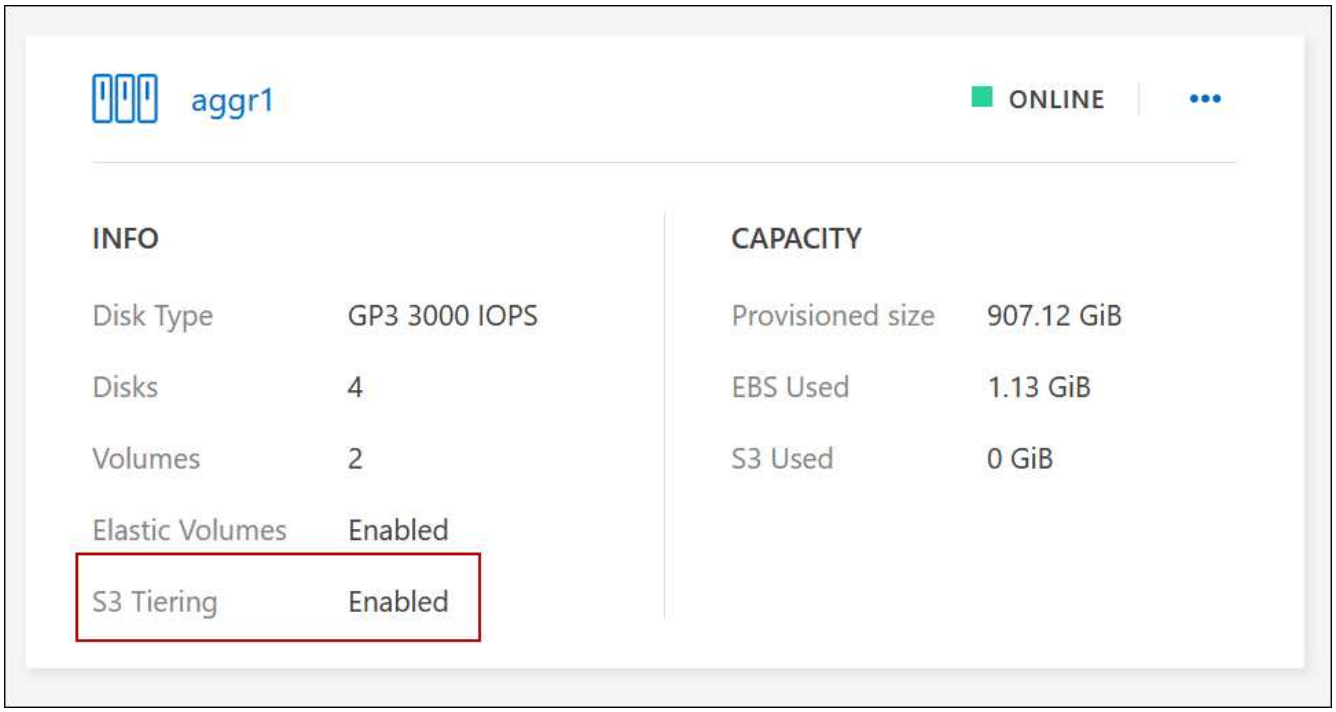
  Se abiliti il tiering dei dati su un nuovo volume, non dovrai preoccuparti di abilitare il tiering dei dati su un aggregato. BlueXP crea il volume su un aggregato esistente che ha attivato il tiering oppure crea un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering dei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

- **Volumi esistenti**

  Per abilitare il tiering dei dati su un volume esistente, assicurati che sia abilitato nell'aggregato sottostante. Se il tiering dei dati non è abilitato nell'aggregato esistente, sarà necessario utilizzare Gestione di sistema di ONTAP per collegare 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 Gestione di sistema di ONTAP, fare clic su **archiviazione > livelli**.
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.

Eseguire il 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

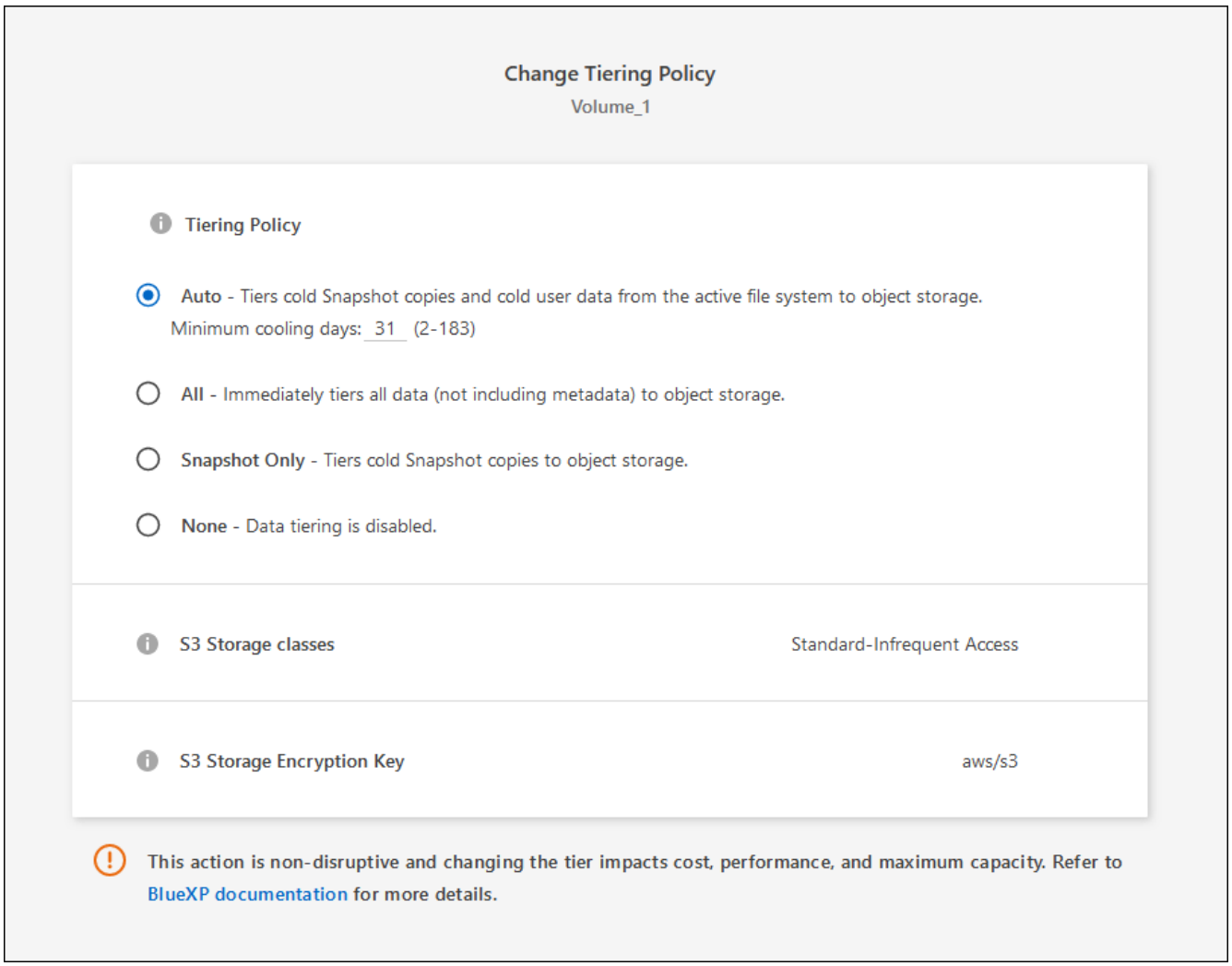
1. Nella scheda Volumes (volumi) dell'ambiente di lavoro, creare un nuovo volume o modificare il livello di un volume esistente:

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, fare riferimento a "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.

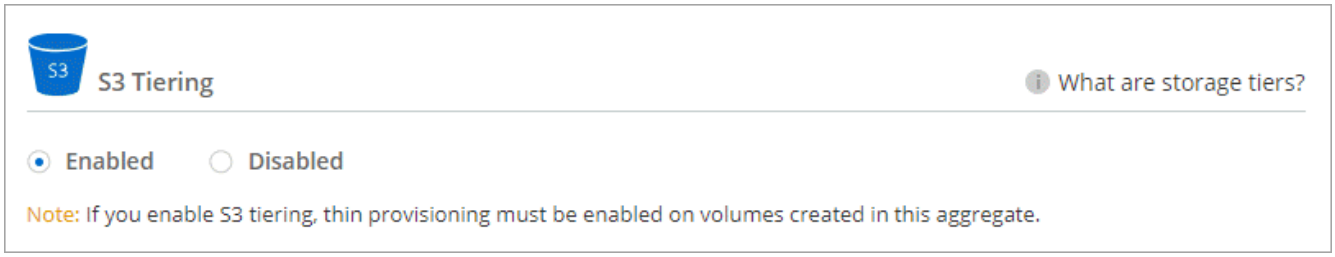
Eseguire il tiering dei dati dai volumi di data Protection

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 informazioni sulla replica dei dati, fare riferimento a "Replica dei dati da e verso il cloud".

Modificare la classe di archiviazione 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 archiviazione supportate, fare riferimento a "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.

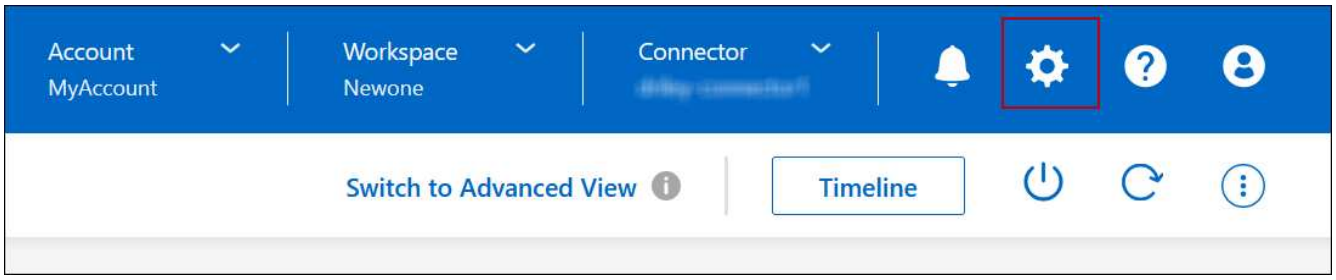
Ad esempio, è possibile scegliere meno del 10% di spazio libero per assicurarsi di utilizzare la capacità acquistata. BlueXP può quindi acquistare dischi aggiuntivi quando è richiesta capacità aggiuntiva (fino a raggiungere il limite di dischi per l'aggregato).

Se lo spazio non è sufficiente, Cloud Volumes ONTAP non è in grado di spostare i dati e potrebbe riscontrare un peggioramento delle prestazioni. 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).

Modificare il 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 utilizzando ONTAP CLI e API.

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.

Rimuovere una benna S3 durante la messa fuori servizio di un ambiente di lavoro

Quando si decommissiona l'ambiente, è possibile eliminare un bucket S3 con il tiering dei dati da un ambiente di lavoro Cloud Volumes ONTAP.

È possibile eliminare il bucket S3 solo se:

- L'ambiente di lavoro Cloud Volume ONTAP viene eliminato da BlueXP .
- Tutti gli oggetti vengono eliminati dal bucket e il bucket S3 è vuoto.

Quando si decommissiona un ambiente di lavoro Cloud Volumes ONTAP, il bucket S3 creato per l'ambiente non viene eliminato automaticamente. Ma rimane in uno stato orfano per prevenire qualsiasi perdita accidentale di dati. È possibile eliminare gli oggetti nel bucket, quindi rimuovere il bucket S3 stesso o conservarlo per un utilizzo successivo. Fare riferimento alla "ONTAP CLI: Eliminazione bucket object-store-server vserver".

Connettersi a un LUN su Cloud Volumes ONTAP dal sistema 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 ONTAP System Manager o dall'interfaccia a riga di comando di ONTAP.

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 i volumi FlexCache su un sistema Cloud Volumes ONTAP

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"

Utilizzare FlexCache quando l'origine è crittografata

Quando si configura FlexCache su un sistema Cloud Volumes ONTAP in cui il volume di origine è crittografato, sono necessari ulteriori passaggi per garantire che il volume FlexCache possa accedere correttamente e memorizzare nella cache i dati crittografati.

Prima di iniziare

1. **Impostazione crittografia**: Verificare che il volume di origine sia completamente crittografato e operativo. Per i sistemi Cloud Volumes ONTAP, ciò implica l'integrazione con servizi di gestione delle chiavi specifici del cloud.

Per AWS, questo generalmente significa utilizzare AWS Key Management Service (KMS). Per informazioni, fare riferimento alla "Gestione delle chiavi con AWS Key Management Service".

Per Azure, è necessario configurare Azure Key Vault per NetApp Volume Encryption (NVE). Per informazioni, fare riferimento alla "Gestisci le chiavi con Azure Key Vault".

Per Google Cloud, si tratta di Google Cloud Key Management Service. Per informazioni, fare riferimento alla "Gestisci le chiavi con il servizio Cloud Key Management di Google".

1. **Servizi di gestione delle chiavi**: Prima di creare un volume FlexCache, verificare che i servizi di gestione delle chiavi siano configurati correttamente sul sistema Cloud Volumes ONTAP. Questa configurazione è essenziale per il volume FlexCache per decrittografare i dati dal volume di origine.
2. **Licenze**: Verificare che sul sistema Cloud Volumes ONTAP sia disponibile e attivata una licenza FlexCache valida.
3. **Versione ONTAP**: Verificare che la versione ONTAP del sistema Cloud Volumes ONTAP supporti FlexCache con volumi crittografati. Per ulteriori informazioni, fare riferimento alla matrice di compatibilità o all'ultima "Note di rilascio di ONTAP" versione.
4. **Configurazione di rete**: Assicurarsi che la configurazione di rete consenta una comunicazione senza interruzioni tra il volume di origine e il volume FlexCache. Ciò include routing e risoluzione DNS corretti in

un ambiente cloud.

Fasi

Creazione di un volume FlexCache sul sistema Cloud Volumes ONTAP con un volume di origine crittografato. Per i passaggi dettagliati e ulteriori considerazioni, fare riferimento alle seguenti sezioni:

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

Amministrazione degli aggregati

Crea un aggregato per i sistemi Cloud Volumes ONTAP

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.

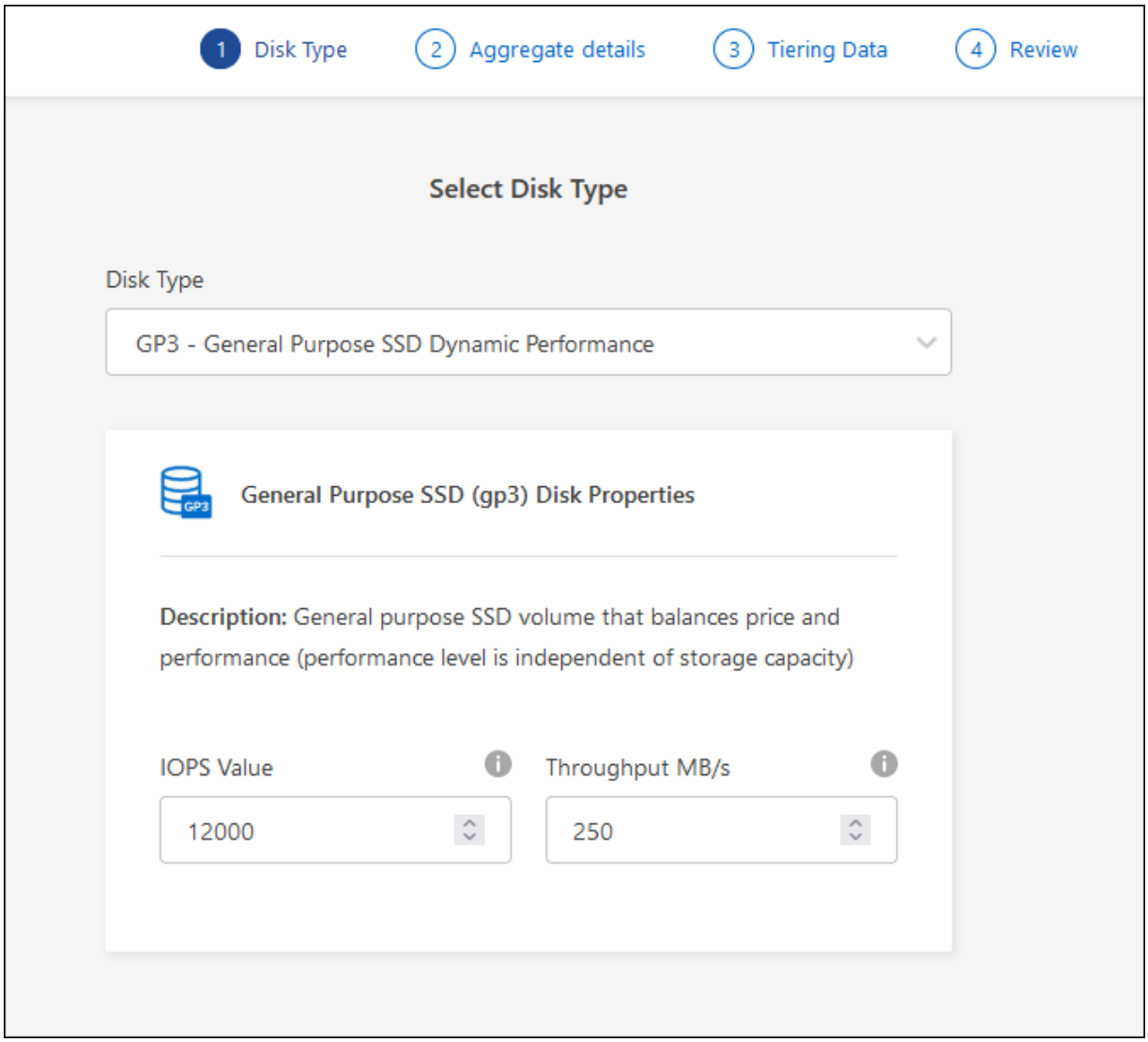
> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da BlueXP. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti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

Gestione degli aggregati per i cluster Cloud Volumes ONTAP

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

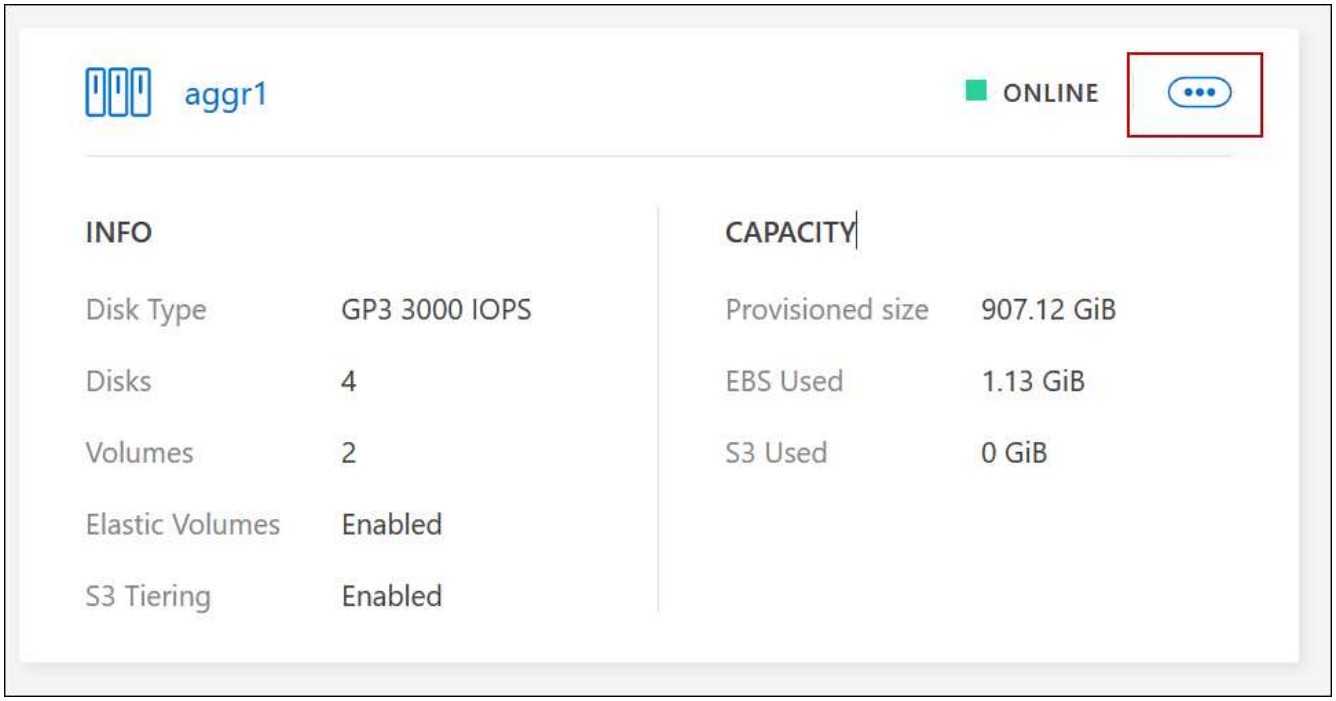
Se si desidera eliminare un aggregato, è necessario prima eliminare i volumi nell'aggregato.

A proposito di questa attività

In caso di esaurimento dello spazio di un aggregato, puoi spostare i volumi in un altro aggregato utilizzando ONTAP 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 ellissi)**.



5. Gestisci i tuoi aggregati:

Attività	Azione
Visualizzare informazioni su un aggregato	Nel menu … (icona ellissi), fare clic su **Visualizza dettagli aggregati**.

Attività	Azione
Creare un volume su un aggregato specifico	Nel menu … (icona ellissi), fare clic su **Aggiungi volume**.
Aggiungere dischi a un aggregato	a. Nel menu … (icona ellissi), 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. Nel menu … (icona ellissi), 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 un riquadro aggregato che non contiene volumi fare clic sul pulsante **… (Icona ellissi) > Elimina**. b. Fare nuovamente clic su **Delete** per confermare.

Gestire la capacità aggregata Cloud Volumes ONTAP su un connettore

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

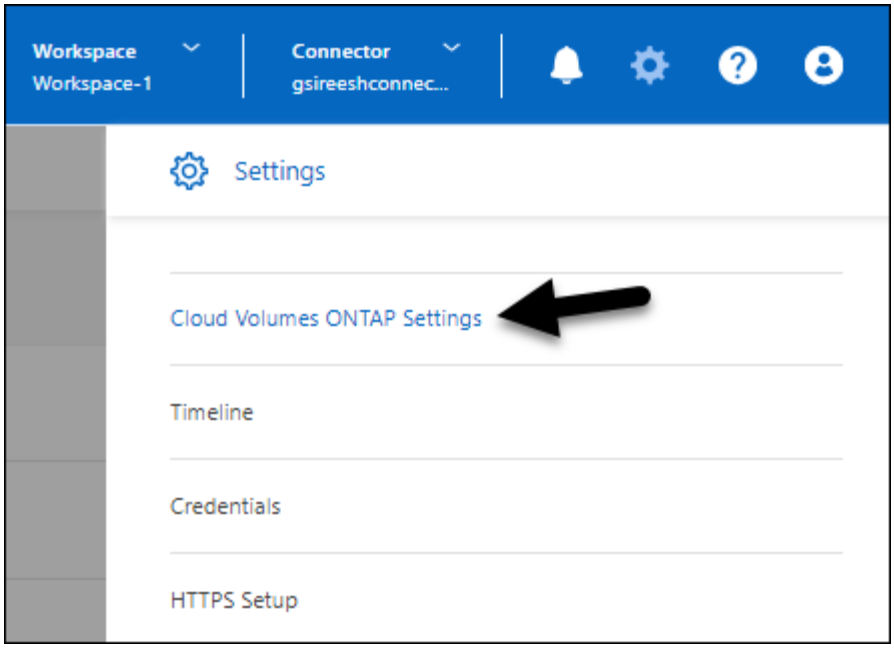
Queste impostazioni influiscono su tutti i sistemi Cloud Volumes ONTAP gestiti da un connettore. Se si dispone di un altro connettore, è possibile configurarlo in modo diverso.

Autorizzazioni richieste

Per modificare le impostazioni di Cloud Volumes ONTAP, è necessario disporre dell'organizzazione BlueXP o dell'account admin Privileges.

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

Fare riferimento a "Gestione automatica della capacità" per ulteriori informazioni su come 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

Gestione delle macchine virtuali di storage per Cloud Volumes ONTAP

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.

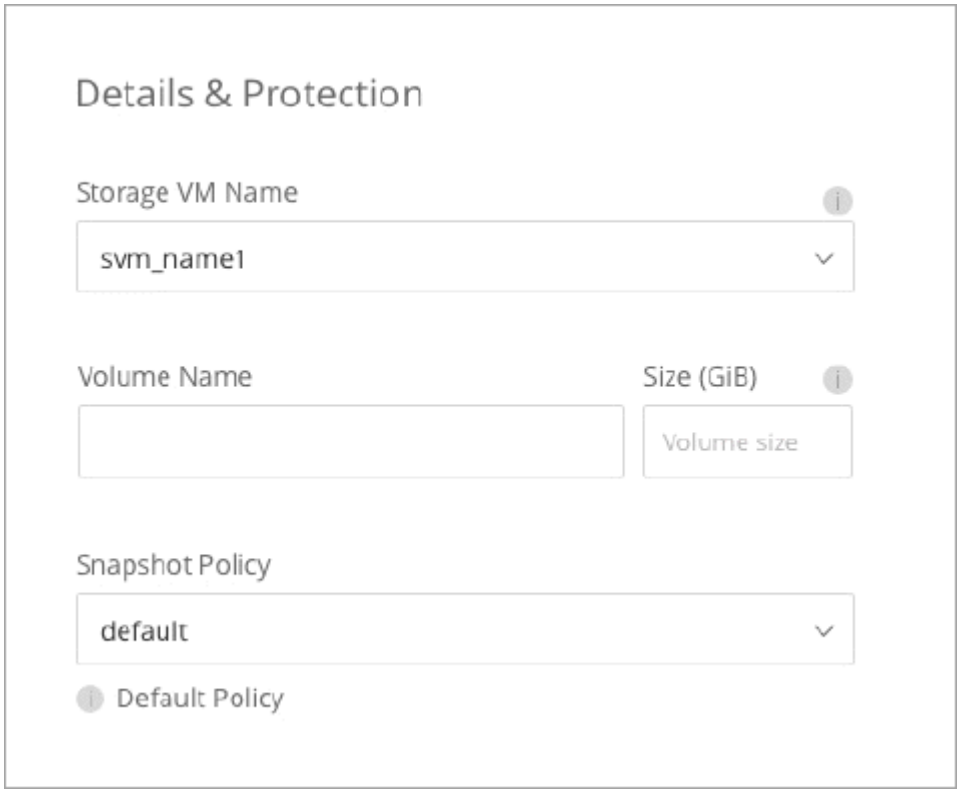
Numero di VM storage supportate

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.

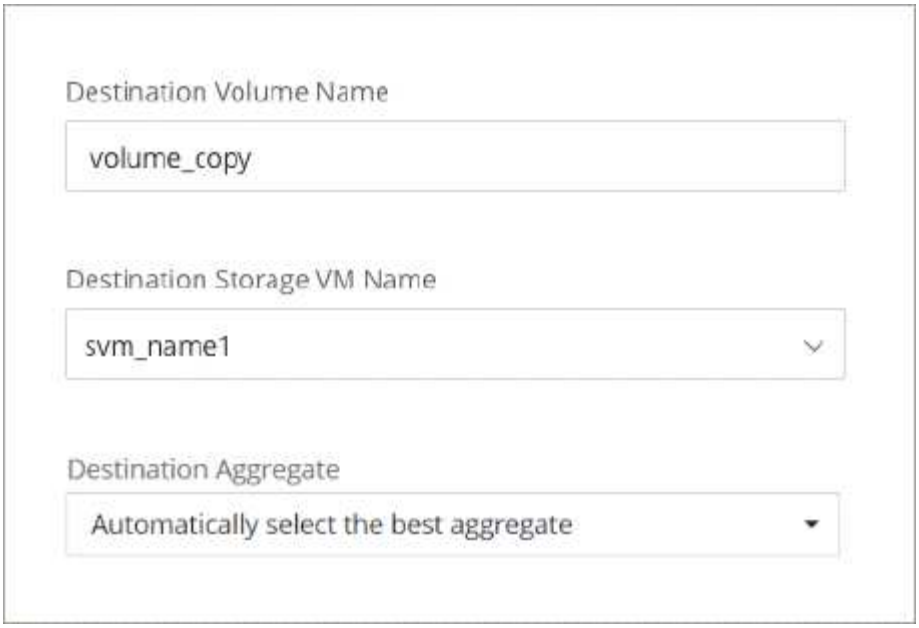
Lavorare con più macchine virtuali storage

BlueXP supporta eventuali macchine virtuali storage aggiuntive create da ONTAP System Manager o dalla CLI di ONTAP.

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 ONTAP System Manager, l'interfaccia a riga di comando o l'API di ONTAP, è possibile modificare il nome della macchina virtuale di storage se si utilizzano rigorosi standard di denominazione. Ad esempio, è possibile che il nome corrisponda a quello delle VM di storage per i cluster ONTAP.

Gestisci le macchine virtuali dello storage di distribuzione dei dati 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.

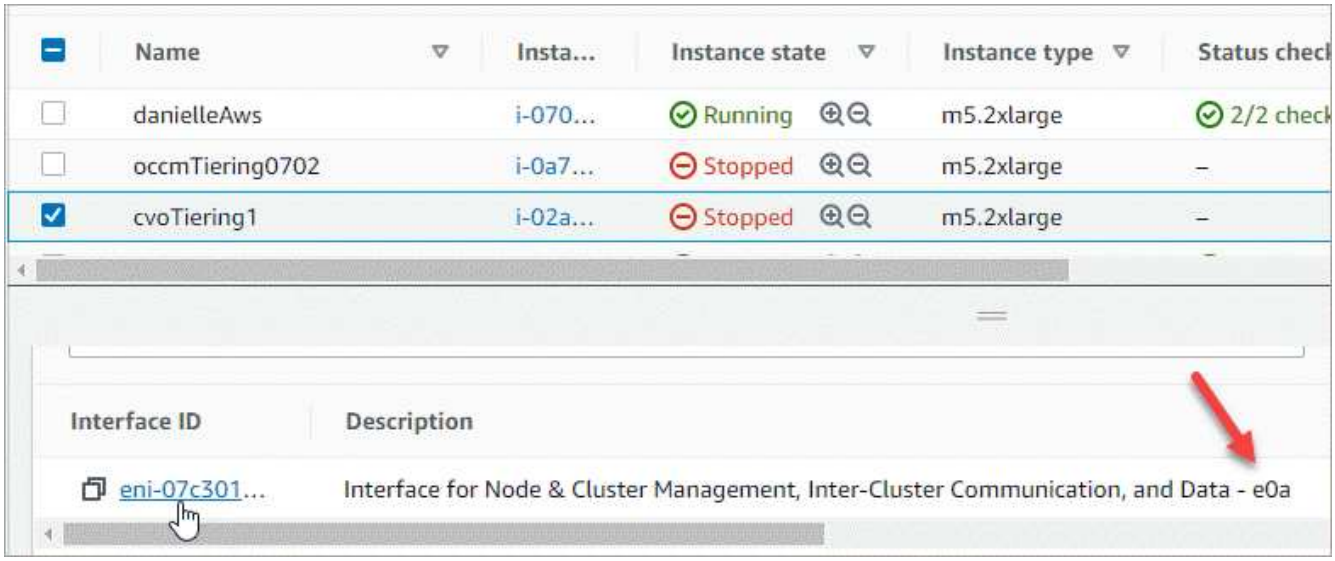
Si noti che una LIF di gestione opzionale per una VM di storage richiede un indirizzo IP privato su un sistema a nodo singolo e su una coppia ha in un singolo AZ. Questa LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

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 di ONTAP per Cloud Volumes ONTAP ed eseguire **network interface show** per confermare che ciascuno di questi indirizzi IP è 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
```

Gestisci le macchine virtuali dello storage di distribuzione dei dati 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*. Per impostazione predefinita, Cloud Volumes ONTAP è configurato con una macchina virtuale storage, ma è possibile creare macchine virtuali storage aggiuntive quando si esegue Cloud Volumes ONTAP in Azure.

Per creare e gestire macchine virtuali storage di altri data-serving in Azure è necessario utilizzare le API BlueXP . Ciò è dovuto al fatto che le API automatizzano il processo di creazione delle macchine virtuali storage e di configurazione delle interfacce di rete richieste. Nel creare le macchine virtuali storage, BlueXP configura i servizi LIF richiesti, così come una LIF iSCSI necessaria per le comunicazioni SMB/CIFS in uscita dalla macchina virtuale storage.

Per informazioni sull'esecuzione di chiamate API Cloud Volumes ONTAP, fare riferimento a "La prima chiamata API".

Numero di VM storage supportate

A partire da Cloud Volumes ONTAP 9,9.0, in base alla licenza in uso, sono supportate più macchine virtuali storage con configurazioni specifiche. Fare riferimento a "Note di rilascio di Cloud Volumes ONTAP" per verificare il numero supportato di macchine virtuali storage per la propria versione di Cloud Volumes ONTAP.

Tutte le versioni di Cloud Volumes ONTAP precedenti alla 9.9.0 supportano una VM di storage di distribuzione dati e una VM di storage di destinazione utilizzate 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

In base alla tua configurazione e al tipo di licenza, puoi creare più macchine virtuali storage su un sistema a nodo singolo o in una configurazione ha (High Availability) utilizzando le API BlueXP .

A proposito di questa attività

Quando crei Storage VM utilizzando le API, insieme alla configurazione delle interfacce di rete richieste, BlueXP modifica anche le `default-data-files` policy sulle macchine virtuali per lo storage dei dati rimuovendo i seguenti servizi dalla LIF dati NAS e aggiungendoli alla LIF dati iSCSI utilizzata per le connessioni di gestione in uscita:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Prima di iniziare

Il connettore richiede autorizzazioni specifiche per creare macchine virtuali storage per Cloud Volumes ONTAP. Le autorizzazioni richieste sono incluse in "Le policy fornite da NetApp".

Sistema a nodo singolo

Utilizza la seguente chiamata API per creare una VM storage su un sistema a nodo singolo.

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

Includere i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

Coppia HA

Utilizza la seguente chiamata API per creare una VM storage su una coppia ha:

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Includere i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Gestire le macchine virtuali di storage su sistemi a nodo singolo e coppie ha

Con le API di BlueXP , puoi rinominare ed eliminare le macchine virtuali storage sia in configurazioni a nodo singolo che in configurazioni ha.

Prima di iniziare

Il connettore richiede autorizzazioni specifiche per la gestione delle macchine virtuali storage per Cloud Volumes ONTAP. Le autorizzazioni richieste sono incluse in "Le policy fornite da NetApp".

Rinominare una VM di storage

Per rinominare una VM di storage, è necessario fornire i nomi della VM di storage esistente e della nuova VM di storage come parametri.

Fasi

- Utilizza la seguente chiamata API per rinominare una VM storage su un sistema a nodo singolo:

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  Includere i seguenti parametri nel corpo della richiesta:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Utilizza la seguente chiamata API per rinominare una VM storage su una coppia ha:

