Documentazione di backup e ripristino BlueXP

BlueXP backup and recovery

NetApp
August 28, 2025

Sommario

Documentazione di backup e ripristino BlueXP

Note di rilascio

Novità nel backup e ripristino di BlueXP

Scopri le novità di BlueXP backup e recovery.

25 agosto 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Supporto per la protezione dei carichi di lavoro VMware in anteprima

Questa versione aggiunge il supporto in anteprima per la protezione dei carichi di lavoro VMware. Esegui il backup di VM VMware e datastore dai sistemi ONTAP locali ad Amazon Web Services e StorageGRID.

> La documentazione sulla protezione dei carichi di lavoro VMware viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

"Scopri di più sulla protezione dei carichi di lavoro VMware con il BlueXP backup and recovery" .

L'indicizzazione ad alte prestazioni per AWS, Azure e GCP è generalmente disponibile

A febbraio 2025 abbiamo annunciato l'anteprima dell'indicizzazione ad alte prestazioni (Indexed Catalog v2) per AWS, Azure e GCP. Questa funzionalità è ora generalmente disponibile (GA). Nel giugno 2025 lo abbiamo fornito di default a tutti i *nuovi* clienti. Con questa versione, il supporto è disponibile per *tutti* i clienti. L'indicizzazione ad alte prestazioni migliora le prestazioni delle operazioni di backup e ripristino per i carichi di lavoro protetti nell'archiviazione di oggetti.

Abilitato per impostazione predefinita:

- Se sei un nuovo cliente, l'indicizzazione ad alte prestazioni è abilitata per impostazione predefinita.
- Se sei un cliente esistente, puoi abilitare la reindicizzazione andando alla sezione Ripristina dell'interfaccia utente.

12 agosto 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Carico di lavoro di Microsoft SQL Server supportato in disponibilità generale (GA)

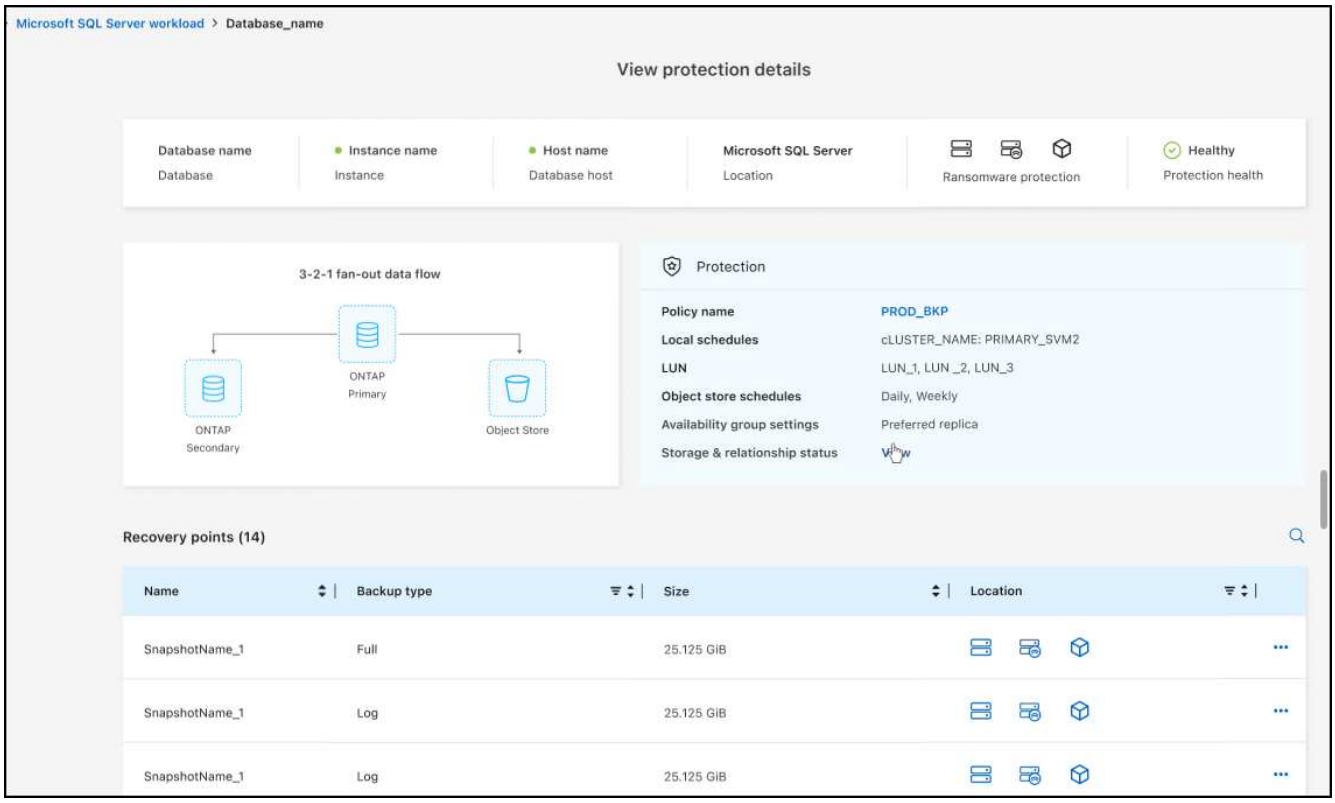
Il supporto del carico di lavoro di Microsoft SQL Server è ora generalmente disponibile (GA) nel BlueXP backup and recovery. Le organizzazioni che utilizzano un ambiente MSSQL su ONTAP, Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP possono ora sfruttare questo nuovo servizio di backup e ripristino per proteggere i propri dati.

Questa versione include i seguenti miglioramenti al supporto del carico di lavoro di Microsoft SQL Server rispetto alla versione di anteprima precedente:

- * Sincronizzazione attiva SnapMirror **: questa versione supporta ora la sincronizzazione attiva SnapMirror (nota anche come SnapMirror Business Continuity [SM-BC]), che consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il**

failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Il BlueXP backup and recovery ora supportano la protezione dei database Microsoft SQL Server in una configurazione SnapMirror ActiveSync e Metrocluster. Le informazioni vengono visualizzate nella sezione *Stato di archiviazione e relazione della pagina Dettagli protezione. Le informazioni sulla relazione vengono visualizzate nella sezione aggiornata **Impostazioni secondarie** della pagina Policy.

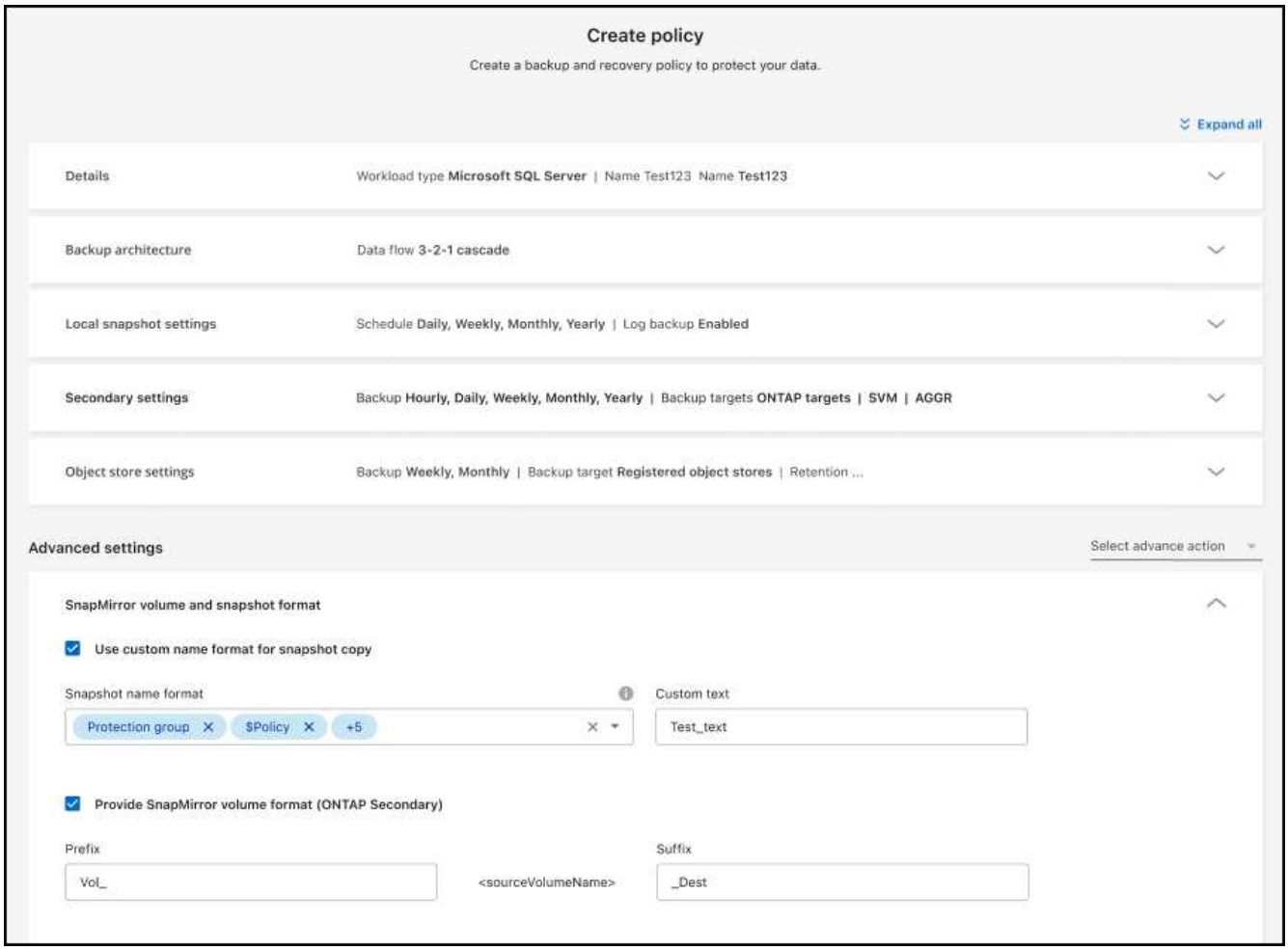
Fare riferimento a "Utilizza policy per proteggere i tuoi carichi di lavoro" .



- **Supporto multi-bucket**: ora puoi proteggere i volumi all'interno di un ambiente di lavoro con un massimo di 6 bucket per ambiente di lavoro su diversi provider cloud.
- **Aggiornamenti di licenze e versioni di prova gratuite** per carichi di lavoro di SQL Server: ora è possibile utilizzare il modello di licenza di backup e ripristino BlueXP esistente per proteggere i carichi di lavoro di SQL Server. Non esiste alcun requisito di licenza separato per i carichi di lavoro di SQL Server.

  Per i dettagli, fare riferimento a "Impostare le licenze per il backup e ripristino BlueXP" .

- **Nome snapshot personalizzato**: ora puoi utilizzare il nome del tuo snapshot in un criterio che regola i backup per i carichi di lavoro di Microsoft SQL Server. Inserisci queste informazioni nella sezione **Impostazioni avanzate** della pagina Policy.

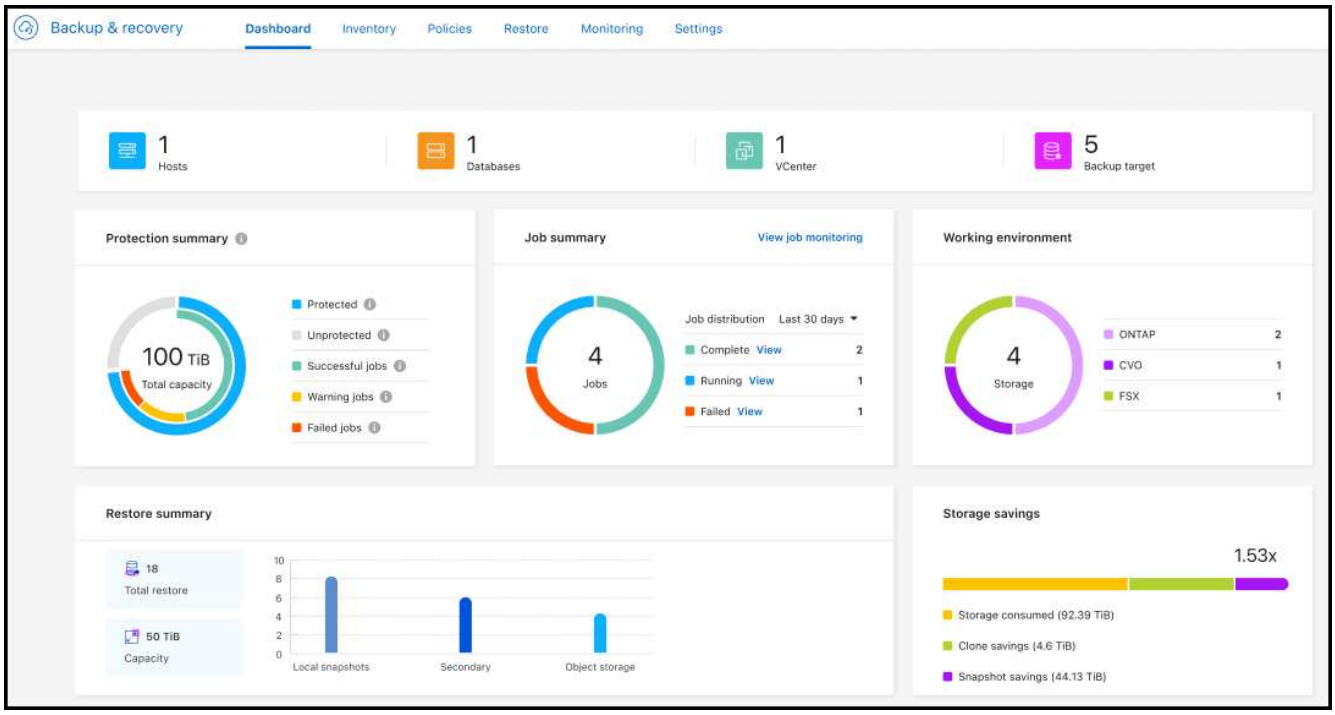


Fare riferimento a "Utilizza policy per proteggere i tuoi carichi di lavoro" .

- **Prefisso e suffisso del volume secondario**: è possibile immettere un prefisso e un suffisso personalizzati nella sezione **Impostazioni avanzate** della pagina Criteri.
- **Gestione delle identità e degli accessi (IAM)**: ora puoi controllare l'accesso degli utenti alle funzionalità.

  Fare riferimento a "Accedi al BlueXP backup and recovery" E "Accesso alle funzionalità BlueXP backup and recovery" .

- **Ripristino da un archivio oggetti a un host alternativo**: ora puoi eseguire il ripristino da un archivio oggetti a un host alternativo anche se l'archivio primario è inattivo.
- **Dati di backup del registro**: la pagina dei dettagli sulla protezione del database ora mostra i backup del registro. È possibile visualizzare la colonna Tipo di backup che indica se il backup è un backup completo o un backup del registro.
- **Dashboard migliorata**: la dashboard ora mostra i risparmi di archiviazione e clonazione.



Miglioramenti del carico di lavoro del volume ONTAP

- *Ripristino multi-cartella per volumi ONTAP *: fino ad ora, era possibile ripristinare una cartella o più file alla volta tramite la funzionalità Sfoglia e ripristina. Il BlueXP backup and recovery ora offrono la possibilità di selezionare più cartelle contemporaneamente utilizzando la funzionalità Sfoglia e ripristina.
- **Visualizzazione e gestione dei backup dei volumi eliminati**: la dashboard BlueXP backup and recovery ora offre un'opzione per visualizzare e gestire i volumi eliminati da ONTAP. Con questo, è possibile visualizzare ed eliminare i backup dai volumi che non esistono più in ONTAP.
- **Eliminazione forzata dei backup**: in alcuni casi estremi, potresti voler impedire BlueXP backup and recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione, è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di ambiente di lavoro).

> Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. Il BlueXP backup and recovery non avranno più accesso a questi backup, anche se non vengono eliminati dall'archivio oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

Fare riferimento a "Proteggere i carichi di lavoro ONTAP" .

28 luglio 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Supporto del carico di lavoro Kubernetes in anteprima

Questa versione di BlueXP backup and recovery introduce il supporto per l'individuazione e la gestione dei carichi di lavoro Kubernetes:

- Scopri i cluster Red Hat OpenShift e Kubernetes open source, supportati da NetApp ONTAP, senza condividere i file kubeconfig.
- Scopri, gestisci e proteggi le applicazioni su più cluster Kubernetes utilizzando un piano di controllo unificato.
- Trasferisci le operazioni di spostamento dei dati per il backup e il ripristino delle applicazioni Kubernetes a NetApp ONTAP.
- Orchestrare i backup delle applicazioni locali e basati su storage di oggetti.
- Esegui il backup e il ripristino di intere applicazioni e singole risorse su qualsiasi cluster Kubernetes.
- Lavora con container e macchine virtuali in esecuzione su Kubernetes.
- Crea backup coerenti con l'applicazione utilizzando modelli e hook di esecuzione.

Per i dettagli sulla protezione dei carichi di lavoro di Kubernetes, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro di Kubernetes" .

14 luglio 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Dashboard del volume ONTAP migliorato

Ad aprile 2025 abbiamo lanciato un'anteprima di una Dashboard del volume ONTAP migliorata, molto più veloce ed efficiente.

Questa dashboard è stata progettata per supportare i clienti aziendali con un elevato numero di carichi di lavoro. Anche per i clienti con 20.000 volumi, la nuova dashboard si carica in meno di 10 secondi.

Dopo un'anteprima di successo e un feedback positivo da parte dei clienti, ora la stiamo rendendo l'esperienza predefinita per tutti i nostri clienti. Preparatevi per una dashboard incredibilmente veloce.

Per ulteriori informazioni, vedere "Visualizza lo stato di protezione nella Dashboard".

Supporto del carico di lavoro di Microsoft SQL Server come anteprima tecnologica pubblica

Questa versione di BlueXP backup and recovery offre un'interfaccia utente aggiornata che consente di gestire i carichi di lavoro di Microsoft SQL Server utilizzando una strategia di protezione 3-2-1, già nota nel servizio di BlueXP backup and recovery . Con questa nuova versione, è possibile eseguire il backup di questi carichi di lavoro sullo storage primario, replicarli sullo storage secondario ed eseguirne il backup sullo storage di oggetti cloud.

Puoi iscriverti all'anteprima completando questo "Anteprima del modulo di registrazione" .

> Questa documentazione sulla protezione dei carichi di lavoro di Microsoft SQL Server viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare dettagli, contenuti e tempistiche prima della disponibilità generale.

Questa versione di BlueXP backup and recovery include i seguenti aggiornamenti:

- **Funzionalità di backup 3-2-1**: questa versione integra le funzionalità SnapCenter , consentendo di gestire e proteggere le risorse SnapCenter con una strategia di protezione dei dati 3-2-1 dall'interfaccia utente BlueXP backup and recovery .
- **Importa da SnapCenter**: puoi importare i dati di backup e i criteri SnapCenter nel BlueXP backup and

recovery.

- **Un'interfaccia utente riprogettata** offre un'esperienza più intuitiva per la gestione delle attività di backup e ripristino.
- **Destinazioni di backup**: puoi aggiungere bucket negli ambienti Amazon Web Services (AWS), Microsoft Azure Blob Storage, StorageGRID e ONTAP S3 da utilizzare come destinazioni di backup per i carichi di lavoro di Microsoft SQL Server.
- **Supporto per i carichi di lavoro**: questa versione consente di eseguire il backup, il ripristino, la verifica e la clonazione di database e gruppi di disponibilità di Microsoft SQL Server. (Il supporto per altri carichi di lavoro verrà aggiunto nelle versioni future.)
- **Opzioni di ripristino flessibili**: questa versione consente di ripristinare i database sia nelle posizioni originali che in quelle alternative in caso di danneggiamento o perdita accidentale dei dati.
- **Copie di produzione istantanee**: genera copie di produzione salvaspazio per sviluppo, test o analisi in pochi minuti anziché in ore o giorni.
- Questa versione include la possibilità di creare report dettagliati.

Per informazioni dettagliate sulla protezione dei carichi di lavoro di Microsoft SQL Server, vedere "Panoramica sulla protezione dei carichi di lavoro di Microsoft SQL Server" .

09 giugno 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Aggiornamenti del supporto del catalogo indicizzato

A febbraio 2025, abbiamo introdotto la funzionalità di indicizzazione aggiornata (Catalogo indicizzato v2) da utilizzare durante il metodo di ripristino dei dati "Cerca e ripristina". La versione precedente ha migliorato significativamente le prestazioni di indicizzazione dei dati negli ambienti on-premise. Con questa versione, il catalogo di indicizzazione è ora disponibile negli ambienti Amazon Web Services, Microsoft Azure e Google Cloud Platform (GCP).

Se sei un nuovo cliente, il Catalogo Indicizzato v2 è abilitato per impostazione predefinita per tutti i nuovi ambienti. Se sei un cliente esistente, puoi reindicizzare il tuo ambiente per sfruttare il Catalogo Indicizzato v2.

Come si attiva l'indicizzazione?

Prima di poter utilizzare il metodo Search & Restore per il ripristino dei dati, è necessario attivare l'indicizzazione in ogni ambiente di lavoro di origine da cui si prevede di ripristinare volumi o file. Selezionare l'opzione **Abilita indicizzazione** quando si esegue una ricerca e un ripristino.

Il catalogo indicizzato può quindi tenere traccia di ogni volume e file di backup, rendendo le ricerche rapide ed efficienti.

Per ulteriori informazioni, fare riferimento a "Abilita l'indicizzazione per Cerca e Ripristina".

Endpoint di collegamento privato di Azure ed endpoint di servizio

In genere, il BlueXP backup and recovery stabiliscono un endpoint privato con il provider cloud per gestire le attività di protezione. Questa versione introduce un'impostazione opzionale che consente di abilitare o disabilitare la creazione automatica di un endpoint privato da parte di BlueXP Backup and Recovery. Questa opzione potrebbe essere utile se si desidera un maggiore controllo sul processo di creazione di endpoint privati.

È possibile abilitare o disabilitare questa opzione quando si abilita la protezione o si avvia il processo di

ripristino.

Se si disabilita questa impostazione, è necessario creare manualmente l'endpoint privato affinché il backup e il ripristino di BlueXP funzionino correttamente. Senza una connettività adeguata, potrebbe non essere possibile eseguire correttamente le attività di backup e ripristino.

Supporto per SnapMirror su Cloud Resync su ONTAP S3

La versione precedente ha introdotto il supporto per SnapMirror to Cloud Resync (SM-C Resync). La funzionalità semplifica la protezione dei dati durante la migrazione dei volumi negli ambienti NetApp. Questa versione aggiunge il supporto per SM-C Resync su ONTAP S3 e su altri provider compatibili con S3, come Wasabi e MinIO.

Porta il tuo bucket per StorageGRID

Quando si creano file di backup nell'archiviazione oggetti per un ambiente di lavoro, per impostazione predefinita, BlueXP Backup and Recovery crea il contenitore (bucket o account di archiviazione) per i file di backup nell'account di archiviazione oggetti configurato. In precedenza, era possibile ignorare questa impostazione e specificare un contenitore personalizzato per Amazon S3, Azure Blob Storage e Google Cloud Storage. Con questa versione, è ora possibile utilizzare il proprio contenitore di archiviazione oggetti StorageGRID.

Vedere "Crea il tuo contenitore di archiviazione di oggetti".

13 maggio 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Risincronizzazione da SnapMirror al cloud per le migrazioni dei volumi

La funzionalità risincronizzazione da SnapMirror al cloud ottimizza la data Protection e la continuità durante le migrazioni dei volumi negli ambienti NetApp. Quando un volume viene migrato usando la replica logica SnapMirror (LRSE), da un'implementazione NetApp on-premise a un'altra o a una soluzione basata sul cloud come Cloud Volumes ONTAP o Cloud Volumes Service, SnapMirror to Cloud Resync garantisce che i backup cloud esistenti rimangano intatti e operativi.

Questa funzionalità elimina la necessità di un'operazione di re-baseline, che richiede molto tempo e risorse, consentendo alle operazioni di backup di continuare anche dopo la migrazione. Questa funzionalità è molto utile negli scenari di migrazione dei carichi di lavoro, a supporto di FlexVol e gruppi di lavoro, ed è disponibile a partire dalla versione 9.16.1 di ONTAP.

Mantenendo la continuità del backup in tutti gli ambienti, SnapMirror to Cloud Resync migliora l'efficienza delle operazioni e riduce la complessità della gestione dei dati nel cloud ibrido e multicloud.

Per informazioni dettagliate su come eseguire l'operazione di risincronizzazione, vedere "Migra i volumi usando SnapMirror per la risincronizzazione del cloud".

Supporto per archivio oggetti MinIO di terze parti (anteprima)

Il backup e ripristino di BlueXP ora estende il suo supporto ad archivi di oggetti di terze parti, con una particolare attenzione al MinIO. Questa nuova funzione di anteprima consente di sfruttare qualsiasi archivio di oggetti compatibile con S3 per le proprie esigenze di backup e recovery.

Con questa versione di anteprima, speriamo di garantire una solida integrazione con gli archivi di oggetti di terze parti prima che venga implementata la funzionalità completa. Siete incoraggiati ad esplorare questa

nuova funzionalità e a fornire feedback per contribuire a migliorare il servizio.

Questa funzione non deve essere utilizzata in produzione.

Limiti del modo Anteprima

Mentre questa funzione è in anteprima, esistono alcune limitazioni:

- Il servizio Bring Your Own Bucket (BYOB) non è supportato.
- L'attivazione di DataLock nel criterio non è supportata.
- L'attivazione della modalità archiviazione nel criterio non è supportata.
- Sono supportati solo gli ambienti ONTAP on-premise.
- MetroCluster non è supportato.
- Le opzioni per abilitare la crittografia a livello di bucket non sono supportate.

Guida introduttiva

Per iniziare a utilizzare questa funzione di anteprima, è necessario attivare un contrassegno sul connettore BlueXP . È quindi possibile immettere i dettagli di connessione dell'archivio oggetti di terze parti MinIO nel flusso di lavoro di protezione scegliendo l'archivio oggetti compatibile con terze parti nella sezione di backup.

16 aprile 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Miglioramenti dell'interfaccia utente

Questa versione migliora l'esperienza dell'utente semplificando l'interfaccia:

- La rimozione della colonna aggregate dalle tabelle Volumes, insieme alle colonne Snapshot Policy, Backup Policy e Replication Policy dalla tabella Volume nella dashboard V2, consente di ottimizzare il layout.
- L'esclusione degli ambienti di lavoro non attivati dall'elenco a discesa rende l'interfaccia meno ingombrante, la navigazione più efficiente e il caricamento più rapido.
- Mentre l'ordinamento nella colonna Tag è disattivato, è comunque possibile visualizzare i tag, garantendo che le informazioni importanti rimangano facilmente accessibili.
- La rimozione delle etichette sulle icone di protezione contribuisce a un aspetto più pulito e riduce i tempi di caricamento.
- Durante il processo di attivazione dell'ambiente di lavoro, una finestra di dialogo visualizza un'icona di caricamento per fornire un feedback fino al completamento del processo di rilevamento, migliorando la trasparenza e la sicurezza nelle operazioni del sistema.

Dashboard volume avanzato (anteprima)

La Volume Dashboard viene ora caricata in meno di 10 secondi, fornendo un'interfaccia molto più veloce ed efficiente. Questa versione in anteprima è disponibile per alcuni clienti, offrendo loro un'anteprima di questi miglioramenti.

Supporto per archivio oggetti Wasabi di terze parti (anteprima)

Il backup e recovery di BlueXP ora estende il suo supporto ad archivi di oggetti di terze parti, con una particolare attenzione al tema di Wasabi. Questa nuova funzione di anteprima consente di sfruttare qualsiasi archivio di oggetti compatibile con S3 per le proprie esigenze di backup e recovery.

Per iniziare con Wasabi

Per iniziare a utilizzare lo storage di terze parti come archivio di oggetti, è necessario abilitare un flag all'interno di BlueXP Connector. Quindi, puoi immettere i dettagli di connessione per l'archivio di oggetti di terze parti e integrarlo nei tuoi flussi di lavoro di backup e recovery.

Fasi

1. SSH nel connettore.
2. Andare nel contenitore di server cbs di backup e ripristino BlueXP :

```
docker exec -it cloudmanager_cbs sh
```

3. Aprire il `default.json` file all'interno della `config` cartella tramite VIM o qualsiasi altro editor:

```
vi default.json
```

4. Modify `allow-s3-compatible`: false to : `allow-s3-compatible` true.
5. Salvare le modifiche.
6. Uscire dal contenitore.
7. Riavviare il contenitore del server cbs di backup e ripristino BlueXP .

Risultato

Una volta RIACCESO IL contenitore, aprire l'interfaccia utente di backup e ripristino di BlueXP . Quando avvii un backup o modifichi una strategia di backup, vengono visualizzati il nuovo provider "S3 compatibile" e gli altri provider di backup di AWS, Microsoft Azure, Google Cloud, StorageGRID e ONTAP S3.

Limitazioni della modalità di anteprima

Mentre questa funzione è in anteprima, considerare le seguenti limitazioni:

- Il servizio Bring Your Own Bucket (BYOB) non è supportato.
- L'attivazione di DataLock in un criterio non è supportata.
- L'attivazione della modalità archiviazione in un criterio non è supportata.
- Sono supportati solo gli ambienti ONTAP on-premise.
- MetroCluster non è supportato.
- Le opzioni per abilitare la crittografia a livello di bucket non sono supportate.

Durante questa anteprima, ti consigliamo di esplorare questa nuova funzionalità e di fornire un feedback sull'integrazione con gli archivi di oggetti di terze parti prima dell'implementazione della funzionalità completa.

17 marzo 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Esplorazione delle istantanee SMB

Questo aggiornamento di backup e ripristino di BlueXP ha risolto un problema che ha impedito ai clienti di sfogliare gli snapshot locali in un ambiente SMB.

Update dell'ambiente AWS GovCloud

Questo aggiornamento di backup e ripristino di BlueXP ha risolto un problema che impediva la connessione dell'interfaccia utente a un ambiente AWS GovCloud a causa di errori di certificato TLS. Il problema è stato risolto utilizzando il nome host del connettore BlueXP anziché l'indirizzo IP.

Limiti di conservazione della politica di backup

In precedenza, l'interfaccia utente di backup e recovery di BlueXP limitava i backup a 999 copie, mentre l'interfaccia a riga di comando consentiva di eseguire ulteriori operazioni. Ora, è possibile collegare fino a 4.000 volumi a una policy di backup e includere 1.018 volumi non collegati a una policy di backup. Questo aggiornamento include convalide aggiuntive che impediscono di superare questi limiti.

Risincronizzazione del cloud SnapMirror

Questo aggiornamento garantisce che la risincronizzazione del cloud SnapMirror non possa essere avviata dal backup e ripristino di BlueXP per le versioni ONTAP non supportate dopo l'eliminazione di una relazione SnapMirror.

21 febbraio 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Indicizzazione ad alte prestazioni

Il backup e ripristino di BlueXP introduce una funzionalità di indicizzazione aggiornata che rende più efficiente l'indicizzazione dei dati nell'ambiente di lavoro di origine. La nuova funzione di indicizzazione include aggiornamenti all'interfaccia utente, prestazioni migliorate del metodo di ricerca e ripristino per il ripristino dei dati, aggiornamenti alle funzionalità di ricerca globale e una migliore scalabilità.

Ecco una descrizione dei miglioramenti:

- **Consolidamento cartelle**: La versione aggiornata raggruppa le cartelle utilizzando nomi che includono identificatori specifici, rendendo più agevole il processo di indicizzazione.
- **Compattazione dei file in parquet**: La versione aggiornata riduce il numero di file utilizzati per l'indicizzazione di ciascun volume, semplificando il processo e eliminando la necessità di un database aggiuntivo.
- **Scale-out con più sessioni**: La nuova versione aggiunge più sessioni per gestire le attività di indicizzazione, velocizzando il processo.
- **Supporto per più contenitori indice**: La nuova versione utilizza più contenitori per gestire e distribuire meglio le attività di indicizzazione.
- **Split index workflow**: La nuova versione divide il processo di indicizzazione in due parti, migliorando l'efficienza.

- **Concorrenza migliorata**: La nuova versione consente di eliminare o spostare le directory contemporaneamente, velocizzando il processo di indicizzazione.

Chi trae vantaggio da questa funzione?

La nuova funzione di indicizzazione è disponibile per tutti i nuovi clienti.

Come si attiva l'indicizzazione?

Prima di poter utilizzare il metodo Search & Restore per il ripristino dei dati, è necessario attivare l'indicizzazione in ogni ambiente di lavoro di origine da cui si prevede di ripristinare volumi o file. Ciò consente al Catalogo indicizzato di tenere traccia di ogni volume e di ogni file di backup, rendendo le ricerche veloci ed efficienti.

Attivare l'indicizzazione nell'ambiente di lavoro di origine selezionando l'opzione "Abilita indicizzazione" quando si esegue una ricerca e ripristino.

Per ulteriori informazioni, consultare la documentazione "Come ripristinare i dati ONTAP utilizzando Cerca Ripristina".

Scala supportata

La nuova funzione di indicizzazione supporta quanto segue:

- Efficienza della ricerca globale in meno di 3 minuti
- Fino a 5 miliardi di file
- Fino a 5000 volumi per cluster
- Fino a 100K snapshot per volume
- Il tempo massimo per l'indicizzazione della linea di base è inferiore a 7 giorni. Il tempo effettivo varia a seconda dell'ambiente.

Miglioramenti alle performance della ricerca globale

Questa versione include anche miglioramenti alle prestazioni della ricerca globale. Verranno ora visualizzati indicatori di avanzamento e risultati di ricerca più dettagliati, inclusi il conteggio dei file e il tempo richiesto per la ricerca. I contenitori dedicati per la ricerca e l'indicizzazione garantiscono che le ricerche globali vengano completate in meno di cinque minuti.

Tenere presente queste considerazioni relative alla ricerca globale:

- Il nuovo indice non viene eseguito sulle istantanee etichettate come ogni ora.
- La nuova funzione di indicizzazione funziona solo sugli snapshot su FlexVol e non sugli snapshot su FlexGroup.

13 febbraio 2025

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Versione di anteprima BlueXP backup and recovery

Questa versione di anteprima del BlueXP backup and recovery fornisce un'interfaccia utente aggiornata che consente di gestire i carichi di lavoro di Microsoft SQL Server utilizzando una strategia di protezione 3-2-1, nota nel servizio BlueXP backup and recovery . Con questa nuova versione, è possibile eseguire il backup di questi carichi di lavoro sullo storage primario, replicarli sullo storage secondario ed eseguirne il backup sullo storage di oggetti cloud.

La presente documentazione viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale.

Questa versione di BlueXP backup and recovery Preview 2025 include i seguenti aggiornamenti.

- Un'interfaccia utente riprogettata che offre un'esperienza più intuitiva per la gestione delle attività di backup e ripristino.
- La versione di anteprima consente di eseguire il backup e il ripristino dei database Microsoft SQL Server. (Il supporto per altri carichi di lavoro verrà aggiunto nelle versioni future.)
- Questa versione integra le funzionalità SnapCenter , consentendo di gestire e proteggere le risorse SnapCenter con una strategia di protezione dei dati 3-2-1 dall'interfaccia utente BlueXP backup and recovery .
- Questa versione consente di importare carichi di lavoro SnapCenter nel BlueXP backup and recovery.

22 novembre 2024

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Modalità di protezione SnapLock Compliance e SnapLock Enterprise

Il backup e recovery di BlueXP ora può eseguire il backup dei volumi on-premise FlexVol e FlexGroup configurati con le modalità di protezione SnapLock Compliance o SnapLock Enterprise. Per supportare questo tipo di supporto, i cluster devono eseguire ONTAP 9,14 o versione successiva. Il backup dei volumi FlexVol utilizzando la modalità SnapLock Enterprise è supportato a partire dalla versione ONTAP 9.11.1. Le release precedenti di ONTAP non supportano il backup di volumi di protezione SnapLock.

Consultare l'elenco completo dei volumi supportati nella "Informazioni su backup e ripristino BlueXP" .

Indicizzazione per il processo di ricerca e ripristino nella pagina dei volumi

Prima di utilizzare Search & Restore, è necessario attivare l'indicizzazione su ogni ambiente di lavoro di origine da cui si desidera ripristinare i dati dei volumi. In questo modo, il catalogo indicizzato può tenere traccia dei file di backup per ogni volume. La pagina volumi ora mostra lo stato di indicizzazione:

- Indicizzato: I volumi sono stati indicizzati.
- In corso
- Non indicizzato
- Indicizzazione in pausa
- Errore
- Non attivato

27 settembre 2024

Questa versione di backup e ripristino di BlueXP include i seguenti aggiornamenti.

Supporto Podman su RHEL 8 o 9 con Browse and Restore

Il backup e il ripristino di BlueXP ora supporta il ripristino di file e cartelle su Red Hat Enterprise Linux (RHEL) versioni 8 e 9 utilizzando il motore Podman. Ciò si applica al metodo di ricerca e ripristino del backup e

ripristino di BlueXP .

BlueXP Connector versione 3.9.40 supporta alcune versioni di Red Hat Enterprise Linux versione 8 e 9 per qualsiasi installazione manuale del software del connettore su un host RHEL 8 o 9, indipendentemente dalla posizione in cui si trovano oltre ai sistemi operativi menzionati nella "requisiti dell'host" . Queste nuove versioni RHEL richiedono il motore Podman anziché Docker. In precedenza, il backup e il ripristino di BlueXP avevano due limitazioni quando si utilizzava il motore Podman. Queste limitazioni sono state rimosse.

"Ulteriori informazioni sul ripristino dei dati ONTAP dai file di backup".

L'indicizzazione più rapida dei cataloghi migliora la ricerca e il ripristino

Questa versione include un indice di catalogo migliorato che completa l'indicizzazione della linea di base molto più velocemente. L'indicizzazione più rapida consente di utilizzare più rapidamente la funzione Cerca e ripristina.

"Ulteriori informazioni sul ripristino dei dati ONTAP dai file di backup".

Limitazioni note con il BlueXP backup and recovery per i volumi ONTAP

Le limitazioni note identificano funzioni non supportate da questa versione di BlueXP backup and recovery o che non interagiscono correttamente con essa. Esaminare attentamente queste limitazioni.

- Backup e recovery di BlueXP che eseguono il backup di Cloud Volume ONTAP in un archivio di oggetti nelle aree Cina di AWS (tra cui Pechino e Ningxia); tuttavia, potrebbe essere necessario modificare manualmente le policy IAM (Identity and Access Management) prima di tutto.

  Per informazioni dettagliate sulla creazione di un connettore in AWS, fare riferimento alla "Installazione di un connettore in AWS".

  Per ulteriori dettagli in un post su un blog, fare riferimento a "Blog della funzione di backup e ripristino BlueXP - maggio 2023".

- Il backup e recovery di BlueXP non supporta le aree geografiche di Microsoft Azure Cina.

  Per informazioni dettagliate sulla creazione di un connettore in Azure, fare riferimento alla sezione "Installazione di un connettore in Azure".

- Il backup e recovery di BlueXP non supporta i backup di FlexCache Volumes.

Limitazioni di replicazione per volumi ONTAP

- È possibile selezionare un solo volume FlexGroup alla volta per la replica. Sarà necessario attivare i backup separatamente per ogni volume FlexGroup.

  Non esistono limiti per i volumi FlexVol: È possibile selezionare tutti i volumi FlexVol nel proprio ambiente di lavoro e assegnare le stesse policy di backup.

- Le seguenti funzionalità sono supportate in "Servizio di replica BlueXP", Ma non quando si utilizza la funzionalità di replica di BlueXP backup e recovery:

- Non è disponibile alcun supporto per una configurazione a cascata in cui la replica avviene dal volume A al volume B e dal volume B al volume C. Il supporto include la replica dal volume A al volume B.
- Non è disponibile alcun supporto per la replica dei dati da e verso FSX per sistemi ONTAP.
- Non è disponibile alcun supporto per la creazione di una replica singola di un volume.

- Quando si creano repliche da sistemi ONTAP on-premise, se la versione di ONTAP sul sistema Cloud Volumes ONTAP di destinazione è 9.8, 9.9 o 9.11, sono consentiti solo i criteri del vault mirror.

Limitazioni del backup su oggetto per i volumi ONTAP

- Durante il backup dei dati, il backup e il ripristino di BlueXP non manterrà la crittografia del volume NetApp (NVE). Ciò significa che i dati crittografati sul volume NVE verranno decrittografati mentre i dati vengono trasferiti alla destinazione e la crittografia non verrà mantenuta.

  Per una spiegazione su questi tipi di crittografia, fare riferimento a "Panoramica sulla configurazione di NetApp Volume Encryption".

- Se gli snapshot di conservazione a lungo termine sono abilitati su un volume di destinazione SnapMirror utilizzando la pianificazione nel criterio SnapMirror, gli snapshot vengono creati direttamente sul volume di destinazione. In questo caso, non è consigliabile eseguire il backup di tali volumi utilizzando il backup e recovery di BlueXP , poiché tali snapshot non verranno spostate nello storage a oggetti.
- Durante il backup dei dati, il backup e il ripristino di BlueXP non manterrà la crittografia del volume NetApp (NVE). Ciò significa che i dati crittografati sul volume NVE verranno decrittografati mentre i dati vengono trasferiti alla destinazione e la crittografia non verrà mantenuta.

  Per una spiegazione su questi tipi di crittografia, fare riferimento a "Panoramica sulla configurazione di NetApp Volume Encryption".

- Se gli snapshot di conservazione a lungo termine sono abilitati su un volume di destinazione SnapMirror utilizzando la pianificazione nel criterio SnapMirror, gli snapshot vengono creati direttamente sul volume di destinazione. In questo caso, non è consigliabile eseguire il backup di tali volumi utilizzando il backup e recovery di BlueXP , poiché tali snapshot non verranno spostate nello storage a oggetti.
- Quando si crea o modifica un criterio di backup quando al criterio non sono assegnati volumi, il numero di backup conservati può essere massimo di 1018. Dopo aver assegnato i volumi al criterio, è possibile modificare il criterio per creare fino a 4000 backup.
- Quando si esegue il backup dei volumi di protezione dei dati (DP):
  - Relazioni con le etichette SnapMirror `app_consistent` e. `all_source_snapshot` non verrà eseguito il backup nel cloud.
  - Se si creano copie locali di Snapshot sul volume di destinazione di SnapMirror (indipendentemente dalle etichette di SnapMirror utilizzate), queste istantanee non verranno spostate nel cloud come backup. A questo punto, è necessario creare una policy Snapshot con le etichette desiderate nel volume DP di origine per eseguire il backup di BlueXP e il ripristino.
- I backup dei volumi FlexGroup non possono essere spostati nello storage di archiviazione.
- I backup dei volumi FlexGroup possono utilizzare la protezione DataLock e ransomware se il cluster esegue ONTAP 9.13.1 o superiore.
- Il backup del volume SVM-DR è supportato con le seguenti restrizioni:
  - I backup sono supportati solo dal secondario ONTAP.
  - Il criterio Snapshot applicato al volume deve essere uno dei criteri riconosciuti dal backup e ripristino BlueXP, inclusi quelli giornalieri, settimanali, mensili e così via Il criterio predefinito "SM_created"

(utilizzato per **Mirror All Snapshots**) non viene riconosciuto e il volume DP non viene visualizzato nell'elenco dei volumi di cui è possibile eseguire il backup.

  - Le soluzioni SVM-DR e backup e recovery dei volumi funzionano in maniera completamente indipendente quando viene eseguito il backup dall'origine o dalla destinazione. L'unica restrizione è che SVM-DR non replica la relazione cloud di SnapMirror. Nello scenario di disaster recovery, quando le SVM vanno online nel luogo secondario, devi aggiornare manualmente la relazione al cloud di SnapMirror.

- Supporto MetroCluster:
  - Quando si utilizza ONTAP 9.12.1 GA o versione successiva, il backup è supportato quando è collegato al sistema primario. L'intera configurazione di backup viene trasferita al sistema secondario in modo che i backup nel cloud continuino automaticamente dopo lo switchover. Non è necessario configurare il backup sul sistema secondario (in realtà, non è necessario farlo).
  - Quando si utilizza ONTAP 9.12.0 e versioni precedenti, il backup è supportato solo dal sistema secondario ONTAP.
  - Al momento non sono supportati i backup dei volumi FlexGroup.
- Il backup del volume ad-hoc con il pulsante **Backup Now** non è supportato sui volumi di protezione dei dati.
- Le configurazioni SM-BC non sono supportate.
- ONTAP non supporta la fan-out delle relazioni di SnapMirror da un singolo volume a più archivi di oggetti; pertanto, questa configurazione non è supportata dal backup e ripristino di BlueXP.
- La modalità WORM/Compliance in un archivio di oggetti è attualmente supportata su Amazon S3, Azure e StorageGRID. Questa funzione è nota come funzionalità DataLock e deve essere gestita utilizzando le impostazioni di backup e ripristino di BlueXP e non l'interfaccia del provider cloud.

Limitazioni di ripristino per i volumi ONTAP

Queste limitazioni si applicano sia ai metodi Search & Restore che Browse & Restore per il ripristino di file e cartelle, a meno che non venga espressamente indicato.

- Browse & Restore consente di ripristinare fino a 100 singoli file alla volta.
- Search & Restore può ripristinare 1 file alla volta.
- Quando si utilizza ONTAP 9.13.0 o versione successiva, Sfoglia e ripristina e Cerca e ripristina una cartella con tutti i file e le sottocartelle al suo interno.

  Quando si utilizza una versione di ONTAP superiore alla 9.11.1 ma precedente alla 9.13.0, l'operazione di ripristino consente di ripristinare solo la cartella selezionata e i file contenuti in tale cartella, senza ripristinare le sottocartelle o i file contenuti nelle sottocartelle.

  Quando si utilizza una versione di ONTAP precedente alla 9.11.1, il ripristino delle cartelle non è supportato.

- Il ripristino di directory/cartelle è supportato per i dati che risiedono nello storage di archiviazione solo quando il cluster esegue ONTAP 9.13.1 e versioni successive.
- Il ripristino di directory/cartelle è supportato per i dati protetti mediante DataLock solo quando il cluster esegue ONTAP 9.13.1 e versioni successive.
- Il ripristino di directory/cartelle non è attualmente supportato da repliche e/o snapshot locali.
- Il ripristino da volumi FlexGroup a volumi FlexVol o da volumi FlexVol a volumi FlexGroup non è supportato.

- Il file da ripristinare deve utilizzare la stessa lingua del volume di destinazione. Se le lingue non sono uguali, viene visualizzato un messaggio di errore.
- La priorità di ripristino *alta* non è supportata quando si ripristinano i dati dallo storage di archivio Azure ai sistemi StorageGRID.
- Se si effettua il backup di un volume DP e si decide di interrompere la relazione di SnapMirror in quel volume, non sarà possibile ripristinare i file in quel volume a meno che non si elimini anche la relazione di SnapMirror o si inverta la direzione di SnapMirror.
- Limitazioni del ripristino rapido:
  - La posizione di destinazione deve essere un sistema Cloud Volumes ONTAP che utilizzi ONTAP 9.13.0 o versioni successive.
  - Non è supportato con i backup che si trovano nell'archivio.
  - I volumi FlexGroup sono supportati solo se il sistema di origine da cui è stato creato il backup cloud eseguiva ONTAP 9.12.1 o versione successiva.
  - I volumi SnapLock sono supportati solo se il sistema di origine da cui è stato creato il backup cloud eseguiva ONTAP 9.11.0 o versione successiva.

Limitazioni note del BlueXP backup and recovery per i carichi di lavoro di Microsoft SQL Server

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.

Supporto del ciclo di vita dei cloni

- La clonazione da un archivio di oggetti non è supportata.
- Le operazioni di clonazione in blocco non sono supportate per i cloni su richiesta.
- La scelta dei gruppi I non è supportata.
- La scelta delle opzioni QOS (throughput massimo) non è supportata.

Solo modalità di distribuzione standard

La versione BlueXP backup and recovery funziona solo in modalità di distribuzione standard, non in modalità riservata o privata.

Restrizione del nome del cluster Windows

Il nome del cluster Windows non può contenere il carattere di sottolineatura (_).

Problemi di migrazione SnapCenter

La migrazione delle risorse da SnapCenter al BlueXP backup and recovery presenta le seguenti limitazioni.

Per i dettagli su come i criteri SnapCenter migrano ai criteri BlueXP backup and recovery , vedere "Criteri in SnapCenter confrontati con quelli nel BlueXP backup and recovery" .

Limitazioni del gruppo di risorse

Se tutte le risorse in un gruppo di risorse sono protette e una di queste risorse è protetta anche all'esterno del gruppo di risorse, la migrazione da SnapCenter viene bloccata.

Soluzione alternativa: proteggere la risorsa in un gruppo di risorse o da sola, ma non in entrambi.

Risorse con più policy che utilizzano lo stesso livello di pianificazione non supportate

Non è possibile assegnare più policy che utilizzano lo stesso livello di pianificazione (ad esempio, oraria, giornaliera, settimanale, ecc.) a una risorsa. Il BlueXP backup and recovery non importeranno tali risorse da SnapCenter.

Soluzione alternativa: associare a una risorsa solo una policy utilizzando lo stesso livello di pianificazione.

Le politiche orarie devono iniziare all'inizio dell'ora

Se si dispone di una policy SnapCenter che si ripete ogni ora, ma le ore non sono a intervalli all'inizio dell'ora, il BlueXP backup and recovery non importeranno la risorsa. Ad esempio, le policy con pianificazioni alle 1:30, 2:30, 3:30, ecc. non sono supportate, mentre le policy con pianificazioni alle 1:00, 2:00, 3:00, ecc. sono supportate.

Soluzione alternativa: utilizzare un criterio che si ripete a intervalli di 1 ora a partire dall'inizio dell'ora.

Non sono supportate le policy giornaliere e mensili associate a una risorsa

Se un criterio SnapCenter si ripete sia a intervalli giornalieri che mensili, il BlueXP backup and recovery non importeranno il criterio.

Ad esempio, non è possibile associare una policy giornaliera (con durata inferiore o uguale a 7 giorni oppure superiore a 7 giorni) a una risorsa e contemporaneamente associare una policy mensile alla stessa risorsa.

Soluzione alternativa: utilizzare un criterio che preveda un intervallo giornaliero o mensile, ma non entrambi.

Criteri di backup su richiesta non migrati

Il BlueXP backup and recovery non importano criteri di backup su richiesta da SnapCenter.

Criteri di backup solo log non migrati

BlueXP backup and recovery non importa i criteri di backup solo log da SnapCenter. Se un criterio di SnapCenter include backup solo log, BlueXP backup and recovery non importerà la risorsa.

Soluzione alternativa: utilizzare un criterio in SnapCenter che utilizzi più dei semplici backup dei soli registri.

Mappatura host

SnapCenter non dispone di cluster di storage o SVM per la mappatura delle risorse sugli host, a differenza di BlueXP backup and recovery . Il cluster ONTAP o SVM locale non verrà mappato a un host nella versione Preview BlueXP backup and recovery . Inoltre, BlueXP non supporta le SVM.

Soluzione alternativa: prima di importare risorse da SnapCenter, creare un ambiente di lavoro in BlueXP backup and recovery per tutti i sistemi di storage ONTAP locali registrati in SnapCenter locale. Quindi, importare le risorse per quel cluster da SnapCenter in BlueXP backup and recovery.

Orari non a intervalli di 15 minuti

Se si dispone di una pianificazione di criteri SnapCenter che inizia a una determinata ora e si ripete ogni tot minuti, ma i minuti non sono a intervalli di 15 minuti, il BlueXP backup and recovery non importeranno la pianificazione.

Soluzione alternativa: utilizzare SnapCenter per modificare il criterio in modo che venga ripetuto a intervalli di 15 minuti.

Limitazioni note del BlueXP backup and recovery per i carichi di lavoro VMware

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.

Le seguenti azioni non sono supportate nella versione di anteprima dei carichi di lavoro VMware nel BlueXP backup and recovery:

- Montare
- Smonta
- Ripristina in posizione alternativa
- Ripristina VMDK
- Allega VMDK
- Stacca VMDK
- Supporto vVol
- Supporto NVMe
- Integrazione e-mail
- Modifica la politica
- Modifica gruppo di protezione
- Supporto per il controllo degli accessi basato sui ruoli (RBAC)

Inizia subito

Informazioni su backup e ripristino BlueXP

Il servizio BlueXP backup and recovery fornisce una protezione dei dati efficiente, sicura e conveniente per volumi ONTAP , istanze e database Microsoft SQL Server, carichi di lavoro VMware (anteprima) e carichi di lavoro Kubernetes (anteprima).

> La documentazione sulla protezione dei carichi di lavoro VMware e Kubernetes viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

Cosa puoi fare con il BlueXP backup and recovery

Utilizza il BlueXP backup and recovery per raggiungere i seguenti obiettivi:

- * Carichi di lavoro del volume ONTAP *:
  - Crea snapshot locali, replica su storage secondario ed esegui il backup di volumi ONTAP da sistemi ONTAP locali o Cloud Volumes ONTAP su storage di oggetti nel tuo account cloud pubblico o privato.
  - Crea backup incrementali permanenti a livello di blocco, che vengono archiviati su un altro cluster ONTAP e nell'archiviazione di oggetti nel cloud.
  - Utilizza il BlueXP backup and recovery insieme a SnapCenter.
  - Fare riferimento a "Proteggere i volumi ONTAP" .
- **Carichi di lavoro di Microsoft SQL Server**:
  - Esegui il backup di istanze e database di Microsoft SQL Server da ONTAP locale, Cloud Volumes ONTAP o Amazon FSx for NetApp ONTAP.
  - Ripristinare i database di Microsoft SQL Server.
  - Clonare i database Microsoft SQL Server.
  - Utilizzare il BlueXP backup and recovery senza SnapCenter.
  - Fare riferimento a "Proteggere i carichi di lavoro di Microsoft SQL Server" .
- **Carichi di lavoro VMware (anteprima con nuova interfaccia utente senza SnapCenter Plug-in for VMware vSphere)**:
  - Proteggi le tue VM VMware e i tuoi datastore con il BlueXP backup and recovery.
  - Esegui il backup dei carichi di lavoro VMware su Amazon Web Services S3 o StorageGRID (per l'anteprima).
  - Ripristina i dati VMware dal cloud al vCenter locale.
  - Utilizzare il BlueXP backup and recovery senza il SnapCenter Plug-in for VMware vSphere.
  - Fare riferimento a "Proteggi i carichi di lavoro VMware" .
- **Carichi di lavoro VMware (con SnapCenter Plug-in for VMware vSphere)**:
  - Esegui il backup di VM e datastore su Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform e StorageGRID e ripristina le VM sul SnapCenter Plug-in for VMware vSphere .
  - Ripristina i dati della VM dal cloud al vCenter locale con il BlueXP backup and recovery. È possibile ripristinare la macchina virtuale esattamente nella stessa posizione da cui è stato eseguito il backup

oppure in una posizione alternativa.

- Utilizza il BlueXP backup and recovery insieme al SnapCenter Plug-in for VMware vSphere.
- Fare riferimento a "Proteggi i carichi di lavoro VMware" .

- **Carichi di lavoro Kubernetes (anteprima)**:
  - Gestisci e proteggi le tue applicazioni e risorse Kubernetes, tutto in un unico posto.
  - Utilizza criteri di protezione per strutturare i tuoi backup incrementali.
  - Ripristinare applicazioni e risorse negli stessi cluster e namespace o in cluster e namespace diversi.
  - Utilizzare il BlueXP backup and recovery senza SnapCenter.
  - Fare riferimento a "Proteggere i carichi di lavoro di Kubernetes" .

Vantaggi dell'utilizzo BlueXP backup and recovery

Il BlueXP backup and recovery offrono i seguenti vantaggi:

- **Efficiente**: il BlueXP backup and recovery eseguono una replica incrementale e continua a livello di blocco, riducendo significativamente la quantità di dati replicati e archiviati. Ciò contribuisce a ridurre al minimo il traffico di rete e i costi di archiviazione.
- **Sicuro**: il BlueXP backup and recovery crittografano i dati in transito e a riposo e utilizzano protocolli di comunicazione sicuri per proteggere i tuoi dati.
- **Conveniente**: il BlueXP backup and recovery utilizzano i livelli di archiviazione più economici disponibili nel tuo account cloud, il che aiuta a ridurre i costi.
- **Automatizzato**: il BlueXP backup and recovery generano automaticamente backup in base a una pianificazione predefinita, il che aiuta a garantire la protezione dei dati.
- **Flessibile**: il BlueXP backup and recovery consentono di ripristinare i dati nello stesso ambiente di lavoro o in uno diverso, garantendo flessibilità nel ripristino dei dati.

Costo

NetApp non ti addebita alcun costo per l'utilizzo della versione di prova. Tuttavia, i costi associati alle risorse cloud che utilizzi, come i costi di storage e di trasferimento dati, sono a tuo carico.

Esistono due tipi di costi associati all'utilizzo della funzionalità di backup su oggetto del BlueXP backup and recovery con i sistemi ONTAP :

- Costi delle risorse
- Costi del servizio

Non vi è alcun costo per la creazione di copie snapshot o volumi replicati, a parte lo spazio su disco necessario per archiviare le copie snapshot e i volumi replicati.

Costi delle risorse

I costi delle risorse vengono pagati al cloud provider per la capacità dello storage a oggetti e per la scrittura e la lettura dei file di backup nel cloud.

- Per il backup su storage a oggetti, pagherai il tuo cloud provider per i costi dello storage a oggetti.

  Poiché il BlueXP backup and recovery preservano l'efficienza di archiviazione del volume di origine, si pagano al provider cloud i costi di archiviazione degli oggetti per i dati *dopo* le efficienze ONTAP (per la

quantità minore di dati dopo l'applicazione della deduplicazione e della compressione).

- Per il ripristino dei dati utilizzando Search & Restore, alcune risorse vengono fornite dal tuo cloud provider e il costo per TIB è associato alla quantità di dati sottoposti a scansione dalle tue richieste di ricerca. (Queste risorse non sono necessarie per Browse & Restore).
  - In AWS, "Amazon Athena" e. "Colla AWS" Le risorse vengono implementate in un nuovo bucket S3.
  - In Azure, An "Spazio di lavoro Azure Synapse" e. "Storage Azure Data Lake" vengono forniti nell'account storage per memorizzare e analizzare i dati.
- In Google, viene distribuito un nuovo bucket e il "Servizi Google Cloud BigQuery" sono forniti a livello di account/progetto. endif::gcp[]
  - Se si prevede di ripristinare i dati del volume da un file di backup spostato nello storage a oggetti di archivio, è prevista una tariffa aggiuntiva per il recupero di GiB e per richiesta addebitata dal cloud provider.
  - Se intendi analizzare un file di backup alla ricerca di ransomware durante il processo di ripristino dei dati del volume (se hai abilitato DataLock e Ransomware Protection per i tuoi backup cloud), dovrai sostenere anche costi di uscita aggiuntivi dal tuo provider cloud.

Costi di servizio

I costi di servizio vengono pagati a NetApp e coprono sia il costo per *creare* backup nello storage a oggetti che per *ripristinare* volumi, o file, da tali backup. Si paga solo per i dati protetti nell'archiviazione di oggetti, calcolati in base alla capacità logica utilizzata all'origine (prima delle efficienze ONTAP) dei volumi ONTAP sottoposti a backup nell'archiviazione di oggetti. Questa capacità è nota anche come terabyte front-end (FETB).

Per Microsoft SQL Server, vengono applicati dei costi quando si avvia la replica di snapshot su una destinazione ONTAP secondaria o su un archivio di oggetti.

Esistono tre modi per pagare il servizio Backup:

- La prima opzione è iscriversi al tuo cloud provider, che ti consente di pagare al mese.
- La seconda opzione consiste nell'ottenere un contratto annuale.
- La terza opzione consiste nell'acquistare le licenze direttamente da NetApp. Leggi il Licensing sezione per i dettagli.

Licensing

Il BlueXP backup and recovery sono disponibili in prova gratuita. È possibile utilizzare il servizio senza una chiave di licenza per un periodo di tempo limitato.

Il backup e ripristino BlueXP è disponibile con i seguenti modelli di consumo:

- **Bring your own license (BYOL)**: licenza acquistata da NetApp che può essere utilizzata con qualsiasi provider cloud.
- **Pagamento in base al consumo (PAYGO)**: un abbonamento orario dal marketplace del tuo provider cloud.
- **Annuale**: Un contratto annuale dal mercato del tuo cloud provider.

Una licenza di backup è richiesta solo per il backup e il ripristino dallo storage a oggetti. La creazione di copie Snapshot e volumi replicati non richiede una licenza.

Porta la tua patente

BYOL è basato sulla durata (1, 2 o 3 anni) e sulla capacità, in incrementi di 1 TiB. Pagherai NetApp per utilizzare il servizio per un periodo di tempo, ad esempio 1 anno, e per una capacità massima, ad esempio 10 TIB.

Riceverai un numero di serie che inserisci nella pagina del portafoglio digitale BlueXP per attivare il servizio. Una volta raggiunto il limite, è necessario rinnovare la licenza. La licenza BYOL di backup si applica a tutti i sistemi sorgente associati alla tua organizzazione o account BlueXP .

"Scopri come impostare le licenze".

Abbonamento a consumo

Il backup e ripristino BlueXP offre licenze basate sui consumi in un modello pay-as-you-go. Dopo aver effettuato l'iscrizione tramite il marketplace del tuo cloud provider, pagherai per ogni GiB i dati di cui hai eseguito il backup, senza alcun pagamento anticipato. Il tuo cloud provider ti addebita la fattura mensile.

Ricorda che una prova gratuita di 30 giorni è disponibile quando ti iscrivi inizialmente con un abbonamento PAYGO.

Contratto annuale

Quando utilizzi AWS, sono disponibili due contratti annuali per 1, 2 o 3 anni:

- Un piano di "backup sul cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.
- Un piano "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Ciò include backup illimitati per i Cloud Volumes ONTAP addebitati su questa licenza (la capacità di backup non viene conteggiata sulla licenza). endif::aws[]

Quando utilizzi Azure, sono disponibili due contratti annuali per 1, 2 o 3 anni:

- Un piano di "backup sul cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.
- Un piano "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Ciò include backup illimitati per i Cloud Volumes ONTAP addebitati su questa licenza (la capacità di backup non viene conteggiata sulla licenza). endif::azure[]

Quando utilizzi GCP, puoi richiedere un'offerta privata da NetApp e quindi selezionare il piano quando ti iscrivi da Google Cloud Marketplace durante l'attivazione BlueXP backup and recovery . endif::gcp[]

Origini dati supportate, ambienti di lavoro e destinazioni di backup

Fonti di dati del carico di lavoro supportate

Il servizio protegge i seguenti carichi di lavoro:

- Volumi ONTAP
- Istanze e database di Microsoft SQL Server per NFS fisico, VMware Virtual Machine File System (VMFS) e VMware Virtual Machine Disk (VMDK)
- VM e datastore VMware
- Carichi di lavoro Kubernetes (anteprima)

Ambienti di lavoro supportati

- SAN ONTAP on-premise (protocollo iSCSI) e NAS (utilizzando protocolli NFS e CIFS) con ONTAP versione 9.8 e successive
- Cloud Volumes ONTAP 9.8 o versione successiva per AWS (utilizzando SAN e NAS)
- Cloud Volumes ONTAP 9.8 o versione successiva per Microsoft Azure (utilizzando SAN e NAS)
- Amazon FSX per NetApp ONTAP

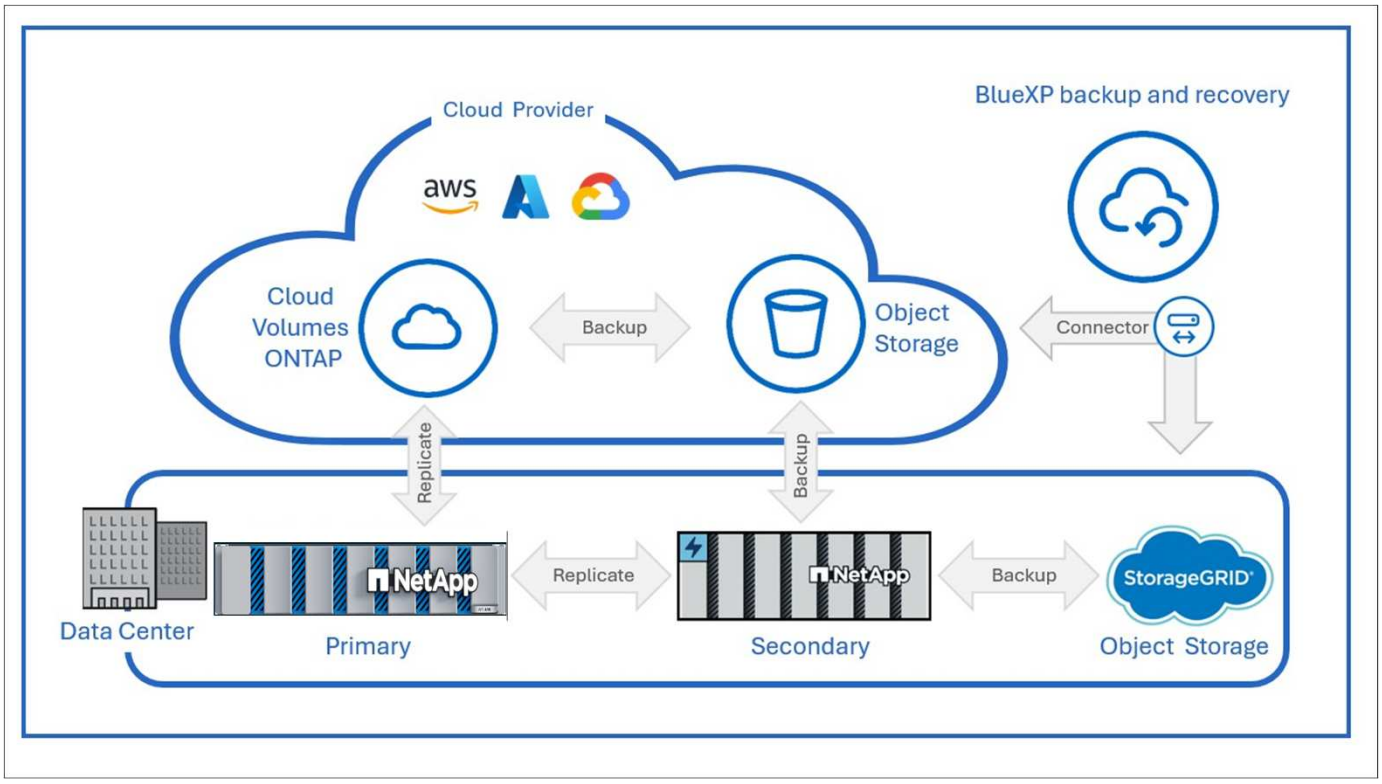
Destinazioni di backup supportate

- Amazon Web Services (AWS) S3
- Microsoft Azure Blob (non disponibile per i carichi di lavoro VMware in anteprima)
- StorageGRID
- ONTAP S3 (non disponibile per carichi di lavoro VMware in anteprima)

Come funziona il backup e ripristino di BlueXP

Abilitando il BlueXP backup and recovery, il servizio esegue un backup completo dei dati. Dopo il backup iniziale, tutti i backup successivi saranno incrementali. In questo modo il traffico di rete viene ridotto al minimo.

L'immagine seguente mostra la relazione tra i componenti.



È supportato anche lo storage primario in quello degli oggetti, non solo quello secondario in quello degli oggetti.

Dove risiedono i backup nelle posizioni dell'archivio oggetti

Le copie di backup vengono memorizzate in un archivio di oggetti creato da BlueXP nel tuo account cloud. Esiste un archivio oggetti per cluster o ambiente di lavoro e BlueXP assegna a tale archivio il seguente nome:

`netapp-backup-clusteruuid` . Assicurarsi di non eliminare questo archivio di oggetti.

- In AWS, BlueXP abilita l' "Funzione di accesso pubblico a blocchi Amazon S3" sul bucket S3. endif::aws[]
- In Azure, BlueXP utilizza un gruppo di risorse nuovo o esistente con un account di storage per il container Blob. BlueXP "blocca l'accesso pubblico ai dati blob" per impostazione predefinita. endif::azure[]
- In StorageGRID, BlueXP utilizza un account di storage esistente per il bucket dell'archivio di oggetti.
- In ONTAP S3, BlueXP utilizza un account utente esistente per il bucket S3.

Le copie di backup sono associate alla tua organizzazione BlueXP

Le copie di backup sono associate all'organizzazione BlueXP in cui risiede BlueXP Connector. "Informazioni sulla gestione delle identità e degli accessi di BlueXP" .

Se nella stessa organizzazione BlueXP sono presenti più connettori, ogni connettore visualizza lo stesso elenco di backup.

Termini che potrebbero aiutarti con il BlueXP backup and recovery

Potrebbe essere utile comprendere un po' di terminologia relativa alla protezione.

- **Protezione**: la protezione nel BlueXP backup and recovery significa garantire che gli snapshot e i backup immutabili vengano eseguiti regolarmente su un dominio di sicurezza diverso mediante criteri di protezione.
- **Carico di lavoro**: un carico di lavoro nel BlueXP backup and recovery può includere volumi ONTAP , istanze e database di Microsoft SQL Server; VM e datastore VMware; oppure cluster e applicazioni Kubernetes.

Prerequisiti per il BlueXP backup and recovery

Inizia a utilizzare il BlueXP backup and recovery verificando la disponibilità del tuo ambiente operativo, del connettore BlueXP e dell'account BlueXP . Per utilizzare il BlueXP backup and recovery, sono necessari i seguenti prerequisiti.

Per ONTAP 9.8 e versioni successive

È necessario abilitare una licenza ONTAP One sull'istanza ONTAP locale.

Prerequisiti per i backup su storage di oggetti

Per utilizzare l'archiviazione di oggetti come destinazione di backup, è necessario un account con AWS S3, Microsoft Azure Blob, StorageGRID o ONTAP e che siano configurate le autorizzazioni di accesso appropriate.

- "Proteggi i dati del tuo volume ONTAP"

Requisiti per la protezione dei carichi di lavoro di Microsoft SQL Server

Per utilizzare il BlueXP backup and recovery per i carichi di lavoro di Microsoft SQL Server, sono necessari i seguenti prerequisiti relativi a sistema host, spazio e dimensioni.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per le informazioni più recenti sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp" .
Versioni di Microsoft SQL Server	Le versioni 2012 e successive sono supportate per VMware Virtual Machine File System (VMFS) e VMware Virtual Machine Disk (VMDK) NFS.
Versione di SnapCenter Server	Per importare i dati esistenti da SnapCenter in BlueXP backup and recovery è richiesta la versione 5.0 o successiva di SnapCenter Server. Se disponi già di SnapCenter, verifica innanzitutto di aver soddisfatto i prerequisiti prima di importare da SnapCenter. Vedere "Prerequisiti per l'importazione di risorse da SnapCenter".
RAM minima per il plug-in sull'host SQL Server	1 GB
Spazio minimo di installazione e registro per il plug-in sull'host SQL Server	5 GB Allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione della cartella dei log. Lo spazio richiesto per i log varia in base al numero di backup eseguiti e alla frequenza delle operazioni di protezione dei dati. Se lo spazio non è sufficiente, i log non verranno creati per le operazioni.
Pacchetti software richiesti	• Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) • PowerShell Core 7.4.2 Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Requisiti per la protezione dei carichi di lavoro VMware

Per individuare e proteggere i carichi di lavoro VMware sono necessari requisiti specifici.

Supporto software

- Sono supportati gli archivi dati NFS e VMFS. I vVol non sono supportati.
- Versioni NFS supportate: NFS 3 e NFS 4.1
- Versioni di VMware ESXi Server supportate: 7.0U1 e successive
- Versioni di VMware vCenter vSphere supportate: 7.0U1 e successive
- Indirizzi IP: IPv4 e IPv6
- VMware TLS: 1.2, 1.3

Requisiti di connessione e porta per la protezione dei carichi di lavoro VMware

Tipo di porto	Porta preconfigurata
Porta del server VMware ESXi	443 (HTTPS), bidirezionale. La funzionalità di ripristino dei file guest utilizza questa porta.
Porta del server VMware vSphere vCenter	Se si proteggono VM vVol, è necessario utilizzare la porta 443.
Cluster di archiviazione o porta VM di archiviazione	443 (HTTPS), bidirezionale. 80 (HTTP), bidirezionale. Questa porta viene utilizzata per la comunicazione tra l'appliance virtuale e la VM di archiviazione o il cluster contenente la VM di archiviazione.

Requisiti di controllo degli accessi basato sui ruoli (RBAC) per la protezione dei carichi di lavoro VMware

L'account amministratore vCenter deve disporre dei privilegi vCenter richiesti.

Per un elenco dei privilegi vCenter necessari, vedere "SnapCenter Plug-in for VMware vSphere Privilegi vCenter necessari" .

Requisiti per la protezione delle applicazioni Kubernetes

Per scoprire le risorse di Kubernetes e proteggere le applicazioni Kubernetes, sono necessari requisiti specifici.

Per i requisiti BlueXP , fare riferimento a A BlueXP .

- Un sistema ONTAP primario (ONTAP 9.16.1 o successivo)
- Un cluster Kubernetes: le distribuzioni e le versioni di Kubernetes supportate includono:
  - Anthos On-Prem (VMware) e Anthos su bare metal 1.16
  - Kubernetes 1.27 - 1.33
  - OpenShift 4.10 - 4.18
  - Motore Kubernetes Rancher 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
- NetApp Trident 24.10 o successivo
- NetApp Trident Protect 25.07 o versione successiva (installato durante la scoperta del carico di lavoro di Kubernetes)
- NetApp Trident Protect Connector 25.07 o versione successiva (installato durante l'individuazione del carico di lavoro di Kubernetes)
  - Assicurarsi che la porta TCP 443 non sia filtrata in uscita tra il cluster Kubernetes, il connettore Trident Protect e il proxy Trident Protect.

A BlueXP

- Un utente BlueXP deve disporre del ruolo e dei privilegi necessari per eseguire operazioni sui carichi di lavoro Microsoft SQL Server e Kubernetes. Per individuare le risorse, è necessario disporre del ruolo di Super amministratore BlueXP backup and recovery . Vedi "Accesso basato sui ruoli BlueXP backup and recovery alle funzionalità" per informazioni dettagliate sui ruoli e le autorizzazioni necessarie per eseguire operazioni BlueXP backup and recovery.

- Un'organizzazione BlueXP con almeno un connettore BlueXP attivo che si connette a cluster ONTAP on-premise o Cloud Volumes ONTAP. Fare riferimento alla **Procedura di configurazione dell'anteprima iniziale** di seguito.
- Almeno un ambiente di lavoro BlueXP con un cluster NetApp ONTAP locale o Cloud Volumes ONTAP .
- Un connettore BlueXP

  Fare riferimento a "Informazioni su come configurare un connettore BlueXP" e "Requisiti standard di BlueXP".

  - La versione Preview richiede il sistema operativo Ubuntu 22.04 LTS per il connettore.

Configurare BlueXP

Il passo successivo è configurare BlueXP e il servizio BlueXP backup and recovery .

Revisione "Requisiti standard di BlueXP".

Crea un connettore BlueXP

Per provare questo servizio, ti consigliamo di contattare il tuo team di prodotto NetApp . Quindi, quando si utilizza il connettore BlueXP, esso includerà le funzionalità appropriate per il servizio.

Per creare un connettore in BlueXP prima di utilizzare il servizio, fare riferimento alla documentazione di BlueXP che descrive "Come creare un connettore BlueXP".

Dove installare il connettore BlueXP

Per completare un'operazione di ripristino, il connettore può essere installato nelle seguenti posizioni:

- Per Amazon S3, il connettore può essere distribuito in sede.
- Per Azure Blob, il connettore può essere distribuito in locale.
- Per StorageGRID, il connettore deve essere distribuito presso la tua sede, con o senza accesso a Internet.
- Per ONTAP S3, il connettore può essere implementato in sede (con o senza accesso a Internet) o in un ambiente cloud provider

I riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS e AFF .

Impostare le licenze per il backup e ripristino BlueXP

Puoi ottenere in licenza il backup e il ripristino di BlueXP acquistando un abbonamento annuale al marketplace * PAYGO (PAY-as-you-go) o ai servizi intelligenti NetApp * dal tuo cloud provider, o acquistando una BYOL (Bring-Your-Own-License) da NetApp. È necessaria una licenza valida per attivare il backup e ripristino BlueXP in un ambiente di lavoro, per creare backup dei dati di produzione e per ripristinare i dati di backup in un sistema di produzione.

Alcune note prima di leggere ulteriori informazioni:

- Se hai già sottoscritto l'abbonamento pay-as-you-go (PAYGO) nel mercato del tuo cloud provider per un sistema Cloud Volumes ONTAP, sarai automaticamente iscritto anche al backup e ripristino BlueXP. Non dovrai più iscriverti.

- Il BYOL (Bring Your Own License) di backup e recovery di BlueXP è una licenza mobile che puoi utilizzare su tutti i sistemi associati alla tua organizzazione o account BlueXP . Quindi, se si dispone di una capacità di backup sufficiente da una licenza BYOL esistente, non sarà necessario acquistare un'altra licenza BYOL.
- Se si utilizza una licenza BYOL, si consiglia di sottoscrivere anche un abbonamento PAYGO. Se si esegue il backup di un numero di dati superiore a quello consentito dalla licenza BYOL, o se la durata della licenza scade, il backup prosegue con l'abbonamento pay-as-you-go, senza interruzioni del servizio.
- Quando si esegue il backup dei dati ONTAP on-premise su StorageGRID, è necessaria una licenza BYOL, ma lo spazio di storage del cloud provider non costa.

"Scopri di più sui costi legati all'utilizzo del backup e ripristino BlueXP."

30 giorni di prova gratuita

Una prova gratuita di 30 giorni di backup e ripristino BlueXP è disponibile se ti iscrivi a un abbonamento pay-as-you-go nel mercato del tuo cloud provider per **servizi intelligenti NetApp**. La versione di prova gratuita inizia dal momento in cui ti iscrivi al marketplace listing. Nota: Se paghi per l'iscrizione al marketplace durante l'implementazione di un sistema Cloud Volumes ONTAP e poi avvia la prova gratuita di backup e recovery di BlueXP 10 giorni dopo, avrai 20 giorni rimanenti per utilizzare la prova gratuita.

Al termine della prova gratuita, potrai passare automaticamente all'abbonamento PAYGO senza interruzioni. Se decidi di non continuare a utilizzare il BlueXP backup and recovery, "Annullare la registrazione del backup e ripristino BlueXP dall'ambiente di lavoro" prima della fine del periodo di prova e non ti verrà addebitato alcun costo.

Termina la prova gratuita

Se desideri continuare a utilizzare BlueXP backup and recovery dopo la scadenza del periodo di prova gratuito, devi sottoscrivere un abbonamento a pagamento. Puoi farlo dall'interfaccia BlueXP andando alla sezione fatturazione e selezionando un piano di abbonamento adatto alle tue esigenze. Se non desideri continuare a utilizzare BlueXP backup and recovery, puoi interrompere la prova gratuita.

Se termini il periodo di prova gratuito senza sottoscrivere un piano a pagamento, i tuoi dati verranno automaticamente eliminati 60 giorni dopo la fine del periodo di prova gratuito. Facoltativamente, puoi fare in modo che il sistema elimini immediatamente i tuoi dati.

Fasi

1. Dalla pagina di destinazione BlueXP backup and recovery , seleziona **Visualizza prova gratuita**.

   DOMANDA AI RECENSORI: Come fanno gli utenti ad arrivare alla landing page se si trovano su altre pagine BR?

2. Seleziona **Termina prova gratuita**.
3. Seleziona **Elimina i dati subito dopo aver terminato la prova gratuita** per eliminare immediatamente i tuoi dati.
4. Digitare **fine prova** nella casella.
5. Selezionare **Fine** per confermare.

Utilizza un abbonamento A PAYGO per il backup e ripristino BlueXP

Per il pay-as-you-go, pagherai il tuo cloud provider per i costi dello storage a oggetti e per le licenze di backup NetApp su base oraria in un singolo abbonamento. È necessario iscriversi a **servizi intelligenti NetApp** nel

mercato anche se si dispone di una versione di prova gratuita o se si porta con sé una propria licenza BYOL:

- L'iscrizione garantisce che il servizio non subisca interruzioni al termine della prova gratuita. Al termine della prova, ti verrà addebitato ogni ora in base alla quantità di dati di cui hai effettuato il backup.
- Se effettui il backup di più dati di quanto consentito dalla licenza BYOL, le operazioni di backup e ripristino dei dati proseguiranno con l'abbonamento pay-as-you-go. Ad esempio, se si dispone di una licenza 10 TIB BYOL, tutta la capacità oltre la 10 TIB viene addebitata tramite l'abbonamento PAYGO.

Non ti verrà addebitato alcun costo dal tuo abbonamento pay-as-you-go durante la prova gratuita o se non hai superato la licenza BYOL.

Esistono alcuni piani PAYGO per il backup e il ripristino BlueXP:

- Un pacchetto di "backup cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.
- Un pacchetto "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Sono inclusi backup illimitati per il sistema Cloud Volumes ONTAP che utilizza la licenza (la capacità di backup non viene conteggiata rispetto alla capacità concessa in licenza). Questa opzione non consente di eseguire il backup dei dati ONTAP on-premise.

  Questa opzione richiede anche un abbonamento PAYGO di backup e recovery, ma non verranno addebitati costi per i sistemi Cloud Volumes ONTAP idonei.

"Scopri di più su questi pacchetti di licenza basati sulla capacità".

Utilizza questi link per iscriverti al backup e ripristino BlueXP dal tuo mercato di cloud provider:

- AWS: "Per i dettagli sui prezzi, consulta l'offerta Marketplace per i servizi intelligenti NetApp" . endif::aws[]
- Azzurro: "Per i dettagli sui prezzi, consulta l'offerta Marketplace per i servizi intelligenti NetApp" . endif::azure[]
- Google Cloud: "Per i dettagli sui prezzi, consulta l'offerta Marketplace per i servizi intelligenti NetApp" . endif::gcp[]

Utilizzare un contratto annuale

Pagare il backup e il ripristino BlueXP ogni anno acquistando un contratto annuale. Sono disponibili in termini di 1, 2 o 3 anni.

Se si dispone di un contratto annuale da un marketplace, tutti i consumi di backup e recovery di BlueXP vengono addebitati a fronte di tale contratto. Non puoi combinare un contratto di mercato annuale con un BYOL.

Quando si utilizza AWS, sono disponibili due contratti annuali da "Pagina AWS Marketplace" per sistemi Cloud Volumes ONTAP e ONTAP on-premise:

- Un piano di "backup sul cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.

  Se si desidera utilizzare questa opzione, impostare l'abbonamento dalla pagina Marketplace, quindi "Associare l'abbonamento alle credenziali AWS". È inoltre necessario pagare i sistemi Cloud Volumes ONTAP utilizzando questo abbonamento annuale, in quanto è possibile assegnare un solo abbonamento attivo alle credenziali AWS in BlueXP.

- Un piano "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Sono inclusi backup illimitati per il sistema Cloud Volumes ONTAP che utilizza la licenza (la capacità di backup non viene conteggiata rispetto alla capacità concessa in licenza). Questa opzione non consente di eseguire il backup dei dati ONTAP on-premise.

  Vedere "Argomento relativo alle licenze Cloud Volumes ONTAP" per ulteriori informazioni su questa opzione di licenza.

  Se desideri utilizzare questa opzione, puoi impostare il contratto annuale quando crei un ambiente di lavoro Cloud Volumes ONTAP e BlueXP ti chiederà di iscriverti ad AWS Marketplace. endif::aws[]

Quando si utilizza Azure, sono disponibili due contratti annuali da "Pagina del marketplace di Azure" per sistemi Cloud Volumes ONTAP e ONTAP on-premise:

- Un piano di "backup sul cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.

  Se si desidera utilizzare questa opzione, impostare l'abbonamento dalla pagina Marketplace, quindi "Associare l'iscrizione alle credenziali Azure". Nota: Dovrai anche pagare per i tuoi sistemi Cloud Volumes ONTAP utilizzando questo abbonamento di contratto annuale, poiché puoi assegnare solo un abbonamento attivo alle tue credenziali Azure in BlueXP.

- Un piano "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Sono inclusi backup illimitati per il sistema Cloud Volumes ONTAP che utilizza la licenza (la capacità di backup non viene conteggiata rispetto alla capacità concessa in licenza). Questa opzione non consente di eseguire il backup dei dati ONTAP on-premise.

  Vedere "Argomento relativo alle licenze Cloud Volumes ONTAP" per ulteriori informazioni su questa opzione di licenza.

  Se desideri utilizzare questa opzione, puoi impostare il contratto annuale quando crei un ambiente di lavoro Cloud Volumes ONTAP e BlueXP ti chiede di iscriverti ad Azure Marketplace. endif::azure[]

Se utilizzi GCP, contatta il tuo rappresentante commerciale NetApp per acquistare un contratto annuale. Il contratto è disponibile come offerta privata in Google Cloud Marketplace.

Dopo che NetApp condividerà con te l'offerta privata, potrai selezionare il piano annuale quando ti iscrivi da Google Cloud Marketplace durante l'attivazione BlueXP backup and recovery . endif::gcp[]

Utilizzare una licenza BYOL di backup e ripristino BlueXP

Le licenze Bring-Your-Own di NetApp offrono termini di 1, 2 o 3 anni. Si paga solo per i dati protetti, calcolati in base alla capacità logica utilizzata (*prima* eventuali efficienze) dei volumi ONTAP di origine di cui viene eseguito il backup. Questa capacità è nota anche come terabyte front-end (FETB).

La licenza di backup e recovery BYOL BlueXP è una licenza mobile, in cui la capacità totale viene condivisa tra tutti i sistemi associati alla tua organizzazione o account BlueXP . Per i sistemi ONTAP, è possibile ottenere una stima approssimativa della capacità necessaria eseguendo il comando CLI per i volumi di cui si intende eseguire `volume show -fields logical-used-by-afs` il backup.

Se non si dispone di una licenza BYOL di backup e ripristino BlueXP, fare clic sull'icona della chat nell'angolo inferiore destro di BlueXP per acquistarne una.

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

utilizzare, è possibile convertirla in una licenza di backup e ripristino BlueXP con la stessa equivalenza in dollari e la stessa data di scadenza. "Fai clic qui per ulteriori informazioni".

Il portafoglio digitale BlueXP consente di gestire le licenze BYOL. È possibile aggiungere nuove licenze, aggiornare le licenze esistenti e visualizzare lo stato della licenza dal portafoglio digitale BlueXP.

"Scopri come aggiungere licenze con il Digital Wallet".

Imposta le destinazioni di backup prima di utilizzare il BlueXP backup and recovery

Prima di utilizzare il BlueXP backup and recovery, eseguire alcuni passaggi per impostare le destinazioni di backup.

Prima di iniziare, verificare "prerequisiti"che l'ambiente sia pronto.

Preparare la destinazione di backup

Preparare una o più delle seguenti destinazioni di backup:

- NetApp StorageGRID.

  Fare riferimento alla "Scopri StorageGRID".

  Fare riferimento a "Documentazione StorageGRID" per i dettagli su StorageGRID.

- Servizi Web di Amazon. Fare riferimento alla "Documentazione di Amazon S3".

  Per preparare AWS come destinazione di backup, procedi come segue:

  - Configurare un account in AWS.
  - Configurare le autorizzazioni S3 in AWS, elencate nella sezione successiva.
  - Per informazioni dettagliate sulla gestione dello storage AWS in BlueXP , fare riferimento alla "Gestisci i bucket Amazon S3".

- Microsoft Azure.
  - Fare riferimento alla "Documentazione Azure NetApp Files".
  - Configurare un account in Azure.
  - Configurare "Autorizzazioni Azure" in Azzurro.
  - Per informazioni dettagliate sulla gestione dell'archiviazione di Azure in BlueXP, fare riferimento a "Gestione degli account storage Azure" .

Dopo aver configurato le opzioni nella destinazione di backup stessa, sarà possibile configurarla in seguito come destinazione di backup nel servizio BlueXP backup and recovery . Per informazioni dettagliate su come configurare la destinazione di backup nel BlueXP backup and recovery, fare riferimento a "Scopri le destinazioni di backup" .

Impostare le autorizzazioni S3

Dovrai configurare due set di autorizzazioni AWS S3:

- Permessi per il connettore per creare e gestire il bucket S3.
- Autorizzazioni per il cluster ONTAP on-premise in modo che possa leggere e scrivere i dati nel bucket S3.

Fasi

1. Assicurarsi che il connettore disponga delle autorizzazioni necessarie. Per ulteriori informazioni, vedere "Autorizzazioni dei criteri BlueXP ".

   Quando si creano backup nelle regioni AWS China, è necessario modificare il nome risorsa AWS "arn" in tutte le sezioni *Resource* delle policy IAM da "aws" a "aws-cn", ad esempio `arn:aws-cn:s3:::netapp-backup-*`.

2. Quando si attiva il servizio, la procedura guidata di backup richiede di inserire una chiave di accesso e una chiave segreta. Queste credenziali vengono passate al cluster ONTAP in modo che ONTAP possa eseguire il backup e il ripristino dei dati nel bucket S3. A tale scopo, è necessario creare un utente IAM con le seguenti autorizzazioni.

   Fare riferimento a. "Documentazione AWS: Creazione di un ruolo per delegare le autorizzazioni a un utente IAM".

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

Accedi al BlueXP backup and recovery

Per accedere al servizio BlueXP backup and recovery , utilizzare NetApp BlueXP .

Il BlueXP backup and recovery utilizzano la gestione dell'identità e dell'accesso per gestire l'accesso di ciascun utente ad azioni specifiche.

Per informazioni dettagliate sulle azioni che ogni ruolo può eseguire, vedere "Ruoli utente BlueXP backup and recovery".

Per accedere a BlueXP , puoi utilizzare le tue credenziali del sito di supporto NetApp oppure iscriverti a un login cloud NetApp utilizzando la tua email e una password. "Scopri di più sull'accesso".

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Amministratore di ripristino di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

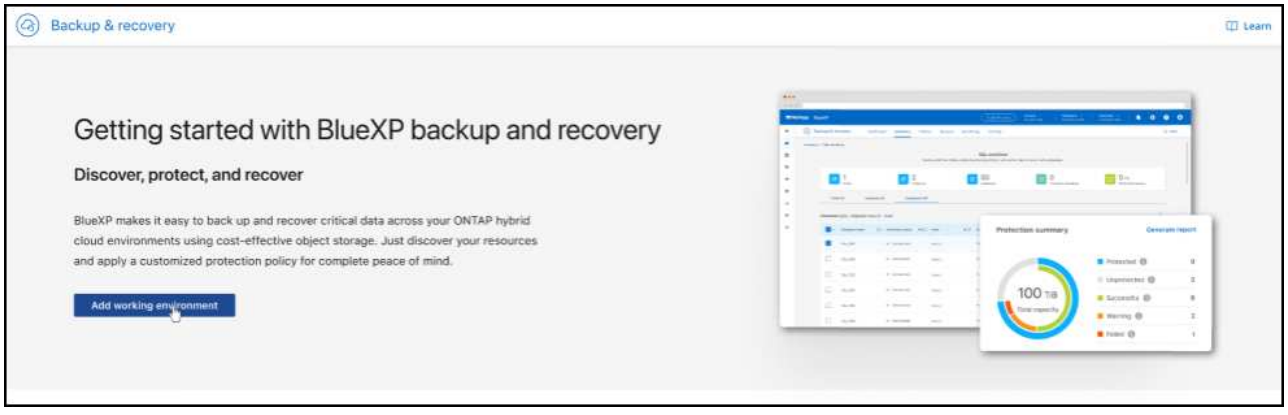
Se è la prima volta che accedi BlueXP backup and recovery e per aggiungere un connettore, devi disporre del ruolo di amministratore dell'organizzazione o di super amministratore di backup e ripristino.

Fasi

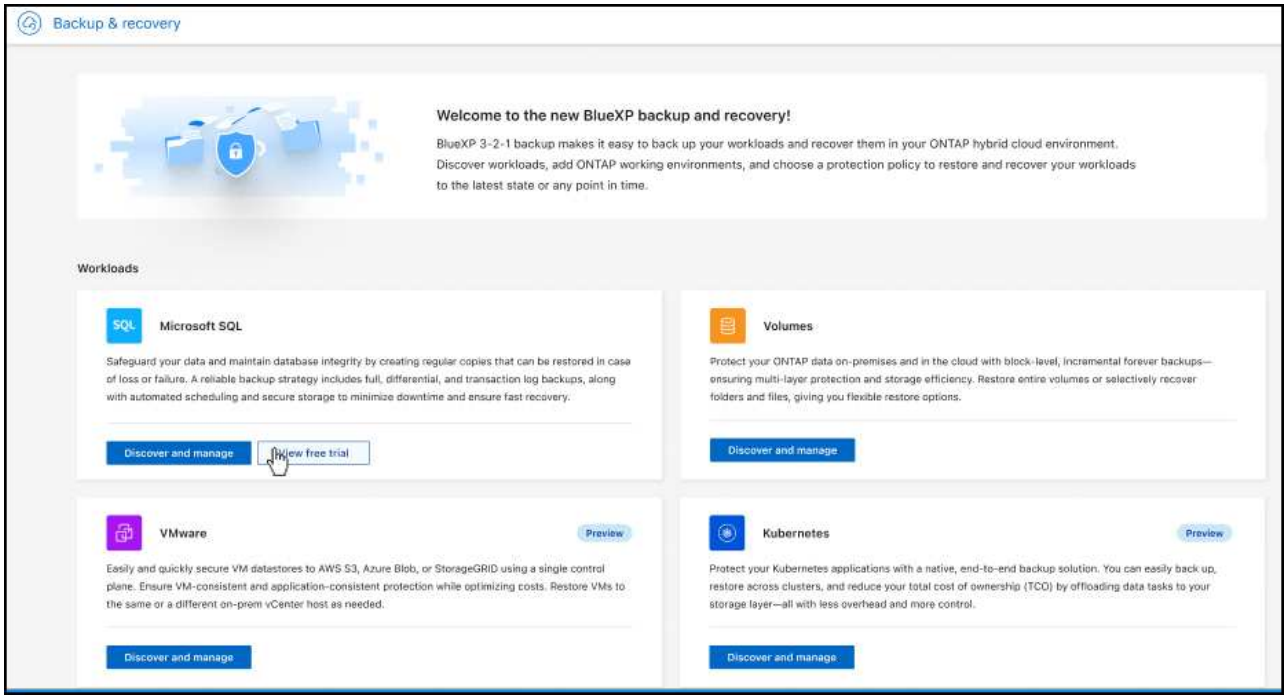
1. Aprire un browser Web e accedere a "Console BlueXP".

   Viene visualizzata la pagina di accesso a NetApp BlueXP.

2. Accedere a BlueXP.
3. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.
   - Se è la prima volta che accedi a questo servizio e non hai ancora un ambiente di lavoro, verrà visualizzata la pagina di destinazione "Benvenuti al nuovo BlueXP backup and recovery" con l'opzione "Aggiungi ambiente di lavoro". Per informazioni dettagliate sull'aggiunta di un ambiente di lavoro a BlueXP, consulta "Introduzione alla modalità standard di BlueXP" .



   - Se è la prima volta che accedi a questo servizio, hai già un ambiente di lavoro in BlueXP, ma non hai ancora iniziato la prova gratuita, verrà visualizzata la pagina di destinazione "Benvenuti nel nuovo BlueXP backup and recovery" con l'opzione **Visualizza prova gratuita**.



- Se è la prima volta che accedi a questo servizio e hai già un ambiente di lavoro in BlueXP, ma non hai ancora individuato alcuna risorsa, verrà visualizzata la pagina di destinazione "Benvenuti nel nuovo BlueXP backup and recovery" con l'opzione **Individuare e gestire**.

4. Se non lo hai ancora fatto, seleziona l'opzione **Scopri e gestisci**.
   - Per i carichi di lavoro di Microsoft SQL Server, fare riferimento a "Scopri i carichi di lavoro di Microsoft SQL Server" .
   - Per i carichi di lavoro VMware, fare riferimento a"Scopri i carichi di lavoro VMware" .
   - Per i carichi di lavoro Kubernetes, fare riferimento a"Scopri i carichi di lavoro di Kubernetes" .

Scopri le destinazioni di backup fuori sede nel BlueXP backup and recovery

Completa alcuni passaggi per scoprire o aggiungere manualmente destinazioni di backup esterne nel BlueXP backup and recovery.

Scopri un target di backup

Prima di utilizzare il BlueXP backup and recovery, è necessario configurare le destinazioni di backup di Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage o StorageGRID.

Puoi scoprire questi obiettivi automaticamente oppure aggiungerli manualmente.

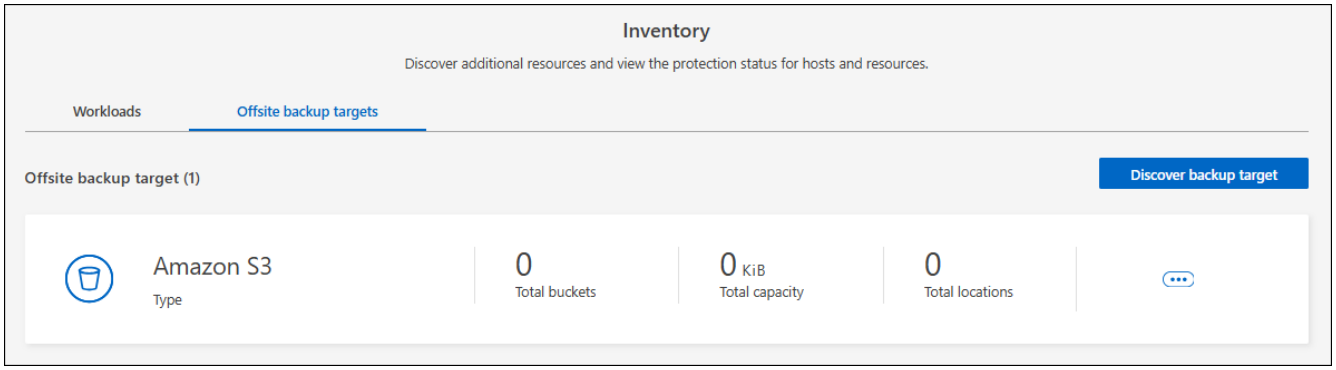
Fornire le credenziali necessarie per accedere al sistema di account di archiviazione. Queste credenziali vengono utilizzate per individuare i carichi di lavoro di cui si desidera eseguire il backup.

Prima di iniziare

Per aggiungere una destinazione di backup offsite, è necessario individuare almeno un carico di lavoro.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Selezionare la scheda **Destinazioni di backup esterne**.



3. Selezionare **Scopri destinazione di backup**.
4. Selezionare uno dei tipi di destinazione del backup: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* o * ONTAP S3*.
5. Nella sezione **Scegli posizione credenziali**, seleziona la posizione in cui risiedono le credenziali, quindi scegli come associarle.
6. Selezionare **Avanti**.
7. Inserisci le informazioni delle credenziali. Le informazioni variano a seconda del tipo di destinazione di backup selezionata e della posizione delle credenziali scelta.
   - Per AWS:
     - **Nome credenziale**: inserisci il nome della credenziale AWS.
     - **Chiave di accesso**: inserisci il segreto AWS.
     - **Chiave segreta**: inserisci la chiave segreta AWS.
   - Per Azure:
     - **Nome credenziale**: immettere il nome della credenziale di Azure Blob Storage.
     - **Segreto client**: immettere il segreto client di Azure Blob Storage.
     - **ID applicazione (client)**: seleziona l'ID applicazione di Azure Blob Storage.
     - **ID tenant directory**: immettere l'ID tenant di Azure Blob Storage.
   - Per StorageGRID:
     - **Nome credenziale**: immettere il nome della credenziale StorageGRID .
     - **FQDN del nodo gateway**: immettere un nome FQDN per StorageGRID.
     - **Porta**: immettere il numero di porta per StorageGRID.
     - **Chiave di accesso**: immettere la chiave di accesso StorageGRID S3.
     - **Chiave segreta**: Inserisci la chiave segreta StorageGRID S3.
   - Per ONTAP S3:
     - **Nome credenziale**: immettere il nome della credenziale ONTAP S3.
     - **FQDN del nodo gateway**: immettere un nome FQDN per ONTAP S3.
     - **Porta**: immettere il numero di porta per ONTAP S3.
     - **Chiave di accesso**: immettere la chiave di accesso ONTAP S3.

- **Chiave segreta**: Inserisci la chiave segreta ONTAP S3.

8. Selezionare **Discover**.

Aggiungi un bucket per una destinazione di backup

Invece di far sì che il BlueXP backup and recovery rilevino automaticamente i bucket, è possibile aggiungerne manualmente uno a una destinazione di backup esterna.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Selezionare **Destinazioni di backup esterne**.
3. Seleziona il target e sulla destra seleziona **Azioni** ••• icona e seleziona **Aggiungi bucket**.
4. Inserisci le informazioni del bucket. Le informazioni variano a seconda del tipo di destinazione di backup selezionata.
   - Per AWS:
     - **Nome bucket**: immettere il nome del bucket S3. Il prefisso "netapp-backup" è obbligatorio e viene aggiunto automaticamente al nome fornito.
     - **Account AWS**: inserisci il nome dell'account AWS.
     - **Regione del bucket**: immetti la regione AWS per il bucket.
     - **Abilita Blocco Oggetti S3**: seleziona questa opzione per abilitare il Blocco Oggetti S3 per il bucket. Il Blocco Oggetti S3 impedisce che gli oggetti vengano eliminati o sovrascritti per un periodo di conservazione specificato, fornendo un ulteriore livello di protezione dei dati. Puoi abilitare questa opzione solo durante la creazione di un bucket e non potrai disattivarla in seguito.
       - **Modalità di governance**: seleziona questa opzione per abilitare la modalità di governance per il bucket S3 Object Lock. La modalità di governance consente di proteggere gli oggetti dall'eliminazione o dalla sovrascrittura da parte della maggior parte degli utenti, ma consente ad alcuni utenti di modificarne le impostazioni di conservazione.
       - **Modalità di conformità**: seleziona questa opzione per abilitare la modalità di conformità per il bucket S3 Object Lock. La modalità di conformità impedisce a qualsiasi utente, incluso l'utente root, di modificare le impostazioni di conservazione o eliminare oggetti fino alla scadenza del periodo di conservazione.
     - **Versioning**: seleziona questa opzione per abilitare il versioning per il bucket S3. Il versioning consente di conservare più versioni degli oggetti nel bucket, il che può essere utile per scopi di backup e ripristino.
     - **Tag**: seleziona i tag per il bucket S3. I tag sono coppie chiave-valore che possono essere utilizzate per organizzare e gestire le risorse S3.
     - **Crittografia**: seleziona il tipo di crittografia per il bucket S3. Le opzioni disponibili sono chiavi gestite da AWS S3 o chiavi di AWS Key Management Service. Se selezioni chiavi di AWS Key Management Service, devi fornire l'ID della chiave.
   - Per Azure:
     - **Sottoscrizione**: seleziona il nome del contenitore di Azure Blob Storage.
     - **Gruppo di risorse**: seleziona il nome del gruppo di risorse di Azure.
     - **Dettagli dell'istanza**:
       - **Nome account di archiviazione**: immetti il nome del contenitore Azure Blob Storage.

        - **Regione di Azure**: immettere la regione di Azure per il contenitore.
        - **Tipo di prestazioni**: seleziona il tipo di prestazioni, standard o premium, per il contenitore Azure Blob Storage, indicando il livello di prestazioni richiesto.
        - **Crittografia**: seleziona il tipo di crittografia per il contenitore di Archiviazione BLOB di Azure. Le opzioni disponibili sono chiavi gestite da Microsoft o chiavi gestite dal cliente. Se selezioni le chiavi gestite dal cliente, devi fornire il nome dell'archivio chiavi e il nome della chiave.
    - Per StorageGRID:
        - **Nome destinazione backup**: seleziona il nome del bucket StorageGRID .
        - **Nome bucket**: immetti il nome del bucket StorageGRID .
        - **Regione**: immettere la regione StorageGRID per il bucket.
        - **Abilita versioning**: seleziona questa opzione per abilitare il versioning per il bucket StorageGRID . Il versioning consente di conservare più versioni degli oggetti nel bucket, il che può essere utile per scopi di backup e ripristino.
        - **Blocco degli oggetti**: seleziona questa opzione per abilitare il blocco degli oggetti per il bucket StorageGRID . Il blocco degli oggetti impedisce che gli oggetti vengano eliminati o sovrascritti per un periodo di conservazione specificato, fornendo un ulteriore livello di protezione dei dati. Puoi abilitare questa opzione solo durante la creazione di un bucket e non potrai disattivarla in seguito.
        - **Capacità**: Inserisci la capacità del bucket StorageGRID . Questa è la quantità massima di dati che può essere archiviata nel bucket.
    - Per ONTAP S3:
        - **Nome destinazione backup**: seleziona il nome del bucket ONTAP S3.
        - **Nome destinazione bucket**: immettere il nome del bucket ONTAP S3.
        - **Capacità**: Inserisci la capacità del bucket ONTAP S3. Questa è la quantità massima di dati che può essere archiviata nel bucket.
        - **Abilita versioning**: seleziona questa opzione per abilitare il versioning per il bucket ONTAP S3. Il versioning consente di conservare più versioni degli oggetti nel bucket, il che può essere utile per scopi di backup e ripristino.
        - **Blocco degli oggetti**: seleziona questa opzione per abilitare il blocco degli oggetti per il bucket ONTAP S3. Il blocco degli oggetti impedisce che gli oggetti vengano eliminati o sovrascritti per un periodo di conservazione specificato, fornendo un ulteriore livello di protezione dei dati. Puoi abilitare questa opzione solo durante la creazione di un bucket e non potrai disattivarla in seguito.
5. Selezionare **Aggiungi**.

Modifica le credenziali per una destinazione di backup

Immettere le credenziali necessarie per accedere alla destinazione di backup.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Selezionare **Destinazioni di backup esterne**.
3. Seleziona il target e sulla destra seleziona **Azioni** ••• icona e seleziona **Modifica credenziali**.
4. Inserisci le nuove credenziali per la destinazione di backup. Le informazioni variano a seconda del tipo di destinazione di backup selezionata.
5. Selezionare **fine**.

Passa a diversi carichi di lavoro BlueXP backup and recovery

È possibile passare da un carico di lavoro all'altro di BlueXP backup and recovery . Alcuni carichi di lavoro utilizzano un'interfaccia utente diversa.

Come fai a sapere quale interfaccia utente stai utilizzando?

La barra delle applicazioni per i carichi di lavoro Microsoft SQL Server, VMware (anteprima senza SnapCenter Plug-in for VMware vSphere) e Kubernetes (anteprima) ha questo aspetto:

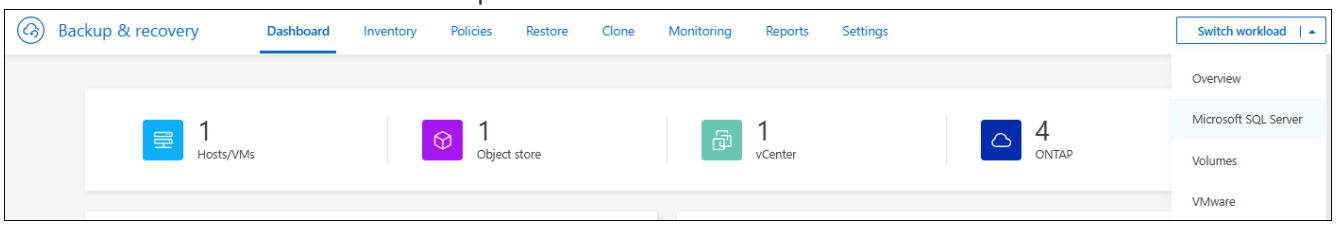
La barra dei menu per i volumi ONTAP e i carichi di lavoro VMware (con il SnapCenter Plug-in for VMware vSphere) si presenta così:

Passa a un carico di lavoro diverso

È possibile passare a un carico di lavoro diverso nell'interfaccia utente BlueXP backup and recovery .

Fasi

1. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.
2. Dall'angolo in alto a destra della pagina, seleziona l'elenco a discesa **Cambia carico di lavoro**.
3. Seleziona il carico di lavoro a cui vuoi passare.



La pagina si aggiorna e mostra il carico di lavoro selezionato nell'interfaccia utente appropriata.

Configurare le impostazioni BlueXP backup and recovery

Dopo aver configurato BlueXP, configura le impostazioni di backup e ripristino, che includono l'aggiunta di credenziali per le risorse host, l'importazione delle risorse SnapCenter , la configurazione delle directory di log e la configurazione delle impostazioni VMware vCenter. È consigliabile eseguire queste operazioni prima di avviare attivamente il backup e il ripristino dei dati.

- Aggiungere credenziali per le risorse host per gli host Windows e SQL Server importati da SnapCenter e aggiungere le credenziali. (Solo carichi di lavoro Microsoft SQL Server)
- Mantenere le impostazioni di VMware vCenter.

- Importa e gestisci le risorse host SnapCenter. (Solo carichi di lavoro di Microsoft SQL Server)
- Configurare le directory di registro negli snapshot per gli host Windows.

Ruolo BlueXP obbligatorio Super amministratore di Backup e Ripristino, amministratore di backup di Backup e Ripristino, amministratore di ripristino di Backup e Ripristino. Scopri di più su "Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Aggiungere credenziali per le risorse host

Aggiungi le credenziali per le risorse host che desideri importare da SnapCenter. Le credenziali host vengono utilizzate per rilevare nuovi carichi di lavoro e applicare policy di backup.

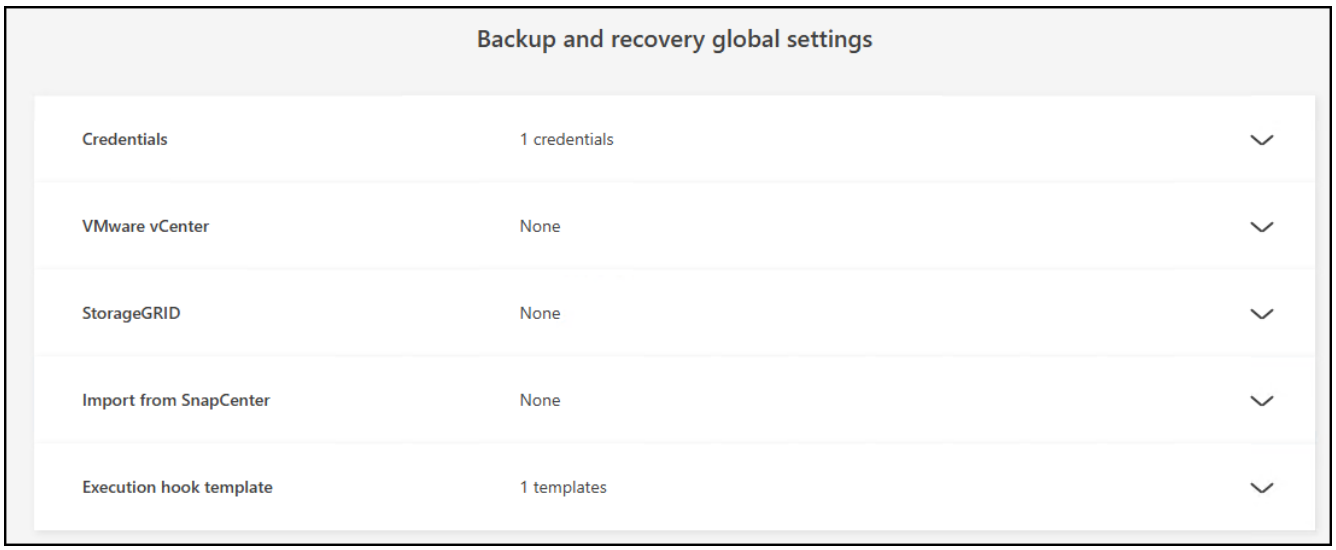
Se non disponi già delle credenziali, puoi crearle. Queste credenziali devono disporre delle autorizzazioni necessarie per accedere e gestire i carichi di lavoro dell'host.

È necessario configurare i seguenti tipi di credenziali:

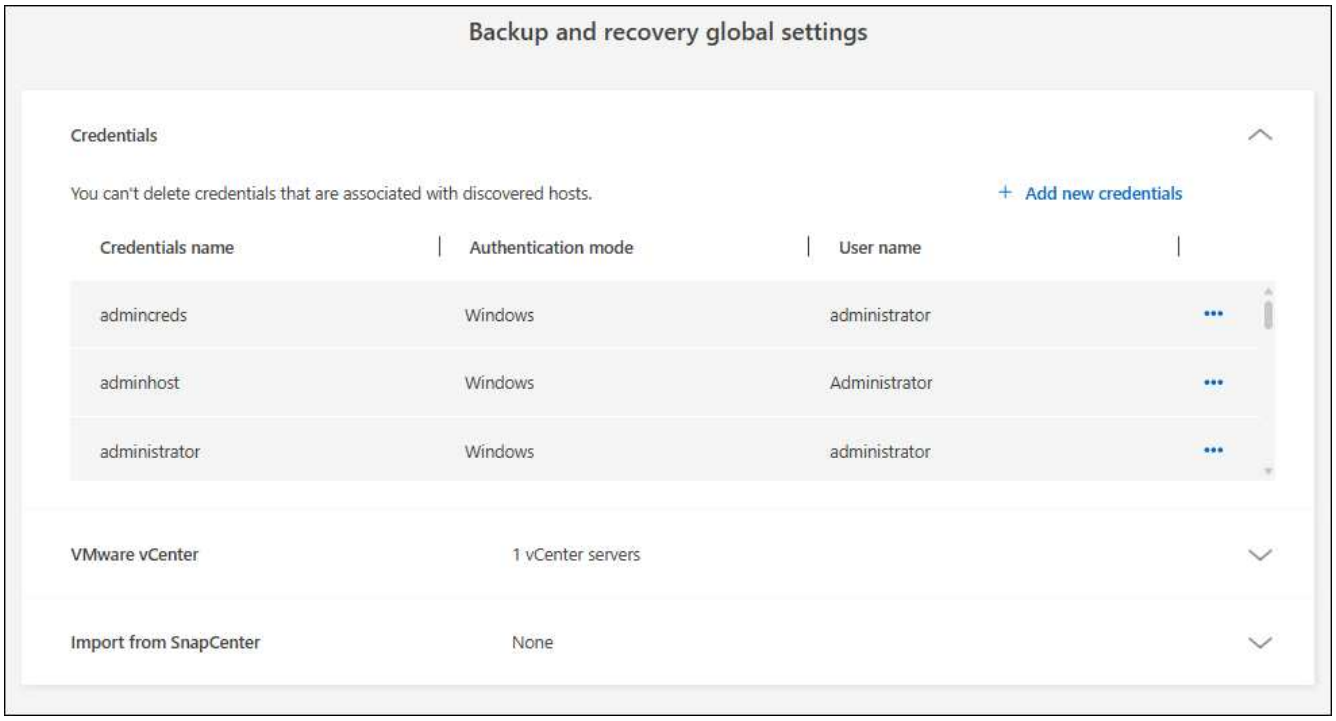
- Credenziali di Microsoft SQL Server
- Credenziali host Windows SnapCenter

Fasi

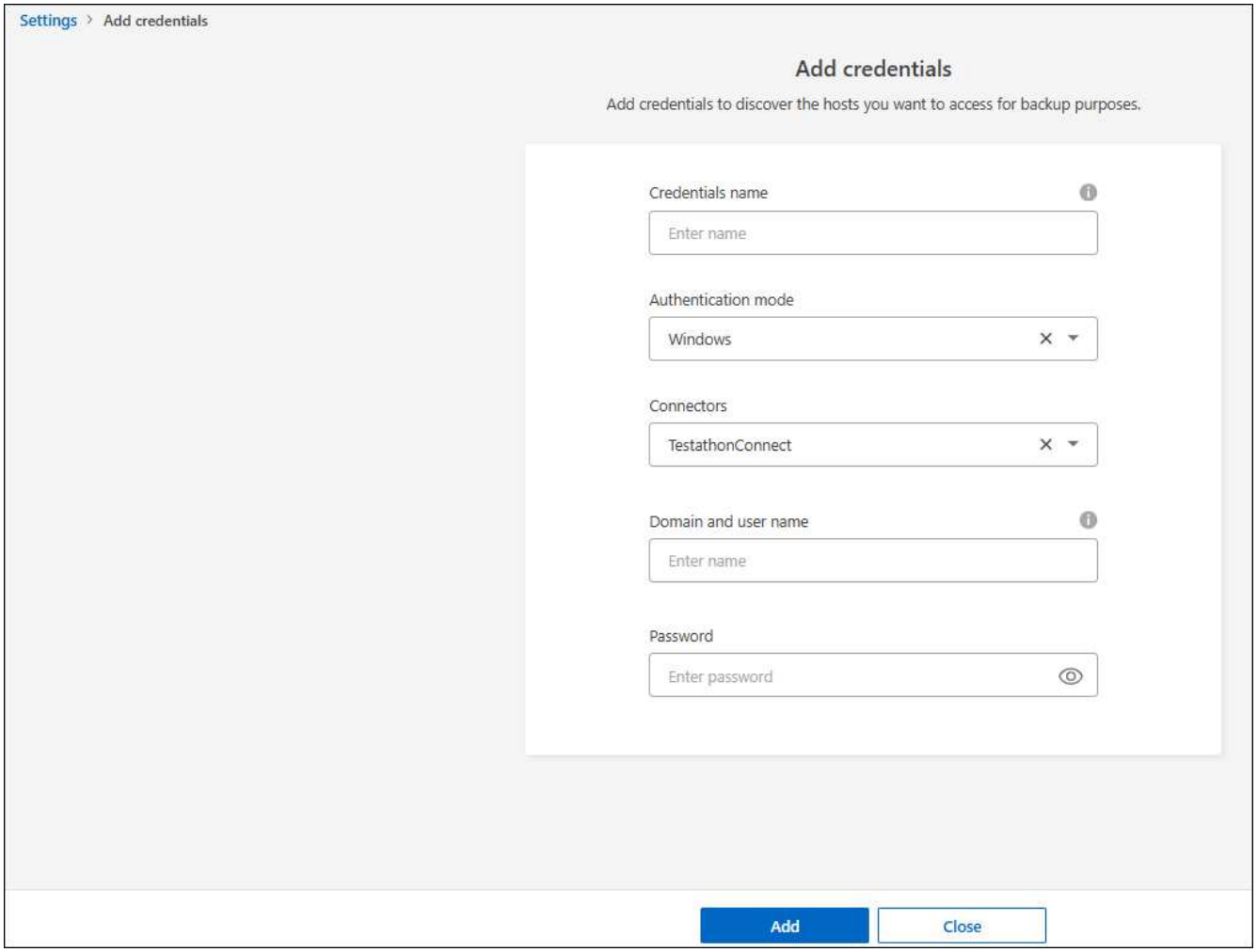
1. Dal menu BlueXP backup and recovery , seleziona **Impostazioni**.



2. Selezionare la freccia rivolta verso il basso per **Credenziali**.



3. Seleziona **Aggiungi nuove credenziali**.



4. Inserisci le informazioni per le credenziali. A seconda della modalità di autenticazione selezionata, vengono visualizzati campi diversi. Seleziona Informazioni **i** per ulteriori informazioni sui campi.
   - **Nome credenziali**: Inserisci un nome per le credenziali.
   - **Modalità di autenticazione**: selezionare **Windows** o **Microsoft SQL**.

   È necessario immettere le credenziali sia per Windows che per Microsoft SQL Server, quindi sarà necessario aggiungere due set di credenziali.

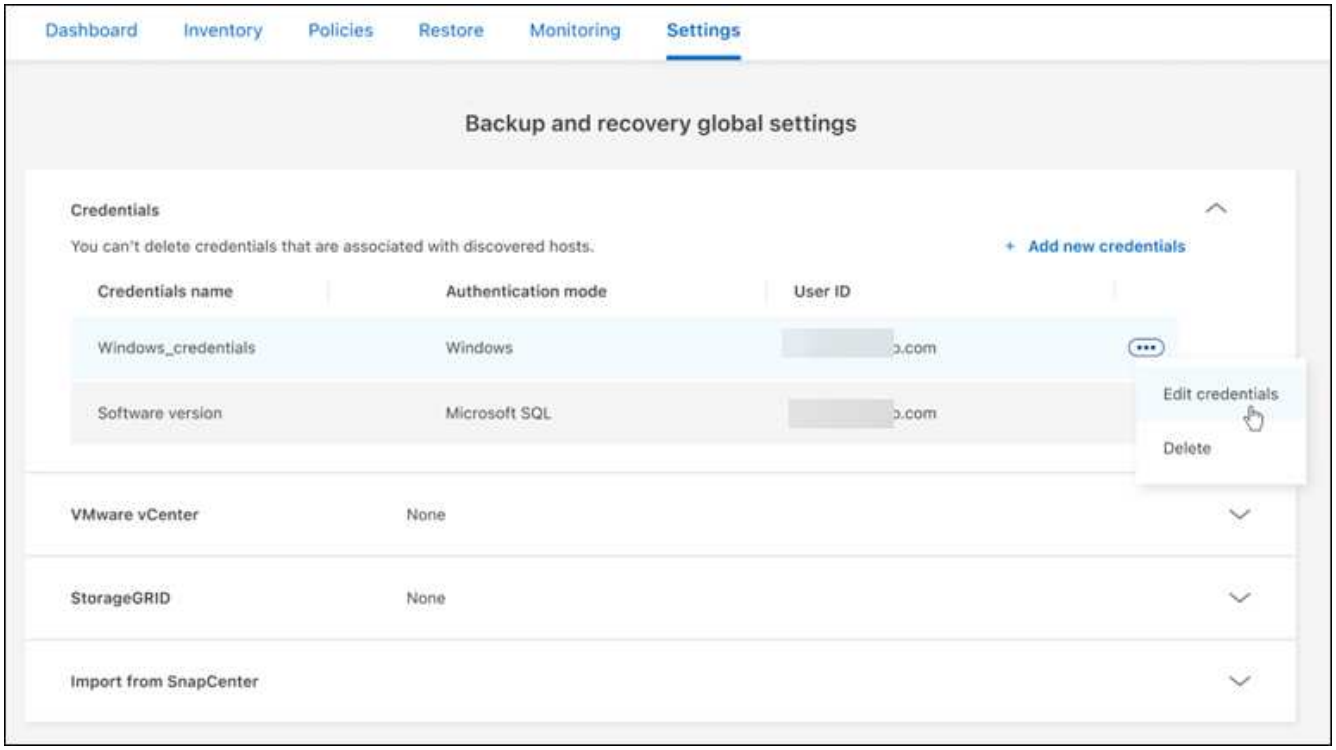
5. Se hai selezionato **Windows**:
   - **Connettore**: immettere l'indirizzo IP del connettore BlueXP .
   - **Dominio e nome utente**: immettere il NetBIOS o il nome FQDN del dominio e il nome utente per le credenziali.
   - **Password**: Inserisci la password per le credenziali.
6. Se hai selezionato **Microsoft SQL**:
   - **Host**: seleziona un indirizzo host di SQL Server scoperto.
   - **Istanza di SQL Server**: seleziona un'istanza di SQL Server individuata.
7. Selezionare **Aggiungi**.

Modifica le credenziali per le risorse host

Successivamente potrai modificare la password per le risorse host importate da SnapCenter.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per espandere la sezione **Credenziali**.



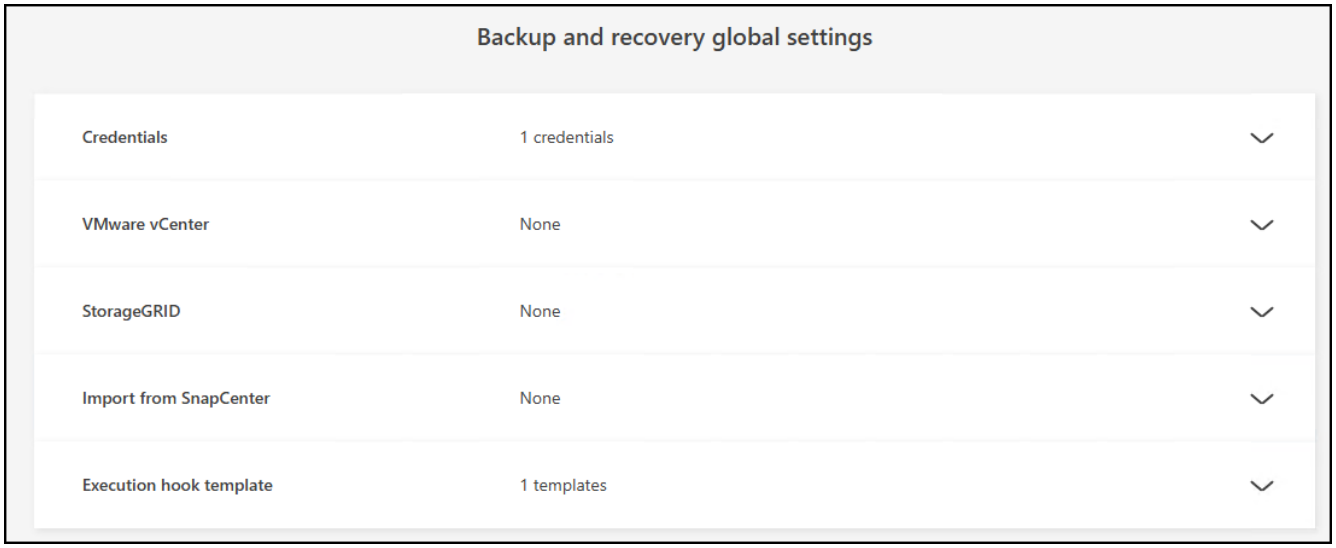
3. Seleziona l'icona Azioni ••• > **Modifica credenziali**.
    - **Password**: Inserisci la password per le credenziali.
4. Selezionare **Salva**.

Mantenere le impostazioni di VMware vCenter

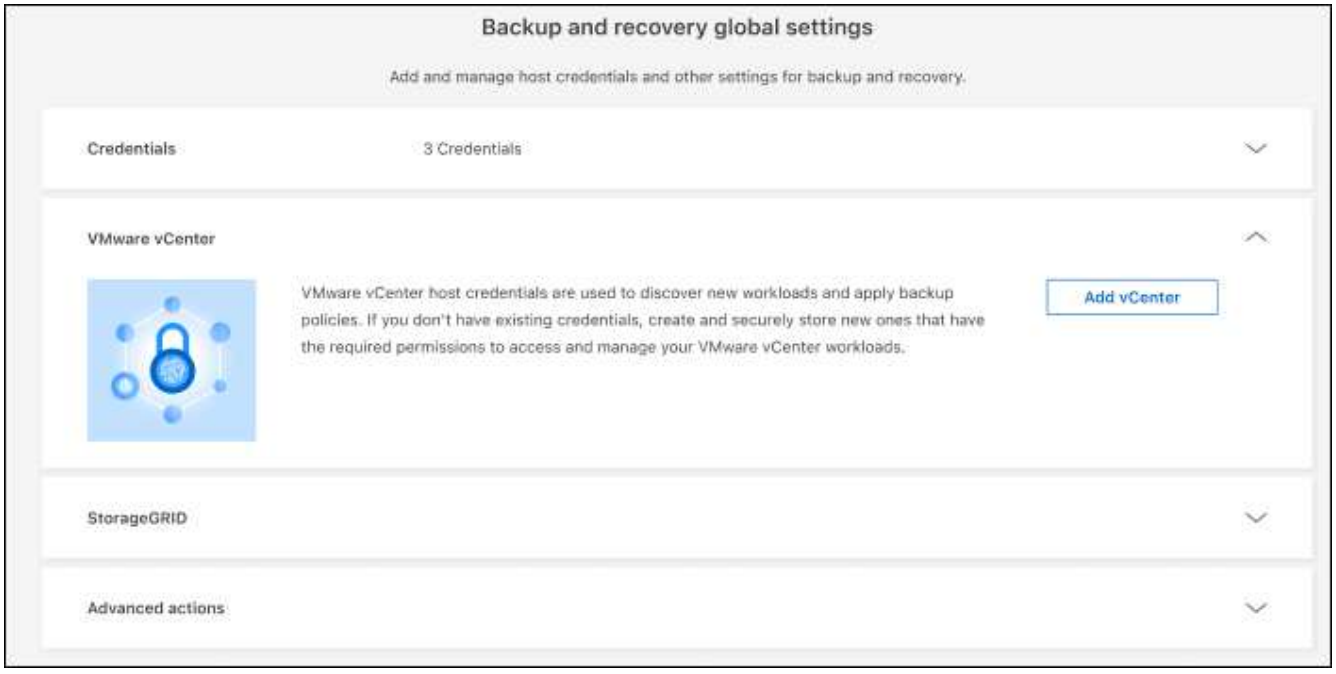
Fornisci le credenziali VMware vCenter per individuare i carichi di lavoro VMware vCenter Server di cui desideri eseguire il backup. Se non disponi di credenziali esistenti, puoi crearle con le autorizzazioni necessarie per accedere e gestire i carichi di lavoro VMware vCenter Server.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Impostazioni**.



2. Selezionare la freccia rivolta verso il basso per espandere la sezione **VMware vCenter**.



3. Selezionare **Aggiungi vCenter**.

4. Immettere le informazioni sul VMware vCenter Server.
   - **FQDN o indirizzo IP vCenter**: immettere un nome FQDN o l'indirizzo IP per VMware vCenter Server.
   - **Nome utente** e **Password**: immettere il nome utente e la password per VMware vCenter Server.
   - **Porta**: immettere il numero di porta per VMware vCenter Server.
   - **Protocollo**: Selezionare **HTTP** o **HTTPS**.
5. Selezionare **Aggiungi**.

Importa e gestisci le risorse host SnapCenter

Se in precedenza hai utilizzato SnapCenter per il backup delle tue risorse, puoi importare e gestire tali risorse in BlueXP backup and recovery. Con questa opzione, puoi importare le informazioni del server SnapCenter per registrare più server SnapCenter e individuare i carichi di lavoro del database.

Si tratta di un processo in due parti:

- Importare l'applicazione SnapCenter Server e le risorse host
- Gestisci le risorse host SnapCenter selezionate

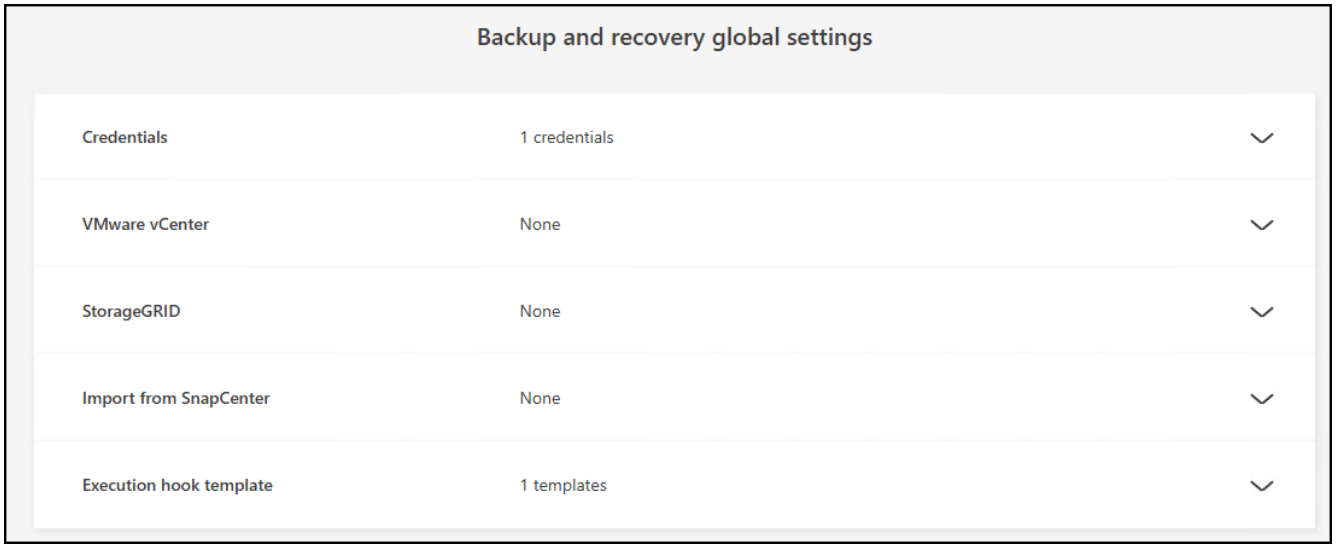
Importare l'applicazione SnapCenter Server e le risorse host

Questo primo passaggio importa le risorse host da SnapCenter e le visualizza nella pagina Inventario di BlueXP backup and recovery . A quel punto, le risorse non sono ancora gestite da BlueXP backup and recovery.

Dopo aver importato le risorse host SnapCenter , BlueXP backup and recovery non assume la gestione della protezione. Per farlo, è necessario selezionare esplicitamente la gestione di queste risorse in BlueXP backup and recovery.