  ```
  PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
  ```

  Includere i seguenti parametri nel corpo della richiesta:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

Eliminare una VM di storage

In una configurazione ha o nodo singolo, puoi rimuovere una VM di storage se non ha volumi attivi.

Fasi

- Utilizza la seguente chiamata API per eliminare una VM storage su un sistema a nodo singolo:

  `DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}`

- Utilizza la seguente chiamata API per eliminare una VM storage su una coppia ha:

  `DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}`

Informazioni correlate

- "Prepararsi a utilizzare l'API"
- "Flussi di lavoro Cloud Volumes ONTAP"
- "Ottieni gli identificatori richiesti"
- "Utilizzare le API REST BlueXP"

Gestisci le macchine virtuali dello storage di 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.

Per creare e gestire macchine virtuali storage aggiuntive di distribuzione di dati in Google Cloud, è necessario utilizzare le API BlueXP . Ciò è dovuto al fatto che le API automatizzano il processo di creazione delle macchine virtuali storage e di configurazione delle interfacce di rete richieste. Nel creare le macchine virtuali storage, BlueXP configura i servizi LIF richiesti, così come una LIF iSCSI necessaria per le comunicazioni SMB/CIFS in uscita dalla macchina virtuale storage.

Per informazioni sull'esecuzione di chiamate API Cloud Volumes ONTAP, fare riferimento a "La prima chiamata API".

Numero di VM storage supportate

A partire da Cloud Volumes ONTAP 9,11.1, in base alla licenza in uso, sono supportate più macchine virtuali storage con configurazioni specifiche. Fare riferimento a "Note di rilascio di Cloud Volumes ONTAP" per verificare il numero supportato di macchine virtuali storage per la propria versione di Cloud Volumes ONTAP.

Tutte le versioni di Cloud Volumes ONTAP precedenti alla 9.11.1 supportano una VM di storage di distribuzione

dati e una VM di storage di destinazione utilizzate 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

In base alla tua configurazione e al tipo di licenza, puoi creare più macchine virtuali storage su un sistema a nodo singolo o in una configurazione ha (High Availability) utilizzando le API BlueXP .

A proposito di questa attività

Quando crei Storage VM utilizzando le API, insieme alla configurazione delle interfacce di rete richieste, BlueXP modifica anche le `default-data-files` policy sulle macchine virtuali per lo storage dei dati rimuovendo i seguenti servizi dalla LIF dati NAS e aggiungendoli alla LIF dati iSCSI utilizzata per le connessioni di gestione in uscita:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Prima di iniziare

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

Sistema a nodo singolo

Utilizza la seguente chiamata API per creare una VM storage su un sistema a nodo singolo.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Includere i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Coppia HA

Utilizza la seguente chiamata API per creare una VM storage su una coppia ha:

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

Includere i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

Gestire le VM di storage

Con le API di BlueXP , puoi rinominare ed eliminare le macchine virtuali storage sia in configurazioni a nodo singolo che in configurazioni ha.

Prima di iniziare

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

Rinominare una VM di storage

Per rinominare una VM di storage, è necessario fornire i nomi della VM di storage esistente e della nuova VM di storage come parametri.

Fasi

- Utilizza la seguente chiamata API per rinominare una VM storage su un sistema a nodo singolo:

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  Includere i seguenti parametri nel corpo della richiesta:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Utilizza la seguente chiamata API per rinominare una VM storage su una coppia ha:

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  Includere i seguenti parametri nel corpo della richiesta:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

Eliminare una VM di storage

In una configurazione ha o nodo singolo, puoi rimuovere una VM di storage se non ha volumi attivi.

Fasi

- Utilizza la seguente chiamata API per eliminare una VM storage su un sistema a nodo singolo:

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Utilizza la seguente chiamata API per eliminare una VM storage su una coppia ha:

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

Informazioni correlate

- "Prepararsi a utilizzare l'API"
- "Flussi di lavoro Cloud Volumes ONTAP"
- "Ottieni gli identificatori richiesti"
- "Utilizzare le API REST BlueXP"

Configurare il disaster recovery delle Storage VM per Cloud Volumes ONTAP

BlueXP non offre supporto per la configurazione o l'orchestrazione per il disaster recovery delle VM di storage (SVM). Per eseguire queste attività, utilizzare ONTAP System Manager o l'interfaccia a riga di comando di ONTAP.

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 dell'interfaccia CLI di ONTAP.

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

Sicurezza e crittografia dei dati

Crittografa i volumi su Cloud Volumes ONTAP con le soluzioni per la 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.

] endif::aws[] ifdef::azure[] endif::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] endif::aws[] endif::aws[] endif::aws[] ifdef::azure[] endif::azure[

Gestisci le chiavi di crittografia Cloud Volumes ONTAP con il servizio di gestione delle chiavi AWS

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 di crittografia Cloud Volumes ONTAP con il vault delle chiavi di Azure

È possibile utilizzare Azure Key Vault (AKV) per proteggere le chiavi di crittografia ONTAP in un'applicazione distribuita da Azure. Fare riferimento alla "Documentazione

Microsoft".

AKV può essere utilizzato per proteggere le chiavi NetApp Volume Encryption (NVE) solo per le SVM di dati. Per ulteriori informazioni, fare riferimento alla "Documentazione ONTAP".

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.
- I nodi Cloud Volumes ONTAP eseguono il polling di AKV ogni 15 minuti per verificare l'accessibilità e la disponibilità delle chiavi. Questo periodo di polling non è configurabile e, dopo quattro errori consecutivi nel tentativo di polling (per un totale di 1 ora), i volumi vengono messi offline.

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.

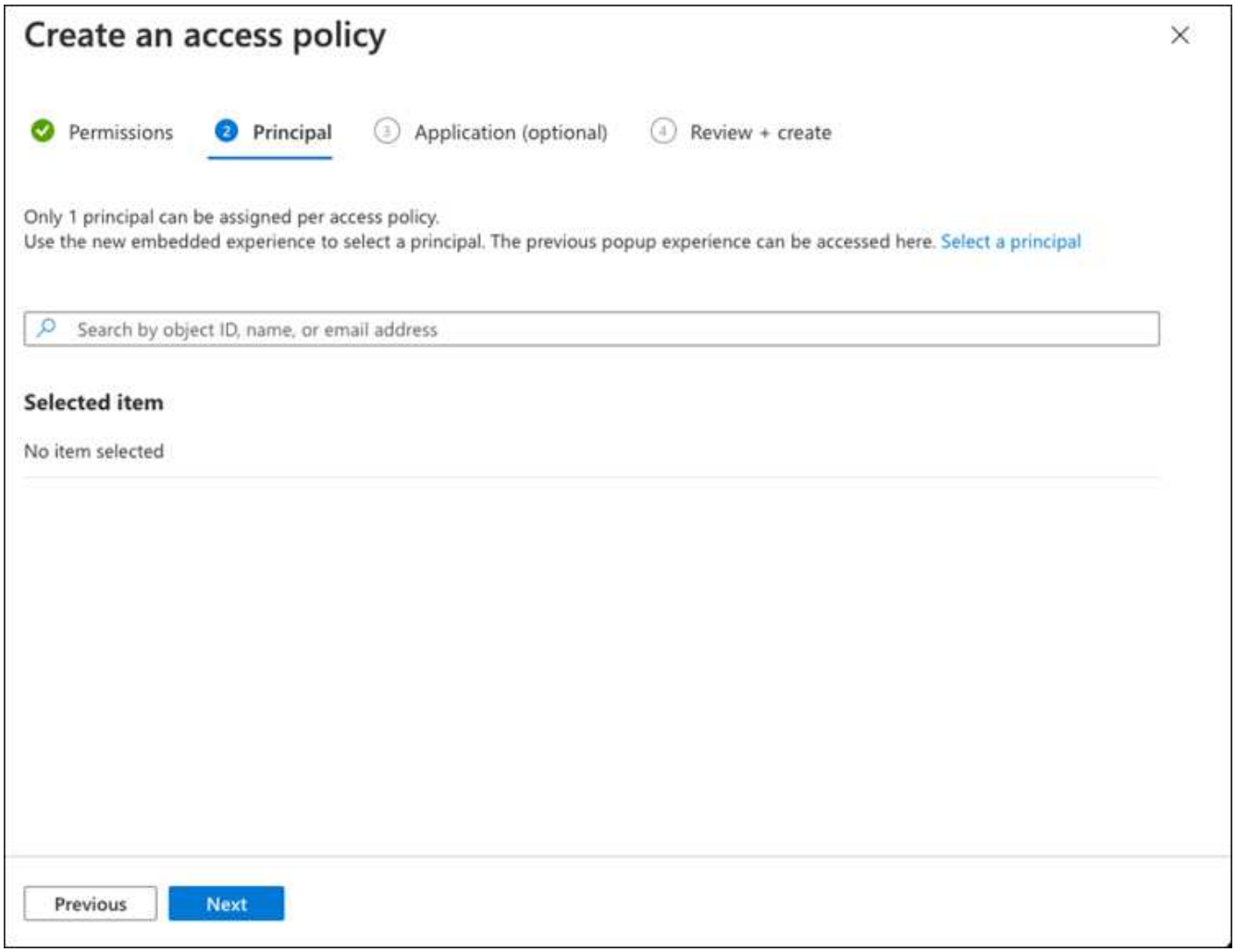
Creare un vault Azure Key

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
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
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

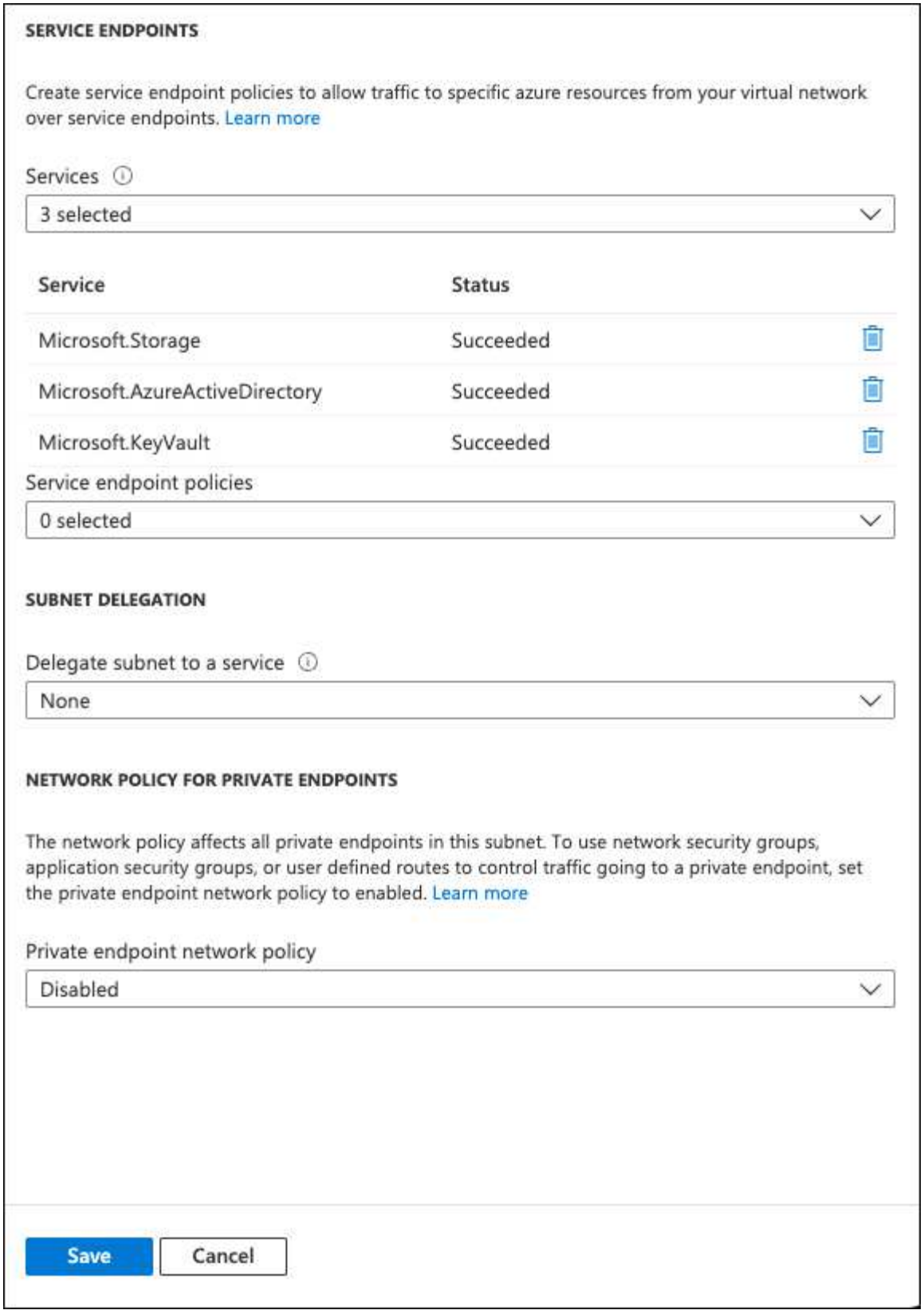
1. Nel menu del vault delle chiavi creato per Cloud Volumes ONTAP, selezionare l'opzione **chiavi**.
2. Selezionare **genera/importa** per creare una nuova chiave.
3. Lasciare l'opzione predefinita impostata su **genera**.
4. Fornire le seguenti informazioni:

- 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` , la SVM non riesce a raggiungere il servizio Azure Key Vault con tutta la connettività e le autorizzazioni necessarie. Assicurarsi che i criteri di rete e il routing di Azure non impediscano alla rete virtuale privata di raggiungere l'endpoint pubblico di Azure Key Vault. 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`
9. Facoltativo: se si desidera aggiornare le credenziali sul certificato di autenticazione di Azure Key Vault, utilizzare il comando seguente:
   `security key-manager external azure update-credentials -vserver v1 -authentication-method certificate`

Link correlati

- "Impostare Cloud Volumes ONTAP in modo che utilizzi una chiave gestita dal cliente in Azure"
- "Microsoft Azure docmentation: Informazioni su Azure Key Vault"
- "Guida di riferimento ai comandi ONTAP"

Gestire le chiavi di crittografia Cloud Volumes ONTAP con il servizio KMS di Google Cloud

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

La gestione delle chiavi con Cloud KMS può essere abilitata con l'interfaccia a riga di comando di ONTAP 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

- Il tuo sistema dovrebbe eseguire Cloud Volumes ONTAP 9.10.1 o versione successiva
- È necessario utilizzare una SVM dati. Cloud KMS può essere configurato solo su una SVM dati.
- Devi essere un amministratore del cluster o di SVM
- La licenza Volume Encryption (VE) deve essere installata sull'SVM
- A partire da Cloud Volumes ONTAP 9.12.1 GA, è necessario installare anche la licenza MTEKM (Multi-tenant Encryption Key Management)

- È richiesto un abbonamento attivo a Google Cloud Platform

Configurazione

Google Cloud

1. Nel tuo ambiente Google Cloud, "Creare un anello e una chiave GCP simmetrici".
2. Assegna un ruolo personalizzato alla chiave Cloud KMS e all'account del servizio Cloud Volumes ONTAP.
   a. Crea il ruolo personalizzato:

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

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. Assegna il ruolo personalizzato che hai creato:
   `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`

> Se utilizzi Cloud Volumes ONTAP 9.13.0 o versioni successive, non è necessario creare un ruolo personalizzato. Puoi assegnare il ruolo predefinito [`cloudkms.cryptoKeyEncrypterDecrypter` ^] ruolo.

3. 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`

Abilita le soluzioni di protezione dal ransomware NetApp per Cloud Volumes ONTAP

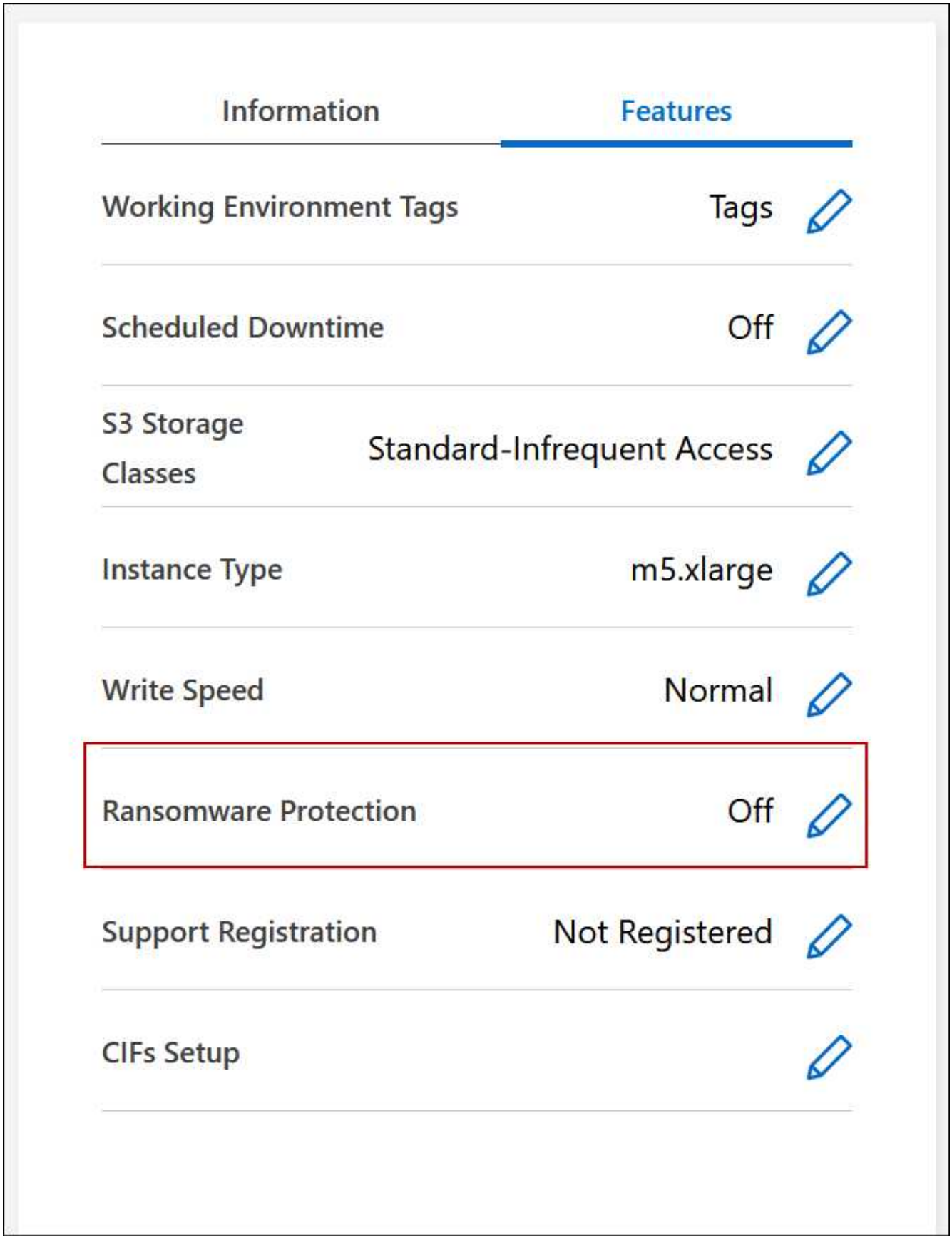
Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. BlueXP ti permette di implementare due soluzioni NetApp per il ransomware: Protezione dalle comuni estensioni di file ransomware e protezione autonoma dal ransomware (ARP). Queste soluzioni forniscono strumenti efficaci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

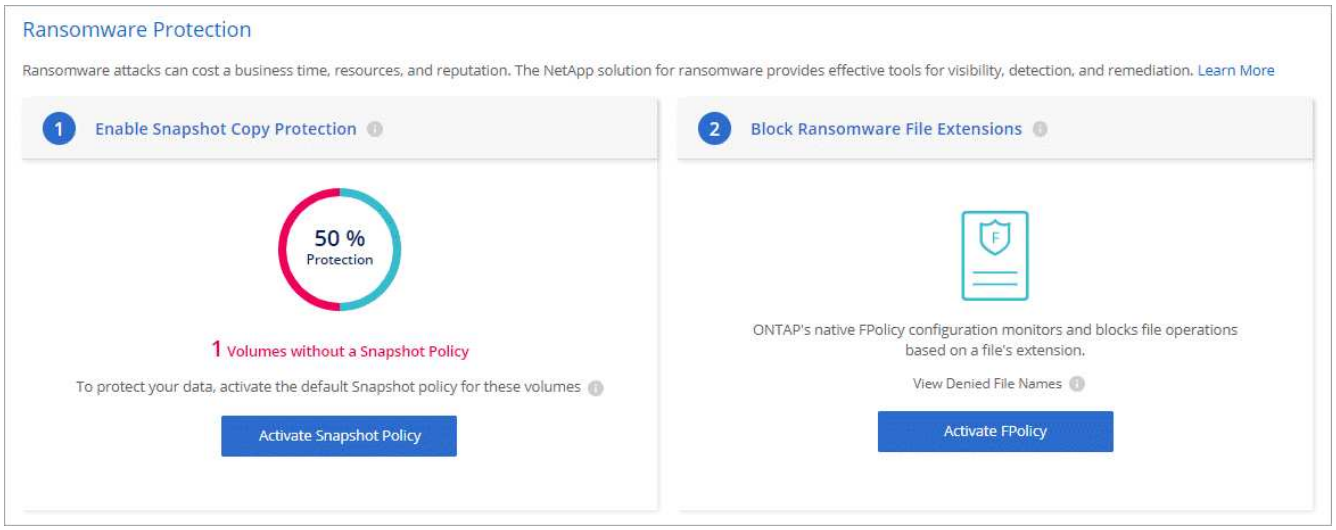
b. Fare clic su **Activate FPolicy** (attiva FPolicy) per attivare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione di un file.

   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.

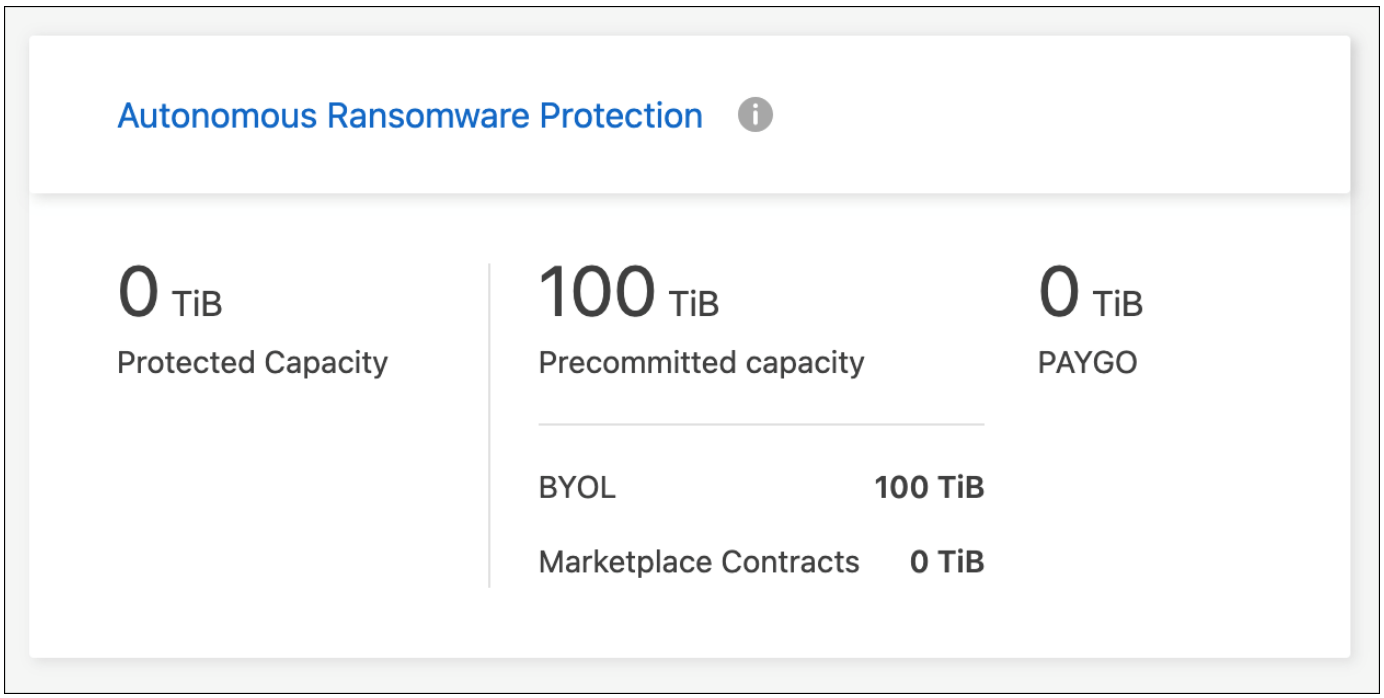
Separare dalle protezioni di estensione file fornite attraverso "impostazione di protezione dal ransomware", La funzione ARP utilizza l'analisi del carico di lavoro per avvisare l'utente in caso di potenziali attacchi in base a "attività anomala" rilevata. Sia l'impostazione di protezione dal ransomware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

La funzione ARP è disponibile per l'utilizzo con le sottoscrizioni Bring Your Own License (BYOL) e Marketplace per le licenze senza costi aggiuntivi.

I volumi abilitati per ARP hanno lo stato designato "modalità di apprendimento" o "attivo".

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 di ONTAP e la CLI di ONTAP, consultare la "Documentazione di ONTAP: Abilita la protezione autonoma da ransomware".



Crea copie Snapshot a prova di manomissione dei file WORM su Cloud Volumes ONTAP

Puoi creare copie Snapshot a prova di manomissione dei file WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP e conservare gli snapshot in forma non modificata per uno specifico periodo di conservazione. Questa funzionalità si basa sulla tecnologia SnapLock e fornisce un livello aggiuntivo di data Protection e conformità.

Prima di iniziare

Verificare che il volume utilizzato per la creazione di copie Snapshot sia un volume SnapLock. Per informazioni sull'attivazione della protezione SnapLock sui volumi, fare riferimento alla "Documentazione ONTAP: Configurare SnapLock" .

Fasi

1. Creare copie Snapshot dal volume SnapLock. Per informazioni sulla creazione di copie Snapshot utilizzando l'interfaccia CLI o System Manager, fare riferimento alla "Documentazione di ONTAP: Panoramica sulle copie Snapshot locali di gestione" .

   Le copie Snapshot ereditano le proprietà WORM del volume, rendendole antimanomissione. La tecnologia SnapLock sottostante garantisce la protezione di uno snapshot dalla modifica e dall'eliminazione fino allo scadere del periodo di conservazione specificato.

2. È possibile modificare il periodo di conservazione se è necessario modificare questi snapshot. Per ulteriori informazioni, fare riferimento alla "Documentazione ONTAP: Impostare il tempo di conservazione" .

Anche se una copia Snapshot è protetta per un periodo di conservazione specifico, il volume di origine può essere eliminato da un amministratore del cluster, poiché lo storage WORM in Cloud Volumes ONTAP opera nell'ambito di un modello di "amministratore dello storage trusted". Inoltre, un amministratore del cloud fidato può eliminare i dati WORM operando sulle risorse di cloud storage.

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 eseguire l'aggiornamento di Cloud Volumes ONTAP utilizzando Gestione di sistema di ONTAP o l'interfaccia a riga di comando di ONTAP. 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
9.15.1	9.16.1 (solo per Azure e Google Cloud)
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1

Versione corrente	Versioni a cui è possibile eseguire direttamente l'aggiornamento
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
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 è disponibile una versione di patch per le tre versioni più recenti di Cloud Volumes ONTAP. Le versioni delle patch sono occasionalmente disponibili per la distribuzione, quando la versione RC o GA non è disponibile per la distribuzione.

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 entro 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 un paio di 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 all'assistenza NetApp per aggiornare il software utilizzando uno dei metodi descritti in questa pagina. Ciò si applica sia al modello pay-as-you-go (PAYGO) che al modello Bring Your Own License (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 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: Comandi per la configurazione dello sconto 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 Gestione di sistema di ONTAP 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

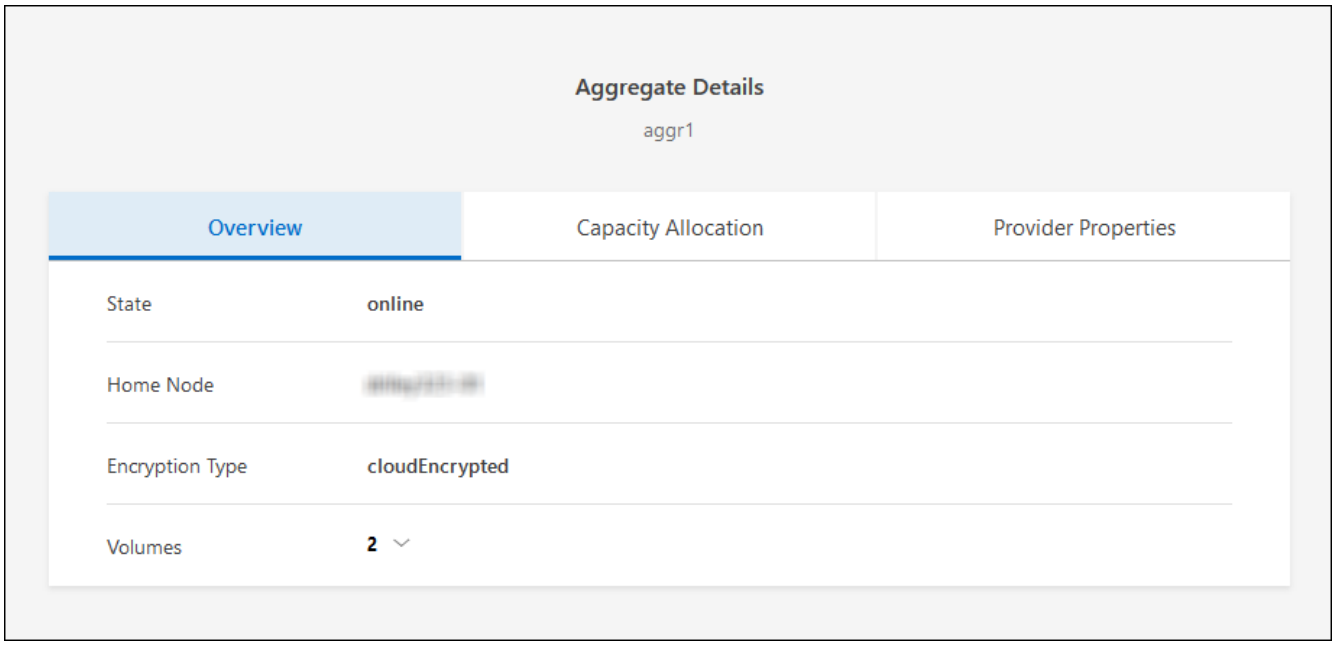
Gli aggregati per Cloud Volumes ONTAP devono essere online prima di aggiornare il software. Gli aggregati devono essere online nella maggior parte delle configurazioni, ma in caso contrario, è necessario portarli online.

A proposito di questa attività

Questa procedura descrive come utilizzare Gestione di sistema di ONTAP per la versione 9,3 e successive.

Fasi

1. Nell'ambiente di lavoro, fare clic sulla scheda **aggregati**.
2. Sotto il titolo aggregato, fare clic sul pulsante puntini di sospensione, quindi selezionare **Visualizza dettagli aggregati**.



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 ONTAP a "Verifica che tutte le LIF siano sulle porte home".

Se si verifica un errore di aggiornamento, consultare l'articolo della Knowledge base (KB) "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:

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

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

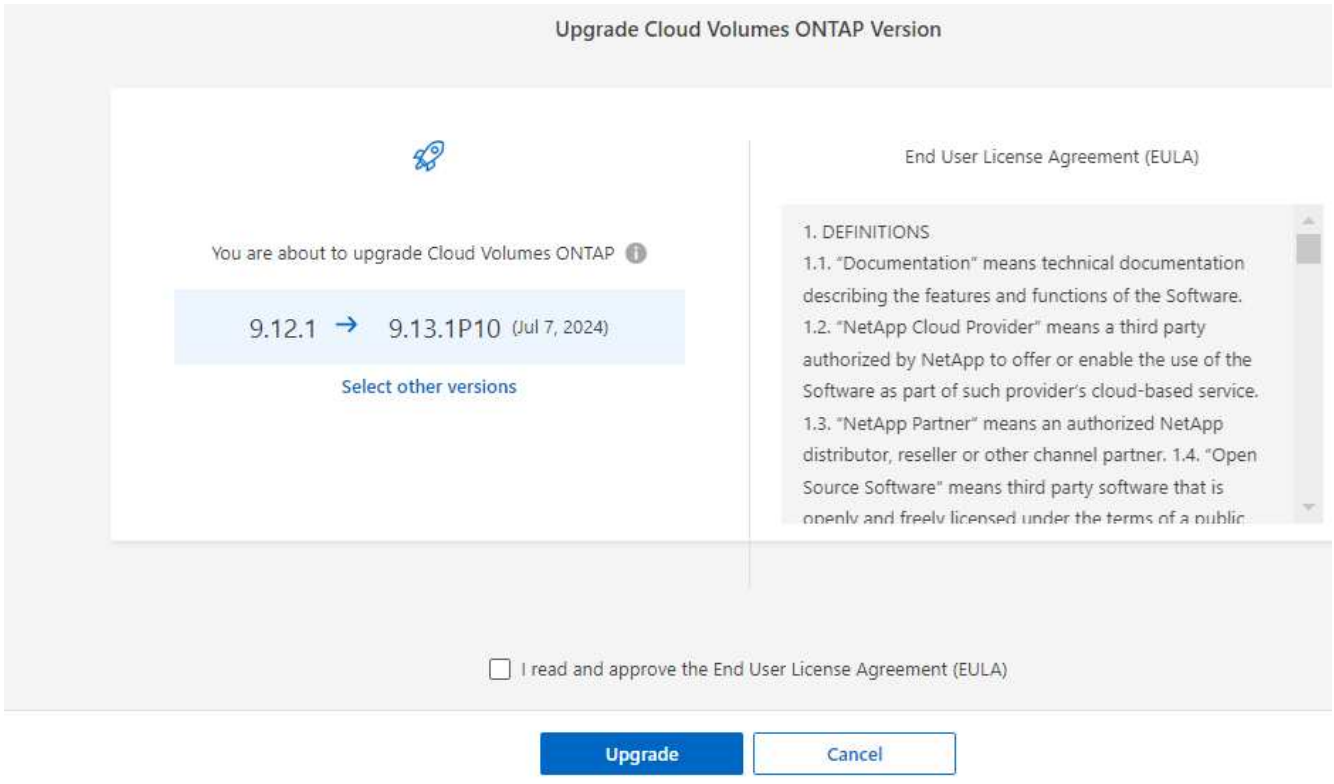
Le operazioni BlueXP, come la creazione di volumi o aggregati, non devono essere in corso sul sistema Cloud Volumes ONTAP.

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:

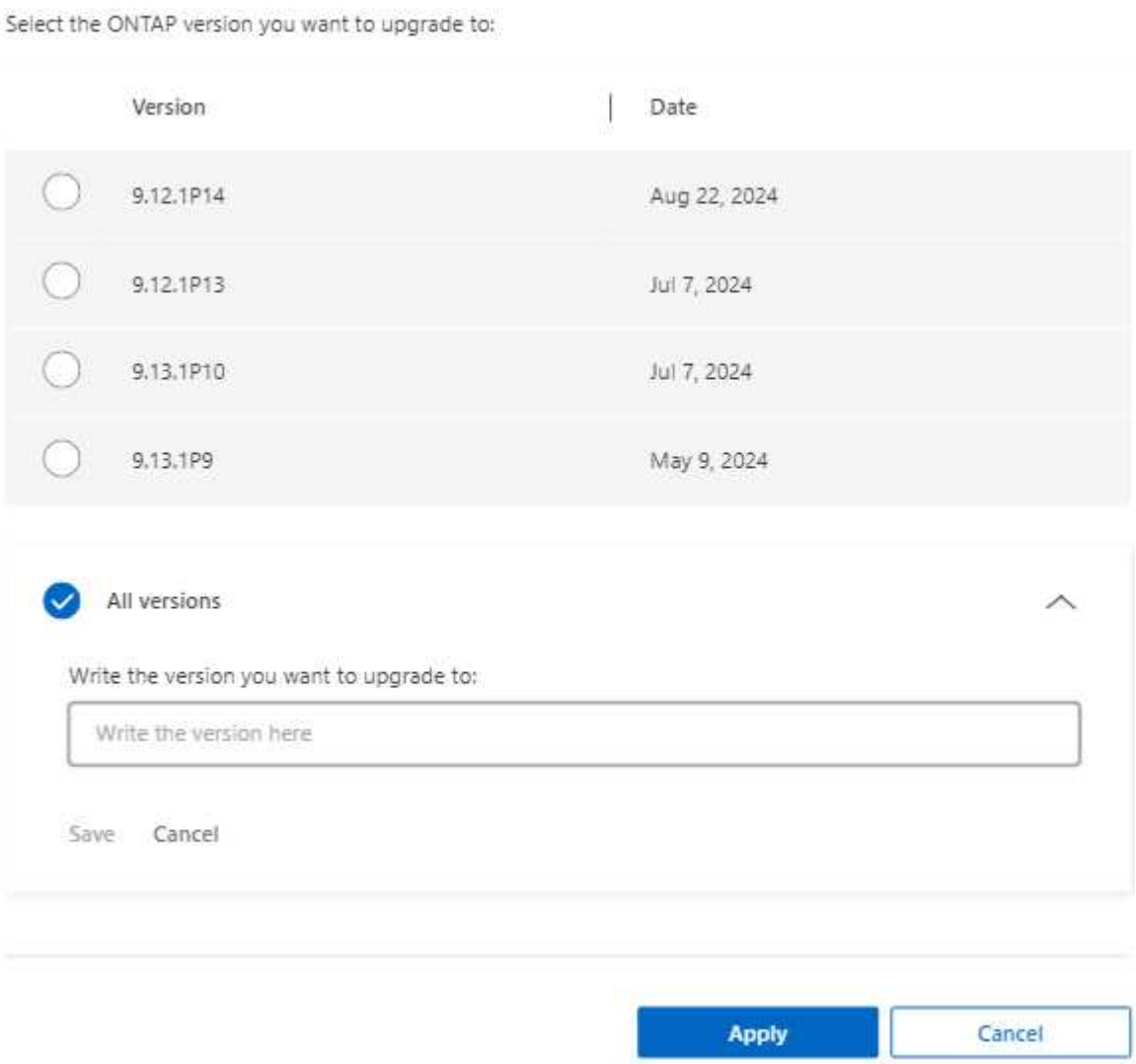
3. Se si desidera aggiornare la versione installata di Cloud Volumes ONTAP, fare clic su **Aggiorna ora!** Per impostazione predefinita, viene visualizzata l'ultima versione compatibile per l'aggiornamento.



   Se si desidera eseguire l'aggiornamento a un'altra versione, fare clic su **Seleziona altre versioni**. Vengono elencate le versioni più recenti di Cloud Volumes ONTAP compatibili con la versione installata sul sistema. Ad esempio, la versione installata sul sistema è 9.12.1P3 e sono disponibili le seguenti versioni compatibili:

- Da 9.12.1P4 a 9.12.1P14
- 9.13.1 e 9.13.1P1 si vede 9.13.1P1 come versione predefinita per l'aggiornamento, e 9.12.1P13, 9.13.1P14, 9.13.1 e 9.13.1P1 come le altre versioni disponibili.

4. Facoltativamente, è possibile fare clic su **tutte le versioni** per immettere un'altra versione alla quale si desidera aggiornare (ad esempio, la patch successiva della versione installata). Per un percorso di aggiornamento compatibile della versione Cloud Volumes ONTAP corrente, fare riferimento a "Percorsi di upgrade supportati".
5. Fare clic su **Salva**, quindi su **Applica**.



6. 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).
7. Fare clic su **Upgrade** (Aggiorna).
8. 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 di BlueXP, fare clic sul pulsante **… (Icona ellissi)**, 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".

Registrare sistemi Cloud Volumes ONTAP pay-as-you-go

Il supporto NetApp è incluso nei sistemi Cloud Volumes ONTAP pay-as-you-go (PAYGO), ma devi 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.

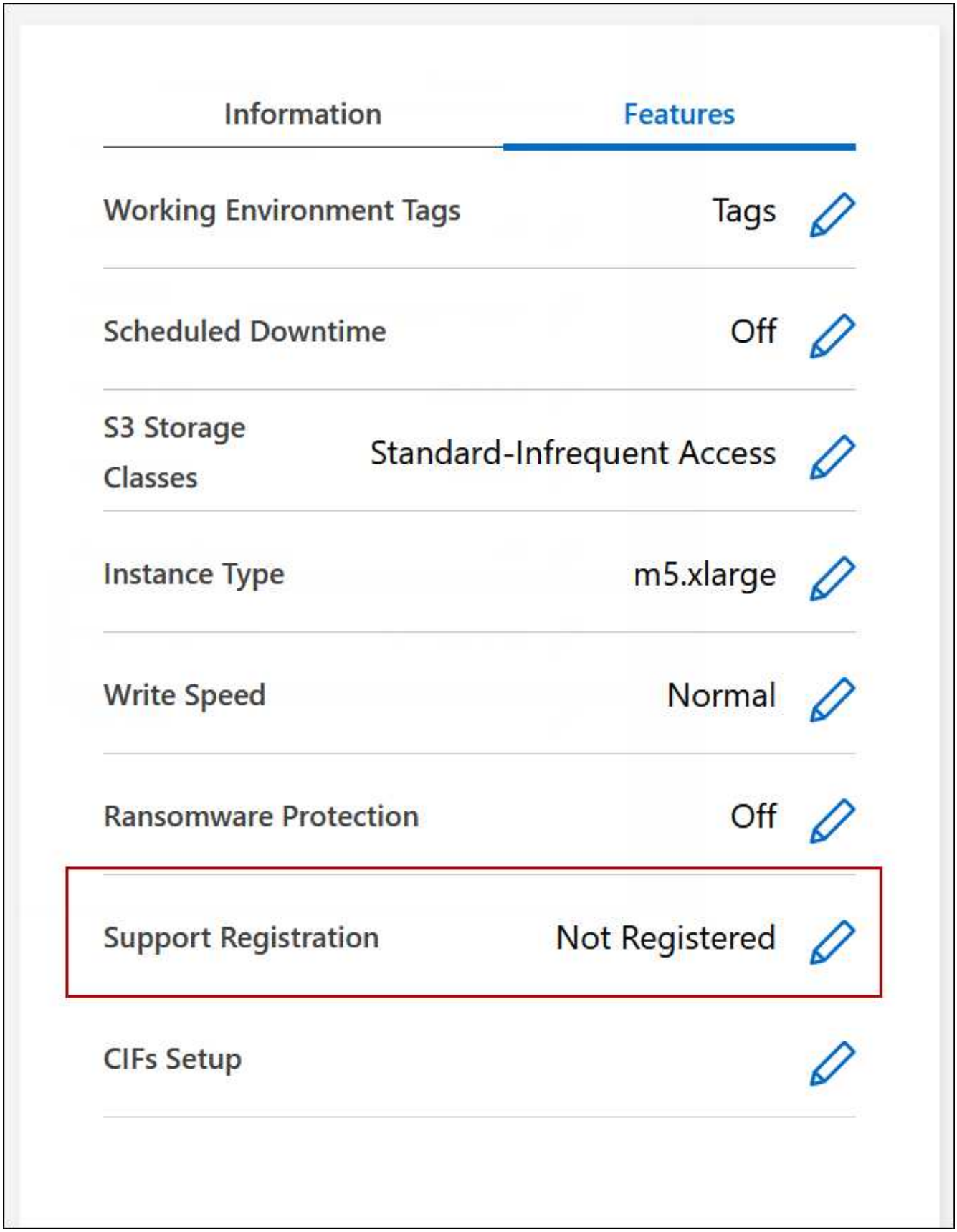
Fasi

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.

Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità

Dopo la fine della disponibilità (EOA) delle licenze basate su nodi, è necessario passare alla licenza basata sulla capacità utilizzando il tool di conversione delle licenze BlueXP .

Per gli impegni annuali o a lungo termine, NetApp consiglia di contattare il rappresentante NetApp prima della data di fine disponibilità (11 novembre, 2024) o della data di scadenza della licenza, per verificare che siano in vigore i prerequisiti per la transizione. Se non disponi di un contratto a lungo termine per un nodo Cloud Volumes ONTAP ed esegui il sistema su un abbonamento PAY-as-you-go (PAYGO) on-demand, è importante pianificare la conversione prima della fine del supporto (EOS) il 31 dicembre, 2024. In entrambi i casi, è necessario assicurarsi che il sistema soddisfi i requisiti prima di utilizzare lo strumento di conversione delle licenze BlueXP per una transizione senza problemi.

Per informazioni sulla fine disponibilità e l'EOS, fare riferimento alla "Fine della disponibilità delle licenze basate su nodi".

A proposito di questa attività

- Quando utilizzi il tool di conversione delle licenze, il passaggio dal modello di licenza basato su nodi a quello basato sulla capacità viene eseguito sul posto e online, in modo da eliminare la necessità di migrazione dei dati o provisioning di risorse cloud aggiuntive.
- Si tratta di un'operazione senza interruzioni e non si verificano interruzioni del servizio o downtime dell'applicazione.
- I dati dell'account e dell'applicazione nel sistema Cloud Volumes ONTAP rimangono intatti.
- Le risorse cloud sottostanti rimangono invariate dopo la conversione.
- Il tool di conversione delle licenze supporta tutti i tipi di implementazione, come nodo singolo, alta disponibilità (ha) in una singola zona di disponibilità (AZ), ha in più AZ, Bring Your Own License (BYOL) e PAYGO.
- Lo strumento supporta tutte le licenze basate su nodi come origine e tutte le licenze basate su capacità come destinazione. Ad esempio, se si dispone di una licenza basata su nodi PAYGO Standard, è possibile convertirla in qualsiasi licenza basata su capacità acquistata tramite il marketplace. NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consultare "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .
- La conversione è supportata per tutti i cloud provider, AWS, Azure e Google Cloud.
- Dopo la conversione, il numero di serie della licenza basata su nodo verrà sostituito da un formato basato sulla capacità. Questa operazione viene eseguita come parte della conversione e si riflette sull'account del sito di supporto NetApp (NSS).
- Durante il passaggio al modello basato sulla capacità, i dati continuano a essere conservati nella stessa posizione della licenza basata su nodi. Questo approccio garantisce l'assenza di interruzioni nel posizionamento dei dati e il rispetto dei principi di sovranità dei dati durante la transizione.

Prima di iniziare

- È necessario disporre di un account NSS con accesso al cliente o all'amministratore.
- L'account NSS deve essere registrato con le credenziali utente BlueXP .
- L'ambiente di lavoro deve essere collegato all'account NSS con accesso al cliente o all'amministratore.

- Devi disporre di una licenza valida basata sulla capacità, che sia una licenza BYOL o un'iscrizione al marketplace.
- Nell'account BlueXP dovrebbe essere disponibile una licenza basata sulla capacità. Questa licenza può essere un'iscrizione al marketplace o un pacchetto BYOL/offerta privata nel portafoglio digitale di BlueXP .
- Prima di selezionare un pacchetto di destinazione, comprendere i seguenti criteri:
  - Se l'account dispone di una licenza BYOL basata sulla capacità, il pacchetto di destinazione selezionato deve allinearsi alle licenze BYOL basate sulla capacità dell'account:
    - Quando `Professional` viene selezionato come pacchetto di destinazione, l'account deve disporre di una licenza BYOL con un pacchetto Professional:
    - Quando `Essentials` viene selezionato come pacchetto di destinazione, l'account deve disporre di una licenza BYOL con il pacchetto Essentials.
  - Se il pacchetto di destinazione non si allinea con la disponibilità della licenza BYOL dell'account, significa che la licenza basata sulla capacità potrebbe non includere il pacchetto selezionato. In questo caso, ti verrà addebitato il costo tramite l'abbonamento al mercato.
  - Se non esiste una licenza BYOL basata sulla capacità ma solo un'iscrizione al marketplace, devi assicurarti che il pacchetto selezionato sia incluso nell'iscrizione al marketplace basato sulla capacità.
  - Se non c'è capacità sufficiente nella tua licenza esistente basata sulla capacità e se hai un'iscrizione al marketplace per addebitare l'utilizzo di capacità aggiuntiva, ti verrà addebitato la capacità aggiuntiva tramite l'iscrizione al marketplace.
  - Se la tua licenza esistente basata sulla capacità non dispone di capacità sufficiente e non disponi di un abbonamento al marketplace per addebitare l'utilizzo della capacità aggiuntiva, la conversione non può avvenire. Devi aggiungere un'iscrizione al marketplace per addebitare la capacità aggiuntiva o estendere la capacità disponibile alla tua licenza attuale.
  - Se il pacchetto di destinazione non si allinea con la disponibilità della licenza BYOL dell'account e anche se non c'è capacità sufficiente nella tua licenza esistente basata sulla capacità, ti verrà addebitato il costo dell'abbonamento al marketplace.

Se uno di questi requisiti non è soddisfatto, la conversione della licenza non avviene. In casi specifici, la licenza potrebbe essere convertita, ma non può essere utilizzata. Fare clic sull'icona delle informazioni per identificare i problemi e intraprendere azioni correttive.

Fasi

1. Nella pagina Canvas, fare doppio clic sul nome dell'ambiente di lavoro per il quale si desidera modificare il tipo di licenza.
2. Nella scheda Panoramica, fare clic sul pannello funzioni.
3. Controllare l'icona a forma di matita accanto a **metodo di ricarica**. Se il metodo di ricarica per il sistema è `Node Based`, è possibile convertirlo in ricarica per capacità.

   L'icona è disattivata se il sistema Cloud Volumes ONTAP è già caricato in base alla capacità o se uno dei requisiti non è soddisfatto.

4. Nella schermata **Converti licenze basate su nodo in basate sulla capacità**, verificare il nome dell'ambiente di lavoro e i dettagli della licenza di origine.
5. Selezionare il pacchetto di destinazione per la conversione della licenza esistente:
   - Indispensabili. Il valore predefinito è `Essentials`.

    - Professionale
6. Se disponi di una licenza BYOL, puoi selezionare la casella di controllo per eliminare la licenza basata su nodo dalla post conversione del Digital Wallet di BlueXP . Se la conversione non è completa, anche selezionando questa casella di controllo, la licenza non verrà eliminata dal portafoglio digitale. Se hai un abbonamento al mercato, questa opzione non è disponibile.
7. Selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **Procedi**.

Al termine

Visualizzare il nuovo numero di serie della licenza e verificare le modifiche apportate al portafoglio digitale di BlueXP .

Prezzi in diversi iperscalari

Per i dettagli sui prezzi, vai a "Sito Web di NetApp BlueXP" .

Per informazioni sulle offerte private in specifici iperscalari, scrivere a:

- AWS - awspo@netapp.com
- Azzurro - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

Avviare e arrestare un sistema 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.

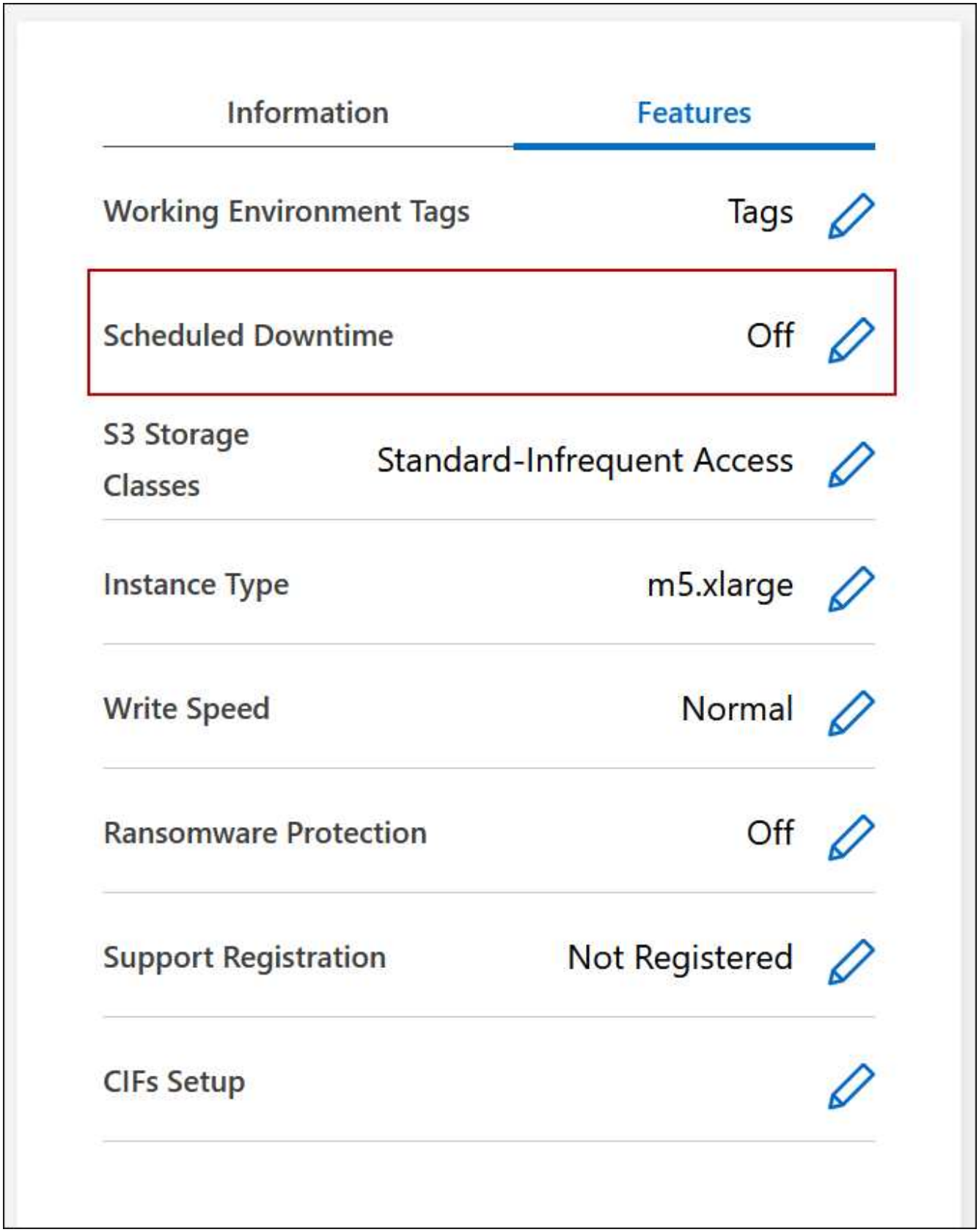
  BlueXP arresta il sistema al termine del trasferimento.

- 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**.



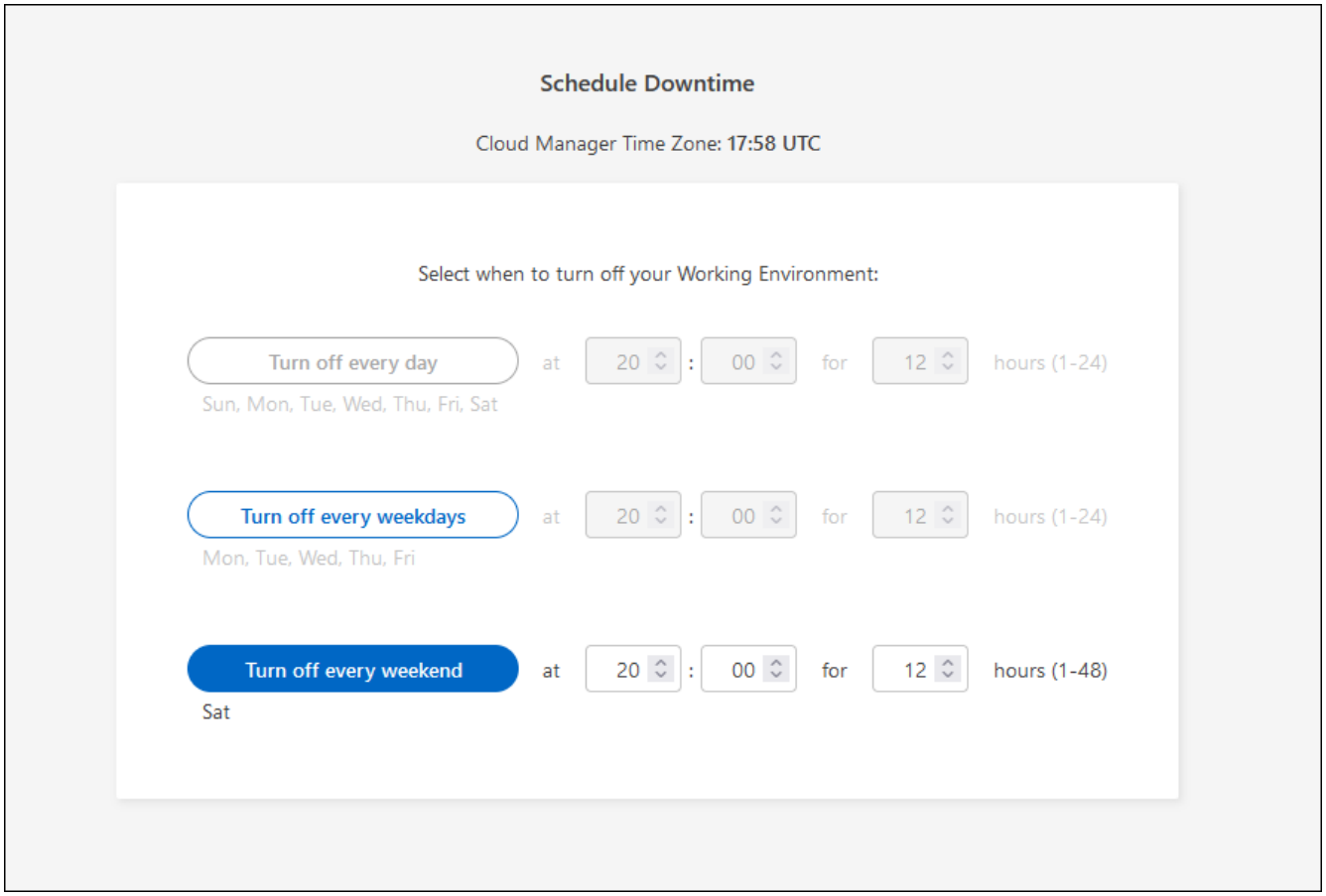
3. Specificare il programma di arresto:

   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.

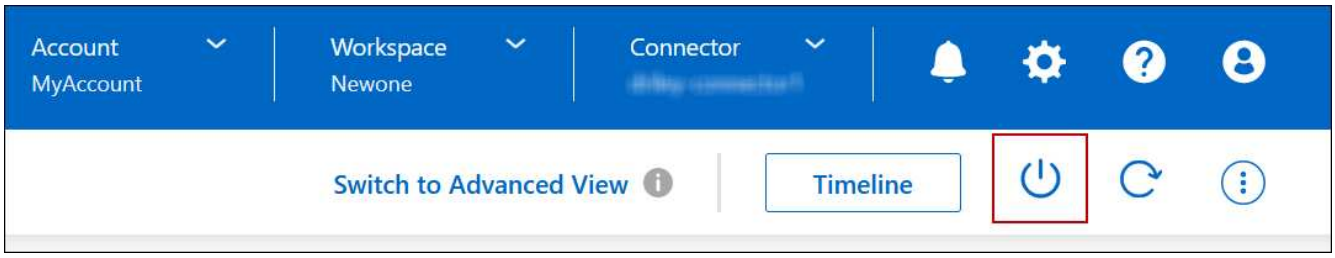
> Per ridurre i costi, BlueXP elimina periodicamente le vecchie snapshot dei dischi root e di boot. Vengono conservati solo i due snapshot più recenti per i dischi root e di boot.

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 Cloud Volumes ONTAP utilizzando il server 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"

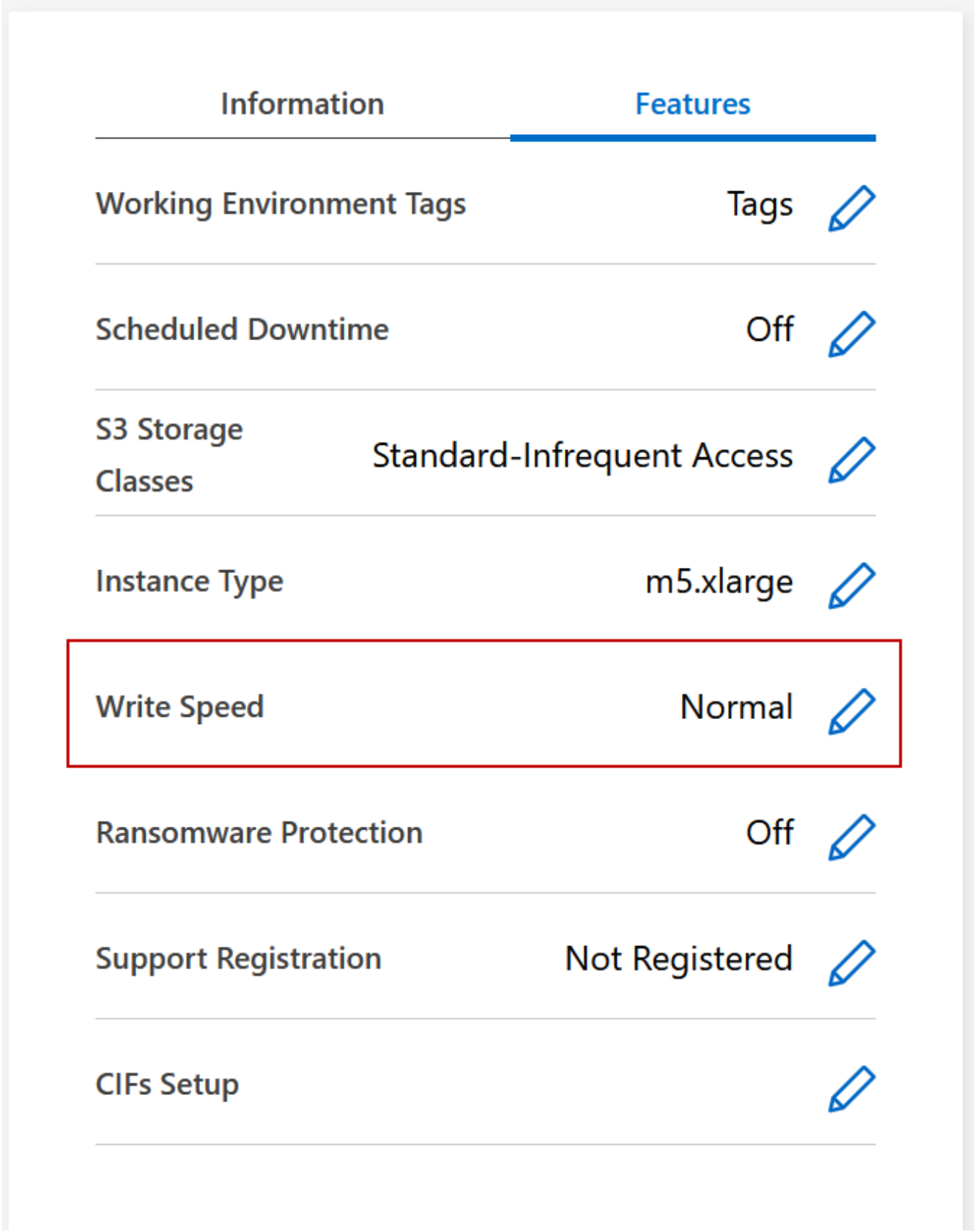
Prima di modificare la velocità di scrittura, è necessario "comprendere le differenze tra le impostazioni normali e quelle alte".

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 di amministrazione del cluster 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 Gestione sistema ONTAP o l'interfaccia CLI ONTAP. La password non verrà riflessa in BlueXP. Di conseguenza, BlueXP non è in grado di monitorare correttamente l'istanza.

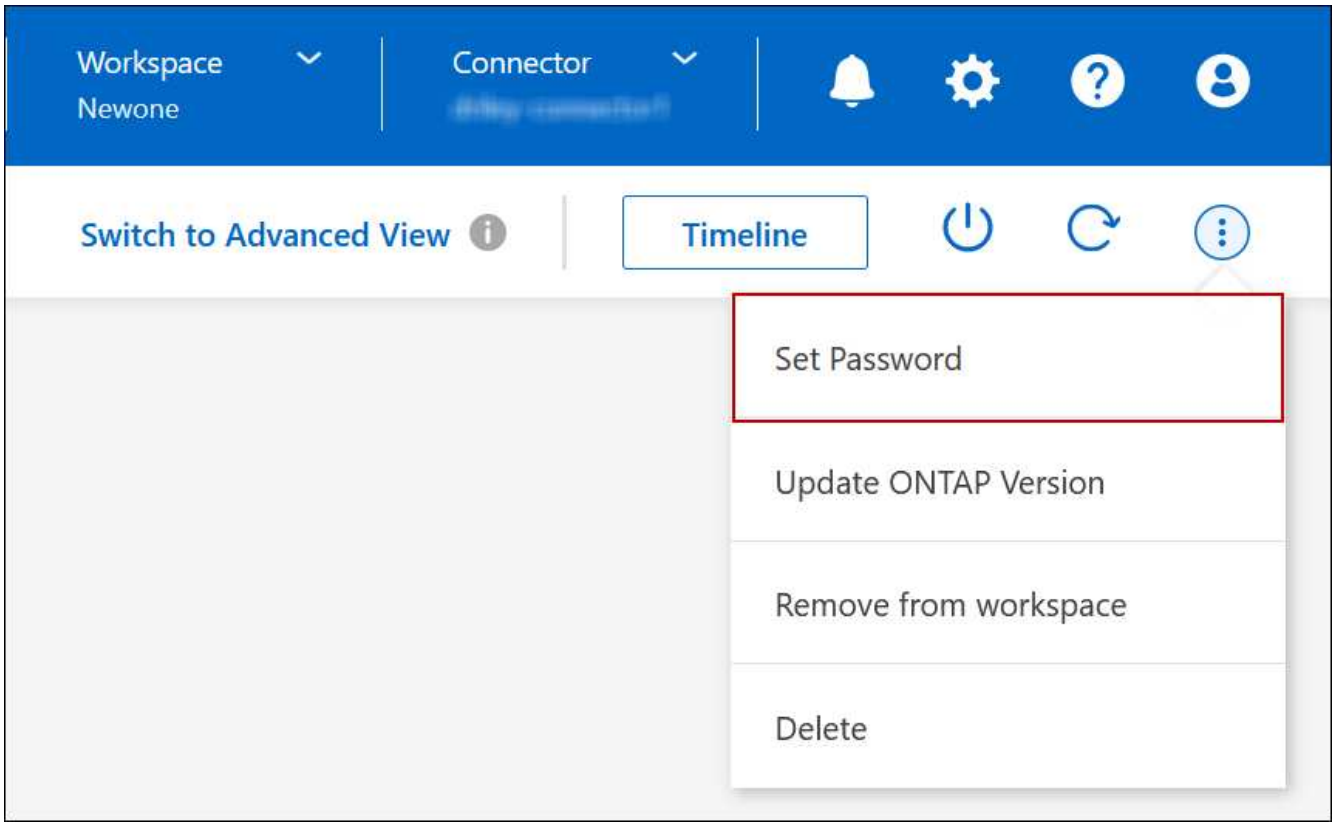
A proposito di questa attività

La password deve rispettare alcune regole. La nuova password:

- Non deve contenere la parola `admin`
- La lunghezza deve essere compresa tra 8 e 50 caratteri
- Deve contenere almeno una lettera inglese e una cifra
- Non deve contenere questi caratteri speciali: `/ ( ) { } [ ] # : % " ? \`

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, fai clic sull'icona con i puntini di sospensione e seleziona **Imposta password**.



Aggiungere, rimuovere o eliminare sistemi

Aggiunta di un sistema Cloud Volumes ONTAP esistente 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.

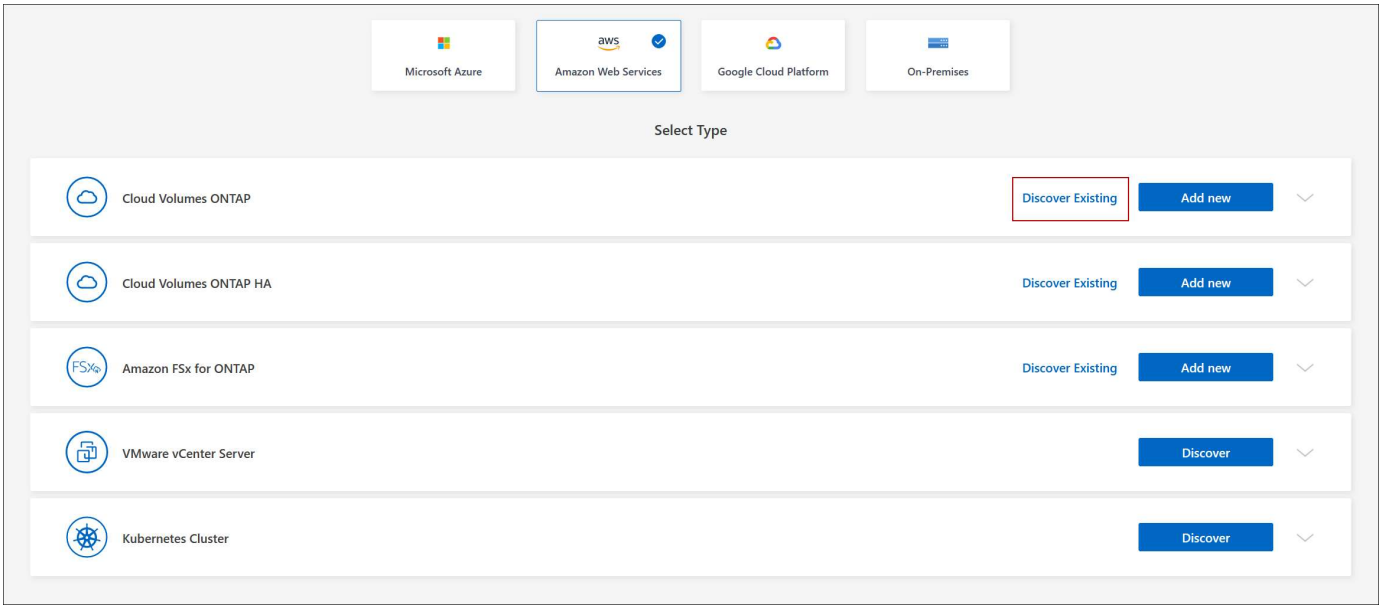
Prima di iniziare

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 da aggiungere.
5. Fare clic sul collegamento per individuare un sistema esistente.

+



1. Nella pagina Regione, selezionare una regione. È possibile visualizzare i sistemi in esecuzione nella regione selezionata.

   I sistemi Cloud Volumes ONTAP sono rappresentati come istanze in questa pagina. Dall'elenco, è possibile selezionare solo le istanze registrate con l'account corrente.

2. Nella pagina credenziali, immettere la password per l'utente amministratore Cloud Volumes ONTAP, quindi selezionare **Vai**.

Risultato

BlueXP aggiunge le istanze Cloud Volumes ONTAP al progetto o all'area di lavoro.

Rimuovere un ambiente di lavoro Cloud Volumes ONTAP da BlueXP

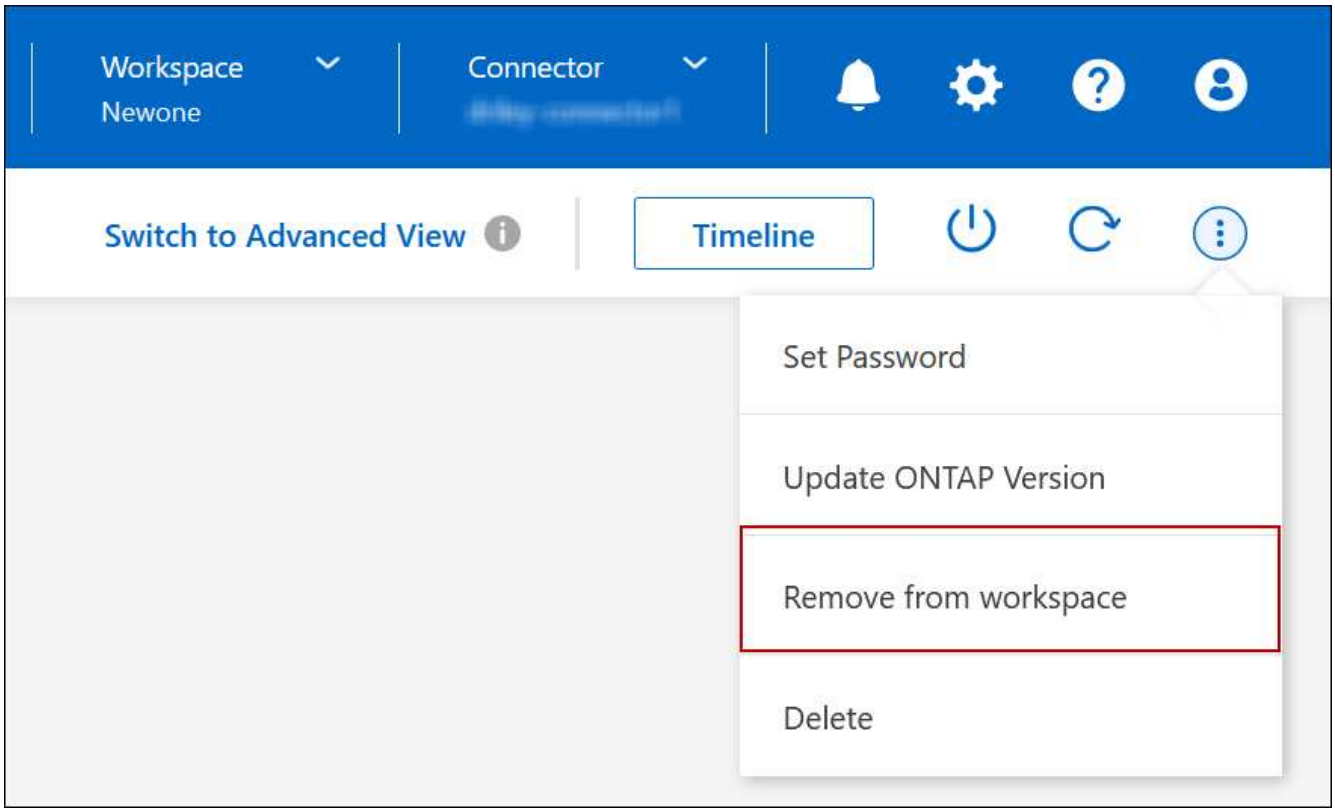
È possibile rimuovere un ambiente di lavoro Cloud Volumes ONTAP per spostarlo in un altro sistema o per risolvere i problemi di rilevamento.

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 è possibile riscoprire l'ambiente di lavoro, ad esempio in caso di problemi durante la ricerca 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 dei puntini di sospensione 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.

Eliminare un sistema Cloud Volumes ONTAP da BlueXP

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.

> Altre risorse, come i backup gestiti da BlueXP backup and recovery e le istanze per la BlueXP classification, non vengono eliminate quando si elimina un ambiente di lavoro. Sarà necessario eliminarli manualmente. In caso contrario, continuerai a dover sostenere 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

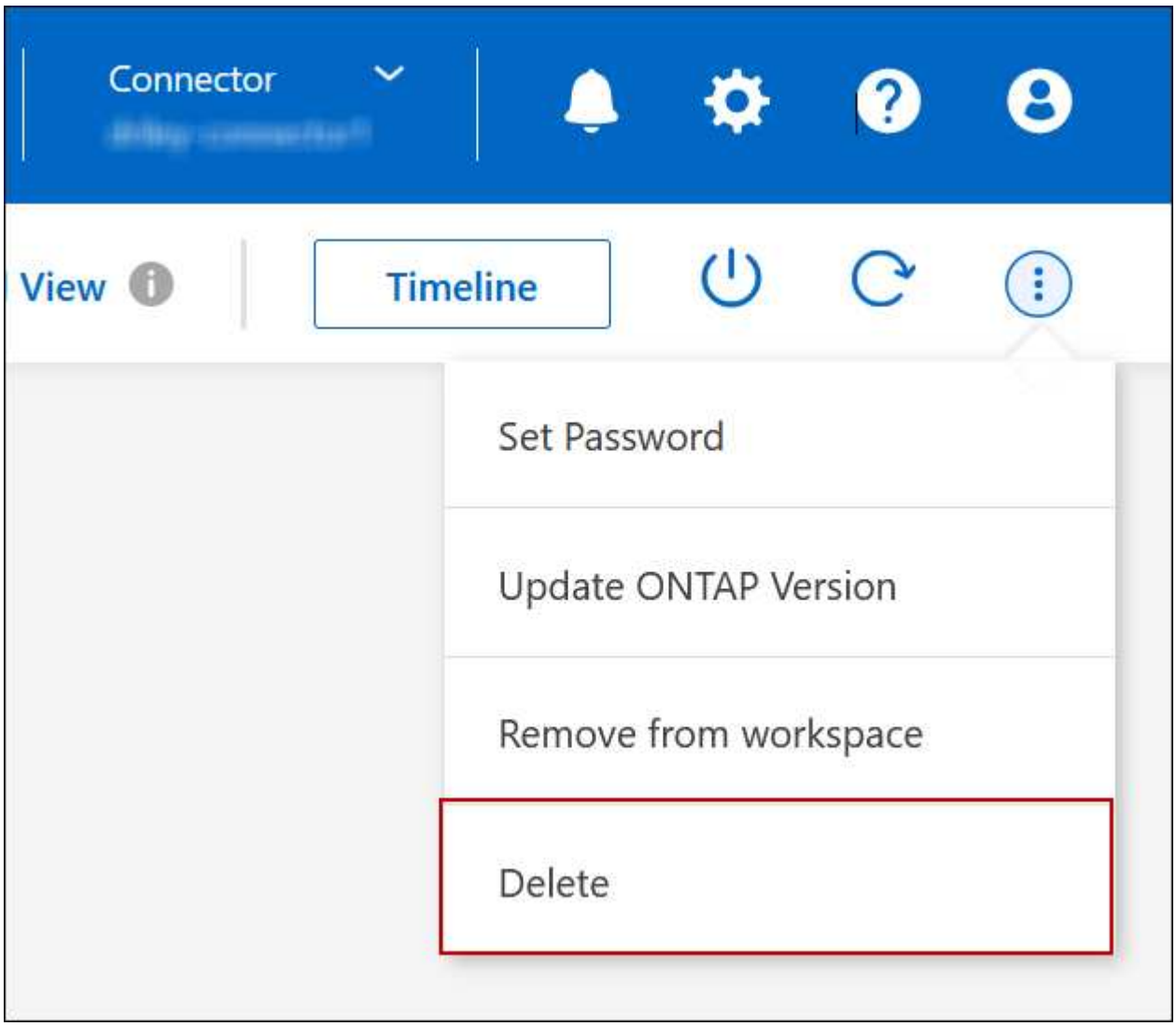
1. Se nell'ambiente di lavoro è stato attivato il backup e il ripristino di BlueXP, determinare se i dati di cui è stato eseguito il backup sono ancora necessari "eliminare i backup, se necessario".

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, fai clic sull'icona con i puntini di sospensione e seleziona **Elimina**.



   c. Nella finestra Elimina ambiente di lavoro, digitare il nome dell'ambiente di lavoro e quindi fare clic su **Elimina**. L'eliminazione dell'ambiente di lavoro potrebbe richiedere fino a cinque minuti.

Il BlueXP backup and recovery sono gratuiti solo per le licenze Cloud Volumes ONTAP Professional. Questo vantaggio gratuito non si applica agli ambienti eliminati. Se le copie di backup dell'ambiente Cloud Volumes ONTAP vengono conservate in un'istanza BlueXP backup and recovery , ti verranno addebitati i costi delle copie di backup finché non verranno eliminate.

Amministrazione di AWS

Modificare il tipo di istanza EC2 per un sistema Cloud Volumes ONTAP in AWS

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 cambia un nodo alla volta avviando il takeover e in attesa del giveback. Il team di controllo qualità di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha riscontrato alcun problema sul lato client. Con il variare delle connessioni, alcuni tentativi sono stati osservati a livello di i/o, ma il livello applicativo ha superato il cablaggio delle connessioni NFS/CIFS.

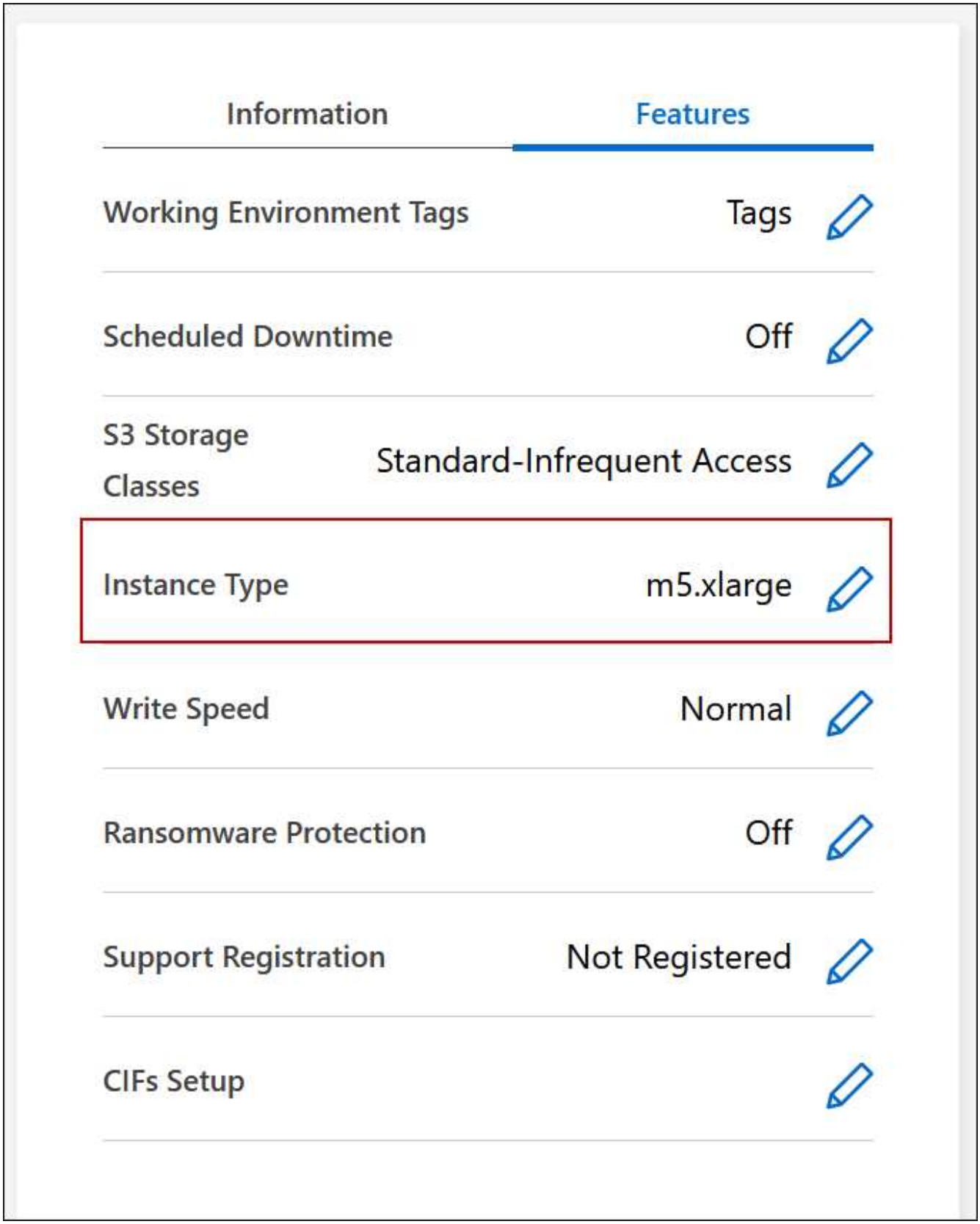
Riferimento

Per un elenco dei tipi di istanza supportati in AWS, fare riferimento a "Istanze EC2 supportate".

Se non è possibile modificare il tipo di istanza da istanze C4, M4 o R4, fare riferimento all'articolo della KB "Conversione di un'istanza CVO Xen di AWS in Nitro (KVM)".

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**.



Se si utilizza una licenza pay as you go (PAYGO) basata su nodo, è possibile scegliere un tipo di licenza e di istanza diverso facendo clic sull'icona a forma di matita accanto a **tipo di licenza**.

1. 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

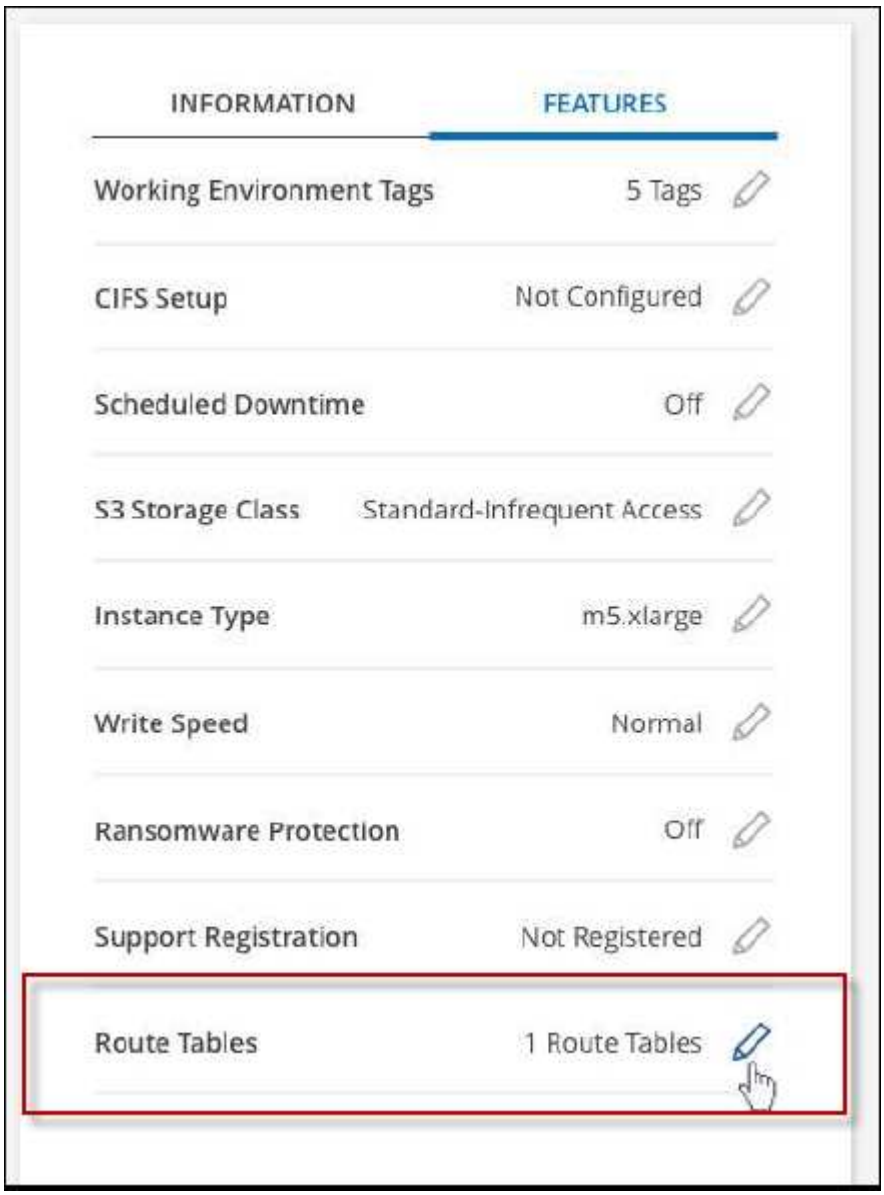
Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Modificare le tabelle di routing per coppie ha Cloud Volumes ONTAP in più AWS AZS

È possibile modificare le tabelle di routing AWS che includono i percorsi verso gli indirizzi IP mobili per una coppia ha 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.

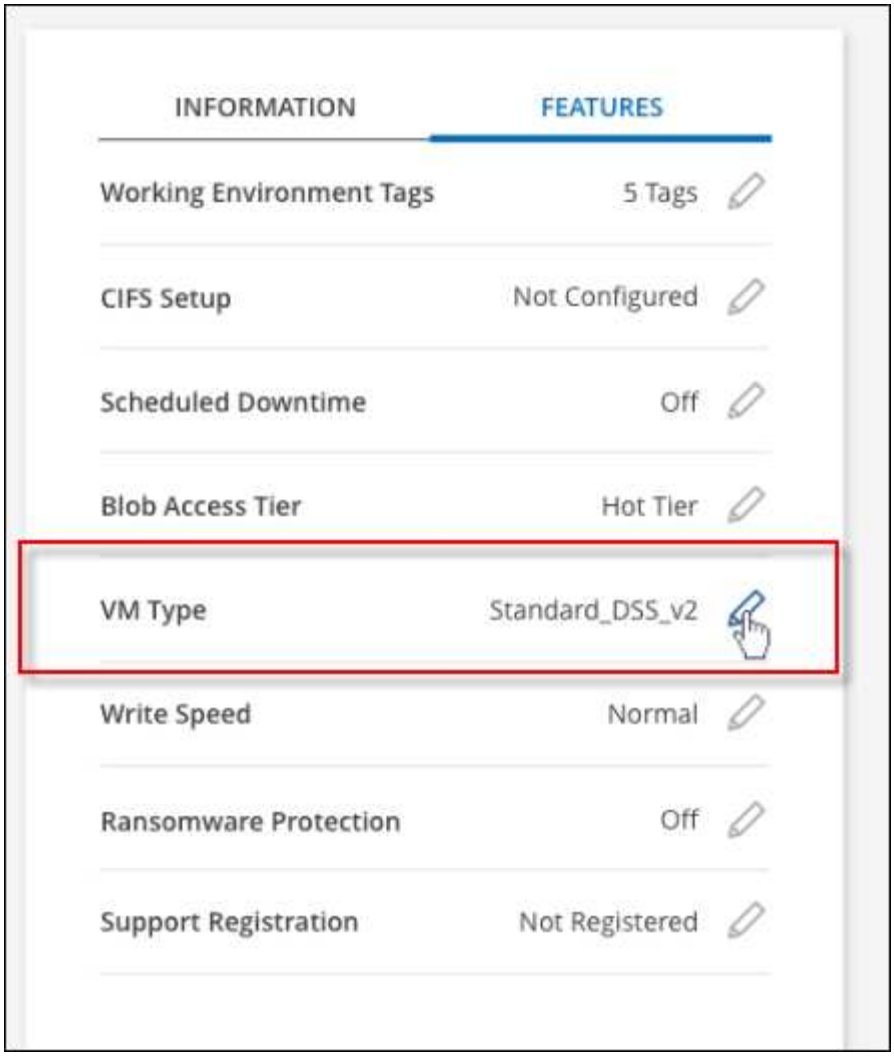
  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

BlueXP cambia un nodo alla volta avviando il takeover e in attesa del giveback. Il team di controllo qualità di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha riscontrato alcun problema sul lato client. Con il variare delle connessioni, alcuni tentativi sono stati osservati a livello di i/o, ma il livello applicativo ha superato il cablaggio 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**.



Se si utilizza una licenza PAYGO (pay-as-you-go) basata su nodi, è possibile scegliere una licenza e un tipo di VM diversi facendo clic sull'icona a forma di matita accanto a **tipo di licenza**.

1. 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.

Override dei blocchi CIFS per coppie ha Cloud Volumes ONTAP in Azure

L'organizzazione o l'amministratore dell'account BlueXP può abilitare un'impostazione in BlueXP per evitare 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.

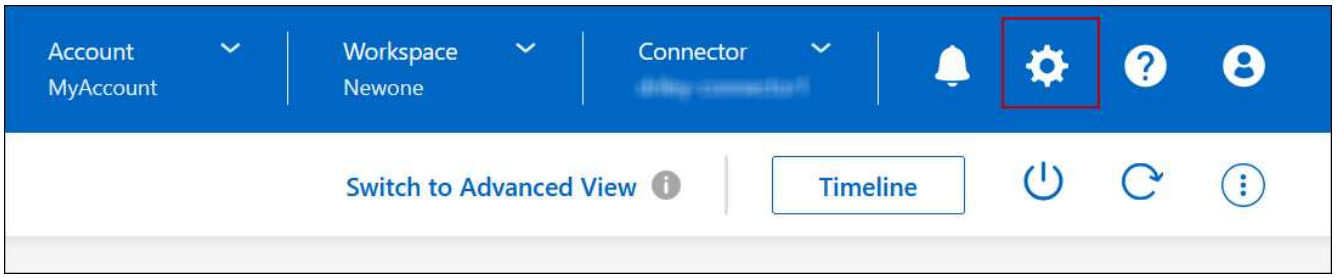
> Questo processo potrebbe interrompere i client CIFS. I dati non impegnati dai client CIFS potrebbero andare persi.

Prima di iniziare

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).

Utilizza un Azure Private link o gli endpoint di servizio per i sistemi Cloud Volumes ONTAP

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.

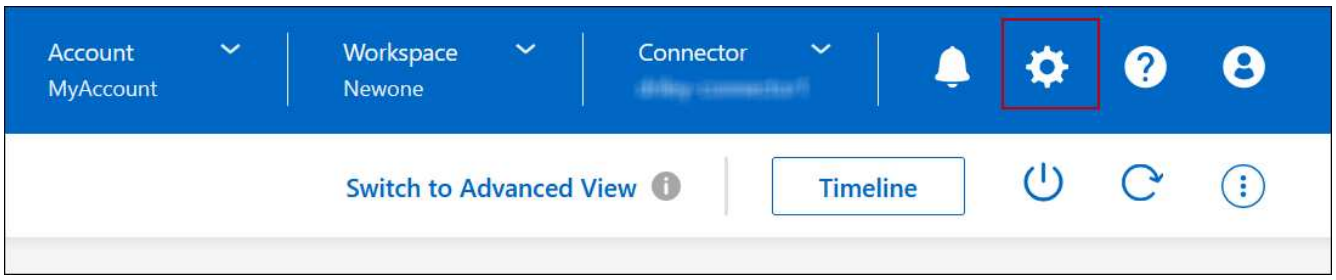
Disattivare Azure Private Links e utilizzare gli endpoint del servizio

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

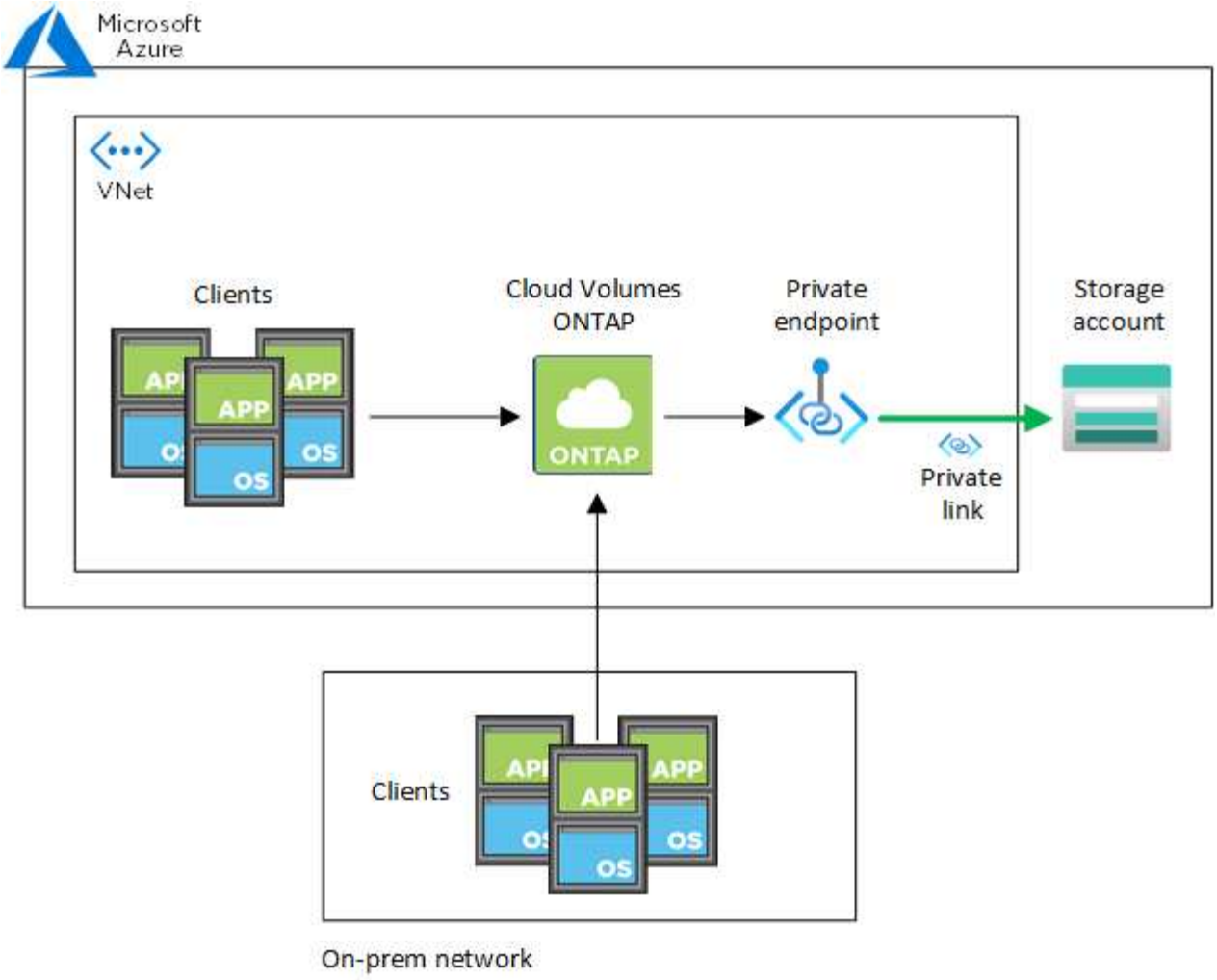
Se si utilizza un DNS personalizzato, è possibile creare un server di inoltro condizionale per la zona DNS privata di Azure dai server DNS personalizzati. Per ulteriori informazioni, fare riferimento a. "Documentazione di Azure sull'utilizzo di un server di inoltro DNS".

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 client tramite un collegamento privato dall'interno della stessa VNet e da una rete locale dotata di una connessione VPN privata 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. Vai a `/opt/application/netapp/cloudmanager/docker_occm/data` elenco.
3. Modificare `app.conf` aggiungendo il `user-private-dns-zone-settings` parametro 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 `subscription` La parola chiave è obbligatoria solo se la zona DNS privata si trova 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.

Sposta un gruppo di risorse di Azure per Cloud Volumes ONTAP nella console di Azure

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, fare riferimento alla "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

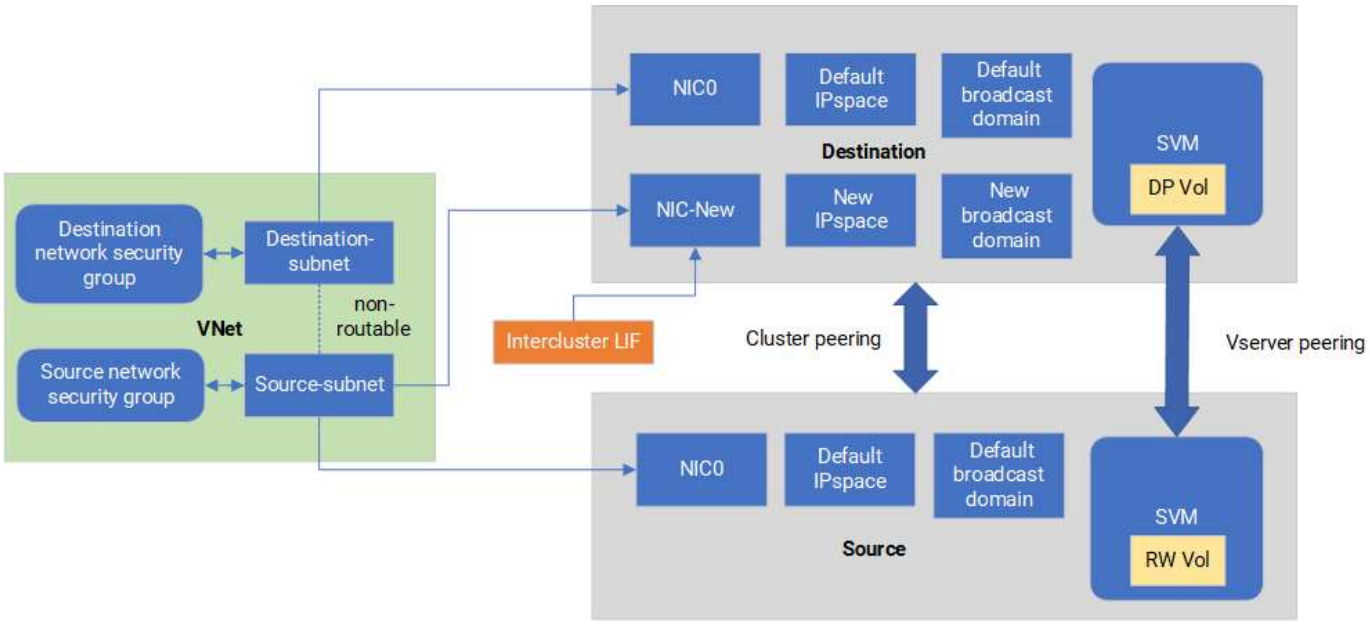
Con Cloud Volumes ONTAP in Azure, puoi separare il traffico di replica SnapMirror dai dati e dal traffico di gestione. Per separare il traffico di replica SnapMirror dal traffico dati, è necessario aggiungere una nuova scheda di interfaccia di rete (NIC), una LIF associata e una subnet non instradabile.

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.

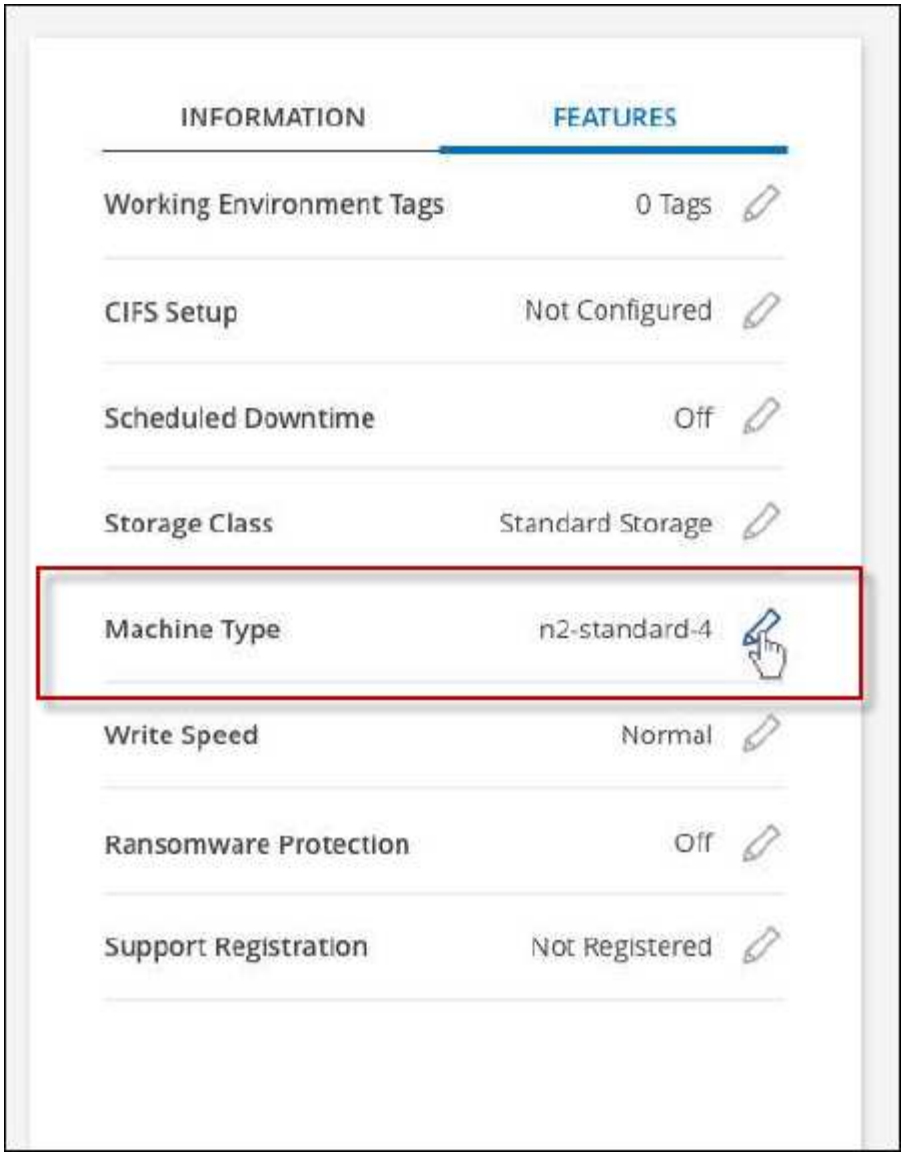
  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

BlueXP cambia un nodo alla volta avviando il takeover e in attesa del giveback. Il team di controllo qualità di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha riscontrato alcun problema sul lato client. Con il variare delle connessioni, alcuni tentativi sono stati osservati a livello di i/o, ma il livello applicativo ha superato il cablaggio 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**.



Se si utilizza una licenza PAYGO (pay-as-you-go) basata su nodi, è possibile scegliere una licenza e un tipo di macchina diversi facendo clic sull'icona a forma di matita accanto a **tipo di licenza**.

1. 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 Gestione di sistema

Le funzionalità avanzate di gestione dello storage in Cloud Volumes ONTAP sono disponibili tramite ONTAP System Manager, un'interfaccia di gestione fornita con i sistemi ONTAP . È possibile accedere a System Manager direttamente da BlueXP.

Caratteristiche

È possibile eseguire diverse funzioni di gestione dello storage utilizzando ONTAP System Manager in BlueXP.

L'elenco seguente include alcune di queste funzionalità, sebbene non sia esaustivo:

- Gestione avanzata dell'archiviazione: gestione di gruppi di coerenza, condivisioni, qtree, quote e VM di archiviazione.
- Spostamento del volume: "Spostare un volume su un aggregato diverso."
- Gestione della rete: gestione di spazi IP, interfacce di rete, set di porte e porte Ethernet.
- Gestisci volumi FlexGroup : puoi creare e gestire volumi FlexGroup solo tramite System Manager. BlueXP non supporta la creazione di volumi FlexGroup .
- Eventi e processi: visualizza registri eventi, avvisi di sistema, processi e registri di controllo.
- Protezione avanzata dei dati: proteggi le VM di storage, le LUN e i gruppi di coerenza.
- Gestione host: configurazione di gruppi di iniziatori SAN e client NFS.
- Gestione dell'archiviazione degli oggetti S3: le funzionalità di gestione dell'archiviazione S3 in Cloud Volumes ONTAP sono disponibili solo in System Manager e non in BlueXP.

Configurazioni supportate

- La gestione avanzata dell'archiviazione tramite ONTAP System Manager è disponibile in Cloud Volumes ONTAP 9.10.0 e versioni successive nelle regioni 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:

- BlueXP tiering: Cloud Volumes ONTAP non supporta il servizio BlueXP tiering . È necessario impostare il tiering dei dati nell'archiviazione degli oggetti direttamente dalla Vista Standard di BlueXP durante la creazione dei volumi.
- Livelli: la gestione degli aggregati (inclusi i livelli locali e cloud) non è supportata da System Manager. È necessario gestire gli aggregati direttamente dalla Vista Standard di BlueXP.
- Aggiornamenti del firmware: Cloud Volumes ONTAP non supporta gli aggiornamenti automatici del firmware dalla pagina **Cluster > Impostazioni**.
- Controllo degli accessi basato sui ruoli: il controllo degli accessi basato sui ruoli da System Manager non è supportato.
- Disponibilità continua SMB (CA): Cloud Volumes ONTAP non supporta "azioni SMB continuamente disponibili" per operazioni non distruttive.

Configurare l'autenticazione per l'accesso a System Manager

In qualità di amministratore, è possibile attivare l'autenticazione per gli utenti che accedono a Gestione sistema ONTAP da BlueXP . È possibile determinare il giusto livello di autorizzazioni di accesso in base ai ruoli utente di ONTAP e abilitare o disabilitare l'autenticazione secondo necessità. Se si abilita l'autenticazione, gli utenti devono immettere le proprie credenziali utente ONTAP ogni volta che accedono a Gestione sistema da BlueXP o quando la pagina viene ricaricata, poiché BlueXP non memorizza internamente le credenziali. Se si disattiva l'autenticazione, gli utenti possono accedere a Gestione sistema utilizzando le credenziali di amministratore di BlueXP .

Questa impostazione è applicabile per BlueXP Connector per gli utenti ONTAP dell'organizzazione o dell'account, indipendentemente dagli ambienti di lavoro Cloud Volumes ONTAP o dai progetti BlueXP .

Autorizzazioni richieste

Per modificare le impostazioni di BlueXP Connector per l'autenticazione utente BlueXP , è necessario assegnare l'organizzazione Cloud Volumes ONTAP o l'account admin Privileges.

Fasi

1. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.
2. Selezionare **Gestisci connettori**.
3. Fare clic sul menu azione ••• per il connettore desiderato e selezionare **Modifica connettore**.
4. In **forza credenziali utente**, selezionare la casella di controllo **Abilita/Disabilita**. Per impostazione predefinita, l'autenticazione è disattivata.

   Se si imposta questo valore su **Abilita**, l'autenticazione viene reimpostata ed è necessario modificare qualsiasi flusso di lavoro esistente per accettare questa modifica.

5. Fare clic su **Save** (Salva).

Inizia subito con System Manager

È possibile accedere a Gestore di sistema di ONTAP da un ambiente di lavoro Cloud Volumes ONTAP.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, selezionare un sistema Cloud Volumes ONTAP.
3. Nel pannello di destra, selezionare **servizi > Gestione sistema > Apri**.
4. Se richiesto, immettere le credenziali utente ONTAP e fare clic su **accesso**.
5. Se viene visualizzato il messaggio di conferma, leggerlo e fare clic su **Chiudi**.
6. Utilizzare Gestione sistema per gestire Cloud Volumes ONTAP.
7. Se necessario, fare clic su **passa alla visualizzazione standard** per tornare alla gestione standard tramite BlueXP.

Guida all'utilizzo di System Manager

Per informazioni dettagliate sull'utilizzo di Gestore di sistema con Cloud Volumes ONTAP, consultare la "Documentazione ONTAP" per le istruzioni dettagliate. Di seguito sono riportati alcuni collegamenti alla documentazione di ONTAP che possono essere utili:

- "Ruoli, applicazioni e autenticazione ONTAP"
- "Utilizzare System Manager per accedere a un cluster".
- "Gestione di volumi e LUN"
- "Gestione della rete"
- "Protezione dei dati"
- "Crea condivisioni SMB costantemente disponibili"

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.

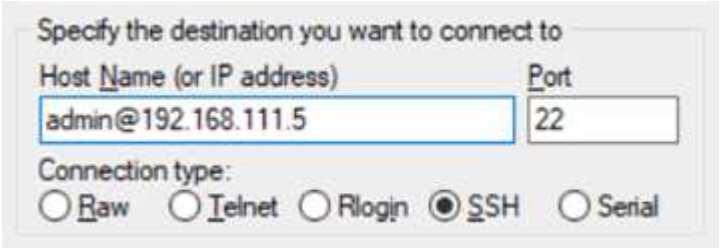
> Quando vengono implementate in più AZS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

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 la configurazione di AutoSupport per Cloud Volumes ONTAP

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.

Le policy di routing e firewall devono consentire il traffico 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.

Se si utilizza una coppia ha, il mediatore ha non richiede l'accesso a Internet in uscita.

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 alla "Documentazione ONTAP: Impostare 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 di ONTAP.

   "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 per i sistemi Cloud Volumes ONTAP

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 alla "Documentazione ONTAP: Panoramica della configurazione EMS" .

Concetti

Licensing

Licensing per Cloud Volumes ONTAP

Per Cloud Volumes ONTAP sono disponibili diverse opzioni di licenza. Ciascuna opzione consente di scegliere un modello di consumo che soddisfi le proprie esigenze.

Panoramica sulle licenze

Per i nuovi clienti sono disponibili le seguenti opzioni di licenza.

Licenze basate sulla capacità
: Paga più sistemi Cloud Volumes ONTAP nel tuo account NetApp in base alla capacità fornita. Include la possibilità di acquistare servizi dati cloud aggiuntivi. Per ulteriori informazioni sui modelli di consumo delle licenze basate sulla capacità, fare riferimento a "Scopri di più sulle licenze basate sulla capacità".

Iscrizione Keystone
: Un servizio pay-as-you-grow e basato su abbonamento che offre un'esperienza di cloud ibrido perfetta per coppie ha (High Availability).

Le sezioni seguenti forniscono ulteriori dettagli su ciascuna di queste opzioni.

Il supporto non è disponibile per l'uso di funzioni con licenza senza licenza.

Licenze basate sulla capacità

I pacchetti di licenza basati sulla capacità consentono di pagare Cloud Volumes ONTAP per TIB di capacità. La licenza è associata al tuo account NetApp e ti consente di addebitare la licenza a più sistemi, purché sia disponibile una capacità sufficiente attraverso la licenza.

Ad esempio, è possibile acquistare una singola licenza 20 TIB, implementare quattro sistemi Cloud Volumes ONTAP e quindi allocare un volume 5 TIB per ciascun sistema, per un totale di 20 TIB. La capacità è disponibile per i volumi su ciascun sistema Cloud Volumes ONTAP implementato in quell'account.

Le licenze basate sulla capacità sono disponibili sotto forma di *pacchetto*. Quando si implementa un sistema Cloud Volumes ONTAP, è possibile scegliere tra diversi pacchetti di licenza in base alle esigenze aziendali.

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 del Cloud Marketplace, nei preventivi di prezzo, nelle descrizioni degli elenchi e in altra documentazione di supporto.

Pacchetti

I seguenti pacchetti basati sulla capacità sono disponibili per Cloud Volumes ONTAP. Per ulteriori informazioni sui pacchetti di licenze basati sulla capacità, fare riferimento a "Scopri di più sulle licenze basate sulla capacità".

Per un elenco dei tipi di VM supportati con i seguenti pacchetti basati sulla capacità, fare riferimento a:

- "Configurazioni supportate in Azure"
- "Configurazioni supportate in Google Cloud"

Freemium

Fornisce tutte le funzionalità Cloud Volumes ONTAP gratuitamente da NetApp (sono ancora applicati i costi per i cloud provider). Un pacchetto Freemium ha le seguenti caratteristiche:

- Non sono necessari contratti o licenze.
- Il supporto di NetApp non è incluso.
- La capacità di provisioning per sistema Cloud Volumes ONTAP è limitata a 500 GiB.
- Puoi utilizzare fino a 10 sistemi Cloud Volumes ONTAP con l'offerta Freemium per account NetApp, per qualsiasi cloud provider.
- Se la capacità sottoposta a provisioning per un sistema Cloud Volumes ONTAP supera i 500 GiB, BlueXP converte il sistema in un pacchetto Essentials.

  Non appena un sistema viene convertito nel pacchetto Essentials, "carica minima"lo applica.

  Un sistema Cloud Volumes ONTAP che è stato convertito in un pacchetto Essentials non può essere commutato nuovamente su Freemium anche se la capacità fornita è ridotta a meno di 500 GiB. Altri sistemi con meno di 500 GiB di capacità fornita utilizzano Freemium (a condizione che siano implementati utilizzando l'offerta Freemium).

Elementi essenziali

Puoi pagare in base alla capacità in diverse configurazioni:

- Scegli la tua configurazione Cloud Volumes ONTAP:
  - Un singolo nodo o sistema ha
  - Storage a blocchi e file o dati secondari per disaster recovery (DR)
- Aggiungi qualsiasi servizio dati cloud di NetApp a un costo aggiuntivo

Professionale

Paga in base alla capacità per qualsiasi tipo di configurazione Cloud Volumes ONTAP con backup illimitati.

- Fornisce licenze per qualsiasi configurazione Cloud Volumes ONTAP

  Nodo singolo o ha con carica della capacità per volumi primari e secondari alla stessa velocità

- Include backup di volumi illimitati utilizzando il backup e il ripristino BlueXP, ma solo per i sistemi Cloud Volumes ONTAP che utilizzano il pacchetto Professional.

  > Per il backup e il ripristino di BlueXP è richiesto un abbonamento PAY-as-you-go (PAYGO), tuttavia non sono previsti costi per l'utilizzo di questo servizio. Per ulteriori informazioni sull'impostazione delle licenze per il backup e il ripristino di BlueXP , consultare "Impostare le licenze per il backup e ripristino BlueXP" .

- Aggiungi qualsiasi servizio dati cloud di NetApp a un costo aggiuntivo

Disponibilità di licenze basate sulla capacità

La disponibilità delle licenze PAYGO e BYOL per i sistemi Cloud Volumes ONTAP richiede che BlueXP Connector sia attivo e funzionante. Per ulteriori informazioni, fare riferimento a "Scopri di più sui connettori".

> NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAPP" .

Come iniziare

Scopri come iniziare a utilizzare le licenze basate sulla capacità:

- "Impostare la licenza per Cloud Volumes ONTAP in AWS"
- "Impostare la licenza per Cloud Volumes ONTAP in Azure"
- "Impostare la licenza per Cloud Volumes ONTAP in Google Cloud"

Iscrizione Keystone

Un servizio pay-as-you-grow basato su abbonamento che offre un'esperienza di cloud ibrido perfetta per coloro che preferiscono i modelli di consumo OpEx per la gestione anticipata di CapEx o il leasing.

La ricarica si basa sulle dimensioni della capacità impegnata per una o più coppie Cloud Volumes ONTAP ha nel tuo abbonamento Keystone.

La capacità fornita per ciascun volume viene aggregata e confrontata periodicamente con la capacità impegnata del tuo abbonamento Keystone e gli eventuali superamenti vengono addebitati come burst sul tuo abbonamento Keystone.

"Scopri di più su NetApp Keystone".

Configurazioni supportate

Gli abbonamenti Keystone sono supportati con le coppie ha. Al momento, questa opzione di licenza non è supportata dai sistemi a nodo singolo.

Limite di capacità

Nel modello di licenza basato sulla capacità, ogni sistema Cloud Volumes ONTAP supporta la suddivisione in livelli per l'archiviazione di oggetti e la capacità totale suddivisa in livelli può essere scalata fino al limite del bucket del provider cloud. Sebbene la licenza non imponga restrizioni di capacità, seguire le "Migliori pratiche FabricPool" per garantire prestazioni ottimali, affidabilità ed efficienza dei costi durante la configurazione e la gestione del tiering.

Per informazioni sui limiti di capacità di ciascun provider cloud, fare riferimento alla relativa documentazione:

- "Documentazione AWS"
- "Documentazione di Azure per i dischi gestiti"E "Documentazione di Azure per l'archiviazione BLOB"
- "Documentazione di Google Cloud"

Come iniziare

Scopri come iniziare con un abbonamento Keystone:

- "Impostare la licenza per Cloud Volumes ONTAP in AWS"
- "Impostare la licenza per Cloud Volumes ONTAP in Azure"
- "Impostare la licenza per Cloud Volumes ONTAP in Google Cloud"

Licenze basate su nodo

La licenza basata su nodo è il modello di licenza di generazione precedente che consente di concedere in licenza Cloud Volumes ONTAP per nodo. Questo modello di licenza non è disponibile per i nuovi clienti. La carica per nodo è stata sostituita con i metodi di carica per capacità descritti in precedenza.

NetApp ha pianificato la fine della disponibilità (EOA) e il supporto (EOS) delle licenze basate su nodi. Dopo la fine dell'EOS e la fine dell'anno, le licenze basate su nodi dovranno essere convertite in licenze basate sulla capacità.

Per informazioni, fare riferimento alla "Comunicazione con i clienti: CPC-00589".

Fine della disponibilità delle licenze basate su nodi

A partire dall'11 novembre 2024, la disponibilità limitata delle licenze basate sui nodi è terminata. Il supporto per le licenze basate sui nodi termina il 31 dicembre 2024.

Se si dispone di un contratto valido basato su nodi che si estende oltre la data di fine disponibilità, è possibile continuare a utilizzare la licenza fino alla scadenza del contratto. Una volta scaduto il contratto, sarà necessario passare al modello di licenza basato sulla capacità. Se non si dispone di un contratto a lungo termine per un nodo Cloud Volumes ONTAP, è importante pianificare la conversione prima della data EOS.

Questa tabella fornisce ulteriori informazioni su ciascun tipo di licenza e sull'impatto della fine disponibilità sul reparto IT:

Tipo di licenza	Impatto dopo la fine del ciclo di vita
Licenza valida basata su nodi acquistata tramite Bring Your Own License (BYOL)	La licenza rimane valida fino alla scadenza. È possibile utilizzare le licenze non utilizzate esistenti basate su nodi per implementare nuovi sistemi Cloud Volumes ONTAP.
Licenza scaduta basata su nodi acquistata tramite BYOL	Non si avrà diritto a distribuire nuovi sistemi Cloud Volumes ONTAP utilizzando questa licenza. I sistemi esistenti potrebbero continuare a funzionare, ma non si riceverà alcun supporto o aggiornamento per i sistemi dopo la data EOS.
Licenza valida basata su nodi con iscrizione PAYGO	Cesserà di ricevere il supporto NetApp dopo la data di EOS, fino a quando l'utente non effettuerà la transizione a una licenza basata sulla capacità.

Esclusioni

NetApp riconosce che determinate situazioni richiedono particolare attenzione e la fine a ed EOS delle licenze basate su nodi non si applicano ai seguenti casi:

- Clienti USA del settore pubblico

- Implementazioni in modalità privata
- Implementazioni nella regione cinese di Cloud Volumes ONTAP in AWS

Per questi scenari particolari, NetApp offrirà supporto per soddisfare i requisiti di licenza esclusivi in conformità agli obblighi contrattuali e alle esigenze operative.

Anche in questi scenari, i rinnovi di licenze e le nuove licenze basate su nodi sono validi per un massimo di un anno dalla data di approvazione.