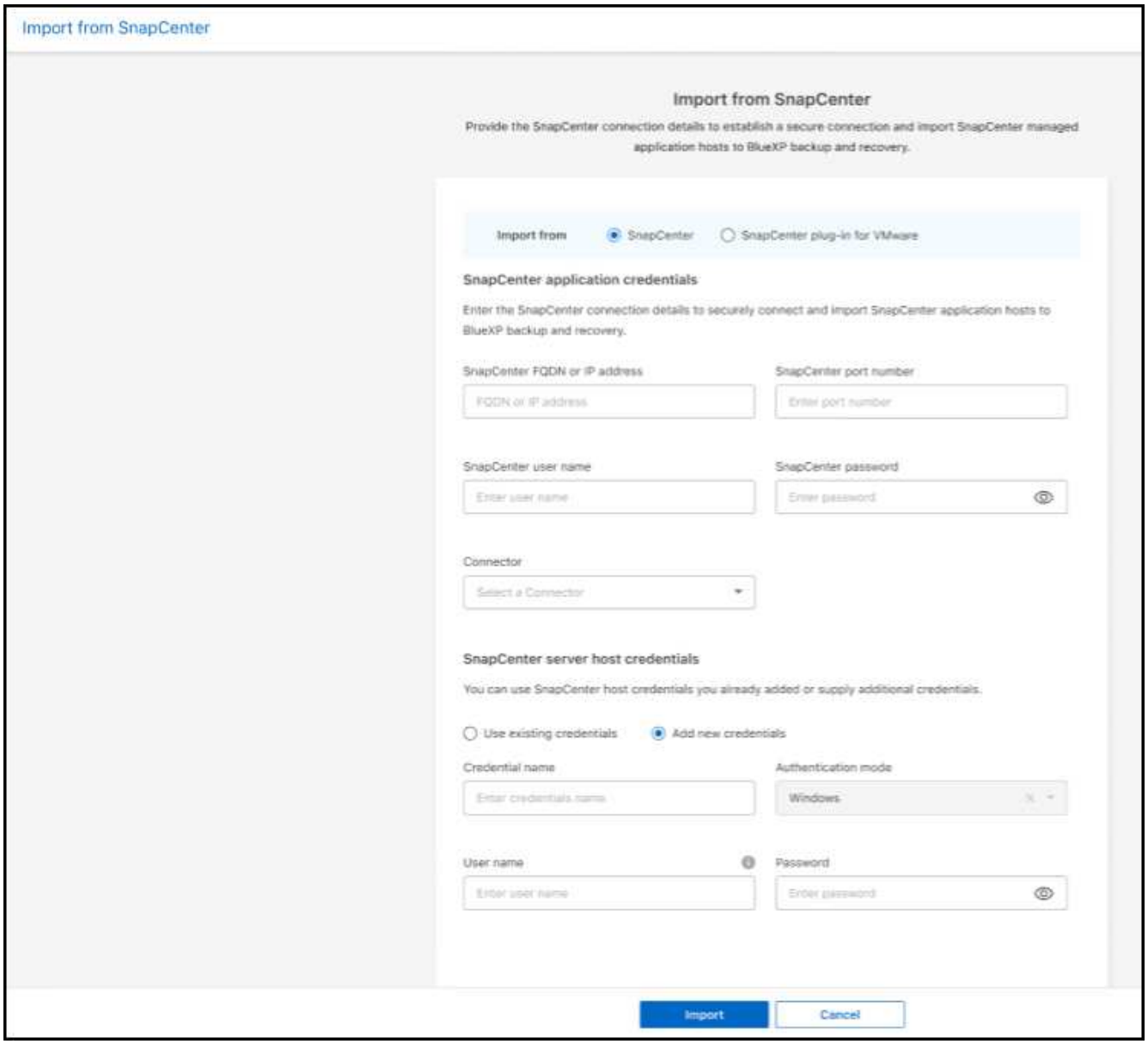
Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Impostazioni**.



2. Selezionare la freccia rivolta verso il basso per espandere la sezione **Importa da SnapCenter**.

3. Selezionare **Importa da SnapCenter** per importare le risorse SnapCenter .

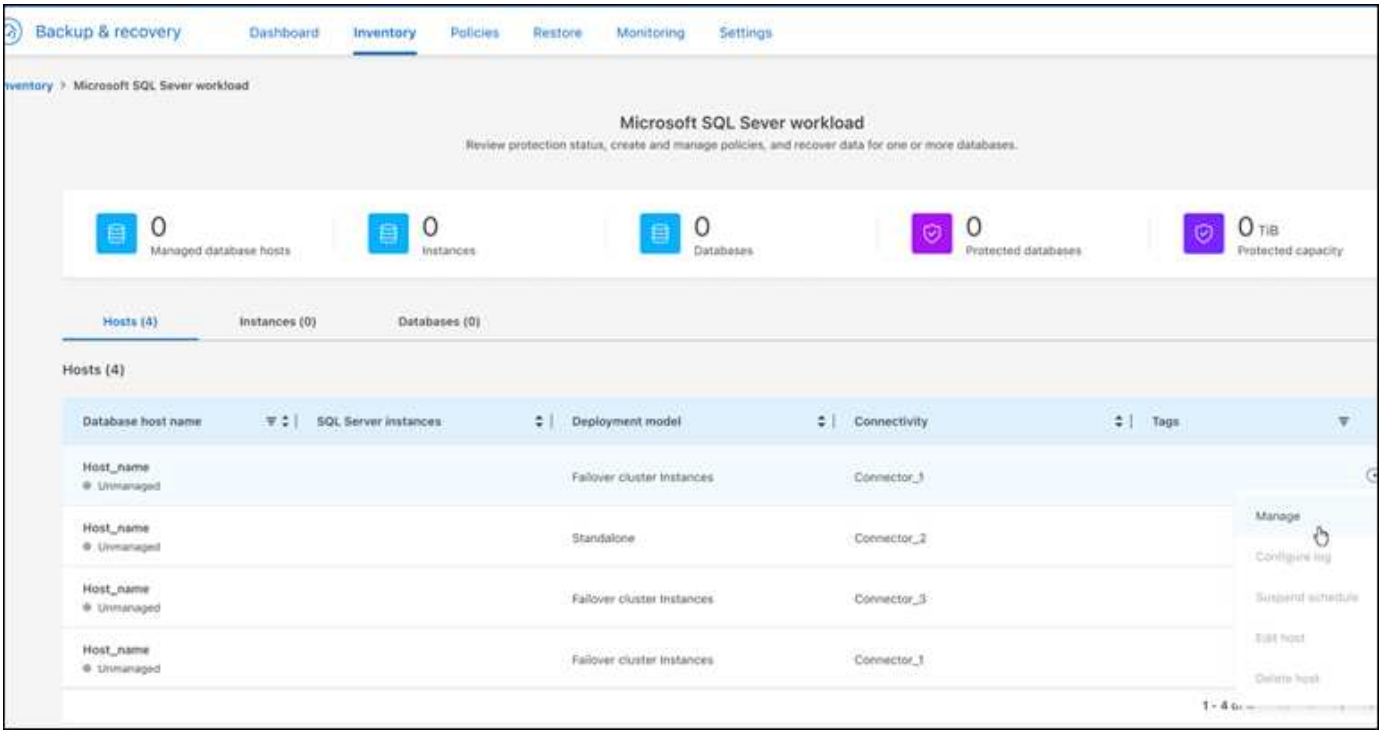


4. Inserisci * credenziali dell'applicazione SnapCenter *:
   a. * FQDN o indirizzo IP SnapCenter *: immettere l'FQDN o l'indirizzo IP dell'applicazione SnapCenter stessa.
   b. **Porta**: immettere il numero di porta per il server SnapCenter .
   c. **Nome utente** e **Password**: inserisci il nome utente e la password per SnapCenter Server.
   d. **Connettore**: seleziona il connettore BlueXP per SnapCenter.
5. Inserisci * credenziali host del server SnapCenter *:
   a. **Credenziali esistenti**: se selezioni questa opzione, puoi utilizzare le credenziali esistenti che hai già aggiunto. Inserisci il nome delle credenziali.
   b. **Aggiungi nuove credenziali**: se non disponi di credenziali host SnapCenter , puoi aggiungerne di nuove. Inserisci il nome delle credenziali, la modalità di autenticazione, il nome utente e la password.
6. Selezionare **Importa** per convalidare le voci e registrare SnapCenter Server.

Se SnapCenter Server è già registrato, è possibile aggiornare i dettagli di registrazione esistenti.

Risultato

La pagina Inventario mostra le risorse SnapCenter importate.

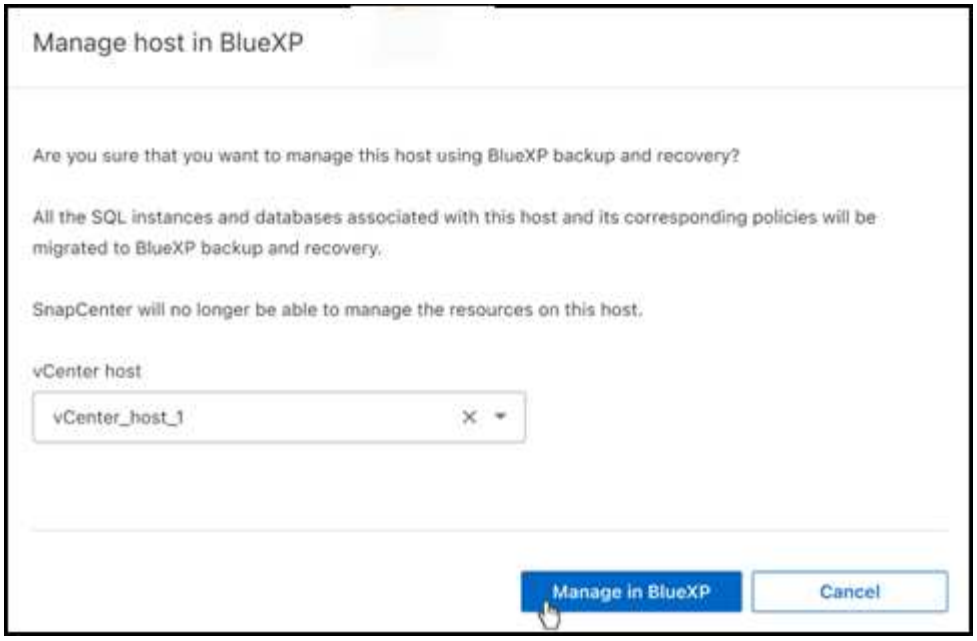


Gestire le risorse host SnapCenter

Dopo aver importato le risorse SnapCenter , gestisci tali risorse host in BlueXP backup and recovery. Dopo aver scelto di gestire le risorse importate, BlueXP backup and recovery può eseguire il backup e il ripristino delle risorse importate da SnapCenter. Non è più necessario gestire tali risorse in SnapCenter Server.

Fasi

1. Dopo aver importato le risorse SnapCenter , nella pagina Inventario visualizzata, seleziona le risorse SnapCenter importate che da ora in poi dovranno essere gestite BlueXP backup and recovery .
2. Seleziona l'icona Azioni ••• > **Gestisci** per gestire le risorse.



3. Selezionare **Gestisci in BlueXP**.

   Nella pagina Inventario viene visualizzato **Gestito** sotto il nome host per indicare che le risorse host selezionate sono ora gestite da BlueXP backup and recovery.

Modifica le risorse SnapCenter importate

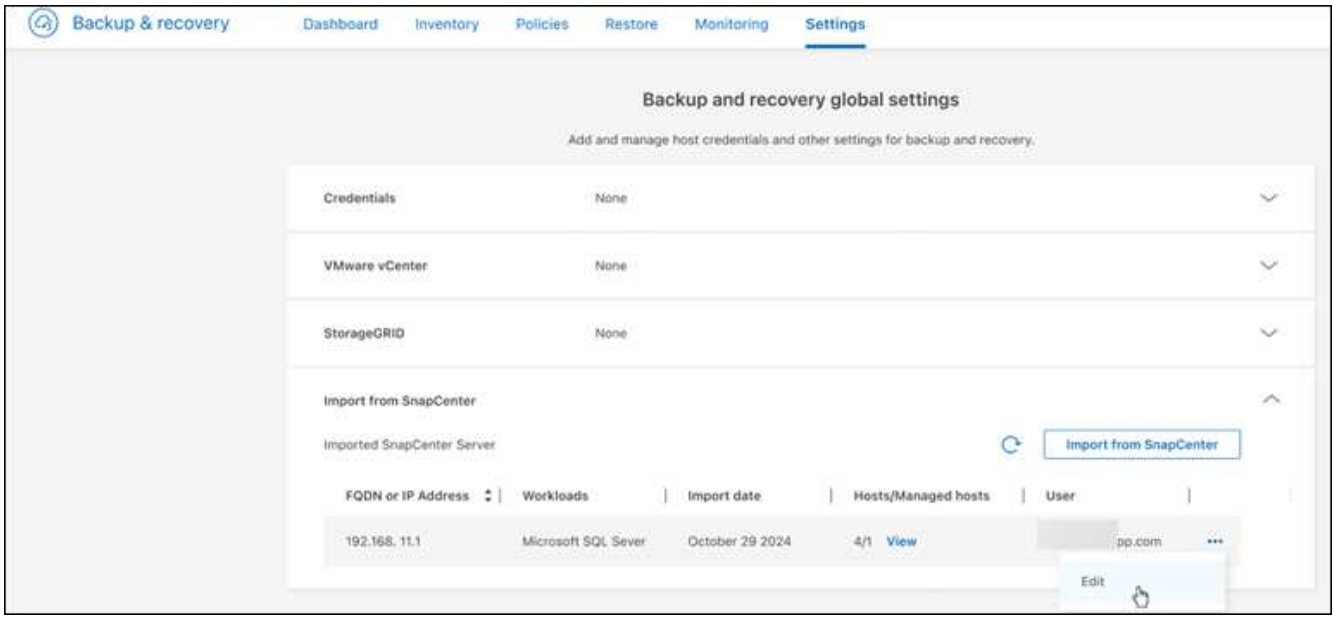
Successivamente potrai reimportare le risorse SnapCenter o modificare le risorse di SnapCenter importate per aggiornare i dettagli di registrazione.

È possibile modificare solo i dettagli della porta e della password per SnapCenter Server.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per **Importa da SnapCenter**.

   La pagina Importa da SnapCenter mostra tutte le importazioni precedenti.



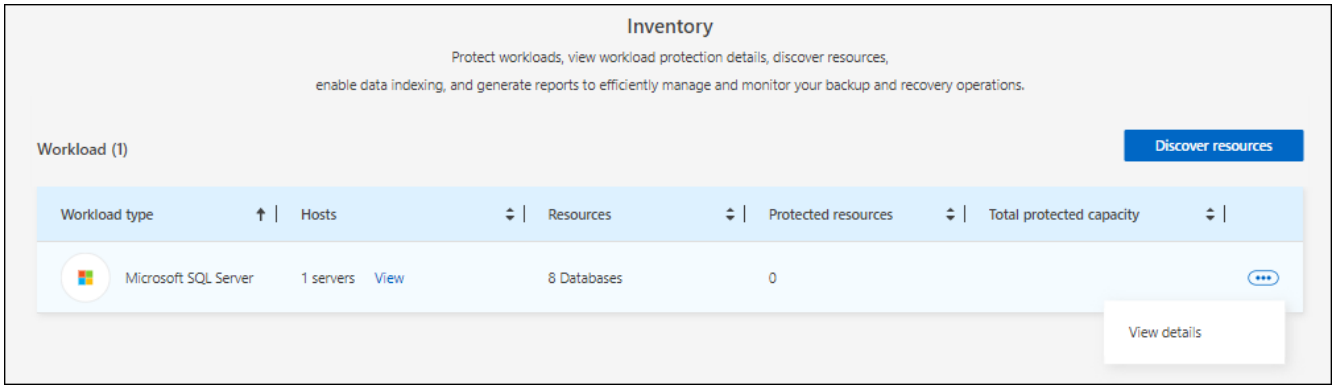
3. Seleziona l'icona Azioni ••• > **Modifica** per aggiornare le risorse.
4. Aggiornare la password e i dettagli della porta di SnapCenter , se necessario.
5. Selezionare **Importa**.

Configurare le directory di registro negli snapshot per gli host Windows

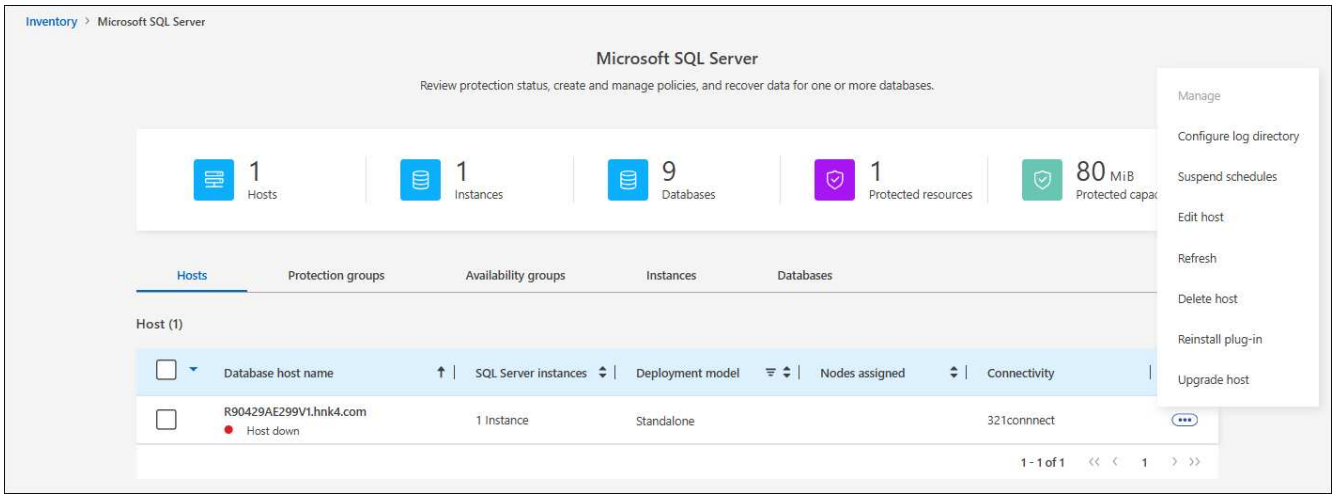
Prima di creare policy per gli host Windows, è necessario configurare le directory di log negli snapshot per gli host Windows. Le directory di log vengono utilizzate per archiviare i log generati durante il processo di backup.

Fasi

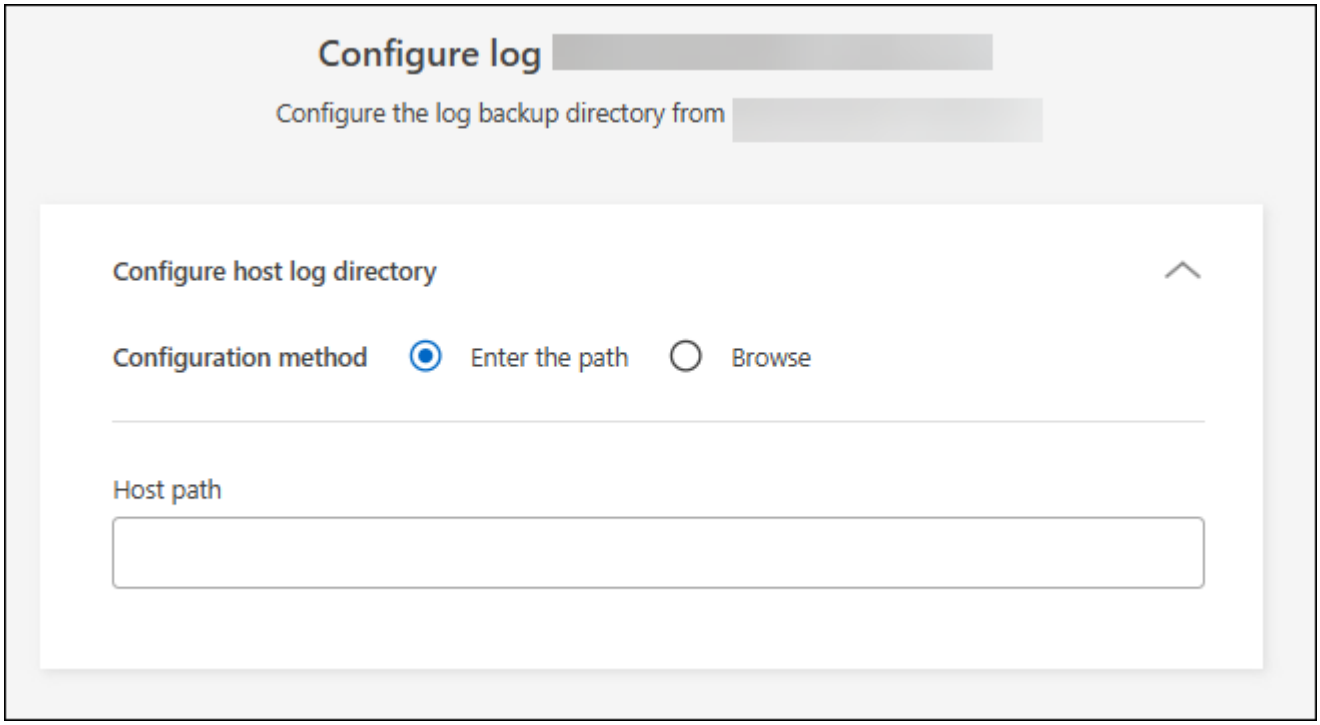
1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Dalla pagina Inventario, seleziona un carico di lavoro e quindi seleziona l'icona Azioni ••• > **Visualizza dettagli** per visualizzare i dettagli del carico di lavoro.
3. Dalla pagina dei dettagli dell'inventario che mostra Microsoft SQL Server, selezionare la scheda Host.



4. Dalla pagina dei dettagli dell'inventario, seleziona un host e seleziona l'icona Azioni ••• > **Configura directory registro**.



5. Sfogliare o immettere il percorso della directory del registro.
6. Selezionare **Salva**.

Utilizza il BlueXP backup and recovery

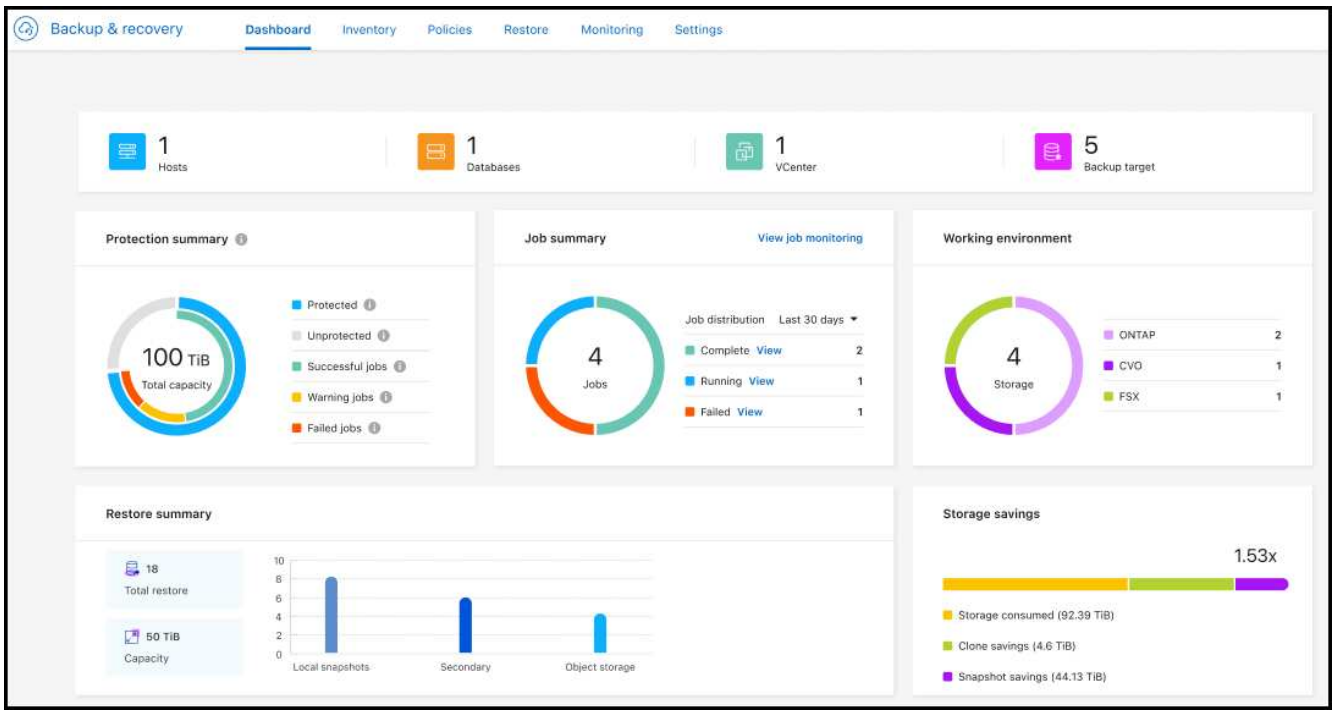
Visualizza lo stato di protezione sulla dashboard BlueXP backup and recovery

Monitorare lo stato dei carichi di lavoro ti consente di essere a conoscenza di eventuali problemi di protezione e di adottare le misure necessarie per risolverli. Visualizza lo stato dei backup e dei ripristini nella dashboard BlueXP backup and recovery . Puoi consultare il riepilogo di sistema, il riepilogo della protezione, il riepilogo dei processi, il riepilogo del ripristino e altro ancora.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di Backup e ripristino, Amministratore di backup di Backup e ripristino, Amministratore di ripristino di Backup e ripristino, Amministratore di clonazione di Backup e ripristino o Ruolo di visualizzatore di Backup e ripristino. Scopri di più su "Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Dashboard**.



Visualizza il riepilogo generale del sistema

Il riepilogo del sistema fornisce le seguenti informazioni:

- Numero di host o VM scoperti
- Numero di cluster Kubernetes scoperti
- Numero di destinazioni di backup su storage di oggetti

- Numero di vCenter
- Numero di cluster di storage in ONTAP

Visualizza il riepilogo della protezione

Esaminare le seguenti informazioni nel Riepilogo della protezione:

- Numero totale di database, VM e datastore protetti e non protetti.

  Un database protetto è un database a cui è assegnata una policy di backup. Un database non protetto è un database a cui non è assegnata una policy di backup.

- Numero di backup riusciti, con avviso o non riusciti.
- Capacità totale rilevata dal servizio di backup e capacità protetta rispetto a quella non protetta. Passa il mouse sull'icona "**i**" per visualizzare i dettagli.

Visualizza il riepilogo del lavoro

Rivedi il totale dei lavori completati, in esecuzione o non riusciti nel Riepilogo lavori.

Fasi

1. Per ogni distribuzione dei lavori, modifica un filtro per visualizzare il riepilogo di quelli non riusciti, in esecuzione e completati in base al numero di giorni, ad esempio gli ultimi 30 giorni, gli ultimi 7 giorni, le ultime 24 ore o l'ultimo anno.
2. Visualizza i dettagli dei lavori non riusciti, in esecuzione e completati selezionando **Visualizza monitoraggio lavori**.

Visualizza il riepilogo del ripristino

Esaminare le seguenti informazioni nel riepilogo del ripristino:

- Numero totale di processi di ripristino eseguiti
- La quantità totale di capacità che è stata ripristinata
- Numero di processi di ripristino eseguiti su storage locale, secondario e object storage. Passa il mouse sul grafico per visualizzare i dettagli.

Crea e gestisci policy per governare i backup nel BlueXP backup and recovery

Nel BlueXP backup and recovery, puoi creare criteri personalizzati che stabiliscono la frequenza del backup, l'ora in cui viene eseguito e il numero di file di backup conservati.

Alcune di queste opzioni e sezioni di configurazione non sono disponibili per tutti i carichi di lavoro.

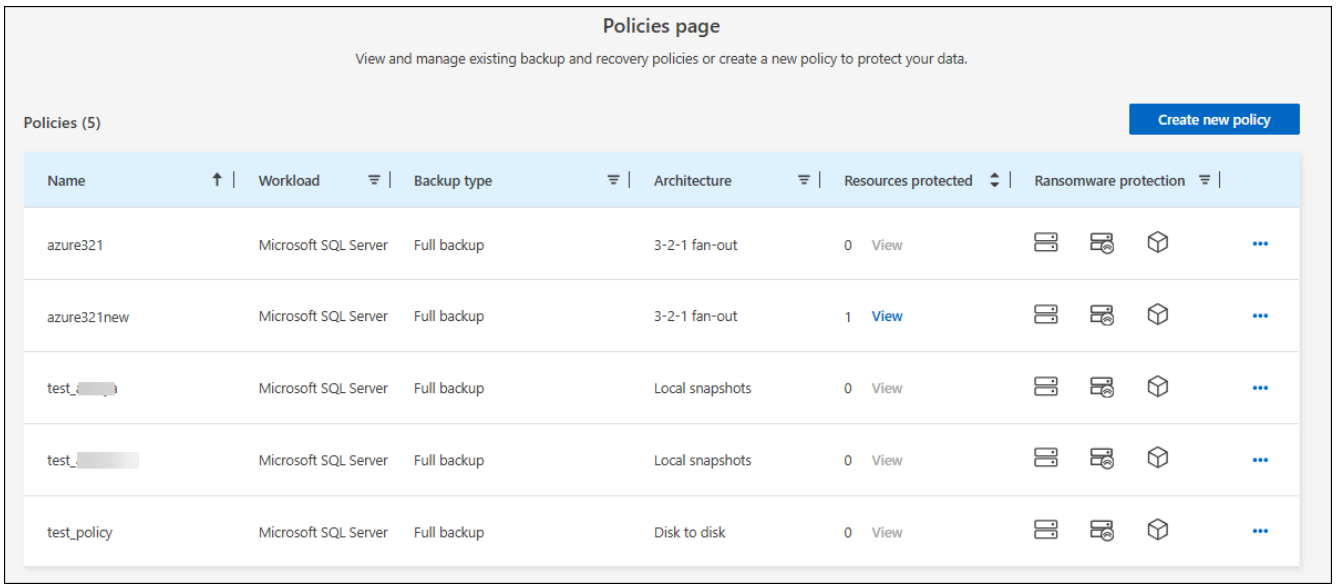
Se si importano risorse da SnapCenter, potrebbero verificarsi alcune differenze tra i criteri utilizzati in SnapCenter e quelli utilizzati nel BlueXP backup and recovery. Vedere "Differenze di policy tra backup e ripristino SnapCenter e BlueXP backup and recovery".

È possibile raggiungere i seguenti obiettivi relativi alle politiche:

- Creare un criterio di snapshot locale
- Creare una policy per la replica su storage secondario
- Creare una policy per le impostazioni di archiviazione degli oggetti
- Configurare le impostazioni avanzate dei criteri
- Modifica policy (non disponibile per i carichi di lavoro VMware Preview)
- Eliminare i criteri

Visualizzare le policy

1. Dal menu BlueXP backup and recovery , seleziona **Criteri**.



2. Esaminare i dettagli di questa politica.
   - **Carico di lavoro**: alcuni esempi includono Microsoft SQL Server, Volumes, VMware o Kubernetes.
   - **Tipo di backup**: alcuni esempi sono il backup completo e il backup del registro.
   - **Architettura**: Alcuni esempi sono snapshot locale, fan-out, cascading, disco su disco e disco su archivio oggetti.
   - **Risorse protette**: mostra quante risorse sul totale delle risorse presenti su quel carico di lavoro sono protette.
   - **Protezione ransomware**: indica se la policy include il blocco degli snapshot sullo snapshot locale, il blocco degli snapshot sull'archiviazione secondaria o il blocco DataLock sull'archiviazione degli oggetti.

Creare un criterio

È possibile creare policy che gestiscano gli snapshot locali, le repliche su storage secondario e i backup su storage a oggetti. Parte della strategia 3-2-1 prevede la creazione di una copia snapshot delle istanze o dei database di Microsoft SQL Server sul sistema di storage **primario**.

Ruolo BlueXP richiesto Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di Backup e ripristino, Amministratore di backup di Backup e ripristino. Scopri di più su "Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Prima di iniziare

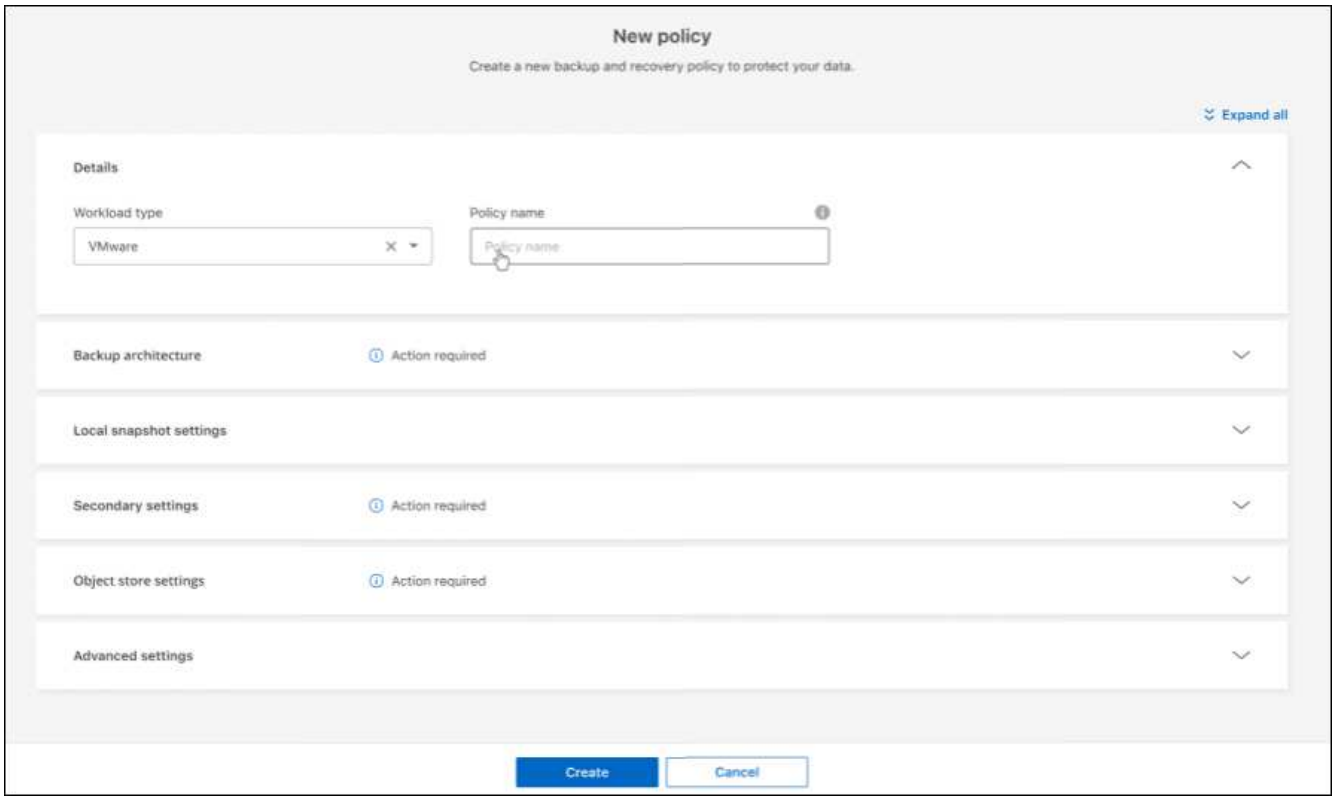
Se si prevede di replicare su storage secondario e si desidera utilizzare il blocco degli snapshot su snapshot locali o su storage secondario ONTAP remoto, è necessario innanzitutto inizializzare il clock di conformità ONTAP a livello di cluster. Questo è un requisito per abilitare il blocco degli snapshot nella policy.

Per istruzioni su come farlo, fare riferimento a "Inizializza l'orologio di conformità in ONTAP" .

Per informazioni generali sul blocco degli snapshot, fare riferimento a "Blocco degli snapshot in ONTAP" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Criteri**.
2. Dalla pagina Criteri, seleziona **Crea nuovo criterio**.



3. Nella pagina Criteri, fornire le seguenti informazioni.
   - Sezione **Dettagli**:
     - Tipo di carico di lavoro: selezionare "Microsoft SQL Server", VMware o Kubernetes.
     - Inserisci un nome per la policy.

       Per un elenco dei personaggi da evitare, vedere il suggerimento.
   - Sezione **Architettura di backup**: selezionare la freccia rivolta verso il basso e scegliere l'architettura per il backup, ad esempio fan-out, a cascata e da disco a disco.
     - **Snapshot locale**: snapshot locale sul volume selezionato (Microsoft SQL Server). Gli snapshot locali sono una componente fondamentale delle strategie di protezione dei dati, poiché catturano lo stato dei dati in momenti specifici. In questo modo vengono create copie di sola lettura e in un dato momento dei volumi di produzione in cui vengono eseguiti i carichi di lavoro. Lo snapshot consuma

uno spazio di archiviazione minimo e comporta un sovraccarico di prestazioni trascurabile perché registra solo le modifiche apportate ai file dall'ultimo snapshot. È possibile utilizzare snapshot locali per ripristinare dati persi o danneggiati, nonché per creare backup per scopi di disaster recovery.

Per i carichi di lavoro VMware, questa operazione configura lo snapshot locale sui datastore o VMware sul sistema di storage primario.

- **Fanout 3-2-1**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco) a cloud (archivio oggetti). Crea più copie di dati su diversi sistemi di archiviazione, ad esempio configurazioni ONTAP su ONTAP e ONTAP su object-store. Può trattarsi di un archivio di oggetti cloud hyperscaler o di un archivio di oggetti privato: StorageGRID. Queste configurazioni aiutano a ottenere una protezione ottimale dei dati e un ripristino in caso di emergenza.

  Questa opzione non è disponibile per Amazon FSx for NetApp ONTAP.

  Per i carichi di lavoro VMware, questa funzionalità non è disponibile nell'anteprima di VMware.

  Per i carichi di lavoro VMware, questa operazione configura lo snapshot locale sui datastore o sulle VM sul primario e lo replica dall'archiviazione su disco primaria all'archiviazione su disco secondaria, nonché dallo storage primario allo storage di oggetti cloud.

- **3-2-1 a cascata**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco) e da storage primario (disco) a storage cloud (archivio oggetti). Può trattarsi di un archivio di oggetti cloud hyperscaler o di un archivio di oggetti privato: StorageGRID. Ciò crea una catena di replicazione dei dati su più sistemi per garantire ridondanza e affidabilità.

  Questa opzione non è disponibile per Amazon FSx for NetApp ONTAP.

Per i carichi di lavoro VMware, questo configura lo snapshot locale sui datastore o sulle VM sullo storage primario e una cascata dallo storage su disco primario allo storage su disco secondario e quindi allo storage di oggetti cloud.

- **Da disco a disco**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco). La strategia di protezione dei dati ONTAP - ONTAP replica i dati tra due sistemi ONTAP per garantire elevata disponibilità e ripristino in caso di emergenza. In genere, questo risultato viene ottenuto utilizzando SnapMirror, che supporta sia la replica sincrona che quella asincrona. Questo metodo garantisce che i tuoi dati siano costantemente aggiornati e disponibili in più posizioni, offrendo una solida protezione contro la perdita di dati.

  Per i carichi di lavoro VMware, questa operazione configura lo snapshot locale sui datastore o VMware sul sistema di storage primario e quindi replica i dati dal sistema di storage su disco primario al sistema di storage su disco secondario.

- **Archiviazione da disco a oggetto**: archiviazione primaria (disco) nel cloud (archivio oggetti). In questo modo, i dati vengono replicati da un sistema ONTAP a un sistema di archiviazione oggetti, come AWS S3, Azure Blob Storage o StorageGRID. Questo risultato viene in genere ottenuto utilizzando SnapMirror Cloud, che fornisce backup incrementali permanenti trasferendo solo i blocchi di dati modificati dopo il trasferimento di base iniziale. Può trattarsi di un archivio oggetti hyperscaler cloud o di un archivio oggetti privato, StorageGRID. Questo metodo è ideale per la conservazione e l'archiviazione dei dati a lungo termine, offrendo una soluzione conveniente e scalabile per la protezione dei dati.

  Per i carichi di lavoro VMWare, questa opzione configura lo snapshot locale sui datastore o sulle

VM sul server primario e la replica dall'archiviazione su disco primario all'archiviazione di oggetti cloud.

- **Fanout da disco a disco**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco) e da storage primario (disco) a storage secondario (disco).

> ⓘ È possibile configurare più impostazioni secondarie per l'opzione fanout da disco a disco.

Per i carichi di lavoro VMware, questa operazione configura l'archiviazione su disco primaria in quella su disco secondaria e replica l'archiviazione su disco primaria in quella su disco secondaria.

Creare un criterio di snapshot locale

Fornire informazioni per lo snapshot locale.

- Seleziona l'opzione **Aggiungi pianificazione** per selezionare la pianificazione o le pianificazioni degli snapshot. Puoi avere un massimo di 5 pianificazioni.
- **Frequenza snapshot**: seleziona la frequenza oraria, giornaliera, settimanale, mensile o annuale. La frequenza annuale non è disponibile per i carichi di lavoro Kubernetes.
- **Conservazione degli snapshot**: inserisci il numero di snapshot da conservare.
- **Abilita backup del registro**: (si applica ai carichi di lavoro di Microsoft SQL Server. (Non disponibile per carichi di lavoro VMware o Kubernetes) Selezionare l'opzione per eseguire il backup dei log e impostare la frequenza e la conservazione dei backup dei log. Per fare ciò, è necessario aver già configurato un backup del registro. Vedere "Configurare le directory di registro" .
- **Provider**: (solo carichi di lavoro Kubernetes) Seleziona il provider di archiviazione che ospita le risorse dell'applicazione Kubernetes.
- **Destinazione di backup**: (solo carichi di lavoro Kubernetes) Seleziona il bucket di archiviazione che ospita le risorse dell'applicazione Kubernetes. Le definizioni delle risorse dell'applicazione al momento dello snapshot vengono archiviate in questo bucket. Assicurarsi che il bucket sia accessibile all'interno dell'ambiente di backup.
- Facoltativamente, seleziona **Avanzate** a destra della pianificazione per impostare l'etichetta SnapMirror e abilitare il blocco degli snapshot (non disponibile per i carichi di lavoro Kubernetes).
  - * Etichetta SnapMirror *: l'etichetta funge da marcatore per il trasferimento di uno snapshot specificato in base alle regole di conservazione della relazione. L'aggiunta di un'etichetta a uno snapshot lo contrassegna come destinazione per la replica SnapMirror .
  - **Offset da un'ora**: immettere il numero di minuti di offset dell'istantanea dall'inizio dell'ora. Ad esempio, se inserisci **15**, l'istantanea verrà scattata 15 minuti dopo l'ora. Disponibile solo per orari.
  - **Abilita ore silenziose**: seleziona se desideri abilitare le ore silenziose. Le ore di silenzio sono un periodo durante il quale non vengono acquisiti snapshot, consentendo così di effettuare operazioni di manutenzione o di altro tipo senza interferenze da parte dei processi di backup. Ciò è utile per ridurre il carico sul sistema durante i periodi di picco di utilizzo o le finestre di manutenzione. Disponibile solo per orari.
  - **Abilita blocco snapshot**: seleziona se desideri abilitare gli snapshot antimanomissione. Abilitando questa opzione si garantisce che gli snapshot non possano essere eliminati o modificati finché non sia scaduto il periodo di conservazione specificato. Questa funzionalità, che sfrutta la tecnologia SnapLock , è fondamentale per proteggere i dati dagli attacchi ransomware e garantirne l'integrità.
  - **Periodo di blocco dello snapshot**: immetti il numero di giorni, mesi o anni per cui desideri bloccare lo snapshot.

Creare una policy per le impostazioni secondarie (replica su storage secondario)

Fornire informazioni per la replicazione su storage secondario. Le informazioni sulla pianificazione delle impostazioni degli snapshot locali vengono visualizzate nelle impostazioni secondarie. Queste impostazioni non sono disponibili per i carichi di lavoro Kubernetes.

- **Backup**: seleziona la frequenza tra oraria, giornaliera, settimanale, mensile o annuale.
- **Destinazione del backup**: seleziona il sistema di destinazione sull'archiviazione secondaria per il backup.
- **Conservazione**: inserisci il numero di snapshot da conservare.
- **Abilita blocco snapshot**: seleziona se desideri abilitare gli snapshot antimanomissione.
- **Periodo di blocco dello snapshot**: immetti il numero di giorni, mesi o anni per cui desideri bloccare lo snapshot.
- **Trasferimento alla secondaria**:
  - L'opzione **Pianificazione del trasferimento ONTAP - Inline** è selezionata per impostazione predefinita e indica che gli snapshot vengono trasferiti immediatamente al sistema di storage secondario. Non è necessario pianificare il backup.
  - Altre opzioni: se si sceglie un trasferimento differito, i trasferimenti non saranno immediati e sarà possibile impostare una pianificazione.
- * Relazione secondaria SMAS tra SnapMirror e SnapVault *: utilizzare le relazioni secondarie SMAS tra SnapMirror e SnapVault per i carichi di lavoro di SQL Server.

Creare una policy per le impostazioni di archiviazione degli oggetti

Fornisci informazioni per il backup nell'archiviazione degli oggetti. Queste impostazioni sono chiamate "Impostazioni di backup" per i carichi di lavoro Kubernetes.

I campi visualizzati variano a seconda del provider e dell'architettura selezionati.

Creare una policy per l'archiviazione degli oggetti AWS

Inserisci le informazioni in questi campi:

- **Provider**: seleziona **AWS**.
- **Account AWS**: seleziona l'account AWS.
- **Destinazione di backup**: seleziona una destinazione di archiviazione di oggetti S3 registrata. Assicurati che la destinazione sia accessibile all'interno del tuo ambiente di backup.
- **Spazio IP**: Seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa opzione è utile se si dispone di più spazi IP e si desidera controllare quale utilizzare per i backup.
- **Impostazioni di pianificazione**: seleziona la pianificazione impostata per gli snapshot locali. Puoi rimuovere una pianificazione, ma non aggiungerne una, perché le pianificazioni sono impostate in base alle pianificazioni degli snapshot locali.
- **Copie di conservazione**: immettere il numero di snapshot da conservare.
- **Esegui a**: seleziona la pianificazione del trasferimento ONTAP per eseguire il backup dei dati nell'archivio oggetti.
- **Suddividi i backup in livelli dall'archivio oggetti allo storage di archiviazione**: se scegli di suddividere i backup in livelli per lo storage di archiviazione (ad esempio, AWS Glacier), seleziona l'opzione del livello e il numero di giorni di archiviazione.

- **Abilita scansione integrità**: (Non disponibile per i carichi di lavoro Kubernetes) Seleziona se desideri abilitare le scansioni di integrità (blocco degli snapshot) sull'archiviazione degli oggetti. Ciò garantisce che i backup siano validi e possano essere ripristinati correttamente. La frequenza di scansione dell'integrità è impostata su 7 giorni per impostazione predefinita. Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Scansione integrità**. La scansione viene eseguita solo sullo snapshot più recente. Puoi abilitare o disabilitare le scansioni di integrità sullo snapshot più recente.

Creare una policy per l'archiviazione degli oggetti di Microsoft Azure

Inserisci le informazioni in questi campi:

- **Provider**: seleziona **Azure**.
- **Sottoscrizione di Azure**: seleziona la sottoscrizione di Azure tra quelle rilevate.
- **Gruppo di risorse di Azure**: seleziona il gruppo di risorse di Azure tra quelli individuati.
- **Destinazione di backup**: seleziona una destinazione di archiviazione di oggetti registrata. Assicurati che la destinazione sia accessibile all'interno del tuo ambiente di backup.
- **Spazio IP**: Seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa opzione è utile se si dispone di più spazi IP e si desidera controllare quale utilizzare per i backup.
- **Impostazioni di pianificazione**: seleziona la pianificazione impostata per gli snapshot locali. Puoi rimuovere una pianificazione, ma non aggiungerne una, perché le pianificazioni sono impostate in base alle pianificazioni degli snapshot locali.
- **Copie di conservazione**: immettere il numero di snapshot da conservare.
- **Esegui a**: seleziona la pianificazione del trasferimento ONTAP per eseguire il backup dei dati nell'archivio oggetti.
- **Suddividi i backup in livelli dall'archivio oggetti allo storage di archiviazione**: se scegli di suddividere i backup in livelli nello storage di archiviazione, seleziona l'opzione del livello e il numero di giorni di archiviazione.
- **Abilita scansione integrità**: (Non disponibile per i carichi di lavoro Kubernetes) Seleziona se desideri abilitare le scansioni di integrità (blocco degli snapshot) sull'archiviazione degli oggetti. Ciò garantisce che i backup siano validi e possano essere ripristinati correttamente. La frequenza di scansione dell'integrità è impostata su 7 giorni per impostazione predefinita. Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Scansione integrità**. La scansione viene eseguita solo sullo snapshot più recente. Puoi abilitare o disabilitare le scansioni di integrità sullo snapshot più recente.

Creare una policy per l'archiviazione degli oggetti StorageGRID

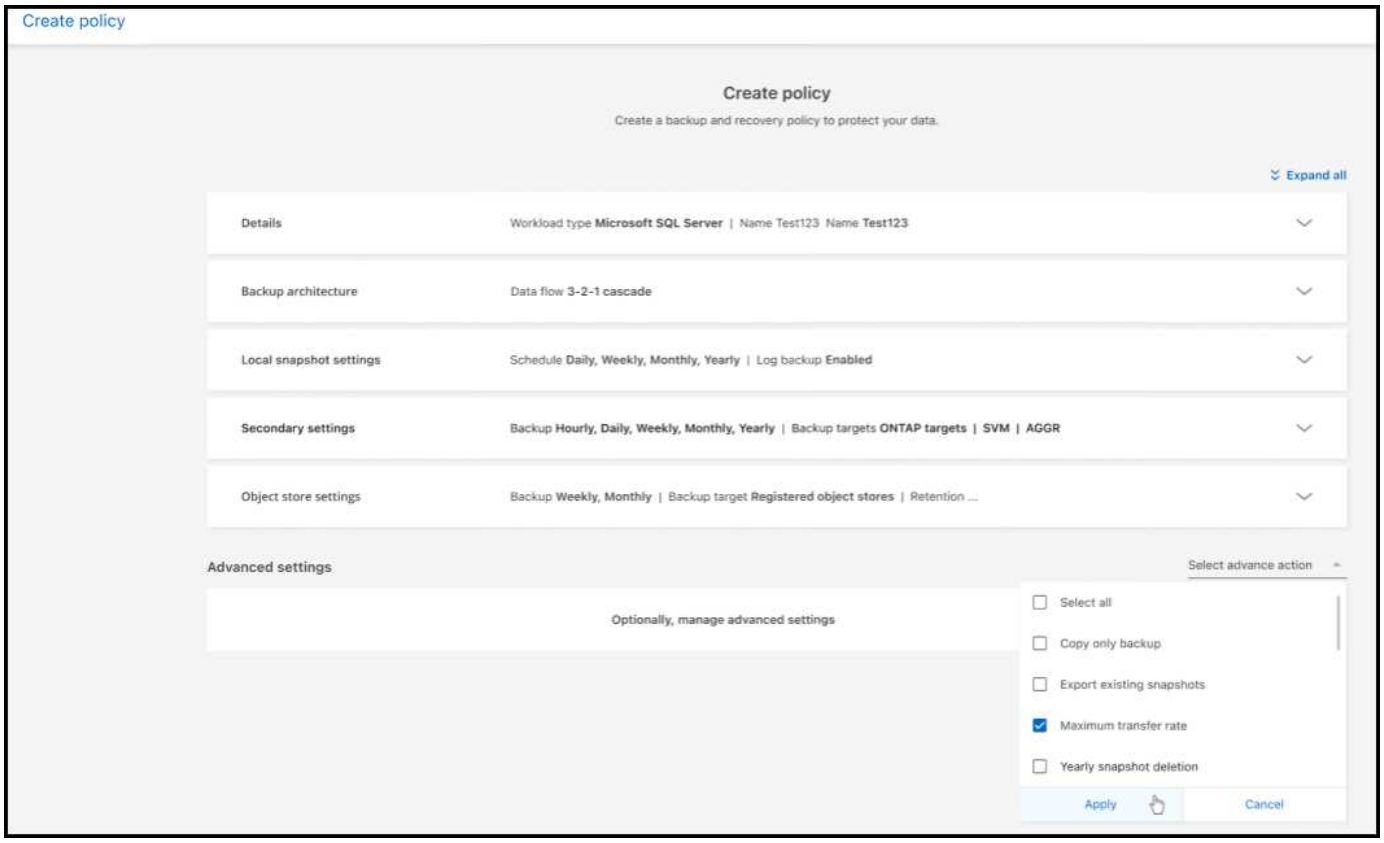
Inserisci le informazioni in questi campi:

- **Provider**: Selezionare **StorageGRID**.
- * Credenziali StorageGRID *: seleziona le credenziali StorageGRID tra quelle rilevate. Queste credenziali vengono utilizzate per accedere al sistema di archiviazione oggetti StorageGRID e sono state inserite nell'opzione Impostazioni.
- **Destinazione di backup**: seleziona una destinazione di archiviazione di oggetti S3 registrata. Assicurati che la destinazione sia accessibile all'interno del tuo ambiente di backup.
- **Spazio IP**: Seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa opzione è utile se si dispone di più spazi IP e si desidera controllare quale utilizzare per i backup.
- **Impostazioni di pianificazione**: seleziona la pianificazione impostata per gli snapshot locali. Puoi rimuovere una pianificazione, ma non aggiungerne una, perché le pianificazioni sono impostate in base alle pianificazioni degli snapshot locali.

- **Copie di conservazione**: immettere il numero di snapshot da conservare per ciascuna frequenza.
- **Pianificazione del trasferimento per l'archiviazione di oggetti**: (non disponibile per i carichi di lavoro Kubernetes) Scegli la pianificazione del trasferimento ONTAP per eseguire il backup dei dati nell'archiviazione di oggetti.
- **Abilita scansione integrità**: (Non disponibile per i carichi di lavoro Kubernetes) Seleziona se desideri abilitare le scansioni di integrità (blocco degli snapshot) sull'archiviazione degli oggetti. Ciò garantisce che i backup siano validi e possano essere ripristinati correttamente. La frequenza di scansione dell'integrità è impostata su 7 giorni per impostazione predefinita. Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Scansione integrità**. La scansione viene eseguita solo sullo snapshot più recente. Puoi abilitare o disabilitare le scansioni di integrità sullo snapshot più recente.
- **Suddividi i backup in livelli dall'archivio oggetti allo storage di archiviazione**: (non disponibile per i carichi di lavoro Kubernetes) Se scegli di suddividere i backup in livelli per lo storage di archiviazione, seleziona l'opzione del livello e il numero di giorni di archiviazione.

Configurare le impostazioni avanzate nella policy

Facoltativamente, è possibile configurare impostazioni avanzate nella policy. Queste impostazioni sono disponibili per tutte le architetture di backup, inclusi snapshot locali, replica su storage secondario e backup su storage di oggetti. Queste impostazioni non sono disponibili per i carichi di lavoro Kubernetes.



Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Criteri**.
2. Dalla pagina Criteri, seleziona **Crea nuovo criterio**.
3. Nella sezione Impostazioni **Criteri > Avanzate**, seleziona la freccia rivolta verso il basso e seleziona l'opzione.
4. Fornire le seguenti informazioni:

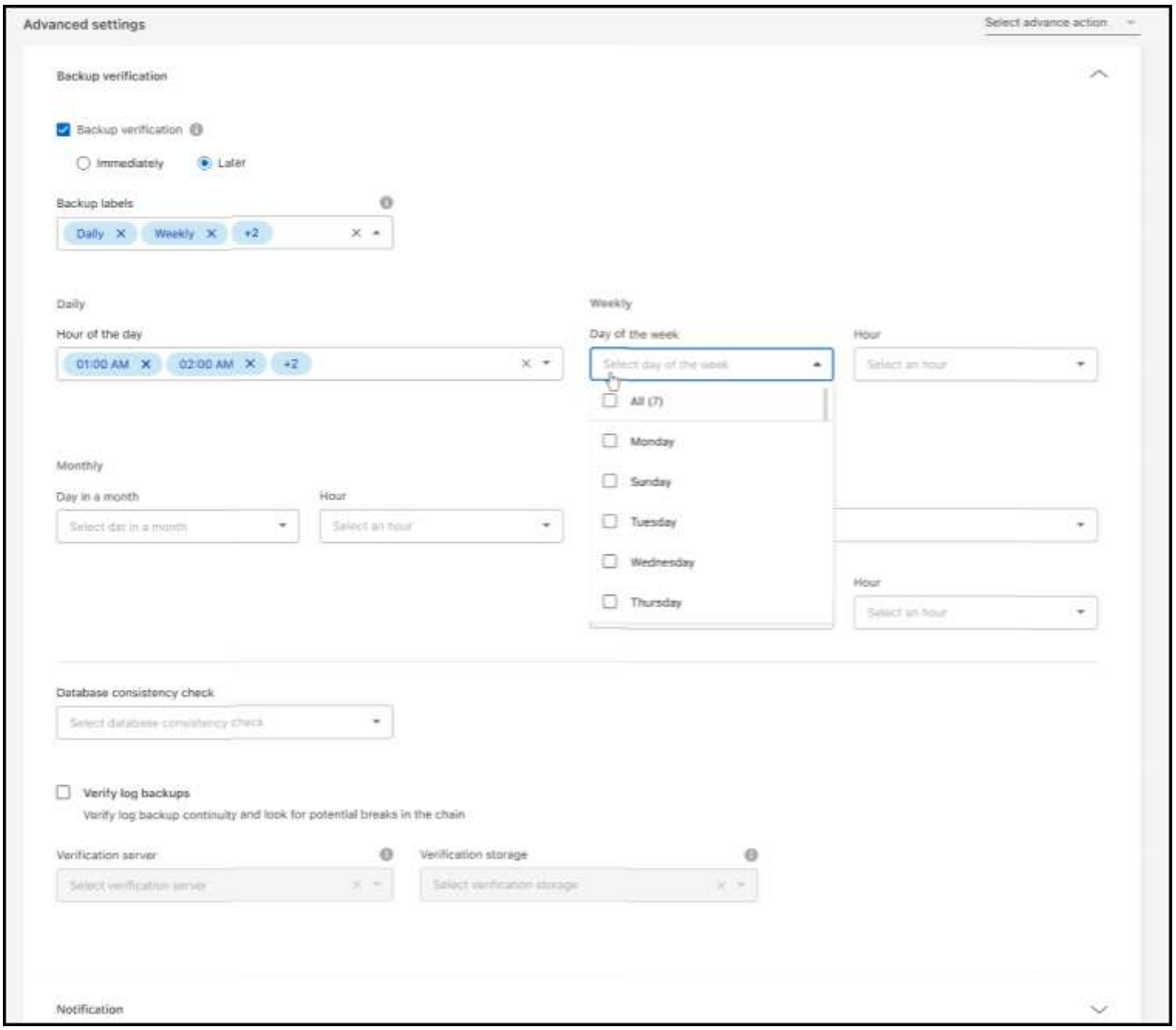
- **Backup di sola copia**: scegli il backup di sola copia (un tipo di backup di Microsoft SQL Server) che ti consente di eseguire il backup delle risorse utilizzando un'altra applicazione di backup.
- **Impostazioni del gruppo di disponibilità**: seleziona le repliche di backup preferite o specificane una specifica. Questa impostazione è utile se si dispone di un gruppo di disponibilità di SQL Server e si desidera controllare quale replica utilizzare per i backup.
- **Velocità di trasferimento massima**: per non impostare un limite all'utilizzo della larghezza di banda, selezionare **Illimitata**. Se si desidera limitare la velocità di trasferimento, selezionare **Limitata** e selezionare la larghezza di banda di rete tra 1 e 1.000 Mbps allocata per caricare i backup sull'archiviazione oggetti. Per impostazione predefinita, ONTAP può utilizzare una quantità di larghezza di banda illimitata per trasferire i dati di backup dai volumi nell'ambiente di lavoro all'archiviazione oggetti. Se si nota che il traffico di backup influisce sui normali carichi di lavoro degli utenti, si consiglia di ridurre la quantità di larghezza di banda di rete utilizzata durante il trasferimento.
- **Nuovi tentativi di backup**: (non applicabile ai carichi di lavoro VMware Preview) Per riprovare il processo in caso di errore o interruzione, selezionare **Abilita nuovi tentativi di processo in caso di errore**. Immettere il numero massimo di tentativi di snapshot e backup e l'intervallo di tempo tra i tentativi. Il riconteggio deve essere inferiore a 10. Questa impostazione è utile se si desidera garantire che il processo di backup venga ripetuto in caso di errore o interruzione.

  Se la frequenza degli snapshot è impostata su 1 ora, il ritardo massimo, insieme al conteggio dei nuovi tentativi, non dovrebbe superare i 45 minuti.

- **Abilita snapshot coerenti con la VM**: (si applica solo ai carichi di lavoro VMware) Seleziona se desideri abilitare snapshot coerenti con la VM. Ciò garantisce che gli snapshot appena creati siano coerenti con lo stato della macchina virtuale al momento dello snapshot. Ciò è utile per garantire che i backup possano essere ripristinati correttamente e che i dati siano in uno stato coerente. Ciò non si applica agli snapshot esistenti.

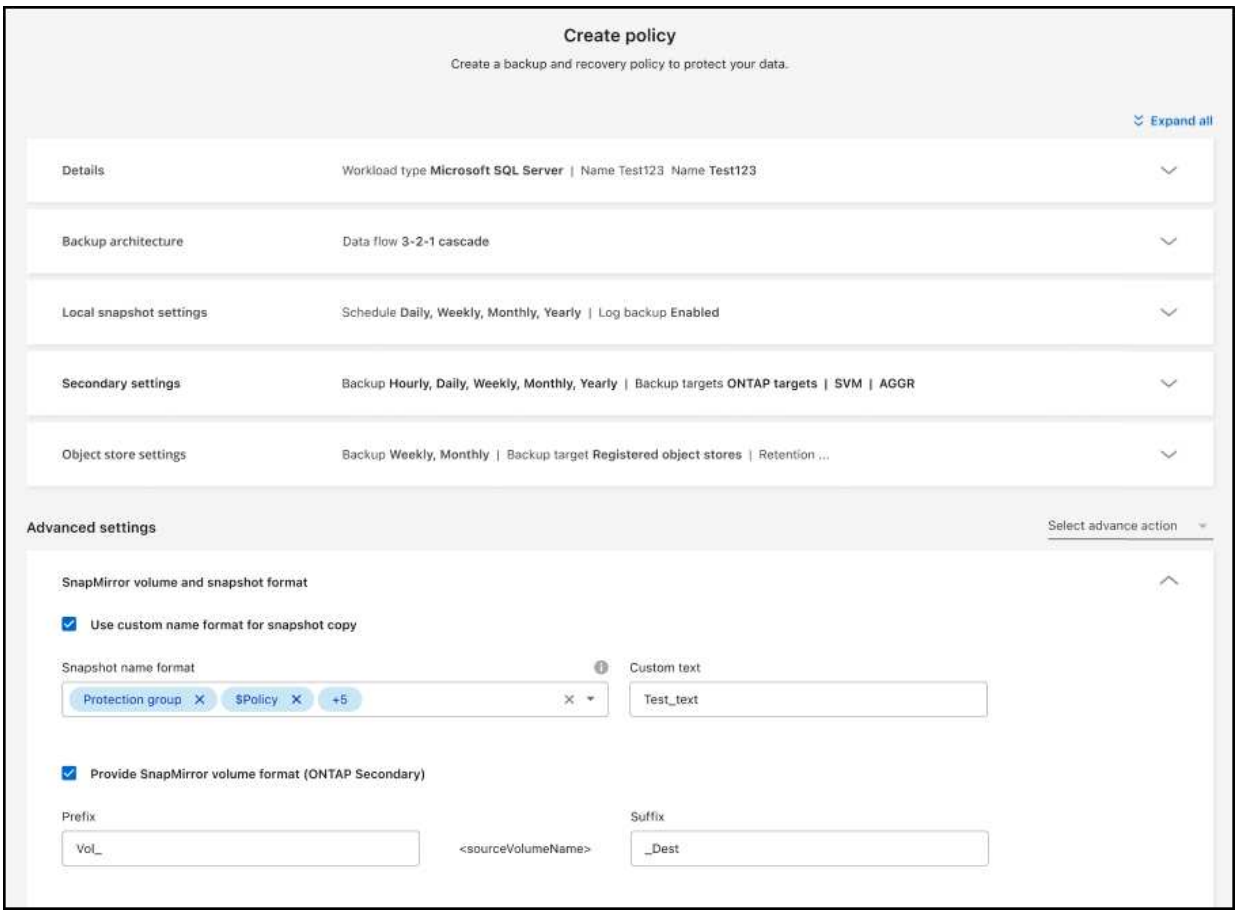
  - **Scansione ransomware**: seleziona se desideri abilitare la scansione ransomware su ciascun bucket. Ciò richiede il blocco DataLock sull'archiviazione degli oggetti. Inserire la frequenza della scansione in giorni. Questa opzione si applica all'archiviazione di oggetti AWS e Microsoft Azure. Tieni presente che questa opzione potrebbe comportare costi aggiuntivi, a seconda del provider cloud.
  - **Verifica del backup**: (non applicabile ai carichi di lavoro VMware Preview) Seleziona se desideri abilitare la verifica del backup e se desideri eseguirla immediatamente o in un secondo momento. Questa funzionalità garantisce che i backup siano validi e possano essere ripristinati correttamente. Ti consigliamo di abilitare questa opzione per garantire l'integrità dei tuoi backup. Per impostazione predefinita, la verifica del backup viene eseguita dall'archivio secondario, se questo è configurato. Se l'archiviazione secondaria non è configurata, la verifica del backup viene eseguita dall'archiviazione primaria.



Inoltre, configura le seguenti opzioni:

- Verifica **Giornaliera**, **Settimanale**, **Mensile** o **Annuale**: se hai scelto **Più tardi** come verifica del backup, seleziona la frequenza della verifica. Questo garantisce che l'integrità dei backup venga verificata regolarmente e che sia possibile ripristinarli correttamente.
- **Etichette di backup**: inserisci un'etichetta per il backup. Questa etichetta serve a identificare il backup nel sistema e può essere utile per tracciare e gestire i backup.
- **Controllo della coerenza del database**: (non applicabile ai carichi di lavoro VMware Preview) Seleziona se desideri abilitare i controlli della coerenza del database. Questa opzione garantisce che i database siano in uno stato coerente prima che venga eseguito il backup, il che è fondamentale per garantire l'integrità dei dati.
- **Verifica backup del registro**: (non applicabile ai carichi di lavoro VMware Preview) Seleziona se desideri verificare i backup del registro. Seleziona il server di verifica. Se hai scelto disk-to-disk o 3-2-1, seleziona anche la posizione di archiviazione della verifica. Questa opzione garantisce che i backup del registro siano validi e possano essere ripristinati correttamente, il che è importante per mantenere l'integrità dei database.
  - **Rete**: seleziona l'interfaccia di rete da utilizzare per le operazioni di backup. Questa opzione è utile se si dispone di più interfacce di rete e si desidera controllare quale utilizzare per i backup.
- **Spazio IP**: Seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa opzione è utile se si dispone di più spazi IP e si desidera controllare quale utilizzare per i backup.