Conversione della licenza

BlueXP permette una conversione perfetta delle licenze basate su nodi in base alla capacità grazie al tool di conversione della licenza. Per informazioni sulla fine disponibilità delle licenze basate su nodi, fare riferimento alla "Fine della disponibilità delle licenze basate su nodi".

Prima di procedere alla transizione, è opportuno familiarizzare con la differenza tra i due modelli di licenza. La licenza basata su nodi include capacità fissa per ogni istanza di ONTAP, che può limitare la flessibilità. Le licenze basate sulla capacità, invece, consentono di creare un pool di storage condiviso su più istanze, offrendo una maggiore flessibilità, ottimizzando l'utilizzo delle risorse e riducendo il potenziale di penalizzazione finanziaria durante la ridistribuzione dei carichi di lavoro. La ricarica basata sulla capacità si adatta perfettamente ai requisiti di storage in continua evoluzione.

Per informazioni su come eseguire questa conversione, fare riferimento alla "Converti una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità".

La conversione di un sistema da licenze basate sulla capacità a licenze basate su nodi non è supportata.

Scopri di più sulle licenze basate sulla capacità per Cloud Volumes ONTAP

Dovresti conoscere l'addebito e l'utilizzo della capacità delle licenze basate sulla capacità

Modelli di consumo

I pacchetti di licenza basati sulla capacità sono disponibili con i seguenti modelli di consumo:

- **BYOL**: Bring Your Own License (BYOL). Una licenza acquistata da NetApp, che può essere utilizzata per implementare Cloud Volumes ONTAP in qualsiasi cloud provider.

  NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

- **PAYGO**: Un abbonamento pay-as-you-go (PAYGO) è un abbonamento orario dal mercato del tuo cloud provider.
- **Annuale**: Un contratto annuale dal mercato del tuo cloud provider.

Tenere presente quanto segue:

- Se acquisti una licenza da NetApp (BYOL), devi anche abbonarti all'offerta PAYGO dal marketplace del tuo provider cloud. NetApp ha limitato le licenze BYOL. Alla scadenza delle licenze BYOL, dovrai sostituirle con abbonamenti al marketplace cloud.

La tua licenza viene sempre addebitata per prima, ma ti verrà addebitato il costo della tariffa oraria sul mercato nei seguenti casi:

  - Se si supera la capacità concessa in licenza
  - Se il periodo di validità della licenza scade

- Se disponi di un contratto annuale da un marketplace, *tutti* i sistemi Cloud Volumes ONTAP implementati vengono addebitati in base a tale contratto. Non puoi combinare un contratto di mercato annuale con BYOL.
- Nelle regioni cinesi sono supportati solo sistemi a singolo nodo con BYOL. Le distribuzioni nella regione cinese sono esenti dalle restrizioni di licenza BYOL.

Cambiare i pacchetti

Dopo l'implementazione, è possibile modificare il pacchetto per un sistema Cloud Volumes ONTAP che utilizza licenze basate sulla capacità. Ad esempio, se hai implementato un sistema Cloud Volumes ONTAP con il pacchetto Essentials, puoi cambiarlo nel pacchetto Professional se le tue esigenze di business sono cambiate.

"Scopri come modificare i metodi di ricarica".

Per informazioni sulla conversione delle licenze basate su nodi in licenze basate sulla capacità, vedere

Prezzi e configurazioni supportate

Per i dettagli sui prezzi, vai a "Sito Web di NetApp BlueXP" .

I pacchetti di licenza basati sulla capacità sono disponibili con Cloud Volumes ONTAP 9.7 e versioni successive.

VM di storage

- Non sono previsti costi di licenza aggiuntivi per le SVM (Data-Serving Storage VM), ma è previsto un costo di capacità minimo di 4 TIB per SVM di servizio dati.
- Le SVM per il disaster recovery vengono addebitate in base alla capacità fornita.

Coppie HA

Per le coppie ha, il costo viene addebitato solo per la capacità fornita su un nodo. I dati sottoposti a mirroring sincrono sul nodo partner non vengono addebitati.

Volumi FlexClone e FlexCache

- La capacità utilizzata dai volumi FlexClone non verrà addebitata.
- I volumi FlexCache di origine e di destinazione sono considerati dati primari e addebitati in base allo spazio fornito.

Limite di capacità

Nel modello di licenza basato sulla capacità, ogni sistema Cloud Volumes ONTAP supporta la suddivisione in livelli per l'archiviazione di oggetti e la capacità totale suddivisa in livelli può essere scalata fino al limite del bucket del provider cloud. Sebbene la licenza non imponga restrizioni di capacità, seguire le "Migliori pratiche FabricPool" per garantire prestazioni ottimali, affidabilità ed efficienza dei costi durante la configurazione e la gestione del tiering.

Per informazioni sui limiti di capacità di ciascun provider cloud, fare riferimento alla relativa documentazione:

- "Documentazione AWS"
- "Documentazione di Azure per i dischi gestiti"E "Documentazione di Azure per l'archiviazione BLOB"
- "Documentazione di Google Cloud"

Numero massimo di sistemi

Con le licenze basate sulla capacità, il numero massimo di sistemi Cloud Volumes ONTAP è limitato a 24 per account BlueXP . Un *sistema* è una coppia Cloud Volumes ONTAP ha, un sistema a nodo singolo Cloud Volumes ONTAP o qualsiasi altra VM storage creata. La VM di storage predefinita non viene contata rispetto al limite. Questo limite si applica a tutti i modelli di licenza.

Ad esempio, supponiamo di disporre di tre ambienti di lavoro:

- Un sistema Cloud Volumes ONTAP a nodo singolo con una VM di storage (si tratta della VM di storage predefinita creata durante l'implementazione di Cloud Volumes ONTAP)

  Questo ambiente di lavoro conta come un unico sistema.

- Un sistema Cloud Volumes ONTAP a nodo singolo con due VM di storage (la VM di storage predefinita, più una VM di storage aggiuntiva creata dall'utente)

  Questo ambiente di lavoro conta come due sistemi: Uno per il sistema a nodo singolo e uno per la VM di storage aggiuntiva.

- Una coppia Cloud Volumes ONTAP ha con tre VM storage (la VM storage predefinita, più due VM storage aggiuntive create)

  Questo ambiente di lavoro conta tre sistemi: Uno per la coppia ha e due per le VM storage aggiuntive.

Si tratta di sei sistemi in totale. Avrai quindi spazio per altri 14 sistemi nel tuo account.

Se si dispone di un'implementazione di grandi dimensioni che richiede più di 24 sistemi, contattare il rappresentante dell'account o il team di vendita.

"Scopri di più sugli account BlueXP".

"Scopri i limiti di archiviazione per AWS, Azure e Google Cloud".

Note sulla ricarica

I seguenti dettagli consentono di comprendere il funzionamento della ricarica con le licenze basate sulla capacità.

Costo minimo

È previsto un costo minimo di 4 TIB per ciascuna VM di storage che fornisce dati e che dispone di almeno un volume primario (lettura/scrittura). Se la somma dei volumi primari è inferiore a 4 TIB, BlueXP applica la carica minima di 4 TIB a quella VM di storage.

Se non hai ancora effettuato il provisioning di volumi, il costo minimo non viene applicato.

Per il pacchetto Essentials, la tariffa per la capacità minima di 4 TiB non si applica alle VM di archiviazione che

contengono solo volumi secondari (di protezione dei dati). Ad esempio, se si dispone di una VM di archiviazione con 1 TiB di dati secondari, verrà addebitato solo quel 1 TiB di dati. Con il tipo di pacchetto Professional, la capacità minima di ricarica di 4 TiB si applica indipendentemente dal tipo di volume.

Eccedendo

Se superi la capacità BYOL, ti verranno addebitati i costi aggiuntivi a tariffe orarie basate sul tuo abbonamento al marketplace. I costi aggiuntivi vengono addebitati alle tariffe del marketplace, con preferenza per l'utilizzo prioritario della capacità disponibile da altre licenze. Se la tua licenza BYOL scade, dovrai passare a un modello di licenza basato sulla capacità tramite i marketplace cloud.

Pacchetto Essentials

Con il pacchetto Essentials, l'addebito viene effettuato in base al tipo di implementazione (ha o nodo singolo) e al tipo di volume (primario o secondario). I prezzi da alto a basso sono nel seguente ordine: *Essentials Primary ha*, *Essentials Primary Single Node*, *Essentials Secondary ha* e *Essentials Secondary Single Node*. In alternativa, quando acquisti un contratto di marketplace o accetti un'offerta privata, le spese in termini di capacità saranno identiche per qualsiasi tipo di implementazione o volume.

Il licensing si basa interamente sul tipo di volume creato all'interno dei sistemi Cloud Volumes ONTAP:

- Nodo singolo Essentials: Volumi in lettura/scrittura creati in un sistema Cloud Volumes ONTAP usando solo un nodo ONTAP.
- Essentials ha: Volumi in lettura/scrittura utilizzando due nodi ONTAP in grado di eseguire il failover l'uno sull'altro per un accesso ai dati senza interruzioni.
- Essentials Secondary Single Node: Volumi di tipo Data Protection (DP), generalmente volumi di destinazione SnapMirror o SnapVault di sola lettura, creati in un sistema Cloud Volumes ONTAP usando solo un nodo ONTAP.

> Se un volume di sola lettura/DP diventa un volume primario, BlueXP lo considera come dati primari e i costi di addebito vengono calcolati in base al tempo in cui il volume si trovava in modalità di lettura/scrittura. Quando il volume viene nuovamente reso di sola lettura/DP, BlueXP lo considera nuovamente come dati secondari e addebita di conseguenza utilizzando la migliore licenza corrispondente nel portafoglio digitale.

- Essentials ha secondaria: Volumi di tipo data Protection (DP) (di norma volumi di destinazione SnapMirror o SnapVault di sola lettura) creati in un sistema Cloud Volumes ONTAP utilizzando due nodi ONTAP in grado di eseguire il failover tra di loro per un accesso ai dati senza interruzioni.

BYOL

Se hai acquistato una licenza Essentials da NetApp (BYOL) e superi la capacità concessa in licenza per quel tipo di implementazione e volume, il Digital Wallet di BlueXP addebiterà le spese eccessive rispetto a una licenza Essentials a prezzo più elevato (se disponibile). Questo accade perché utilizziamo prima la capacità disponibile che hai già acquistato come capacità prepagata prima di addebitare sul mercato. In assenza di capacità disponibile con la licenza BYOL, tale capacità superata verrà addebitata alle tariffe orarie on-demand del marketplace (PAYGO) e aggiungerà i costi alla fattura mensile.

Ecco un esempio. Supponiamo di disporre delle seguenti licenze per il pacchetto Essentials:

- Una licenza 500 TIB *Essentials Secondary ha* con 500 TIB di capacità impegnata
- Una licenza 500 TIB *Essentials Single Node* che ha solo 100 TIB di capacità impegnata

Un altro 50 TIB viene fornito su una coppia ha con volumi secondari. Invece di addebitare 50 TIB a PAYGO, il

portafoglio digitale BlueXP addebita il 50 TIB in eccesso rispetto alla licenza *Essentials Single Node*. Tale licenza ha un prezzo superiore a *Essentials Secondary ha*, ma utilizza una licenza già acquistata e non aggiunge costi alla fattura mensile.

Nel portafoglio digitale BlueXP, il 50 TIB verrà indicato come addebitato rispetto alla licenza *Essentials Single Node*.

Ecco un altro esempio. Supponiamo di disporre delle seguenti licenze per il pacchetto Essentials:

- Una licenza 500 TIB *Essentials Secondary ha* con 500 TIB di capacità impegnata
- Una licenza 500 TIB *Essentials Single Node* che ha solo 100 TIB di capacità impegnata

Un altro TIB 100 viene sottoposto a provisioning su una coppia ha con volumi primari. La licenza acquistata non dispone di *Essentials Primary ha* commit Capacity. Il prezzo della licenza *Essentials Primary ha* è superiore a quello delle licenze *Essentials Primary Single Node* e *Essentials Secondary ha*.

In questo esempio, il Digital Wallet di BlueXP addebita le spese eccessive alla tariffa di marketplace per i 100 TiB aggiuntivi. Le spese di eccedenza compariranno sulla vostra fattura mensile.

Contratti di mercato o offerte private

Se hai acquistato una licenza Essentials come parte di un contratto di marketplace o di un'offerta privata, la logica BYOL non si applica e devi disporre dell'esatto tipo di licenza per l'utilizzo. Il tipo di licenza include il tipo di volume (primario o secondario) e il tipo di implementazione (ha o nodo singolo).

Ad esempio, supponiamo di distribuire un'istanza di Cloud Volumes ONTAP con la licenza Essentials. Esegui quindi il provisioning dei volumi in lettura-scrittura (nodo singolo primario) e di sola lettura (nodo singolo secondario). Il contratto del marketplace o l'offerta privata deve includere la capacità di *Essentials Single Node* e *Essentials Secondary Single Node* per coprire la capacità fornita. Tutte le capacità fornite che non fanno parte del contratto del marketplace o dell'offerta privata verranno addebitate alle tariffe orarie on-demand (PAYGO) e aggiungeranno i costi alla fattura mensile.

Storage

Protocolli client supportati per Cloud Volumes ONTAP

Cloud Volumes ONTAP supporta i protocolli client iSCSI, NFS, SMB, NVMe-TCP e S3.

ISCSI

ISCSI è un protocollo a blocchi che può essere eseguito su reti Ethernet standard. La maggior parte dei sistemi operativi client offre un iniziatore software che viene eseguito su una porta Ethernet standard.

NFS

NFS è il protocollo di accesso ai file tradizionale per i sistemi UNIX e LINUX. I client possono accedere ai file nei volumi ONTAP utilizzando i protocolli NFSv3, NFSv4 e NFSv4.1. È possibile controllare l'accesso ai file utilizzando permessi di stile UNIX, permessi di stile NTFS o una combinazione di entrambi.

I client possono accedere agli stessi file utilizzando i protocolli NFS e SMB.

PMI

SMB è il protocollo di accesso ai file tradizionale per i sistemi Windows. I client possono accedere ai file nei

volumi ONTAP utilizzando i protocolli SMB 2.0, SMB 2.1, SMB 3.0 e SMB 3.1.1. Come per NFS, sono supportati diversi stili di permesso.

S3

Cloud Volumes ONTAP supporta S3 come opzione per lo storage scale-out. Il supporto del protocollo S3 consente di configurare l'accesso del client S3 agli oggetti contenuti in un bucket in una VM di storage (SVM).

"Documentazione ONTAP: Scopri come funziona il protocollo S3". "Documentazione di ONTAP: Scopri come configurare e gestire i servizi di storage a oggetti S3 in ONTAP".

NVMe-TCP

A partire dalla versione 9.12.1 di ONTAP, NVMe-TCP è supportato per i cloud provider. BlueXP non fornisce alcuna funzionalità di gestione per NVMe-TCP.

Per ulteriori informazioni sulla configurazione di NVMe tramite ONTAP, fare riferimento alla "Documentazione di ONTAP: Configurare una VM storage per NVMe" .

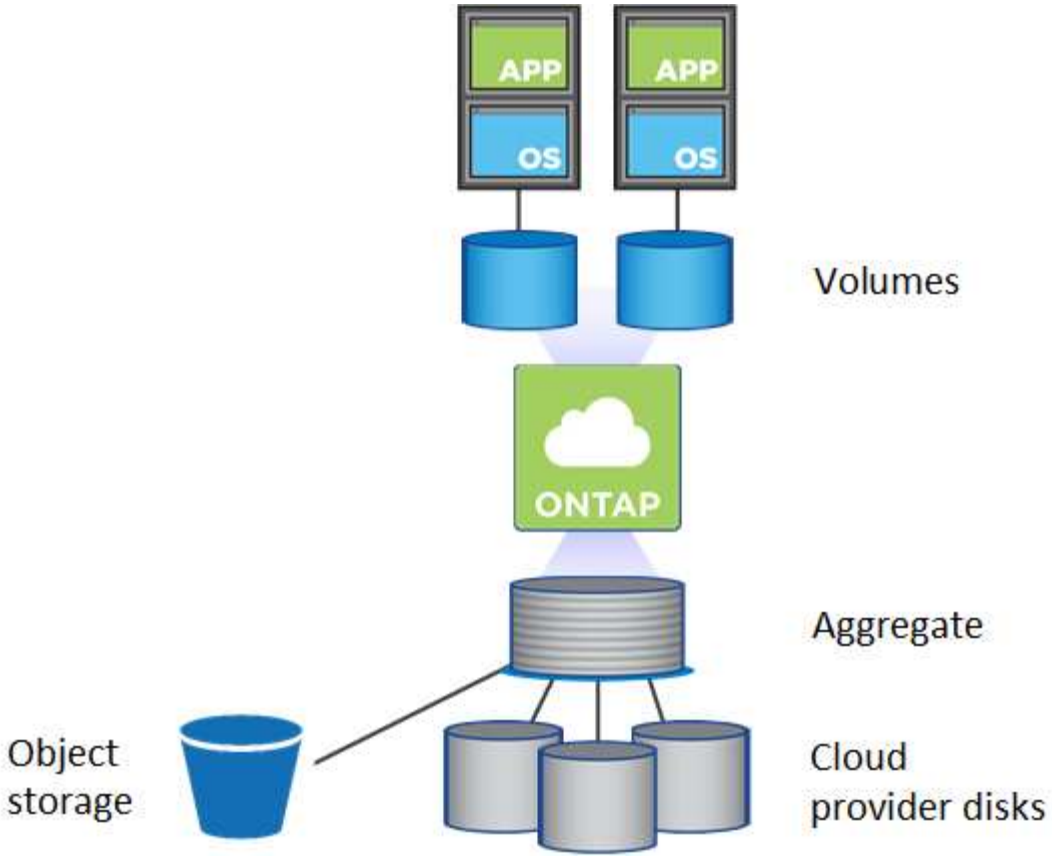
Dischi e aggregati utilizzati per i cluster Cloud Volumes ONTAP

Comprendere come Cloud Volumes ONTAP utilizza il cloud storage può aiutarti a comprendere i costi dello storage.

> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da 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.

Panoramica

Cloud Volumes ONTAP utilizza lo storage del cloud provider come dischi e li raggruppa in uno o più aggregati. Gli aggregati forniscono storage a uno o più volumi.



Sono supportati diversi tipi di dischi cloud. Quando si crea un volume e si sceglie il tipo di disco e la dimensione predefinita del disco quando si implementa Cloud Volumes ONTAP.

La quantità totale di storage acquistata da un cloud provider è la *capacità raw*. La *capacità utilizzabile* è inferiore perché circa il 12-14% è un overhead riservato all'utilizzo di Cloud Volumes ONTAP. Ad esempio, se BlueXP crea un aggregato da 500 GiB, la capacità utilizzabile è di 442.94 GiB.

Storage AWS

In AWS, Cloud Volumes ONTAP utilizza lo storage EBS per i dati dell'utente e lo storage NVMe locale come cache flash su alcuni tipi di istanze EC2.

Storage EBS

In AWS, un aggregato può contenere fino a 6 dischi delle stesse dimensioni. Tuttavia, se si dispone di una configurazione che supporta la funzione Amazon EBS Elastic Volumes, un aggregato può contenere fino a 8 dischi. "Scopri di più sul supporto per volumi elastici".

La dimensione massima del disco è 16 TIB.

Il tipo di disco EBS sottostante può essere SSD General Purpose (gp3 o gp2), SSD IOPS con provisioning (io1) o HDD con throughput ottimizzato (st1). È possibile associare un disco EBS con Amazon S3 a "storage a oggetti a basso costo".

Si sconsiglia di eseguire il tiering dei dati sullo storage a oggetti quando si utilizzano HDD ottimizzati per il throughput (st1).

Storage NVMe locale

Alcuni tipi di istanze EC2 includono lo storage NVMe locale, utilizzato da Cloud Volumes ONTAP "Flash cache".

Link correlati

- "Documentazione AWS: Tipi di volume EBS"
- "Scopri come scegliere i tipi di dischi e le dimensioni dei dischi per i tuoi sistemi in AWS"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in AWS"
- "Analisi delle configurazioni supportate per Cloud Volumes ONTAP in AWS"

Storage Azure

In Azure, un aggregato può contenere fino a 12 dischi delle stesse dimensioni. Il tipo di disco e le dimensioni massime dipendono dall'utilizzo di un sistema a nodo singolo o di una coppia ha:

Sistemi a nodo singolo

I sistemi a nodo singolo possono utilizzare questi tipi di dischi gestiti di Azure:

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- *Dischi gestiti Premium SSD da v2 GB* offrono prestazioni più elevate con latenza inferiore a un costo inferiore sia per coppie ha che per nodo singolo, rispetto ai dischi gestiti Premium SSD.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.
- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

  Ogni tipo di disco gestito ha una dimensione massima di 32 TIB.

  È possibile associare un disco gestito con l'archiviazione BLOB di Azure a "storage a oggetti a basso costo".

Coppie HA

Le coppie HA utilizzano due tipi di dischi che offrono performance elevate per i carichi di lavoro i/o-intensive a un costo più elevato:

- *Premium page blob* con una dimensione massima del disco di 8 TIB
- *Dischi gestiti* con una dimensione massima del disco di 32 TIB

Link correlati

- "Scopri come scegliere i tipi di dischi e le dimensioni dei dischi per i tuoi sistemi in Azure"
- "Lancia una coppia ha Cloud Volumes ONTAP in Azure"
- "Documentazione di Microsoft Azure: Tipi di dischi gestiti da Azure"
- "Documentazione di Microsoft Azure: Panoramica delle pagine di Azure"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in Azure"

Storage Google Cloud

In Google Cloud, un aggregato può contenere fino a 6 dischi delle stesse dimensioni. La dimensione massima del disco è 64 TIB.

Il tipo di disco può essere *dischi persistenti SSD Zonal*, *dischi persistenti bilanciati Zonal* o *dischi persistenti standard Zonal*. È possibile associare i dischi persistenti con un bucket Google Storage a "storage a oggetti a basso costo".

Link correlati

- "Documentazione di Google Cloud: Opzioni di storage"
- "Esamina i limiti di storage per Cloud Volumes ONTAP in Google Cloud"

Tipo RAID

Il tipo di RAID per ciascun aggregato Cloud Volumes ONTAP è RAID0 (striping). Cloud Volumes ONTAP si affida al cloud provider per la disponibilità e la durata dei dischi. Non sono supportati altri tipi di RAID.

Hot spare

RAID0 non supporta l'utilizzo di hot spare per la ridondanza.

La creazione di dischi inutilizzati (hot spare) collegati a un'istanza di Cloud Volumes ONTAP è una spesa non necessaria e può impedire il provisioning di spazio aggiuntivo in base alle necessità. Pertanto, non è consigliato.

Scopri di più sul supporto per volumi elastici AWS con Cloud Volumes ONTAP

Il supporto per la funzionalità dei volumi elastici di Amazon EBS con un aggregato Cloud Volumes ONTAP offre performance migliori e capacità aggiuntiva, consentendo a BlueXP di aumentare automaticamente la capacità del disco sottostante in base alle necessità.

Benefici

- Crescita dinamica dei dischi

  BlueXP può aumentare dinamicamente le dimensioni dei dischi mentre Cloud Volumes ONTAP è in esecuzione e mentre i dischi sono ancora collegati.

- Migliori performance

  Gli aggregati abilitati con volumi elastici possono avere fino a otto dischi che vengono utilizzati in modo uguale in due gruppi RAID. Questa configurazione offre un throughput maggiore e performance costanti.

- Aggregati più grandi

  Il supporto per otto dischi offre una capacità aggregata massima di 128 TIB. Questi limiti sono superiori al limite di sei dischi e al limite di 96 TIB per gli aggregati che non sono abilitati con la funzione Elastic Volumes.

  Si noti che i limiti di capacità totale del sistema rimangono invariati.

"Documentazione AWS: Scopri di più sui volumi elastici AWS"

Configurazioni supportate

La funzione Amazon EBS Elastic Volumes è supportata con versioni Cloud Volumes ONTAP specifiche e tipi di dischi EBS specifici.

Versione di Cloud Volumes ONTAP

La funzione Elastic Volumes è supportata con i *nuovi* sistemi Cloud Volumes ONTAP creati a partire dalla versione 9.11.0 o successiva. La funzionalità è *non* supportata con i sistemi Cloud Volumes ONTAP esistenti implementati prima del 9.11.0.

Ad esempio, la funzione Elastic Volumes (volumi elastici) non è supportata se è stato creato un sistema Cloud Volumes ONTAP 9.9.0 e successivamente aggiornato alla versione 9.11.0. Deve essere un nuovo sistema distribuito utilizzando la versione 9.11.0 o successiva.

Tipi di dischi EBS

La funzione Elastic Volumes (volumi elastici) viene attivata automaticamente a livello di aggregato quando si utilizzano SSD General Purpose (gp3) o SSD IOPS con provisioning (io1). La funzione Elastic Volumes non è supportata con aggregati che utilizzano altri tipi di disco.

Autorizzazioni AWS richieste

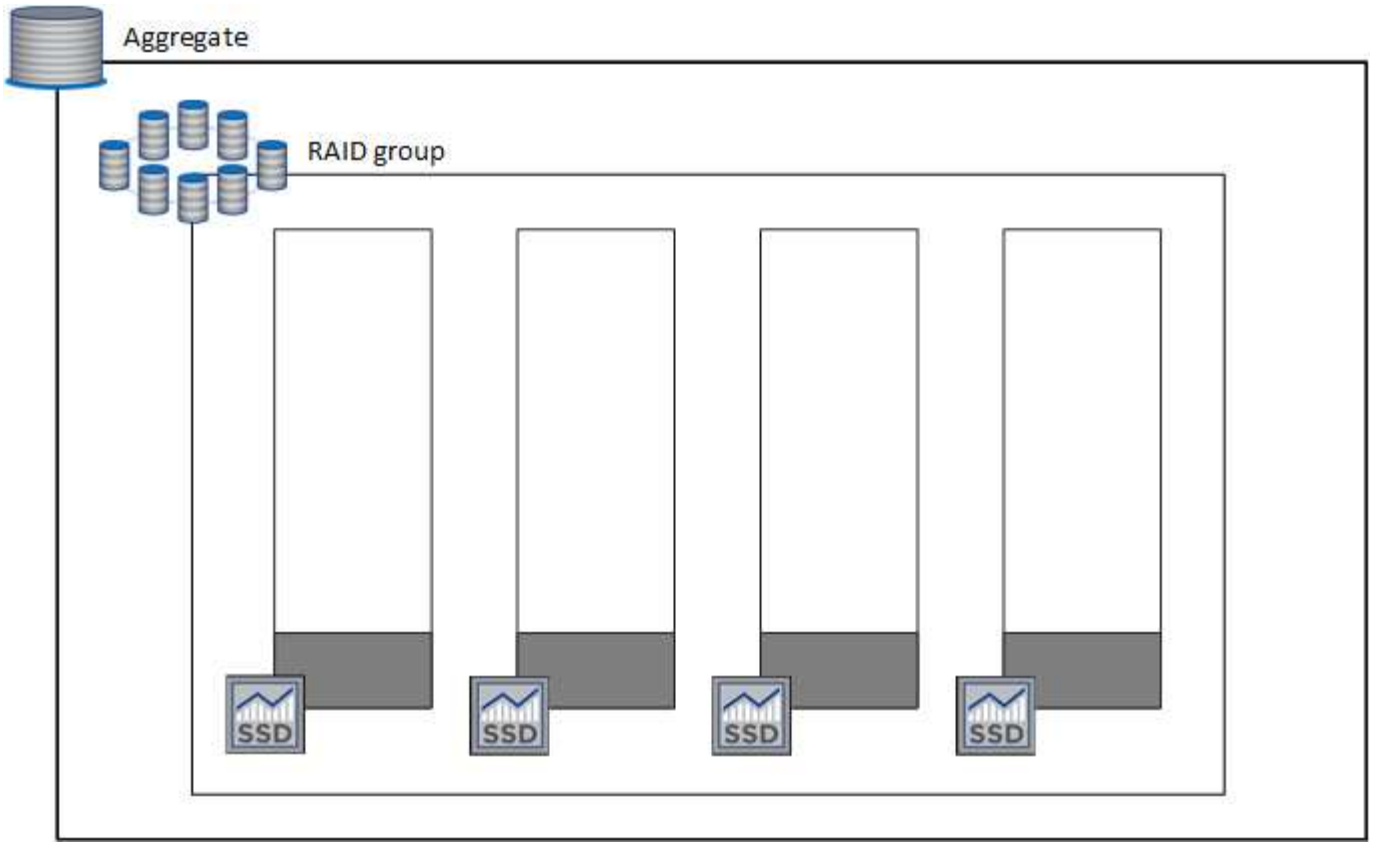
A partire dalla versione 3.9.19, il connettore richiede le seguenti autorizzazioni per attivare e gestire la funzione Elastic Volumes su un aggregato Cloud Volumes ONTAP:

- ec2:DescripteVolumesModificazioni
- ec2:ModifyVolume

Queste autorizzazioni sono incluse in "Le policy fornite da NetApp"

Come funziona il supporto per i volumi elastici

Un aggregato con la funzione Elastic Volumes attivata è costituito da uno o due gruppi RAID. Ogni gruppo RAID ha quattro dischi identici che hanno la stessa capacità. Ecco un esempio di aggregato 10 TIB con quattro dischi da 2.5 TIB ciascuno:



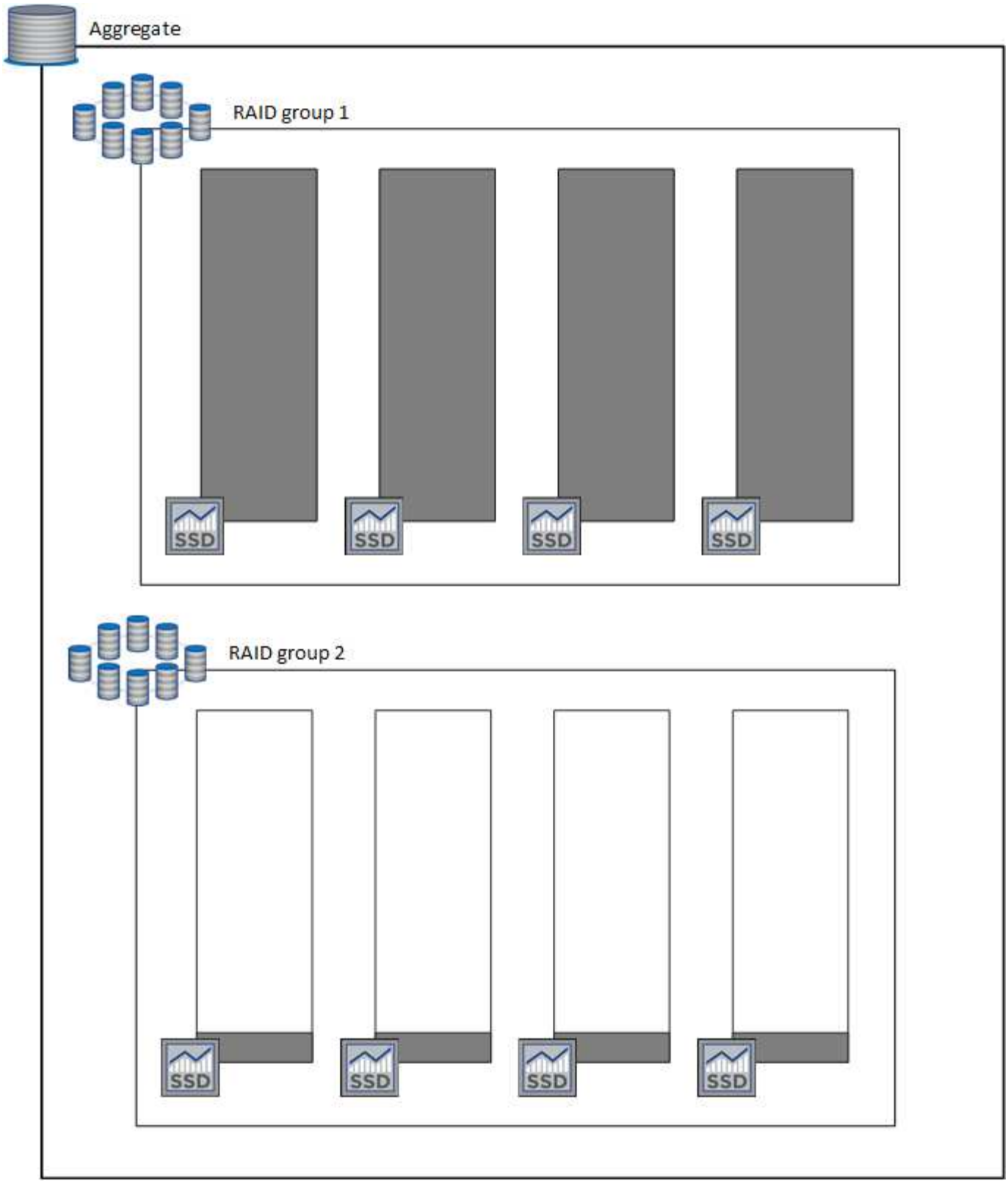
Quando BlueXP crea un aggregato, inizia con un gruppo RAID. Se è necessaria una capacità aggiuntiva, BlueXP aumenta l'aggregato aumentando la capacità di tutti i dischi nel gruppo RAID della stessa quantità. L'aumento di capacità è pari o a un minimo di 256 GiB o al 10% delle dimensioni dell'aggregato.

Ad esempio, se si dispone di un aggregato 1 TIB, ogni disco è 250 GiB. Il 10% della capacità aggregata è di 100 GiB. Si tratta di un valore inferiore a 256 GiB, pertanto le dimensioni dell'aggregato sono aumentate di almeno 256 GiB (o 64 GiB per ciascun disco).

BlueXP aumenta le dimensioni dei dischi mentre il sistema Cloud Volumes ONTAP è in esecuzione e mentre i dischi sono ancora collegati. Il cambiamento è senza interruzioni.

Se un aggregato raggiunge 64 TIB (o 16 TIB su ciascun disco), BlueXP crea un secondo gruppo RAID per una capacità aggiuntiva. Questo secondo gruppo RAID funziona esattamente come il primo: Dispone di quattro dischi con la stessa capacità e può crescere fino a 64 TIB. Ciò significa che un aggregato può avere una capacità massima di 128 TIB.

Ecco un esempio di aggregato con due gruppi RAID. Il limite di capacità è stato raggiunto sul primo gruppo RAID, mentre i dischi nel secondo gruppo RAID hanno molto spazio libero.



Cosa accade quando si crea un volume

Se si crea un volume che utilizza dischi gp3 o io1, BlueXP crea il volume su un aggregato come segue:

- Se esiste già un aggregato gp3 o io1 con volumi elastici attivati, BlueXP crea il volume su quell'aggregato.
- Se sono presenti più aggregati gp3 o io1 con volumi elastici attivati, BlueXP crea il volume sull'aggregato

che richiede la minore quantità di risorse.

- Se il sistema dispone solo di aggregati gp3 o io1 che non sono abilitati per i volumi elastici, il volume viene creato su tale aggregato.

  Anche se questo scenario è improbabile, è possibile in due casi:

  - La funzione Elastic Volumes (volumi elastici) è stata disattivata esplicitamente quando si crea un aggregato dall'API.
  - È stato creato un nuovo sistema Cloud Volumes ONTAP dall'interfaccia utente, nel qual caso la funzione Elastic Volumes (volumi elastici) viene disattivata nell'aggregato iniziale. Revisione Limitazioni di seguito per ulteriori informazioni.

- Se nessun aggregato esistente dispone di capacità sufficiente, BlueXP crea l'aggregato con i volumi elastici abilitati e crea il volume sul nuovo aggregato.

  Le dimensioni dell'aggregato si basano sulle dimensioni del volume richiesto e su una capacità aggiuntiva del 10%.

Modalità di gestione della capacità

La modalità di gestione della capacità per un connettore funziona con volumi elastici in modo simile a come funziona con altri tipi di aggregati:

- Quando è attivata la modalità automatica (impostazione predefinita), BlueXP aumenta automaticamente le dimensioni degli aggregati se è necessaria una capacità aggiuntiva.
- Se si imposta la modalità di gestione della capacità su Manuale, BlueXP richiede l'approvazione per l'acquisto di capacità aggiuntiva.

"Scopri di più sulla modalità di gestione della capacità".

Limitazioni