- **Configurazione endpoint privato**: se si utilizza un endpoint privato per l'archiviazione degli oggetti, selezionare la configurazione dell'endpoint privato da utilizzare per le operazioni di backup. Questa opzione è utile se si desidera garantire che i backup vengano trasferiti in modo sicuro tramite una connessione di rete privata.
  - **Notifica**: seleziona se desideri abilitare le notifiche email per le operazioni di backup. Questa opzione è utile se desideri essere avvisato quando un'operazione di backup viene avviata, completata o non riesce.
  - **Dischi indipendenti**: (applicabile ai carichi di lavoro di VMware Preview) Selezionare questa opzione per includere nel backup tutti gli archivi dati con dischi indipendenti che contengono dati temporanei. Un disco indipendente è un disco VM non incluso negli snapshot VMware.
  - * Formato SnapMirror e snapshot*: facoltativamente, inserisci il nome del tuo snapshot in un criterio che regola i backup per i carichi di lavoro di Microsoft SQL Server. Inserisci il formato e il testo personalizzato. Se si sceglie di eseguire il backup su un archivio secondario, è anche possibile aggiungere un prefisso e un suffisso del volume SnapMirror .



Modificare un criterio

È possibile modificare l'architettura di backup, la frequenza di backup, i criteri di conservazione e altre impostazioni per un criterio.

Questa funzionalità non è disponibile per i carichi di lavoro VMware Preview.

È possibile aggiungere un ulteriore livello di protezione quando si modifica una policy, ma non è possibile rimuovere un livello di protezione. Ad esempio, se la policy protegge solo gli snapshot locali, è possibile

aggiungere la replica all'archiviazione secondaria o i backup all'archiviazione oggetti. Se si dispone di snapshot e replica locali, è possibile aggiungere l'archiviazione oggetti. Tuttavia, se si dispone di snapshot, replica e archiviazione oggetti locali, non è possibile rimuovere uno di questi livelli.

Se si modifica un criterio che esegue il backup nell'archiviazione di oggetti, è possibile abilitare l'archiviazione.

Se hai importato risorse da SnapCenter, potresti riscontrare alcune differenze tra i criteri utilizzati in SnapCenter e quelli utilizzati nel BlueXP backup and recovery. Vedere "Differenze di policy tra backup e ripristino SnapCenter e BlueXP backup and recovery".

Ruolo BlueXP richiesto

Amministratore dell'organizzazione o amministratore della cartella o del progetto. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. In BlueXP, vai su **Protezione** > **Backup e ripristino**.
2. Selezionare la scheda **Criteri**.
3. Seleziona la policy che vuoi modificare.
4. Seleziona **Azioni** ••• icona e seleziona **Modifica**.

Eliminazione di un criterio

Puoi eliminare una policy se non ti serve più.

Non è possibile eliminare un criterio associato a un carico di lavoro.

Fasi

1. In BlueXP, vai su **Protezione** > **Backup e ripristino**.
2. Selezionare la scheda **Criteri**.
3. Seleziona la policy che vuoi eliminare.
4. Seleziona **Azioni** ••• icona e seleziona **Elimina**.
5. Controllare le informazioni nella finestra di dialogo di conferma e selezionare **Elimina**.

Proteggere i carichi di lavoro del volume ONTAP

Proteggi i dati dei volumi ONTAP utilizzando il backup e ripristino BlueXP

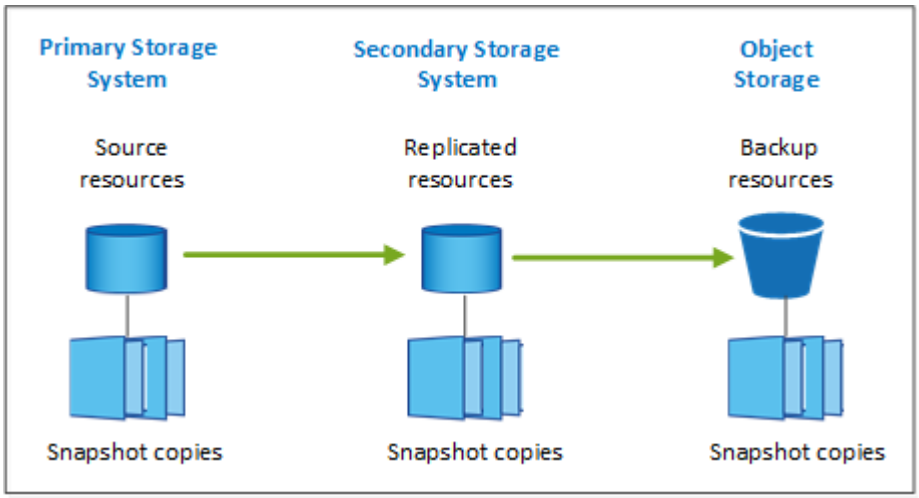
Il servizio di backup e ripristino BlueXP offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del volume ONTAP. Puoi implementare una strategia 3-2-1 in cui hai 3 copie dei dati di origine su 2 sistemi storage diversi insieme a una copia nel cloud.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Dopo l'attivazione, il backup e il ripristino creano backup incrementali a livello di blocco per sempre,

memorizzati su un altro cluster ONTAP e nello storage a oggetti nel cloud. Oltre al volume di origine, si avrà a disposizione:

- Copia Snapshot del volume sul sistema di origine
- Volume replicato su un sistema storage diverso
- Backup del volume nello storage a oggetti



Il backup e ripristino BlueXP sfrutta la tecnologia di replica dei dati SnapMirror di NetApp per garantire che tutti i backup siano completamente sincronizzati creando copie Snapshot e trasferendole nelle posizioni di backup.

I vantaggi dell'approccio 3-2-1 includono:

- Copie multiple dei dati offrono protezione multi-layer contro le minacce interne (interne) e esterne alla cybersicurezza.
- Diversi tipi di supporti garantiscono la fattibilità del failover in caso di guasto fisico o logico di un tipo di supporto.
- La copia on-site facilita ripristini rapidi, con le copie off-site pronte nel caso in cui la copia on-site venga compromessa.

Se necessario, è possibile ripristinare un intero *volume*, una *cartella* o uno o più *file* da una qualsiasi delle copie di backup nello stesso ambiente di lavoro o in un ambiente di lavoro diverso.

Caratteristiche

Funzioni di replica:

- Replica dei dati tra sistemi storage ONTAP per supportare backup e disaster recovery.
- Garantisci l'affidabilità del tuo ambiente DR con disponibilità elevata.
- Crittografia nativa ONTAP in-flight impostata tramite chiave precondivisa (PSK) tra i due sistemi.
- I dati copiati sono immutabili fino a quando non vengono scritti e pronti per l'uso.
- La replica ripara automaticamente in caso di errore di trasferimento.
- Rispetto al "Servizio di replica BlueXP", La replica nel backup e ripristino di BlueXP include le seguenti funzionalità:
  - Replica di più volumi FlexVol alla volta su un sistema secondario.

- Ripristinare un volume replicato nel sistema di origine o in un sistema diverso utilizzando l'interfaccia utente.

Vedere "Limitazioni di replicazione per volumi ONTAP" per un elenco delle funzionalità di replicazione non disponibili con il BlueXP backup and recovery per i volumi ONTAP .

Caratteristiche di backup su oggetto:

- Eseguire il backup di copie indipendenti dei volumi di dati in uno storage a oggetti a basso costo.
- Applicare una singola policy di backup a tutti i volumi di un cluster oppure assegnare policy di backup diverse a volumi che hanno obiettivi di punto di ripristino univoci.
- Creare un criterio di backup da applicare a tutti i volumi futuri creati nel cluster.
- Rendere i file di backup immutabili in modo che siano bloccati e protetti per il periodo di conservazione.
- Esegui la scansione dei file di backup per individuare eventuali attacchi ransomware e rimuovi/sostituisci automaticamente i backup infetti.
- Eseguire il Tier dei file di backup più vecchi sullo storage di archiviazione per risparmiare sui costi.
- Eliminare la relazione di backup in modo da poter archiviare i volumi di origine non necessari mantenendo i backup dei volumi.
- Backup dal cloud al cloud e dai sistemi on-premise al cloud pubblico o privato.
- I dati di backup sono protetti con crittografia AES-256 bit a riposo e connessioni HTTPS TLS 1.2 in volo.
- Utilizza le tue chiavi gestite dal cliente per la crittografia dei dati invece di utilizzare le chiavi di crittografia predefinite del tuo cloud provider.
- Supporto di un massimo di 4,000 backup di un singolo volume.

Funzionalità di ripristino:

- Ripristinare i dati da un punto specifico di tempo da copie Snapshot locali, volumi replicati o volumi di backup nello storage a oggetti.
- Ripristinare un volume, una cartella o singoli file nel sistema di origine o in un sistema diverso.
- Ripristinare i dati in un ambiente di lavoro utilizzando un abbonamento/account diverso o che si trova in un'altra regione.
- Eseguire un *ripristino rapido* di un volume dal cloud storage a un sistema Cloud Volumes ONTAP o a un sistema on-premise; perfetto per situazioni di disaster recovery in cui è necessario fornire l'accesso a un volume il prima possibile.
- Ripristinare i dati a livello di blocco, posizionando i dati direttamente nella posizione specificata, il tutto mantenendo gli ACL originali.
- Sfoglia e cerca nei cataloghi di file per selezionare facilmente singole cartelle e file per il ripristino di un singolo file.

Ambienti di lavoro supportati per le operazioni di backup e ripristino

Il backup e ripristino BlueXP supporta gli ambienti di lavoro ONTAP e i provider di cloud pubblici e privati.

Regioni supportate

Il backup e recovery di BlueXP è supportato con Cloud Volumes ONTAP in molte regioni di Amazon Web Services, Microsoft Azure e Google Cloud.

"Ulteriori informazioni utilizzando la mappa delle regioni globali"

Destinazioni di backup supportate

Il backup e ripristino BlueXP consente di eseguire il backup dei volumi ONTAP dai seguenti ambienti di lavoro di origine ai seguenti ambienti di lavoro secondari e storage a oggetti nei provider di cloud pubblici e privati. Le copie Snapshot risiedono nell'ambiente di lavoro di origine.

Ambiente di lavoro di origine	Ambiente di lavoro secondario (replica)	Archivio oggetti di destinazione (backup)
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise	Amazon S3 endif::aws[] ifdef::Azure[]
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise	Azure Blob endif::Azure[] ifdef::gcp[]
Cloud Volumes ONTAP in Google	Cloud Volumes ONTAP in Google Sistema ONTAP on-premise	Google Cloud Storage endif::gcp[]
Sistema ONTAP on-premise	Cloud Volumes ONTAP Sistema ONTAP on-premise	ifdef::aws[] Amazon S3 Azure Blob Storage Google Cloud NetApp StorageGRID ONTAP S3

Destinazioni di ripristino supportate

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un ambiente di lavoro secondario (un volume replicato) o nello storage a oggetti (un file di backup) nei seguenti ambienti di lavoro. Le copie Snapshot risiedono nell'ambiente di lavoro di origine e possono essere ripristinate solo sullo stesso sistema.

Percorso del file di backup		Ambiente di lavoro di destinazione
Archivio oggetti (backup)	**Sistema secondario (replica)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise	Cloud Volumes ONTAP in AWS on-premise ONTAP system endif::aws[] ifdef::Azure[]
Azure Blob	Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise	Cloud Volumes ONTAP in Azure on-premise ONTAP system endif::Azure[] ifdef::gcp[]

Percorso del file di backup		Ambiente di lavoro di destinazione
Storage Google Cloud	Cloud Volumes ONTAP in Google Sistema ONTAP on-premise	Cloud Volumes ONTAP in Google on-premise ONTAP system endif::gcp[]
NetApp StorageGRID	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP on-premise
ONTAP S3	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP on-premise

Si noti che i riferimenti ai "sistemi ONTAP on-premise" includono i sistemi FAS, AFF e ONTAP Select.

Volumi supportati

Il backup e ripristino di BlueXP supporta i seguenti tipi di volumi:

- Volumi di lettura/scrittura FlexVol
- FlexGroup Volumes (richiede ONTAP 9.12.1 o versione successiva)
- Volumi aziendali SnapLock (richiede ONTAP 9.11.1 o versione successiva)
- SnapLock Compliance per volumi on-premise (richiede ONTAP 9.14 o versioni successive)
- Volumi di destinazione SnapMirror Data Protection (DP)

Il backup e recovery di BlueXP non supporta i backup di FlexCache Volumes.

Vedi le sezioni su "Limitazioni di backup e ripristino per ONTAP Volumes" per requisiti e limitazioni aggiuntivi.

Costo

Esistono due tipi di costi associati all'utilizzo del backup e ripristino BlueXP con i sistemi ONTAP: Costi delle risorse e costi del servizio. Entrambi i costi sono relativi alla parte del servizio di backup a oggetto.

La creazione di copie Snapshot o volumi replicati è gratuita, a parte lo spazio su disco necessario per memorizzare le copie Snapshot e i volumi replicati.

Costi delle risorse

I costi delle risorse vengono pagati al cloud provider per la capacità dello storage a oggetti e per la scrittura e la lettura dei file di backup nel cloud.

- Per il backup su storage a oggetti, pagherai il tuo cloud provider per i costi dello storage a oggetti.

  Poiché il backup e ripristino BlueXP preserva l'efficienza dello storage del volume di origine, il cloud provider paga i costi dello storage a oggetti per l'efficienza dei dati *dopo* ONTAP (per la minore quantità di dati dopo l'applicazione della deduplica e della compressione).

- Per il ripristino dei dati utilizzando Search & Restore, alcune risorse vengono fornite dal tuo cloud provider e il costo per TIB è associato alla quantità di dati sottoposti a scansione dalle tue richieste di ricerca. (Queste risorse non sono necessarie per Browse & Restore).
  - In AWS, "Amazon Athena" e. "Colla AWS" Le risorse vengono implementate in un nuovo bucket S3.

    - In Azure, An "Spazio di lavoro Azure Synapse" e. "Storage Azure Data Lake" vengono forniti nell'account storage per memorizzare e analizzare i dati.
- In Google, viene implementato un nuovo bucket e "Servizi Google Cloud BigQuery" sono forniti a livello di account/progetto.
- Se si prevede di ripristinare i dati del volume da un file di backup spostato nello storage a oggetti di archivio, è prevista una tariffa aggiuntiva per il recupero di GiB e per richiesta addebitata dal cloud provider.
- Se intendi analizzare un file di backup per un ransomware durante il processo di ripristino dei dati dei volumi (se hai attivato DataLock e protezione dal ransomware per i backup nel cloud), ti verranno addebitati anche costi di uscita extra da parte del tuo cloud provider.

Costi di servizio

I costi di servizio vengono pagati a NetApp e coprono sia il costo per *creare* backup nello storage a oggetti che per *ripristinare* volumi, o file, da tali backup. Si paga solo per i dati che si proteggono nello storage a oggetti, calcolati in base alla capacità logica utilizzata di origine (*before* efficienze ONTAP) dei volumi ONTAP di cui viene eseguito il backup nello storage a oggetti. Questa capacità è nota anche come terabyte front-end (FETB).

Esistono tre modi per pagare il servizio di backup. La prima opzione è iscriversi al tuo cloud provider, che ti consente di pagare al mese. La seconda opzione consiste nell'ottenere un contratto annuale. La terza opzione consiste nell'acquistare le licenze direttamente da NetApp.

Licensing

Il backup e ripristino BlueXP è disponibile con i seguenti modelli di consumo:

- **BYOL**: Licenza acquistata da NetApp e utilizzabile con qualsiasi cloud provider.
- **PAYGO**: Un abbonamento orario dal mercato del tuo cloud provider.
- **Annuale**: Un contratto annuale dal mercato del tuo cloud provider.

Una licenza di backup è richiesta solo per il backup e il ripristino dallo storage a oggetti. La creazione di copie Snapshot e volumi replicati non richiede una licenza.

Porta la tua licenza

Il BYOL è basato sulla capacità a termine (1, 2 o 3 anni) *e* in incrementi di 1 TiB. Pagherai NetApp per utilizzare il servizio per un periodo di tempo, ad esempio 1 anno, e per una capacità massima, ad esempio 10 TIB.

Riceverai un numero di serie che inserisci nella pagina del portafoglio digitale BlueXP per attivare il servizio. Una volta raggiunto il limite, è necessario rinnovare la licenza. La licenza BYOL di backup si applica a tutti i sistemi sorgente associati alla tua organizzazione o account BlueXP .

"Scopri come gestire le tue licenze BYOL".

Abbonamento pay-as-you-go

Il backup e ripristino BlueXP offre licenze basate sui consumi in un modello pay-as-you-go. Dopo aver effettuato l'iscrizione tramite il marketplace del tuo cloud provider, pagherai per ogni GiB i dati di cui hai eseguito il backup, senza alcun pagamento anticipato. Il tuo cloud provider ti addebita la fattura mensile.

"Scopri come impostare un abbonamento pay-as-you-go".

Ricorda che una prova gratuita di 30 giorni è disponibile quando ti iscrivi inizialmente con un abbonamento PAYGO.

Contratto annuale

Quando utilizzi AWS, sono disponibili due contratti annuali per i termini da 1, 2 o 3 anni:

- Un piano di "backup sul cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.
- Un piano "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Questo include backup illimitati per volumi Cloud Volumes ONTAP addebitati a fronte di questa licenza (la capacità di backup non viene conteggiata rispetto alla licenza).

Quando utilizzi Azure, sono disponibili due contratti annuali per i termini di 1, 2 o 3 anni:

- Un piano di "backup sul cloud" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise.
- Un piano "CVO Professional" che consente di unire backup e ripristino di Cloud Volumes ONTAP e BlueXP. Questo include backup illimitati per volumi Cloud Volumes ONTAP addebitati a fronte di questa licenza (la capacità di backup non viene conteggiata rispetto alla licenza).

Quando utilizzi GCP, puoi richiedere un'offerta privata da NetApp, e quindi selezionare il piano quando ti iscrivi da Google Cloud Marketplace durante l'attivazione di backup e recovery di BlueXP .

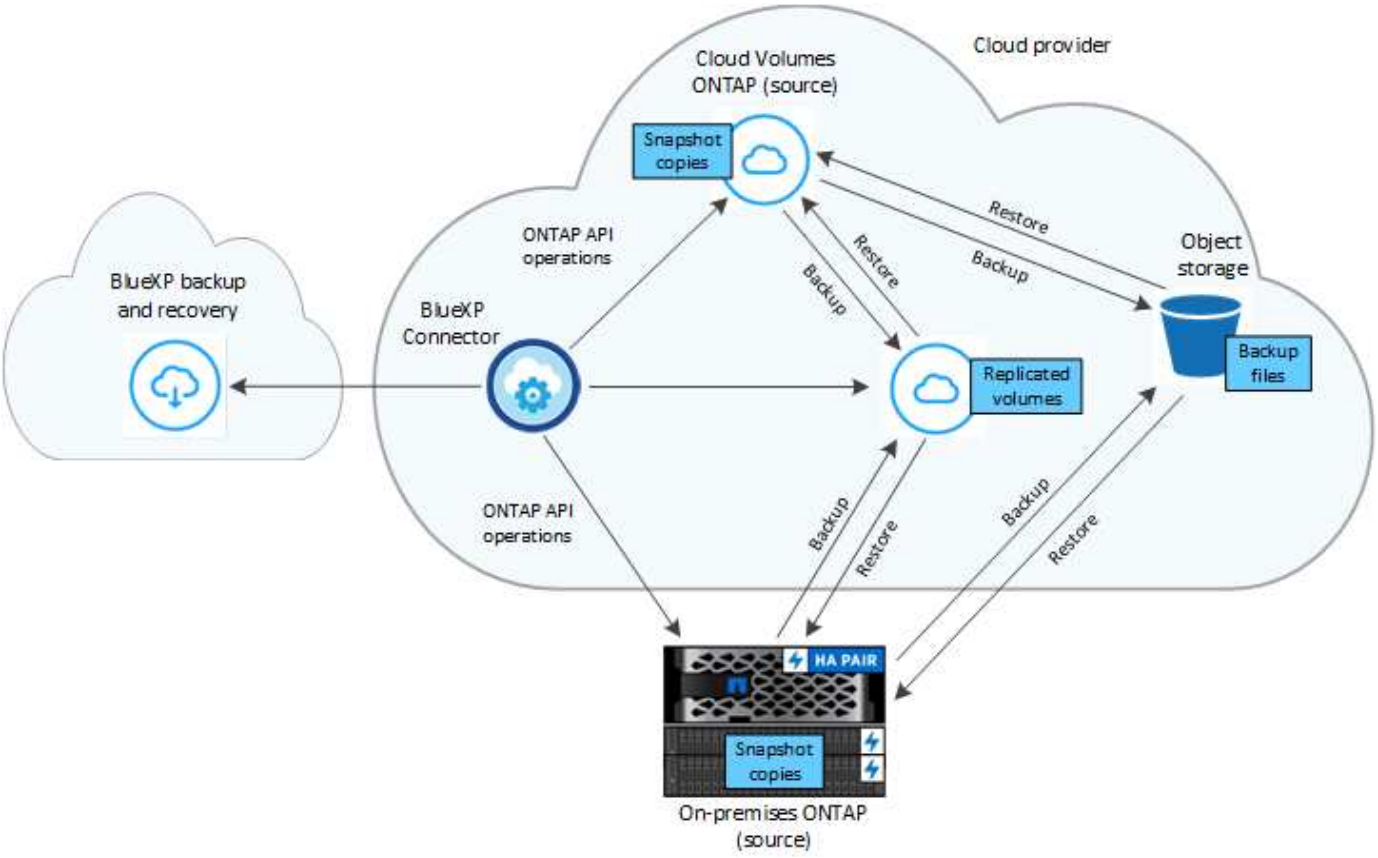
"Scopri come impostare i contratti annuali".

Come funziona il backup e ripristino di BlueXP

Quando si abilita il backup e ripristino BlueXP su un sistema Cloud Volumes ONTAP o ONTAP on-premise, il servizio esegue un backup completo dei dati. Dopo il backup iniziale, tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e dei nuovi blocchi. In questo modo il traffico di rete viene ridotto al minimo. Il backup sullo storage a oggetti si basa su "Tecnologia NetApp SnapMirror Cloud".

Qualsiasi azione intrapresa direttamente dall'ambiente del cloud provider per gestire o modificare i file di backup del cloud potrebbe corrompere i file e causare una configurazione non supportata.

La seguente immagine mostra la relazione tra ciascun componente:



Questo diagramma mostra i volumi replicati in un sistema Cloud Volumes ONTAP, ma i volumi possono essere replicati anche in un sistema ONTAP on-premise.

Dove risiedono i backup

I backup risiedono in posizioni diverse a seconda del tipo di backup:

- *Copie Snapshot* risiedono nel volume di origine nell'ambiente di lavoro di origine.
- *Volumi replicati* risiedono nel sistema di storage secondario, un sistema Cloud Volumes ONTAP o ONTAP on-premise.
- *Copie di backup* vengono memorizzate in un archivio di oggetti creato da BlueXP nel tuo account cloud. C'è un archivio di oggetti per cluster/ambiente di lavoro e BlueXP nomina l'archivio di oggetti come segue: "netapp-backup-clusteruid". Assicurarsi di non eliminare questo archivio di oggetti.
  - In AWS, BlueXP attiva "Funzione di accesso pubblico a blocchi Amazon S3" Sul bucket S3.
  - In Azure, BlueXP utilizza un gruppo di risorse nuovo o esistente con un account di storage per il container Blob. BlueXP "blocca l'accesso pubblico ai dati blob" per impostazione predefinita.
  - In GCP, BlueXP utilizza un progetto nuovo o esistente con un account di storage per il bucket di Google Cloud Storage.
  - In StorageGRID, BlueXP usa un account tenant esistente per il bucket S3.
  - In ONTAP S3, BlueXP usa un account utente esistente per il bucket S3.

Se in futuro si desidera modificare l'archivio oggetti di destinazione per un cluster, sarà necessario "Annullare la registrazione del backup e ripristino BlueXP per l'ambiente di lavoro" e quindi abilitare il BlueXP backup and recovery utilizzando le informazioni del nuovo provider cloud.

Pianificazione di backup e impostazioni di conservazione personalizzabili

Quando si abilita il backup e ripristino BlueXP per un ambiente di lavoro, tutti i volumi selezionati inizialmente vengono sottoposti a backup utilizzando i criteri selezionati. È possibile selezionare policy separate per le copie Snapshot, i volumi replicati e i file di backup. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi RPO (Recovery Point Objective) diversi, è possibile creare criteri aggiuntivi per tale cluster e assegnare tali criteri agli altri volumi dopo l'attivazione del backup e ripristino di BlueXP.

È possibile scegliere una combinazione di backup orari, giornalieri, settimanali, mensili e annuali di tutti i volumi. Per il backup su oggetto è inoltre possibile selezionare una delle policy definite dal sistema che fornisce backup e conservazione per 3 mesi, 1 anno e 7 anni. Le policy di protezione del backup create sul cluster utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP verranno visualizzate come selezioni. Sono inclusi i criteri creati utilizzando etichette SnapMirror personalizzate.

Il criterio Snapshot applicato al volume deve avere una delle etichette utilizzate nel criterio di replica e nel criterio di backup su oggetto. Se le etichette corrispondenti non vengono trovate, non verranno creati file di backup. Ad esempio, se si desidera creare volumi replicati e file di backup "settimanali", è necessario utilizzare una policy Snapshot che crei copie Snapshot "settimanali".

Una volta raggiunto il numero massimo di backup per una categoria o un intervallo, i backup più vecchi vengono rimossi, in modo da avere sempre a disposizione i backup più recenti (e in modo che i backup obsoleti non continuino a occupare spazio).

Il periodo di conservazione per i backup dei volumi di protezione dei dati è lo stesso definito nella relazione SnapMirror di origine. È possibile modificare questa impostazione utilizzando l'API.

Impostazioni di protezione del file di backup

Se il cluster utilizza ONTAP 9.11.1 o versione successiva, è possibile proteggere i backup nello storage a oggetti da attacchi ransomware e di eliminazione. Ogni policy di backup fornisce una sezione per *DataLock e ransomware Protection* che può essere applicata ai file di backup per un periodo di tempo specifico, il *periodo di conservazione*.

- *DataLock* protegge i file di backup da modifiche o eliminazioni.
- *Ransomware Protection* esegue la scansione dei file di backup per cercare la prova di un attacco ransomware quando viene creato un file di backup e quando vengono ripristinati i dati di un file di backup.

Le scansioni pianificate di protezione dal ransomware sono abilitate per impostazione predefinita. L'impostazione predefinita per la frequenza di scansione è di 7 giorni. La scansione viene eseguita solo sull'ultima copia Snapshot. Le scansioni pianificate possono essere disattivate per ridurre i costi. Puoi abilitare o disabilitare le scansioni ransomware pianificate sull'ultima copia Snapshot utilizzando l'opzione nella pagina Advanced Settings (Impostazioni avanzate). Se si attiva, le scansioni vengono eseguite settimanalmente per impostazione predefinita. È possibile modificare la pianificazione in giorni o settimane o disattivarla, risparmiando sui costi.

Il periodo di conservazione dei backup è lo stesso del periodo di conservazione della pianificazione dei backup, più un buffer massimo di 31 giorni. Ad esempio, i backup *settimanali* con *5* copie conservate bloccano ogni file di backup per 5 settimane. I backup *mensili* con *6* copie conservate bloccano ogni file di backup per 6 mesi.

Il supporto è attualmente disponibile quando la destinazione del backup è Amazon S3, Azure Blob o NetApp StorageGRID. Le destinazioni di altri provider di storage verranno aggiunte nelle versioni future.

Per ulteriori informazioni, fare riferimento a queste informazioni:

- "Funzionamento di DataLock e protezione ransomware".
- "Come aggiornare le opzioni di protezione dal ransomware nella pagina Impostazioni avanzate".

Non è possibile attivare DataLock se si stanno eseguendo il tiering dei backup nello storage di archiviazione.

Storage di archiviazione per file di backup meno recenti

Quando si utilizza un determinato cloud storage, è possibile spostare i file di backup meno recenti su un livello di accesso/classe di storage meno costoso dopo un certo numero di giorni. Puoi anche scegliere di inviare immediatamente i file di backup allo storage di archivio senza essere scritti su cloud storage standard. Nota: Non è possibile utilizzare lo storage di archiviazione se è stato attivato DataLock.

- In AWS, i backup iniziano nella classe di storage *Standard* e passano alla classe di storage *Standard-infrequent Access* dopo 30 giorni.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile scegliere di raggruppare i backup più vecchi in uno storage *S3 Glacier* o *S3 Glacier Deep Archive* nell'interfaccia utente di backup e ripristino BlueXP dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sullo storage di archiviazione AWS".

- In Azure, i backup sono associati al Tier di accesso *Cool*.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile scegliere di raggruppare i backup meno recenti in storage *Azure Archive* nell'interfaccia utente di backup e ripristino di BlueXP dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sullo storage di archivio Azure".

- In GCP, i backup sono associati alla classe di storage *Standard*.

  Se il cluster utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di raggruppare i backup meno recenti in storage *Archive* nell'interfaccia utente di backup e ripristino BlueXP dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sullo storage di archivio di Google".

- In StorageGRID, i backup sono associati alla classe di storage *Standard*.

  Se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza 11.4 o versione successiva, è possibile archiviare i file di backup meno recenti nello storage di archiviazione del cloud pubblico dopo un certo numero di giorni. Attualmente il supporto è per i Tier di storage AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. "Scopri di più sull'archiviazione dei file di backup da StorageGRID".

Per maggiori dettagli sull'archiviazione dei vecchi file di backup, vedere il collegamento:prev-ontap-policy-object-options.html.

Considerazioni sui criteri di tiering FabricPool

È necessario tenere presente che il volume di cui si esegue il backup risiede in un aggregato FabricPool e dispone di un criterio di tiering assegnato diverso da `none`:

- Il primo backup di un volume a livelli FabricPool richiede la lettura di tutti i dati locali e tutti i dati a livelli (dall'archivio di oggetti). Un'operazione di backup non "riscalda" i dati cold a più livelli nello storage a oggetti.

Questa operazione potrebbe causare un aumento dei costi una tantum per la lettura dei dati dal tuo cloud provider.

  - I backup successivi sono incrementali e non hanno questo effetto.
  - Se il criterio di tiering viene assegnato al volume al momento della sua creazione iniziale, il problema non viene visualizzato.

- Considerare l'impatto dei backup prima di assegnare `all` policy di tiering sui volumi. Poiché i dati vengono immediatamente suddivisi in più livelli, il backup e ripristino BlueXP legge i dati dal livello cloud piuttosto che dal livello locale. Poiché le operazioni di backup simultanee condividono il collegamento di rete con l'archivio di oggetti cloud, potrebbe verificarsi un peggioramento delle performance se le risorse di rete diventano saturate. In questo caso, è possibile configurare in modo proattivo più interfacce di rete (LIFF) per ridurre questo tipo di saturazione di rete.

Pianifica il tuo percorso di protezione con il backup e il ripristino di BlueXP

Il servizio di backup e ripristino BlueXP consente di creare fino a tre copie dei volumi di origine per proteggere i dati. Quando si attiva questo servizio sui volumi, è possibile selezionare numerose opzioni, pertanto è necessario rivedere le scelte in modo da essere pronti.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Esamineremo le seguenti opzioni:

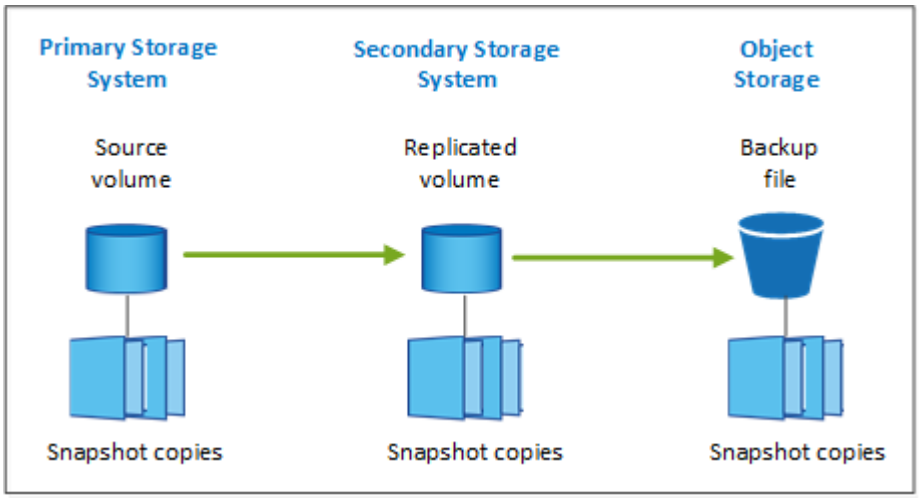
- Quali funzionalità di protezione userai: Copie Snapshot, volumi replicati e/o backup nel cloud
- Quale architettura di backup utilizzerai: Un backup a cascata o fan-out dei tuoi volumi
- Verranno utilizzati i criteri di backup predefiniti o è necessario creare criteri personalizzati
- Vuoi che il servizio crei i bucket cloud per te o vuoi creare i container di storage a oggetti prima di iniziare
- Quale modalità di implementazione di BlueXP Connector utilizzi (modalità standard, limitata o privata)

Quali funzioni di protezione utilizzerai

Prima di selezionare le funzioni da utilizzare, ecco una rapida spiegazione delle funzioni di ciascuna funzione e del tipo di protezione fornito.

Tipo di backup	Descrizione
Snapshot	Consente di creare un'immagine point-in-time in sola lettura di un volume all'interno del volume di origine come copia snapshot. È possibile utilizzare la copia snapshot per recuperare singoli file o per ripristinare l'intero contenuto di un volume.
Replica	Crea una copia secondaria dei tuoi dati su un altro sistema storage ONTAP e aggiorna continuamente i dati secondari. I tuoi dati vengono mantenuti aggiornati e rimangono disponibili ogni volta che ne hai bisogno.
Backup nel cloud	Crea backup dei tuoi dati nel cloud per motivi di protezione e archiviazione a lungo termine. Se necessario, è possibile ripristinare un volume, una cartella o singoli file dal backup nello stesso ambiente di lavoro o in un ambiente diverso.

Gli snapshot sono la base di tutti i metodi di backup e sono necessari per utilizzare il servizio di backup e ripristino. Una copia snapshot è un'immagine di sola lettura point-in-time di un volume. L'immagine consuma uno spazio di storage minimo e subisce un overhead delle performance trascurabile poiché registra solo le modifiche ai file dall'ultima copia snapshot effettuata. La copia snapshot creata sul volume viene utilizzata per mantenere il volume replicato e il file di backup sincronizzati con le modifiche apportate al volume di origine, come mostrato nella figura.



È possibile scegliere di creare volumi replicati su un altro sistema storage ONTAP e file di backup nel cloud. In alternativa, puoi scegliere di creare volumi replicati o file di backup.

In sintesi, questi sono i flussi di protezione validi che è possibile creare per i volumi nel proprio ambiente di lavoro ONTAP:

- Volume di origine → copia Snapshot → volume replicato → file di backup
- Volume di origine → copia Snapshot → file di backup
- Volume di origine → copia Snapshot → volume replicato

La creazione iniziale di un volume replicato o di un file di backup include una copia completa dei dati di origine, chiamata *trasferimento baseline*. I trasferimenti successivi contengono solo copie differenziali dei dati di origine (lo snapshot).

Confronto dei diversi metodi di backup

La tabella seguente mostra un confronto generalizzato dei tre metodi di backup. Sebbene lo spazio di storage a oggetti sia in genere meno costoso dello storage su disco on-premise, se pensi di poter ripristinare frequentemente i dati dal cloud, le tariffe di uscita dai cloud provider possono ridurre alcuni dei tuoi risparmi. Sarà necessario identificare la frequenza con cui è necessario ripristinare i dati dai file di backup nel cloud.

Oltre a questi criteri, lo storage cloud offre opzioni di sicurezza aggiuntive se si utilizza la funzionalità DataLock e ransomware Protection, oltre a risparmi aggiuntivi selezionando classi di storage di archiviazione per i file di backup meno recenti. "Scopri di più sulla protezione DataLock e Ransomware e sulle impostazioni di archiviazione".

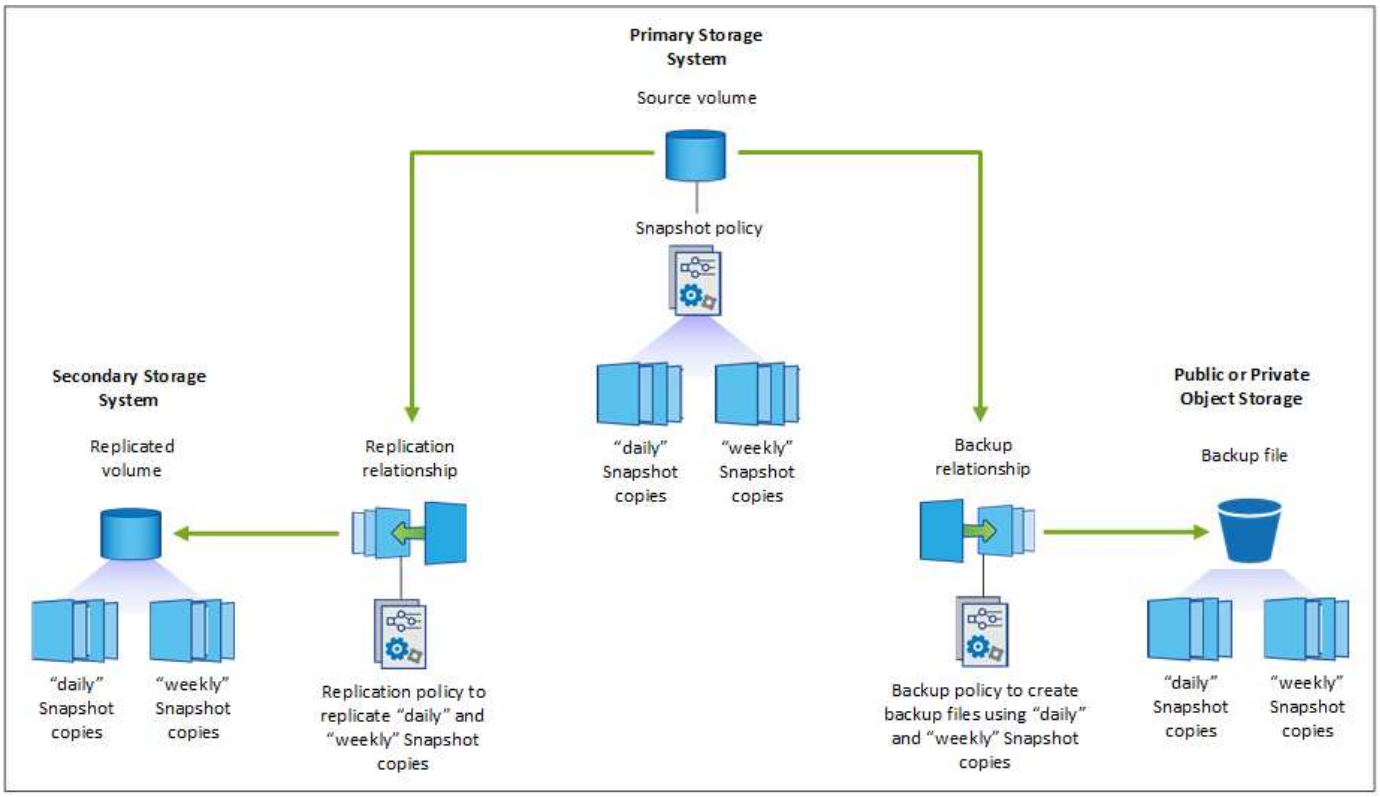
Tipo di backup	Velocità di backup	Costi di backup	Velocità di ripristino	Costi di ripristino
Istantanea	Alto	Basso (spazio su disco)	Alto	Basso

Tipo di backup	Velocità di backup	Costi di backup	Velocità di ripristino	Costi di ripristino
Replication	Medio	Media (spazio su disco)	Medio	Medio (rete)
Backup cloud	Basso	Basso (spazio oggetto)	Basso	Elevato (tariffe provider)

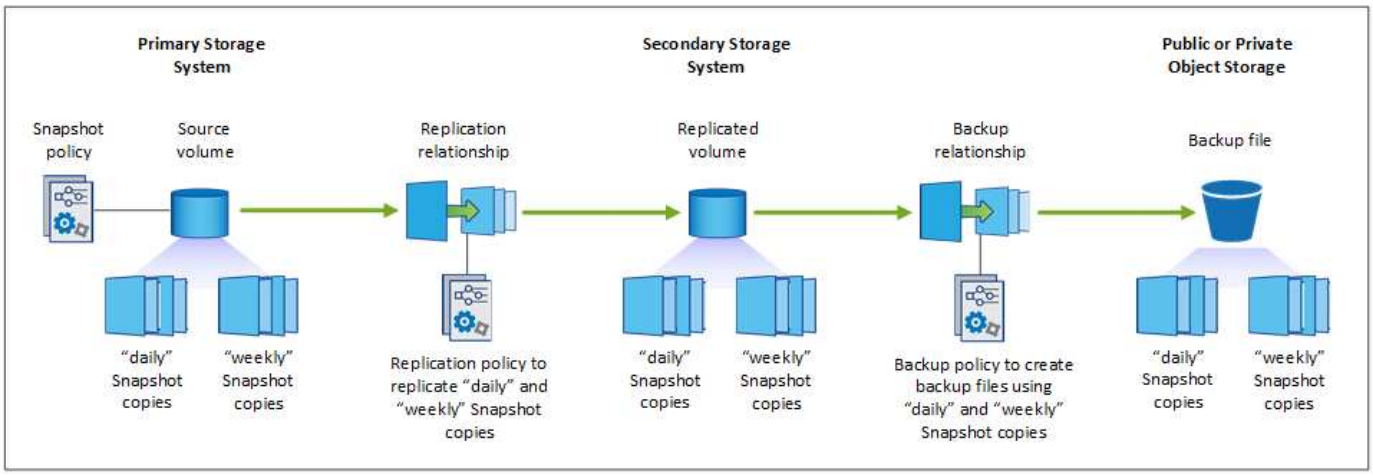
Quale architettura di backup utilizzerai

Quando si creano volumi replicati e file di backup, è possibile scegliere un'architettura fan-out o a cascata per eseguire il backup dei volumi.

Un'architettura **fan-out** trasferisce la copia snapshot in modo indipendente nel sistema di storage di destinazione e nell'oggetto di backup nel cloud.



Un'architettura **a cascata** trasferisce prima la copia snapshot nel sistema di storage di destinazione, quindi il sistema trasferisce la copia nell'oggetto di backup nel cloud.



Confronto delle diverse scelte di architettura

Questa tabella fornisce un confronto tra le architetture fan-out e cascata.

Fan-out	Cascata
Piccolo impatto sulle prestazioni del sistema di origine perché invia copie snapshot a 2 sistemi distinti	Minori effetti sulle performance del sistema storage di origine perché invia la copia Snapshot solo una volta
È più semplice da configurare perché tutte le policy, le reti e le configurazioni ONTAP vengono eseguite sul sistema di origine	Richiede alcune configurazioni di rete e ONTAP anche dal sistema secondario.

Verranno utilizzati i criteri predefiniti per istantanee, repliche e backup

È possibile utilizzare i criteri predefiniti forniti da NetApp per creare i backup oppure creare criteri personalizzati. Quando si utilizza la procedura guidata di attivazione per attivare il servizio di backup e ripristino per i volumi, è possibile scegliere tra i criteri predefiniti e gli altri criteri già presenti nell'ambiente di lavoro (sistema Cloud Volumes ONTAP o ONTAP on-premise). Se si desidera utilizzare un criterio diverso da quello esistente, è possibile crearne uno prima di avviare o durante l'attivazione guidata.

- Il criterio di snapshot predefinito crea copie snapshot ogni ora, ogni giorno e ogni settimana, conservando 6 copie snapshot ogni ora, 2 al giorno e 2 copie snapshot ogni settimana.
- Il criterio di replica predefinito replica le copie snapshot giornaliere e settimanali, conservando 7 copie snapshot giornaliere e 52 settimanali.
- Il criterio di backup predefinito replica le copie snapshot giornaliere e settimanali, conservando 7 copie snapshot giornaliere e 52 settimanali.

Se si creano criteri personalizzati per la replica o il backup, le etichette dei criteri (ad esempio, "giornaliero" o "settimanale") devono corrispondere alle etichette presenti nei criteri snapshot o nei volumi replicati e nei file di backup non verranno creati.

Puoi creare policy di backup, replica e backup su storage a oggetti nell'interfaccia utente di backup e recovery di BlueXP . Per ulteriori informazioni, vedere la sezione "aggiunta di un nuovo criterio di backup".

Oltre a utilizzare il backup e il ripristino di BlueXP per creare policy personalizzate, puoi utilizzare System Manager o l'interfaccia a riga di comando (CLI) di ONTAP:

- "Creare una policy di snapshot utilizzando System Manager o l'interfaccia a riga di comando di ONTAP"

- "Creare un criterio di replica utilizzando System Manager o l'interfaccia a riga di comando di ONTAP"

Nota: quando si utilizza System Manager, selezionare **Asynchronous** come tipo di policy per le policy di replica e selezionare **Asynchronous** e **Backup nel cloud** per le policy di backup su oggetti.

Di seguito sono riportati alcuni comandi CLI di ONTAP di esempio che potrebbero essere utili per la creazione di criteri personalizzati. Tenere presente che è necessario utilizzare il server virtuale *admin* (VM di storage) come `<vserver_name>` in questi comandi.

Descrizione policy	Comando
Policy di snapshot semplice	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
Backup semplice sul cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Backup su cloud con DataLock e protezione ransomware	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
Backup su cloud con storage di classe archivistica	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Replica semplice su un altro sistema storage	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Per le relazioni di backup su cloud è possibile utilizzare solo le policy del vault.

Dove risiedono le policy?

I criteri di backup si trovano in posizioni diverse a seconda dell'architettura di backup che si intende utilizzare: Fan-out o Cascading. I criteri di replica e i criteri di backup non sono progettati allo stesso modo perché le repliche associano due sistemi storage ONTAP e il backup su oggetto utilizza un provider di storage come destinazione.

- Le policy di Snapshot risiedono sempre nel sistema di storage primario.
- I criteri di replica risiedono sempre nel sistema di storage secondario.
- Le policy di backup su oggetto vengono create nel sistema in cui risiede il volume di origine, ovvero il cluster primario per le configurazioni fan-out e il cluster secondario per le configurazioni a cascata.

Queste differenze sono indicate nella tabella.

Architettura	Policy di Snapshot	Policy di replica	Policy di backup
Fan-out	Primario	Secondario	Primario
Cascade	Primario	Secondario	Secondario

Pertanto, se si prevede di creare policy personalizzate quando si utilizza l'architettura a cascata, sarà necessario creare la replica e il backup su policy a oggetti sul sistema secondario in cui verranno creati i volumi replicati. Se si prevede di creare policy personalizzate quando si utilizza l'architettura fan-out, sarà necessario creare policy di replica sul sistema secondario in cui verranno creati i volumi replicati e eseguire il backup su policy a oggetti sul sistema primario.

Se si utilizzano i criteri predefiniti presenti in tutti i sistemi ONTAP, tutti i criteri sono impostati.

Si desidera creare un container di storage a oggetti personalizzato

Per impostazione predefinita, quando si creano file di backup nello storage a oggetti per un ambiente di lavoro, il servizio di backup e recovery crea il container (bucket o account di storage) per i file di backup nell'account di storage a oggetti configurato. Per impostazione predefinita, il bucket AWS o GCP è denominato "netapp-backup-<uuid>". L'account di storage Azure Blob è denominato "<uuid>".

Se si desidera utilizzare un determinato prefisso o assegnare proprietà speciali, è possibile creare il container direttamente nell'account del provider di oggetti. Se si desidera creare un container personalizzato, è necessario crearlo prima di avviare l'attivazione guidata. Il backup e recovery di BlueXP può utilizzare qualsiasi bucket e condividere. La procedura guidata di attivazione del backup rileva automaticamente i container forniti per l'account e le credenziali selezionati, in modo da poter selezionare quello che si desidera utilizzare.

Puoi creare il bucket da BlueXP o dal tuo cloud provider.

- "Crea bucket Amazon S3 da BlueXP"
- "Creare account di storage Azure Blob da BlueXP"
- "Crea bucket di storage Google Cloud da BlueXP"

Se si prevede di utilizzare un prefisso bucket diverso da "netapp-backup-xxxxxx", sarà necessario modificare le autorizzazioni S3 per il ruolo IAM del connettore.

Impostazioni benna avanzate

Se si prevede di spostare i file di backup meno recenti nello storage di archiviazione, o se si intende attivare la protezione DataLock e ransomware per bloccare i file di backup ed eseguirne la scansione per eventuali ransomware, è necessario creare il container con determinate impostazioni di configurazione:

- Lo storage di archiviazione sui bucket è attualmente supportato nello storage AWS S3 quando si utilizza ONTAP 9.10.1 o software superiore sui cluster. Per impostazione predefinita, i backup iniziano nella classe di storage S3 *Standard*. Assicurarsi di creare il bucket con le regole del ciclo di vita appropriate:
  - Sposta gli oggetti nell'intero ambito del bucket in S3 *Standard-IA* dopo 30 giorni.
  - Spostare gli oggetti con il tag "smc_push_to_archive: True" in *Glacier Flexible Retrieval* (in precedenza S3 Glacier)
- La protezione DataLock e Ransomware è supportata nell'archiviazione AWS quando si utilizza il software ONTAP 9.11.1 o versione successiva sui cluster e nell'archiviazione Azure quando si utilizza il software

ONTAP 9.12.1 o versione successiva.

- Per AWS, è necessario attivare il blocco degli oggetti sul bucket utilizzando un periodo di conservazione di 30 giorni.
- Per Azure, è necessario creare la classe di storage con il supporto dell'immutabilità a livello di versione.

Quale modalità di implementazione di BlueXP Connector si sta utilizzando

Se si utilizza già BlueXP per gestire lo storage, è già stato installato un connettore BlueXP. Se si prevede di utilizzare lo stesso connettore con il backup e ripristino di BlueXP, si è tutti impostati. Se è necessario utilizzare un connettore diverso, è necessario installarlo prima di iniziare l'implementazione del backup e ripristino.

BlueXP offre diverse modalità di implementazione che consentono di utilizzare BlueXP in modo da soddisfare i requisiti di sicurezza e di business. *Standard mode* sfrutta il layer BlueXP SaaS per fornire funzionalità complete, mentre *restricted mode* e *private mode* sono disponibili per le organizzazioni con restrizioni di connettività.

"Scopri di più sulle modalità di implementazione di BlueXP".

Supporto per siti con connettività Internet completa

Quando il backup e recovery di BlueXP viene utilizzato in un sito con connettività Internet completa (nota anche come *modalità standard* o *modalità SaaS*), puoi creare volumi replicati su qualsiasi sistema ONTAP o Cloud Volumes ONTAP on-premise gestito da BlueXP, inoltre, puoi creare file di backup sullo storage a oggetti in qualsiasi cloud provider supportato. "Consulta l'elenco completo delle destinazioni di backup supportate".

Per un elenco di posizioni dei connettori valide, fare riferimento a una delle seguenti procedure di backup per il provider cloud in cui si intende creare i file di backup. Esistono alcune limitazioni per le quali il connettore deve essere installato manualmente su una macchina Linux o implementato in uno specifico cloud provider.

- "Eseguire il backup dei dati Cloud Volumes ONTAP su Amazon S3"
- "Eseguire il backup dei dati Cloud Volumes ONTAP in Azure Blob"
- "Eseguire il backup dei dati Cloud Volumes ONTAP su Google Cloud"
- "Eseguire il backup dei dati ONTAP on-premise su Amazon S3"
- "Backup dei dati ONTAP on-premise su Azure Blob"
- "Eseguire il backup dei dati ONTAP on-premise su Google Cloud"
- "Eseguire il backup dei dati ONTAP on-premise su StorageGRID"
- "Esegui il backup da ONTAP on-premise a ONTAP S3"

Supporto per siti con connettività Internet limitata

Il backup e recovery di BlueXP può essere utilizzato in un sito con connettività Internet limitata (nota anche come *modalità limitata*) per eseguire il backup dei dati del volume. In questo caso, sarà necessario implementare BlueXP Connector nell'area cloud di destinazione.

- Puoi effettuare il backup dei dati dai sistemi ONTAP on-premise o dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali AWS su Amazon S3. "Eseguire il backup dei dati Cloud Volumes ONTAP su Amazon S3".
- Puoi effettuare il backup dei dati dai sistemi ONTAP on-premise o dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali di Azure in Azure Blob. "Eseguire il backup dei dati Cloud Volumes ONTAP

in Azure Blob".

Supporto per siti senza connessione a Internet

Il backup e recovery di BlueXP può essere utilizzato in un sito senza connettività Internet (nota anche come siti *private mode* o *dark*) per effettuare il backup dei dati dei volumi. In questo caso, sarà necessario implementare BlueXP Connector su un host Linux nello stesso sito.

- È possibile eseguire il backup dei dati dai sistemi ONTAP locali on-premise ai sistemi NetApp StorageGRID locali. "Eseguire il backup dei dati ONTAP on-premise su StorageGRID".
- Puoi effettuare il backup dei dati dai sistemi ONTAP locali on-premise ai sistemi ONTAP locali on-premise o ai sistemi Cloud Volumes ONTAP configurati per lo storage a oggetti S3. "Effettua il backup dei dati ONTAP on-premise su ONTAP S3" . ifdef::aws[]

Gestire le policy di backup per i volumi ONTAP con il backup e il ripristino BlueXP

Con il backup e il ripristino di BlueXP, puoi utilizzare i criteri di backup predefiniti forniti da NetApp per creare i tuoi backup oppure creare criteri personalizzati. Le policy regolano la frequenza, l'ora di esecuzione del backup e il numero dei file di backup che vengono conservati.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Quando si utilizza la procedura guidata di attivazione per attivare il servizio di backup e ripristino per i volumi, è possibile scegliere tra i criteri predefiniti e gli altri criteri già presenti nell'ambiente di lavoro (sistema Cloud Volumes ONTAP o ONTAP on-premise). Se si desidera utilizzare un criterio diverso da quello esistente, è possibile crearne uno prima o durante l'utilizzo della procedura guidata di attivazione.

Per informazioni sulle policy di backup predefinite fornite, fare riferimento a "Pianifica il tuo percorso di protezione" .

Il backup e recovery di BlueXP offre tre tipi di backup di dati ONTAP: Snapshot, repliche e backup sullo storage a oggetti. Le loro policy risiedono in sedi diverse, in base all'architettura che utilizzi e al tipo di backup:

Architettura	Posizione di archiviazione della policy di snapshot	Posizione di archiviazione dei criteri di replica	Backup nella posizione di storage della policy a oggetti
Fan-out	Primario	Secondario	Primario
Cascade	Primario	Secondario	Secondario

Creare criteri di backup utilizzando i seguenti strumenti a seconda dell'ambiente, delle preferenze e del tipo di protezione:

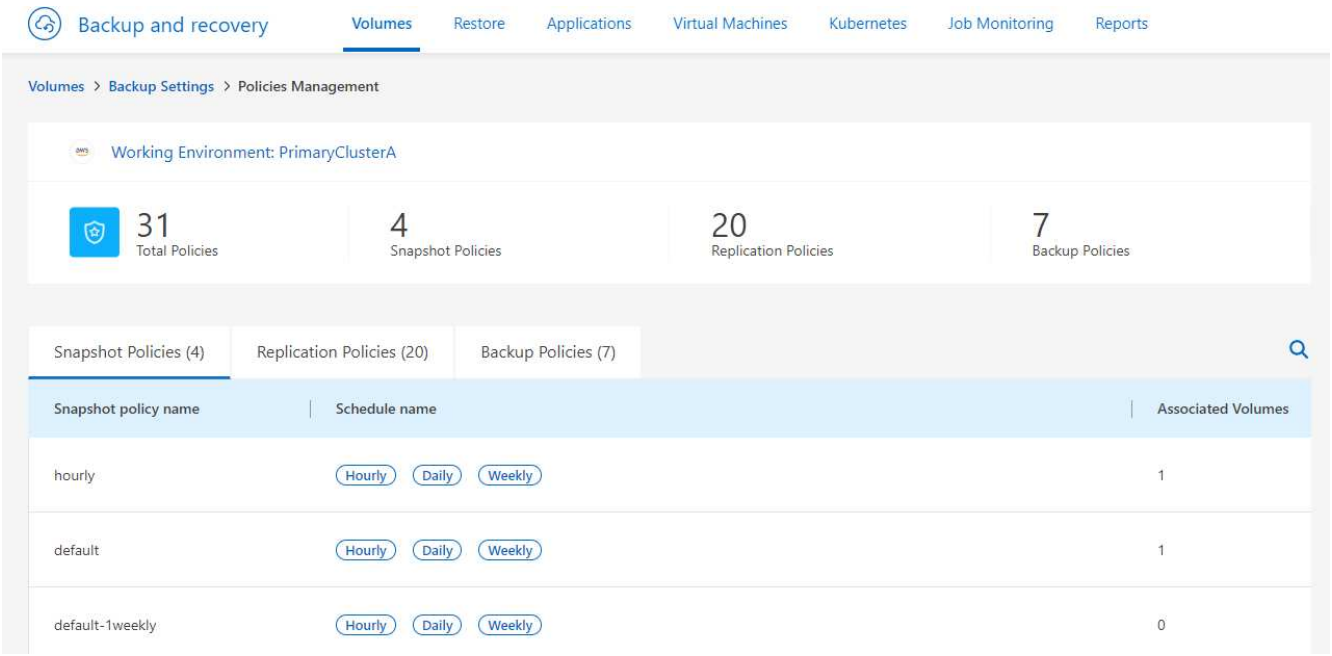
- Interfaccia utente di BlueXP
- Interfaccia utente di System Manager
- CLI ONTAP

Quando si utilizza System Manager, selezionare **asincrono** come tipo di criterio per i criteri di replica e selezionare **asincrono** e **Backup su cloud** per i criteri di backup su oggetti.

Visualizzare i criteri per un ambiente di lavoro

1. Nell'interfaccia utente di BlueXP, selezionare **volumi** > **Impostazioni di backup**.
2. Nella pagina Backup Settings (Impostazioni di backup), selezionare l'ambiente di lavoro, quindi selezionare **Actions** ••• E selezionare **Gestione criteri**.

   Viene visualizzata la pagina Gestione criteri.



   Per impostazione predefinita, le policy degli snapshot vengono visualizzate.

3. Per visualizzare altri criteri esistenti nell'ambiente di lavoro, selezionare **Criteri di replica** o **Criteri di backup**. Se è possibile utilizzare le policy esistenti per i piani di backup, è tutto impostato. Se è necessario disporre di un criterio con caratteristiche diverse, è possibile creare nuovi criteri da questa pagina.

Creare policy

È possibile creare policy che regolano le copie snapshot, le repliche e i backup nell'archiviazione di oggetti:

- Creare un criterio di snapshot prima di avviare lo snapshot
- Creare un criterio di replica prima di avviare la replica
- Creare una policy di backup sullo storage a oggetti prima di iniziare il backup

Creare un criterio di snapshot prima di avviare lo snapshot

Una parte della strategia 3-2-1 prevede la creazione di una copia istantanea del volume sul sistema di archiviazione **primario**.

Una parte del processo di creazione delle policy prevede l'identificazione delle etichette snapshot e SnapMirror che indicano la pianificazione e la conservazione. È possibile utilizzare etichette predefinite o crearne di proprie.

Fasi

1. Nell'interfaccia utente di BlueXP, selezionare **volumi** > **Impostazioni di backup**.
2. Nella pagina Backup Settings (Impostazioni di backup), selezionare l'ambiente di lavoro, quindi selezionare **Actions** ••• E selezionare **Gestione criteri**.

   Viene visualizzata la pagina Gestione criteri.

3. Nella pagina Criteri, selezionare **Crea criterio** > **Crea criterio istantanea**.
4. Specificare il nome del criterio.
5. Selezionare la pianificazione o le pianificazioni degli snapshot. È possibile avere un massimo di 5 etichette. In alternativa, creare una pianificazione.
6. Se si sceglie di creare una pianificazione:
   a. Selezionare la frequenza oraria, giornaliera, settimanale, mensile o annuale.
   b. Specificare le etichette degli snapshot che indicano la pianificazione e la conservazione.
   c. Inserisci quando e con quale frequenza verrà scattata l'istantanea.
   d. Conservazione: immettere il numero di snapshot da conservare.
7. Selezionare **Crea**.

Esempio di criterio Snapshot utilizzando un'architettura a cascata

Questo esempio crea un criterio di snapshot con due cluster:

1. Cluster 1:
   a. Selezionare Cluster 1 nella pagina dei criteri.
   b. Ignorare le sezioni dei criteri Replica e Backup su oggetto.
   c. Creare il criterio di snapshot.
2. Cluster 2:
   a. Selezionare Cluster 2 nella pagina Policy.
   b. Ignora la sezione relativa ai criteri di snapshot.
   c. Configurare i criteri di replica e backup su oggetti.

Creare un criterio di replica prima di avviare la replica

La strategia 3-2-1 potrebbe includere la replica di un volume su un sistema di storage diverso. Il criterio di replica risiede nel sistema di archiviazione **secondario**.

Fasi

1. Nella pagina Criteri, selezionare **Crea criterio** > **Crea criterio di replica**.
2. Nella sezione Dettagli policy, specificare il nome del policy.
3. Specifica le etichette SnapMirror (massimo 5) che indicano la conservazione per ciascuna etichetta.
4. Specificare la pianificazione del trasferimento.
5. Selezionare **Crea**.

Creare una policy di backup sullo storage a oggetti prima di iniziare il backup

La tua strategia 3-2-1 potrebbe includere il backup di un volume sullo storage a oggetti.

Questo criterio di storage risiede in diverse ubicazioni dei sistemi di storage, a seconda dell'architettura di backup:

- Fan-out: Sistema di storage primario
- A cascata: Sistema storage secondario

Fasi

1. Nella pagina Gestione criteri, selezionare **Crea criterio** > **Crea criterio di backup**.
2. Nella sezione Dettagli policy, specificare il nome del policy.
3. Specifica le etichette SnapMirror (massimo 5) che indicano la conservazione per ciascuna etichetta.
4. Specificare le impostazioni, incluso il programma di trasferimento e quando archiviare i backup.
5. (Facoltativo) per spostare i file di backup meno recenti in una classe di archiviazione o livello di accesso meno costosi dopo un certo numero di giorni, selezionare l'opzione **Archivio** e indicare il numero di giorni che devono trascorrere prima che i dati vengano archiviati. Immettere **0** come "Archivia dopo giorni" per inviare il file di backup direttamente all'archivio.

   "Scopri di più sulle impostazioni dello storage di archiviazione".

6. (Opzionale) per proteggere i backup dalla modifica o dall'eliminazione, selezionare l'opzione **DataLock & ransomware Protection**.

   Se il cluster utilizza ONTAP 9.11.1 o versioni successive, puoi scegliere di proteggere i backup dall'eliminazione configurando *DataLock* e *ransomware Protection*.

   "Scopri di più sulle impostazioni DataLock disponibili".

7. Selezionare **Crea**.

Modificare un criterio

È possibile modificare uno snapshot, una replica o un criterio di backup personalizzati.

La modifica del criterio di backup influisce su tutti i volumi che utilizzano tale criterio.

Fasi

1. Nella pagina Gestione criteri, selezionare il criterio, quindi selezionare **azioni** ••• E selezionare **Modifica criterio**.

   Il processo è lo stesso per i criteri di replica e backup.

2. Nella pagina Modifica criterio, apportare le modifiche.
3. Selezionare **Salva**.

Eliminazione di un criterio

È possibile eliminare criteri non associati a alcun volume.

Se un criterio è associato a un volume e si desidera eliminarlo, è necessario prima rimuoverlo dal volume.

Fasi

1. Nella pagina Gestione criteri, selezionare il criterio, quindi selezionare **azioni** ••• E selezionare **Elimina criterio istantanea**.
2. Selezionare **Delete** (Elimina).

Trova ulteriori informazioni

Per istruzioni sulla creazione di policy con System Manager o l'interfaccia a riga di comando di ONTAP, vedere quanto segue:

"Creare una policy Snapshot utilizzando System Manager"
"Creare una policy Snapshot utilizzando l'interfaccia a riga di comando di ONTAP"
"Creare un criterio di replica utilizzando System Manager"
"Creare un criterio di replica utilizzando l'interfaccia utente di ONTAP"
"Creare una policy di backup sullo storage a oggetti utilizzando System Manager"
"Creare una policy di backup sullo storage a oggetti utilizzando l'interfaccia a riga di comando di ONTAP"

Opzioni della policy di backup su oggetto nel backup e ripristino di BlueXP

Il BlueXP backup and recovery consentono di creare policy di backup con una varietà di impostazioni per i sistemi ONTAP locali e Cloud Volumes ONTAP .

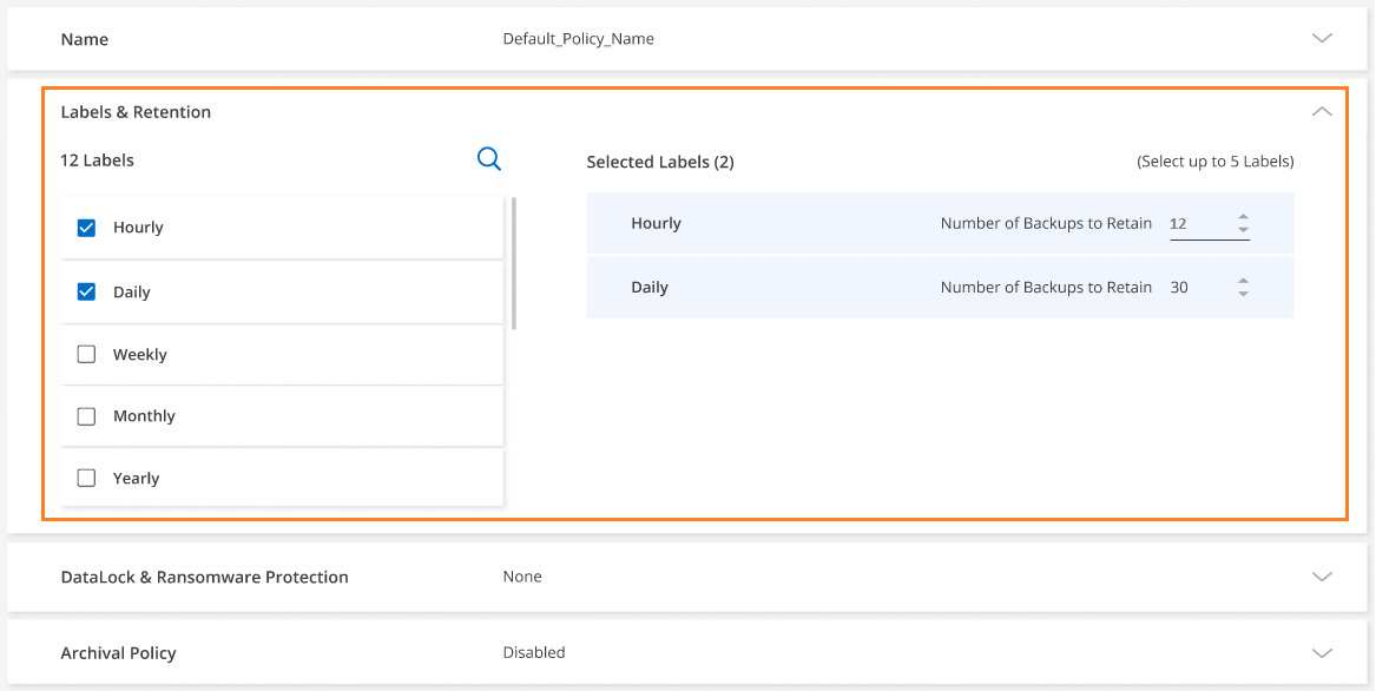
Queste impostazioni di policy sono rilevanti solo per il backup sullo storage a oggetti. Nessuna di queste impostazioni influisce sui criteri di snapshot o replica.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Opzioni di pianificazione del backup

Il backup e ripristino BlueXP consente di creare più policy di backup con pianificazioni univoche per ciascun ambiente di lavoro (cluster). È possibile assegnare criteri di backup diversi a volumi con obiettivi RPO (Recovery Point Objective) diversi.