L'aumento delle dimensioni di un aggregato può richiedere fino a 6 ore. Durante questo periodo, BlueXP non può richiedere alcuna capacità aggiuntiva per quell'aggregato.

Come lavorare con volumi elastici

È possibile utilizzare volumi elastici in BlueXP come segue:

- Creare un nuovo sistema con volumi elastici attivati sull'aggregato iniziale quando si utilizzano dischi gp3 o io1

  "Scopri come creare un sistema Cloud Volumes ONTAP"

- Creare un nuovo volume su un aggregato con volumi elastici abilitati

  Se si crea un volume che utilizza dischi gp3 o io1, BlueXP crea automaticamente il volume su un aggregato con volumi elastici attivati. Per ulteriori informazioni, fare riferimento a. Cosa accade quando si crea un volume.

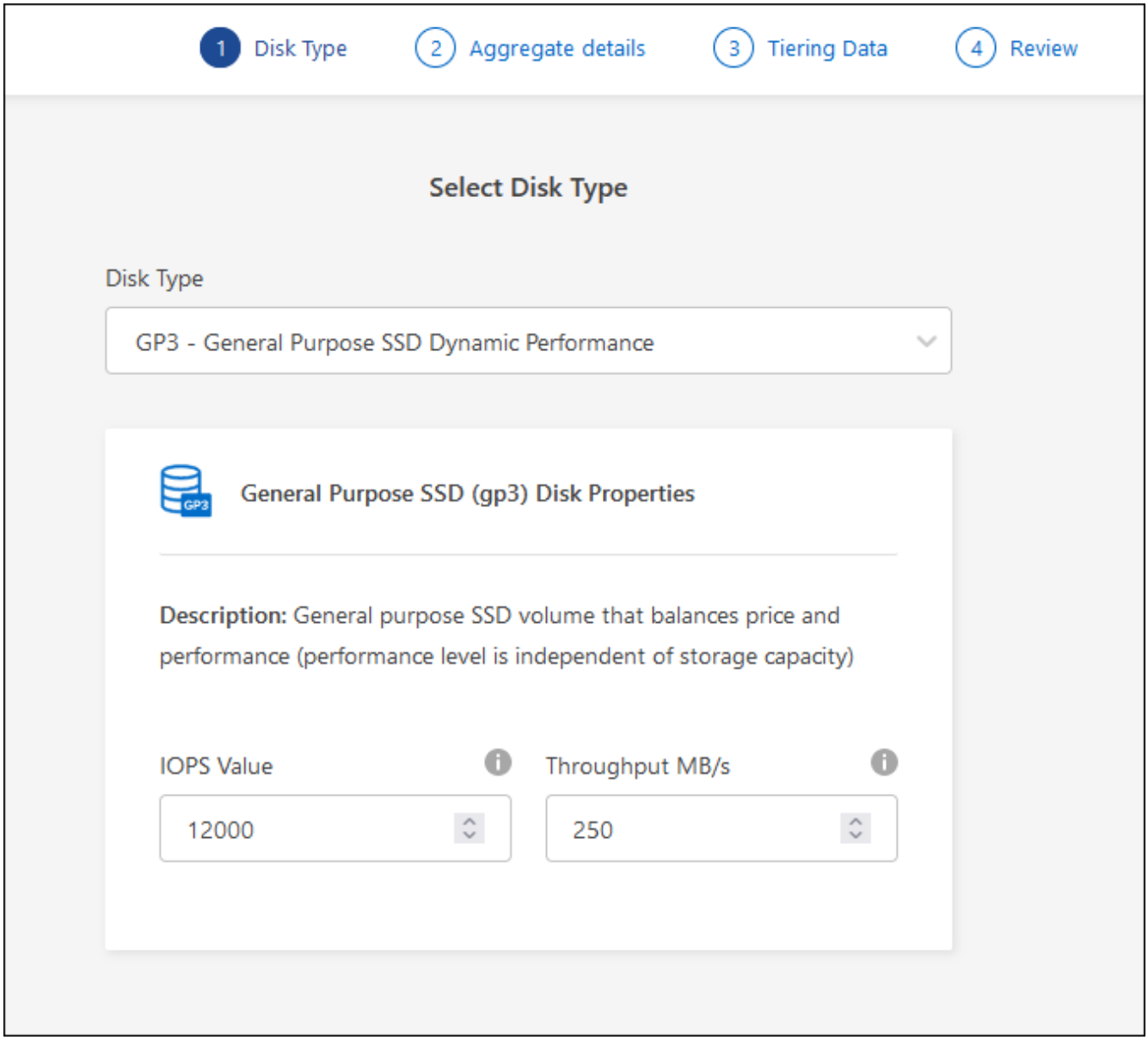
  "Scopri come creare volumi".

- Creare un nuovo aggregato con volumi elastici abilitati

I volumi elastici vengono attivati automaticamente sui nuovi aggregati che utilizzano dischi gp3 o io1, a condizione che il sistema Cloud Volumes ONTAP sia stato creato a partire dalla versione 9.11.0 o successiva.

Quando si crea l'aggregato, BlueXP richiede di specificare le dimensioni della capacità dell'aggregato. Si tratta di una configurazione diversa dalle altre, in cui è possibile scegliere una dimensione e un numero di dischi.

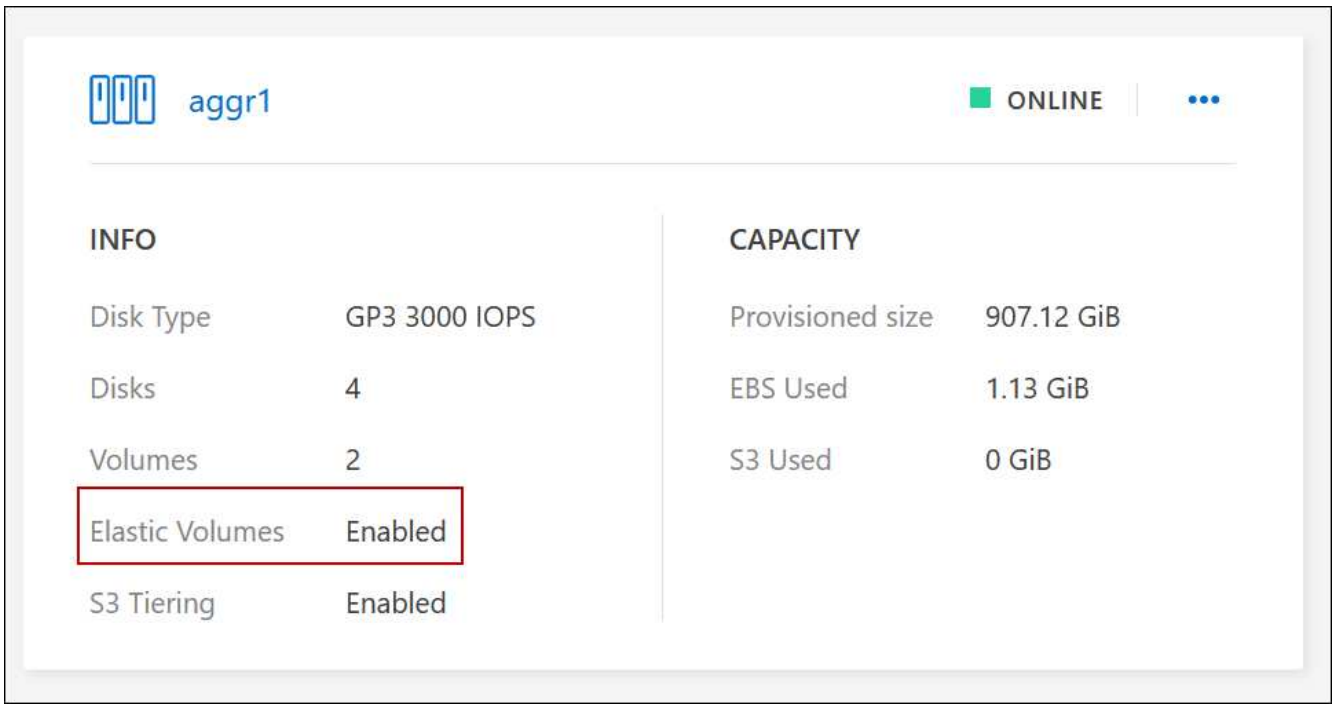
La seguente schermata mostra un esempio di un nuovo aggregato composto da dischi gp3.



"Scopri come creare aggregati".

- Identificare gli aggregati con volumi elastici abilitati

  Quando si accede alla pagina Advanced Allocation (allocazione avanzata), è possibile identificare se la funzione Elastic Volumes (volumi elastici) è attivata su un aggregato. Nell'esempio seguente, aggr1 ha attivato i volumi elastici.



- Aggiungere capacità a un aggregato

  Mentre BlueXP aggiunge automaticamente capacità agli aggregati in base alle necessità, è possibile aumentare manualmente la capacità.

  "Scopri come aumentare la capacità aggregata".

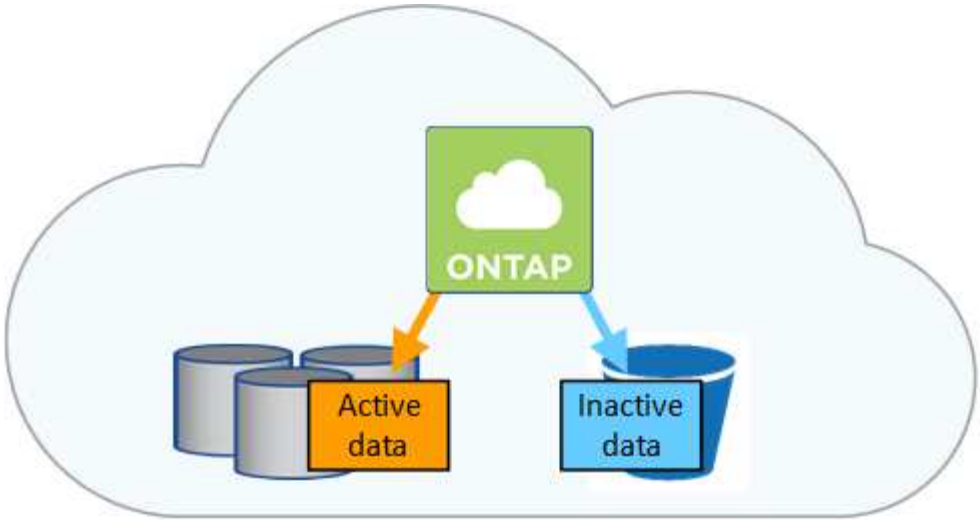
- Replica dei dati su un aggregato con volumi elastici abilitati

  Se il sistema Cloud Volumes ONTAP di destinazione supporta volumi elastici, un volume di destinazione viene posizionato su un aggregato con volumi elastici attivati (purché si scelga un disco gp3 o io1).

  "Scopri come configurare la replica dei dati"

Scopri di più sul tiering dei dati con Cloud Volumes ONTAP in AWS, Azure o Google Cloud

Riduci i costi di storage abilitando il tiering automatizzato dei dati inattivi su storage a oggetti a basso costo. I dati attivi rimangono in SSD o HDD ad alte prestazioni, mentre i dati inattivi vengono suddivisi in livelli per lo storage a oggetti a basso costo. In questo modo è possibile recuperare spazio sullo storage primario e ridurre lo storage secondario.



Il tiering dei dati è basato sulla tecnologia FabricPool. Cloud Volumes ONTAP offre tiering dei dati per tutti i cluster Cloud Volumes ONTAP senza una licenza aggiuntiva. Quando abiliti il tiering dei dati, sono previsti costi per il tiering dei dati nello storage a oggetti. Fare riferimento alla documentazione del cloud provider per i dettagli sui costi dello storage a oggetti.

Tiering dei dati in AWS

Quando si abilita il tiering dei dati in AWS, Cloud Volumes ONTAP utilizza EBS come Tier di performance per i dati hot e AWS S3 come Tier di capacità per i dati inattivi.

Tier di performance

Il livello di performance può essere SSD General Purpose (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).

Tier di capacità

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi in un singolo bucket S3.

BlueXP crea un singolo bucket S3 per ogni ambiente di lavoro e lo nomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket S3 diverso per ciascun volume.

Quando BlueXP crea il bucket S3, utilizza le seguenti impostazioni predefinite:

- Classe di storage: Standard
- Crittografia predefinita: Disattivata
- Blocca accesso pubblico: Blocca tutti gli accessi pubblici
- Proprietà dell'oggetto: ACL attivati
- Versione bucket: Disattivata
- Blocco oggetto: Disattivato

Classi di storage

La classe di storage predefinita per i dati Tiered in AWS è *Standard*. Standard è ideale per i dati ad accesso frequente memorizzati in più zone di disponibilità.

Se non si prevede di accedere ai dati inattivi, è possibile ridurre i costi di storage cambiando la classe di

storage in una delle seguenti opzioni: *Intelligent Tiering*, *One-zone infrequent Access*, *Standard-infrequent Access* o *S3 Glacier Instant Retrieval*. Quando si modifica la classe di storage, i dati inattivi vengono avviati nella classe di storage Standard e vengono passati alla classe di storage selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, è consigliabile tenerli in considerazione prima di modificare la classe di storage. "Documentazione su Amazon S3: Scopri di più sulle classi storage di Amazon S3".

È possibile selezionare una classe di archiviazione quando si crea l'ambiente di lavoro e modificarla in qualsiasi momento. Per istruzioni sulla modifica della classe di archiviazione, fare riferimento alla "Tiering dei dati inattivi in uno storage a oggetti a basso costo".

La classe di storage per il tiering dei dati è estesa a tutto il sistema, non per volume.

Tiering dei dati in Azure

Quando abiliti il tiering dei dati in Azure, Cloud Volumes ONTAP utilizza i dischi gestiti da Azure come Tier di performance per i dati hot e lo storage Blob Azure come Tier di capacità per i dati inattivi.

Tier di performance

Il Tier di performance può essere SSD o HDD.

Tier di capacità

Un sistema Cloud Volumes ONTAP esegue il tiering dei dati inattivi in un singolo contenitore Blob.

BlueXP crea un nuovo account storage con un container per ogni ambiente di lavoro Cloud Volumes ONTAP. Il nome dell'account di storage è casuale. Non viene creato un container diverso per ogni volume.

BlueXP crea l'account storage con le seguenti impostazioni:

- Tier di accesso: Hot
- Performance: Standard
- Ridondanza: in base alla distribuzione di Cloud Volume ONTAP
  - Zona di disponibilità singola: archiviazione ridondante locale (LRS)
  - Zona di disponibilità multipla: archiviazione con ridondanza di zona (ZRS)
- Account: StorageV2 (General Purpose v2)
- Richiedi trasferimento sicuro per le operazioni API REST: Abilitato
- Access key account storage: Enabled (accesso chiave account storage)
- Versione minima TLS: Versione 1.2
- Crittografia dell'infrastruttura: Disattivata

Tier di accesso allo storage

Il Tier di accesso allo storage predefinito per i dati a più livelli in Azure è il *hot* Tier. Il Tier hot è ideale per i dati con accesso frequente nel Tier di capacità.

Se non hai intenzione di accedere ai dati inattivi nel Tier di capacità, puoi scegliere il Tier di storage *cool*, in cui i dati inattivi vengono conservati per un minimo di 30 giorni. Puoi anche optare per il livello *cold*, in cui i dati inattivi vengono archiviati per un minimo di 90 giorni. In base ai tuoi requisiti di storage e alle tue considerazioni sui costi, puoi scegliere il Tier più adatto alle tue esigenze. Quando modifichi il Tier di

storage in *cool* o *cold*, i dati del Tier di capacità inattivo vengono spostati direttamente nel Tier di storage cold o cold. I Tier "cool" e "cold" offrono costi di storage inferiori rispetto al Tier "hot", ma prevedono costi di accesso più elevati. Prima di modificare il Tier storage, è necessario tenerne conto. Fare riferimento alla "Documentazione di Microsoft Azure: Scopri di più sui Tier di accesso allo storage BLOB di Azure".

È possibile selezionare un Tier di storage quando si crea l'ambiente di lavoro e modificarlo in un secondo momento. Per ulteriori informazioni sulla modifica del livello di archiviazione, fare riferimento alla "Tiering dei dati inattivi in uno storage a oggetti a basso costo".

Il Tier di accesso allo storage per il tiering dei dati è esteso a tutto il sistema, non per volume.

Tiering dei dati in Google Cloud

Quando abiliti il tiering dei dati in Google Cloud, Cloud Volumes ONTAP utilizza i dischi persistenti come Tier di performance per i dati hot e un bucket di storage cloud come Tier di capacità per i dati inattivi.

Tier di performance

Il Tier di performance può essere costituito da dischi persistenti SSD, dischi persistenti bilanciati o dischi persistenti standard.

Tier di capacità

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi in un singolo bucket di storage cloud di Google.

BlueXP crea un bucket per ogni ambiente di lavoro e lo nomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket diverso per ogni volume.

Quando BlueXP crea il bucket, utilizza le seguenti impostazioni predefinite:

- Tipo di ubicazione: Regione
- Classe di storage: Standard
- Accesso pubblico: Soggetto a ACL a oggetti
- Controllo degli accessi: Granulare
- Protezione: Nessuna
- Crittografia dei dati: Chiave gestita da Google

Classi di storage

La classe di storage predefinita per i dati a più livelli è la classe *Standard Storage*. Se l'accesso ai dati non è frequente, puoi ridurre i costi di storage passando a *Nearline Storage* o *Coldline Storage*. Quando si modifica la classe di archiviazione, i dati inattivi successivi vengono spostati direttamente nella classe selezionata.

> Tutti i dati inattivi esistenti manterranno la classe di archiviazione predefinita quando si modifica la classe di archiviazione. Per modificare la classe di archiviazione per i dati inattivi esistenti, è necessario eseguire la designazione manualmente.

I costi di accesso sono più elevati se si accede ai dati, quindi tenere in considerazione questo aspetto prima di modificare la classe di storage. Per ulteriori informazioni, fare riferimento a "Documentazione di Google Cloud: Classi di storage".

È possibile selezionare un Tier di storage quando si crea l'ambiente di lavoro e modificarlo in un secondo momento. Per informazioni dettagliate sulla modifica della classe di archiviazione, fare riferimento alla

"Tiering dei dati inattivi in uno storage a oggetti a basso costo".

La classe di storage per il tiering dei dati è estesa a tutto il sistema, non per volume.

Tiering dei dati e limiti di capacità

Se si abilita il tiering dei dati, il limite di capacità di un sistema rimane invariato. Il limite viene distribuito tra il Tier di performance e il Tier di capacità.

Policy di tiering dei volumi

Per attivare il tiering dei dati, è necessario selezionare una policy di tiering dei volumi quando si crea, modifica o replica un volume. È possibile selezionare un criterio diverso per ciascun volume.

Alcuni criteri di tiering hanno un periodo di raffreddamento minimo associato, che imposta il tempo in cui i dati dell'utente in un volume devono rimanere inattivi per essere considerati "freddi" e spostati al livello di capacità. Il periodo di raffreddamento inizia quando i dati vengono scritti nell'aggregato.

È possibile modificare il periodo di raffreddamento minimo e la soglia aggregata predefinita del 50% (ulteriori informazioni su quelle riportate di seguito). "Scopri come modificare il periodo di raffreddamento" e. "scopri come modificare la soglia".

BlueXP consente di scegliere tra le seguenti policy di tiering dei volumi quando si crea o si modifica un volume:

Solo Snapshot

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei dati cold user delle copie Snapshot non associate al file system attivo al Tier di capacità. Il periodo di raffreddamento è di circa 2 giorni.

In lettura, i blocchi di dati cold sul Tier di capacità diventano hot e vengono spostati sul Tier di performance.

Tutto

Tutti i dati (non inclusi i metadati) vengono immediatamente contrassegnati come cold e tiered per lo storage a oggetti il più presto possibile. Non è necessario attendere 48 ore affinché i nuovi blocchi di un volume si raffreddino. Tenere presente che i blocchi situati nel volume prima dell'impostazione del criterio All richiedono 48 ore per diventare freddi.

In caso di lettura, i blocchi di dati cold nel Tier cloud restano freddi e non vengono riscritti nel Tier di performance. Questo criterio è disponibile a partire da ONTAP 9.6.

Automatico

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei blocchi di dati cold in un volume fino a raggiungere un livello di capacità. I dati cold non includono solo le copie Snapshot, ma anche i dati cold user dal file system attivo. Il periodo di raffreddamento è di circa 31 giorni.

Questo criterio è supportato a partire da Cloud Volumes ONTAP 9.4.

Se letti in modo casuale, i blocchi di dati cold nel Tier di capacità diventano hot e passano al Tier di performance. Se letti in base a letture sequenziali, come quelle associate a scansioni di indice e antivirus, i blocchi di dati cold rimangono freddi e non passano al livello di performance.

Nessuno

Mantiene i dati di un volume nel Tier di performance, evitando che vengano spostati nel Tier di capacità.

Quando si replica un volume, è possibile scegliere se eseguire il Tier dei dati sullo storage a oggetti. In tal caso, BlueXP applica il criterio **Backup** al volume di protezione dei dati. A partire da Cloud Volumes ONTAP 9.6, la policy di tiering **all** sostituisce la policy di backup.

La disattivazione di Cloud Volumes ONTAP influisce sul periodo di raffreddamento

I blocchi di dati vengono raffreddati mediante scansioni di raffreddamento. Durante questo processo, i blocchi che non sono stati utilizzati hanno spostato la temperatura del blocco (raffreddato) al valore successivo più basso. Il tempo di raffreddamento predefinito dipende dalla policy di tiering del volume:

- Auto: 31 giorni
- Solo snapshot: 2 giorni

Affinché la scansione di raffreddamento funzioni, è necessario che Cloud Volumes ONTAP sia in esecuzione. Se Cloud Volumes ONTAP è disattivato, anche il raffreddamento si interrompe. Di conseguenza, è possibile ottenere tempi di raffreddamento più lunghi.

> Quando Cloud Volumes ONTAP è disattivato, la temperatura di ciascun blocco viene mantenuta fino al riavvio del sistema. Ad esempio, se la temperatura di un blocco è 5 quando si spegne il sistema, la temperatura rimane 5 quando si riaccende il sistema.

Impostazione del tiering dei dati

Per istruzioni e un elenco delle configurazioni supportate, fare riferimento a "Tiering dei dati inattivi in uno storage a oggetti a basso costo".

Gestione dello storage Cloud Volumes ONTAP

BlueXP offre una gestione semplificata e avanzata dello storage Cloud Volumes ONTAP.

> 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.

Provisioning dello storage

BlueXP semplifica il provisioning dello storage per Cloud Volumes ONTAP acquistando dischi e gestendo aggregati. È sufficiente creare volumi. Se lo si desidera, è possibile utilizzare un'opzione di allocazione avanzata per eseguire il provisioning degli aggregati.

Provisioning semplificato

Gli aggregati forniscono lo storage cloud ai volumi. BlueXP crea aggregati per l'utente al momento del lancio di un'istanza e del provisioning di volumi aggiuntivi.

Quando si crea un volume, BlueXP esegue una delle tre operazioni seguenti:

- Posiziona il volume su un aggregato esistente con spazio libero sufficiente.
- Il volume viene inserito in un aggregato esistente acquistando più dischi per tale aggregato.

Inoltre, nel caso di un aggregato in AWS che supporta volumi elastici, BlueXP aumenta anche le dimensioni dei dischi in un gruppo RAID. "Scopri di più sul supporto per volumi elastici".

- L'IT acquista dischi per un nuovo aggregato e colloca il volume su tale aggregato.

BlueXP determina dove posizionare un nuovo volume prendendo in considerazione diversi fattori: La dimensione massima di un aggregato, l'attivazione del thin provisioning e le soglie di spazio libero per gli aggregati.

Selezione delle dimensioni dei dischi per gli aggregati in AWS

Quando BlueXP crea nuovi aggregati per Cloud Volumes ONTAP in AWS, aumenta gradualmente la dimensione del disco in un aggregato, con l'aumentare del numero di aggregati nel sistema. BlueXP garantisce che sia possibile utilizzare la capacità massima del sistema prima che raggiunga il numero massimo di dischi dati consentito da AWS.

Ad esempio, BlueXP potrebbe scegliere le seguenti dimensioni dei dischi:

Numero aggregato	Dimensioni del disco	Capacità aggregata massima
1	500 GiB	3 TIB
4	1 TIB	6 TIB
6	2 TIB	12 TIB

Questo comportamento non si applica agli aggregati che supportano la funzionalità Amazon EBS Elastic Volumes. Gli aggregati con volumi elastici abilitati sono costituiti da uno o due gruppi RAID. Ogni gruppo RAID ha quattro dischi identici che hanno la stessa capacità. "Scopri di più sul supporto per volumi elastici".

È possibile scegliere autonomamente le dimensioni del disco utilizzando l'opzione Advanced allocation (allocazione avanzata).

Allocazione avanzata

Invece di consentire a BlueXP di gestire gli aggregati, puoi farlo da solo. "Dalla pagina **allocazione avanzata**", è possibile creare nuovi aggregati che includono un numero specifico di dischi, aggiungere dischi a un aggregato esistente e creare volumi in aggregati specifici.

Gestione della capacità

L'organizzazione o l'amministratore dell'account BlueXP può scegliere se BlueXP ti notifica delle decisioni relative alla capacità di storage o se BlueXP gestisce automaticamente i requisiti di capacità per il tuo business.

Questo comportamento è determinato dalla *modalità di gestione della capacità* di un connettore. La modalità di gestione della capacità influisce su tutti i sistemi Cloud Volumes ONTAP gestiti da tale connettore. Se si dispone di un altro connettore, è possibile configurarlo in modo diverso.

Gestione automatica della capacità

Per impostazione predefinita, Capacity Management Mode (modalità di gestione della capacità) è impostata su Automatic (automatica). In questa modalità, BlueXP controlla il rapporto di spazio libero ogni 15 minuti per determinare se il rapporto di spazio libero scende al di sotto della soglia specificata. Se occorre maggiore capacità, BlueXP avvia automaticamente l'acquisto di nuovi dischi, elimina le raccolte inutilizzate di dischi (aggregati), sposta i volumi tra gli aggregati in base alle necessità e tenta di prevenire i guasti ai dischi.

I seguenti esempi illustrano il funzionamento di questa modalità:

- Se un aggregato raggiunge la soglia di capacità e dispone di spazio per più dischi, BlueXP acquista automaticamente nuovi dischi per quell'aggregato in modo che i volumi possano continuare a crescere.

Nel caso di un aggregato in AWS che supporta volumi elastici, BlueXP aumenta anche la dimensione dei dischi di un gruppo RAID. "Scopri di più sul supporto per volumi elastici".

+
* Se un aggregato raggiunge la soglia di capacità e non supporta dischi aggiuntivi, BlueXP sposta automaticamente un volume da quell'aggregato a un aggregato con capacità disponibile o a un nuovo aggregato.

+
Se BlueXP crea un nuovo aggregato per il volume, sceglie una dimensione del disco che si adatta alle dimensioni del volume.

+
Si noti che lo spazio libero è ora disponibile sull'aggregato originale. I volumi esistenti o nuovi volumi possono utilizzare tale spazio. Non è possibile restituire lo spazio al cloud provider in questo scenario.

- Se un aggregato non contiene volumi per più di 12 ore, BlueXP lo elimina.

Gestione delle LUN con gestione automatica della capacità

La gestione automatica della capacità di BlueXP non si applica alle LUN. Quando BlueXP crea un LUN, disattiva la funzione di crescita automatica.

Gestione manuale della capacità

Se l'organizzazione o l'amministratore dell'account BlueXP impostano la modalità di gestione della capacità su manuale, BlueXP visualizza i messaggi azione richiesta quando è necessario prendere decisioni sulla capacità. Gli stessi esempi descritti nella modalità automatica si applicano alla modalità manuale, ma spetta all'utente accettare le azioni.

Scopri di più

"Scopri come modificare la modalità di gestione della capacità".

Velocità di scrittura

BlueXP consente di scegliere la velocità di scrittura normale o elevata per la maggior parte delle configurazioni Cloud Volumes ONTAP. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normali e alte e i rischi e le raccomandazioni quando si utilizza un'elevata velocità di scrittura.

Velocità di scrittura normale

Quando si sceglie la normale velocità di scrittura, i dati vengono scritti direttamente su disco. Quando i dati vengono scritti direttamente su disco, riduce la probabilità di perdita di dati in caso di un'interruzione non pianificata del sistema o di un guasto a cascata che comporta un'interruzione non pianificata del sistema (solo coppie ha).

L'opzione predefinita è la velocità di scrittura normale.

Elevata velocità di scrittura

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati nel buffer prima che vengano scritti su disco, garantendo prestazioni di scrittura più rapide. A causa di questo caching, vi è la possibilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

La quantità di dati che è possibile perdere in caso di interruzione non pianificata del sistema è l'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'azione di scrittura dei dati bufferizzati su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale condizione si verifica per prima). Tuttavia, le performance dello storage fornito dal tuo cloud provider possono influire sulla coerenza del tempo di elaborazione dei punti.

Quando utilizzare un'elevata velocità di scrittura

L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide e se è possibile resistere al rischio di perdita di dati in caso di un'interruzione non pianificata del sistema o di un guasto a cascata che comporta un'interruzione non pianificata del sistema (solo coppie ha).

Consigli quando si utilizza un'elevata velocità di scrittura

Se si attiva un'elevata velocità di scrittura, è necessario garantire la protezione in scrittura a livello di applicazione o che le applicazioni possano tollerare la perdita di dati, se si verifica.

Elevata velocità di scrittura con una coppia ha in AWS

Se si prevede di abilitare un'elevata velocità di scrittura su una coppia ha in AWS, è necessario comprendere la differenza dei livelli di protezione tra un'implementazione di zone di disponibilità multiple (AZ) e un'implementazione di AZ singola. L'implementazione di una coppia ha in più AZS offre una maggiore resilienza e può contribuire a ridurre il rischio di perdita di dati.

"Scopri di più sulle coppie ha in AWS".

Configurazioni che supportano un'elevata velocità di scrittura

Non tutte le configurazioni Cloud Volumes ONTAP supportano un'elevata velocità di scrittura. Per impostazione predefinita, queste configurazioni utilizzano la normale velocità di scrittura.

AWS

Se si utilizza un sistema a nodo singolo, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con tutti i tipi di istanze.

A partire dalla versione 9.8, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con coppie ha quando si utilizzano quasi tutti i tipi di istanze EC2 supportati, ad eccezione di m5.xlarge e r5.xlarge.

"Scopri di più sulle istanze di Amazon EC2 supportate da Cloud Volumes ONTAP".

Azure

Se si utilizza un sistema a nodo singolo, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con tutti i tipi di macchine virtuali.

Se si utilizza una coppia ha, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con diversi tipi di macchine virtuali, a partire dalla versione 9.8. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" Per visualizzare i tipi di macchine virtuali che supportano un'elevata velocità di scrittura.

Google Cloud

Se si utilizza un sistema a nodo singolo, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con tutti i tipi di computer.

Se si utilizza una coppia ha, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con diversi tipi di macchine virtuali, a partire dalla versione 9.13.0. Accedere alla "Note di rilascio di Cloud Volumes ONTAP" Per visualizzare i tipi di macchine virtuali che supportano un'elevata velocità di scrittura.

"Scopri di più sui tipi di computer Google Cloud supportati da Cloud Volumes ONTAP".

Come selezionare una velocità di scrittura

È possibile scegliere una velocità di scrittura quando si crea un nuovo ambiente di lavoro "modificare la velocità di scrittura per un sistema esistente".

Cosa aspettarsi in caso di perdita di dati

Se la perdita di dati si verifica a causa dell'elevata velocità di scrittura, il sistema di gestione degli eventi (EMS) segnala i seguenti due eventi:

- Cloud Volumes ONTAP 9.12.1 o versione successiva

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP da 9.11.0 a 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP da 9.8 a 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

In questo caso, Cloud Volumes ONTAP dovrebbe essere in grado di avviarsi e continuare a fornire i dati senza l'intervento dell'utente.

Come interrompere l'accesso ai dati in caso di perdita di dati

Se si è preoccupati della perdita di dati, si desidera che le applicazioni smettano di funzionare in caso di perdita di dati e che l'accesso ai dati venga ripristinato dopo che il problema di perdita di dati è stato risolto correttamente, è possibile utilizzare l'opzione NVFAIL della CLI per raggiungere tale obiettivo.

Per attivare l'opzione NVFAIL

```
vol modify -volume <vol-name> -nvfail on
```

Per controllare le impostazioni NVFAIL

```
vol show -volume <vol-name> -fields nvfail
```

Per disattivare l'opzione NVFAIL

```
vol modify -volume <vol-name> -nvfail off
```

Quando si verifica una perdita di dati, un volume NFS o iSCSI con NVFAIL attivato dovrebbe interrompere la fornitura dei dati (non c'è alcun impatto su CIFS, che è un protocollo stateless). Per ulteriori informazioni, fare riferimento a. "Impatto di NVFAIL sull'accesso ai volumi NFS o alle LUN".

Per controllare lo stato NVFAIL

```
vol show -fields in-nvfailed-state
```

Una volta risolto correttamente il problema della perdita di dati, è possibile cancellare lo stato NVFAIL e il volume sarà disponibile per l'accesso ai dati.

Per cancellare lo stato NVFAIL

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash cache

Alcune configurazioni Cloud Volumes ONTAP includono lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance.

Cos'è Flash cache?

Flash cache accelera l'accesso ai dati attraverso il caching intelligente in tempo reale dei dati utente recentemente letti e dei metadati NetApp. È efficace per i carichi di lavoro a lettura intensiva, inclusi database, e-mail e file service.

Configurazioni supportate

Flash cache è supportata con configurazioni Cloud Volumes ONTAP specifiche. Visualizzare le configurazioni supportate in "Note di rilascio di Cloud Volumes ONTAP"

Limitazioni

- Quando si configura Flash cache per Cloud Volumes ONTAP 9.12.0 o versione precedente in AWS, la compressione deve essere disattivata su tutti i volumi per sfruttare i miglioramenti delle performance di Flash cache. Quando si implementa o si esegue l'aggiornamento a Cloud Volumes ONTAP 9.12.1 o versioni successive, non è necessario disattivare la compressione.

  Non scegliere l'efficienza dello storage quando si crea un volume da BlueXP, oppure creare un volume e

poi "Disattivare la compressione dei dati utilizzando l'interfaccia CLI".

- Il ripristino della cache dopo un riavvio non è supportato con Cloud Volumes ONTAP.

Scopri lo storage WORM su Cloud Volumes ONTAP

È possibile attivare lo storage WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP per conservare i file in forma non modificata per un periodo di conservazione specificato. Lo storage cloud WORM è basato sulla tecnologia SnapLock, il che significa che i file WORM sono protetti a livello di file.

La funzionalità WORM è disponibile per l'utilizzo con iscrizioni BYOL (Bring Your Own License) e al marketplace per le tue licenze senza costi aggiuntivi. Contattare il rappresentante commerciale NetApp per aggiungere WORM alla licenza corrente.

Come funziona lo storage WORM

Una volta che un file è stato impegnato nello storage WORM, non può essere modificato, anche dopo la scadenza del periodo di conservazione. Un clock a prova di manomissione determina quando è trascorso il periodo di conservazione di un file WORM.

Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari.

Attivazione dello storage WORM

La modalità di attivazione dello storage WORM dipende dalla versione di Cloud Volumes ONTAP in uso.

Versione 9.10.1 e successive

A partire da Cloud Volumes ONTAP 9.10.1, è possibile attivare o disattivare il WORM a livello di volume,

Quando si crea un nuovo ambiente di lavoro Cloud Volumes ONTAP, viene richiesto di attivare o disattivare lo storage WORM:

- Se si attiva lo storage WORM durante la creazione di un ambiente di lavoro, ogni volume creato da BlueXP ha abilitato WORM. Tuttavia, puoi utilizzare System Manager di ONTAP o l'interfaccia a riga di comando di ONTAP per creare volumi che hanno IL WORM disattivato.
- Se disattivi lo storage WORM al momento della creazione di un ambiente di lavoro, ogni volume creato da BlueXP , ONTAP System Manager o dalla CLI di ONTAP ha disattivato WORM.

Versione 9.10.0 e precedenti

È possibile attivare lo storage WORM su un sistema Cloud Volumes ONTAP quando si crea un nuovo ambiente di lavoro. Ogni volume creato da BlueXP ha abilitato WORM. Non è possibile disattivare lo storage WORM su singoli volumi.

Commit dei file in WORM

È possibile utilizzare un'applicazione per il commit dei file in WORM su NFS o CIFS oppure utilizzare l'interfaccia utente di ONTAP per il commit automatico dei file in WORM. È inoltre possibile utilizzare un file .WORM appendibile per conservare i dati scritti in modo incrementale, ad esempio le informazioni di log.

Dopo aver attivato lo storage WORM su un sistema Cloud Volumes ONTAP, è necessario utilizzare l'interfaccia utente di ONTAP per la gestione dello storage WORM. Per istruzioni, fare riferimento alla "Documentazione ONTAP su SnapLock" .

Abilitazione DI WORM in un ambiente di lavoro Cloud Volumes ONTAP

Puoi abilitare lo storage WORM durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP su BlueXP . È inoltre possibile abilitare IL WORM in un ambiente di lavoro se il WORM non è attivato durante la creazione. Una volta attivato, non è possibile disattivare IL WORM.

A proposito di questa attività

- WORM è supportato in ONTAP 9.10,1 e versioni successive.
- WORM con backup è supportato su ONTAP 9.11,1 e versioni successive.

Fasi

1. Nella pagina Canvas, fare doppio clic sul nome dell'ambiente di lavoro in cui si desidera attivare il WORM.
2. Nella scheda Panoramica, fare clic sul pannello funzioni, quindi fare clic sull'icona a forma di matita accanto a **WORM**.

   Se il WORM è già attivato sul sistema, l'icona a forma di matita è disattivata.

3. Nella pagina **WORM**, impostare il periodo di conservazione per il clock di conformità del cluster.

   Per ulteriori informazioni, fare riferimento alla "Documentazione ONTAP: Inizializzare l'orologio di conformità" .

4. Fare clic su **Set** (Imposta).

Al termine

È possibile verificare lo stato di **WORM** nel pannello funzioni. Una volta abilitato il WORM, la licenza SnapLock viene installata automaticamente nel cluster. È possibile visualizzare la licenza SnapLock su Gestione sistema ONTAP.

Eliminazione dei file WORM

È possibile eliminare i file WORM durante il periodo di conservazione utilizzando la funzione di eliminazione con privilegi.

Per istruzioni, fare riferimento alla "Documentazione ONTAP" .

WORM e tiering dei dati

Quando si crea un nuovo sistema Cloud Volumes ONTAP 9.8 o versione successiva, è possibile abilitare contemporaneamente il tiering dei dati e lo storage WORM. L'abilitazione del tiering dei dati con lo storage WORM consente di eseguire il tiering dei dati in un archivio di oggetti nel cloud.

È necessario comprendere quanto segue sull'abilitazione del tiering dei dati e dello storage WORM:

- I dati a più livelli per lo storage a oggetti non includono la funzionalità WORM di ONTAP. Per garantire la funzionalità WORM end-to-end, è necessario impostare correttamente le autorizzazioni del bucket.
- I dati che vengono suddivisi in livelli per lo storage a oggetti non sono dotati della funzionalità WORM, il che significa che chiunque abbia accesso completo ai bucket e ai container può eliminare gli oggetti suddivisi in livelli da ONTAP.

- Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 viene bloccato dopo l'abilitazione DI WORM e tiering.

Limitazioni

- Lo storage WORM in Cloud Volumes ONTAP opera sotto un modello "trusted storage Administrator". Mentre i file WORM sono protetti da modifiche o modifiche, i volumi possono essere cancellati da un amministratore del cluster anche se tali volumi contengono dati WORM non scaduti.
- Oltre al modello di amministratore dello storage fidato, lo storage WORM in Cloud Volumes ONTAP opera implicitamente anche sotto un modello di "amministratore del cloud fidato". Un amministratore del cloud può eliminare i dati WORM prima della data di scadenza, rimuovendo o modificando il cloud storage direttamente dal cloud provider.

Link correlato

- "Crea copie Snapshot a prova di manomissione per lo storage WORM"

Coppie ad alta disponibilità

Scopri di più sulle coppie ha di Cloud Volumes ONTAP in AWS

Una configurazione ha (High Availability) di Cloud Volumes ONTAP offre operazioni senza interruzioni e tolleranza agli errori. In AWS, i dati vengono sottoposti a mirroring sincrono tra i due nodi.

Componenti HA

In AWS, le configurazioni Cloud Volumes ONTAP ha includono i seguenti componenti:

- Due nodi Cloud Volumes ONTAP i cui dati vengono sottoposti a mirroring sincrono l'uno con l'altro.
- Istanza di mediatore che fornisce un canale di comunicazione tra i nodi per assistere nei processi di acquisizione e giveback dello storage.

Mediatore

Di seguito sono riportati alcuni dettagli chiave sull'istanza del mediatore in AWS:

Tipo di istanza
t3-micro

Dischi
Due dischi ST1 da 8 GiB e 4 GiB

Sistema operativo
Debian 11

> Per Cloud Volumes ONTAP 9.10.0 e versioni precedenti, Debian 10 è stata installata sul mediatore.

Aggiornamenti
Quando si aggiorna Cloud Volumes ONTAP, BlueXP aggiorna anche l'istanza del mediatore in base alle necessità.

Accesso all'istanza

Quando si crea una coppia Cloud Volumes ONTAP ha da BlueXP, viene richiesto di fornire una coppia di chiavi per l'istanza del mediatore. È possibile utilizzare tale coppia di chiavi per l'accesso SSH utilizzando `admin` utente.

Agenti di terze parti

Gli agenti di terze parti o le estensioni delle macchine virtuali non sono supportati sull'istanza del mediatore.

Takeover e giveback dello storage

Se un nodo non funziona, l'altro nodo può servire i dati per il proprio partner per fornire un servizio dati continuo. I client possono accedere agli stessi dati dal nodo partner perché i dati sono stati sottoposti a mirroring sincrono con il partner.

Dopo il riavvio del nodo, il partner deve risincronizzare i dati prima di poter restituire lo storage. Il tempo necessario per la risincronizzazione dei dati dipende dalla quantità di dati modificati mentre il nodo era inattivo.

Per impostazione predefinita, le funzioni di Takeover, risync e giveback dello storage sono tutte automatiche. Non è richiesta alcuna azione da parte dell'utente.

RPO e RTO

Una configurazione ha mantiene l'alta disponibilità dei dati come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi. I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.
- L'obiettivo del tempo di ripristino (RTO) è di 120 secondi. In caso di interruzione, i dati devono essere disponibili in 120 secondi o meno.

Modelli di implementazione HA

Puoi garantire l'elevata disponibilità dei tuoi dati implementando una configurazione ha in più zone di disponibilità (AZ) o in una singola zona di disponibilità (AZ). Per scegliere la configurazione più adatta alle proprie esigenze, è necessario esaminare ulteriori dettagli su ciascuna configurazione.

Più zone di disponibilità

L'implementazione di una configurazione ha in più zone di disponibilità (AZ) garantisce un'elevata disponibilità dei dati in caso di errore con una AZ o un'istanza che esegue un nodo Cloud Volumes ONTAP. È necessario comprendere in che modo gli indirizzi IP NAS influiscono sull'accesso ai dati e sul failover dello storage.

Accesso ai dati NFS e CIFS

Quando una configurazione ha viene distribuita in più zone di disponibilità, *indirizzi IP mobili* abilitano l'accesso al client NAS. Gli indirizzi IP mobili, che devono essere al di fuori dei blocchi CIDR per tutti i VPC della regione, possono migrare tra i nodi in caso di guasti. Non sono accessibili in modo nativo ai client che si trovano al di fuori del VPC, a meno che non si "Configurare un gateway di transito AWS".

Se non è possibile configurare un gateway di transito, gli indirizzi IP privati sono disponibili per i client NAS esterni al VPC. Tuttavia, questi indirizzi IP sono statici e non possono eseguire il failover tra i nodi.

Prima di distribuire una configurazione ha in più zone di disponibilità, è necessario esaminare i requisiti per gli indirizzi IP mobili e le tabelle di routing. È necessario specificare gli indirizzi IP mobili quando si implementa la configurazione. Gli indirizzi IP privati vengono creati automaticamente da BlueXP.

Per ulteriori informazioni, fare riferimento a "Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS".

Accesso ai dati iSCSI

La comunicazione dati tra più VPC non è un problema, poiché iSCSI non utilizza indirizzi IP mobili.

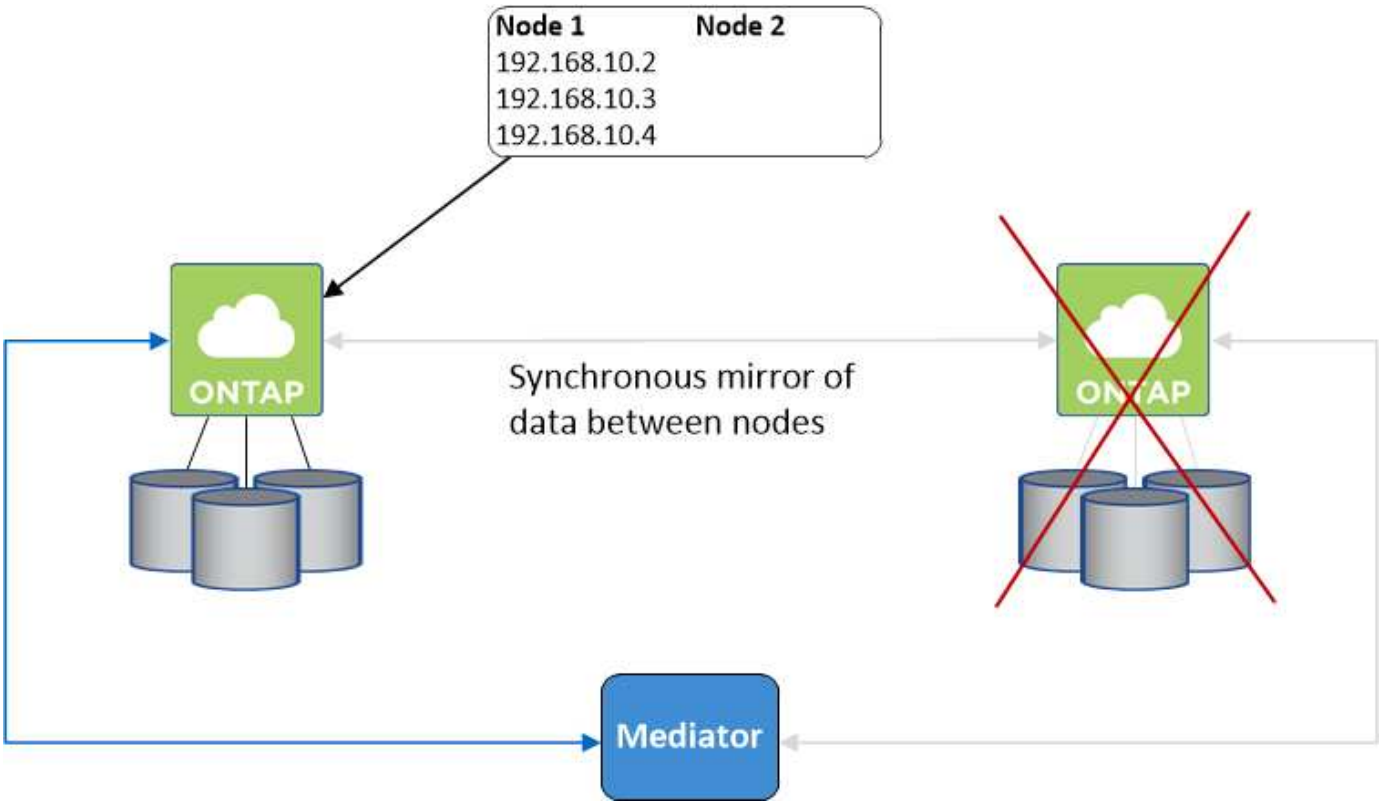
Takeover e giveback per iSCSI

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

> Per informazioni sulle specifiche configurazioni host che supportano ALUA, consultare la "Tool di matrice di interoperabilità NetApp" e la "Guida agli host SAN e ai client cloud" per il sistema operativo host in uso.

Takeover e giveback per NAS

Quando l'acquisizione avviene in una configurazione NAS utilizzando IP mobili, l'indirizzo IP mobile del nodo utilizzato dai client per accedere ai dati viene spostato nell'altro nodo. L'immagine seguente mostra l'acquisizione dello storage in una configurazione NAS utilizzando IP mobili. Se il nodo 2 non funziona, l'indirizzo IP mobile per il nodo 2 passa al nodo 1.



Gli IP dei dati NAS utilizzati per l'accesso VPC esterno non possono migrare tra i nodi in caso di guasti. Se un nodo non è in linea, è necessario rimontarlo manualmente sui client esterni al VPC utilizzando l'indirizzo IP sull'altro nodo.

Una volta che il nodo guasto torna in linea, rimontare i client sui volumi utilizzando l'indirizzo IP originale. Questo passaggio è necessario per evitare il trasferimento di dati non necessari tra due nodi ha, che può causare un impatto significativo sulle performance e sulla stabilità.

È possibile identificare facilmente l'indirizzo IP corretto da BlueXP selezionando il volume e facendo clic su **Mount Command**.

Singola zona di disponibilità

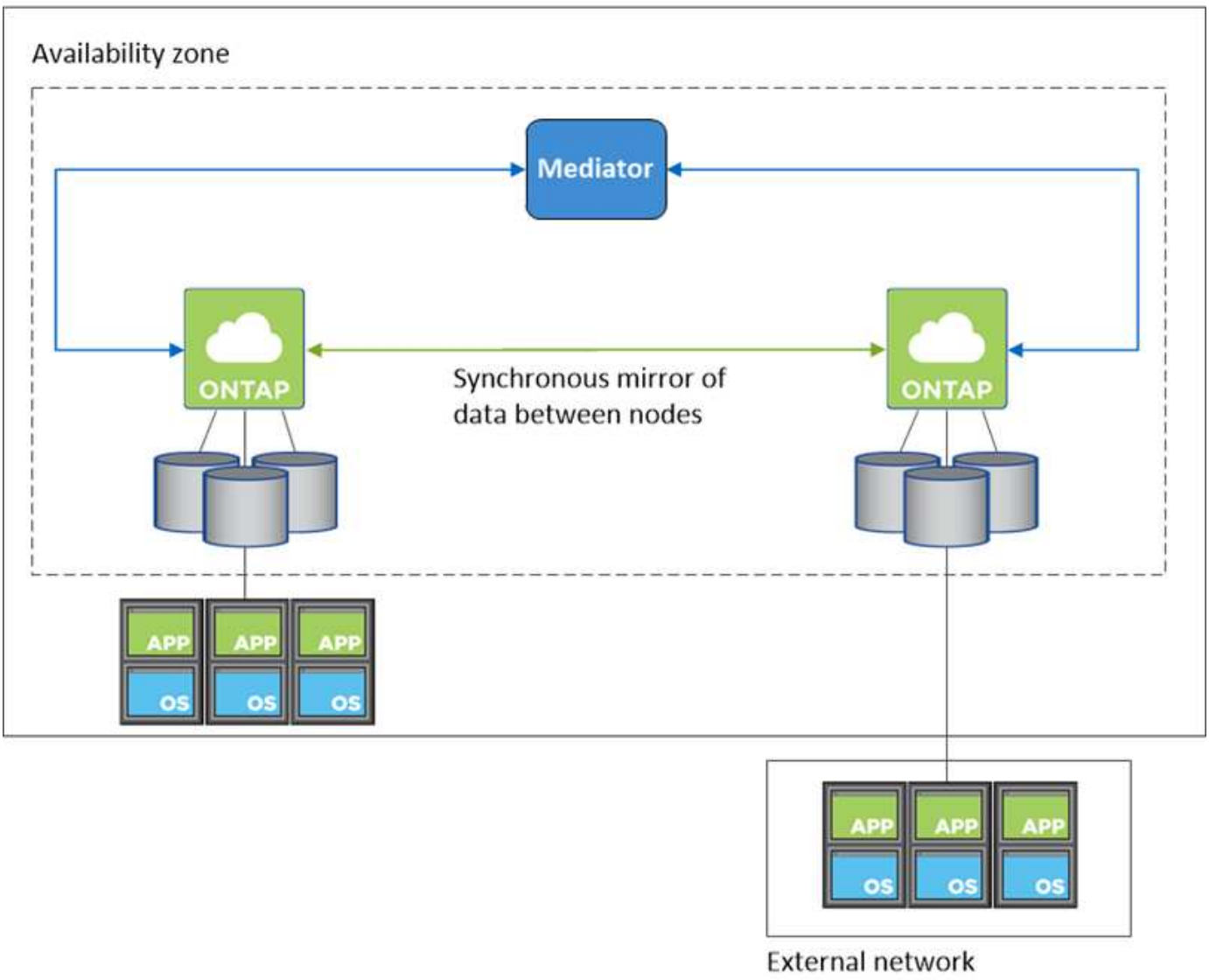
L'implementazione di una configurazione ha in una singola zona di disponibilità (AZ) può garantire l'elevata disponibilità dei dati in caso di guasto di un'istanza che esegue un nodo Cloud Volumes ONTAP. Tutti i dati sono accessibili in modo nativo dall'esterno del VPC.

> BlueXP crea un "Documentazione AWS: gruppo di posizionamento diffuso AWS" e avvia i due nodi HA in quel gruppo di posizionamento. Il gruppo di posizionamento riduce il rischio di guasti simultanei distribuendo le istanze su hardware sottostanti distinti. Questa funzionalità migliora la ridondanza dal punto di vista del calcolo e non da quello dei guasti del disco.

Accesso ai dati

Poiché questa configurazione si trova in un singolo AZ, non richiede indirizzi IP mobili. È possibile utilizzare lo stesso indirizzo IP per l'accesso ai dati dall'interno del VPC e dall'esterno del VPC.

La seguente immagine mostra una configurazione ha in un singolo AZ. I dati sono accessibili dall'interno del VPC e dall'esterno del VPC.



Takeover e giveback

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

> Per informazioni sulle specifiche configurazioni host che supportano ALUA, consultare la "Tool di matrice di interoperabilità NetApp" e la "Guida agli host SAN e ai client cloud" per il sistema operativo host in uso.

Per le configurazioni NAS, gli indirizzi IP dei dati possono migrare tra i nodi ha in caso di guasti. In questo modo si garantisce l'accesso del client allo storage.

Zone locali di AWS

Le zone locali di AWS sono un'implementazione dell'infrastruttura in cui storage, calcolo, database e altri servizi AWS selezionati sono situati vicino a grandi città e aree del settore. Con le zone locali di AWS è possibile avvicinare i servizi AWS per migliorare la latenza dei carichi di lavoro e gestire i database localmente. Su Cloud Volumes ONTAP,

Puoi implementare una configurazione con AZ singolo o AZ multiplo in zone locali di AWS.

> Le zone locali AWS sono supportate quando si utilizza BlueXP in modalità standard e privata. Al momento, i fusi locali di AWS non sono supportati quando si utilizza BlueXP in modalità limitata.

Esempio di configurazioni della zona locale di AWS

Cloud Volumes ONTAP in AWS supporta solo la modalità ha (High Availability) in una singola zona di disponibilità. Le implementazioni a nodo singolo non sono supportate.

Cloud Volumes ONTAP non supporta il tiering dei dati, il tiering cloud e istanze non qualificate nelle zone locali di AWS.

Di seguito sono riportate le configurazioni di esempio:

- Singola zona di disponibilità: Entrambi i nodi del cluster e il mediatore si trovano nella stessa zona locale.
- Più zone di disponibilità
  In più configurazioni di zone di disponibilità, esistono tre istanze, due nodi e un mediatore. Un'istanza delle tre istanze deve trovarsi in una zona separata. È possibile scegliere la modalità di configurazione.

  Di seguito sono riportati tre esempi di configurazioni:

  - Ogni nodo del cluster si trova in una zona locale diversa e il mediatore in una zona di disponibilità pubblica.
  - Un nodo cluster in una zona locale, il mediatore in una zona locale e il secondo nodo cluster si trovano in una zona di disponibilità.
  - Ciascun nodo del cluster e il mediatore si trovano in zone locali separate.

Dischi e tipi di istanza supportati

L'unico tipo di disco supportato è GP2. Sono attualmente supportate le seguenti famiglie di tipi di istanza EC2 con dimensioni da xlarge a 4XLarge:

- M5
- C5
- C5d
- R5
- R5d

> Cloud Volumes ONTAP supporta solo queste configurazioni. La selezione di tipi di dischi non supportati o istanze non qualificate nella configurazione della zona locale AWS potrebbe causare un errore di implementazione. Il tiering dei dati in AWS S3 non è disponibile nelle zone locali di AWS a causa della mancanza di connettività.

Fare riferimento alla documentazione AWS per i dettagli più recenti e completi di"Documentazione AWS: Tipi di istanza EC2 nelle zone locali" .

Come funziona lo storage in una coppia ha

A differenza di un cluster ONTAP, lo storage in una coppia Cloud Volumes ONTAP ha non viene condiviso tra i nodi. I dati vengono invece sottoposti a mirroring sincrono tra i nodi in modo che siano disponibili in caso di guasto.

Allocazione dello storage

Quando si crea un nuovo volume e sono necessari dischi aggiuntivi, BlueXP assegna lo stesso numero di dischi a entrambi i nodi, crea un aggregato mirrorato e crea il nuovo volume. Ad esempio, se sono necessari due dischi per il volume, BlueXP assegna due dischi per nodo per un totale di quattro dischi.

Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto lo storage per il nodo attivo.

È possibile impostare una configurazione Active-Active solo quando si utilizza BlueXP nella vista del sistema di storage.

Aspettative di performance

Una configurazione Cloud Volumes ONTAP ha replica in modo sincrono i dati tra i nodi, consumando la larghezza di banda della rete. Di conseguenza, rispetto a una configurazione Cloud Volumes ONTAP a nodo singolo, è possibile aspettarsi le seguenti performance:

- Per le configurazioni ha che servono dati da un solo nodo, le prestazioni di lettura sono paragonabili alle prestazioni di lettura di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono inferiori.
- Per le configurazioni ha che servono dati da entrambi i nodi, le performance di lettura sono superiori rispetto alle performance di lettura di una configurazione a nodo singolo e le performance di scrittura sono uguali o superiori.

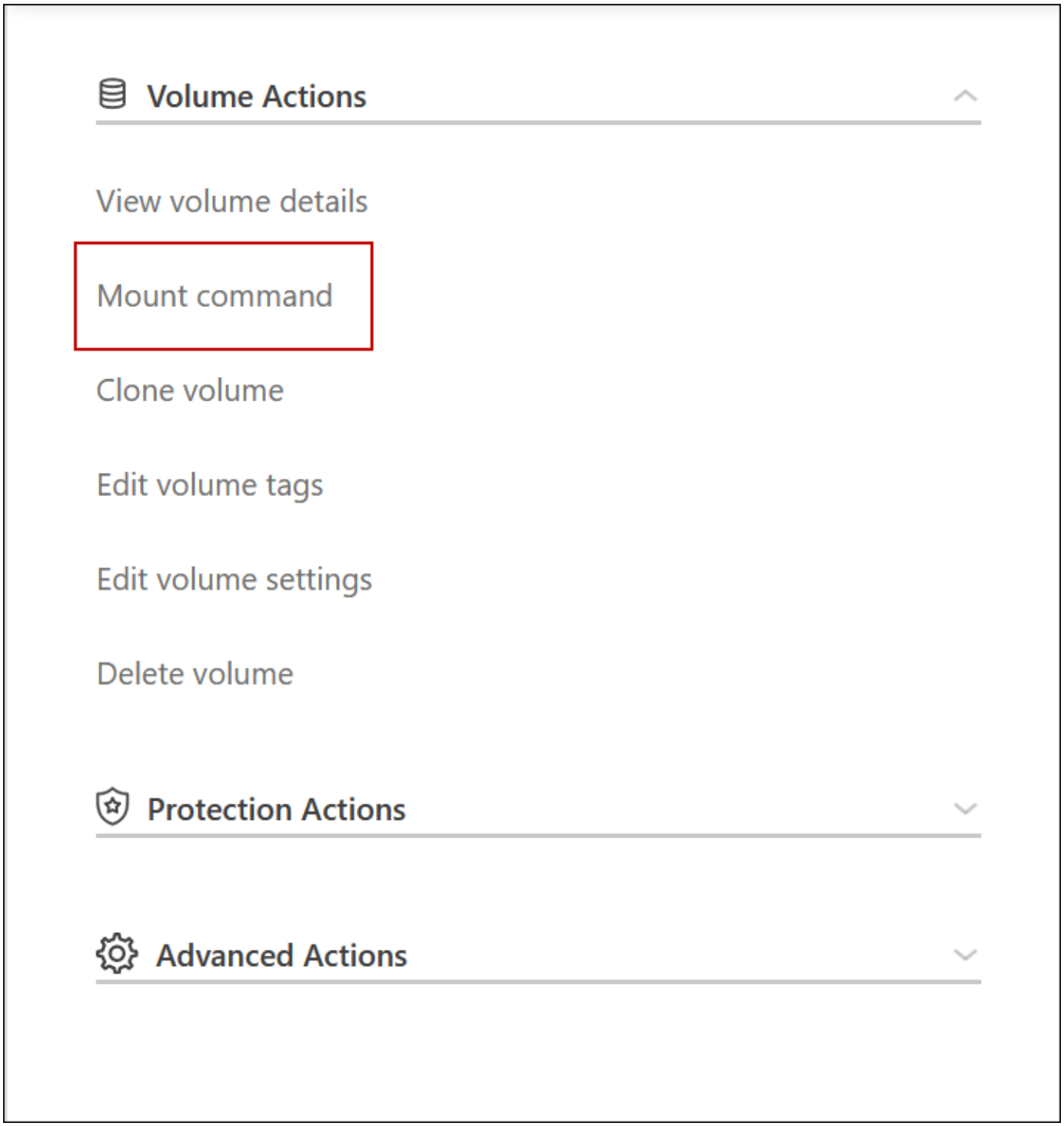
Per ulteriori informazioni sulle prestazioni di Cloud Volumes ONTAP, fare riferimento a "Performance".

Accesso client allo storage

I client devono accedere ai volumi NFS e CIFS utilizzando l'indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l'indirizzo IP del nodo partner, il traffico passa tra entrambi i nodi, riducendo le performance.

Se si sposta un volume tra nodi in una coppia ha, è necessario rimontarlo utilizzando l'indirizzo IP dell'altro nodo. In caso contrario, si possono ottenere prestazioni ridotte. Se i client supportano i riferimenti NFSv4 o il reindirizzamento delle cartelle per CIFS, è possibile attivare tali funzionalità sui sistemi Cloud Volumes ONTAP per evitare di rimontare il volume. Per ulteriori informazioni, fare riferimento alla documentazione di ONTAP.

È possibile identificare facilmente l'indirizzo IP corretto tramite l'opzione *Mount Command* nel pannello Manage Volumes (Gestisci volumi) di BlueXP.



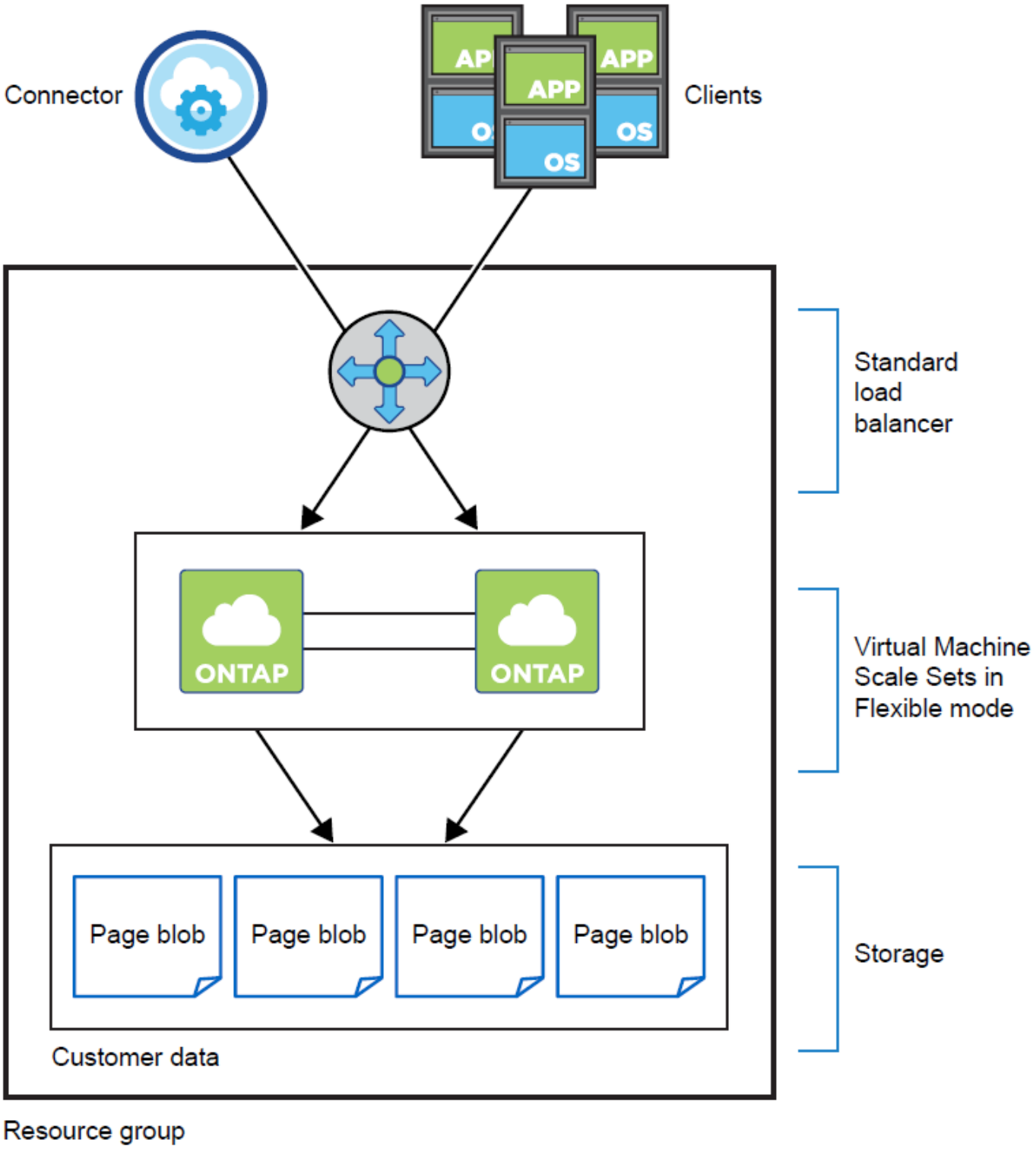
Scopri di più sulle coppie ha di Cloud Volumes ONTAP in Azure

Una coppia ha (high Availability) di Cloud Volumes ONTAP offre affidabilità di livello Enterprise e operazioni continue in caso di guasti nel tuo ambiente cloud. In Azure, lo storage viene condiviso tra i due nodi.

Componenti HA

HA configurazione di una singola zona di disponibilità con blob di pagina

La configurazione di un blob di pagina Cloud Volumes ONTAP ha in Azure include i seguenti componenti:



Tenere presente quanto segue sui componenti di Azure che BlueXP implementa per te:

Bilanciamento del carico standard Azure

Il bilanciamento del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP ha.

Macchine virtuali in singole zone di disponibilità