Ogni policy di backup fornisce una sezione per *etichette e conservazione* che è possibile applicare ai file di backup. Tenere presente che il criterio Snapshot applicato al volume deve essere uno dei criteri riconosciuti dal backup di BlueXP e che i file di ripristino o di backup non verranno creati.



Il programma è suddiviso in due parti: Etichetta e valore di conservazione:

- L'etichetta * definisce la frequenza con cui viene creato (o aggiornato) un file di backup dal volume. È possibile scegliere tra i seguenti tipi di etichette:
  - È possibile scegliere una o una combinazione di, **oraria**, **giornaliera**, **settimanale**, **mensile**, e tempi **annuali**.
  - È possibile selezionare una delle policy definite dal sistema che fornisce backup e conservazione per 3 mesi, 1 anno o 7 anni.
  - Se sono state create policy di protezione del backup personalizzate sul cluster utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP, è possibile selezionare una di queste policy.
- Il valore **Retention** definisce quanti file di backup per ciascuna etichetta (periodo di tempo) vengono conservati. Una volta raggiunto il numero massimo di backup in una categoria o intervallo, i backup meno recenti vengono rimossi in modo da avere sempre i backup più aggiornati. Ciò consente anche di risparmiare sui costi di storage, poiché i backup obsoleti non continuano a occupare spazio nel cloud.

Ad esempio, supponiamo di creare una policy di backup che crei 7 backup * settimanali* e 12 backup * mensili*:

- ogni settimana e ogni mese viene creato un file di backup per il volume
- all'ottava settimana, il primo backup settimanale viene rimosso e viene aggiunto il nuovo backup settimanale per l'ottava settimana (mantenendo un massimo di 7 backup settimanali)
- al 13° mese, il primo backup mensile viene rimosso e viene aggiunto il nuovo backup mensile per il 13° mese (mantenendo un massimo di 12 backup mensili)

I backup annuali vengono eliminati automaticamente dal sistema di origine dopo il trasferimento all'archiviazione degli oggetti. Questo comportamento predefinito può essere modificato nella pagina Impostazioni avanzate dell'ambiente di lavoro.

Opzioni di protezione DataLock e ransomware

Il backup e ripristino BlueXP fornisce supporto per la protezione DataLock e ransomware per i backup dei volumi. Queste funzionalità consentono di bloccare i file di backup e di eseguirne la scansione per rilevare eventuali ransomware sui file di backup. Si tratta di un'impostazione opzionale che è possibile definire nei criteri di backup quando si desidera una protezione aggiuntiva per i backup dei volumi per un cluster.

Entrambe queste funzionalità proteggono i file di backup in modo che sia sempre disponibile un file di backup valido per il ripristino dei dati in caso di attacco ransomware ai backup. È inoltre utile soddisfare alcuni requisiti normativi in cui i backup devono essere bloccati e conservati per un certo periodo di tempo. Una volta abilitata l'opzione DataLock e protezione dal ransomware, il bucket cloud su cui viene eseguito il provisioning come parte dell'attivazione di backup e recovery di BlueXP avrà abilitato il blocco degli oggetti e la versione degli oggetti.

"Per ulteriori informazioni, consulta il blog sulla protezione di DataLock e ransomware".

Questa funzione non fornisce protezione per i volumi di origine, ma solo per i backup di tali volumi di origine. Utilizzare alcuni dei "Protezioni anti-ransomware fornite da ONTAP" per proteggere i volumi sorgente.

- Se intendi utilizzare DataLock e la protezione dal ransomware, puoi abilitarla durante la creazione della prima policy di backup e l'attivazione di backup e recovery di BlueXP per quel cluster. In seguito, puoi abilitare o disabilitare la scansione ransomware utilizzando le impostazioni avanzate di backup e ripristino di BlueXP .
- Quando BlueXP analizza un file di backup per ransomware durante il ripristino dei dati di volume, si verificheranno costi aggiuntivi in uscita dal cloud provider per accedere ai contenuti del file di backup.

Cos'è DataLock

Con questa funzionalità, è possibile bloccare gli snapshot cloud replicati tramite SnapMirror sul cloud e abilitare la funzionalità per rilevare un attacco ransomware e ripristinare una copia coerente dello snapshot nell'archivio oggetti. Questa funzionalità è supportata su AWS, Azure e StorageGRID.

DataLock protegge i file di backup da modifiche o eliminazioni per un certo periodo di tempo, denominato anche *storage immutabile*. Questa funzionalità utilizza la tecnologia del provider di storage a oggetti per il "blocco degli oggetti".

I provider cloud utilizzano una data di conservazione (RUD), calcolata in base al periodo di conservazione degli snapshot. Il periodo di conservazione degli snapshot viene calcolato in base all'etichetta e al conteggio dei dati di conservazione definiti nella policy di backup.

Il periodo minimo di conservazione degli snapshot è di 30 giorni. Diamo un'occhiata ad alcuni esempi di funzionamento:

- Se si sceglie l'etichetta **Giornaliera** con conteggio conservazione 20, il periodo di conservazione dello snapshot è di 20 giorni, che per impostazione predefinita è il minimo di 30 giorni.
- Se si sceglie l'etichetta **Settimanale** con conteggio conservazione 4, il periodo di conservazione dello snapshot è di 28 giorni, che per impostazione predefinita è il minimo di 30 giorni.
- Se si sceglie l'etichetta **Mensile** con conteggio conservazione 3, il periodo di conservazione dello snapshot è di 90 giorni.
- Se si sceglie l'etichetta **Annuale** con Conteggio conservazione 1, il periodo di conservazione dello snapshot è di 365 giorni.

Che cosa è la data di conservazione fino alla data (RUD) e come viene calcolata?

La data di conservazione fino alla data (RUD) viene determinata in base al periodo di conservazione degli snapshot. La data di conservazione fino alla data indicata viene calcolata sommando il periodo di conservazione dello snapshot e un buffer.

- Il buffer è il buffer per il tempo di trasferimento (3 giorni) + il buffer per l'ottimizzazione dei costi (28 giorni), per un totale di 31 giorni.
- La data di conservazione minima è 30 giorni + 31 giorni di buffer = 61 giorni.

Ecco alcuni esempi:

- Se si crea una pianificazione di backup mensile con 12 conservazioni, i backup vengono bloccati per 12 mesi (più 31 giorni) prima di essere eliminati (sostituiti dal file di backup successivo).
- Se si crea un criterio di backup che crea 30 backup giornalieri, 7 settimanali e 12 mensili, sono presenti tre periodi di conservazione bloccati:
  - I backup "30 giornalieri" vengono conservati per 61 giorni (30 giorni più 31 giorni di buffer),
  - I backup "settimanali" vengono conservati per 11 settimane (7 settimane più 31 giorni) e
  - I backup "mensili" vengono conservati per 12 mesi (più 31 giorni).
- Se si crea una pianificazione di backup oraria con 24 ritentions, si potrebbe pensare che i backup siano bloccati per 24 ore. Tuttavia, poiché questo è inferiore al minimo di 30 giorni, ogni backup verrà bloccato e conservato per 61 giorni (30 giorni più 31 giorni di buffer).

> I vecchi backup vengono eliminati dopo la scadenza del periodo di conservazione di DataLock, non dopo il periodo di conservazione dei criteri di backup.

L'impostazione di conservazione di DataLock sostituisce l'impostazione di conservazione dei criteri dei criteri di backup. Ciò potrebbe influire sui costi di storage, in quanto i file di backup verranno salvati nell'archivio di oggetti per un periodo di tempo più lungo.

Abilita la protezione DataLock e Ransomware

È possibile abilitare la protezione DataLock e Ransomware durante la creazione di una policy. Non è possibile abilitare, modificare o disabilitare questa opzione dopo la creazione della policy.

1. Quando si crea un criterio, espandere la sezione **Protezione DataLock e Ransomware**.
2. Scegliere una delle seguenti opzioni:
   - **Nessuno**: la protezione DataLock e la protezione ransomware sono disabilitate.
   - **Sbloccato**: la protezione DataLock e la protezione ransomware sono abilitate. Gli utenti con autorizzazioni specifiche possono sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.
   - **Bloccato**: la protezione DataLock e la protezione ransomware sono abilitate. Nessun utente può sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione. Ciò soddisfa la piena conformità normativa.

Fare riferimento alla "Come aggiornare le opzioni di protezione dal ransomware nella pagina Impostazioni avanzate".

Cos'è la protezione ransomware

La protezione ransomware esegue la scansione dei file di backup per cercare la prova di un attacco ransomware. Il rilevamento di attacchi ransomware viene eseguito utilizzando un confronto checksum. Se viene identificato un potenziale ransomware in un nuovo file di backup rispetto al file di backup precedente, il file di backup più recente viene sostituito dal file di backup più recente che non mostra segni di un attacco ransomware. (Il file identificato come un attacco ransomware viene cancellato 1 giorno dopo la sua sostituzione).

Le scansioni si verificano nelle seguenti situazioni:

- Le scansioni sugli oggetti di backup nel cloud vengono avviate subito dopo il loro trasferimento nell'archivio oggetti nel cloud. La scansione non viene eseguita sul file di backup quando viene scritto per la prima volta nell'archivio cloud, ma quando viene scritto il file di backup successivo.
- Le scansioni ransomware possono essere avviate quando il backup viene selezionato per il processo di ripristino.
- Le scansioni possono essere eseguite su richiesta in qualsiasi momento.

Come funziona il processo di recupero?

Quando viene rilevato un attacco ransomware, il servizio utilizza l'API REST di Active Data Connector Integrity Checker per avviare il processo di ripristino. La versione più vecchia degli oggetti dati è la fonte attendibile e viene convertita nella versione corrente durante il processo di ripristino.

Vediamo come funziona:

- In caso di attacco ransomware, il servizio tenta di sovrascrivere o eliminare l'oggetto nel bucket.
- Poiché l'archiviazione cloud è abilitata per il controllo delle versioni, crea automaticamente una nuova versione dell'oggetto di backup. Se un oggetto viene eliminato con il controllo delle versioni attivato, viene contrassegnato come eliminato ma è ancora recuperabile. Se un oggetto viene sovrascritto, le versioni precedenti vengono archiviate e contrassegnate.
- Quando viene avviata una scansione ransomware, i checksum vengono convalidati per entrambe le versioni dell'oggetto e confrontati. Se i checksum sono incoerenti, è stato rilevato un potenziale ransomware.
- Il processo di recupero prevede il ripristino dell'ultima copia funzionante conosciuta.

Ambienti di lavoro supportati e provider di storage a oggetti

È possibile attivare la protezione DataLock e ransomware sui volumi ONTAP dai seguenti ambienti di lavoro quando si utilizza lo storage a oggetti nei seguenti provider di cloud pubblico e privato. Ulteriori cloud provider verranno aggiunti nelle versioni future.

Ambiente di lavoro di origine	Destinazione del file di backup ifdef::aws[]
Cloud Volumes ONTAP in AWS	Amazon S3 endif::aws[] ifdef::Azure[]
Cloud Volumes ONTAP in Azure	Azure Blob endif::Azure[] ifdef::gcp[] endif::gcp[]
Sistema ONTAP on-premise	Ifdef::aws[] Amazzonia S3 endif::aws[] ifdef::Azure[] Azure Blob endif::Azure[] ifdef::gcp[] endif::gcp[] NetApp StorageGRID

Requisiti

- Per AWS:
  - I cluster devono eseguire ONTAP 9.11.1 o versione successiva
  - Il connettore può essere implementato nel cloud o on-premise
  - Le seguenti autorizzazioni S3 devono far parte del ruolo IAM che fornisce al connettore le autorizzazioni. Si trovano nella sezione "backupS3Policy" per la risorsa "arn:aws:s3:::netapp-backup-*":

    Autorizzazioni di AWS S3

    - s3:GetObjectVersionTagging
    - s3:GetBucketObjectLockConfiguration
    - s3:GetObjectVersionAcl
    - s3:PutObjectTagging
    - s3:DeleteObject
    - s3:DeleteObjectTagging
    - s3:GetObjectRetention
    - s3:DeleteObjectVersionTagging
    - s3:PutObject
    - s3:GetObject
    - s3:PutBucketObjectLockConfiguration
    - s3:GetLifecycleConfiguration
    - s3:GetBucketTagging
    - s3:DeleteObjectVersion
    - s3:ListBucketVersions
    - s3:ListBucket
    - s3:PutBucketTagging
    - s3:GetObjectTagging
    - s3:PutBucketVersioning
    - s3:PutObjectVersionTagging
    - s3:GetBucketVersioning
    - s3:GetBucketAcl
    - s3:BypassGovernanceRetention
    - s3:PutObjectRetention
    - s3:GetBucketLocation
    - s3:GetObjectVersion

    "Visualizza il formato JSON completo per la policy in cui è possibile copiare e incollare le autorizzazioni richieste".

- Per Azure:
  - I cluster devono eseguire ONTAP 9.12.1 o versione successiva
  - Il connettore può essere implementato nel cloud o on-premise
- Per StorageGRID:
  - I cluster devono eseguire ONTAP 9.11.1 o versione successiva
  - I sistemi StorageGRID devono eseguire la versione 11.6.0.3 o superiore
  - Il connettore deve essere implementato in sede (può essere installato in un sito con o senza accesso a Internet)
  - Le seguenti autorizzazioni S3 devono far parte del ruolo IAM che fornisce al connettore le autorizzazioni:

    Autorizzazioni di StorageGRID S3

    - s3:GetObjectVersionTagging
    - s3:GetBucketObjectLockConfiguration
    - s3:GetObjectVersionAcl
    - s3:PutObjectTagging
    - s3:DeleteObject
    - s3:DeleteObjectTagging
    - s3:GetObjectRetention
    - s3:DeleteObjectVersionTagging
    - s3:PutObject
    - s3:GetObject
    - s3:PutBucketObjectLockConfiguration
    - s3:GetLifecycleConfiguration
    - s3:GetBucketTagging
    - s3:DeleteObjectVersion
    - s3:ListBucketVersions
    - s3:ListBucket
    - s3:PutBucketTagging
    - s3:GetObjectTagging
    - s3:PutBucketVersioning
    - s3:PutObjectVersionTagging
    - s3:GetBucketVersioning
    - s3:GetBucketAcl
    - s3:PutObjectRetention
    - s3:GetBucketLocation
    - s3:GetObjectVersion

Restrizioni

- La funzionalità di protezione DataLock e ransomware non è disponibile se è stato configurato lo storage di archivio nel criterio di backup.
- L'opzione DataLock selezionata quando si attiva il backup e il ripristino BlueXP deve essere utilizzata per tutti i criteri di backup per quel cluster.
- Non è possibile utilizzare più modalità DataLock su un singolo cluster.
- Se si attiva DataLock, tutti i backup dei volumi verranno bloccati. Non è possibile combinare backup di volumi bloccati e non bloccati per un singolo cluster.
- La protezione DataLock e ransomware è applicabile per i nuovi backup dei volumi utilizzando una policy di backup con DataLock e la protezione ransomware attivata. È possibile abilitare o disabilitare queste funzioni in un secondo momento utilizzando l'opzione Impostazioni avanzate.
- I volumi FlexGroup possono utilizzare la protezione DataLock e ransomware solo quando si utilizza ONTAP 9.13.1 o superiore.

Suggerimenti su come ridurre i costi di DataLock

È possibile attivare o disattivare la funzione di scansione ransomware mantenendo attiva la funzione DataLock. Per evitare costi aggiuntivi, puoi disabilitare le scansioni pianificate dal ransomware. In questo modo potrai personalizzare le impostazioni di sicurezza ed evitare di sostenere i costi del cloud provider.

Anche se le scansioni pianificate anti-ransomware sono disattivate, puoi comunque eseguire scansioni on-demand quando necessario.

È possibile scegliere diversi livelli di protezione:

- **DataLock *without* ransomware scan**: Fornisce protezione per i dati di backup nello storage di destinazione che può essere in modalità Governance o Compliance.
  - **Modalità governance**: Offre agli amministratori la flessibilità di sovrascrivere o eliminare i dati protetti.
  - **Modalità conformità**: Fornisce una completa cancellabilità fino alla scadenza del periodo di conservazione. Questo consente di soddisfare i più rigorosi requisiti di sicurezza dei dati in ambienti altamente regolamentati. Non è possibile sovrascrivere o modificare i dati durante il loro ciclo di vita, offrendo il livello di protezione più elevato per le copie di backup.

    Microsoft Azure utilizza invece la modalità di blocco e sblocco.

- **DataLock *with* ransomware scans**: Fornisce un ulteriore livello di sicurezza per i tuoi dati. Questa funzione consente di rilevare eventuali tentativi di modifica delle copie di backup. In caso di tentativo, viene creata una nuova versione dei dati in modo discreto. La frequenza di scansione può essere modificata in 1, 2, 3, 4, 5, 6 o 7 giorni. Se le scansioni sono impostate su ogni 7 giorni, i costi diminuiscono significativamente.

Per ulteriori suggerimenti su come ridurre i costi di DataLock, fare riferimento a. https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-BlueXP-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475

Inoltre, è possibile ottenere stime del costo associato a DataLock visitando il sito "Calcolatore del TCO (Total Cost of Ownership) di backup e recovery di BlueXP".

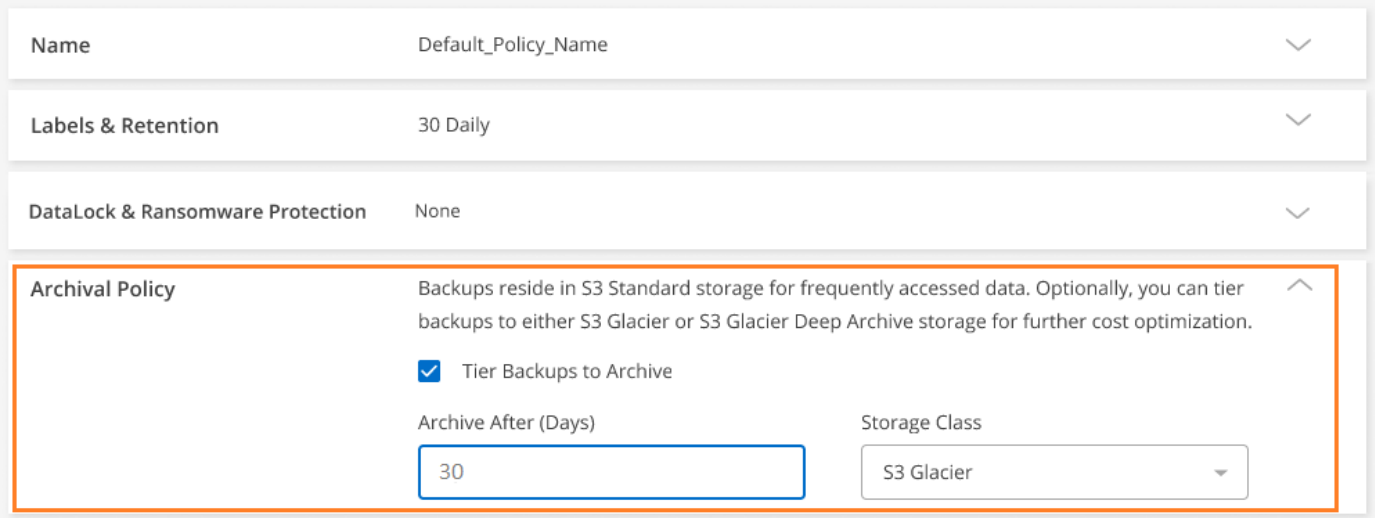
Opzioni di archiviazione

Quando si utilizza il cloud storage AWS, Azure o Google, dopo un certo numero di giorni è possibile spostare i file di backup meno recenti in una classe di archiviazione o un Tier di accesso meno costosi. Puoi anche scegliere di inviare immediatamente i file di backup allo storage di archivio senza essere scritti su cloud storage standard. È sufficiente inserire **0** come "Archivia dopo giorni" per inviare il file di backup direttamente all'archivio. Ciò può risultare particolarmente utile per gli utenti che raramente hanno bisogno di accedere ai dati da backup del cloud o per gli utenti che stanno sostituendo una soluzione di backup su nastro.

Non è possibile accedere immediatamente ai dati nei livelli di archiviazione quando necessario e richiede un costo di recupero più elevato, pertanto è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati dai file di backup prima di decidere di archiviare i file di backup.

- Anche se selezioni "0" per inviare tutti i blocchi di dati al cloud storage di archiviazione, i blocchi di metadati vengono sempre scritti nel cloud storage standard.
- Non è possibile utilizzare lo storage di archiviazione se è stato attivato DataLock.
- Non è possibile modificare il criterio di archiviazione dopo aver selezionato **0** giorni (archiviare immediatamente).

Ogni policy di backup fornisce una sezione per *Archival Policy* che è possibile applicare ai file di backup.



- In AWS, i backup iniziano nella classe di storage *Standard* e passano alla classe di storage *Standard-infrequent Access* dopo 30 giorni.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile eseguire il tiering dei backup più vecchi nello storage *S3 Glacier* o *S3 Glacier Deep Archive*. "Scopri di più sullo storage di archiviazione AWS".

  - Se non si seleziona alcun livello di archiviazione nella prima policy di backup quando si attiva il backup e ripristino BlueXP, *S3 Glacier* sarà l'unica opzione di archiviazione per le policy future.
  - Se si seleziona *S3 Glacier* nella prima policy di backup, è possibile passare al livello *S3 Glacier Deep Archive* per le policy di backup future per quel cluster.
  - Se si seleziona *S3 Glacier Deep Archive* nella prima policy di backup, tale Tier sarà l'unico Tier di archiviazione disponibile per future policy di backup per quel cluster.
- In Azure, i backup sono associati al Tier di accesso *Cool*.

Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile eseguire il tiering dei backup più vecchi allo storage *Azure Archive*. "Scopri di più sullo storage di archivio Azure".

- In GCP, i backup sono associati alla classe di storage *Standard*.

  Se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di raggruppare i backup più vecchi in storage *Archive* nell'interfaccia utente di backup e ripristino BlueXP dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sullo storage di archivio di Google".

- In StorageGRID, i backup sono associati alla classe di storage *Standard*.

  Se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza 11.4 o versione successiva, è possibile archiviare i file di backup meno recenti nello storage di archiviazione del cloud pubblico.

+ ** per AWS, è possibile eseguire il tiering dei backup nello storage AWS *S3 Glacier* o *S3 Glacier Deep Archive*. "Scopri di più sullo storage di archiviazione AWS".

+ ** per Azure, è possibile eseguire il tiering dei backup più vecchi sullo storage *Azure Archive*. "Scopri di più sullo storage di archivio Azure".

Gestisci le opzioni di archiviazione del backup su oggetto nelle Impostazioni avanzate BlueXP backup and recovery

Puoi modificare le impostazioni dello storage di backup su oggetti a livello di cluster impostate al momento dell'attivazione del backup e recovery di BlueXP per ogni sistema ONTAP usando la pagina Impostazioni avanzate. È inoltre possibile modificare alcune impostazioni applicate come impostazioni di backup predefinite. Ciò include la modifica della velocità di trasferimento dei backup nello storage a oggetti, se le copie Snapshot storiche vengono esportate come file di backup e l'attivazione o la disattivazione delle scansioni ransomware per un ambiente di lavoro.

Queste impostazioni sono disponibili solo per lo storage a oggetti di backup. Nessuna di queste impostazioni influisce sulle impostazioni di Snapshot o di replica.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Nella pagina Impostazioni avanzate è possibile modificare le seguenti opzioni:

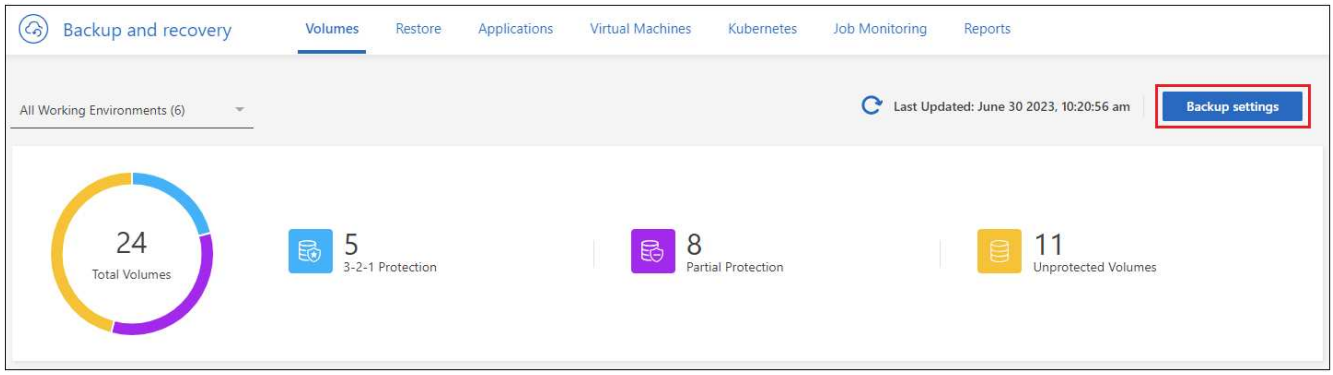
- Modifica della larghezza di banda di rete allocata per caricare i backup nell'archiviazione a oggetti utilizzando l'opzione velocità di trasferimento massima
- Modifica dell'eventuale esportazione delle copie Snapshot storiche come file di backup e inclusione nei file di backup di base iniziali per volumi futuri
- Modifica della rimozione delle snapshot "annuali" dal sistema di origine
- Abilitazione o disabilitazione delle scansioni ransomware per un ambiente di lavoro, incluse le scansioni pianificate

Visualizzare le impostazioni di backup a livello di cluster

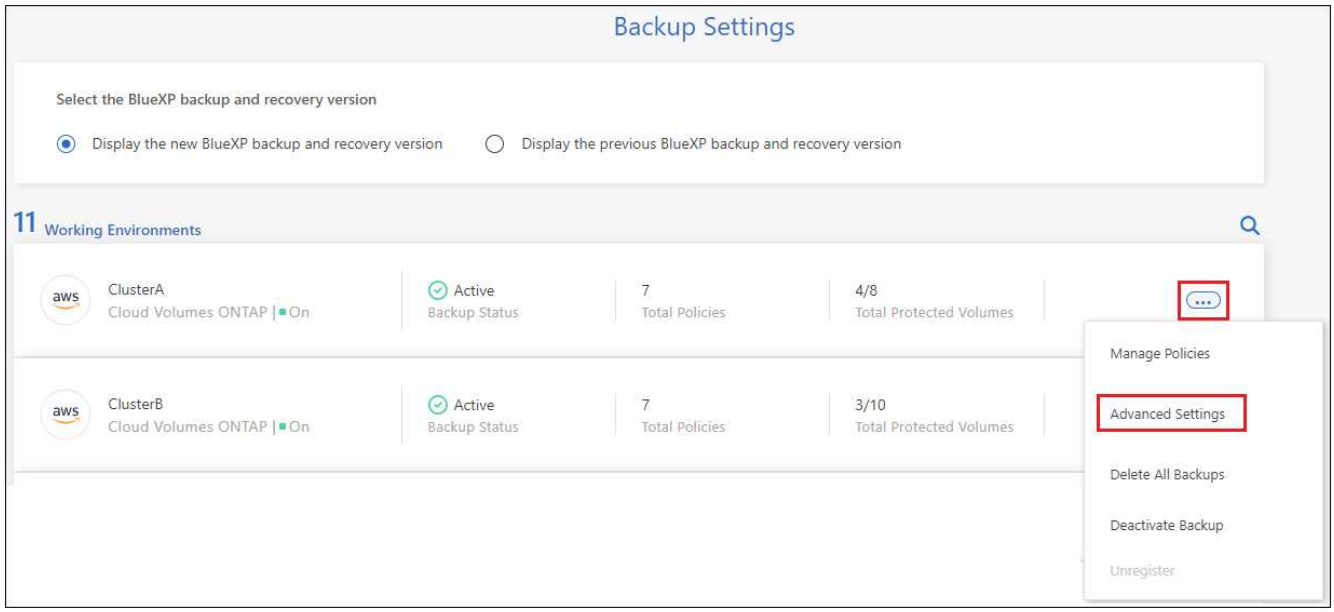
È possibile visualizzare le impostazioni di backup a livello di cluster per ciascun ambiente di lavoro.

Fasi

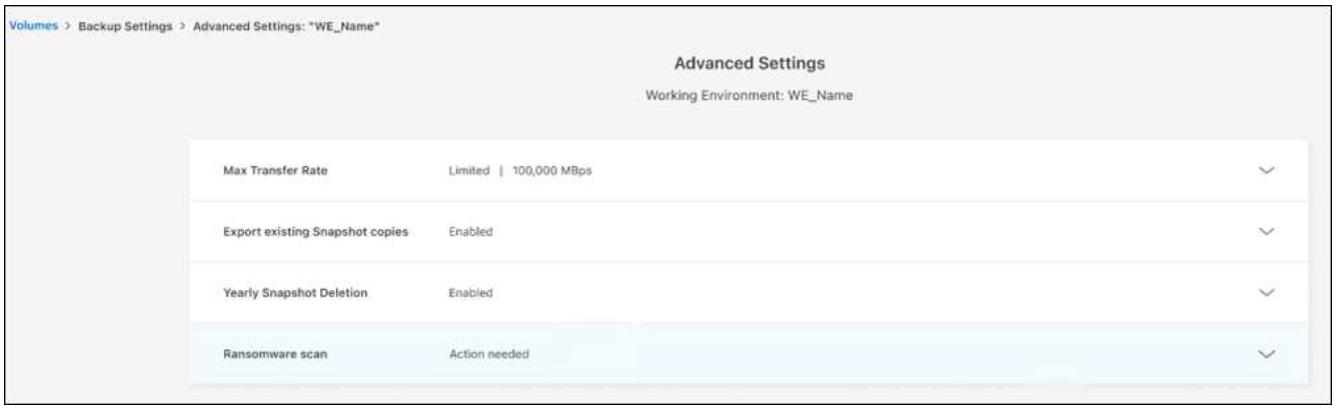
1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



3. Dalla pagina *Impostazioni di backup*, fare clic su ••• per l'ambiente di lavoro e selezionare **Impostazioni avanzate**.



Nella pagina *Advanced Settings* vengono visualizzate le impostazioni correnti dell'ambiente di lavoro.



4. Espandere l'opzione e apportare la modifica.

Tutte le operazioni di backup successive alla modifica utilizzeranno i nuovi valori.

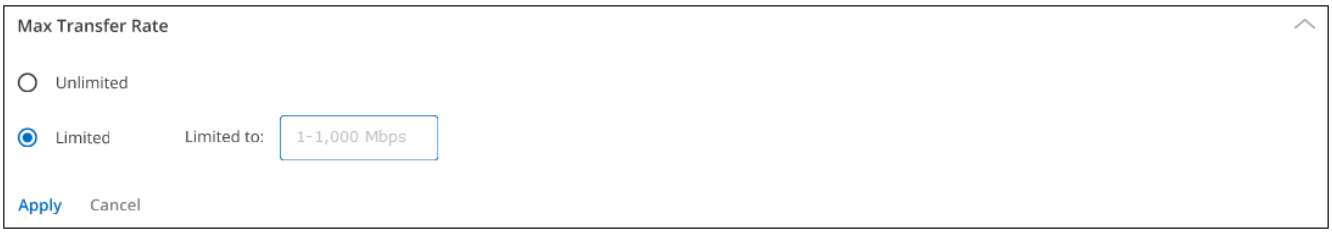
Tenere presente che alcune opzioni non sono disponibili in base alla versione di ONTAP nel cluster di origine e alla destinazione del provider cloud in cui risiedono i backup.

Modificare la larghezza di banda della rete disponibile per caricare i backup nello storage a oggetti

Quando si attiva il backup e ripristino BlueXP per un ambiente di lavoro, per impostazione predefinita, ONTAP può utilizzare una larghezza di banda illimitata per trasferire i dati di backup dai volumi dell'ambiente di lavoro allo storage a oggetti. Se si nota che il traffico di backup influisce sui normali carichi di lavoro degli utenti, è possibile ridurre la quantità di larghezza di banda utilizzata durante il trasferimento utilizzando l'opzione velocità di trasferimento massima nella pagina Impostazioni avanzate.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per l'ambiente di lavoro e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandere la sezione **velocità di trasferimento massima**.



4. Scegliere un valore compreso tra 1 e 1.000 Mbps come velocità di trasferimento massima.
5. Selezionare il pulsante di opzione **limitato** e immettere la larghezza di banda massima utilizzabile oppure selezionare **illimitato** per indicare che non esiste alcun limite.
6. Selezionare **Applica**.

Questa impostazione non influisce sulla larghezza di banda allocata ad altre relazioni di replica che possono essere configurate per i volumi nell'ambiente di lavoro.

Modifica se le copie degli snapshot storici vengono esportate come file di backup

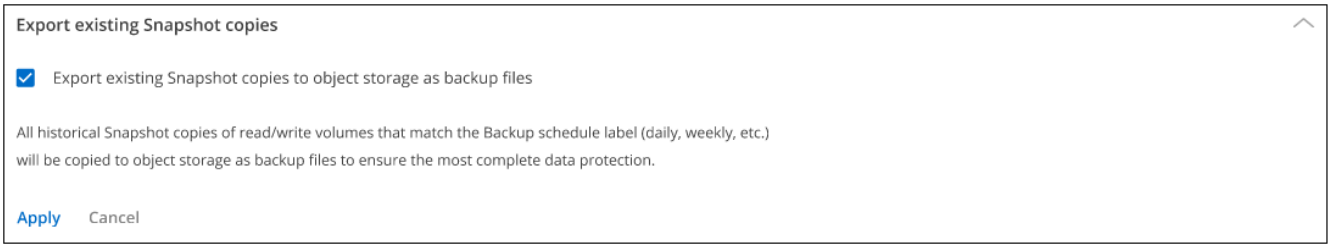
Se sono presenti copie snapshot locali per volumi che corrispondono all'etichetta di pianificazione del backup

utilizzata in questo ambiente di lavoro (ad esempio, giornaliera, settimanale, ecc.), è possibile esportare tali snapshot storici nell'archiviazione degli oggetti come file di backup. Ciò consente di inizializzare i backup nel cloud spostando le copie snapshot meno recenti nella copia di backup di riferimento.

Si noti che questa opzione si applica solo ai nuovi file di backup per nuovi volumi di lettura/scrittura e non è supportata con i volumi di data Protection (DP).

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per l'ambiente di lavoro e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandere la sezione **Esporta copie snapshot esistenti**.



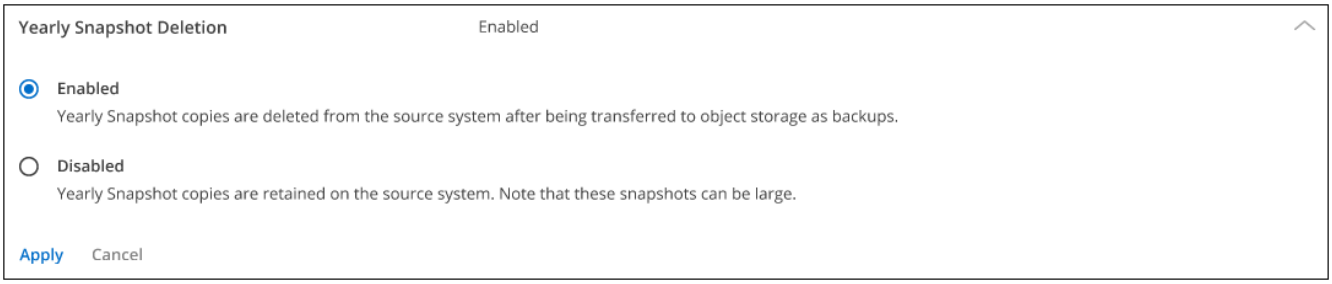
4. Selezionare se si desidera esportare le copie Snapshot esistenti.
5. Selezionare **Applica**.

Modificare se le snapshot "annuali" vengono rimosse dal sistema di origine

Quando si seleziona l'etichetta di backup "annuale" per una policy di backup per qualsiasi volume, la copia Snapshot creata è molto grande. Per impostazione predefinita, queste snapshot annuali vengono eliminate automaticamente dal sistema di origine dopo essere state trasferite allo storage a oggetti. È possibile modificare questo comportamento predefinito dalla sezione eliminazione istantanea annuale.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per l'ambiente di lavoro e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandere la sezione **eliminazione istantanea annuale**.



4. Selezionare **Disabled** (Disattivato) per conservare le istantanee annuali sul sistema di origine.
5. Selezionare **Applica**.

Abilitare o disabilitare le scansioni ransomware

Le scansioni di protezione ransomware sono abilitate per impostazione predefinita. L'impostazione predefinita per la frequenza di scansione è di 7 giorni. La scansione viene eseguita solo sull'ultima copia dello snapshot. È possibile abilitare o disabilitare le scansioni ransomware sull'ultima copia dello snapshot utilizzando l'opzione nella pagina Impostazioni avanzate. Se si attiva, le scansioni vengono eseguite ogni 7 giorni per impostazione predefinita.

Per i dettagli sulle opzioni di protezione DataLock e Ransomware, fare riferimento a "Opzioni di protezione DataLock e ransomware" .

È possibile modificare la pianificazione in giorni o settimane o disattivarla, risparmiando sui costi.

L'abilitazione delle scansioni ransomware comporterà costi aggiuntivi in base al cloud provider.

Le scansioni ransomware pianificate vengono eseguite solo sulla copia snapshot più recente.

Se le scansioni pianificate tramite ransomware sono disattivate, è comunque possibile eseguire scansioni on-demand e durante un'operazione di ripristino.

Fare riferimento a "Gestire le policy" per maggiori dettagli sulla gestione delle policy che implementano il rilevamento del ransomware.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per l'ambiente di lavoro e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandere la sezione **scansione ransomware**.
4. Abilita o disabilita la **Scansione ransomware**.
5. Selezionare **scansione ransomware pianificata**.
6. Facoltativamente, modificare la scansione predefinita ogni settimana in giorni o settimane.
7. Impostare la frequenza in giorni o settimane di esecuzione della scansione.
8. Selezionare **Applica**.

Esegui il backup dei dati di Cloud Volumes ONTAP su Amazon S3 con backup e ripristino BlueXP

Completa alcuni passaggi nel backup e ripristino di BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP su Amazon S3.

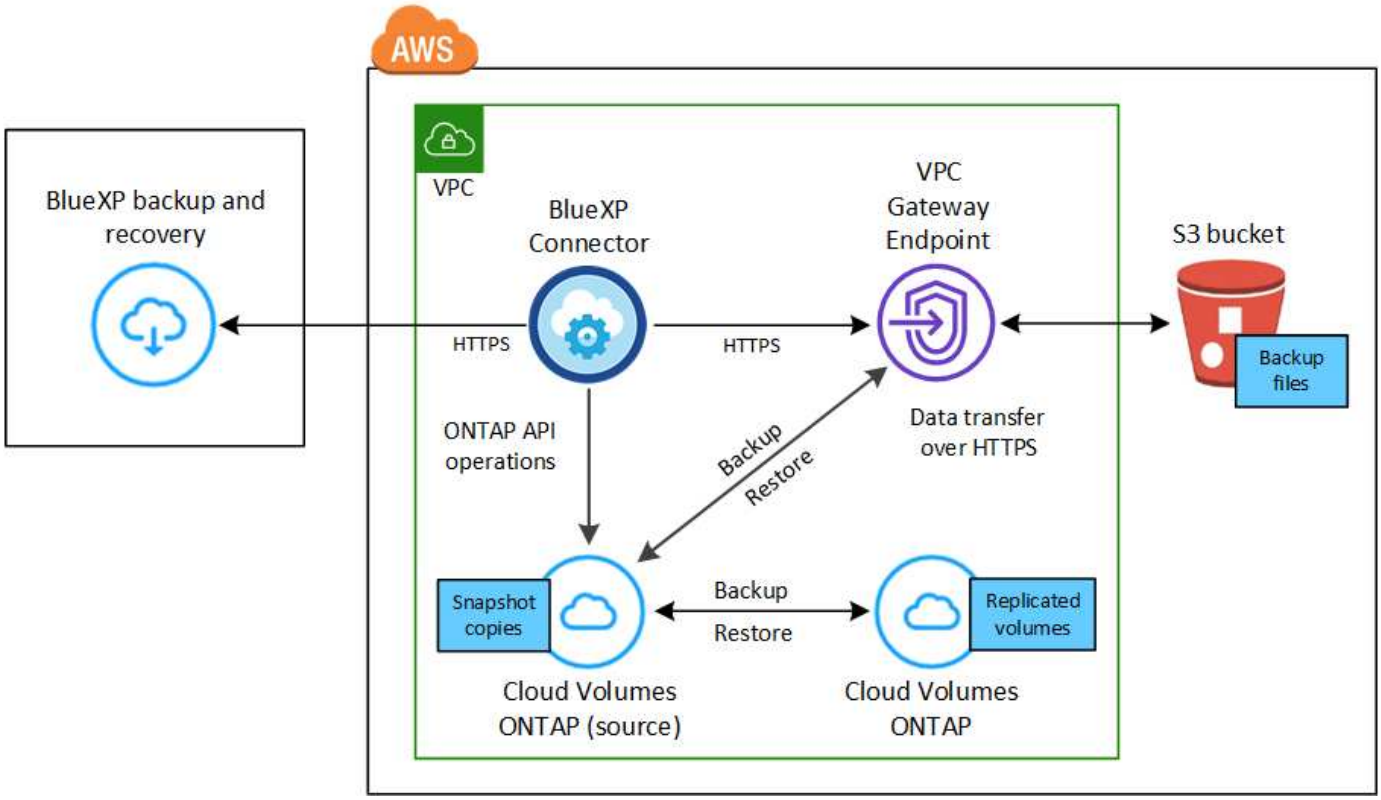
NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Verificare il supporto per la configurazione

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi in S3.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi.

In alternativa, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.



L'endpoint del gateway VPC deve già esistere nel VPC. "Scopri di più sugli endpoint gateway".

Versioni di ONTAP supportate

Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.

Informazioni richieste per l'utilizzo delle chiavi gestite dal cliente per la crittografia dei dati

Nella procedura guidata di attivazione è possibile scegliere le chiavi gestite dal cliente per la crittografia dei dati invece di utilizzare le chiavi di crittografia Amazon S3 predefinite. In questo caso, è necessario che le chiavi gestite per la crittografia siano già impostate. "Scopri come utilizzare le tue chiavi".

Verificare i requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è disponibile un abbonamento BlueXP nel marketplace AWS che consente le implementazioni di backup e ripristino di Cloud Volumes ONTAP e BlueXP. È necessario "Iscriviti a questo abbonamento BlueXP" Prima di attivare il backup e ripristino BlueXP. La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento.

Per un contratto annuale che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise, è necessario iscriversi al "Pagina AWS Marketplace" e poi "Associare l'abbonamento alle credenziali AWS".

Per un contratto annuale che consente di raggruppare backup e ripristino di Cloud Volumes ONTAP e BlueXP, è necessario impostare il contratto annuale quando si crea un ambiente di lavoro Cloud Volumes ONTAP. Questa opzione non consente di eseguire il backup dei dati on-premise.

Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL". È necessario utilizzare una licenza BYOL quando il connettore e il sistema Cloud Volumes ONTAP vengono implementati in un sito buio.

Inoltre, è necessario disporre di un account AWS per lo spazio di storage in cui verranno collocati i backup.

Preparare il connettore BlueXP

Il connettore deve essere installato in una regione AWS con accesso a Internet completo o limitato (modalità "standard" o "limitata"). "Per ulteriori informazioni, vedere modalità di implementazione di BlueXP".

- "Scopri di più sui connettori"
- "Implementare un connettore in AWS in modalità standard (accesso a Internet completo)"
- "Installazione del connettore in modalità limitata (accesso in uscita limitato)"

Verificare o aggiungere le autorizzazioni al connettore

vedere "Documentazione AWS: Modifica delle policy IAM" .

Di seguito sono riportate le autorizzazioni specifiche della policy:

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectVersionAcl",
                "s3:PutObjectTagging",
                "s3:DeleteObjectTagging",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObjectVersion",
                "s3:GetObjectTagging",
                "s3:PutBucketVersioning",
                "s3:PutObjectVersionTagging",
                "s3:GetBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
```

```
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Quando si creano backup nelle regioni AWS China, è necessario modificare il nome risorsa AWS "arn" in tutte le sezioni *Resource* delle policy IAM da "aws" a "aws-cn", ad esempio `arn:aws-cn:s3:::netapp-backup-*`.

Autorizzazioni AWS Cloud Volumes ONTAP richieste

Quando il sistema Cloud Volumes ONTAP esegue il software ONTAP 9.12.1 o versione successiva, il ruolo IAM che fornisce l'ambiente di lavoro con autorizzazioni deve includere un nuovo set di autorizzazioni S3 specifico per il backup e il ripristino BlueXP dalla versione più recente "Policy Cloud Volumes ONTAP".

Se l'ambiente di lavoro Cloud Volumes ONTAP è stato creato utilizzando BlueXP versione 3.9.23 o successiva, queste autorizzazioni dovrebbero già far parte del ruolo IAM. In caso contrario, sarà necessario aggiungere le autorizzazioni mancanti.

Regioni AWS supportate

Il backup e il ripristino di BlueXP sono supportati in tutte le regioni AWS, comprese le regioni AWS GovCloud.

Configurazione richiesta per la creazione di backup in un account AWS diverso

Per impostazione predefinita, i backup vengono creati utilizzando lo stesso account utilizzato per il sistema Cloud Volumes ONTAP. Se si desidera utilizzare un account AWS diverso per i backup, è necessario:

- Verificare che le autorizzazioni "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" facciano parte del ruolo IAM che fornisce le autorizzazioni a BlueXP Connector.
- Aggiungere le credenziali dell'account AWS di destinazione in BlueXP. "Scopri come farlo".
- Aggiungere le seguenti autorizzazioni nelle credenziali utente nel secondo account:

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea i bucket. Se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione di bucket personalizzati".

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.
- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).

Abilitare il backup e ripristino BlueXP su Cloud Volumes ONTAP

L'abilitazione del backup e ripristino BlueXP è semplice. I passaggi variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o nuovo.

Attivare il backup e il ripristino BlueXP su un nuovo sistema

Il backup e ripristino BlueXP è attivato per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Vedere "Avvio di Cloud Volumes ONTAP in AWS" Per i requisiti e i dettagli per la creazione del sistema Cloud Volumes ONTAP.

Fasi

1. Da BlueXP Canvas, selezionare **Add Working Environment** (Aggiungi ambiente di lavoro), scegliere il provider cloud e selezionare **Add New** (Aggiungi nuovo). Selezionare **Crea Cloud Volumes ONTAP**.
2. Selezionare **Amazon Web Services** come cloud provider e scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina servizi, lasciare attivato il servizio e selezionare **continua**.
5. Completare le pagine della procedura guidata per implementare il sistema.

Risultato

Il backup e ripristino BlueXP è attivato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare il BlueXP backup and recovery e "attivare il backup su ciascun volume che si desidera proteggere" .

Attivare il backup e il ripristino BlueXP su un sistema esistente

Abilitare il backup e il ripristino BlueXP su un sistema esistente in qualsiasi momento direttamente dall'ambiente di lavoro.

Fasi

1. Da BlueXP Canvas, selezionare l'ambiente di lavoro e selezionare **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.

   Se la destinazione Amazon S3 per i backup esiste come ambiente di lavoro su Canvas, puoi trascinare il cluster sull'ambiente di lavoro Amazon S3 per avviare l'installazione guidata.

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

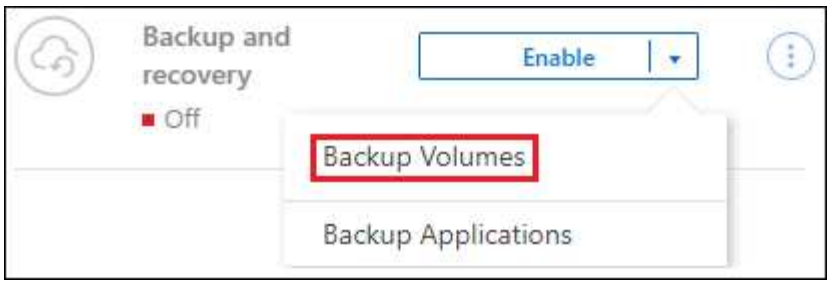
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:

   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.



Se la destinazione AWS per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster ONTAP sullo storage a oggetti AWS.

- Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare **azioni** ••• E selezionare **attiva backup** per un singolo volume (per il quale non è già stata attivata la replica o il backup nello storage a oggetti).

La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Continuare con le seguenti opzioni:
   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Per volume protetto si intende un volume con una o più delle seguenti opzioni: Policy di snapshot, policy di replica, policy di backup su oggetti.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Sia che si desideri una o tutte le opzioni di backup: Snapshot locali, replica e backup su storage a oggetti
- Architettura
- Criterio di snapshot locale
- Target e policy di replica

> Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Snapshot locali**: se si esegue una replica o un backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi nello storage a oggetti.
2. **Architettura**: Se si sceglie la replica e il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di informazioni dal sistema di storage primario al secondario e dallo storage secondario a oggetti.
   - **Fan out**: Le informazioni vengono trasmesse dal sistema di storage primario al *and* secondario dallo storage primario a quello a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   > Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Selezionare **Crea**.
4. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno.

     > Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

- Immettere il nome del criterio.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Selezionare **Crea**.

5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **Amazon Web Services**.
   - **Impostazioni provider**: Immettere i dettagli del provider e la regione in cui verranno memorizzati i backup.

     Inserire l'account AWS utilizzato per memorizzare i backup. Può trattarsi di un account diverso da quello in cui risiede il sistema Cloud Volumes ONTAP.

     Se si desidera utilizzare un account AWS diverso per i backup, è necessario aggiungere le credenziali dell'account AWS di destinazione in BlueXP e aggiungere le autorizzazioni "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" al ruolo IAM che fornisce a BlueXP le autorizzazioni.

     Selezionare la regione in cui verranno memorizzati i backup. Può trattarsi di una regione diversa da quella in cui risiede il sistema Cloud Volumes ONTAP.

     Creare un nuovo bucket o selezionarne uno esistente.

   - **Chiave di crittografia**: Se è stato creato un nuovo bucket, immettere le informazioni sulla chiave di crittografia fornite dal provider. Per gestire la crittografia dei dati, scegliere se utilizzare le chiavi di crittografia AWS predefinite o le chiavi gestite dal cliente dall'account AWS. ("Scopri come utilizzare le tue chiavi di crittografia").

     Se si sceglie di utilizzare le proprie chiavi gestite dal cliente, inserire l'archivio delle chiavi e le informazioni sulle chiavi.

     Se si sceglie un bucket esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario immetterle ora.

   - **Criterio di backup**: Selezionare un criterio di archiviazione di backup su oggetti esistente o crearne uno.

     Per creare una policy personalizzata prima di attivare il backup, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per i dettagli su DataLock e Ransomware Protection, fare riferimento a "Impostazioni dei criteri di backup su oggetti" .
     - Selezionare **Crea**.

   - **Esporta copie Snapshot esistenti nello storage a oggetti come copie di backup**: Se vi sono copie Snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliero,

settimanale, ecc.), viene visualizzata questa richiesta aggiuntiva. Selezionare questa casella per copiare tutte le istantanee storiche nello storage a oggetti come file di backup per garantire la protezione più completa per i volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati degli snapshot con un'etichetta che corrisponde alle etichette nei criteri di replicazione e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati del sistema di storage primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di storage primario contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di storage primario.

Nell'account di servizio viene creato un bucket S3 indicato dalla chiave di accesso S3 e dalla chiave segreta immessa, in cui vengono memorizzati i file di backup.

Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati di Cloud Volumes ONTAP nell'archiviazione BLOB di Azure con backup e ripristino BlueXP

Completa alcuni passaggi nel backup e ripristino di BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP all'archiviazione BLOB di Azure.

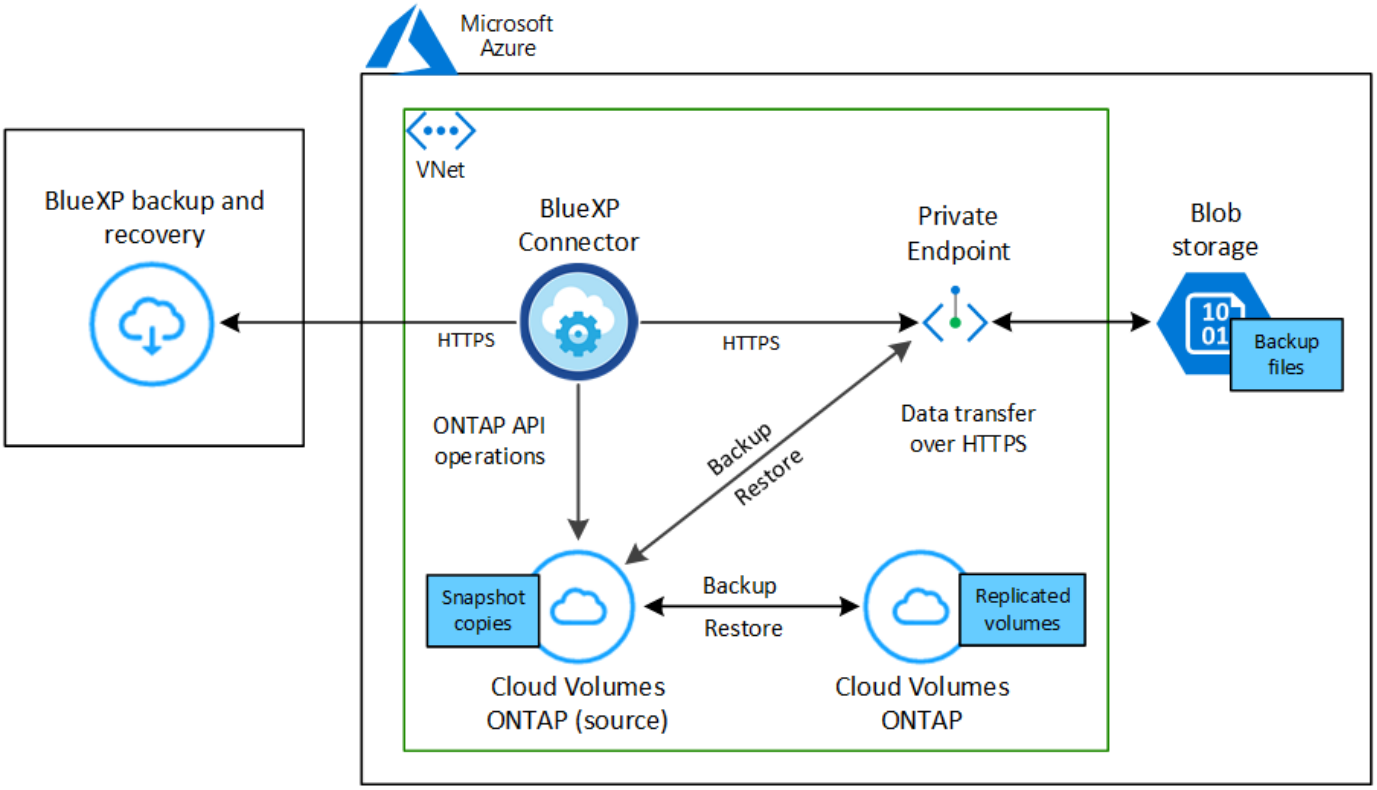
NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Verificare il supporto per la configurazione

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei volumi nello storage Azure Blob.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi.

In alternativa, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.



Versioni di ONTAP supportate

Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.

Aree Azure supportate

Il backup e il ripristino di BlueXP sono supportati in tutte le regioni di Azure, comprese le regioni di Azure Government.

Per impostazione predefinita, il backup e ripristino BlueXP esegue il provisioning del container Blob con ridondanza locale (LRS) per l'ottimizzazione dei costi. È possibile modificare questa impostazione in ZRS (zone Redundancy) dopo l'attivazione del backup e ripristino di BlueXP se si desidera garantire che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modifica della modalità di replica dell'account storage".

Configurazione richiesta per la creazione di backup in un abbonamento Azure diverso

Per impostazione predefinita, i backup vengono creati utilizzando la stessa sottoscrizione utilizzata per il sistema Cloud Volumes ONTAP.

Verificare i requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento tramite Azure Marketplace prima di attivare il backup e ripristino BlueXP. La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento. "È possibile iscriversi dalla pagina Dettagli credenziali della procedura guidata dell'ambiente di lavoro".

Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL". È necessario utilizzare una licenza BYOL quando il connettore e il sistema Cloud Volumes ONTAP sono implementati in un sito buio ("modalità privata").

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di storage in cui verranno collocati i backup.

Preparare il connettore BlueXP

Il connettore può essere installato in una regione Azure con accesso a Internet completo o limitato (modalità "standard" o "limitata"). "Per ulteriori informazioni, vedere modalità di implementazione di BlueXP".

- "Scopri di più sui connettori"
- "Implementare un connettore in Azure in modalità standard (accesso a Internet completo)"
- "Installazione del connettore in modalità limitata (accesso in uscita limitato)"

Verificare o aggiungere le autorizzazioni al connettore

Per utilizzare la funzionalità di backup e ripristino di BlueXP, è necessario disporre di autorizzazioni specifiche nel ruolo del connettore in modo che possa accedere all'area di lavoro di Azure Synapse e all'account di storage di Data Lake. Consultare le autorizzazioni riportate di seguito e seguire la procedura per modificare il criterio.

Prima di iniziare

- È necessario registrare Azure Synapse Analytics Resource Provider (chiamato "Microsoft.Synapse") con l'abbonamento. "Scopri come registrare questo provider di risorse per l'abbonamento". Per registrare il provider di risorse, è necessario essere il proprietario dell'abbonamento* o il collaboratore*.
- La porta 1433 deve essere aperta per la comunicazione tra il connettore e i servizi SQL di Azure Synapse.

Fasi

1. Identificare il ruolo assegnato alla macchina virtuale Connector:
   a. Nel portale Azure, aprire il servizio macchine virtuali.
   b. Selezionare la macchina virtuale Connector.
   c. In Impostazioni, selezionare **identità**.
   d. Selezionare **assegnazioni dei ruoli Azure**.
   e. Prendere nota del ruolo personalizzato assegnato alla macchina virtuale del connettore.
2. Aggiornare il ruolo personalizzato:

a. Nel portale Azure, apri il tuo abbonamento ad Azure.

b. Selezionare **controllo accesso (IAM) > ruoli**.

c. Selezionare i puntini di sospensione (**…**) per il ruolo personalizzato, quindi selezionare **Modifica**.

d. Selezionare **JSON** e aggiungere le seguenti autorizzazioni:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Visualizza il formato JSON completo per la policy"

e. Selezionare **Revisione + aggiornamento**, quindi selezionare **Aggiorna**.

Informazioni richieste per l'utilizzo delle chiavi gestite dal cliente per la crittografia dei dati

È possibile utilizzare le proprie chiavi gestite dal cliente per la crittografia dei dati nella procedura guidata di attivazione invece di utilizzare le chiavi di crittografia predefinite gestite da Microsoft. In questo caso, è necessario disporre dell'abbonamento Azure, del nome del vault delle chiavi e della chiave. "Scopri come utilizzare le tue chiavi".

Il backup e ripristino BlueXP supporta *le policy di accesso di Azure*, il modello di autorizzazione *Azure role-based access control* (Azure RBAC) e il *Managed hardware Security Model* (HSM) (fare riferimento alla "Che cos'è Azure Key Vault Managed HSM?").

Crea il tuo account di storage Azure Blob

Per impostazione predefinita, il servizio crea account di storage. Se si desidera utilizzare i propri account di storage, è possibile crearli prima di avviare la procedura guidata di attivazione del backup, quindi selezionare tali account di storage nella procedura guidata.

"Scopri di più sulla creazione di account storage personalizzati".

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.
- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).

Abilitare il backup e ripristino BlueXP su Cloud Volumes ONTAP

L'abilitazione del backup e ripristino BlueXP è semplice. I passaggi variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o nuovo.

Attivare il backup e il ripristino BlueXP su un nuovo sistema

Il backup e ripristino BlueXP è attivato per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Vedere "Lancio di Cloud Volumes ONTAP in Azure" Per i requisiti e i dettagli per la creazione del sistema Cloud Volumes ONTAP.

> Se si desidera selezionare il nome del gruppo di risorse, **disabilitare** il backup e il ripristino di BlueXP durante la distribuzione di Cloud Volumes ONTAP.

Fasi

1. Da BlueXP Canvas, selezionare **Add Working Environment** (Aggiungi ambiente di lavoro), scegliere il provider cloud e selezionare **Add New** (Aggiungi nuovo). Selezionare **Crea Cloud Volumes ONTAP**.
2. Selezionare **Microsoft Azure** come cloud provider e scegliere un singolo nodo o sistema ha.
3. Nella pagina Definisci credenziali di Azure, immetti il nome delle credenziali, l'ID client, il segreto client e l'ID directory, quindi seleziona **Continua**.
4. Compila la pagina Dettagli e credenziali e assicurati che sia attiva una sottoscrizione ad Azure Marketplace, quindi seleziona **Continua**.
5. Nella pagina servizi, lasciare attivato il servizio e selezionare **continua**.
6. Completare le pagine della procedura guidata per implementare il sistema.

Risultato

Il backup e ripristino BlueXP è attivato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare il BlueXP backup and recovery e "attivare il backup su ciascun volume che si desidera proteggere" .

Attivare il backup e il ripristino BlueXP su un sistema esistente

Abilitare il backup e il ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro.

Fasi

1. Da BlueXP Canvas, selezionare l'ambiente di lavoro e selezionare **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.

   Se la destinazione di Azure Blob per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster nell'ambiente di lavoro di Azure Blob per avviare l'installazione guidata.

2. Completare le pagine della procedura guidata per implementare il backup e il ripristino BlueXP.
3. Per avviare i backup, continuare con Attivare i backup sui volumi ONTAP.

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:

   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.

     Se la destinazione di Azure per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster ONTAP sullo storage a oggetti di Azure Blob.

   - Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare **azioni** ••• E selezionare **attiva backup** per un singolo volume (che non ha già attivato la replica o il backup nell'archiviazione a oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Continuare con le seguenti opzioni:
   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Un volume protetto presenta uno o più dei seguenti elementi: Policy di snapshot, policy di replica, policy di backup su oggetto.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare All FlexVol Volumes (tutti i volumi). (I volumi FlexGroup possono essere selezionati solo uno alla volta.) Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Target e policy di replica

> Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Snapshot locali**: se si esegue una replica o un backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi nello storage a oggetti.
2. **Architettura**: Se si sceglie la replica e il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di informazioni dal sistema di storage primario al secondario e dallo storage secondario a oggetti.
   - **Fan out**: Le informazioni vengono trasmesse dal sistema di storage primario al *and* secondario dallo storage primario a quello a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno.

   > Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Selezionare **Crea**.
4. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno.

Per creare una policy personalizzata prima di attivare la replica, fare riferimento a "Creare un criterio" .

Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

- Immettere il nome del criterio.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Selezionare **Crea**.

5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **Microsoft Azure**.
   - **Impostazioni provider**: Inserire i dettagli del provider.

     Inserire la regione in cui verranno memorizzati i backup. Può trattarsi di una regione diversa da quella in cui risiede il sistema Cloud Volumes ONTAP.

     Creare un nuovo account storage o selezionarne uno esistente.

     Inserire l'abbonamento Azure utilizzato per memorizzare i backup. Può trattarsi di un abbonamento diverso da quello in cui risiede il sistema Cloud Volumes ONTAP.

     Creare il proprio gruppo di risorse che gestisce il contenitore Blob oppure selezionare il tipo e il gruppo di risorse.

     Se si desidera proteggere i file di backup da modifiche o eliminazioni, assicurarsi che l'account di storage sia stato creato con lo storage immutabile abilitato utilizzando un periodo di conservazione di 30 giorni.

     Se si desidera eseguire il tiering dei file di backup più vecchi in Azure Archive Storage per un'ulteriore ottimizzazione dei costi, assicurarsi che l'account di storage disponga della regola del ciclo di vita appropriata.

   - **Chiave di crittografia**: Se è stato creato un nuovo account di storage Azure, immettere le informazioni sulla chiave di crittografia fornite dal provider. Per gestire la crittografia dei dati, scegli se utilizzare le chiavi di crittografia predefinite di Azure o le chiavi gestite dal cliente dall'account Azure.

     Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere l'archivio chiavi e le informazioni sulla chiave. "Scopri come utilizzare le tue chiavi" .

     Se si sceglie un account di storage Microsoft esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario immetterle ora.

   - **Rete**: Scegliere IPSpace e scegliere se si desidera utilizzare un endpoint privato. L'endpoint privato è disattivato per impostazione predefinita.
     i. IPSpace nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
     ii. Facoltativamente, scegli se utilizzerai un endpoint privato di Azure configurato in precedenza. "Scopri come utilizzare un endpoint privato Azure" .
   - **Criterio di backup**: Selezionare un criterio di archiviazione backup su oggetti esistente.

Per creare una policy personalizzata prima di attivare il backup, fare riferimento a "Creare un criterio" .

Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

- Immettere il nome del criterio.
- Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per i dettagli su DataLock e Ransomware Protection, fare riferimento a "Impostazioni dei criteri di backup su oggetti" .
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Selezionare **Crea**.

◦ **Esporta copie snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti copie snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliero, settimanale, ecc.), viene visualizzato questo messaggio aggiuntivo. Selezionare questa casella per copiare tutte le istantanee storiche nello storage a oggetti come file di backup per garantire la protezione più completa per i volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo, vengono create istantanee con un'etichetta che corrisponde alle etichette dei criteri di replica e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati del sistema di storage primario. I trasferimenti successivi contengono copie differenziali dei dati dello storage primario contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume primario.

Nel gruppo di risorse inserito viene creato un contenitore di storage Blob e i file di backup vengono memorizzati in tale gruppo.

Per impostazione predefinita, il backup e ripristino BlueXP esegue il provisioning del container Blob con ridondanza locale (LRS) per l'ottimizzazione dei costi. È possibile modificare questa impostazione in ZRS (zone Redundancy, ridondanza di zona) se si desidera assicurarsi che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modifica della modalità di replica dell'account storage".

Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Quali sono le prossime novità?