A partire da Cloud Volumes ONTAP 9.15.1, puoi creare e gestire macchine virtuali eterogenee (VM) in una singola zona di disponibilità (AZ). È possibile implementare nodi ad alta disponibilità (ha) in domini di errore separati all'interno della stessa AZ, garantendo una disponibilità ottimale. Per ulteriori informazioni sulla modalità di orchestrazione flessibile che abilita questa funzionalità, consultare la sezione "Documentazione di Microsoft Azure: Set di scalabilità delle macchine virtuali".

Dischi

I dati dei clienti si trovano nelle pagine di Premium Storage. Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre richiesto storage aggiuntivo per "dati di boot, root e core".

Account storage

- Per i dischi gestiti è necessario un account di storage.
- Per le pagine blob dello storage Premium sono necessari uno o più account di storage, in quanto viene raggiunto il limite di capacità del disco per account di storage.

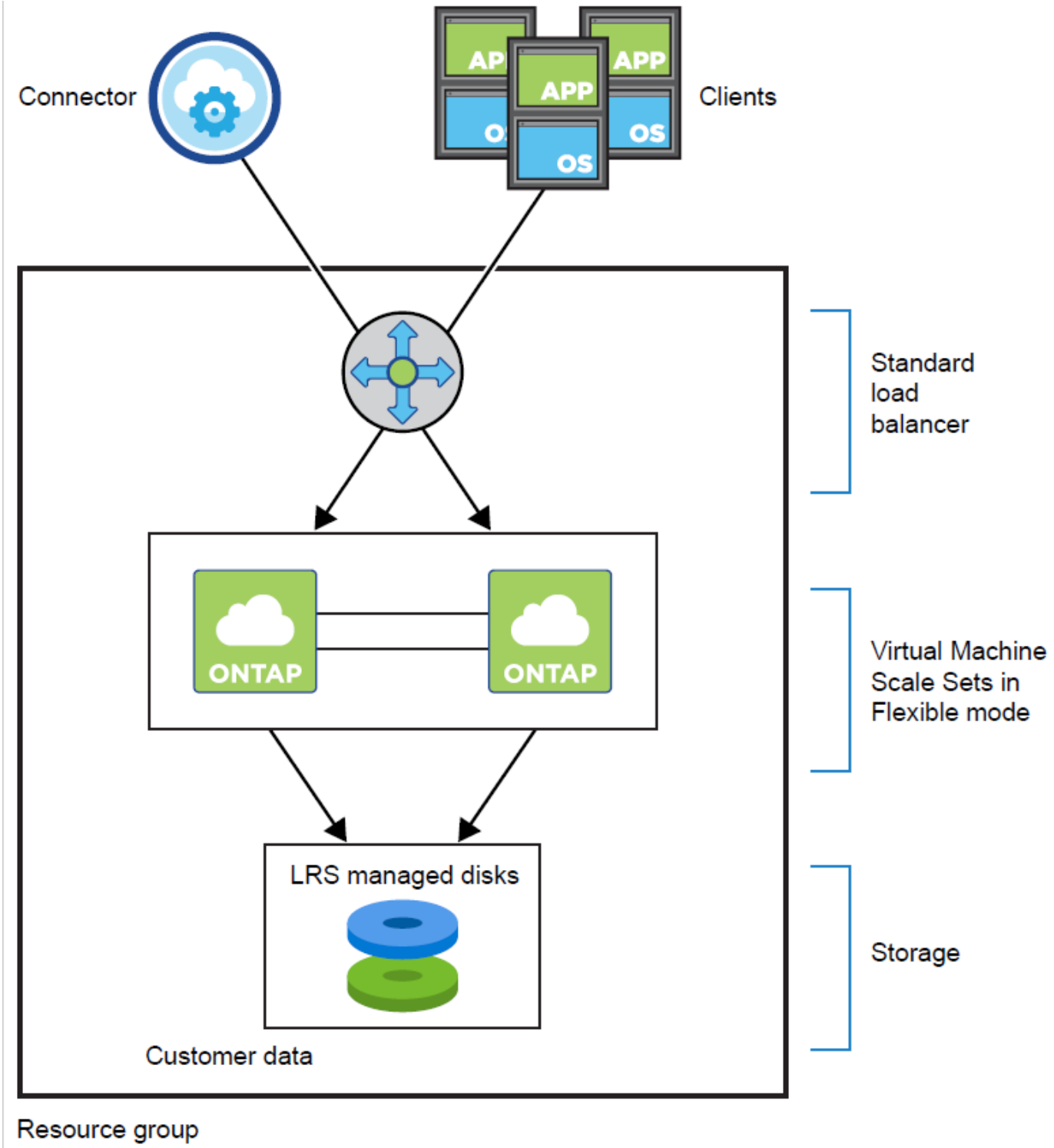
  "Documentazione Microsoft Azure: Obiettivi di performance e scalabilità dello storage Azure per gli account storage".

- Per il tiering dei dati sullo storage Azure Blob è necessario un account storage.
- A partire da Cloud Volumes ONTAP 9.7, gli account storage creati da BlueXP per le coppie ha sono account storage v2 generici.
- Durante la creazione di un ambiente di lavoro, è possibile attivare una connessione HTTPS da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage Azure. L'attivazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato l'ambiente di lavoro.

> A partire da Cloud Volumes ONTAP 9.15.0P1, i blob delle pagine di Azure non sono più supportati per le nuove implementazioni di coppie ad alta disponibilità. Se al momento utilizzi Azure page blob in implementazioni esistenti di coppie ad alta disponibilità, puoi migrare a tipi di istanze di macchine virtuali più recenti nelle macchine virtuali della serie Edsv4 e nelle macchine virtuali della serie Edsv5. "Scopri di più sulle configurazioni supportate in Azure".

Configurazione DI una singola zona di disponibilità HA con dischi gestiti condivisi

La configurazione di una singola zona di disponibilità di Cloud Volumes ONTAP ha eseguita su un disco gestito condiviso include i seguenti componenti:



Tenere presente quanto segue sui componenti di Azure che BlueXP implementa per te:

Bilanciamento del carico standard Azure

Il bilanciamento del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP ha.

Macchine virtuali in singole zone di disponibilità

A partire da Cloud Volumes ONTAP 9.15.1, puoi creare e gestire macchine virtuali eterogenee (VM) in una singola zona di disponibilità (AZ). È possibile implementare nodi ad alta disponibilità (ha) in domini di errore separati all'interno della stessa AZ, garantendo una disponibilità ottimale. Per ulteriori informazioni sulla modalità di orchestrazione flessibile che abilita questa funzionalità, consultare la sezione "Documentazione

di Microsoft Azure: Set di scalabilità delle macchine virtuali".

L'implementazione zonale utilizza dischi gestiti SSD Premium da v2 GB quando vengono soddisfatte le seguenti condizioni:

- La versione di Cloud Volumes ONTAP è la 9.15.1 o successiva.
- La regione e la zona selezionate supportano dischi gestiti SSD Premium da v2 GB. Per informazioni sulle regioni supportate, fare riferimento a "Sito Web di Microsoft Azure: Prodotti disponibili per area geografica".
- L'abbonamento è registrato per Microsoft "Funzione Microsoft.Compute/VMOrchestratorZonalMultiFD".

Dischi

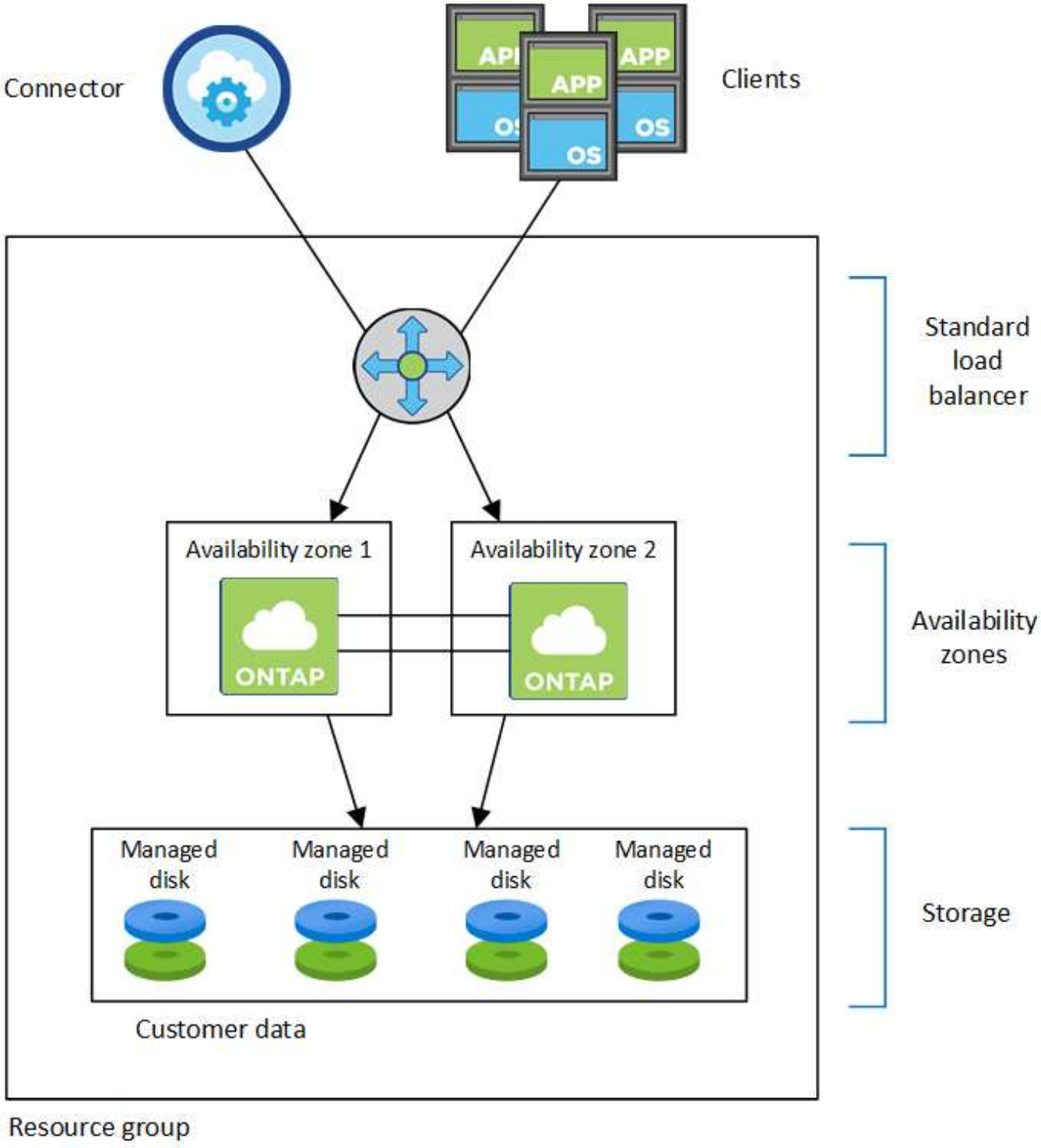
I dati del cliente risiedono su dischi gestiti LRS (Local Redundant Storage). Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre necessario ulteriore spazio di archiviazione per "Dati di boot, root, partner root, core e NVRAM".

Account storage

Gli account storage vengono utilizzati per le implementazioni gestite basate su disco per gestire i log diagnostici e il tiering per lo storage blob.

HA configurazione di più zone di disponibilità

La configurazione di una zona di disponibilità multipla Cloud Volumes ONTAP ha in Azure include i seguenti componenti:



Tenere presente quanto segue sui componenti di Azure che BlueXP implementa per te:

Bilanciamento del carico standard Azure

Il bilanciamento del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP ha.

Zone di disponibilità

LA configurazione HA a più zone di disponibilità utilizza un modello di implementazione in cui due nodi Cloud Volumes ONTAP vengono implementati in diverse zone di disponibilità, assicurandosi che i nodi si trovino in diversi domini di errore per fornire ridondanza e disponibilità. Per scoprire in che modo i set di scalabilità delle macchine virtuali in modalità di orchestrazione flessibile possono utilizzare le zone di

disponibilità in Azure, consultare "Documentazione di Microsoft Azure: Creare un set di scalabilità della macchina virtuale che utilizzi le zone di disponibilità" .

Dischi

I dati del cliente risiedono su dischi gestiti con ZRS (zone-Redundant Storage). Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre richiesto storage aggiuntivo per "dati di boot, root, root partner e core".

Account storage

Gli account storage vengono utilizzati per le implementazioni gestite basate su disco per gestire i log diagnostici e il tiering per lo storage blob.

RPO e RTO

Una configurazione ad alta disponibilità dei dati viene mantenuta come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi. I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.
- L'obiettivo del tempo di ripristino (RTO) è di 120 secondi. In caso di interruzione, i dati devono essere disponibili in 120 secondi o meno.

Takeover e giveback dello storage

Analogamente a un cluster ONTAP fisico, lo storage in una coppia Azure ha viene condiviso tra i nodi. Le connessioni allo storage del partner consentono a ciascun nodo di accedere allo storage dell'altro in caso di *takeover*. I meccanismi di failover del percorso di rete garantiscono che client e host continuino a comunicare con il nodo esistente. Il partner _restituisce lo storage quando il nodo viene riportato in linea.

Per le configurazioni NAS, gli indirizzi IP dei dati migrano automaticamente tra i nodi ha in caso di guasti.

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

> Per informazioni sulle specifiche configurazioni host che supportano ALUA, consultare la "Tool di matrice di interoperabilità NetApp" e la "Guida agli host SAN e ai client cloud" per il sistema operativo host in uso.

Per impostazione predefinita, le funzioni di Takeover, risync e giveback dello storage sono tutte automatiche. Non è richiesta alcuna azione da parte dell'utente.

Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi forniscono dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto il controllo dello storage per il nodo attivo.

Scopri di più sulle coppie ha di Cloud Volumes ONTAP in Google Cloud

Una configurazione ha (High Availability) di Cloud Volumes ONTAP offre operazioni senza interruzioni e tolleranza agli errori. In Google Cloud, i dati vengono sottoposti a mirroring sincrono tra i due nodi.

Componenti HA

Le configurazioni Cloud Volumes ONTAP ha in Google Cloud includono i seguenti componenti:

- Due nodi Cloud Volumes ONTAP i cui dati vengono sottoposti a mirroring sincrono l'uno con l'altro.
- Istanza di mediatore che fornisce un canale di comunicazione tra i nodi per assistere nei processi di acquisizione e giveback dello storage.
- Una o tre zone (consigliato).

  Se si sceglie tre zone, i due nodi e il mediatore si trovano in zone Google Cloud separate.

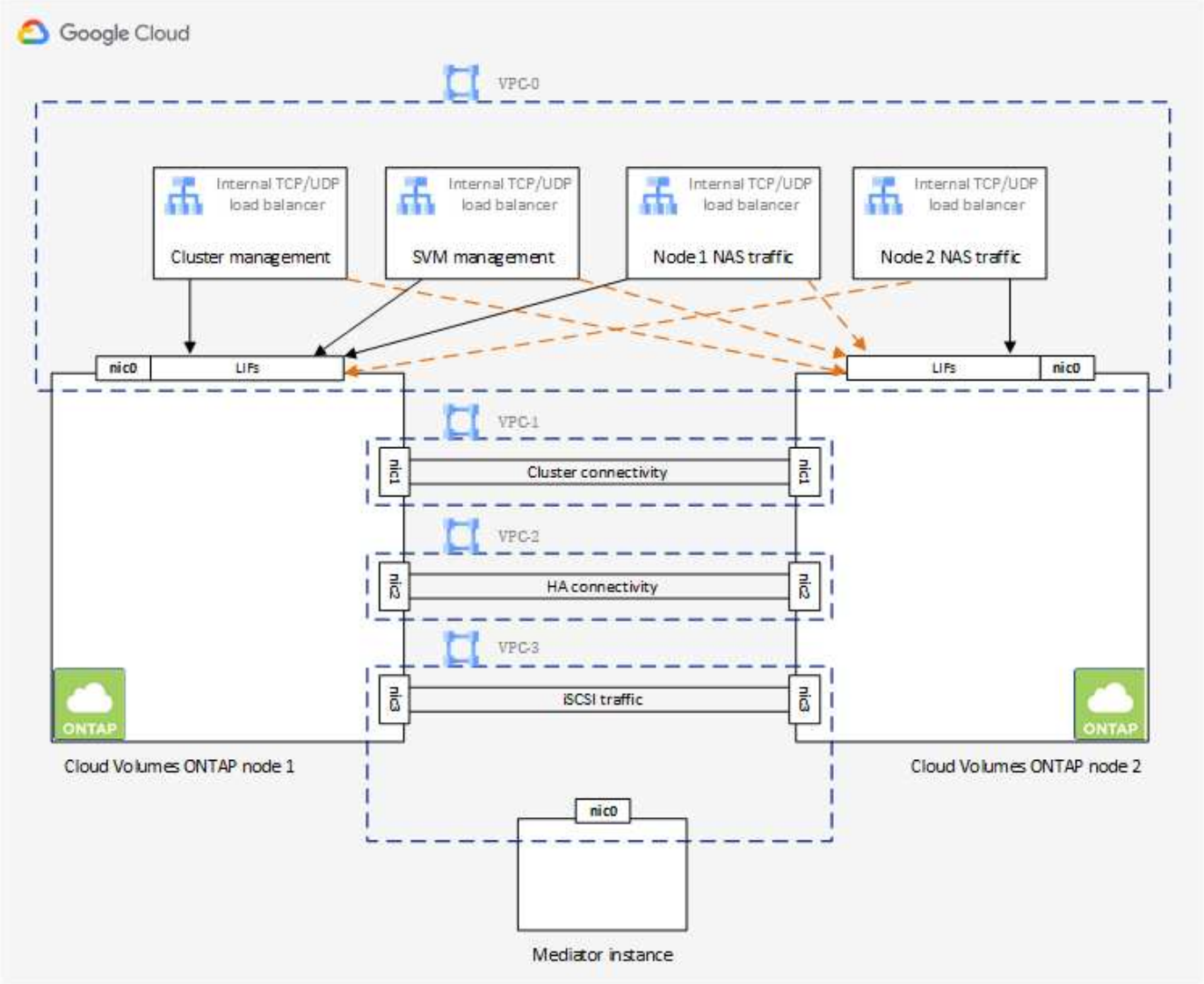
- Quattro Virtual Private Clouds (VPC).

  La configurazione utilizza quattro VPC perché GCP richiede che ogni interfaccia di rete risieda in una rete VPC separata.

- Quattro bilanciatori di carico interni di Google Cloud (TCP/UDP) che gestiscono il traffico in entrata verso la coppia Cloud Volumes ONTAP ha.

"Scopri i requisiti di rete", Tra cui ulteriori dettagli su bilanciamento del carico, VPC, indirizzi IP interni, subnet e altro ancora.

La seguente immagine concettuale mostra una coppia Cloud Volumes ONTAP ha e i suoi componenti:



Mediatore

Di seguito sono riportati alcuni dettagli chiave sull'istanza di mediatore in Google Cloud:

Tipo di istanza

e2-micro (in precedenza era stata utilizzata un'istanza f1-micro)

Dischi

Due dischi persistenti standard da 10 GiB ciascuno

Sistema operativo

Debian 11

> Per Cloud Volumes ONTAP 9.10.0 e versioni precedenti, Debian 10 è stata installata sul mediatore.

Aggiornamenti

Quando si aggiorna Cloud Volumes ONTAP, BlueXP aggiorna anche l'istanza del mediatore in base alle necessità.

Accesso all'istanza

Per Debian, l'utente cloud predefinito è `admin`. Google Cloud crea e aggiunge certificati per `admin` Utente quando viene richiesto l'accesso SSH tramite la console Google Cloud o la riga di comando gcloud. È possibile specificare `sudo` per ottenere i privilegi di root.

Agenti di terze parti

Gli agenti di terze parti o le estensioni delle macchine virtuali non sono supportati sull'istanza del mediatore.

Takeover e giveback dello storage

Se un nodo non funziona, l'altro nodo può servire i dati per il proprio partner per fornire un servizio dati continuo. I client possono accedere agli stessi dati dal nodo partner perché i dati sono stati sottoposti a mirroring sincrono con il partner.

Dopo il riavvio del nodo, il partner deve risincronizzare i dati prima di poter restituire lo storage. Il tempo necessario per la risincronizzazione dei dati dipende dalla quantità di dati modificati mentre il nodo era inattivo.

Per impostazione predefinita, le funzioni di Takeover, risync e giveback dello storage sono tutte automatiche. Non è richiesta alcuna azione da parte dell'utente.

RPO e RTO

Una configurazione ad alta disponibilità dei dati viene mantenuta come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi.

  I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.

- L'obiettivo del tempo di ripristino (RTO) è di 120 secondi.

  In caso di interruzione, i dati devono essere disponibili in 120 secondi o meno.

Modelli di implementazione HA

È possibile garantire l'elevata disponibilità dei dati implementando una configurazione ha in più zone o in una singola zona.

Zone multiple (consigliato)

L'implementazione di una configurazione ha in tre zone garantisce la disponibilità continua dei dati in caso di guasto all'interno di una zona. Si noti che le prestazioni di scrittura sono leggermente inferiori rispetto all'utilizzo di una singola zona, ma sono minime.

Zona singola

Quando viene implementato in una singola zona, una configurazione Cloud Volumes ONTAP ha utilizza una policy di posizionamento distribuita. Questa policy garantisce che una configurazione ha sia protetta da un singolo punto di guasto all'interno della zona, senza dover utilizzare zone separate per ottenere l'isolamento degli errori.

Questo modello di implementazione riduce i costi perché non sono previsti costi di uscita dei dati tra le zone.

Come funziona lo storage in una coppia ha

A differenza di un cluster ONTAP, lo storage in una coppia Cloud Volumes ONTAP ha in GCP non viene condiviso tra i nodi. I dati vengono invece sottoposti a mirroring sincrono tra i nodi in modo che siano disponibili in caso di guasto.

Allocazione dello storage

Quando si crea un nuovo volume e sono necessari dischi aggiuntivi, BlueXP assegna lo stesso numero di dischi a entrambi i nodi, crea un aggregato mirrorato e crea il nuovo volume. Ad esempio, se sono necessari due dischi per il volume, BlueXP assegna due dischi per nodo per un totale di quattro dischi.

Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto lo storage per il nodo attivo.

Aspettative di performance per una configurazione ha

Una configurazione Cloud Volumes ONTAP ha replica in modo sincrono i dati tra i nodi, consumando la larghezza di banda della rete. Di conseguenza, rispetto a una configurazione Cloud Volumes ONTAP a nodo singolo, è possibile aspettarsi le seguenti performance:

- Per le configurazioni ha che servono dati da un solo nodo, le prestazioni di lettura sono paragonabili alle prestazioni di lettura di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono inferiori.
- Per le configurazioni ha che servono dati da entrambi i nodi, le performance di lettura sono superiori rispetto alle performance di lettura di una configurazione a nodo singolo e le performance di scrittura sono uguali o superiori.

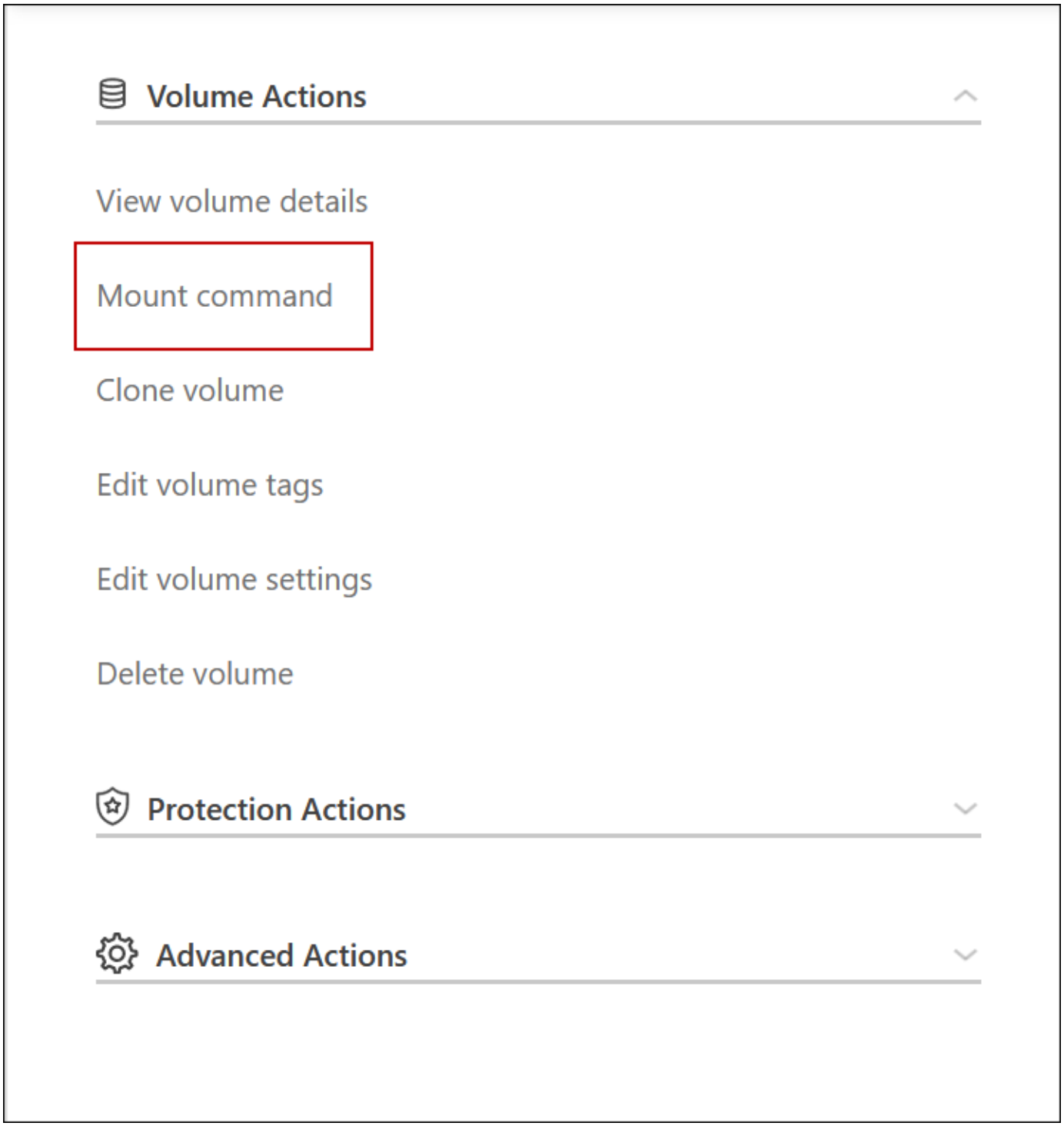
Per ulteriori informazioni sulle prestazioni di Cloud Volumes ONTAP, fare riferimento a "Performance".

Accesso client allo storage

I client devono accedere ai volumi NFS e CIFS utilizzando l'indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l'indirizzo IP del nodo partner, il traffico passa tra entrambi i nodi, riducendo le performance.

Se si sposta un volume tra nodi in una coppia ha, è necessario rimontarlo utilizzando l'indirizzo IP dell'altro nodo. In caso contrario, si possono ottenere prestazioni ridotte. Se i client supportano i riferimenti NFSv4 o il reindirizzamento delle cartelle per CIFS, è possibile attivare tali funzionalità sui sistemi Cloud Volumes ONTAP per evitare di rimontare il volume. Per ulteriori informazioni, fare riferimento alla documentazione di ONTAP.

È possibile identificare facilmente l'indirizzo IP corretto tramite l'opzione *Mount Command* nel pannello Manage Volumes (Gestisci volumi) di BlueXP.



Link correlati

- "Scopri i requisiti di rete"
- "Scopri come iniziare a utilizzare GCP"

Operazioni non disponibili quando un nodo nella coppia ha Cloud Volumes ONTAP è offline

Quando un nodo in una coppia ha non è disponibile, l'altro nodo serve i dati per il partner per fornire un servizio dati continuo. Si chiama *storage Takeover*. Diverse azioni non

sono disponibili fino al completamento del giveback in storage.

Quando un nodo in una coppia ha non è disponibile, lo stato dell'ambiente di lavoro in BlueXP è *degradato*.

Le seguenti azioni non sono disponibili dall'acquisizione dello storage BlueXP:

- Registrazione del supporto
- Modifiche della licenza
- Modifiche all'istanza o al tipo di macchina virtuale
- La velocità di scrittura cambia
- Configurazione CIFS
- Modifica della posizione dei backup di configurazione
- Impostazione della password del cluster
- Gestione di dischi e aggregati (allocazione avanzata)

Queste azioni sono nuovamente disponibili al termine del giveback dello storage e quando lo stato dell'ambiente di lavoro torna alla normalità.

Scopri la crittografia dei dati e la protezione dal ransomware di Cloud Volumes ONTAP

Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.

Crittografia dei dati inattivi

Cloud Volumes ONTAP supporta le seguenti tecnologie di crittografia:

- Soluzioni di crittografia NetApp (NVE e NAE)
- Servizio di gestione delle chiavi AWS
- Azure Storage Service Encryption
- Crittografia predefinita di Google Cloud Platform

Puoi utilizzare le soluzioni di crittografia NetApp con crittografia nativa del tuo cloud provider, che crittografa i dati a livello di hypervisor. In questo modo si fornirebbe una doppia crittografia, che potrebbe essere utile per i dati molto sensibili. Quando si accede ai dati crittografati, questi vengono crittografati due volte, una volta a livello di hypervisor (utilizzando le chiavi del cloud provider) e poi di nuovo utilizzando le soluzioni di crittografia NetApp (utilizzando le chiavi di un gestore di chiavi esterno).

Soluzioni di crittografia NetApp (NVE e NAE)

Cloud Volumes ONTAP supporta "NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE)". NVE e NAE sono soluzioni basate su software che consentono la crittografia dei dati a riposo dei volumi conforme allo standard FIPS 140-2. Sia NVE che NAE utilizzano la crittografia AES a 256 bit.

- NVE crittografa i dati inattivi un volume alla volta. Ogni volume di dati dispone di una chiave di crittografia univoca.

- NAE è un'estensione di NVE, che crittografa i dati per ogni volume e i volumi condividono una chiave nell'aggregato. NAE consente inoltre di deduplicare i blocchi comuni di tutti i volumi dell'aggregato.

Cloud Volumes ONTAP supporta sia NVE che NAE con servizi di gestione delle chiavi esterni (EKM) forniti da AWS, Azure e Google Cloud, incluse soluzioni di terze parti come Fortanix. A differenza di ONTAP, per Cloud Volumes ONTAP le chiavi di crittografia vengono generate dal provider cloud, non in ONTAP.

Cloud Volumes ONTAP utilizza i servizi standard KMIP (Key Management Interoperability Protocol) utilizzati da ONTAP. Per ulteriori informazioni sui servizi supportati, fare riferimento a "Tool di matrice di interoperabilità" .

Se utilizzi NVE, hai la possibilità di utilizzare il key vault del tuo provider cloud per proteggere le chiavi di crittografia ONTAP:

- AWS Key Management Service (KMS)
- Azure Key Vault (AKV)
- Servizio di gestione delle chiavi Google Cloud

I nuovi aggregati hanno NetApp aggregate Encryption (NAE) abilitato per impostazione predefinita dopo aver configurato un gestore di chiavi esterno. Nei nuovi volumi che non fanno parte di un aggregato NAE, NVE è abilitato per impostazione predefinita (ad esempio, se sono presenti aggregati esistenti creati prima di configurare un gestore chiavi esterno).

La configurazione di un gestore di chiavi supportato è l'unica operazione necessaria. Per istruzioni sulla configurazione, fare riferimento alla "Crittografa i volumi con le soluzioni per la crittografia NetApp".

Servizio di gestione delle chiavi AWS

Quando si avvia un sistema Cloud Volumes ONTAP in AWS, è possibile attivare la crittografia dei dati utilizzando "AWS Key Management Service (KMS)". BlueXP richiede le chiavi dati utilizzando una chiave master del cliente (CMK).

Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP.

Se si desidera utilizzare questa opzione di crittografia, assicurarsi che AWS KMS sia configurato correttamente. Per informazioni, fare riferimento alla "Configurazione di AWS KMS".

Azure Storage Service Encryption

I dati vengono automaticamente crittografati in Cloud Volumes ONTAP in Azure utilizzando una chiave gestita da "Azure Storage Service Encryption" Microsoft.

Se preferisci, puoi utilizzare le tue chiavi di crittografia. "Scopri come configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure".

Crittografia predefinita di Google Cloud Platform

"Crittografia dei dati inattivi di Google Cloud Platform" È attivato per impostazione predefinita per Cloud Volumes ONTAP. Non è richiesta alcuna configurazione.

Mentre Google Cloud Storage crittografa sempre i tuoi dati prima che vengano scritti su disco, puoi utilizzare le API BlueXP per creare un sistema Cloud Volumes ONTAP che utilizza *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che vengono generate e gestite in GCP utilizzando il Cloud Key Management Service.

"Scopri di più".

Scansione virus ONTAP

È possibile utilizzare la funzionalità antivirus integrata nei sistemi ONTAP per proteggere i dati da virus o altri codici dannosi.

La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

Per informazioni sui fornitori, il software e le versioni supportate da Vscan, fare riferimento alla "Matrice di interoperabilità NetApp" .

Per informazioni su come configurare e gestire la funzionalità antivirus sui sistemi ONTAP, fare riferimento alla "Guida alla configurazione antivirus di ONTAP 9" .

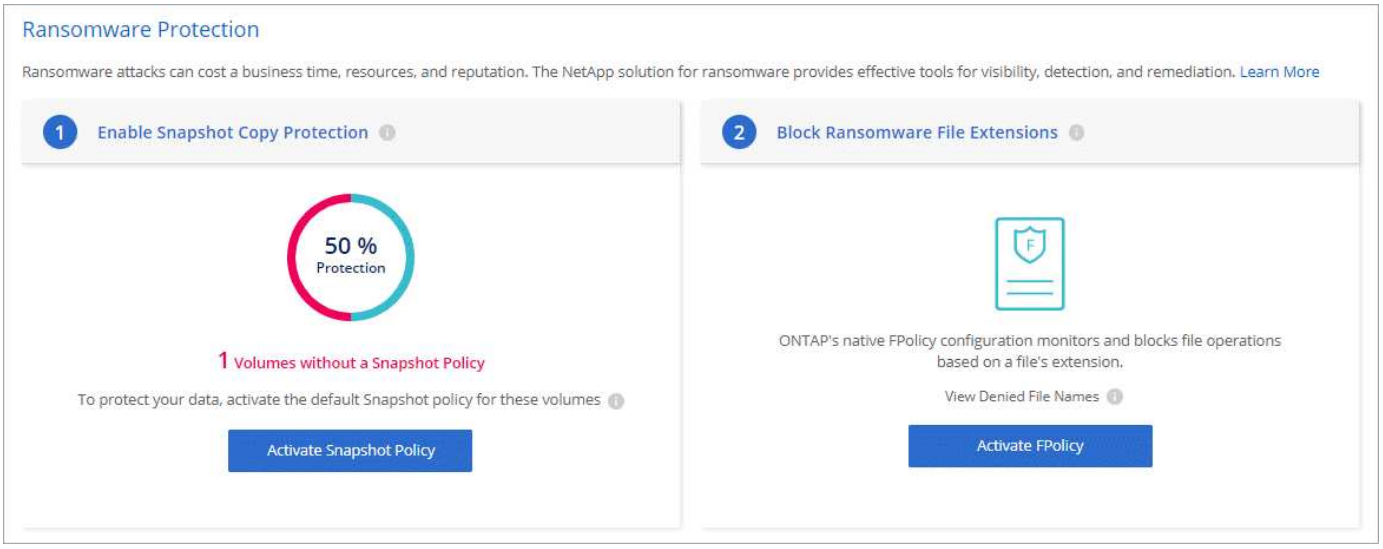
Protezione ransomware

Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. BlueXP consente di implementare la soluzione NetApp per ransomware, che fornisce strumenti efficaci per la visibilità, il rilevamento e la risoluzione dei problemi.

- BlueXP identifica i volumi che non sono protetti da un criterio Snapshot e consente di attivare il criterio Snapshot predefinito su tali volumi.

  Le copie Snapshot sono di sola lettura, impedendo la corruzione del ransomware. Possono inoltre offrire la granularità necessaria per creare immagini di una singola copia di file o di una soluzione completa di disaster recovery.

- BlueXP consente inoltre di bloccare le estensioni di file ransomware comuni attivando la soluzione FPolicy di ONTAP.



"Scopri come implementare la soluzione NetApp per ransomware".

Scopri il monitoraggio delle performance per i workload Cloud Volumes ONTAP

Puoi esaminare i risultati delle performance per aiutarti a decidere quali carichi di lavoro sono appropriati per Cloud Volumes ONTAP.

Report tecnici sulle performance

- Cloud Volumes ONTAP per AWS

  "Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni"

- Cloud Volumes ONTAP per Microsoft Azure

  "Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi"

- Cloud Volumes ONTAP per Google Cloud

  "Report tecnico NetApp 4816: Caratterizzazione delle performance di Cloud Volumes ONTAP per Google Cloud"

Performance della CPU

I nodi Cloud Volumes ONTAP risultano altamente utilizzati (oltre il 90%) dagli strumenti di monitoraggio del tuo cloud provider. Questo perché ONTAP riserva tutte le vCPU presentate alla macchina virtuale in modo che siano disponibili quando necessario.