- È possibile "gestire i file di backup e le policy di backup". Ciò include l'avvio e l'arresto dei backup, l'eliminazione dei backup, l'aggiunta e la modifica della pianificazione di backup e molto altro ancora.
- È possibile "gestire le impostazioni di backup a livello di cluster". Ciò include la modifica delle chiavi di storage utilizzate da ONTAP per accedere allo storage cloud, la modifica della larghezza di banda della rete disponibile per caricare i backup nello storage a oggetti, la modifica dell'impostazione di backup automatico per i volumi futuri e molto altro ancora.
- Puoi anche "ripristinare volumi, cartelle o singoli file da un file di backup" a un sistema Cloud Volumes ONTAP in AWS oppure a un sistema ONTAP locale.

Esegui il backup dei dati di Cloud Volumes ONTAP su Google Cloud Storage con backup e ripristino BlueXP

Completa alcuni passaggi del backup e del ripristino BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP su Google Cloud Storage.

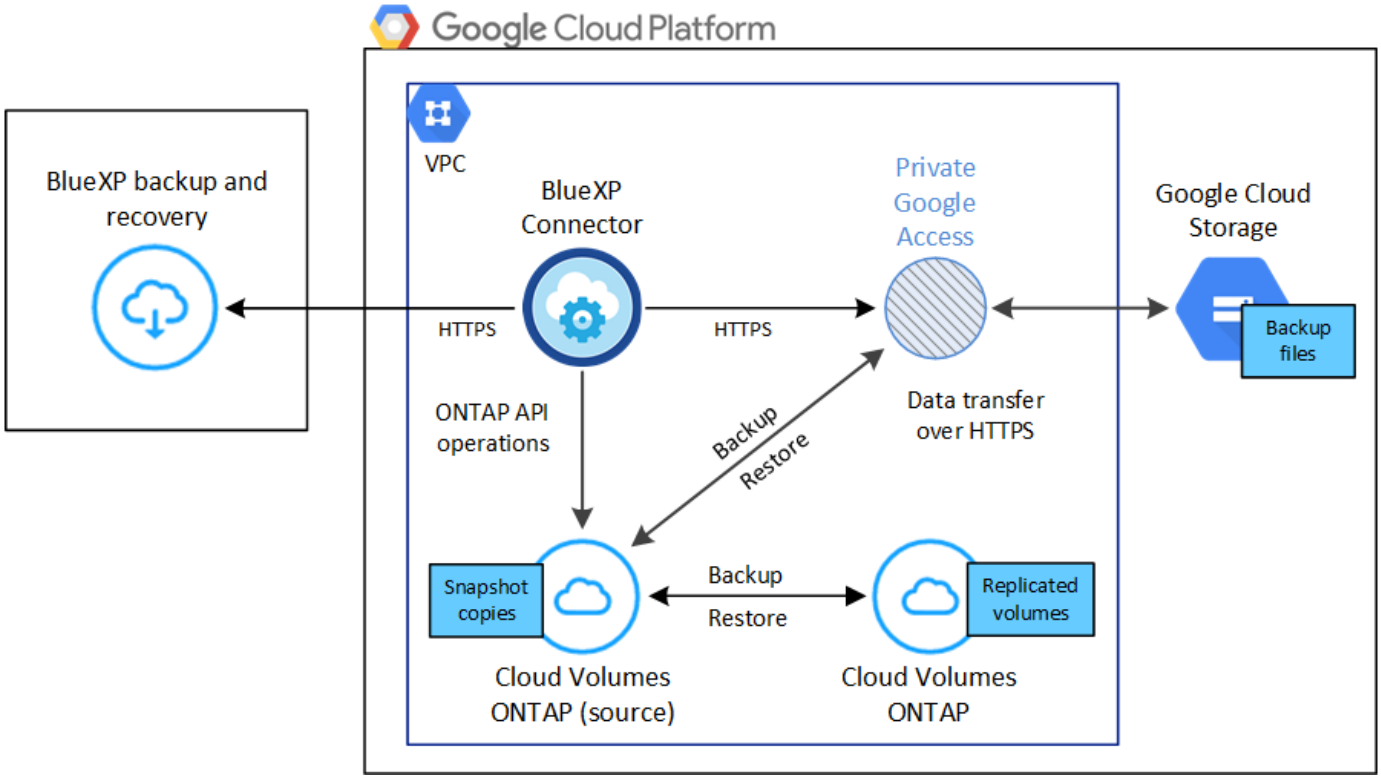
NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Verificare il supporto per la configurazione

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei volumi su Google Cloud Storage.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi.

In alternativa, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.



Versioni di ONTAP supportate

Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.

Regioni GCP supportate

Il backup e il ripristino di BlueXP sono supportati in tutte le regioni GCP.

Account di servizio GCP

Devi disporre di un account di servizio nel tuo Google Cloud Project che abbia il ruolo personalizzato. "Scopri come creare un account di servizio"

Il ruolo di amministratore dello storage non è più necessario per l'account di servizio che abilita il backup e recovery di BlueXP per accedere ai bucket Google Cloud Storage.

Verificare i requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è disponibile un abbonamento BlueXP nel Google Marketplace che consente le implementazioni di backup e ripristino di Cloud Volumes ONTAP e BlueXP. È necessario "Iscriviti a questo abbonamento BlueXP" Prima di attivare il backup e ripristino BlueXP. La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento. "È possibile iscriversi dalla pagina Dettagli credenziali della procedura guidata dell'ambiente di lavoro".

Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL".

Inoltre, è necessario disporre di un abbonamento Google per lo spazio di storage in cui verranno collocati i backup.

Preparare il connettore BlueXP

Il connettore deve essere installato in una regione Google con accesso a Internet.

- "Scopri di più sui connettori"
- "Implementare un connettore in Google Cloud"

Verificare o aggiungere le autorizzazioni al connettore

Per utilizzare la funzionalità di backup e ripristino di BlueXP, è necessario disporre di autorizzazioni specifiche nel ruolo del connettore in modo che possa accedere al servizio Google Cloud BigQuery. Consultare le autorizzazioni riportate di seguito e seguire la procedura per modificare il criterio.

Fasi

1. In "Console Google Cloud", Accedere alla pagina **ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, selezionare il progetto o l'organizzazione che contiene il ruolo che si desidera modificare.
3. Selezionare un ruolo personalizzato.
4. Selezionare **Edit role** (Modifica ruolo) per aggiornare le autorizzazioni del ruolo.
5. Selezionare **Add Permissions** (Aggiungi permessi) per aggiungere le seguenti nuove autorizzazioni al ruolo.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Selezionare **Aggiorna** per salvare il ruolo modificato.

Informazioni richieste per l'utilizzo delle chiavi di crittografia gestite dal cliente (CMEK)

È possibile utilizzare le proprie chiavi gestite dal cliente per la crittografia dei dati invece di utilizzare le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi cross-region che cross-project, in modo da poter scegliere un progetto per un bucket diverso dal progetto della chiave CMEK. Se stai pensando di utilizzare le tue chiavi gestite dal cliente:

- Per aggiungere queste informazioni nell'attivazione guidata, è necessario disporre di Key Ring e Key Name (Nome chiave). "Scopri di più sulle chiavi di crittografia gestite dal cliente".
- È necessario verificare che le autorizzazioni richieste siano incluse nel ruolo del connettore:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- È necessario verificare che l'API "Cloud Key Management Service (KMS)" di Google sia attivata nel progetto. Per "Documentazione di Google Cloud: Abilitazione delle API" ulteriori informazioni, vedere la .

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate dall'hardware) che quelle generate dal software.
- Sono supportate entrambe le chiavi Cloud KMS appena create o importate.
- Sono supportate solo le chiavi regionali; le chiavi globali non sono supportate.
- Attualmente, è supportato solo lo scopo di "crittografia/decrittografia simmetrica".
- All'agente di servizio associato all'account di storage viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (role/cloudkms.cryptKeyEncrypterDecrypter)" dal backup e ripristino BlueXP.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea i bucket. Se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione di bucket personalizzati".

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).

Abilitare il backup e ripristino BlueXP su Cloud Volumes ONTAP

I passaggi per l'abilitazione BlueXP backup and recovery variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Attivare il backup e il ripristino BlueXP su un nuovo sistema

È possibile attivare il backup e il ripristino BlueXP al termine della procedura guidata dell'ambiente di lavoro per creare un nuovo sistema Cloud Volumes ONTAP.

È necessario disporre di un account di servizio già configurato. Se non si seleziona un account di servizio quando si crea il sistema Cloud Volumes ONTAP, è necessario spegnere il sistema e aggiungere l'account di servizio a Cloud Volumes ONTAP dalla console GCP.

Vedere "Avvio di Cloud Volumes ONTAP in GCP" Per i requisiti e i dettagli per la creazione del sistema Cloud Volumes ONTAP.

Fasi

1. Da BlueXP Canvas, selezionare **Add Working Environment** (Aggiungi ambiente di lavoro), scegliere il provider cloud e selezionare **Add New** (Aggiungi nuovo). Selezionare **Crea Cloud Volumes ONTAP**.
2. **Scegli una località**: Seleziona **Google Cloud Platform**.
3. **Choose Type** (Scegli tipo): Selezionare **Cloud Volumes ONTAP** (nodo singolo o alta disponibilità).
4. **Dettagli e credenziali**: Inserire le seguenti informazioni:
   a. Fare clic su **Edit Project** (Modifica progetto) e selezionare un nuovo progetto se quello che si desidera utilizzare è diverso dal progetto predefinito (dove si trova il connettore).
   b. Specificare il nome del cluster.
   c. Attivare l'opzione **account servizio** e selezionare l'account servizio con il ruolo di amministratore dello storage predefinito. Questo è necessario per abilitare i backup e il tiering.
   d. Specificare le credenziali.

      Assicurarsi che sia disponibile un abbonamento a GCP Marketplace.
5. **Servizi**: Lasciare attivato il servizio di backup e ripristino BlueXP e fare clic su **continua**.
6. Completare le pagine della procedura guidata per implementare il sistema come descritto in "Avvio di Cloud Volumes ONTAP in GCP".

Risultato

Il backup e ripristino BlueXP è attivato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare il BlueXP backup and recovery e "attivare il backup su ciascun volume che si desidera proteggere" .

Attivare il backup e il ripristino BlueXP su un sistema esistente

È possibile abilitare il backup e il ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro.

Fasi

1. Da BlueXP Canvas, selezionare l'ambiente di lavoro e selezionare **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.

Se la destinazione di Google Cloud Storage per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster sull'ambiente di lavoro di Google Cloud Storage per avviare la procedura di installazione guidata.

Preparare Google Cloud Storage come destinazione di backup

La preparazione di Google Cloud Storage come destinazione di backup prevede i seguenti passaggi:

- Impostare le autorizzazioni.
- (Facoltativo) Crea i tuoi bucket. (Il servizio creerà i bucket per te, se lo desideri).
- (Facoltativo) impostare le chiavi gestite dal cliente per la crittografia dei dati

Impostare le autorizzazioni

È necessario fornire chiavi di accesso allo storage per un account di servizio che disponga di autorizzazioni specifiche utilizzando un ruolo personalizzato. Un account di servizio consente il backup e il recovery di BlueXP per autenticare e accedere ai bucket Cloud Storage utilizzati per memorizzare i backup. Le chiavi sono necessarie in modo che Google Cloud Storage sappia chi sta effettuando la richiesta.

Fasi

1. In "Console Google Cloud", Accedere alla pagina **ruoli**.
2. "Creare un nuovo ruolo" con le seguenti autorizzazioni:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Nella console di Google Cloud, "Accedere alla pagina Service accounts (account servizio)".
4. Seleziona il tuo progetto Cloud.
5. Selezionare **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**: Seleziona il ruolo personalizzato appena creato.
   c. Selezionare **fine**.
6. Passare a. "Impostazioni storage GCP" e creare le chiavi di accesso per l'account di servizio:
   a. Selezionare un progetto e scegliere **interoperabilità**. Se non è già stato fatto, selezionare **Enable Interoperability access** (attiva accesso all'interoperabilità).

b. In **chiavi di accesso per gli account di servizio**, selezionare **Crea una chiave per un account di servizio**, selezionare l'account di servizio appena creato e fare clic su **Crea chiave**.

   Quando si configura il servizio di backup, sarà necessario inserire le chiavi in BlueXP backup and Recovery in un secondo momento.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea i bucket. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione di bucket personalizzati".

Impostare le chiavi di crittografia gestite dal cliente (CMEK) per la crittografia dei dati

È possibile utilizzare le proprie chiavi gestite dal cliente per la crittografia dei dati invece di utilizzare le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi cross-region che cross-project, in modo da poter scegliere un progetto per un bucket diverso dal progetto della chiave CMEK.

Se stai pensando di utilizzare le tue chiavi gestite dal cliente:

- Per aggiungere queste informazioni nell'attivazione guidata, è necessario disporre di Key Ring e Key Name (Nome chiave). "Scopri di più sulle chiavi di crittografia gestite dal cliente".
- È necessario verificare che le autorizzazioni richieste siano incluse nel ruolo del connettore:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- È necessario verificare che l'API "Cloud Key Management Service (KMS)" di Google sia attivata nel progetto. Per "Documentazione di Google Cloud: Abilitazione delle API" ulteriori informazioni, vedere la .

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (hardware-backed) che quelle generate dal software.
- Sono supportate entrambe le chiavi Cloud KMS appena create o importate.
- Sono supportate solo le chiavi regionali, le chiavi globali non sono supportate.
- Attualmente, è supportato solo lo scopo di "crittografia/decrittografia simmetrica".
- All'agente di servizio associato all'account di storage viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (role/cloudkms.cryptKeyEncrypterDecrypter)" dal backup e ripristino BlueXP.

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:

   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.

     Se la destinazione GCP per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster ONTAP sullo storage a oggetti GCP.

   - Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare **azioni** ••• E selezionare **attiva backup** per un singolo volume (che non ha già attivato la replica o il backup nell'archiviazione a oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Continuare con le seguenti opzioni:
   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Per volume protetto si intende un volume con una o più delle seguenti opzioni: Policy di snapshot, policy di replica, policy di backup su oggetti.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se per i volumi selezionati sono già state applicate le policy di snapshot o replica, le policy selezionate in seguito sovrascriveranno quelle esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Sia che si desideri una o tutte le opzioni di backup: Snapshot locali, replica e backup su storage a oggetti
- Architettura
- Criterio di snapshot locale
- Target e policy di replica

> Se i volumi scelti hanno policy di replica e snapshot diverse da quelle selezionate in questa fase, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Snapshot locali**: se si esegue una replica o un backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi nello storage a oggetti.
2. **Architettura**: Se si sceglie la replica e il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di informazioni dal sistema di storage primario al secondario e dallo storage secondario a oggetti.
   - **Fan out**: Le informazioni vengono trasmesse dal sistema di storage primario al *and* secondario dallo storage primario a quello a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno.

   > Per creare una policy personalizzata prima di attivare il backup, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

- Immettere il nome del criterio.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Selezionare **Crea**.

4. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Selezionare **Crea**.
5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **Google Cloud**.
   - **Impostazioni provider**: Immettere i dettagli del provider e la regione in cui verranno memorizzati i backup.

     Creare un nuovo bucket o selezionarne uno esistente.
   - **Chiave di crittografia**: Se è stato creato un nuovo bucket Google, immettere le informazioni sulla chiave di crittografia fornite dal provider. Per gestire la crittografia dei dati, scegli se utilizzare le chiavi di crittografia predefinite di Google Cloud o le chiavi gestite dal cliente dall'account Google.

     Se si sceglie di utilizzare le proprie chiavi gestite dal cliente, inserire l'archivio delle chiavi e le informazioni sulle chiavi.

     Se hai scelto un bucket Google Cloud esistente, le informazioni sulla crittografia sono già disponibili, quindi non devi immetterle ora.
   - **Criterio di backup**: Selezionare un criterio di archiviazione di backup su oggetti esistente o crearne uno.

     Per creare una policy personalizzata prima di attivare il backup, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Selezionare **Crea**.
   - **Esporta copie Snapshot esistenti nello storage a oggetti come copie di backup**: Se vi sono copie Snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di

pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliero, settimanale, ecc.), viene visualizzata questa richiesta aggiuntiva. Selezionare questa casella per copiare tutte le istantanee storiche nello storage a oggetti come file di backup per garantire la protezione più completa per i volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo, vengono create istantanee con un'etichetta che corrisponde alle etichette dei criteri di replica e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati del sistema di storage primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di storage primario contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume del sistema di storage primario.

Viene creato un bucket di Google Cloud Storage nell'account di servizio indicato dalla chiave di accesso e dalla chiave segreta di Google immessi e i file di backup vengono memorizzati in tale account.

Per impostazione predefinita, i backup sono associati alla classe di storage *Standard*. È possibile utilizzare le classi di storage *Nearline*, *Coldline* o *Archive* a basso costo. Tuttavia, la classe di storage viene configurata tramite Google, non tramite l'interfaccia utente di backup e ripristino di BlueXP. Consulta l'argomento di Google "Modifica della classe di storage predefinita di un bucket" per ulteriori informazioni.

Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Quali sono le prossime novità?

- È possibile "gestire i file di backup e le policy di backup". Ciò include l'avvio e l'arresto dei backup, l'eliminazione dei backup, l'aggiunta e la modifica della pianificazione di backup e molto altro ancora.

- È possibile "gestire le impostazioni di backup a livello di cluster". Ciò include la modifica delle chiavi di storage utilizzate da ONTAP per accedere allo storage cloud, la modifica della larghezza di banda della rete disponibile per caricare i backup nello storage a oggetti, la modifica dell'impostazione di backup automatico per i volumi futuri e molto altro ancora.
- Puoi anche "ripristinare volumi, cartelle o singoli file da un file di backup" a un sistema Cloud Volumes ONTAP in AWS oppure a un sistema ONTAP locale.

Esegui il backup dei dati ONTAP locali su Amazon S3 con backup e ripristino BlueXP

Completa alcuni passaggi del backup e del ripristino BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali a un sistema di archiviazione secondario e all'archiviazione cloud Amazon S3.

I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

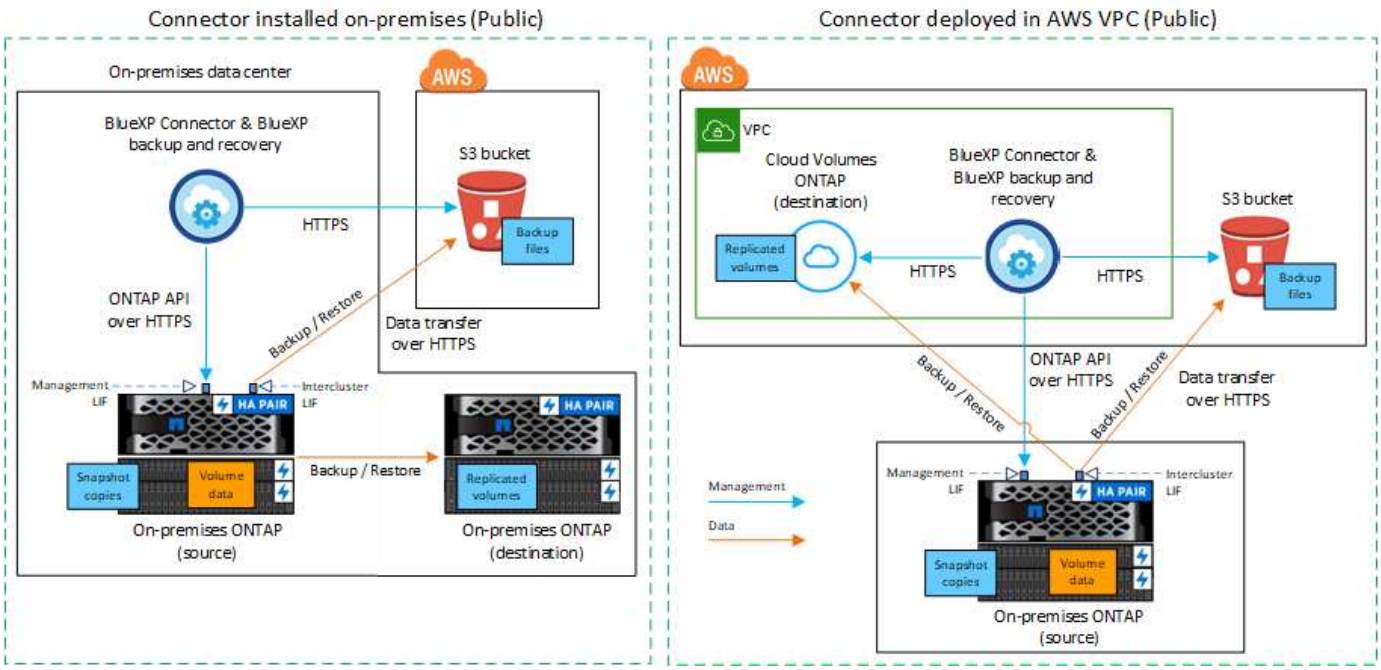
Identificare il metodo di connessione

Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup da sistemi ONTAP on-premise ad AWS S3.

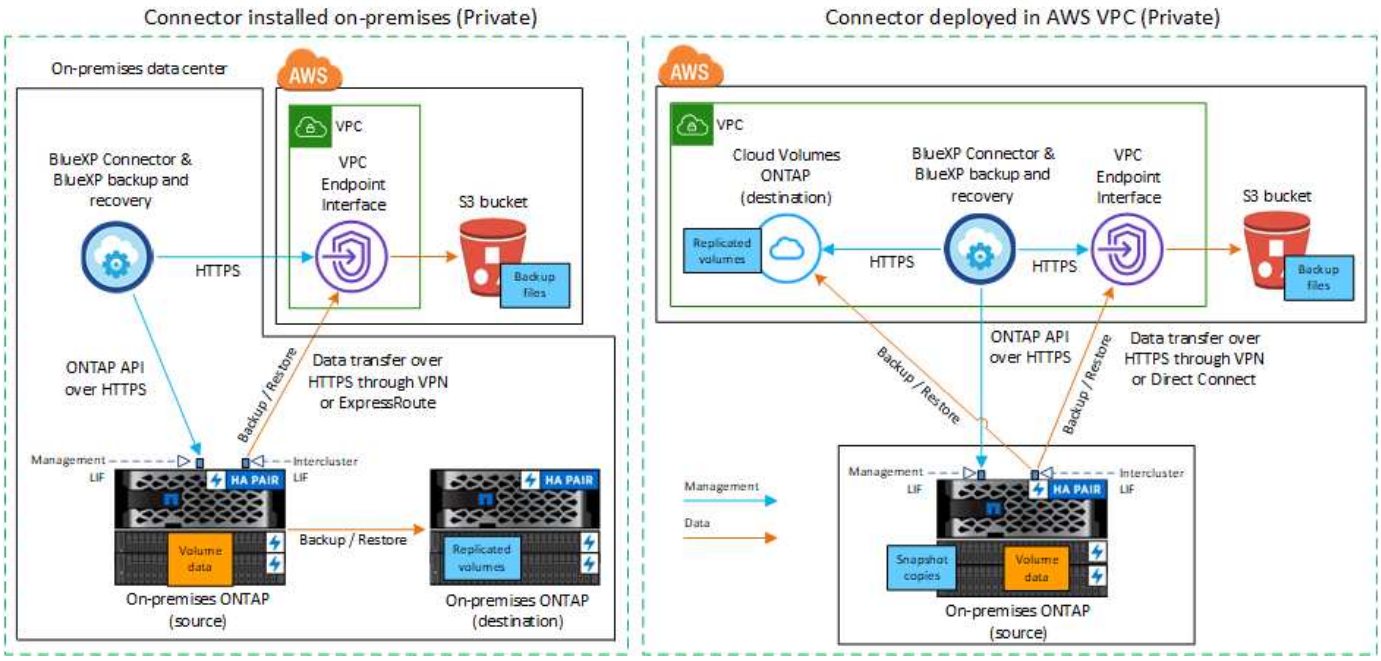
- **Connessione pubblica** - connette direttamente il sistema ONTAP ad AWS S3 utilizzando un endpoint pubblico S3.
- **Connessione privata** - utilizza una connessione VPN o AWS Direct e instrada il traffico attraverso un'interfaccia endpoint VPC che utilizza un indirizzo IP privato.

In alternativa, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.

Il seguente diagramma mostra il metodo **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un connettore installato in sede o un connettore implementato in AWS VPC.



Il seguente diagramma mostra il metodo **private Connection** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un connettore installato in sede o un connettore implementato in AWS VPC.



Preparare il connettore BlueXP

BlueXP Connector è il software principale per la funzionalità BlueXP. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un connettore.

Creare o cambiare connettori

Se si dispone già di un connettore implementato in AWS VPC o on-premise, si è tutti pronti.

In caso contrario, sarà necessario creare un connettore in una di queste posizioni per eseguire il backup dei dati ONTAP nello storage AWS S3. Non puoi utilizzare un connettore implementato in un altro provider cloud.

- "Scopri di più sui connettori"
- "Installare un connettore in AWS"
- "Installare un connettore in sede"
- "Installare un connettore in un'area AWS GovCloud"

  Il backup e ripristino BlueXP è supportato nelle regioni di GovCloud quando il connettore viene implementato nel cloud, non quando viene installato nelle vostre sedi. Inoltre, è necessario implementare il connettore da AWS Marketplace. Non è possibile implementare il connettore in un'area governativa dal sito Web di BlueXP SaaS.

Preparare i requisiti di rete dei connettori

Verificare che siano soddisfatti i seguenti requisiti di rete:

- Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:
  - Una connessione HTTPS tramite la porta 443 al servizio di backup e ripristino BlueXP e allo storage a oggetti S3 ("vedere l'elenco degli endpoint")
  - Una connessione HTTPS sulla porta 443 alla LIF di gestione del cluster ONTAP
  - Per le implementazioni di AWS e AWS GovCloud sono richieste regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per il connettore in AWS" per ulteriori informazioni.
- Se si dispone di una connessione diretta o VPN dal cluster ONTAP al VPC e si desidera che la comunicazione tra il connettore e S3 rimanga nella rete interna AWS (una connessione **privata**), è necessario attivare un'interfaccia endpoint VPC su S3. Configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC.

Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per AWS e BlueXP:

- Prima di poter attivare il backup e il ripristino BlueXP per il cluster, è necessario sottoscrivere un'offerta di pagamento a consumo (PAYGO) BlueXP Marketplace di AWS oppure acquistare e attivare una licenza BYOL di backup e ripristino BlueXP di NetApp. Queste licenze sono destinate al tuo account e possono essere utilizzate su più sistemi.
  - Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento a "Offerta NetApp BlueXP di AWS Marketplace". La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento.
  - Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza.
- È necessario disporre di un abbonamento AWS per lo spazio di storage a oggetti in cui verranno collocati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali su Amazon S3 in tutte le regioni, comprese le regioni AWS GovCloud. Specificare la regione in cui verranno memorizzati i backup quando si imposta il servizio.

Preparare i cluster ONTAP

Dovrai preparare il tuo sistema ONTAP on-premise di origine e qualsiasi altro sistema ONTAP o Cloud Volumes ONTAP secondario on-premise.

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP in BlueXP
- Verificare i requisiti di sistema di ONTAP
- Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti
- Verificare i requisiti di rete di ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP in BlueXP

Il sistema ONTAP di origine on-premise e qualsiasi sistema ONTAP o Cloud Volumes ONTAP secondario on-premise devono essere disponibili su BlueXP Canvas.

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore.
"Scopri come individuare un cluster".

Verificare i requisiti di sistema di ONTAP

Assicurarsi che siano soddisfatti i seguenti requisiti ONTAP:

- Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa nel Premium Bundle o nel Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza il backup e ripristino BlueXP.

  Scopri come "gestire le licenze del cluster".

- L'ora e il fuso orario sono impostati correttamente. Scopri come "configurare l'ora del cluster".
- Se si intende replicare i dati, è necessario verificare che i sistemi di origine e di destinazione eseguano versioni di ONTAP compatibili prima di replicare i dati.

  "Visualizza le versioni di ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette allo storage a oggetti.

- Per un'architettura di backup fan-out, configurare le seguenti impostazioni sul sistema *primario*.
- Per un'architettura di backup a cascata, configurare le seguenti impostazioni sul sistema *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP:

- Il cluster richiede una connessione HTTPS in entrata dal connettore alla LIF di gestione del cluster.
- Su ogni nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup è richiesta una LIF intercluster. Queste LIF intercluster devono essere in grado di accedere all'archivio di oggetti.

  Il cluster avvia una connessione HTTPS in uscita sulla porta 443 dalle LIF dell'intercluster allo storage Amazon S3 per le operazioni di backup e ripristino. ONTAP legge e scrive i dati da e verso lo storage a oggetti: Lo storage a oggetti non viene mai avviato, ma risponde.

- Le LIF dell'intercluster devono essere associate a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti. "Scopri di più su IPspaces".

Quando si imposta il backup e il ripristino di BlueXP, viene richiesto di utilizzare IPSpace. È necessario scegliere l'IPSpace a cui sono associate queste LIF. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

Se si utilizza un IPSpace diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere allo storage a oggetti.

Tutte le LIF di intercluster all'interno di IPSpace devono avere accesso all'archivio di oggetti. Se non è possibile configurare questa opzione per l'IPSpace corrente, è necessario creare un IPSpace dedicato in cui tutte le LIF dell'intercluster abbiano accesso all'archivio di oggetti.

- I server DNS devono essere stati configurati per la VM di storage in cui si trovano i volumi. Scopri come "Configurare i servizi DNS per SVM".
- Aggiornare le regole del firewall, se necessario, per consentire le connessioni di backup e ripristino BlueXP da ONTAP allo storage a oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM dello storage al server DNS tramite la porta 53 (TCP/UDP).
- Se si utilizza un endpoint dell'interfaccia VPC privata in AWS per la connessione S3, per utilizzare HTTPS/443, è necessario caricare il certificato dell'endpoint S3 nel cluster ONTAP. Configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC. *[Assicurarsi che il cluster ONTAP disponga delle autorizzazioni per accedere al bucket S3.

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.

Preparare Amazon S3 come destinazione di backup

La preparazione di Amazon S3 come destinazione di backup prevede i seguenti passaggi:

- Impostare le autorizzazioni S3.
- (Facoltativo) Crea i tuoi bucket S3. (Il servizio creerà i bucket per te, se lo desideri).
- (Facoltativo) impostare le chiavi AWS gestite dal cliente per la crittografia dei dati.
- (Facoltativo) configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC.

Impostare le autorizzazioni S3

È necessario configurare due set di autorizzazioni:

- Permessi per il connettore per creare e gestire il bucket S3.
- Autorizzazioni per il cluster ONTAP on-premise in modo che possa leggere e scrivere i dati nel bucket S3.

Fasi

1. Assicurarsi che il connettore disponga delle autorizzazioni necessarie. Per ulteriori informazioni, vedere "Autorizzazioni dei criteri BlueXP ".

   > Quando si creano backup nelle regioni AWS China, è necessario modificare il nome risorsa AWS "arn" in tutte le sezioni *Resource* delle policy IAM da "aws" a "aws-cn", ad esempio `arn:aws-cn:s3:::netapp-backup-*`.

2. Quando si attiva il servizio, la procedura guidata di backup richiede di inserire una chiave di accesso e una chiave segreta. Queste credenziali vengono passate al cluster ONTAP in modo che ONTAP possa eseguire il backup e il ripristino dei dati nel bucket S3. A tale scopo, è necessario creare un utente IAM con le seguenti autorizzazioni.

   Fare riferimento a. "Documentazione AWS: Creazione di un ruolo per delegare le autorizzazioni a un utente IAM".

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

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea i bucket. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione di bucket personalizzati".

Se si creano i propri bucket, è necessario utilizzare il nome del bucket "netapp-backup". Se si desidera utilizzare un nome personalizzato, modificare `ontapcloud-instance-policy-netapp-backup` IAMRole per i CVO esistenti e aggiungere il seguente elenco ai permessi S3. Devi includere `"Resource": "arn:aws:s3:::*"` e assegnare tutte le autorizzazioni necessarie che devono essere associate al bucket.

```
"Azione": [
"S3:ListBucket"
"S3:GetBucketLocation"
]
"Risorsa": "arn:aws:s3:::*",
"Effetto": "Consenti"
},
{
"Azione": [
"S3:GetObject",
"S3:PutObject",
"S3:DeleteObject",
"S3:ListAllMyBucket",
"S3:PutObjectTagging",
"S3:GetObjectTagging",
"S3:RestoreObject",
"S3:GetBucketObjectLockConfiguration",
"S3:GetObjectRetention",
"S3:PutBucketObjectLockConfiguration",
"S3:PutObjectRetention"
]
"Risorsa": "arn:aws:s3:::*",
```

Configurare le chiavi AWS gestite dal cliente per la crittografia dei dati

Se si desidera utilizzare le chiavi di crittografia predefinite di Amazon S3 per crittografare i dati trasferiti tra il cluster on-premise e il bucket S3, l'installazione predefinita utilizza questo tipo di crittografia.

Se invece si desidera utilizzare le proprie chiavi gestite dal cliente per la crittografia dei dati piuttosto che le chiavi predefinite, è necessario che le chiavi gestite per la crittografia siano già impostate prima di avviare la procedura guidata di backup e ripristino BlueXP.

"Consulta come utilizzare le tue chiavi di crittografia Amazon con Cloud Volumes ONTAP".

"Consulta come utilizzare le tue chiavi di crittografia Amazon con backup e recovery di BlueXP ".

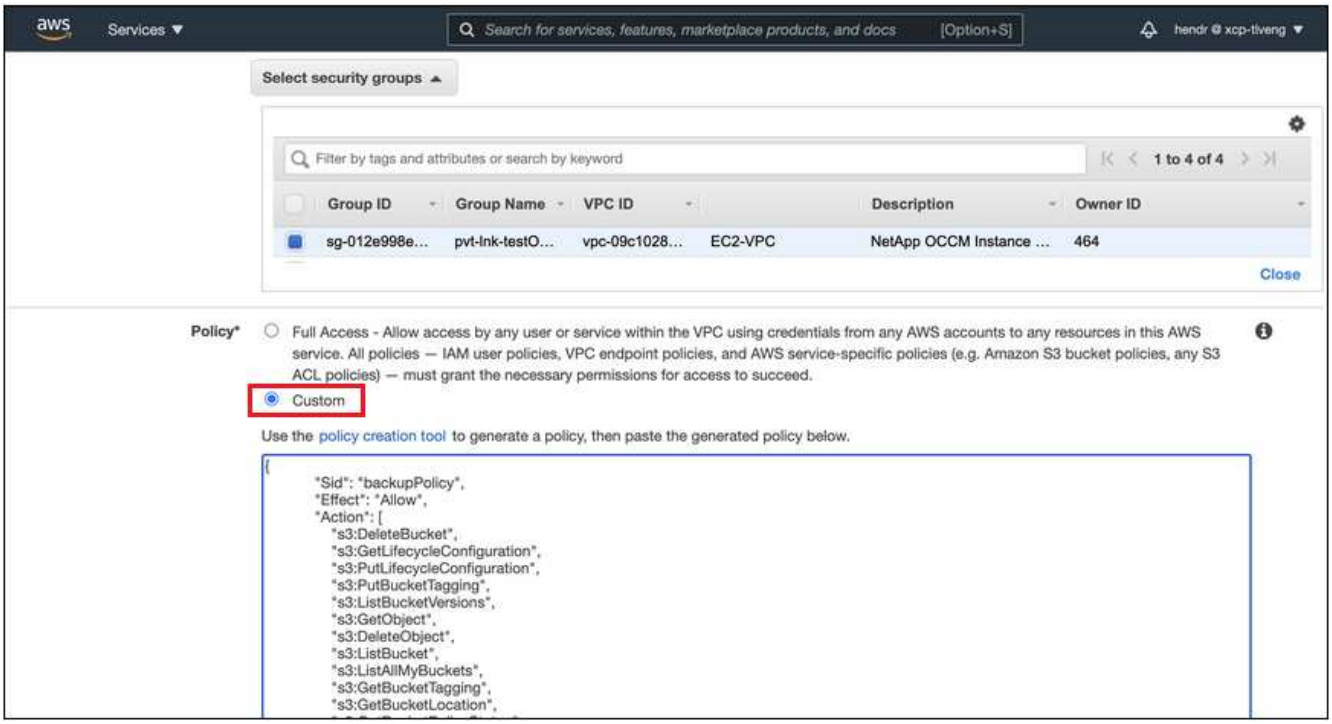
Configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC

Se si desidera utilizzare una connessione Internet pubblica standard, tutte le autorizzazioni vengono impostate dal connettore e non è necessario eseguire altre operazioni.

Se si desidera una connessione più sicura via Internet dal data center on-premise al VPC, è possibile selezionare una connessione AWS PrivateLink nella procedura guidata di attivazione del backup. È necessario se si intende utilizzare una VPN o una connessione diretta AWS per collegare il sistema on-premise tramite un'interfaccia endpoint VPC che utilizza un indirizzo IP privato.

Fasi

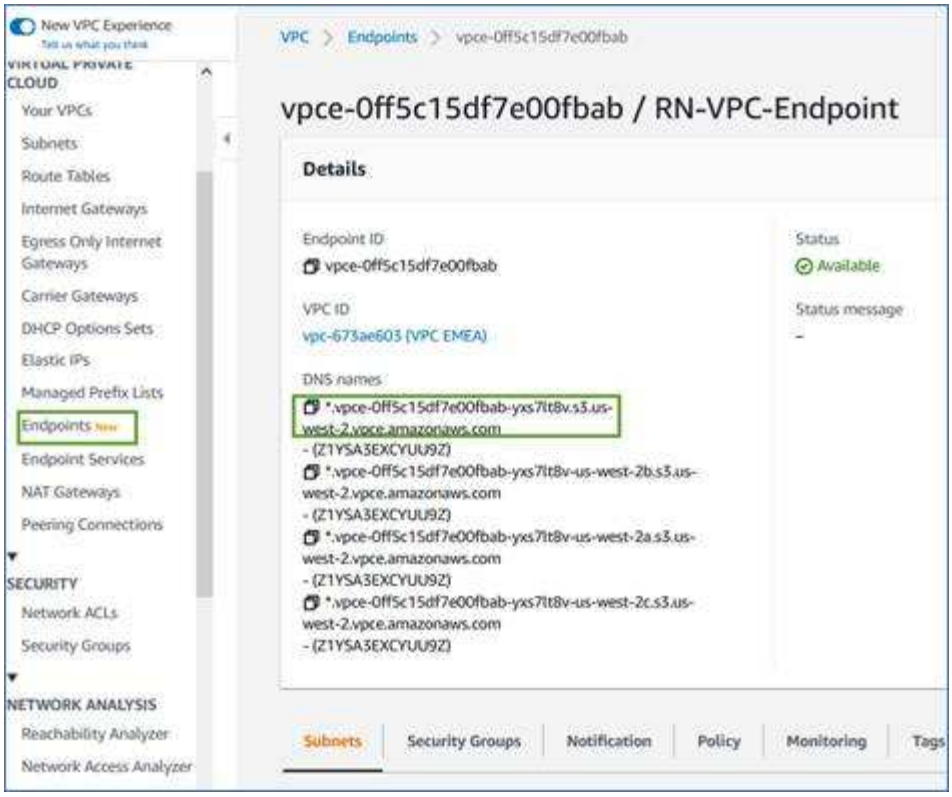
1. Creare una configurazione dell'endpoint dell'interfaccia utilizzando la console Amazon VPC o la riga di comando. "Consulta i dettagli sull'utilizzo di AWS PrivateLink per Amazon S3".
2. Modificare la configurazione del gruppo di protezione associata a BlueXP Connector. È necessario modificare la policy in "Custom" (da "Full Access") Aggiungere le autorizzazioni S3 dal criterio di backup come mostrato in precedenza.



Se si utilizza la porta 80 (HTTP) per la comunicazione con l'endpoint privato, si è tutti impostati. È ora possibile attivare il backup e il ripristino BlueXP sul cluster.

Se si utilizza la porta 443 (HTTPS) per la comunicazione con l'endpoint privato, è necessario copiare il certificato dall'endpoint VPC S3 e aggiungerlo al cluster ONTAP, come illustrato nei 4 passaggi successivi.

3. Ottenere il nome DNS dell'endpoint dalla console AWS.



4. Ottenere il certificato dall'endpoint VPC S3. Lo fai entro "Accesso alla macchina virtuale che ospita BlueXP Connector" ed eseguire il seguente comando. Quando si immette il nome DNS dell'endpoint, aggiungere "bucket" all'inizio, sostituendo "*":