Per ulteriori informazioni, fare riferimento a. "Articolo della Knowledge base di NetApp su come monitorare l'utilizzo della CPU ONTAP utilizzando la CLI"

Gestione delle licenze per BYOL basato su nodo

Ogni sistema Cloud Volumes ONTAP con una BYOL (Bring Your Own License) basato su nodo deve disporre di una licenza di sistema installata con un abbonamento attivo. BlueXP semplifica il processo gestendo le licenze e visualizzando un avviso prima della scadenza.

> Una licenza basata su nodi è la licenza di precedente generazione per Cloud Volumes ONTAP. Una licenza basata su nodi può essere acquistata da NetApp (BYOL) ed è disponibile per i rinnovi di licenza solo in casi specifici.

"Scopri di più sulle opzioni di licenza Cloud Volumes ONTAP".

"Scopri di più su come gestire le licenze basate su nodo".

Licenze di sistema BYOL

Le licenze basate su nodi possono essere acquistate da NetApp. Il numero di licenze acquistabili per un

singolo sistema a nodo o per una coppia HA è illimitato.

> NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, fare riferimento a "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAPP" .

Una licenza basata su nodi fornisce fino a 368 TiB di capacità per un singolo nodo o una coppia HA. Potresti aver acquistato più licenze per un sistema BYOL Cloud Volumes ONTAP per allocare più di 368 TiB di capacità. Ad esempio, potresti avere due licenze per allocare fino a 736 TiB di capacità a Cloud Volumes ONTAP. Oppure potresti avere quattro licenze per ottenere fino a 1,4 PiB.

Tenere presente che i limiti dei dischi possono impedire di raggiungere il limite di capacità utilizzando solo i dischi. È possibile superare il limite di dischi di "tiering dei dati inattivi sullo storage a oggetti". Per informazioni sui limiti dei dischi, fare riferimento a. "Limiti di storage nelle note di rilascio di Cloud Volumes ONTAP".

Gestione delle licenze per un nuovo sistema

Quando si crea un sistema BYOL basato su nodo, BlueXP richiede il numero di serie della licenza e l'account NetApp Support Site. BlueXP utilizza l'account per scaricare il file di licenza da NetApp e installarlo sul sistema Cloud Volumes ONTAP.

"Scopri come aggiungere account NetApp Support Site a BlueXP".

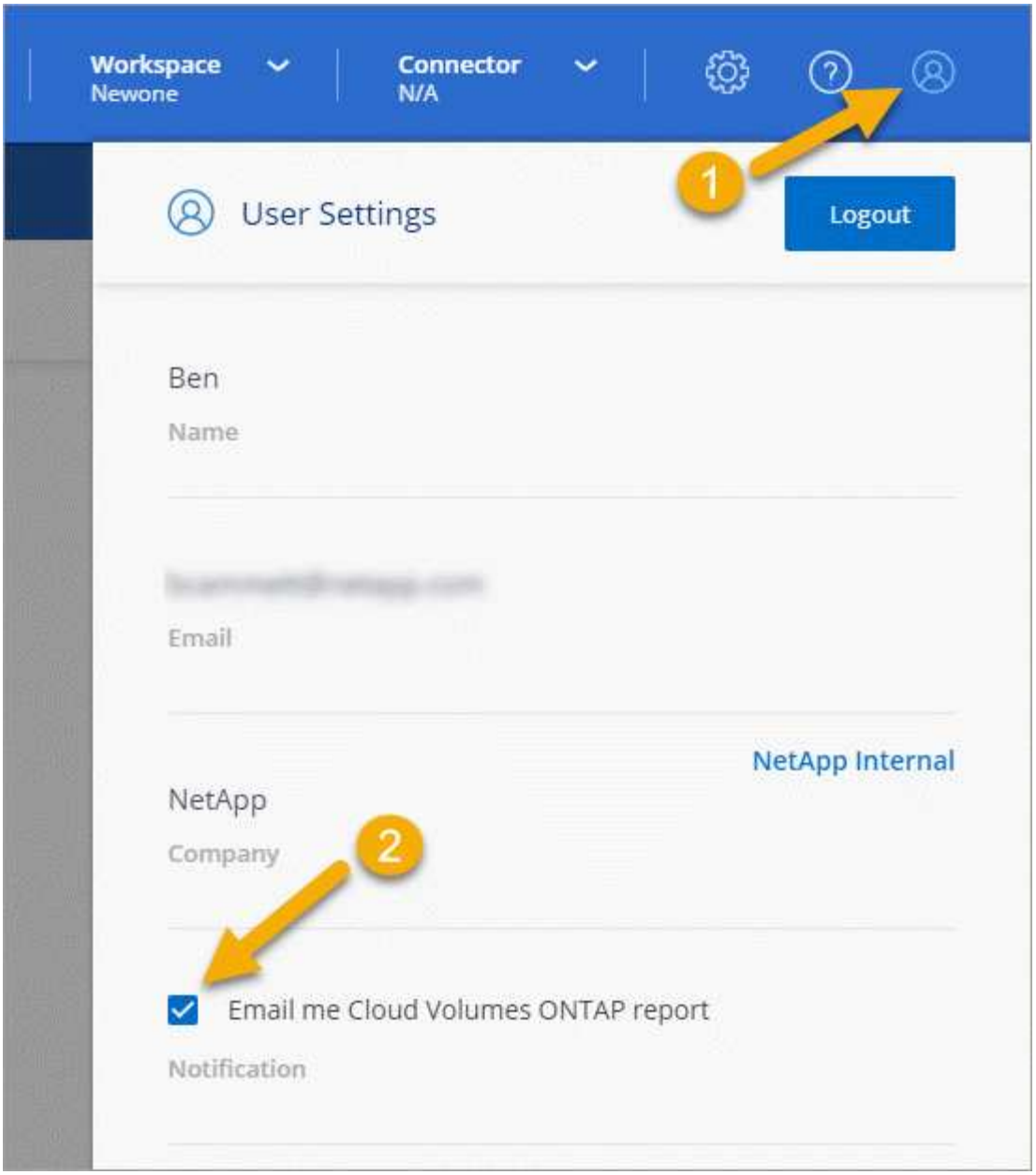
Se BlueXP non riesce ad accedere al file di licenza tramite la connessione Internet sicura, è possibile "Procurarsi il file e caricarlo manualmente su BlueXP".

Scadenza della licenza

BlueXP visualizza un avviso 30 giorni prima della scadenza di una licenza basata su nodo e di nuovo alla scadenza della licenza. La seguente immagine mostra un avviso di scadenza di 30 giorni visualizzato nell'interfaccia utente:

È possibile selezionare l'ambiente di lavoro per rivedere il messaggio.

BlueXP include un avviso di scadenza della licenza nel report Cloud Volumes ONTAP inviato tramite e-mail, se sei un amministratore dell'organizzazione o dell'account BlueXP e hai attivato l'opzione:



Il report inviato tramite e-mail include l'avviso di scadenza della licenza ogni 2 settimane.

Se la licenza non viene rinnovata in tempo, il sistema Cloud Volumes ONTAP si spegne automaticamente. Se viene riavviato, si spegne di nuovo.

Rinnovo della licenza

Se si rinnova un abbonamento BYOL basato su nodi 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 la connessione Internet sicura, è possibile "Procurarsi il file e caricarlo manualmente su BlueXP".

Trasferimento della licenza a un nuovo sistema

Una licenza BYOL basata su nodo è trasferibile tra sistemi Cloud Volumes ONTAP quando si elimina un sistema esistente e ne si crea uno nuovo utilizzando la stessa licenza.

Ad esempio, è possibile eliminare un sistema con licenza esistente e utilizzare la licenza con un nuovo sistema BYOL in un VPC/VNET o provider cloud diverso. Nota: Solo i numeri seriali *indipendenti dal cloud* funzionano in qualsiasi cloud provider. I numeri di serie indipendenti dal cloud iniziano con il prefisso *908xxxx*.

È importante notare che la licenza BYOL è legata alla tua azienda e a un set specifico di credenziali del sito di supporto NetApp.

Scopri in che modo AutoSupport e Digital Advisor vengono utilizzati per Cloud Volumes ONTAP

Il componente AutoSupport di ONTAP raccoglie la telemetria e la invia per l'analisi. Il consulente digitale Active IQ (o consulente digitale) analizza i dati di AutoSupport e offre assistenza e ottimizzazione proattive. Utilizzando l'intelligenza artificiale, il Digital Advisor può identificare i potenziali problemi e aiutarti a risolverli prima che abbiano un impatto sul tuo business.

Digital Advisor ti consente di ottimizzare la tua infrastruttura dati nel tuo cloud ibrido globale offrendo analisi predittive e supporto proattivo attraverso un portale basato sul cloud e un'app mobile. Le informazioni e i consigli basati sui dati di Digital Advisor sono disponibili per tutti i clienti NetApp con un contratto SupportEdge attivo (le funzionalità variano in base al prodotto e al Tier di supporto).

Ecco alcune cose che potete fare con Digital Advisor:

- Pianificare gli aggiornamenti.

  Digital Advisor identifica i problemi dell'ambiente che possono essere risolti effettuando l'aggiornamento a una versione più recente di ONTAP, mentre il componente Upgrade Advisor consente di pianificare un aggiornamento di successo.

- Visualizza lo stato di salute del sistema.

  Il dashboard di Digital Advisor segnala eventuali problemi relativi al funzionamento e ti aiuta a risolverli. Monitorare la capacità del sistema per assicurarsi di non esaurire mai lo spazio di storage. Visualizza i casi di supporto per il tuo sistema.

- Gestire le performance.

  Digital Advisor mostra le prestazioni del sistema per un periodo più lungo di quanto sia possibile vedere in Gestione di sistema di ONTAP. Identificare i problemi di configurazione e di sistema che influiscono sulle performance.
  Massimizza l'efficienza. Visualizza le metriche di efficienza dello storage e identifica i modi per memorizzare più dati in meno spazio.

- Visualizza l'inventario e la configurazione.

  Digital Advisor visualizza l'inventario completo e le informazioni sulla configurazione di software e hardware. Controlla quando i contratti di servizio stanno per scadere e rinnovarli per assicurarti di rimanere supportati.

Link correlati

- "Documentazione NetApp: Consulente digitale"

- "Avviare Digital Advisor"
- "Servizi SupportEdge"

Configurazioni predefinite supportate per Cloud Volumes ONTAP

La configurazione predefinita di Cloud Volumes ONTAP consente di configurare e amministrare i sistemi, in particolare se si conosce ONTAP perché la configurazione predefinita di Cloud Volumes ONTAP è diversa da ONTAP.

Impostazione predefinita

- BlueXP crea una VM di storage per il servizio dei dati quando implementa Cloud Volumes ONTAP. Alcune configurazioni supportano macchine virtuali storage aggiuntive. "Scopri di più sulla gestione delle VM di storage".

  A partire dalla versione BlueXP 3.9.5, il reporting dello spazio logico viene attivato sulla VM di storage iniziale. Quando lo spazio viene segnalato logicamente, ONTAP riporta lo spazio del volume in modo che tutto lo spazio fisico salvato dalle funzionalità di efficienza dello storage venga riportato come utilizzato. Per informazioni sulle funzionalità di efficienza dello storage inline, consultare l'articolo della Knowledge base "KB: Quali funzionalità di efficienza dello storage inline sono supportate in CVO?"

- BlueXP installa automaticamente le seguenti licenze di ONTAP Feature su Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - Gestione delle chiavi di crittografia multi-tenant (MTEKM), a partire da Cloud Volumes ONTAP 9.12.1 GA
  - Crittografia dei volumi di NetApp (solo per sistemi BYOL (Bring Your Own License) o pay-as-you-go (PAYGO) registrati)
  - NFS ifdef::aws[] endif::aws[] ifdef::aura[] endif::aura[]
  - SnapMirror
  - SnapRestore
  - SnapVault
- Per impostazione predefinita, vengono create diverse interfacce di rete:
  - Una LIF di gestione del cluster
  - Un LIF intercluster
- Una LIF di gestione SVM sui sistemi ha in Azure
- Una LIF di gestione SVM sui sistemi ha in Google Cloud
- LIF di gestione SVM su sistemi a nodo singolo in AWS
- Una LIF di gestione dei nodi

+ in Google Cloud, questa LIF è combinata con la LIF intercluster.

- Una LIF di dati iSCSI
- Una LIF di dati CIFS e NFS

> Il failover LIF è disattivato per impostazione predefinita per Cloud Volumes ONTAP a causa dei requisiti del cloud provider. La migrazione di una LIF a una porta diversa interrompe la mappatura esterna tra gli indirizzi IP e le interfacce di rete sull'istanza, rendendo la LIF inaccessibile.

  - Cloud Volumes ONTAP invia i backup della configurazione al connettore utilizzando HTTP.

    I backup sono accessibili da http://ipaddress/occm/offboxconfig/ dove *ipaddress* è l'indirizzo IP dell'host del connettore.

    È possibile utilizzare i backup per riconfigurare il sistema Cloud Volumes ONTAP. Per ulteriori informazioni sui backup della configurazione, consultare "Documentazione ONTAP" .

  - BlueXP imposta alcuni attributi di volume in modo diverso rispetto ad altri strumenti di gestione (ad esempio, ONTAP System Manager o la CLI di ONTAP).

    Nella tabella seguente sono elencati gli attributi del volume impostati da BlueXP in modo diverso dai valori predefiniti:

Attributo	Valore impostato da BlueXP
Modalità di dimensionamento automatico	crescere
Dimensionamento automatico massimo	1,000% L'organizzazione o l'amministratore dell'account BlueXP può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per CIFS Volumes UNIX per NFS Volumes
Stile garanzia di spazio	nessuno
Autorizzazioni UNIX (solo NFS)	777

+
Per informazioni su questi attributi, fare riferimento a "ONTAP *volume create* man page".

Dischi interni per i dati di sistema

Oltre allo storage per i dati degli utenti, BlueXP acquista anche lo storage cloud per i dati di sistema.

AWS

- Tre dischi per nodo per i dati di boot, root e core:

- 47 disco GiB io1 per i dati di avvio
- Disco gp3 da 140 GiB per i dati root
- Disco gp2 da 540 GiB per i dati principali

- Per coppie ha:
  - Due volumi EBS da ST1 gb per l'istanza del mediatore, uno di circa 8 GiB come disco root e uno di 4 GiB come disco dati
  - Un disco da 140 GiB GP3 in ciascun nodo per contenere una copia dei dati root dell'altro nodo

    In alcune zone, il tipo di disco EBS disponibile può essere solo GP2.

- Un'istantanea EBS per ogni disco di boot e disco root

  Le snapshot vengono create automaticamente al riavvio.

- Quando si attiva la crittografia dei dati in AWS utilizzando il servizio di gestione delle chiavi (KMS), vengono crittografati anche i dischi di avvio e i dischi root per Cloud Volumes ONTAP. Questo include il disco di boot per l'istanza del mediatore in una coppia ha. I dischi vengono crittografati utilizzando la CMK selezionata quando si crea l'ambiente di lavoro.

In AWS, la NVRAM si trova sul disco di avvio.

Azure (nodo singolo)

- Tre dischi SSD Premium:
  - Un disco da 10 GiB per i dati di avvio
  - Un disco da 140 GiB per i dati root
  - Un disco da 512 GiB per NVRAM

    Se la macchina virtuale scelta per Cloud Volumes ONTAP supporta gli SSD Ultra, il sistema utilizza un SSD Ultra da 32 GB per la NVRAM, anziché un SSD Premium.

- Un disco HDD standard da 1024 GiB per il risparmio dei core
- Uno snapshot Azure per ogni disco di boot e disco root
- Per impostazione predefinita, ogni disco in Azure viene crittografato a riposo.

  Se la macchina virtuale scelta per Cloud Volumes ONTAP supporta il disco SSD Premium v2 gestito come dischi dati, il sistema utilizza un disco gestito v2 GiB Premium SSD da 32 GB per NVRAM e un altro disco come disco principale.

Azure (coppia ha)

COPPIE HA con il blob di pagina

- Due dischi SSD Premium da 10 GiB per il volume di boot (uno per nodo)
- Due blob di pagina 140 GiB Premium Storage per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GiB per il risparmio di core (uno per nodo)
- Due dischi SSD Premium da 512 GiB per NVRAM (uno per nodo)

- Uno snapshot Azure per ogni disco di boot e disco root

  Le snapshot vengono create automaticamente al riavvio.

- Per impostazione predefinita, ogni disco in Azure viene crittografato a riposo.

Coppie HA con dischi gestiti condivisi in più zone di disponibilità

- Due dischi SSD Premium da 10 GiB per il volume di boot (uno per nodo)
- Due dischi SSD GiB Premium da 512 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GiB per il risparmio di core (uno per nodo)
- Due dischi SSD Premium da 512 GiB per NVRAM (uno per nodo)
- Uno snapshot Azure per ogni disco di boot e disco root

  Le snapshot vengono create automaticamente al riavvio.

- Per impostazione predefinita, ogni disco in Azure viene crittografato a riposo.

Coppie HA con dischi gestiti condivisi in singole zone di disponibilità

- Due dischi SSD Premium da 10 GiB per il volume di boot (uno per nodo)
- Due dischi SSD Shared Managed Premium da 512 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GiB per il risparmio di core (uno per nodo)
- Due dischi gestiti SSD Premium da 512 GiB per NVRAM (uno per nodo)

Se la macchina virtuale supporta dischi SSD Premium v2 gestiti come dischi dati, utilizza 32 dischi SSD Premium v2 GiB per NVRAM e 512 dischi gestiti condivisi SSD Premium v2 GiB per il volume root.

Puoi implementare coppie ha in una singola zona di disponibilità e utilizzare dischi gestiti SSD Premium da v2 TB quando sono soddisfatte le seguenti condizioni:

- La versione di Cloud Volumes ONTAP è la 9.15.1 o successiva.
- La regione e la zona selezionate supportano dischi gestiti SSD Premium da v2 GB. Per informazioni sulle regioni supportate, fare riferimento a "Sito Web di Microsoft Azure: Prodotti disponibili per area geografica".
- L'abbonamento è registrato per Microsoft "Funzione Microsoft.Compute/VMOrchestratorZonalMultiFD".

Google Cloud (nodo singolo)

- Un disco persistente SSD da 10 GiB per i dati di avvio
- Un disco persistente SSD da 64 GiB per i dati root
- Un disco persistente SSD da 500 GiB per NVRAM
- Un disco persistente standard da 315 GiB per il risparmio dei core
- Snapshot per i dati di boot e root

  Le snapshot vengono create automaticamente al riavvio.

- I dischi di boot e root sono crittografati per impostazione predefinita.

Google Cloud (coppia ha)

- Due dischi persistenti SSD da 10 GiB per i dati di avvio
- Quattro dischi persistenti SSD da 64 GiB per i dati root
- Due dischi persistenti SSD da 500 GiB per NVRAM
- Due dischi persistenti standard da 315 GiB per il risparmio dei core
- Un disco persistente standard da 10 GiB per i dati del mediatore
- Un disco persistente standard da 10 GiB per i dati di avvio del mediatore
- Snapshot per i dati di boot e root

  Le snapshot vengono create automaticamente al riavvio.

- I dischi di boot e root sono crittografati per impostazione predefinita.

Dove risiedono i dischi

BlueXP definisce lo storage come segue:

- I dati di avvio risiedono su un disco collegato all'istanza o alla macchina virtuale.

  Questo disco, che contiene l'immagine di avvio, non è disponibile per Cloud Volumes ONTAP.

- I dati root, che contengono la configurazione del sistema e i log, risiedono in aggr0.
- Il volume root della macchina virtuale di storage (SVM) risiede in aggr1.
- I volumi di dati risiedono anche in aggr1.

Conoscenza e supporto

Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione del numero di serie dell'account BlueXP (il numero di serie 960xxxxxxxx a 20 cifre si trova nella pagina risorse di supporto di BlueXP).

  Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

- Registrazione dei numeri di serie Cloud Volumes ONTAP associati a un abbonamento nel mercato del provider cloud (si tratta di numeri di serie 909201xxxxxxxx a 20 cifre).

  Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

Registrare BlueXP per ricevere assistenza NetApp

Per registrarsi per ricevere assistenza e attivare i diritti di supporto, un utente dell'organizzazione (o account) BlueXP deve associare un account del sito di supporto NetApp al proprio login BlueXP . La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

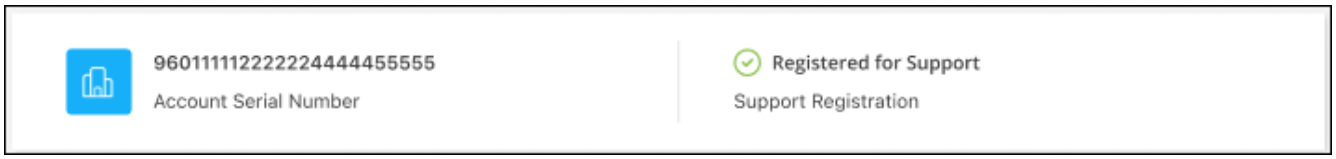
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

   La pagina **risorse** dovrebbe mostrare che l'organizzazione BlueXP è registrata per il supporto.



   Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che la tua organizzazione BlueXP non sia registrata per il supporto. Finché un utente dell'organizzazione ha seguito questi passaggi, l'organizzazione è stata registrata.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

Fasi

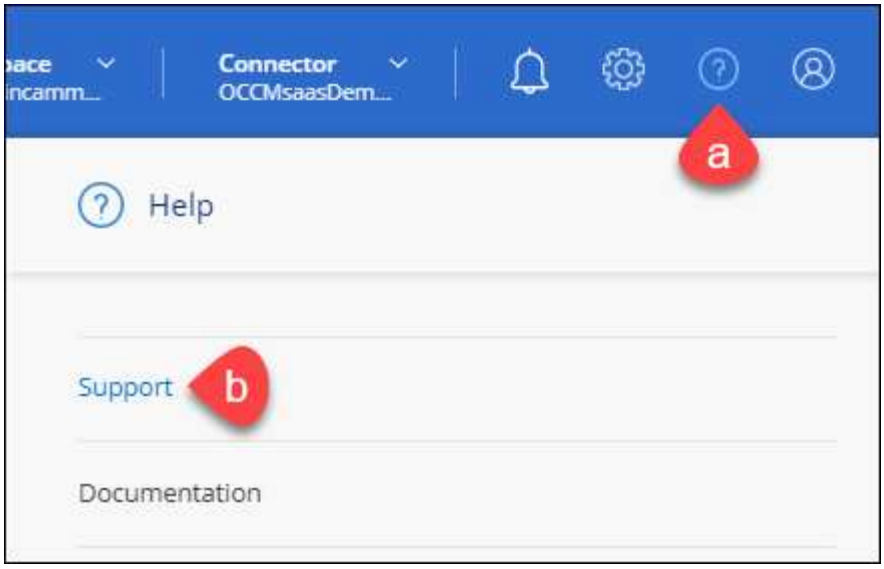
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto Cliente esistente con un account NSS.

Novità di NetApp

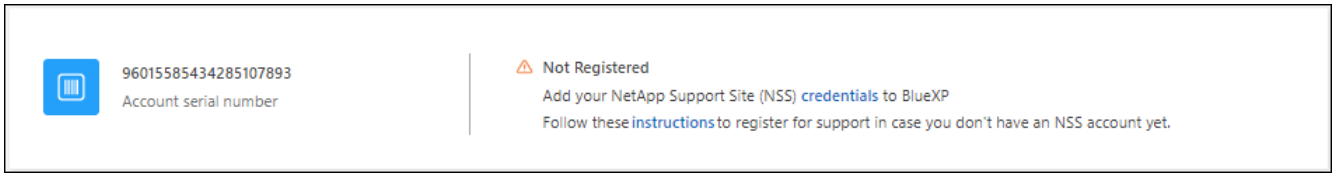
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare "Sito per la registrazione del supporto NetApp" E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

   Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

7. Confermare l'azione dall'interno dell'e-mail.

   La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

8. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account (960xxxx) utilizzato in precedenza per il campo del numero di serie. Ciò velocizzerà l'elaborazione.

Al termine

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di assunzione per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in Cliente esistente con un account NSS.

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

È necessario associare le credenziali del sito di supporto NetApp alla propria organizzazione BlueXP per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

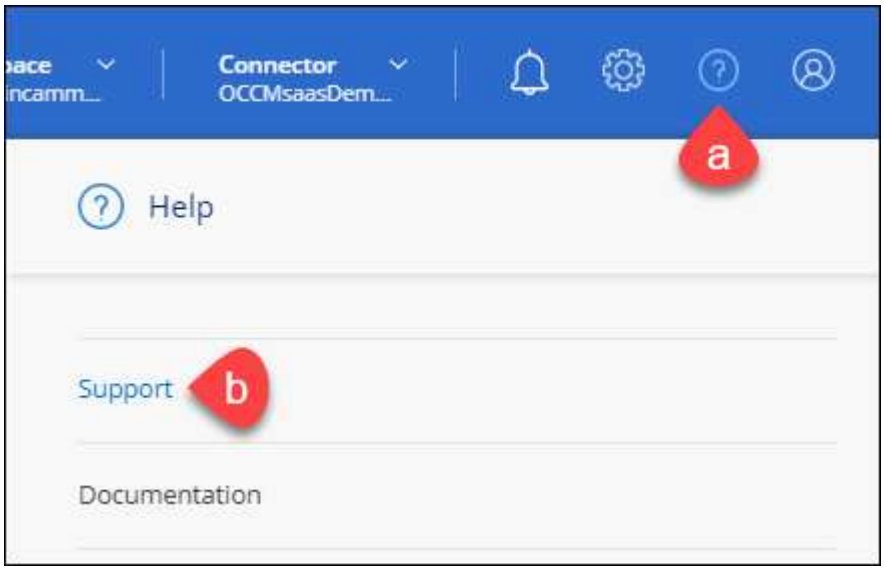
L'associazione delle credenziali NSS all'organizzazione BlueXP è diversa dall'account NSS associato a un accesso utente BlueXP .

Queste credenziali NSS sono associate all'ID organizzazione BlueXP specifico dell'utente. Gli utenti che appartengono all'organizzazione BlueXP possono accedere a queste credenziali da **supporto > Gestione NSS**.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili ampie opzioni di supporto autonomo gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include supporto tecnico remoto tramite ticket web.

Ottieni supporto per un file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

  Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- "Community"

  Unisciti alla community BlueXP per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo l'attivazione del supporto.

Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. "Scopri come gestire le credenziali associate all'accesso a BlueXP".
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:

   a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.

   b. Selezionare **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp:

      - **Servizio**: Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
      - **Ambiente di lavoro**: Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

        L'elenco degli ambienti di lavoro rientra nell'ambito dell'organizzazione (o account), del progetto (o dell'area di lavoro) BlueXP e del connettore selezionato nell'intestazione superiore del servizio.

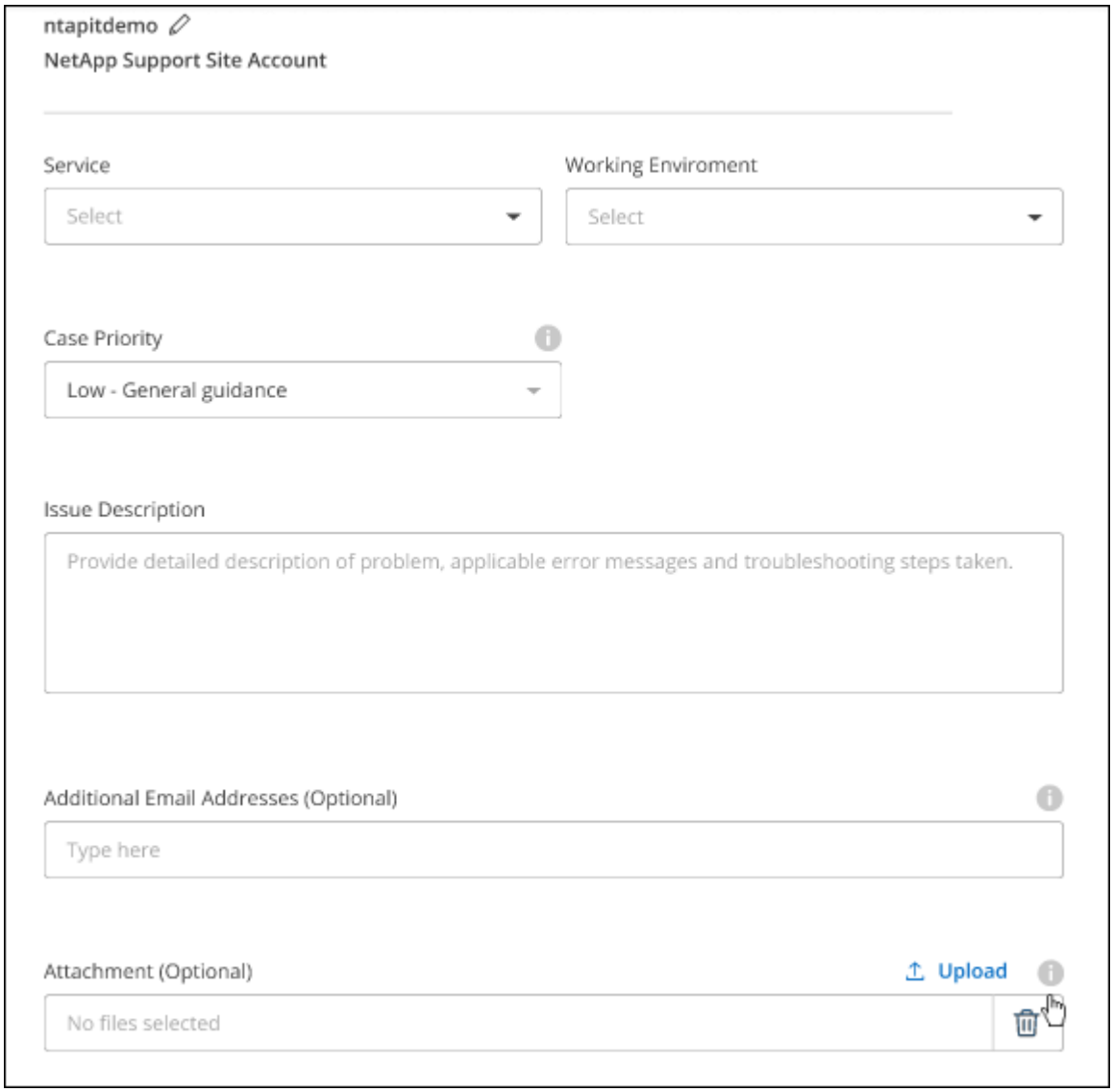
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.

      - **Descrizione del problema**: Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
      - **Indirizzi e-mail aggiuntivi**: Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale)**: Carica fino a cinque allegati, uno alla volta.

  Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo https://mysupport.netapp.com/site/help

Gestire i casi di supporto (anteprima)

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

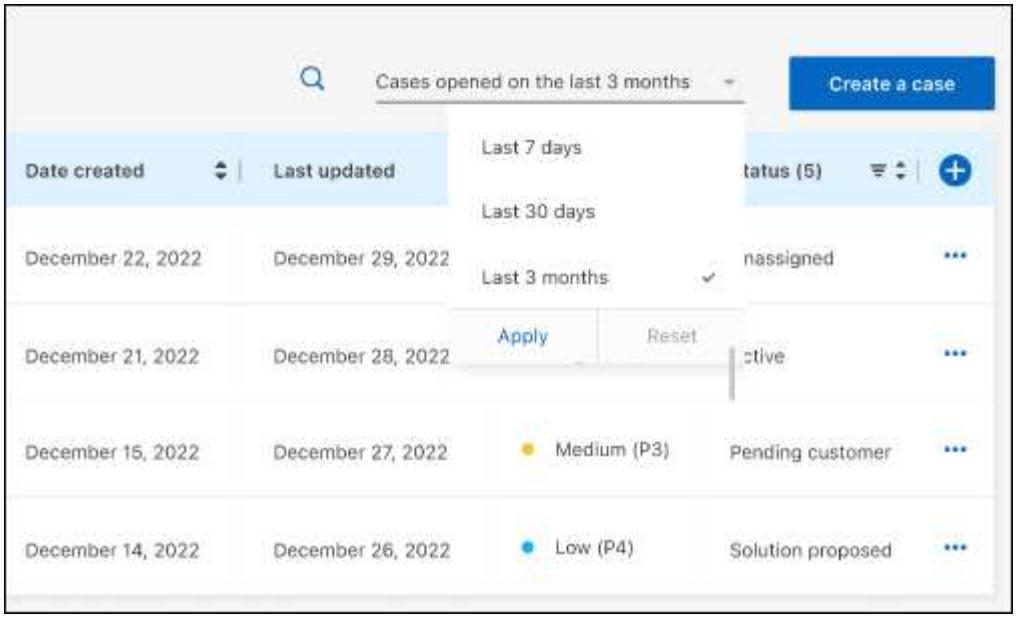
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  Per ulteriori informazioni, consulta la procedura riportata di seguito.
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

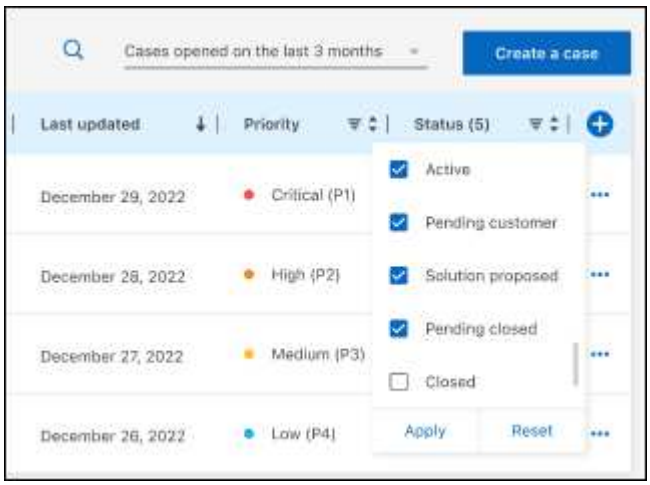
Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.

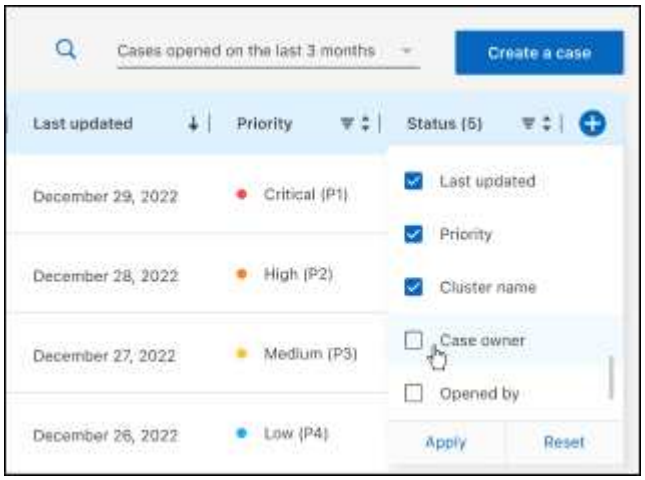
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
   - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.



- Modificare le colonne visualizzate nella tabella selezionando e quindi scegliere le colonne che si desidera visualizzare.

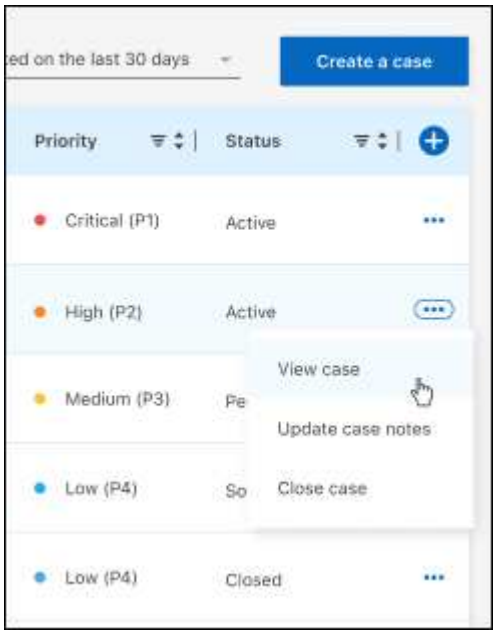


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

   - **Visualizza caso**: Visualizza tutti i dettagli relativi a un caso specifico.
   - **Aggiorna note sul caso**: Fornisci ulteriori dettagli sul problema oppure seleziona **carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - **Chiudi caso**: Fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.



Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per BlueXP"
- "Avviso per Cloud Volumes ONTAP"
- "Avviso per ONTAP"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.