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-
0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443
-showcerts
```

5. Dall'output di questo comando, copiare i dati per il certificato S3 (tutti i dati compresi tra i tag BEGIN / END CERTIFICATE):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Accedere alla CLI del cluster ONTAP e applicare il certificato copiato utilizzando il seguente comando (sostituire il proprio nome della VM di storage):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:

   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.

     Se la destinazione Amazon S3 per i backup esiste come ambiente di lavoro su Canvas, puoi trascinare il cluster ONTAP sullo storage a oggetti Amazon S3.

   - Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare **azioni** ••• E selezionare **attiva backup** per un singolo volume (che non ha già attivato la replica o il backup nell'archiviazione a oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Continuare con le seguenti opzioni:

   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Per volume protetto si intende un volume con una o più delle seguenti opzioni: Policy di snapshot, policy di replica, policy di backup su oggetti.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Target e policy di replica

  Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Snapshot locali**: se si esegue una replica o un backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi nello storage a oggetti.
2. **Architettura**: Se si sceglie la replica e il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di informazioni dal primario al secondario allo storage a oggetti e dal secondario allo storage a oggetti.
   - **Fan out**: I flussi di informazioni dal primario al secondario *e* dallo storage primario a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a "Creare un criterio" .

4. Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per i dettagli su DataLock e Ransomware Protection, fare riferimento a "Impostazioni dei criteri di backup su oggetti" .
   - Selezionare **Crea**.
5. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Selezionare **Crea**.
6. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **Amazon Web Services**.
   - **Provider settings** (Impostazioni provider): Inserire i dettagli del provider e la regione AWS in cui verranno memorizzati i backup.

     La chiave di accesso e la chiave segreta sono destinate all'utente IAM creato per consentire al cluster ONTAP di accedere al bucket S3.
   - **Bucket**: Scegliere un bucket S3 esistente o crearne uno nuovo. Fare riferimento a. "Aggiungere i bucket S3".
   - **Chiave di crittografia**: Se è stato creato un nuovo bucket S3, immettere le informazioni sulla chiave di crittografia fornite dal provider. Per gestire la crittografia dei dati, scegli se utilizzare le chiavi di crittografia Amazon S3 predefinite o le chiavi gestite dal cliente dall'account AWS.

     Se si sceglie un bucket esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario immetterle ora.
   - **Rete**: Scegliere IPSpace e scegliere se si desidera utilizzare un endpoint privato. L'endpoint privato è disattivato per impostazione predefinita.
     i. IPSpace nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.

ii. Se si desidera, scegliere se utilizzare un AWS PrivateLink precedentemente configurato. "Scopri i dettagli sull'utilizzo di AWS PrivateLink per Amazon S3".

- **Criterio di backup**: Selezionare un criterio di backup esistente o crearne uno.

  Per creare una policy personalizzata prima di attivare il backup, fare riferimento a "Creare un criterio" .

  Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

  - Immettere il nome del criterio.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Selezionare **Crea**.

- **Esporta copie snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti copie snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo messaggio aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup e garantire la protezione più completa per i tuoi volumi.

7. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo, vengono create istantanee con un'etichetta che corrisponde alle etichette dei criteri di replica e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati del sistema di storage primario. I trasferimenti successivi contengono copie differenziali dei dati primari contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di storage primario.

Il bucket S3 viene creato nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immessa e i file di backup vengono memorizzati in tale account. Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali nell'archiviazione BLOB di Azure con backup e ripristino BlueXP

Completa alcuni passaggi nel backup e ripristino di BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali a un sistema di archiviazione secondario e all'archiviazione BLOB di Azure.

I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

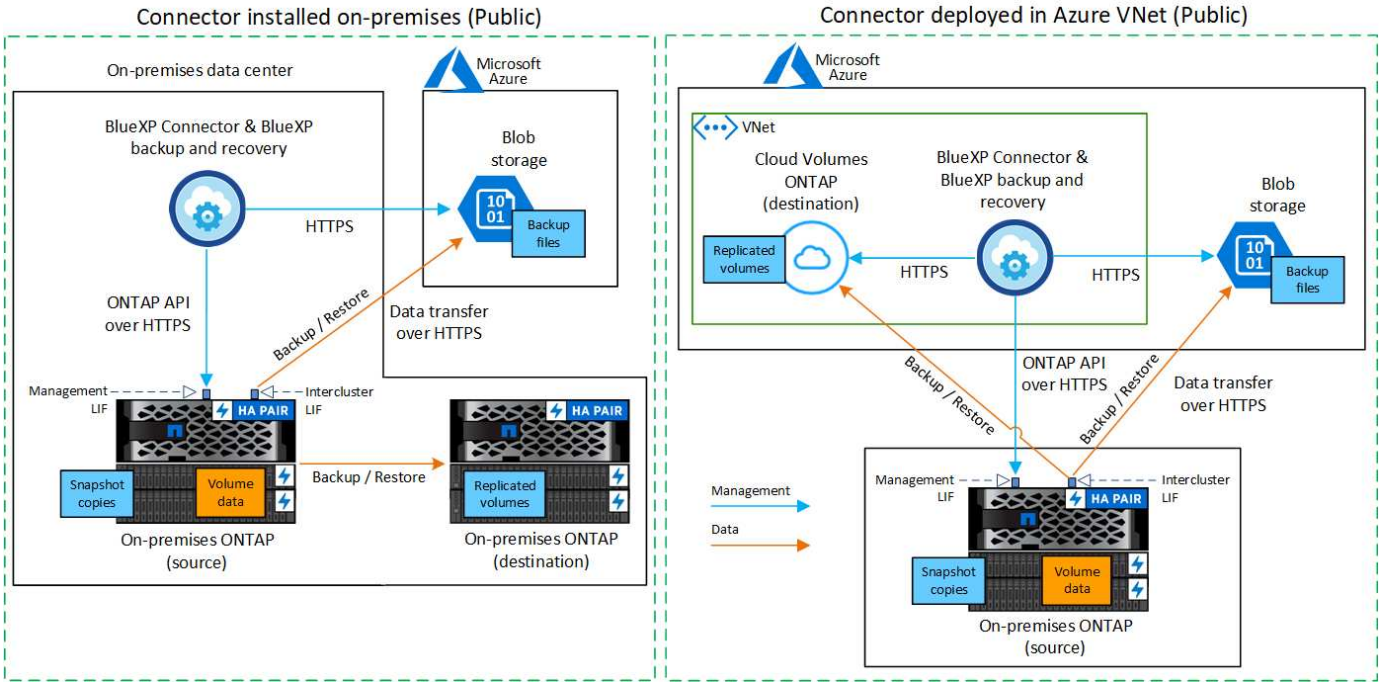
Identificare il metodo di connessione

Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup da sistemi ONTAP on-premise a Azure Blob.

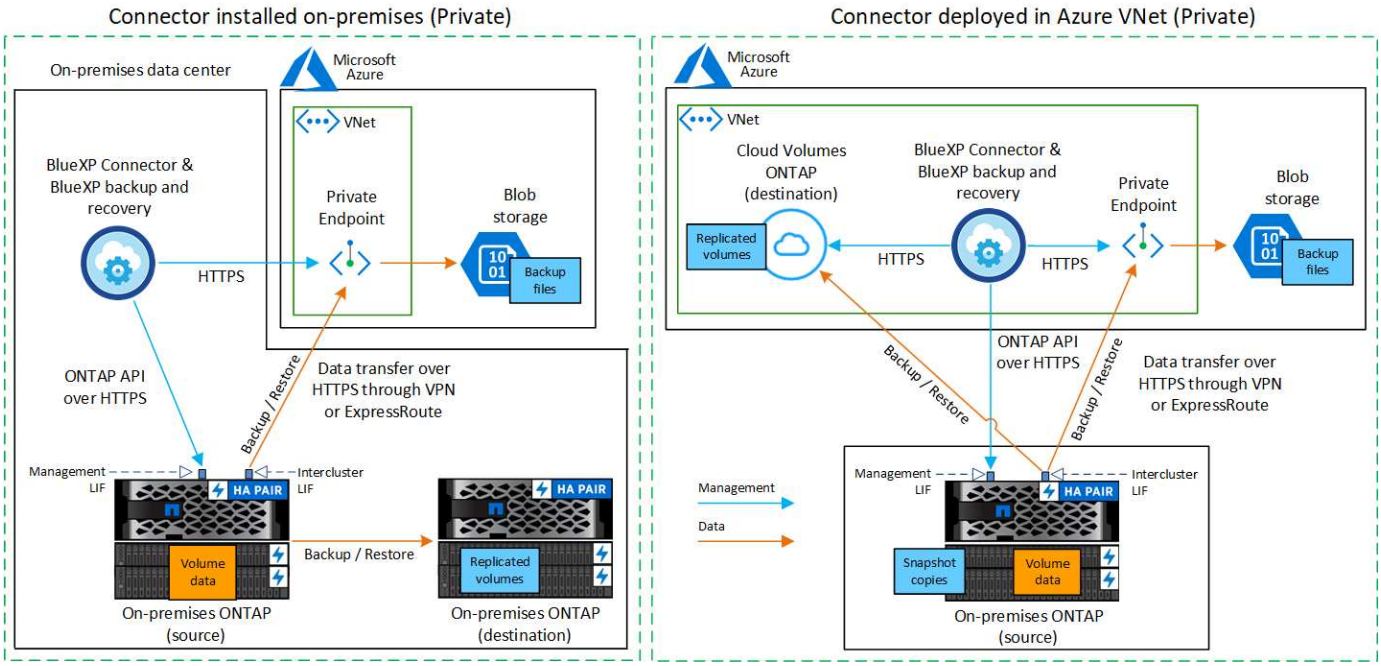
- **Connessione pubblica** - connette direttamente il sistema ONTAP allo storage Azure Blob utilizzando un endpoint Azure pubblico.
- **Connessione privata** - utilizza una VPN o ExpressRoute e instrada il traffico attraverso un VNET Private Endpoint che utilizza un indirizzo IP privato.

In alternativa, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.

Il seguente diagramma mostra il metodo **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un connettore installato in sede o un connettore implementato in Azure VNET.



Il seguente diagramma mostra il metodo **private Connection** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un connettore installato in sede o un connettore implementato in Azure VNET.



Preparare il connettore BlueXP

BlueXP Connector è il software principale per la funzionalità BlueXP. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un connettore.

Creare o cambiare connettori

Se hai già un connettore implementato in Azure VNET o on-premise, allora sei tutto impostato.

In caso contrario, sarà necessario creare un connettore in una di queste posizioni per eseguire il backup dei dati ONTAP nello storage Azure Blob. Non puoi utilizzare un connettore implementato in un altro provider cloud.

- "Scopri di più sui connettori"
- "Installare un connettore in Azure"
- "Installare un connettore in sede"
- "Installare un connettore in un'area governativa Azure"

  Il backup e ripristino BlueXP è supportato nelle regioni governative di Azure quando il connettore viene implementato nel cloud, non quando viene installato nelle vostre sedi. Inoltre, è necessario implementare il connettore da Azure Marketplace. Non è possibile implementare il connettore in un'area governativa dal sito Web di BlueXP SaaS.

Preparare il collegamento in rete per il connettore

Assicurarsi che il connettore disponga delle connessioni di rete richieste.

Fasi

1. Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:
   - Una connessione HTTPS tramite la porta 443 al servizio di backup e ripristino BlueXP e allo storage a oggetti Blob ("vedere l'elenco degli endpoint")
   - Una connessione HTTPS sulla porta 443 alla LIF di gestione del cluster ONTAP
   - Affinché la funzionalità di ricerca e ripristino di BlueXP funzioni, la porta 1433 deve essere aperta per la comunicazione tra il connettore e i servizi SQL di Azure Synapse.
   - Per le implementazioni di Azure e Azure Government sono richieste regole aggiuntive per i gruppi di sicurezza in entrata. Vedere "Regole per il connettore in Azure" per ulteriori informazioni.
2. Abilitare un endpoint privato VNET allo storage Azure. Questa opzione è necessaria se si dispone di una connessione ExpressRoute o VPN dal cluster ONTAP a VNET e si desidera che la comunicazione tra il connettore e lo storage Blob rimanga nella rete privata virtuale (una connessione **privata**).

Verificare o aggiungere le autorizzazioni al connettore

Per utilizzare la funzionalità di backup e ripristino di BlueXP, è necessario disporre di autorizzazioni specifiche nel ruolo del connettore in modo che possa accedere all'area di lavoro di Azure Synapse e all'account di storage di Data Lake. Consultare le autorizzazioni riportate di seguito e seguire la procedura per modificare il criterio.

Prima di iniziare

È necessario registrare Azure Synapse Analytics Resource Provider (chiamato "Microsoft.Synapse") con l'abbonamento. "Scopri come registrare questo provider di risorse per l'abbonamento". Per registrare il provider di risorse, è necessario essere il proprietario dell'abbonamento* o il collaboratore*.

Fasi

1. Identificare il ruolo assegnato alla macchina virtuale Connector:
   a. Nel portale Azure, aprire il servizio macchine virtuali.
   b. Selezionare la macchina virtuale Connector.
   c. In **Impostazioni**, selezionare **identità**.

d. Selezionare **assegnazioni dei ruoli Azure**.

e. Prendere nota del ruolo personalizzato assegnato alla macchina virtuale del connettore.

2. Aggiornare il ruolo personalizzato:

a. Nel portale Azure, apri il tuo abbonamento ad Azure.

b. Selezionare **controllo accesso (IAM) > ruoli**.

c. Selezionare i puntini di sospensione (**…**) per il ruolo personalizzato, quindi selezionare **Modifica**.

d. Selezionare **JSON** e aggiungere le seguenti autorizzazioni:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Visualizza il formato JSON completo per la policy"

e. Selezionare **Revisione + aggiornamento**, quindi selezionare **Aggiorna**.

Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per Azure e BlueXP:

- Prima di poter attivare il backup e il ripristino BlueXP per il cluster, è necessario sottoscrivere un'offerta di pagamento a consumo (PAYGO) BlueXP Marketplace di Azure oppure acquistare e attivare una licenza BYOL di backup e ripristino BlueXP di NetApp. Queste licenze sono destinate al tuo account e possono essere utilizzate su più sistemi.
  - Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento a "Offerta NetApp BlueXP di Azure Marketplace". La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento.
  - Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL".
- È necessario disporre di un abbonamento Azure per lo spazio di storage a oggetti in cui verranno collocati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali ad Azure Blob in tutte le regioni, comprese le regioni di Azure Government. Specificare la regione in cui verranno memorizzati i backup quando si configura il servizio.

Preparare i cluster ONTAP

Dovrai preparare il tuo sistema ONTAP on-premise di origine e qualsiasi altro sistema ONTAP o Cloud Volumes ONTAP secondario on-premise.

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP in BlueXP
- Verificare i requisiti di sistema di ONTAP
- Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti
- Verificare i requisiti di rete di ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP in BlueXP

Il sistema ONTAP di origine on-premise e qualsiasi sistema ONTAP o Cloud Volumes ONTAP secondario on-premise devono essere disponibili su BlueXP Canvas.

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore.
"Scopri come individuare un cluster".

Verificare i requisiti di sistema di ONTAP

Assicurarsi che siano soddisfatti i seguenti requisiti ONTAP:

- Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa nel Premium Bundle o nel Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza il backup e ripristino BlueXP.

Scopri come "gestire le licenze del cluster".

- L'ora e il fuso orario sono impostati correttamente. Scopri come "configurare l'ora del cluster".
- Se si intende replicare i dati, è necessario verificare che i sistemi di origine e di destinazione eseguano versioni di ONTAP compatibili prima di replicare i dati.

  "Visualizza le versioni di ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette allo storage a oggetti.

- Per un'architettura di backup fan-out, configurare le seguenti impostazioni sul sistema *primario*.
- Per un'architettura di backup a cascata, configurare le seguenti impostazioni sul sistema *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP:

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 dal LIF dell'intercluster allo storage Azure Blob per le operazioni di backup e ripristino.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

- ONTAP richiede una connessione in entrata dal connettore alla LIF di gestione del cluster. Il connettore può risiedere in un Azure VNET.
- Su ogni nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti. "Scopri di più su IPspaces".

  Quando si imposta il backup e il ripristino di BlueXP, viene richiesto di utilizzare IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

- Le LIF dei nodi e dell'intercluster possono accedere all'archivio di oggetti.
- I server DNS sono stati configurati per la VM di storage in cui si trovano i volumi. Scopri come "Configurare i servizi DNS per SVM".
- Se si utilizza un IPSpace diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere allo storage a oggetti.
- Aggiornare le regole del firewall, se necessario, per consentire le connessioni del servizio di backup e ripristino BlueXP da ONTAP allo storage a oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM dello storage al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.

- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.

Preparare Azure Blob come destinazione di backup

1. È possibile utilizzare le proprie chiavi personalizzate per la crittografia dei dati nella procedura guidata di attivazione invece di utilizzare le chiavi di crittografia predefinite gestite da Microsoft. In questo caso, è necessario disporre dell'abbonamento Azure, del nome del vault delle chiavi e della chiave. "Scopri come utilizzare le tue chiavi".

   Tenere presente che il backup e il ripristino supportano *policy di accesso Azure* come modello di autorizzazione. Il modello di autorizzazione *Azure RBAC (role-based access control*) non è attualmente supportato.

2. Se si desidera una connessione più sicura su Internet pubblico dal data center on-premise a VNET, è possibile configurare un endpoint privato Azure nella procedura guidata di attivazione. In questo caso, è necessario conoscere VNET e Subnet per questa connessione. "Fare riferimento ai dettagli sull'utilizzo di un endpoint privato".

Crea il tuo account di storage Azure Blob

Per impostazione predefinita, il servizio crea account di storage. Se si desidera utilizzare i propri account di storage, è possibile crearli prima di avviare la procedura guidata di attivazione del backup, quindi selezionare tali account di storage nella procedura guidata.

"Scopri di più sulla creazione di account storage personalizzati".

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

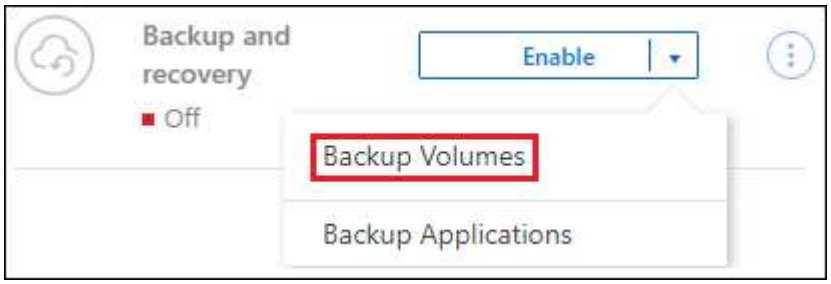
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:

- Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.



  Se la destinazione di Azure per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster ONTAP sullo storage a oggetti di Azure Blob.

- Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare **azioni** ••• E selezionare **attiva backup** per un singolo volume (che non ha già attivato la replica o il backup nell'archiviazione a oggetti).

La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Continuare con le seguenti opzioni:
   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Per volume protetto si intende un volume con una o più delle seguenti opzioni: Policy di snapshot, policy di replica, policy di backup su oggetti.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se per i volumi selezionati sono già state applicate le policy di snapshot o replica, le policy selezionate in seguito sovrascriveranno quelle esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.

- Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.

2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Sia che si desideri una o tutte le opzioni di backup: Snapshot locali, replica e backup su storage a oggetti
- Architettura
- Policy Snapshot locale
- Target e policy di replica

> Se i volumi scelti hanno policy di replica e snapshot diverse da quelle selezionate in questa fase, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Snapshot locali**: se si esegue una replica o un backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi nello storage a oggetti.
2. **Architettura**: Se si sceglie la replica e il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di informazioni dal primario al secondario e dallo storage secondario allo storage a oggetti.
   - **Fan out**: I flussi di informazioni dal primario al secondario *e* dallo storage primario a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   > Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Selezionare **Crea**.
4. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.

- **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno nuovo.

  Per creare una policy personalizzata prima di attivare la replica, fare riferimento a "Creare un criterio" .

  Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

  - Immettere il nome del criterio.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Selezionare **Crea**.

5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **Microsoft Azure**.
   - **Impostazioni provider**: Immettere i dettagli del provider e la regione in cui verranno memorizzati i backup.

     Creare un nuovo account storage o selezionarne uno esistente.

     Creare il proprio gruppo di risorse che gestisce il contenitore Blob oppure selezionare il tipo e il gruppo di risorse.

     Se si desidera proteggere i file di backup da modifiche o eliminazioni, assicurarsi che l'account di storage sia stato creato con lo storage immutabile abilitato utilizzando un periodo di conservazione di 30 giorni.

     Se si desidera eseguire il tiering dei file di backup più vecchi in Azure Archive Storage per un'ulteriore ottimizzazione dei costi, assicurarsi che l'account di storage disponga della regola del ciclo di vita appropriata.

   - **Chiave di crittografia**: Se è stato creato un nuovo account di storage Azure, immettere le informazioni sulla chiave di crittografia fornite dal provider. Per gestire la crittografia dei dati, scegli se utilizzare le chiavi di crittografia predefinite di Azure o le chiavi gestite dal cliente dall'account Azure.

     Se si sceglie di utilizzare le proprie chiavi gestite dal cliente, inserire l'archivio delle chiavi e le informazioni sulle chiavi.

     Se si sceglie un account di storage Microsoft esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario immetterle ora.

   - **Rete**: Scegliere IPSpace e scegliere se si desidera utilizzare un endpoint privato. L'endpoint privato è disattivato per impostazione predefinita.
     i. IPSpace nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
     ii. Facoltativamente, scegli se utilizzerai un endpoint privato di Azure configurato in precedenza. "Scopri come utilizzare un endpoint privato Azure" .
   - **Criterio di backup**: Selezionare un criterio di archiviazione di Backup in oggetto esistente o crearne uno nuovo.

Per creare una policy personalizzata prima di attivare il backup, fare riferimento a "Creare un criterio" .

Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

- Immettere il nome del criterio.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per i dettagli su DataLock e Ransomware Protection, fare riferimento a "Impostazioni dei criteri di backup su oggetti" .
- Selezionare **Crea**.

◦ **Esporta copie snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti copie snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliero, settimanale, ecc.), viene visualizzato questo messaggio aggiuntivo. Selezionare questa casella per copiare tutte le istantanee storiche nello storage a oggetti come file di backup per garantire la protezione più completa per i volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo, vengono create istantanee con un'etichetta che corrisponde alle etichette dei criteri di replica e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati del sistema di storage primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di storage primario contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume primario.

Viene creato un account di storage Blob nel gruppo di risorse inserito e i file di backup vengono memorizzati in tale gruppo. Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su Google Cloud Storage con il backup e il ripristino di BlueXP

Completa alcuni passaggi del backup e del ripristino BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP primari locali a un sistema di archiviazione secondario e a Google Cloud Storage.

I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

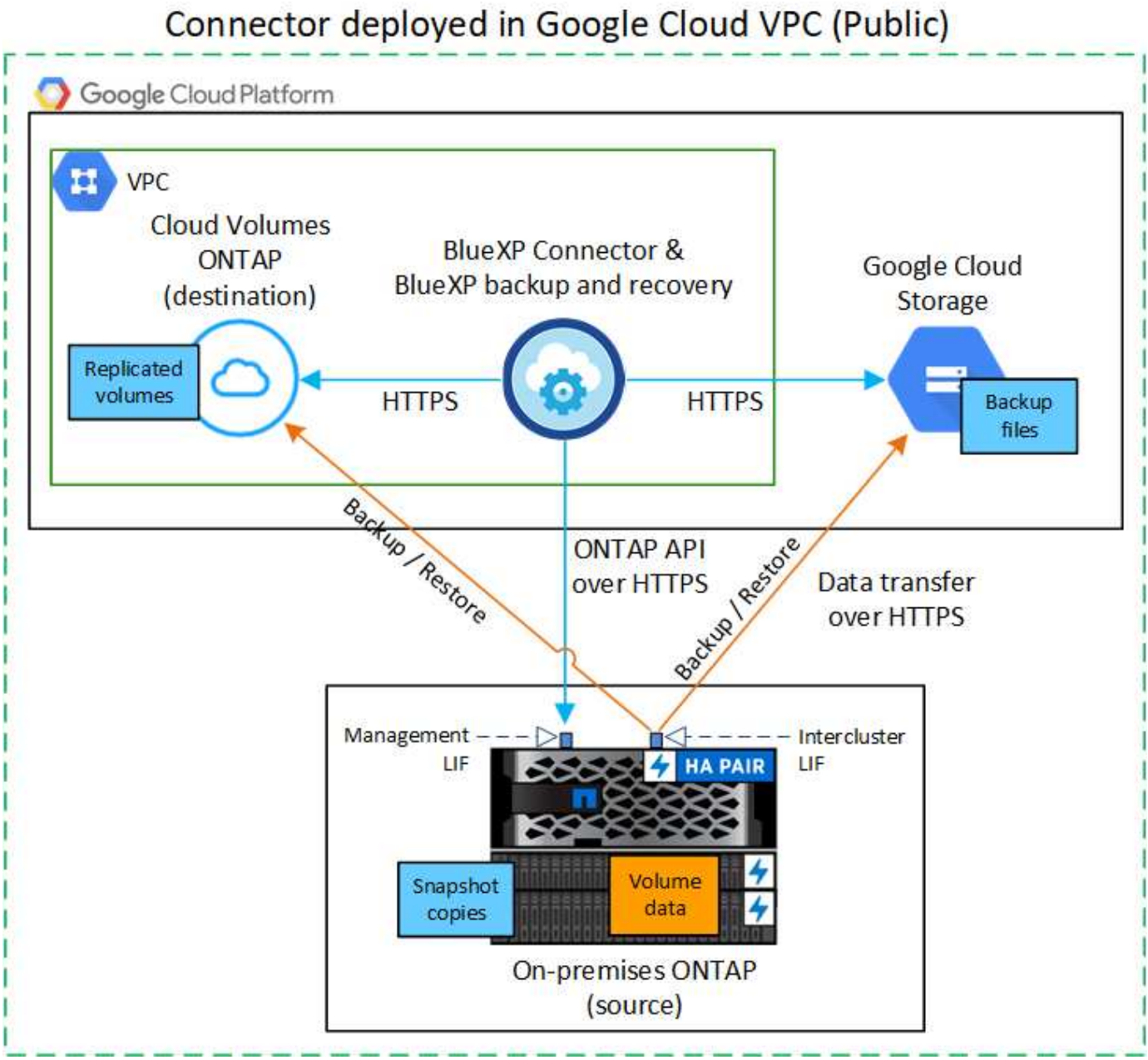
Identificare il metodo di connessione

Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup dai sistemi ONTAP on-premise allo storage cloud Google.

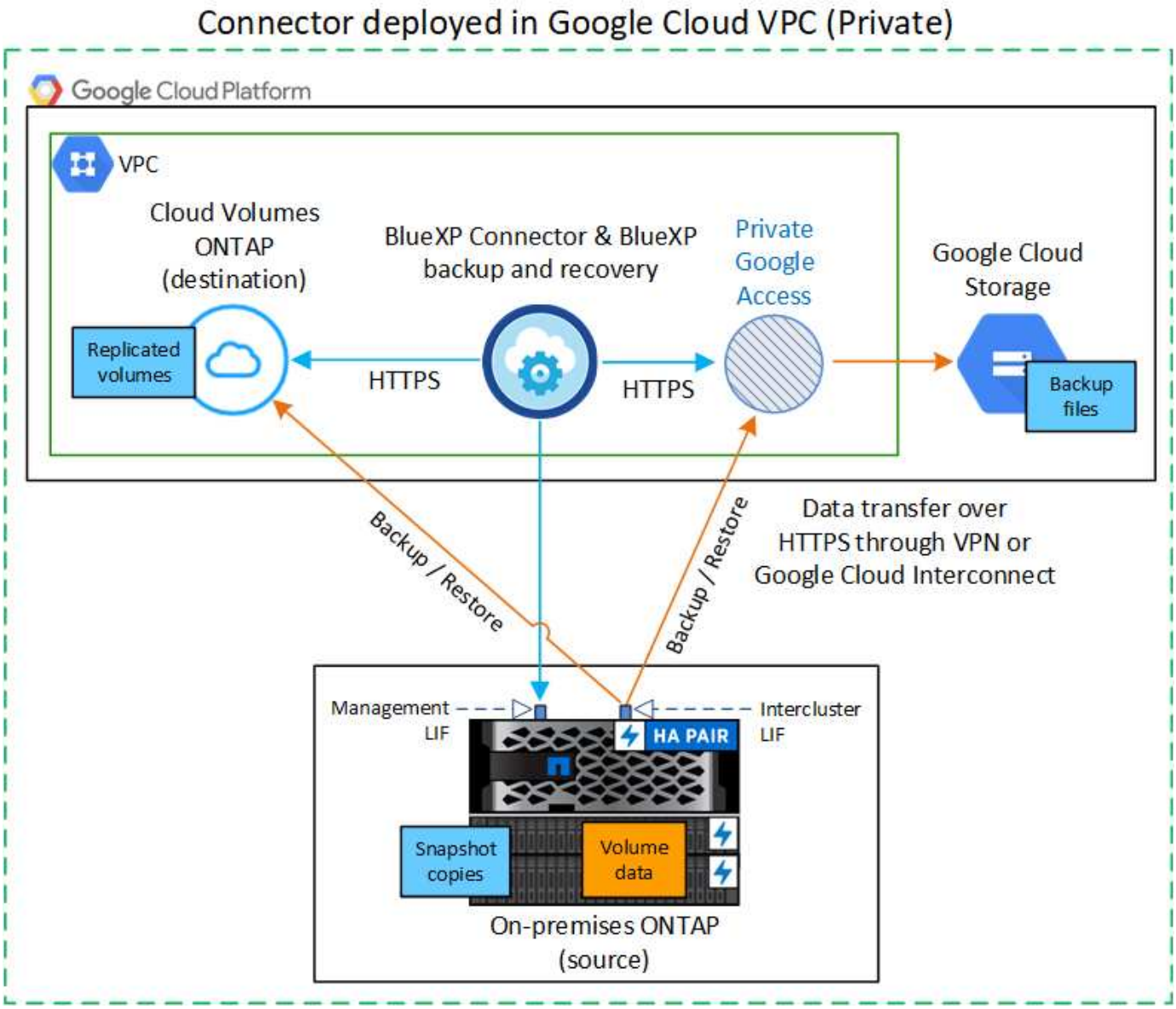
- **Connessione pubblica** - consente di connettere direttamente il sistema ONTAP allo storage cloud di Google utilizzando un endpoint pubblico di Google.
- **Connessione privata** - utilizza una VPN o Google Cloud Interconnect e instrada il traffico attraverso un'interfaccia privata di Google Access che utilizza un indirizzo IP privato.

In alternativa, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.

Il seguente diagramma mostra il metodo **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. Il connettore deve essere implementato in Google Cloud Platform VPC.



Il seguente diagramma mostra il metodo **private Connection** e le connessioni che è necessario preparare tra i componenti. Il connettore deve essere implementato in Google Cloud Platform VPC.



Preparare il connettore BlueXP

BlueXP Connector è il software principale per la funzionalità BlueXP. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un connettore.

Creare o cambiare connettori

Se hai già un connettore implementato nel tuo VPC Google Cloud Platform, allora sei tutto impostato.

In caso contrario, sarà necessario creare un connettore in tale posizione per eseguire il backup dei dati ONTAP su Google Cloud Storage. Non puoi utilizzare un connettore implementato in un altro cloud provider o on-premise.

- "Scopri di più sui connettori"
- "Installare un connettore nel GCP"

Preparare il collegamento in rete per il connettore

Assicurarsi che il connettore disponga delle connessioni di rete richieste.

Fasi

1. Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:
   - Una connessione HTTPS tramite la porta 443 al servizio di backup e ripristino BlueXP e allo storage Google Cloud ("vedere l'elenco degli endpoint")
   - Una connessione HTTPS sulla porta 443 alla LIF di gestione del cluster ONTAP
2. Abilitare Private Google Access (o Private Service Connect) sulla subnet in cui si intende implementare il connettore. "Accesso privato a Google" oppure "Connessione al servizio privato" Sono necessari se si dispone di una connessione diretta dal cluster ONTAP al VPC e si desidera che la comunicazione tra il connettore e lo storage cloud di Google rimanga nella rete privata virtuale (una connessione **privata**).

   Seguire le istruzioni di Google per configurare queste opzioni di accesso privato. Assicurarsi che i server DNS siano configurati in modo da puntare `www.googleapis.com` e. `storage.googleapis.com` Agli indirizzi IP interni (privati) corretti.

Verificare o aggiungere le autorizzazioni al connettore

Per utilizzare la funzionalità di backup e ripristino di BlueXP, è necessario disporre di autorizzazioni specifiche nel ruolo del connettore in modo che possa accedere al servizio Google Cloud BigQuery. Esaminare le autorizzazioni riportate di seguito e seguire la procedura per modificare il criterio.

Fasi

1. In "Console Google Cloud", Accedere alla pagina **ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, selezionare il progetto o l'organizzazione che contiene il ruolo che si desidera modificare.
3. Selezionare un ruolo personalizzato.
4. Selezionare **Edit role** (Modifica ruolo) per aggiornare le autorizzazioni del ruolo.
5. Selezionare **Add Permissions** (Aggiungi permessi) per aggiungere le seguenti nuove autorizzazioni al ruolo.

   ```
   bigquery.jobs.get
   bigquery.jobs.list
   bigquery.jobs.listAll
   bigquery.datasets.create
   bigquery.datasets.get
   bigquery.jobs.create
   bigquery.tables.get
   bigquery.tables.getData
   bigquery.tables.list
   bigquery.tables.create
   ```

6. Selezionare **Aggiorna** per salvare il ruolo modificato.

Verificare i requisiti di licenza

- Prima di poter attivare il backup e il ripristino BlueXP per il cluster, è necessario sottoscrivere un'offerta PayGo BlueXP Marketplace di Google oppure acquistare e attivare una licenza BYOL di backup e ripristino BlueXP da NetApp. Queste licenze sono destinate al tuo account e possono essere utilizzate su più sistemi.
  - Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento a "Offerta NetApp BlueXP di Google Marketplace". La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento.
  - Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL".
- È necessario disporre di un abbonamento Google per lo spazio di storage a oggetti in cui verranno posizionati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali su Google Cloud Storage in tutte le regioni. Specificare la regione in cui verranno memorizzati i backup quando si imposta il servizio.

Preparare i cluster ONTAP

Dovrai preparare il tuo sistema ONTAP on-premise di origine e qualsiasi altro sistema ONTAP o Cloud Volumes ONTAP secondario on-premise.

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP in BlueXP
- Verificare i requisiti di sistema di ONTAP
- Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti
- Verificare i requisiti di rete di ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP in BlueXP

Il sistema ONTAP di origine on-premise e qualsiasi sistema ONTAP o Cloud Volumes ONTAP secondario on-premise devono essere disponibili su BlueXP Canvas.

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore.
"Scopri come individuare un cluster".

Verificare i requisiti di sistema di ONTAP

Assicurarsi che siano soddisfatti i seguenti requisiti ONTAP:

- Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa nel Premium Bundle o nel Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza il backup e ripristino BlueXP.

  Scopri come "gestire le licenze del cluster".

- L'ora e il fuso orario sono impostati correttamente. Scopri come "configurare l'ora del cluster".
- Se si intende replicare i dati, è necessario verificare che i sistemi di origine e di destinazione eseguano versioni di ONTAP compatibili prima di replicare i dati.

  "Visualizza le versioni di ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette allo storage a oggetti.

- Per un'architettura di backup fan-out, configurare le seguenti impostazioni sul sistema *primario*.
- Per un'architettura di backup a cascata, configurare le seguenti impostazioni sul sistema *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP:

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 dalla LIF dell'intercluster allo storage cloud di Google per le operazioni di backup e ripristino.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

- ONTAP richiede una connessione in entrata dal connettore alla LIF di gestione del cluster. Il connettore può risiedere in un VPC Google Cloud Platform.
- Su ogni nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti. "Scopri di più su IPspaces".

  Quando si imposta il backup e il ripristino di BlueXP, viene richiesto di utilizzare IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

- I LIF intercluster dei nodi sono in grado di accedere all'archivio di oggetti.
- I server DNS sono stati configurati per la VM di storage in cui si trovano i volumi. Scopri come "Configurare i servizi DNS per SVM".

  Se si utilizza Private Google Access o Private Service Connect, assicurarsi che i server DNS siano configurati in modo da puntare `storage.googleapis.com` Al corretto indirizzo IP interno (privato).

- Se si utilizza un IPSpace diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere allo storage a oggetti.
- Aggiornare le regole del firewall, se necessario, per consentire le connessioni di backup e ripristino BlueXP da ONTAP allo storage a oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM dello storage al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete

virtuale nel cloud provider. Si tratta in genere di una connessione VPN.

- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.

Preparare Google Cloud Storage come destinazione di backup

La preparazione di Google Cloud Storage come destinazione di backup prevede i seguenti passaggi:

- Impostare le autorizzazioni.
- (Facoltativo) Crea i tuoi bucket. (Il servizio creerà i bucket per te, se lo desideri).
- (Facoltativo) impostare le chiavi gestite dal cliente per la crittografia dei dati

Impostare le autorizzazioni

È necessario fornire chiavi di accesso allo storage per un account di servizio che disponga di autorizzazioni specifiche utilizzando un ruolo personalizzato. Un account di servizio consente il backup e il recovery di BlueXP per autenticare e accedere ai bucket Cloud Storage utilizzati per memorizzare i backup. Le chiavi sono necessarie in modo che Google Cloud Storage sappia chi sta effettuando la richiesta.

Fasi

1. In "Console Google Cloud", Accedere alla pagina **ruoli**.
2. "Creare un nuovo ruolo" con le seguenti autorizzazioni:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Nella console di Google Cloud, "Accedere alla pagina Service accounts (account servizio)".
4. Seleziona il tuo progetto Cloud.
5. Selezionare **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**: Seleziona il ruolo personalizzato appena creato.

c. Selezionare **fine**.

6. Passare a. "Impostazioni storage GCP" e creare le chiavi di accesso per l'account di servizio:

a. Selezionare un progetto e scegliere **interoperabilità**. Se non è già stato fatto, selezionare **Enable Interoperability access** (attiva accesso all'interoperabilità).

b. In **chiavi di accesso per gli account di servizio**, selezionare **Crea una chiave per un account di servizio**, selezionare l'account di servizio appena creato e fare clic su **Crea chiave**.

Quando si configura il servizio di backup, sarà necessario inserire le chiavi in BlueXP backup and Recovery in un secondo momento.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea i bucket. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione di bucket personalizzati".

Impostare le chiavi di crittografia gestite dal cliente (CMEK) per la crittografia dei dati

È possibile utilizzare le proprie chiavi gestite dal cliente per la crittografia dei dati invece di utilizzare le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi cross-region che cross-project, in modo da poter scegliere un progetto per un bucket diverso dal progetto della chiave CMEK.

Se stai pensando di utilizzare le tue chiavi gestite dal cliente:

- Per aggiungere queste informazioni nell'attivazione guidata, è necessario disporre di Key Ring e Key Name (Nome chiave). "Scopri di più sulle chiavi di crittografia gestite dal cliente".
- È necessario verificare che le autorizzazioni richieste siano incluse nel ruolo del connettore:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- È necessario verificare che l'API "Cloud Key Management Service (KMS)" di Google sia attivata nel progetto. Per "Documentazione di Google Cloud: Abilitazione delle API" ulteriori informazioni, vedere la .

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (hardware-backed) che quelle generate dal software.

- Sono supportate entrambe le chiavi Cloud KMS appena create o importate.
- Sono supportate solo le chiavi regionali, le chiavi globali non sono supportate.
- Attualmente, è supportato solo lo scopo di "crittografia/decrittografia simmetrica".
- All'agente di servizio associato all'account di storage viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (role/cloudkms.cryptKeyEncrypterDecrypter)" dal backup e ripristino BlueXP.

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

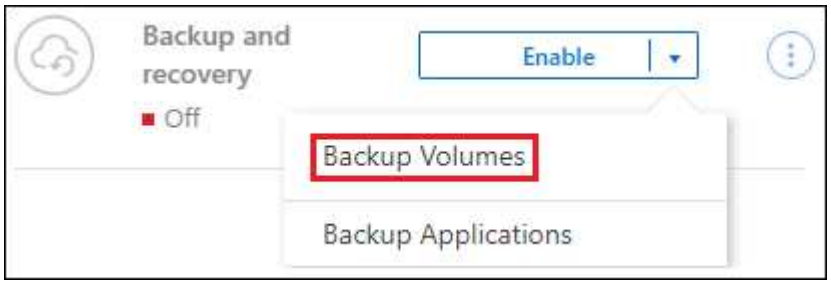
- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:
   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.

     Se la destinazione di Google Cloud Storage per i backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster ONTAP sullo storage a oggetti di Google Cloud.
   - Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare **azioni** ••• E selezionare **attiva backup** per un singolo volume (che non ha già attivato la replica o il backup nell'archiviazione a oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.
2. Continuare con le seguenti opzioni:
   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Per volume protetto si intende un volume con una o più delle seguenti opzioni: Policy di snapshot, policy di replica, policy di backup su oggetti.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Target e policy di replica

Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Local Snapshots**: Se si esegue la replica o il backup sullo storage a oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.

- **Backup**: Esegue il backup dei volumi nello storage a oggetti.

2. **Architettura**: Se si sceglie la replica e il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di informazioni dal primario al secondario e dal secondario allo storage a oggetti.
   - **Fan out**: I flussi di informazioni dal primario al secondario *e* dallo storage primario a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Selezionare **Crea**.

4. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno nuovo.

     Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Selezionare **Crea**.

5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **Google Cloud**.
   - **Impostazioni provider**: Immettere i dettagli del provider e la regione in cui verranno memorizzati i backup.

     Creare un nuovo bucket o selezionarne uno già creato.

     Se si desidera eseguire il tiering dei file di backup più vecchi sullo storage di Google Cloud Archive per un'ulteriore ottimizzazione dei costi, assicurarsi che il bucket disponga della regola del ciclo di vita appropriata.

     Immettere la chiave di accesso e la chiave segreta di Google Cloud.

   - **Chiave di crittografia**: Se è stato creato un nuovo account di storage Google Cloud, immettere le informazioni sulla chiave di crittografia fornite dal provider. Per gestire la crittografia dei dati, scegli se utilizzare le chiavi di crittografia predefinite di Google Cloud o le chiavi gestite dal cliente dall'account Google Cloud.

Se hai scelto un account di storage Google Cloud esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario immetterle ora.

Se si sceglie di utilizzare le proprie chiavi gestite dal cliente, inserire il portachiavi e il nome della chiave. "Scopri di più sulle chiavi di crittografia gestite dal cliente".

- **Networking**: Scegliere IPSpace.

  IPSpace nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.

- **Criterio di backup**: Selezionare un criterio di archiviazione di Backup in oggetto esistente o crearne uno nuovo.

  Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

  Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

  - Immettere il nome del criterio.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Selezionare **Crea**.

- **Esporta copie snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti copie snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliero, settimanale, ecc.), viene visualizzato questo messaggio aggiuntivo. Selezionare questa casella per copiare tutte le istantanee storiche nello storage a oggetti come file di backup per garantire la protezione più completa per i volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati degli snapshot con un'etichetta che corrisponde alle etichette nei criteri di replicazione e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati del sistema di storage primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di storage primario contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di origine.

Un bucket di Google Cloud Storage viene creato automaticamente nell'account di servizio indicato dalla chiave di accesso e dalla chiave segreta di Google immessi e i file di backup vengono memorizzati in tale account. Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su ONTAP S3 con backup e ripristino BlueXP

Completa alcuni passaggi nel backup e ripristino di BlueXP per iniziare a eseguire il backup dei dati di volume dai tuoi sistemi ONTAP locali principali. Puoi inviare backup a un sistema storage ONTAP secondario (un volume replicato) o a un bucket su un sistema ONTAP configurato come server S3 (un file di backup) o a entrambi.

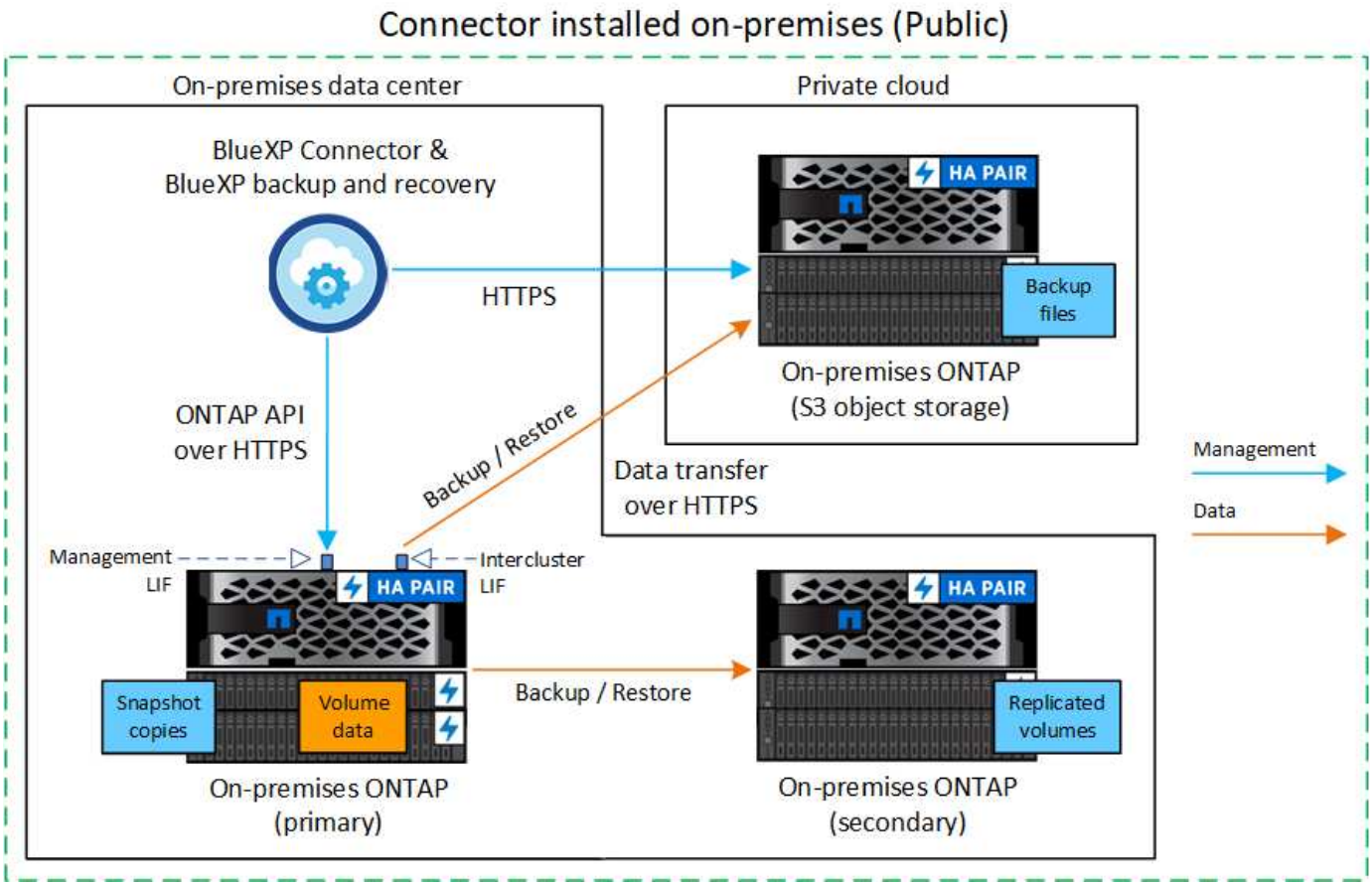
Il sistema ONTAP on-premise primario può essere un sistema FAS, AFF o ONTAP Select. Il sistema ONTAP secondario può essere un sistema ONTAP o Cloud Volumes ONTAP on-premise. Lo storage a oggetti può trovarsi su un sistema ONTAP on-premise o su un sistema Cloud Volumes ONTAP in cui hai abilitato un server per lo storage a oggetti Simple Storage Service (S3).

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Identificare il metodo di connessione

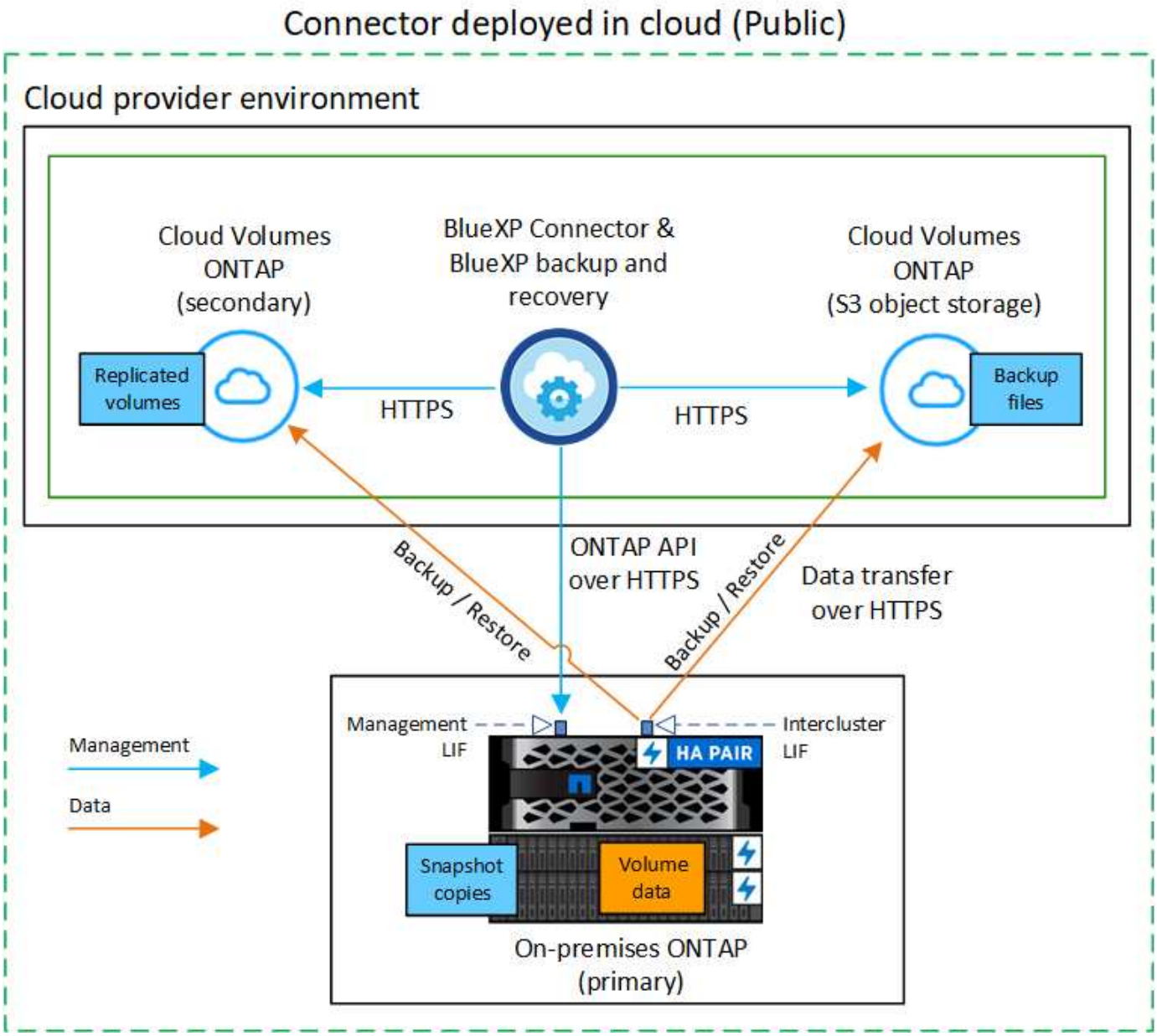
Esistono molte configurazioni in cui è possibile creare backup in un bucket S3 su un sistema ONTAP. Di seguito sono illustrati due scenari.

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario on-premise su un sistema ONTAP on-premise configurato per S3 e le connessioni da preparare tra di essi. Mostra inoltre una connessione a un sistema ONTAP secondario nella stessa posizione on-premise per replicare i volumi.



Quando il connettore e il sistema ONTAP primario on-premise vengono installati in un ambiente interno senza accesso a Internet (una distribuzione in modalità "privata"), il sistema ONTAP S3 deve trovarsi nello stesso data center on-premise.

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario in sede su un sistema Cloud Volumes ONTAP configurato per S3 e le connessioni da preparare tra di essi. Mostra inoltre una connessione a un sistema Cloud Volumes ONTAP secondario nello stesso ambiente di cloud provider per replicare i volumi.



In questo scenario, il connettore deve essere implementato nello stesso ambiente di cloud provider in cui vengono implementati i sistemi Cloud Volumes ONTAP.

Preparare il connettore BlueXP

BlueXP Connector è il software principale per la funzionalità BlueXP. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un connettore.

Creare o cambiare connettori

Quando effettui il backup dei dati su ONTAP S3, deve essere disponibile un connettore BlueXP on-premise o nel cloud. Sarà necessario installare un nuovo connettore o assicurarsi che il connettore attualmente selezionato si trovi in una di queste posizioni. Il connettore in loco può essere installato in un sito con o senza accesso a Internet.

- "Scopri di più sui connettori"
- "Installare il connettore nell'ambiente cloud"

- "Installazione del connettore su un host Linux con accesso a Internet"
- "Installazione del connettore su un host Linux senza accesso a Internet"
- "Passaggio da un connettore all'altro"

Preparare i requisiti di rete dei connettori

Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:

- Una connessione HTTPS sulla porta 443 al server ONTAP S3
- Una connessione HTTPS tramite la porta 443 alla LIF di gestione cluster ONTAP di origine
- Una connessione Internet in uscita tramite la porta 443 per il backup e ripristino di BlueXP (non necessaria quando il connettore viene installato in un sito "buio")

Considerazioni sulla modalità privata (sito scuro)

La funzionalità di backup e ripristino BlueXP è integrata nel connettore BlueXP. Una volta installato in modalità privata, è necessario aggiornare periodicamente il software del connettore per accedere alle nuove funzioni. Controllare "Novità di BlueXP per backup e ripristino" Per visualizzare le nuove funzionalità di ogni versione di backup e ripristino di BlueXP. Per utilizzare le nuove funzioni, seguire i passaggi da a. "Aggiornare il software del connettore".

Quando utilizzi il backup e recovery di BlueXP in un ambiente SaaS standard, i dati di configurazione di backup e recovery di BlueXP vengono sottoposti a backup nel cloud. Quando utilizzi il backup e recovery di BlueXP in un sito senza accesso a Internet, i dati di configurazione del backup e recovery di BlueXP vengono sottoposti a backup nel bucket ONTAP S3 in cui vengono archiviati i backup.

Verificare i requisiti di licenza

Prima di attivare il backup e il ripristino BlueXP per il cluster, è necessario acquistare e attivare una licenza BYOL di backup e ripristino BlueXP da NetApp. La licenza serve per il backup e il ripristino nello storage a oggetti, senza che sia necessaria alcuna licenza per creare copie Snapshot o volumi replicati. Questa licenza è destinata all'account e può essere utilizzata su più sistemi.

È necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL".

La licenza PAYGO non è supportata quando si esegue il backup dei file su ONTAP S3.

Preparare i cluster ONTAP

Dovrai preparare il tuo sistema ONTAP on-premise di origine e qualsiasi altro sistema ONTAP o Cloud Volumes ONTAP secondario on-premise.

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP in BlueXP
- Verificare i requisiti di sistema di ONTAP
- Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti
- Verificare i requisiti di rete di ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP in BlueXP

Il sistema ONTAP di origine on-premise e qualsiasi sistema ONTAP o Cloud Volumes ONTAP secondario on-premise devono essere disponibili su BlueXP Canvas.

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore.
"Scopri come individuare un cluster".

Verificare i requisiti di sistema di ONTAP

Assicurarsi che siano soddisfatti i seguenti requisiti ONTAP:

- Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa nel Premium Bundle o nel Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza il backup e ripristino BlueXP.

  Scopri come "gestire le licenze del cluster".

- L'ora e il fuso orario sono impostati correttamente. Scopri come "configurare l'ora del cluster".
- Se si intende replicare i dati, è necessario verificare che i sistemi di origine e di destinazione eseguano versioni di ONTAP compatibili prima di replicare i dati.

  "Visualizza le versioni di ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti

È necessario verificare che il sistema che si connette allo storage a oggetti soddisfi i seguenti requisiti.

- Quando si utilizza un'architettura di backup fan-out, le impostazioni devono essere configurate sul sistema di storage *primario*.
- Quando si utilizza un'architettura di backup a cascata, le impostazioni devono essere configurate sul sistema di storage *secondario*.

  "Ulteriori informazioni sui tipi di architettura di backup".

Sono necessari i seguenti requisiti di rete del cluster ONTAP:

- Il cluster ONTAP avvia una connessione HTTPS su una porta specificata dall'utente dalla LIF al server ONTAP S3 per le operazioni di backup e ripristino. La porta è configurabile durante la configurazione del backup.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

- ONTAP richiede una connessione in entrata dal connettore alla LIF di gestione del cluster.
- Su ogni nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti. "Scopri di più su IPspaces".

  Quando si imposta il backup e il ripristino di BlueXP, viene richiesto di utilizzare IPSpace. È necessario

scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

- I LIF intercluster dei nodi possono accedere all'archivio di oggetti (non necessario quando il connettore viene installato in un sito "buio").
- I server DNS sono stati configurati per la VM di storage in cui si trovano i volumi. Scopri come "Configurare i servizi DNS per SVM".
- Se si utilizza un IPSpace diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per ottenere l'accesso all'archivio oggetti.
- Aggiornare le regole del firewall, se necessario, per consentire le connessioni del servizio di backup e ripristino BlueXP da ONTAP allo storage a oggetti attraverso la porta specificata (in genere la porta 443) e il traffico di risoluzione dei nomi dalla VM di storage al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.

Preparare ONTAP S3 come destinazione di backup

È necessario abilitare un server per lo storage a oggetti Simple Storage Service (S3) nel cluster ONTAP che si intende utilizzare per i backup dello storage a oggetti. Vedere "Documentazione di ONTAP S3" per ulteriori informazioni.

Nota: è possibile rilevare questo cluster in BlueXP Canvas, ma non è identificato come server di storage a oggetti S3 e non è possibile trascinare e rilasciare un ambiente di lavoro di origine in questo ambiente di lavoro S3 per avviare l'attivazione del backup.

Questo sistema ONTAP deve soddisfare i seguenti requisiti.

Versioni di ONTAP supportate

Per i sistemi ONTAP on-premise è richiesto ONTAP 9,8 e versioni successive.
Per i sistemi Cloud Volumes ONTAP è richiesto ONTAP 9.9.1 e versioni successive.

Credenziali S3

È necessario aver creato un utente S3 per controllare l'accesso allo storage ONTAP S3. "Per ulteriori informazioni, consultare i documenti di ONTAP S3".

Quando si imposta il backup su ONTAP S3, la procedura guidata di backup richiede una chiave di accesso S3 e una chiave segreta per un account utente. L'account utente consente il backup e il recovery di BlueXP per autenticare e accedere ai bucket ONTAP S3 utilizzati per archiviare i backup. Le chiavi sono necessarie in modo che ONTAP S3 sappia chi sta effettuando la richiesta.

Queste chiavi di accesso devono essere associate a un utente che dispone delle seguenti autorizzazioni:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire policy e strategia di backup
- Rivedere le selezioni

Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:
   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.
   - Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda volumi, selezionare l'opzione **azioni (…)** e selezionare **attiva backup** per un singolo volume (che non ha già attivato la replica o il backup nell'archiviazione a oggetti).

   Nella pagina Introduzione della procedura guidata vengono mostrate le opzioni di protezione, tra cui snapshot locali, repliche e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.
2. Continuare con le seguenti opzioni:
   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Un volume protetto è un volume che presenta una o più delle

seguenti caratteristiche: criteri di snapshot, criteri di replica, criteri di backup su oggetto.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se per i volumi selezionati sono già state applicate le policy di snapshot o replica, le policy selezionate in seguito sovrascriveranno quelle esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup comporta la configurazione delle seguenti opzioni:

- Opzioni di protezione: se desideri implementare una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura: Se vuoi utilizzare un'architettura di backup fan-out o a cascata
- Criterio di snapshot locale
- Target e policy di replica
- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le seguenti opzioni. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Istantanee locali**: Crea copie istantanee locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi in un bucket su un sistema ONTAP configurato per S3.
2. **Architettura**: Se si sceglie sia la replica che il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Flussi di dati di backup dal sistema primario a quello secondario, quindi dallo storage secondario a quello a oggetti.
   - **Fan out**: Flussi di dati di backup dal sistema primario a quello secondario *e* dallo storage primario a quello a oggetti.

Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Se si desidera creare una policy personalizzata prima di attivare la snapshot, è possibile utilizzare Gestione di sistema o l'interfaccia a riga di comando di ONTAP `snapmirror policy create` comando. Fare riferimento a..

   Per creare una policy personalizzata utilizzando questo servizio, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Selezionare **Crea**.

4. **Replica**: Se si seleziona **Replica**, impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. In alternativa, selezionare l'aggregato di destinazione (o gli aggregati per volumi FlexGroup) e un prefisso o suffisso che verrà aggiunto al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno nuovo.

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Selezionare **Crea**.

5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **ONTAP S3**.
   - **Impostazioni provider**: Immettere i dettagli FQDN del server S3, la porta, la chiave di accesso e la chiave segreta degli utenti.

     La chiave di accesso e la chiave segreta si riferiscono all'utente creato per fornire al cluster ONTAP l'accesso al bucket S3.

   - **Rete**: Scegliere IPSpace nel cluster ONTAP di origine in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita (non richiesto quando il connettore viene installato in un sito "buio").

     Selezionando l'IPSpace corretto, il backup e recovery di BlueXP può configurare una connessione da ONTAP allo storage a oggetti ONTAP S3.

   - **Criterio di backup**: Selezionare un criterio di backup esistente o crearne uno nuovo.

     È possibile creare una policy con System Manager o l'interfaccia a riga di comando di ONTAP. Per creare un criterio personalizzato utilizzando l'interfaccia CLI di ONTAP `snapmirror policy create` fare riferimento a..

Per creare una policy personalizzata utilizzando questo servizio, fare riferimento a "Creare un criterio" .

Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

- Immettere il nome del criterio.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per i dettagli su DataLock e Ransomware Protection, fare riferimento a "Impostazioni dei criteri di backup su oggetti" .
- Selezionare **Crea**.

◦ **Esporta copie snapshot esistenti nell'archivio oggetti come file di backup**: se sono presenti copie snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta della pianificazione di backup appena selezionata (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo messaggio aggiuntivo. Selezionare questa casella per copiare tutte le istantanee storiche nello storage a oggetti come file di backup per garantire la protezione più completa per i volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo, vengono create istantanee con un'etichetta che corrisponde alle etichette dei criteri di replica e backup. Se i criteri non corrispondono, i backup non verranno creati.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti nelle copie snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di storage primario.

Nell'account di servizio viene creato un bucket S3 indicato dalla chiave di accesso S3 e dalla chiave segreta immessa, in cui vengono memorizzati i file di backup.

Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su StorageGRID con backup e ripristino BlueXP

Completa alcuni passaggi nel backup e ripristino di BlueXP per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP primari locali a un sistema di storage secondario e allo storage di oggetti nei tuoi sistemi NetApp StorageGRID.

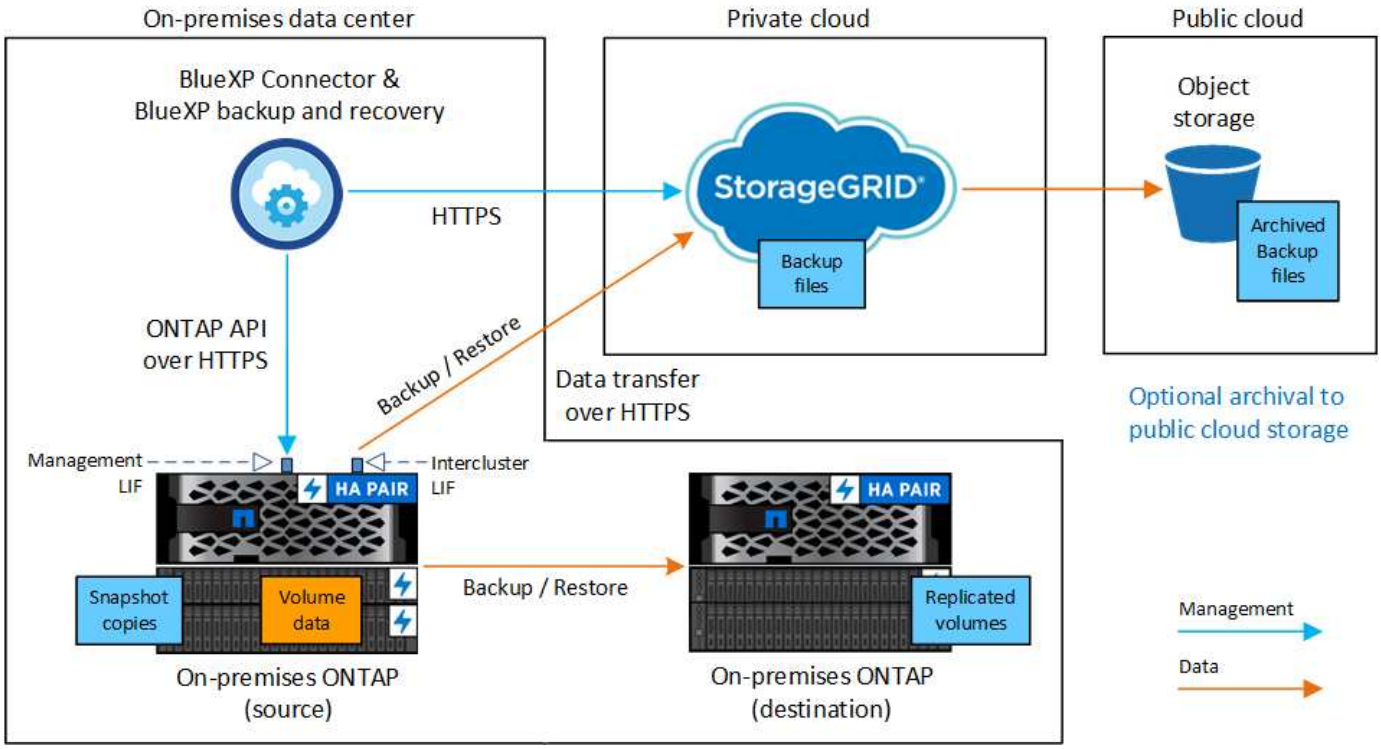
I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Identificare il metodo di connessione

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP on-premise su StorageGRID e le connessioni necessarie per prepararlo tra di loro.

In alternativa, è possibile connettersi a un sistema ONTAP secondario nella stessa posizione on-premise per replicare i volumi.



Quando il connettore e il sistema ONTAP on-premise sono installati in una posizione on-premise senza accesso a Internet (un "sito oscuro"), il sistema StorageGRID deve essere situato nello stesso data center on-

premise. L'archiviazione di file di backup meno recenti nel cloud pubblico non è supportata nelle configurazioni di siti oscuri.

Preparare il connettore BlueXP

BlueXP Connector è il software principale per la funzionalità BlueXP. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un connettore.

Creare o cambiare connettori

Quando si esegue il backup dei dati su StorageGRID, è necessario che sul posto sia disponibile un connettore BlueXP. È necessario installare un nuovo connettore o assicurarsi che il connettore attualmente selezionato risieda on-premise. Il connettore può essere installato in un sito con o senza accesso a Internet.

- "Scopri di più sui connettori"
- "Installazione del connettore su un host Linux con accesso a Internet"
- "Installazione del connettore su un host Linux senza accesso a Internet"
- "Passaggio da un connettore all'altro"

Preparare i requisiti di rete dei connettori

Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:

- Una connessione HTTPS tramite la porta 443 al nodo gateway StorageGRID
- Una connessione HTTPS sulla porta 443 alla LIF di gestione del cluster ONTAP
- Una connessione Internet in uscita tramite la porta 443 per il backup e ripristino di BlueXP (non necessaria quando il connettore viene installato in un sito "buio")

Considerazioni sulla modalità privata (sito scuro)

- La funzionalità di backup e ripristino BlueXP è integrata nel connettore BlueXP. Una volta installato in modalità privata, è necessario aggiornare periodicamente il software del connettore per accedere alle nuove funzioni. Controllare "Novità di BlueXP per backup e ripristino" Per visualizzare le nuove funzionalità di ogni versione di backup e ripristino di BlueXP. Per utilizzare le nuove funzioni, seguire i passaggi da a. "Aggiornare il software del connettore".

  La nuova versione di backup e ripristino di BlueXP, che include la possibilità di pianificare e creare copie Snapshot e volumi replicati, oltre alla creazione di backup nello storage a oggetti, richiede l'utilizzo della versione 3.9.31 o superiore di BlueXP Connector. Pertanto, si consiglia di ottenere questa versione più recente per gestire tutti i backup.

- Quando si utilizza il backup e ripristino BlueXP in un ambiente SaaS, viene eseguito il backup dei dati di configurazione di backup e ripristino BlueXP nel cloud. Quando si utilizza il backup e ripristino BlueXP in un sito senza accesso a Internet, viene eseguito il backup dei dati di configurazione di backup e ripristino BlueXP nel bucket StorageGRID in cui vengono memorizzati i backup.

Verificare i requisiti di licenza

Prima di attivare il backup e il ripristino BlueXP per il cluster, è necessario acquistare e attivare una licenza BYOL di backup e ripristino BlueXP da NetApp. Questa licenza è destinata all'account e può essere utilizzata su più sistemi.

È necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della

licenza. "Scopri come gestire le tue licenze BYOL".

La licenza PAYGO non è supportata quando si esegue il backup dei file su StorageGRID.

Preparare i cluster ONTAP

Dovrai preparare il tuo sistema ONTAP on-premise di origine e qualsiasi altro sistema ONTAP o Cloud Volumes ONTAP secondario on-premise.

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP in BlueXP
- Verificare i requisiti di sistema di ONTAP
- Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti
- Verificare i requisiti di rete di ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP in BlueXP

Il sistema ONTAP di origine on-premise e qualsiasi sistema ONTAP o Cloud Volumes ONTAP secondario on-premise devono essere disponibili su BlueXP Canvas.

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore.
"Scopri come individuare un cluster".

Verificare i requisiti di sistema di ONTAP

Assicurarsi che siano soddisfatti i seguenti requisiti ONTAP:

- Almeno ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa nel Premium Bundle o nel Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza il backup e ripristino BlueXP.

  Scopri come "gestire le licenze del cluster".

- L'ora e il fuso orario sono impostati correttamente. Scopri come "configurare l'ora del cluster".
- Se si intende replicare i dati, è necessario verificare che i sistemi di origine e di destinazione eseguano versioni di ONTAP compatibili prima di replicare i dati.

  "Visualizza le versioni di ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete di ONTAP per il backup dei dati nello storage a oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette allo storage a oggetti.

- Quando si utilizza un'architettura di backup fan-out, è necessario configurare le seguenti impostazioni sul sistema di storage *primario*.
- Quando si utilizza un'architettura di backup a cascata, è necessario configurare le seguenti impostazioni sul sistema di storage *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP:

- Il cluster ONTAP avvia una connessione HTTPS su una porta specificata dall'utente dal LIF dell'intercluster al nodo gateway StorageGRID per le operazioni di backup e ripristino. La porta è configurabile durante la configurazione del backup.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

- ONTAP richiede una connessione in entrata dal connettore alla LIF di gestione del cluster. Il connettore deve risiedere in sede.
- Su ogni nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti. "Scopri di più su IPspaces".

  Quando si imposta il backup e il ripristino di BlueXP, viene richiesto di utilizzare IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

- I LIF intercluster dei nodi possono accedere all'archivio di oggetti (non necessario quando il connettore viene installato in un sito "buio").
- I server DNS sono stati configurati per la VM di storage in cui si trovano i volumi. Scopri come "Configurare i servizi DNS per SVM".
- Se si utilizza un IPSpace diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere allo storage a oggetti.
- Aggiornare le regole del firewall, se necessario, per consentire le connessioni del servizio di backup e ripristino BlueXP da ONTAP allo storage a oggetti attraverso la porta specificata (in genere la porta 443) e il traffico di risoluzione dei nomi dalla VM di storage al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete di ONTAP per la replica dei volumi

Se intendi creare volumi replicati su un sistema ONTAP secondario utilizzando il backup e recovery di BlueXP, assicurati che i sistemi di origine e destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP on-premise

- Se il cluster si trova in sede, è necessario disporre di una connessione dalla rete aziendale alla rete virtuale nel cloud provider. Si tratta in genere di una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Poiché è possibile eseguire la replica su sistemi Cloud Volumes ONTAP o on-premise, esaminare i requisiti di peering per i sistemi ONTAP on-premise. "Visualizzare i prerequisiti per il peering dei cluster nella documentazione di ONTAP".

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di protezione predefinito.

Preparare StorageGRID come destinazione del backup

StorageGRID deve soddisfare i seguenti requisiti. Vedere "Documentazione StorageGRID" per ulteriori informazioni.

Per ulteriori informazioni sui requisiti di protezione DataLock e ransomware per StorageGRID, fare riferimento a "Opzioni di policy backup su oggetti".

Versioni di StorageGRID supportate

È supportato StorageGRID 10.3 e versioni successive.

Per utilizzare la protezione DataLock e ransomware per i backup, i sistemi StorageGRID devono disporre della versione 11.6.0.3 o superiore.

Per eseguire il tiering dei backup più vecchi nello storage di archiviazione cloud, i sistemi StorageGRID devono eseguire la versione 11.3 o superiore. Inoltre, i sistemi StorageGRID devono essere rilevati in BlueXP Canvas.

Per l'archiviazione degli utenti è necessario l'accesso IP al nodo di amministrazione.

L'accesso IP al gateway è sempre necessario.

Credenziali S3

È necessario aver creato un account tenant S3 per controllare l'accesso allo storage StorageGRID. "Per ulteriori informazioni, consultare la documentazione di StorageGRID".

Quando si imposta il backup su StorageGRID, la procedura guidata di backup richiede una chiave di accesso S3 e una chiave segreta per un account tenant. L'account tenant consente al backup e ripristino BlueXP di autenticare e accedere ai bucket StorageGRID utilizzati per memorizzare i backup. Le chiavi sono necessarie in modo che StorageGRID sappia chi sta effettuando la richiesta.

Queste chiavi di accesso devono essere associate a un utente che dispone delle seguenti autorizzazioni:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Versione degli oggetti

Non è necessario attivare manualmente la versione degli oggetti StorageGRID nel bucket dell'archivio di oggetti.

Preparatevi ad archiviare i file di backup meno recenti nello storage di cloud pubblico

Il tiering dei file di backup più vecchi nello storage di archiviazione consente di risparmiare denaro utilizzando una classe di storage meno costosa per i backup che potrebbero non essere necessari. StorageGRID è una soluzione on-premise (cloud privato) che non fornisce storage di archiviazione, ma è possibile spostare i file di backup meno recenti nello storage di archiviazione del cloud pubblico. Quando vengono utilizzati in questo modo, i dati che vengono trasferiti allo storage cloud o ripristinati dallo storage cloud, vanno tra StorageGRID e lo storage cloud - BlueXP non è coinvolto in questo trasferimento di dati.

Il supporto attuale consente di archiviare i backup nello storage AWS *S3 Glacier*/*S3 Glacier Deep Archive* o *Azure Archive*.

Requisiti ONTAP

- Il cluster deve utilizzare ONTAP 9.12.1 o versione successiva.

Requisiti StorageGRID

- StorageGRID deve utilizzare 11.4 o una versione successiva.
- Il StorageGRID deve essere "Scoperta e disponibile in BlueXP Canvas".

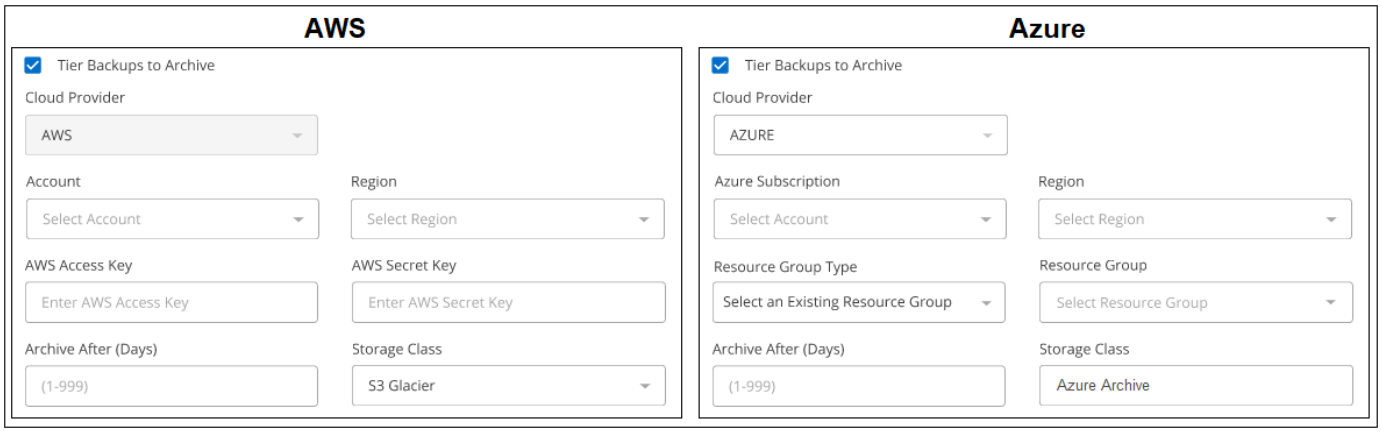
Requisiti Amazon S3

- Dovrai creare un account Amazon S3 per lo spazio di storage in cui verranno archiviati i backup.
- È possibile scegliere di eseguire il Tier dei backup nello storage AWS S3 Glacier o S3 Glacier Deep Archive. "Scopri di più sui Tier di archiviazione AWS".
- StorageGRID deve avere accesso completo al bucket (`s3:*`); tuttavia, se ciò non è possibile, il criterio bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Requisiti di Azure Blob*

- È necessario iscriversi a un abbonamento Azure per lo spazio di storage in cui verranno collocati i backup archiviati.
- L'attivazione guidata consente di utilizzare un gruppo di risorse esistente per gestire il container Blob che memorizzerà i backup oppure di creare un nuovo gruppo di risorse.

Quando si definiscono le impostazioni di archiviazione per il criterio di backup del cluster, immettere le credenziali del provider cloud e selezionare la classe di storage che si desidera utilizzare. Il backup e ripristino BlueXP crea il bucket cloud quando si attiva il backup per il cluster. Di seguito sono riportate le informazioni necessarie per lo storage di archiviazione AWS e Azure.



Le impostazioni dei criteri di archiviazione selezionate genereranno un criterio di gestione del ciclo di vita delle informazioni (ILM) in StorageGRID e aggiungeranno le impostazioni come "regole".

- Se esiste già un criterio ILM attivo, verranno aggiunte nuove regole al criterio ILM per spostare i dati nel livello di archiviazione.
- Se esiste un criterio ILM esistente nello stato "proposto", non sarà possibile creare e attivare un nuovo criterio ILM. "Scopri di più sulle policy e le regole ILM di StorageGRID".

Attivare i backup sui volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dall'ambiente di lavoro on-premise.

La procedura guidata consente di eseguire le seguenti operazioni principali:

- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

Avviare la procedura guidata

Fasi

1. Accedere alla procedura guidata attiva backup e ripristino utilizzando uno dei seguenti metodi:

   - Nell'area di lavoro di BlueXP, selezionare l'ambiente di lavoro e selezionare **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello a destra.

     Se la destinazione dei backup esiste come ambiente di lavoro su Canvas, è possibile trascinare il cluster ONTAP sullo storage a oggetti.

   - Selezionare **Volumes** (volumi) nella barra Backup and Recovery (Backup e ripristino). Dalla scheda Volumes (volumi), selezionare l'opzione **Actions (…)** e selezionare **Activate Backup** (attiva backup) per un singolo volume (che non dispone già di replica o backup su storage a oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se è stata eseguita la seconda opzione in questa fase, viene visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Continuare con le seguenti opzioni:

   - Se si dispone già di un connettore BlueXP, tutti i dispositivi sono impostati. Seleziona **Avanti**.
   - Se non si dispone già di un connettore BlueXP, viene visualizzata l'opzione **Aggiungi un connettore**. Fare riferimento a. Preparare il connettore BlueXP.

Selezionare i volumi di cui si desidera eseguire il backup

Scegliere i volumi che si desidera proteggere. Per volume protetto si intende un volume con una o più delle seguenti opzioni: Policy di snapshot, policy di replica, policy di backup su oggetti.

Puoi scegliere di proteggere volumi FlexVol o FlexGroup; tuttavia, non puoi selezionare un mix di questi volumi quando si attiva il backup per un ambiente di lavoro. Scopri come "attivare il backup per volumi aggiuntivi nell'ambiente di lavoro" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock. Tutti i volumi devono avere abilitato SnapLock Enterprise o avere disattivato SnapLock.

Fasi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Select Volumes (Seleziona volumi), selezionare il volume o i volumi che si desidera proteggere.
   - In alternativa, filtrare le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (è possibile selezionare solo i volumi FlexGroup uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume, quindi selezionare la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup implica l'impostazione delle seguenti opzioni:

- Sia che si desideri una o tutte le opzioni di backup: Snapshot locali, replica e backup su storage a oggetti
- Architettura
- Criterio di snapshot locale
- Target e policy di replica

  Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni sullo storage a oggetti (provider, crittografia, rete, policy di backup e opzioni di esportazione).

Fasi

1. Nella pagina Definisci strategia di backup, scegliere una o tutte le opzioni seguenti. Per impostazione predefinita, vengono selezionate tutte e tre le opzioni:
   - **Snapshot locali**: se si esegue una replica o un backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replication**: Consente di creare volumi replicati su un altro sistema storage ONTAP.
   - **Backup**: Esegue il backup dei volumi nello storage a oggetti.
2. **Architettura**: Se si sceglie sia la replica che il backup, scegliere uno dei seguenti flussi di informazioni:
   - **Cascading**: Le informazioni passano dal primario al secondario, quindi dal secondario allo storage a oggetti.
   - **Fan out**: I flussi di informazioni dal primario al secondario *e* dallo storage primario a oggetti.

     Per i dettagli su queste architetture, fare riferimento a "Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

   - Immettere il nome del criterio.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Selezionare **Crea**.

4. **Replication**: Impostare le seguenti opzioni:
   - **Destinazione della replica**: Selezionare l'ambiente di lavoro di destinazione e SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o suffisso da aggiungere al nome del volume replicato.
   - **Criterio di replica**: Scegliere un criterio di replica esistente o crearne uno.

     Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Selezionare **Crea**.

5. **Backup su oggetto**: Se si seleziona **Backup**, impostare le seguenti opzioni:
   - **Provider**: Selezionare **StorageGRID**.
   - **Provider settings** (Impostazioni provider): Immettere i dettagli FQDN del nodo gateway del provider, la porta, la chiave di accesso e la chiave segreta.

     La chiave di accesso e la chiave segreta sono destinate all'utente IAM creato per consentire al cluster ONTAP di accedere al bucket.

   - **Rete**: Scegliere l'IPSpace nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita (non richiesto quando il connettore viene installato in un sito "buio").

     La selezione dell'IPSpace corretto garantisce che il backup e ripristino BlueXP possa configurare una connessione da ONTAP allo storage a oggetti StorageGRID.

   - **Criterio di backup**: Selezionare un criterio di archiviazione Backup su oggetti esistente o crearne uno.

     Per creare una policy personalizzata, fare riferimento a "Creare un criterio" .

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:

     - Immettere il nome del criterio.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per i dettagli su DataLock e Ransomware Protection, fare riferimento a "Impostazioni dei criteri di

backup su oggetti" .

Se il cluster utilizza ONTAP 9.11.1 o versione successiva, è possibile scegliere di proteggere i backup da attacchi ransomware e di eliminazione configurando *DataLock e ransomware Protection*. *DataLock* protegge i file di backup dalla modifica o dall'eliminazione, e *ransomware Protection* analizza i file di backup per individuare la prova di un attacco ransomware nei file di backup.

- Selezionare **Crea**.

Se il cluster utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o successiva, è possibile scegliere di raggruppare i backup meno recenti in Tier di archivio del cloud pubblico dopo un certo numero di giorni. Attualmente il supporto è per i Tier di storage AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. Scopri come configurare i tuoi sistemi per questa funzionalità.

- **Tier backup to public cloud**: Seleziona il provider cloud a cui vuoi eseguire il Tier backup e inserisci i dettagli del provider.

  Selezionare o creare un nuovo cluster StorageGRID. Per ulteriori informazioni sulla creazione di un cluster StorageGRID in modo che BlueXP possa rilevarlo, fare riferimento a. "Documentazione StorageGRID".

- **Esporta copie snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti copie snapshot locali per i volumi in questo ambiente di lavoro che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo ambiente di lavoro (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo messaggio aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup e garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedere le selezioni

Questa è la possibilità di rivedere le selezioni e apportare eventuali modifiche.

Fasi

1. Nella pagina Review (esamina), rivedere le selezioni.
2. Facoltativamente, selezionare la casella **Sincronizza automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo, vengono create istantanee con un'etichetta che corrisponde alle etichette dei criteri di replica e backup.
3. Selezionare **Activate Backup** (attiva backup).

Risultato

Il backup e ripristino di BlueXP inizia a eseguire i backup iniziali dei volumi. Il trasferimento di riferimento del volume replicato e del file di backup include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati dello storage primario contenuti nelle copie Snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di storage primario.

Nell'account di servizio viene creato un bucket S3 indicato dalla chiave di accesso S3 e dalla chiave segreta immessa, in cui vengono memorizzati i file di backup.

Viene visualizzata la dashboard di backup del volume, che consente di monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando "Pagina Job Monitoring" .

Mostra i comandi API

È possibile visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata attiva backup e ripristino. Questa operazione potrebbe essere utile per automatizzare l'attivazione del backup negli ambienti di lavoro futuri.

Fasi

1. Dalla procedura guidata Activate backup and recovery (attiva backup e ripristino), selezionare **View API request** (Visualizza richiesta API).
2. Per copiare i comandi negli Appunti, selezionare l'icona **Copia**.

Migrazione dei volumi tramite SnapMirror su Cloud Resync con backup e ripristino BlueXP

La funzionalità SnapMirror to Cloud Resync nel backup e ripristino di BlueXP semplifica la protezione e la continuità dei dati durante le migrazioni dei volumi negli ambienti NetApp. Quando un volume viene migrato usando la replica logica SnapMirror (LRSE), da un'implementazione NetApp on-premise a un'altra o a una soluzione basata sul cloud come Cloud Volumes ONTAP o Cloud Volumes Service, SnapMirror to Cloud Resync garantisce che i backup cloud esistenti rimangano intatti e operativi.

Questa funzionalità elimina la necessità di un'operazione di re-baseline, che richiede molto tempo e risorse, consentendo alle operazioni di backup di continuare anche dopo la migrazione. Questa funzionalità è molto utile negli scenari di migrazione dei carichi di lavoro, a supporto di FlexVol e gruppi di lavoro, ed è disponibile a partire dalla versione 9.16.1 di ONTAP.

Questa funzionalità è disponibile a partire dalla versione 4.0.3 BlueXP backup and recovery, rilasciata a maggio 2025.

Mantenendo la continuità del backup in tutti gli ambienti, SnapMirror to Cloud Resync migliora l'efficienza delle operazioni e riduce la complessità della gestione dei dati nel cloud ibrido e multicloud.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster ONTAP di destinazione deve eseguire ONTAP versione 9.16.1 o successiva.
- Il vecchio cluster ONTAP di origine deve essere protetto tramite BlueXP backup and recovery.
- La funzionalità SnapMirror to Cloud Resync è disponibile a partire dalla versione 4.0.3 BlueXP backup and recovery, rilasciata a maggio 2025.
- L'ultimo backup nell'archivio oggetti deve essere lo snapshot comune tra la vecchia origine, la nuova origine e l'archivio oggetti. Lo snapshot comune non può essere più vecchio dell'ultimo snapshot sottoposto a backup nell'archivio oggetti.
- Sia i criteri snapshot che quelli SnapMirror , utilizzati sul vecchio ONTAP , devono essere creati sul nuovo

cluster ONTAP prima di avviare l'operazione di risincronizzazione. Se nel processo di risincronizzazione verrà utilizzata una policy, sarà necessario crearla. L'operazione di risincronizzazione non crea i criteri.

- Assicurarsi che il criterio SnapMirror applicato alla relazione SnapMirror del volume di migrazione includa la stessa etichetta utilizzata dalla relazione cloud. Per evitare problemi, utilizzare la policy che gestisce un mirror esatto del volume e di tutti gli snapshot.

Risincronizzazione di SnapMirror al cloud dopo le migrazioni che utilizzano i metodi SVM-Migrate, SVM-DR o Head Swap non sono attualmente supportati.

Come funziona il BlueXP backup and recovery SnapMirror a Cloud Resync

Se completi un refresh tecnico o migra i volumi da un cluster ONTAP a un altro, è importante che i tuoi backup continuino a funzionare senza interruzioni. SnapMirror to Cloud Resync di BlueXP consente di eseguire backup e recovery garantendo che i backup nel cloud restino coerenti anche dopo la migrazione dei volumi.

Ecco un esempio:

Immagina di avere un volume on-premise chiamato Vol1a. Questo volume dispone di tre snapshot: S1, S2 e S3. Queste snapshot sono come punti di ripristino. VOL1 sta già eseguendo il backup su un endpoint dell'archivio di oggetti cloud utilizzando SnapMirror to Cloud (SM-C). Tuttavia, finora solo S1 e S2 sono stati sottoposti a backup nell'archivio oggetti.

Adesso vuoi migrare Vol1 PB a un altro cluster ONTAP, A tale scopo, è necessario creare una relazione LRSE (SnapMirror Logical Replication) con un nuovo volume cloud denominato Vol1b. In questo modo è possibile trasferire tutte e tre le snapshot (S1, S2 e S3) da Vol1a a Vol1b.

Al termine della migrazione, è possibile eseguire la seguente configurazione:

- La relazione SM-C originale (archivio oggetti Vol1a →) viene eliminata.
- Viene anche eliminata la relazione LRSE (Vol1a → Vol1b).
- Vol1b è ora il volume attivo.

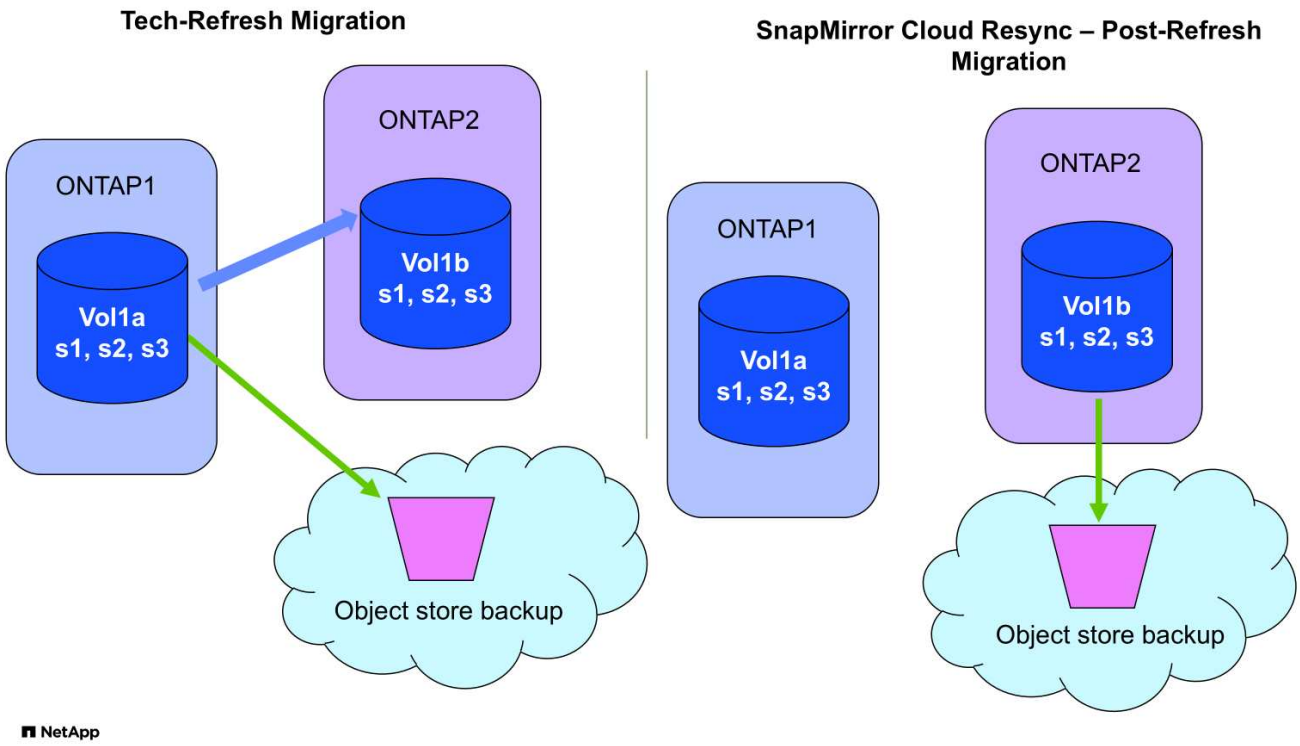
A questo punto, si desidera continuare il backup di Vol1b nello stesso endpoint cloud. Tuttavia, invece di eseguire un backup completo da zero (che richiederebbe tempo e risorse), è possibile utilizzare SnapMirror per la risincronizzazione del cloud.

Ecco come funziona la risincronizzazione:

- Il sistema verifica la presenza di uno snapshot comune tra Vol1a e l'archivio di oggetti. In questo caso, entrambi hanno S2.
- A causa di questa istantanea condivisa, il sistema deve trasferire solo le modifiche incrementali tra S2 e S3.

Ciò significa che all'archivio di oggetti vengono aggiunti solo i nuovi dati dopo l'invio di S2, non l'intero volume.

Questo processo consente di evitare l'invio di dati già sottoposti a backup, di risparmiare larghezza di banda e di garantire che la catena di backup continui senza problemi dopo la migrazione.



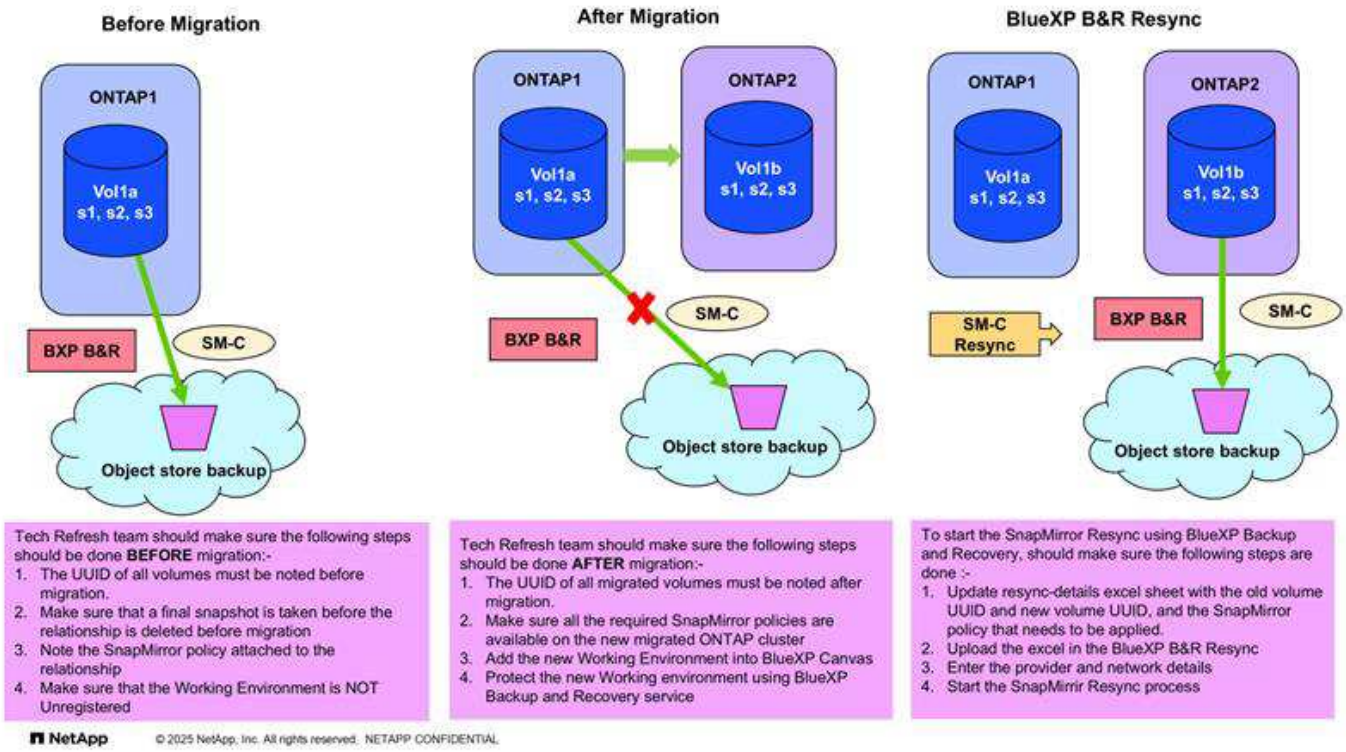
Note sulla procedura

- Le migrazioni e i tech refresh non vengono eseguiti utilizzando backup e recovery di BlueXP . Devono essere eseguite da un team di Professional Services o da un amministratore dello storage qualificato.
- Un team di migrazione NetApp si occupa della creazione di una relazione SnapMirror tra i cluster ONTAP di origine e di destinazione per facilitare la migrazione dei volumi.
- Assicurati che la migrazione durante un tech refresh si basi su una migrazione basata su SnapMirror.

Come eseguire la migrazione dei volumi usando SnapMirror per la risincronizzazione del cloud

La migrazione dei volumi che utilizzano SnapMirror per la risincronizzazione del cloud comporta i seguenti passaggi principali, ciascuno descritto in maggior dettaglio di seguito:

- **Follow a pre-Migration Checklist**: Prima di iniziare la migrazione, un team Tech Refresh di NetApp garantisce la soddisfazione dei seguenti prerequisiti per evitare la perdita di dati e garantire un processo di migrazione senza problemi.
- **Follow a post-Migration Checklist**: Dopo la migrazione, un team Tech Refresh di NetApp si assicura che siano completati i seguenti passaggi per stabilire la protezione e prepararsi alla risincronizzazione.
- **Eseguire una risincronizzazione da SnapMirror al cloud**: Dopo la migrazione, un team Tech Refresh di NetApp esegue un'operazione di risincronizzazione da SnapMirror al cloud per riprendere i backup nel cloud dai volumi appena migrati.



Segui l'elenco di controllo pre-migrazione

Prima di iniziare la migrazione, il team Tech Refresh di NetApp garantisce che vengano soddisfatti i seguenti prerequisiti per evitare perdite di dati e assicurare un processo di migrazione agevole.

1. Assicurati che tutti i volumi da migrare siano protetti utilizzando il backup e il recovery di BlueXP .
2. Registra UUID istanza volume. Annotare gli UUID di istanza di tutti i volumi prima di iniziare la migrazione. Questi identificatori sono fondamentali per la mappatura e la risincronizzazione delle operazioni in un secondo momento.
3. Creare una snapshot finale di ciascun volume per preservare lo stato più recente, prima di eliminare qualsiasi relazione SnapMirror.
4. Documentare i criteri SnapMirror. Registrare il criterio SnapMirror attualmente allegato alla relazione di ciascun volume. Questa operazione sarà necessaria in seguito durante il processo di risincronizzazione da SnapMirror al cloud.
5. Elimina le relazioni cloud SnapMirror con l'archivio di oggetti.
6. Creazione di una relazione SnapMirror standard con il nuovo cluster ONTAP per migrare il volume nel nuovo cluster ONTAP di destinazione.

Segui la checklist post-migrazione

Dopo la migrazione, un team Tech Refresh di NetApp garantisce che siano completate le seguenti fasi per stabilire la protezione e prepararsi alla risincronizzazione.

1. Registrare nuovi UUID istanze di volume di tutti i volumi migrati nel cluster ONTAP di destinazione.
2. Verificare che tutte le policy SnapMirror richieste, disponibili nel vecchio cluster ONTAP, siano configurate correttamente nel nuovo cluster ONTAP.
3. Aggiungi il nuovo cluster ONTAP come ambiente di lavoro in BlueXP Canvas.

Deve essere utilizzato l'UUID dell'istanza del volume, non l'ID del volume. L'UUID dell'istanza del volume è un identificatore univoco che rimane coerente durante le migrazioni, mentre l'ID del volume può cambiare dopo la migrazione.

Eseguire una risincronizzazione da SnapMirror al cloud

Dopo la migrazione, un team Tech Refresh di NetApp esegue un'operazione di risincronizzazione da SnapMirror al cloud per riprendere i backup cloud dai volumi appena migrati.

1. Aggiungi il nuovo cluster ONTAP come ambiente di lavoro in BlueXP Canvas.
2. Esaminare la pagina dei volumi di backup e ripristino di BlueXP per verificare che siano disponibili i dettagli del vecchio ambiente di lavoro di origine.
3. Nella pagina volumi di backup e ripristino di BlueXP , selezionare **Impostazioni di backup**.
   - Nella pagina Impostazioni di backup, seleziona **Visualizza tutto**.
   - Dal menu Azioni … a destra della *nuova* origine, seleziona **Risincronizza backup**.
4. Nella pagina Resync Working Environment (ambiente di lavoro risincronizzato), effettuare le seguenti operazioni:
   a. **Nuovo ambiente di lavoro di origine**: Immettere il nuovo cluster ONTAP in cui sono stati migrati i volumi.
   b. **Archivio oggetti di destinazione esistente**: Selezionare l'archivio oggetti di destinazione che contiene i backup dal vecchio ambiente di lavoro di origine.
5. Selezionare **Scarica modello CSV** per scaricare il foglio Excel Dettagli risincronizzazione. Utilizzare questo foglio per immettere i dettagli dei volumi da migrare. Nel file CSV, immettere i seguenti dettagli:
   - UUID della vecchia istanza di volume dal cluster di origine
   - Il nuovo UUID dell'istanza di volume dal cluster di destinazione
   - La policy SnapMirror da applicare alla nuova relazione.
6. Selezionare **carica** sotto **carica dettagli mappatura volume** per caricare il foglio CSV completato nell'interfaccia utente di backup e ripristino di BlueXP .

   Deve essere utilizzato l'UUID dell'istanza del volume, non l'ID del volume. L'UUID dell'istanza del volume è un identificatore univoco che rimane coerente durante le migrazioni, mentre l'ID del volume può cambiare dopo la migrazione.

7. Immettere le informazioni di configurazione del provider e della rete richieste per l'operazione di risincronizzazione.
8. Selezionare **Invia** per avviare il processo di convalida.

   Il BlueXP backup and recovery verificano che ogni volume selezionato per la risincronizzazione sia lo snapshot più recente e disponga di almeno uno snapshot comune. Ciò garantisce che i volumi siano pronti per l'operazione SnapMirror to Cloud Resync.

9. Esaminare i risultati della convalida, inclusi i nuovi nomi del volume di origine e lo stato di risincronizzazione di ogni volume.
10. Verificare l'idoneità del volume. Il sistema verifica se i volumi sono idonei per la risincronizzazione. Se un volume non è idoneo, significa che non si tratta dell'ultimo snapshot oppure non è stato trovato alcun snapshot comune.

Per garantire che i volumi rimangano idonei per l'operazione di risincronizzazione di SnapMirror sul cloud, creare un snapshot finale di ciascun volume prima di eliminare qualsiasi relazione SnapMirror durante la fase di pre-migrazione. In questo modo, viene conservato lo stato più recente dei dati.

11. Selezionare **Risincronizzazione** per avviare l'operazione di risincronizzazione. Il sistema utilizza lo snapshot più recente e comune per trasferire solo le modifiche incrementali, garantendo la continuità del backup.
12. Monitorare il processo di risincronizzazione nella pagina Job Monitor.

Ripristinare i dati di configurazione BlueXP backup and recovery in un sito oscuro

Quando si utilizza il BlueXP backup and recovery in un sito senza accesso a Internet, noto come *modalità privata*, i dati di configurazione BlueXP backup and recovery vengono sottoposti a backup nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host di BlueXP Connector, è possibile distribuire un nuovo Connector e ripristinare i dati critici BlueXP backup and recovery .

Questa procedura si applica solo ai dati di volume ONTAP .

Quando si utilizza il BlueXP backup and recovery in un ambiente SaaS in cui BlueXP Connector è distribuito presso il provider cloud o sul proprio sistema host con accesso a Internet, tutti i dati importanti di configurazione BlueXP backup and recovery vengono sottoposti a backup e protetti nel cloud. Se riscontri un problema con il connettore, crea semplicemente un nuovo connettore e aggiungi i tuoi ambienti di lavoro: i dettagli del backup verranno ripristinati automaticamente.

Esistono due tipi di dati sottoposti a backup:

- Database BlueXP backup and recovery : contiene un elenco di tutti i volumi, file di backup, criteri di backup e informazioni di configurazione.
- File di catalogo indicizzati: contengono indici dettagliati utilizzati per la funzionalità di ricerca e ripristino, che rendono le ricerche molto rapide ed efficienti quando si cercano dati di volume che si desidera ripristinare.

Questi dati vengono sottoposti a backup una volta al giorno a mezzanotte e vengono conservate al massimo 7 copie di ciascun file. Se il connettore gestisce più ambienti di lavoro ONTAP locali, i file BlueXP backup and recovery saranno posizionati nel bucket dell'ambiente di lavoro attivato per primo.

Nessun dato di volume viene mai incluso nel database BlueXP backup and recovery o nei file del catalogo indicizzato.

Ripristina i dati BlueXP backup and recovery su un nuovo connettore BlueXP

Se il tuo BlueXP Connector locale subisce un errore catastrofico, dovrai installare un nuovo Connector e quindi ripristinare i dati BlueXP backup and recovery sul nuovo Connector.

Per ripristinare il funzionamento del sistema BlueXP backup and recovery, è necessario eseguire le seguenti operazioni:

- Installa un nuovo connettore BlueXP
- Ripristinare il database BlueXP backup and recovery
- Ripristina i file del catalogo indicizzato
- Riscopri tutti i tuoi sistemi ONTAP on-premise e i sistemi StorageGRID nell'interfaccia utente BlueXP

Una volta verificato che il sistema è tornato a funzionare, ti consigliamo di creare nuovi file di backup.

Cosa ti servirà

Sarà necessario accedere ai backup più recenti del database e dell'indice dal bucket StorageGRID o ONTAP S3 in cui sono archiviati i file di backup:

- File di database MySQL BlueXP backup and recovery

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/` , e si chiama `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- File zip di backup del catalogo indicizzato

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/catalog_backup/` , e si chiama `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installa un nuovo connettore su un nuovo host Linux locale

Quando installi un nuovo BlueXP Connector, assicurati di scaricare la stessa versione del software installata sul Connector originale. Le modifiche periodiche alla struttura del database BlueXP backup and recovery potrebbero rendere le nuove versioni del software incompatibili con i backup del database originali. Puoi "aggiornare il software Connector alla versione più recente dopo aver ripristinato il database di backup" .

1. "Installa BlueXP Connector su un nuovo host Linux locale"
2. Accedi a BlueXP utilizzando le credenziali utente amministratore appena create.

Ripristinare il database BlueXP backup and recovery

1. Copiare il backup MySQL dalla posizione di backup al nuovo host del connettore. Di seguito utilizzeremo il nome file di esempio "CBS_DB_Backup_23_05_2023.sql".
2. Copiare il backup nel contenitore Docker MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

   ```
   docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
   ```

   ```
   podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
   ```

3. Accedere alla shell del contenitore MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

   ```
   docker exec -it ds_mysql_1 sh
   ```

```
podman exec -it ds_mysql_1 sh
```

4. Nella shell del contenitore, distribuire "env".
5. Ti servirà la password del database MySQL, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il BlueXP backup and recovery utilizzando il seguente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verificare che il BlueXP backup and recovery siano stati ripristinati correttamente utilizzando i seguenti comandi SQL:

```
mysql -u root -p cloud_backup
```

Inserisci la password.

```
mysql> show tables;
mysql> select * from volume;
```

Controlla se i volumi mostrati sono gli stessi presenti nell'ambiente originale.

Ripristina i file del catalogo indicizzato

1. Copiare il file zip di backup del catalogo indicizzato (utilizzeremo il nome file di esempio "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") dalla posizione di backup al nuovo host del connettore nella cartella "/opt/application/netapp/cbs".
2. Decomprimere il file "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" utilizzando il seguente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Eseguire il comando **ls** per assicurarsi che sia stata creata la cartella "catalogdb1" con le sottocartelle "changes" e "snapshots".

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti gli ambienti di lavoro ONTAP on-prem"che erano disponibili nel tuo ambiente precedente. Ciò include il sistema ONTAP utilizzato come server S3.
2. "Scopri i tuoi sistemi StorageGRID" .

Impostare i dettagli dell'ambiente StorageGRID

Aggiungere i dettagli del sistema StorageGRID associato ai propri ambienti di lavoro ONTAP così come sono

stati configurati nella configurazione originale del connettore utilizzando "API BlueXP" .

Le seguenti informazioni si applicano alle installazioni in modalità privata a partire da BlueXP 3.9.xx. Per le versioni precedenti, utilizzare la seguente procedura: "DarkSite Cloud Backup: backup e ripristino di MySQL e catalogo indicizzato" .

Sarà necessario eseguire questi passaggi per ogni sistema che esegue il backup dei dati su StorageGRID.

1. Estrarre il token di autorizzazione utilizzando la seguente API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d
'{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pa
ssword"}
> '
```

   Mentre l'indirizzo IP, il nome utente e le password sono valori personalizzati, il nome dell'account non lo è. Il nome dell'account è sempre "account-DARKSITE1". Inoltre, il nome utente deve essere formattato come indirizzo email.

   Questa API restituirà una risposta simile alla seguente. È possibile recuperare il token di autorizzazione come mostrato di seguito.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Estrarre l'ID dell'ambiente di lavoro e l'X-Agent-Id utilizzando l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Questa API restituirà una risposta simile alla seguente. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-agent-id*.

3. Aggiornare il database BlueXP backup and recovery con i dettagli del sistema StorageGRID associato agli ambienti di lavoro. Assicurarsi di immettere il nome di dominio completo di StorageGRID, nonché la chiave di accesso e la chiave di archiviazione come mostrato di seguito:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verificare le impostazioni BlueXP backup and recovery

1. Selezionare ciascun ambiente di lavoro ONTAP e fare clic su **Visualizza backup** accanto al servizio Backup e ripristino nel pannello di destra.

   Dovresti essere in grado di vedere tutti i backup creati per i tuoi volumi.

2. Nella Dashboard di ripristino, nella sezione Cerca e ripristina, fai clic su **Impostazioni di indicizzazione**.

   Assicurarsi che gli ambienti di lavoro in cui era precedentemente abilitata la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Cerca e ripristina, esegui alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato sia stato completato correttamente.

Gestisci i backup per i tuoi sistemi ONTAP con il backup e il ripristino BlueXP

Con il BlueXP backup and recovery, gestisci i backup per i tuoi sistemi Cloud Volumes ONTAP e ONTAP on-premise modificando la pianificazione dei backup, abilitando/disabilitando i backup dei volumi, sospendendo i backup, eliminando i backup, forzando l'eliminazione dei backup e altro ancora. Ciò include tutti i tipi di backup, tra cui copie snapshot, volumi replicati e file di backup nell'archiviazione di oggetti. È anche possibile annullare la registrazione BlueXP backup and recovery.

Non gestire o modificare i file di backup direttamente sui sistemi storage o dall'ambiente del cloud provider. Questo potrebbe danneggiare i file e causare una configurazione non supportata.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Visualizzare lo stato di backup dei volumi negli ambienti di lavoro

È possibile visualizzare un elenco di tutti i volumi di cui si sta effettuando il backup nella dashboard di backup dei volumi. Ciò include tutti i tipi di backup, tra cui copie snapshot, volumi replicati e file di backup nell'archiviazione di oggetti. È inoltre possibile visualizzare i volumi degli ambienti di lavoro che non sono attualmente sottoposti a backup.

Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Selezionare la scheda **Volumi** per visualizzare l'elenco dei volumi sottoposti a backup per i sistemi Cloud Volumes ONTAP e ONTAP locali.
3. Se si cercano volumi specifici in determinati ambienti di lavoro, è possibile perfezionare l'elenco in base all'ambiente di lavoro e al volume. È inoltre possibile utilizzare il filtro di ricerca oppure ordinare le colonne in base allo stile del volume (FlexVol o FlexGroup), al tipo di volume e altro ancora.

   Per visualizzare colonne aggiuntive (aggregati, stile di sicurezza (Windows o UNIX), criterio di snapshot, criterio di replica e criterio di backup), selezionare il segno più.

4. Esaminare lo stato delle opzioni di protezione nella colonna "Existing Protection" (protezione esistente). Le

3 icone stanno per "Copie snapshot locali", "Volumi replicati" e "Backup nell'archiviazione di oggetti".

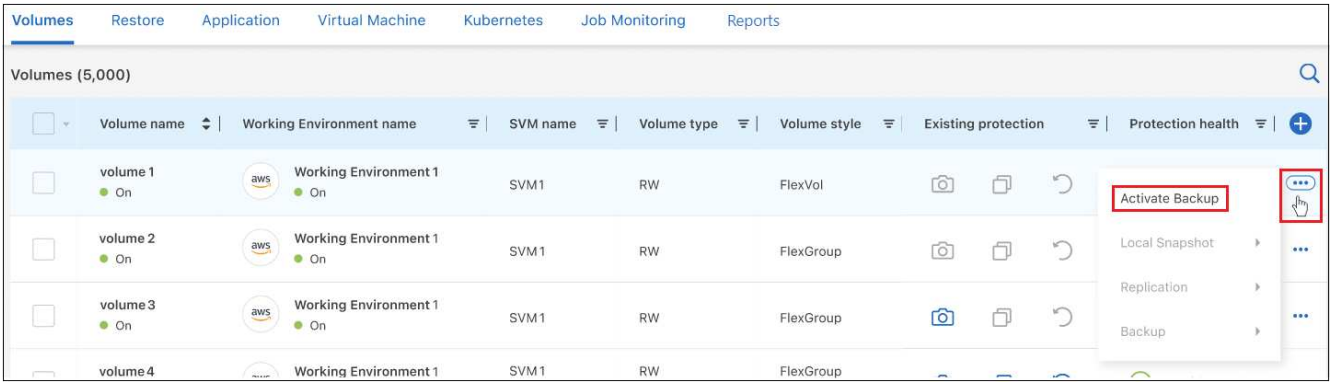
Ogni icona è blu quando il tipo di backup è attivato e grigia quando il tipo di backup è inattivo. È possibile spostare il cursore su ciascuna icona per visualizzare la policy di backup utilizzata e altre informazioni pertinenti per ciascun tipo di backup.

Attivare il backup su volumi aggiuntivi in un ambiente di lavoro

Se è stato attivato il backup solo su alcuni volumi in un ambiente di lavoro quando è stato attivato il backup e ripristino BlueXP per la prima volta, è possibile attivare i backup su volumi aggiuntivi in un secondo momento.

Fasi

1. Dalla scheda **Volumes** (volumi), identificare il volume su cui si desidera attivare i backup e selezionare il menu Actions (azioni) ••• Alla fine della riga e selezionare **Activate backup** (attiva backup).



2. Nella pagina *define backup strategy*, selezionare l'architettura di backup, quindi definire i criteri e altri dettagli per le copie Snapshot locali, i volumi replicati e i file di backup. Consultare i dettagli relativi alle opzioni di backup dei volumi iniziali attivati in questo ambiente di lavoro. Quindi selezionare **Avanti**.
3. Controllare le impostazioni di backup per questo volume, quindi selezionare **Attiva backup**.

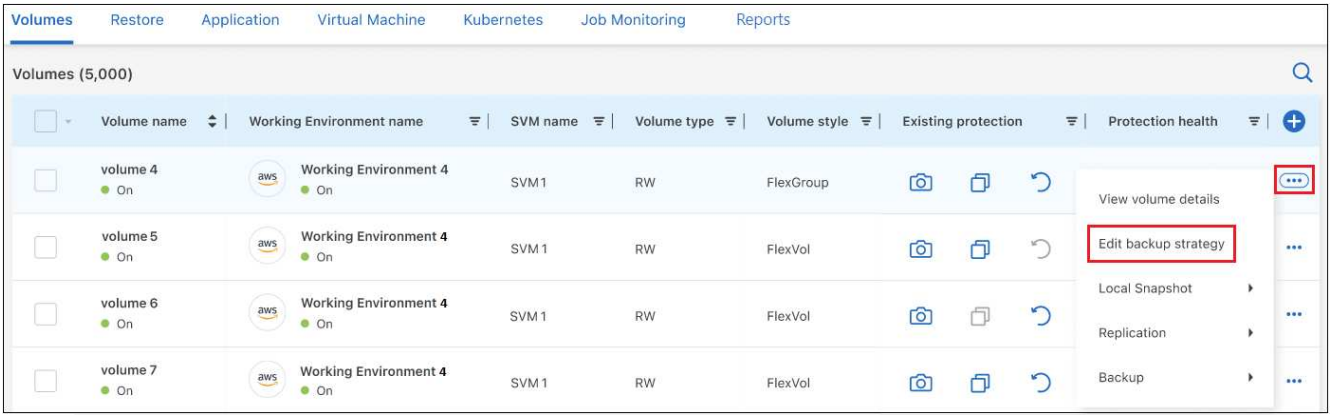
Modificare le impostazioni di backup assegnate ai volumi esistenti

È possibile modificare i criteri di backup assegnati ai volumi esistenti che hanno assegnato criteri. È possibile modificare i criteri per le copie snapshot locali, i volumi replicati e i file di backup. Qualsiasi nuovo criterio di snapshot, replica o backup che si desidera applicare ai volumi deve essere già esistente.

Modificare le impostazioni di backup su un singolo volume

Fasi

1. Dalla scheda **Volumes** (volumi), identificare il volume che si desidera modificare, quindi selezionare il menu Actions (azioni) ••• Alla fine della riga e selezionare **Modifica strategia di backup**.



2. Nella pagina *Modifica strategia di backup*, apporta le modifiche ai criteri di backup esistenti per le copie Snapshot locali, i volumi replicati e i file di backup e seleziona **Avanti**.

   Se sono stati attivati *DataLock e ransomware Protection* per i backup cloud nella policy di backup iniziale quando si attiva il backup e ripristino BlueXP per questo cluster, verranno visualizzati solo gli altri criteri configurati con DataLock. Inoltre, se non sono stati attivati *DataLock e ransomware Protection* durante l'attivazione del backup e ripristino BlueXP, verranno visualizzate solo altre policy di backup cloud che non dispongono di DataLock configurato.

3. Controllare le impostazioni di backup per questo volume, quindi selezionare **Attiva backup**.

Modificare le impostazioni di backup su più volumi

Se si desidera utilizzare le stesse impostazioni di backup su più volumi, è possibile attivare o modificare le impostazioni di backup su più volumi contemporaneamente. È possibile selezionare volumi privi di impostazioni di backup, con solo impostazioni di snapshot, con solo impostazioni di backup su cloud e così via, e apportare modifiche in blocco su tutti questi volumi con diverse impostazioni di backup.

Quando si lavora con più volumi, tutti i volumi devono avere le seguenti caratteristiche comuni:

- stesso ambiente di lavoro
- Stesso stile (volume FlexVol o FlexGroup)
- Stesso tipo (volume Read-write o Data Protection)

Se per il backup sono abilitati più di cinque volumi, il backup e ripristino di BlueXP inizializza solo cinque volumi alla volta. Al termine di queste operazioni, viene creato il batch successivo di cinque sottolavori per avviare il set successivo e continua fino all'inizializzazione di tutti i volumi.

Fasi

1. Dalla scheda **Volumes** (volumi), filtrare in base all'ambiente di lavoro in cui risiedono i volumi.
2. Selezionare tutti i volumi su cui si desidera gestire le impostazioni di backup.
3. A seconda del tipo di azione di backup che si desidera configurare, fare clic sul pulsante nel menu azioni in blocco:

Azione di backup…	Selezionare questo pulsante…
Gestisci le impostazioni di backup degli snapshot	**Gestisci snapshot locali**
Gestisci le impostazioni di backup della replica	**Gestisci replica**
Gestisci le impostazioni di backup sul cloud	**Gestisci backup**

Azione di backup…	Selezionare questo pulsante…
Gestire diversi tipi di impostazioni di backup. Questa opzione consente di modificare anche l'architettura di backup.	**Gestisci backup e ripristino**

4. Nella pagina di backup visualizzata, apporta le modifiche ai criteri di backup esistenti per le copie Snapshot locali, i volumi replicati o i file di backup e seleziona **Salva**.

   Se sono stati attivati *DataLock e ransomware Protection* per i backup cloud nella policy di backup iniziale quando si attiva il backup e ripristino BlueXP per questo cluster, verranno visualizzati solo gli altri criteri configurati con DataLock. Inoltre, se non sono stati attivati *DataLock e ransomware Protection* durante l'attivazione del backup e ripristino BlueXP, verranno visualizzate solo altre policy di backup cloud che non dispongono di DataLock configurato.

Creare un backup manuale del volume in qualsiasi momento

È possibile creare un backup on-demand in qualsiasi momento per acquisire lo stato corrente del volume. Questo può essere utile se sono state apportate modifiche molto importanti a un volume e non si desidera attendere il successivo backup pianificato per proteggere tali dati. È inoltre possibile utilizzare questa funzionalità per creare un backup per un volume che non viene attualmente sottoposto a backup e che si desidera acquisire lo stato corrente.

È possibile creare una copia snapshot ad hoc o un backup dell'oggetto di un volume. Non è possibile creare un volume replicato ad-hoc.

Il nome del backup include la data e l'ora in modo da poter identificare il backup on-demand di altri backup pianificati.

Se sono stati attivati *DataLock e ransomware Protection* durante l'attivazione del backup e ripristino BlueXP per questo cluster, anche il backup on-demand verrà configurato con DataLock e il periodo di conservazione sarà di 30 giorni. Le scansioni ransomware non sono supportate per i backup ad-hoc. "Scopri di più su DataLock e la protezione ransomware".

Quando si crea un backup ad hoc, viene creato uno snapshot sul volume di origine. Poiché questo snapshot non fa parte di una normale pianificazione di snapshot, non verrà disattivato. Potrebbe essere necessario eliminare manualmente questo snapshot dal volume di origine al termine del backup. Ciò consentirà di liberare i blocchi relativi a questo snapshot. Il nome dello snapshot inizierà con `cbs-snapshot-adhoc-` . "Scopri come eliminare un'istantanea utilizzando la CLI di ONTAP" .

Il backup dei volumi on-demand non è supportato sui volumi di protezione dei dati.

Fasi

1. Dalla scheda **Volumi**, seleziona ••• per il volume e seleziona **Backup** > **Crea backup ad hoc**.

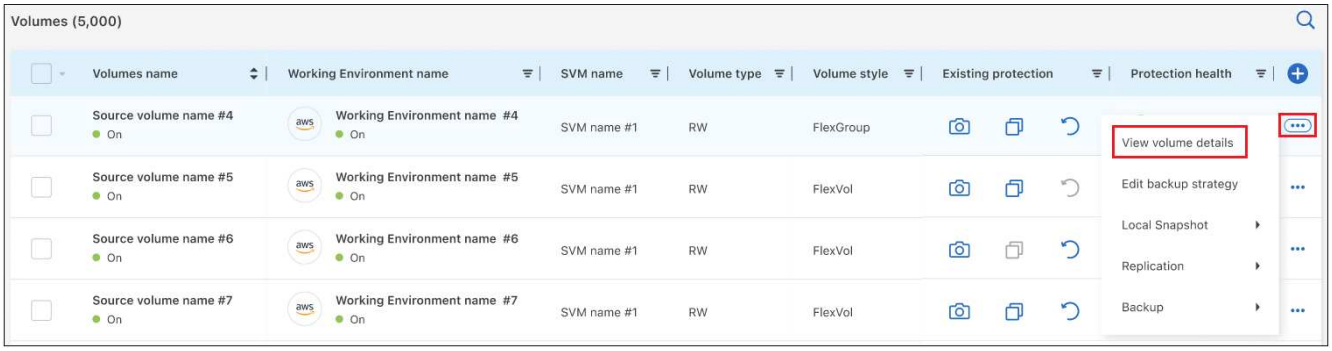
La colonna Backup Status (Stato backup) per quel volume visualizza "in corso" fino alla creazione del backup.

Visualizzare l'elenco dei backup per ciascun volume

È possibile visualizzare l'elenco di tutti i file di backup esistenti per ciascun volume. In questa pagina vengono visualizzati i dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup, ad esempio l'ultimo backup eseguito, la policy di backup corrente, le dimensioni del file di backup e altro ancora.

Fasi

1. Dalla scheda **Volumi**, seleziona ••• per il volume sorgente e selezionare **Visualizza dettagli volume**.



Vengono visualizzati i dettagli del volume e l'elenco delle copie snapshot.

2. Selezionare **Snapshot**, **Replication** o **Backup** per visualizzare l'elenco di tutti i file di backup per ciascun tipo di backup.

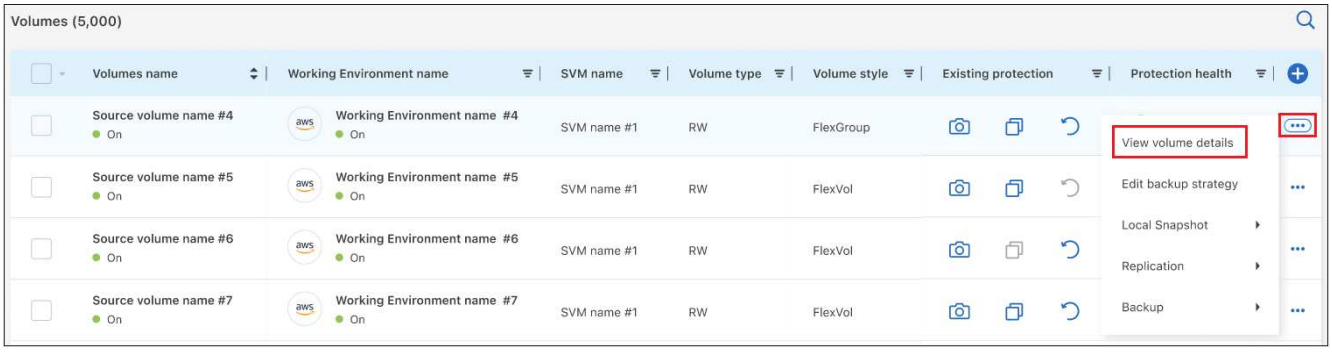
Eseguire una scansione ransomware su un backup di un volume nello storage a oggetti

BlueXP backup and recovery analizza i file di backup per cercare prove di un attacco ransomware durante la creazione di un backup su file oggetto e durante il ripristino dei dati da un file di backup. È inoltre possibile eseguire una scansione su richiesta in qualsiasi momento per verificare l'usabilità di uno specifico file di backup nell'archivio oggetti. Questa operazione può essere utile se si è verificato un problema ransomware su un determinato volume e si desidera verificare che i backup di tale volume non siano interessati.

Questa funzionalità è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.11.1 o versione successiva e se è stata abilitata la protezione *DataLock e Ransomware* nel criterio di backup su oggetto.

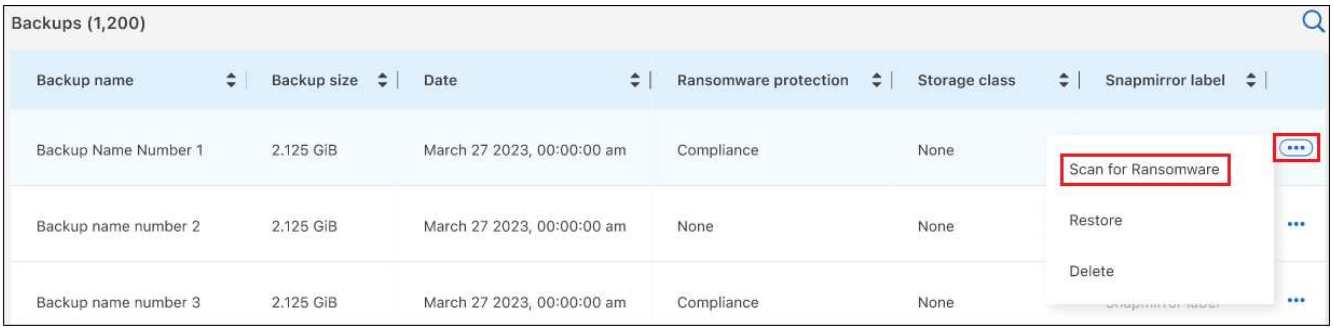
Fasi

1. Dalla scheda **Volumi**, seleziona ••• per il volume sorgente e selezionare **Visualizza dettagli volume**.



Vengono visualizzati i dettagli del volume.

2. Selezionare **Backup** per visualizzare l'elenco dei file di backup nello storage a oggetti.
3. Selezionare ••• per il file di backup del volume che vuoi analizzare alla ricerca di ransomware e clicca su **Scansione per ransomware**.



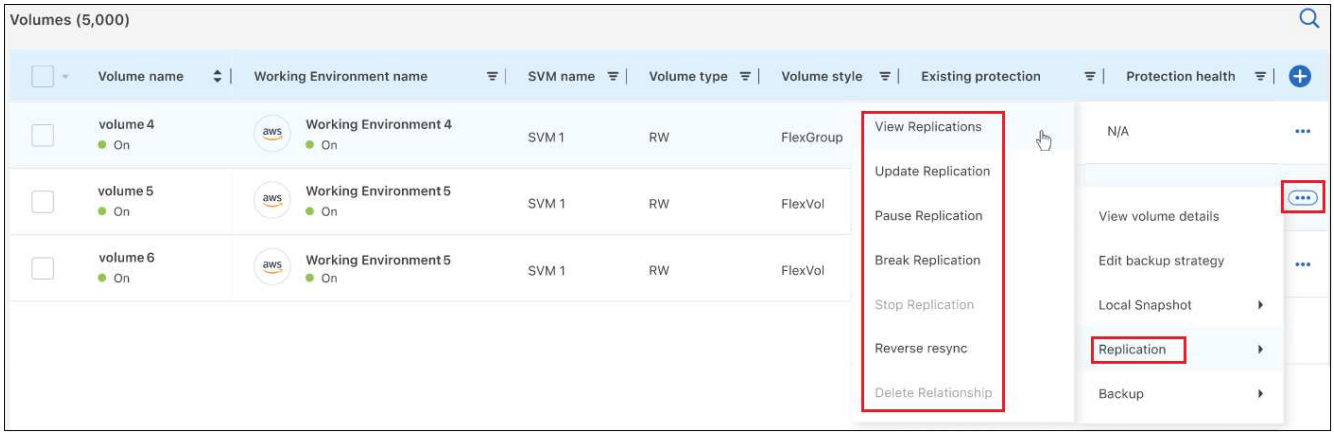
La colonna Protezione ransomware mostra che la scansione è In corso.

Gestire la relazione di replica con il volume di origine

Dopo aver impostato la replica dei dati tra due sistemi, è possibile gestire la relazione di replica dei dati.

Fasi

1. Dalla scheda **Volumi**, seleziona ••• per il volume sorgente e selezionare l'opzione **Replica**. È possibile visualizzare tutte le opzioni disponibili.
2. Selezionare l'azione di replica che si desidera eseguire.



La seguente tabella descrive le azioni disponibili:

Azione	Descrizione
Visualizza replica	Mostra i dettagli sulla relazione del volume: Informazioni sul trasferimento, informazioni sull'ultimo trasferimento, dettagli sul volume e informazioni sulla policy di protezione assegnata alla relazione.
Replica degli aggiornamenti	Avvia un trasferimento incrementale per aggiornare il volume di destinazione da sincronizzare con il volume di origine.
Sospendere la replica	Sospendere il trasferimento incrementale delle copie Snapshot per aggiornare il volume di destinazione. È possibile riprendere in seguito se si desidera riavviare gli aggiornamenti incrementali.

Azione	Descrizione
Interrompere la replica	Interrompe la relazione tra i volumi di origine e di destinazione e attiva il volume di destinazione per l'accesso ai dati, rendendolo di lettura/scrittura. Questa opzione viene generalmente utilizzata quando il volume di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline. "Scopri come configurare un volume di destinazione per l'accesso ai dati e riattivare un volume di origine nella documentazione di ONTAP"
Interrompere la replica	Disattiva i backup di questo volume nel sistema di destinazione e disattiva la possibilità di ripristinare un volume. I backup esistenti non verranno eliminati. In questo modo non viene eliminata la relazione di protezione dei dati tra i volumi di origine e di destinazione.
Risincronizzazione inversa	Inverte i ruoli dei volumi di origine e di destinazione. Il contenuto del volume di origine originale viene sovrascritto dal contenuto del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline. Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati.
Elimina relazione	Elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione, il che significa che la replica dei dati non avviene più tra i volumi. Questa azione non attiva il volume di destinazione per l'accesso ai dati, il che significa che non lo rende di lettura/scrittura. Questa azione elimina anche la relazione peer del cluster e la relazione peer di Storage VM (SVM), se non sono presenti altre relazioni di protezione dei dati tra i sistemi.

Risultato

Dopo aver selezionato un'azione, BlueXP aggiorna la relazione.

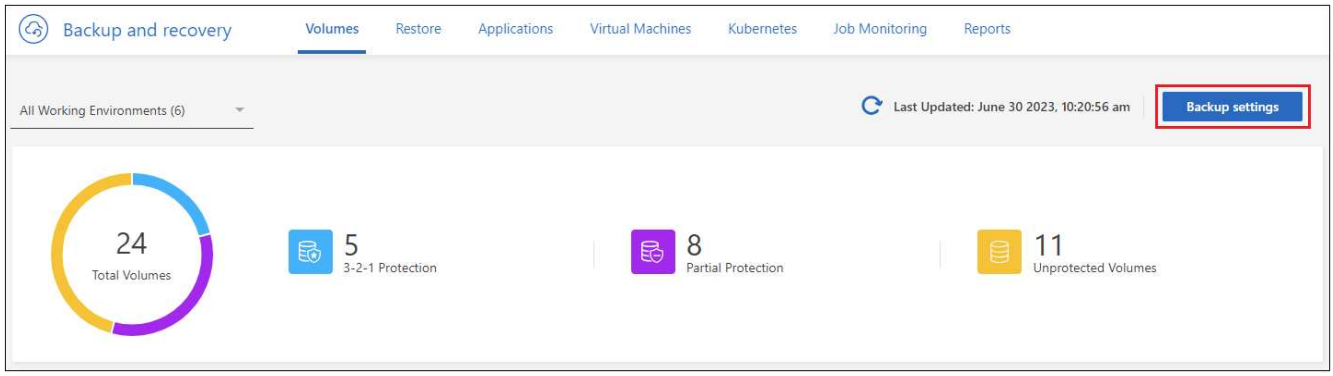
Modifica di una policy di backup nel cloud esistente

È possibile modificare gli attributi di un criterio di backup attualmente applicato ai volumi in un ambiente di lavoro. La modifica del criterio di backup influisce su tutti i volumi esistenti che utilizzano il criterio.

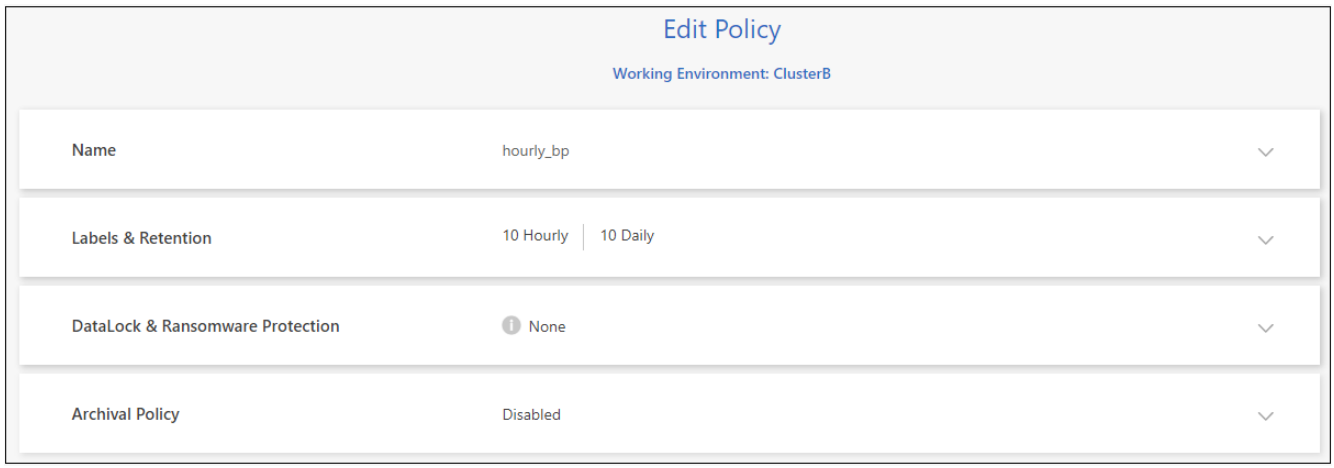
- Se sono stati attivati *DataLock e ransomware Protection* nel criterio iniziale quando si attiva il backup e il ripristino di BlueXP per questo cluster, tutti i criteri modificati devono essere configurati con la stessa impostazione DataLock (Governance o Compliance). Inoltre, se non sono stati attivati *DataLock e ransomware Protection* durante l'attivazione del backup e ripristino di BlueXP, non è possibile attivare DataLock ora.
- Quando si creano backup su AWS, se si sceglie *S3 Glacier* o *S3 Glacier Deep Archive* nella prima policy di backup quando si attiva il backup e il ripristino BlueXP, tale Tier sarà l'unico livello di archiviazione disponibile quando si modificano le policy di backup. E se non hai selezionato alcun livello di archiviazione nella tua prima policy di backup, *S3 Glacier* sarà l'unica opzione di archiviazione per la modifica di una policy.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Dalla pagina *Impostazioni di backup*, seleziona ••• per l'ambiente di lavoro in cui si desidera modificare le impostazioni dei criteri e selezionare **Gestisci criteri**.
3. Dalla pagina *Gestisci criteri*, seleziona **Modifica** per il criterio di backup che desideri modificare in quell'ambiente di lavoro.
4. Dalla pagina *Modifica policy*, seleziona la freccia rivolta verso il basso per espandere la sezione *Etichette e conservazione* per modificare la pianificazione e/o la conservazione del backup, quindi seleziona **Salva**.



Se nel cluster è in esecuzione ONTAP 9.10.1 o versione successiva, è possibile attivare o disattivare il tiering dei backup nello storage di archiviazione dopo un certo numero di giorni.

"Scopri di più sull'utilizzo dello storage di archiviazione AWS".

"Scopri di più sull'utilizzo dello storage di archiviazione Azure".

"Scopri di più sull'utilizzo dello storage di archiviazione di Google". (Richiede ONTAP 9.12.1).

+ Nota: Tutti i file di backup che sono stati trasferiti allo storage di archiviazione su più livelli vengono lasciati in tale Tier se si interrompe il tiering dei backup da archiviare, ma non vengono automaticamente spostati di nuovo al Tier standard. Solo i nuovi backup dei volumi risiedono nel Tier standard.

Aggiungi una nuova policy di backup nel cloud

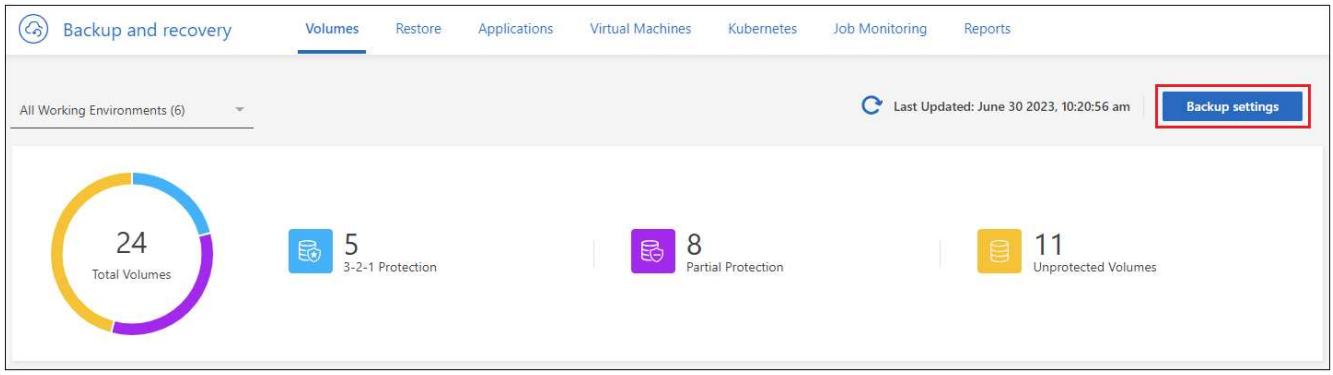
Quando si attiva il backup e il ripristino BlueXP per un ambiente di lavoro, tutti i volumi selezionati inizialmente vengono sottoposti a backup utilizzando il criterio di backup predefinito definito. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi RPO (Recovery Point Objective) diversi, è possibile creare criteri aggiuntivi per tale cluster e assegnarli ad altri volumi.

Se si desidera applicare un nuovo criterio di backup a determinati volumi in un ambiente di lavoro, è necessario prima aggiungere il criterio di backup all'ambiente di lavoro. Allora è possibile applicare il criterio ai volumi in tale ambiente di lavoro.

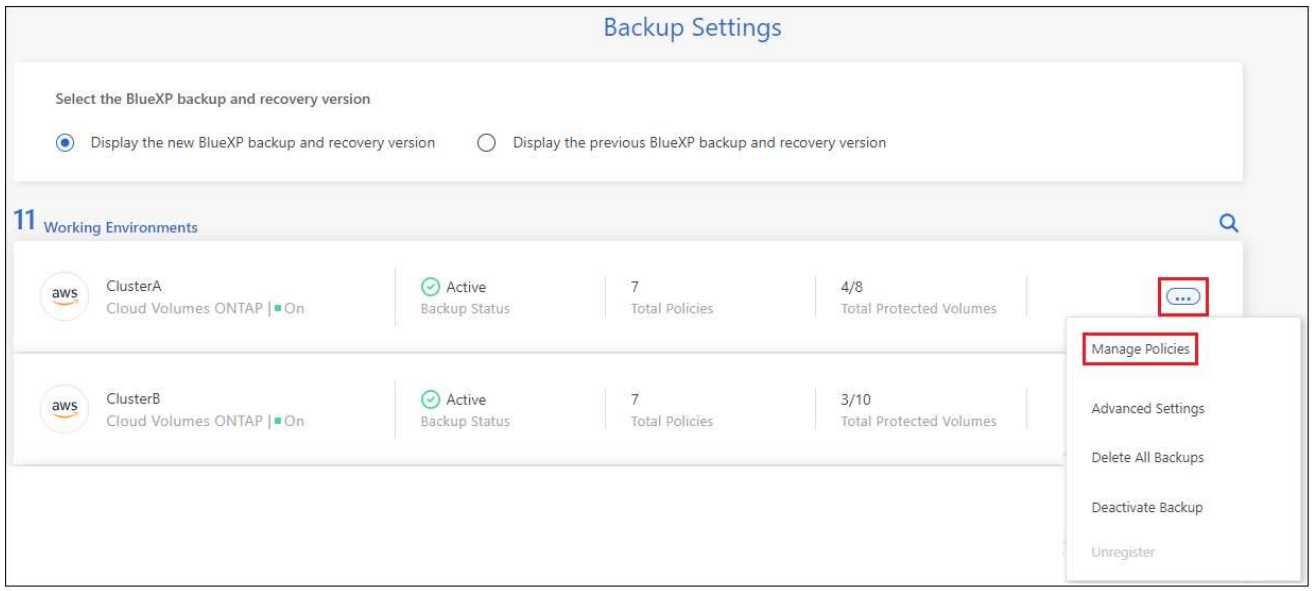
- Se sono stati attivati *DataLock e ransomware Protection* nella policy iniziale quando si attiva il backup e il ripristino di BlueXP per questo cluster, qualsiasi policy aggiuntiva creata deve essere configurata con la stessa impostazione DataLock (Governance o Compliance). Inoltre, se non sono stati attivati *DataLock e ransomware Protection* durante l'attivazione del backup e ripristino di BlueXP, non è possibile creare nuove policy che utilizzano DataLock.
- Quando si creano backup su AWS, se si sceglie *S3 Glacier* o *S3 Glacier Deep Archive* nella prima policy di backup quando si attiva il backup e il ripristino BlueXP, tale Tier sarà l'unico Tier di archiviazione disponibile per le policy di backup future per quel cluster. Inoltre, se non hai selezionato alcun livello di archiviazione nella tua prima policy di backup, *S3 Glacier* sarà l'unica opzione di archiviazione per le policy future.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).

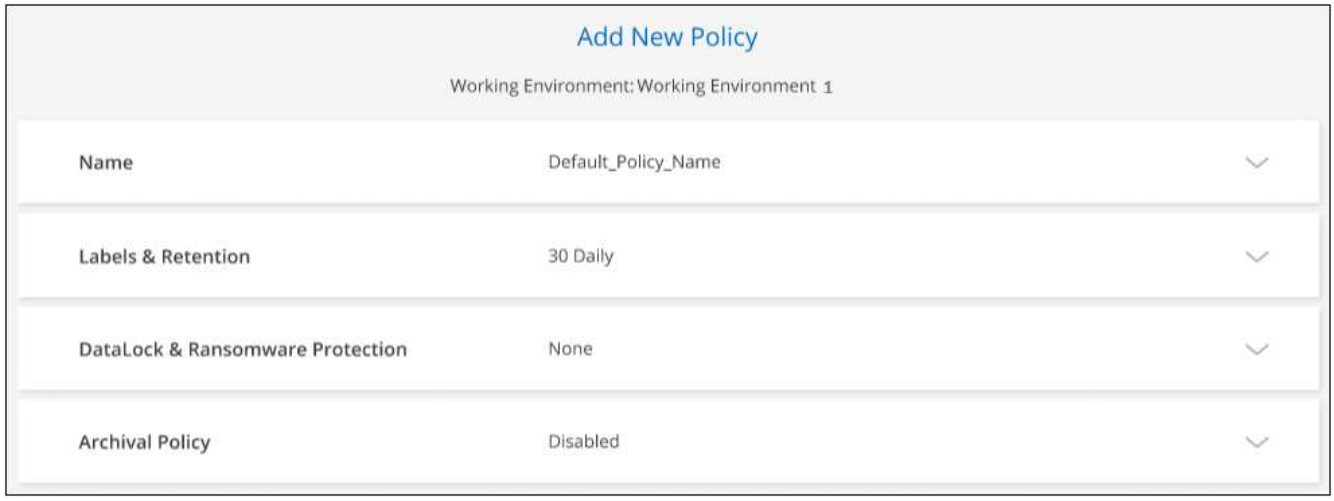


2. Dalla pagina *Impostazioni di backup*, seleziona ••• per l'ambiente di lavoro in cui si desidera aggiungere la nuova policy e selezionare **Gestisci policy**.



3. Dalla pagina *Gestisci criteri*, seleziona **Aggiungi nuovo criterio**.

4. Dalla pagina *Aggiungi nuova policy*, seleziona la freccia rivolta verso il basso per espandere la sezione *Etichette e conservazione* per definire la pianificazione e la conservazione del backup, quindi seleziona **Salva**.



Se nel cluster è in esecuzione ONTAP 9.10.1 o versione successiva, è possibile attivare o disattivare il tiering dei backup nello storage di archiviazione dopo un certo numero di giorni.

"Scopri di più sull'utilizzo dello storage di archiviazione AWS".

"Scopri di più sull'utilizzo dello storage di archiviazione Azure".

"Scopri di più sull'utilizzo dello storage di archiviazione di Google". (Richiede ONTAP 9.12.1).

Eliminare i backup

Il backup e ripristino BlueXP consente di eliminare un singolo file di backup, eliminare tutti i backup di un volume o eliminare tutti i backup di tutti i volumi in un ambiente di lavoro. È possibile eliminare tutti i backup se non sono più necessari o se il volume di origine è stato eliminato e si desidera rimuovere tutti i backup.

Non è possibile eliminare i file di backup bloccati tramite DataLock e protezione Ransomware. L'opzione "Elimina" non sarà disponibile nell'interfaccia utente se sono stati selezionati uno o più file di backup bloccati.

Se si prevede di eliminare un ambiente di lavoro o un cluster con backup, è necessario eliminare i backup **prima** di eliminare il sistema. Il backup e il ripristino di BlueXP non eliminano automaticamente i backup quando si elimina un sistema e non esiste attualmente alcun supporto nell'interfaccia utente per eliminare i backup dopo che il sistema è stato eliminato. I costi di storage a oggetti per i backup rimanenti continueranno a essere addebitati.

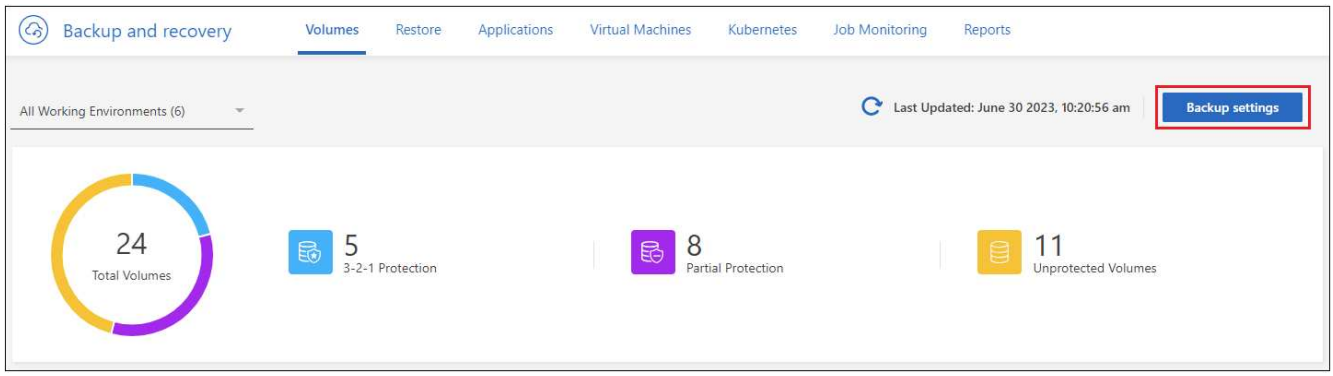
Eliminare tutti i file di backup per un ambiente di lavoro

L'eliminazione di tutti i backup sullo storage a oggetti per un ambiente di lavoro non disattiva i backup futuri dei volumi in questo ambiente di lavoro. Se si desidera interrompere la creazione di backup di tutti i volumi in un ambiente di lavoro, è possibile disattivare i backup come descritto qui.

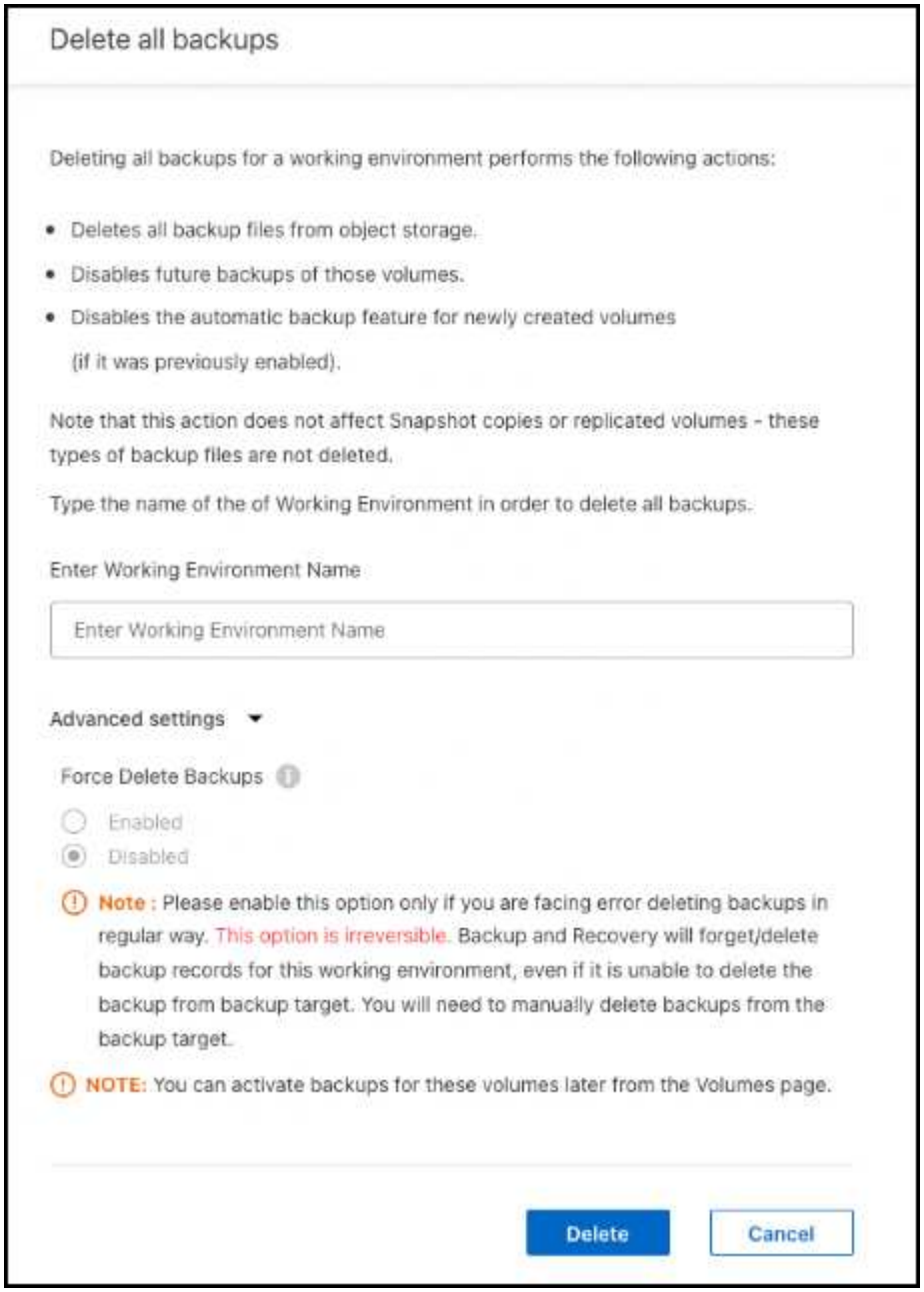
Si noti che questa azione non influisce sulle copie Snapshot o sui volumi replicati: Questi tipi di file di backup non vengono eliminati.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Selezionare ••• per l'ambiente di lavoro in cui si desidera eliminare tutti i backup e selezionare **Elimina tutti i backup**.



3. Nella finestra di dialogo di conferma, immettere il nome dell'ambiente di lavoro.
4. Selezionare **Impostazioni avanzate**.
5. **Forza eliminazione backup**: indica se desideri o meno forzare l'eliminazione di tutti i backup.

   In alcuni casi estremi, potresti voler impedire BlueXP backup and recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione, è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di ambiente di lavoro).

   > Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. Il BlueXP backup and recovery non avranno più accesso a questi backup, anche se non vengono eliminati dall'archivio oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

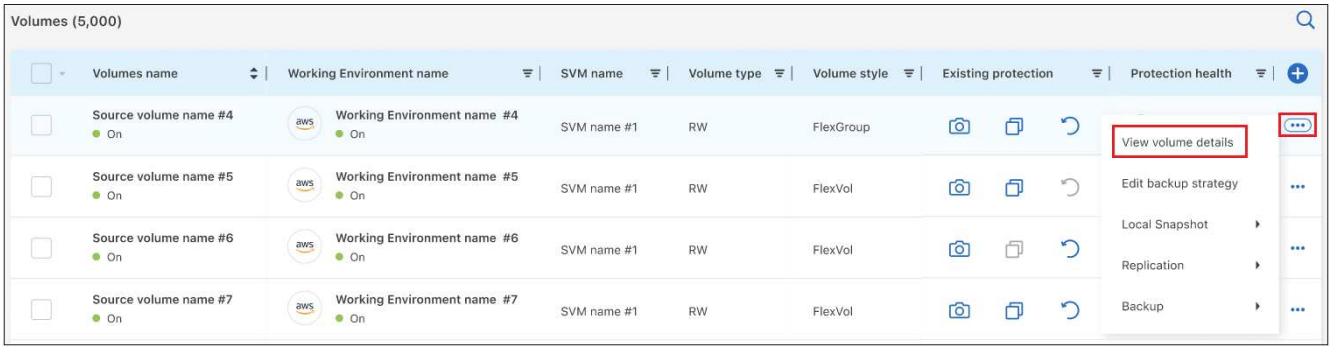
6. Selezionare **Delete** (Elimina).

Elimina tutti i file di backup per un volume

L'eliminazione di tutti i backup per un volume disattiva anche i backup futuri per quel volume.

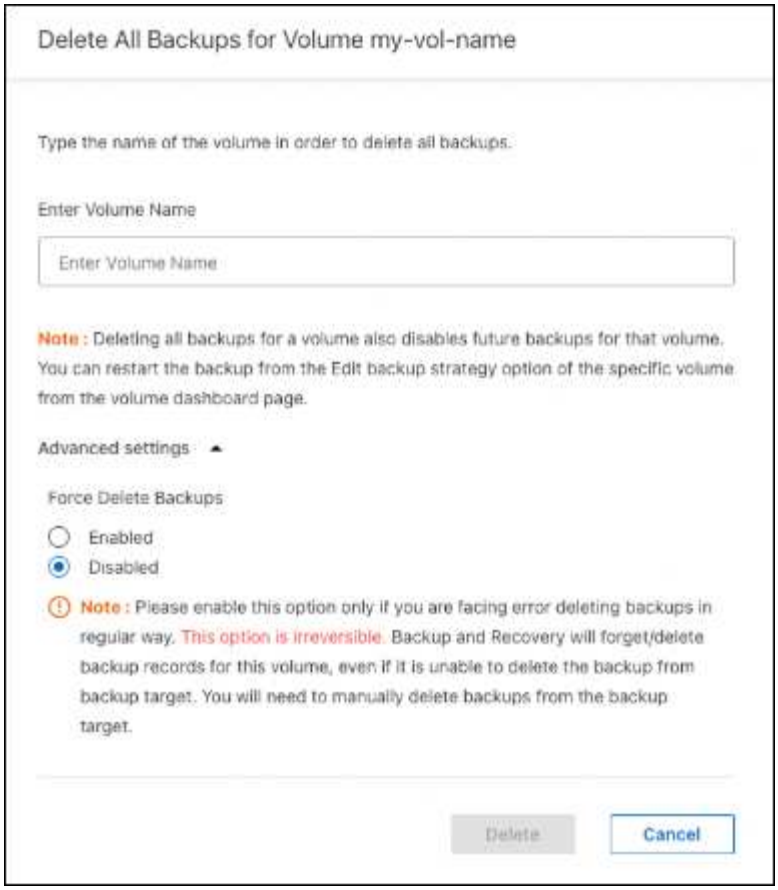
Fasi

1. Dalla scheda **Volumi**, fare clic su ••• per il volume di origine e selezionare **Dettagli e elenco di backup**.



   Viene visualizzato l'elenco di tutti i file di backup.

2. Selezionare **Azioni** > **Elimina tutti i backup**.



3. Immettere il nome del volume.
4. Selezionare **Impostazioni avanzate**.
5. **Forza eliminazione backup**: indica se desideri o meno forzare l'eliminazione di tutti i backup.

   In alcuni casi estremi, potresti voler impedire BlueXP backup and recovery di accedere più ai backup. Ciò potrebbe verificarsi, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non li si desidera più. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione, è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di ambiente di lavoro).

   Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. Il BlueXP backup and recovery non avranno più accesso a questi backup, anche se non vengono eliminati dall'archivio oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

6. Selezionare **Delete** (Elimina).

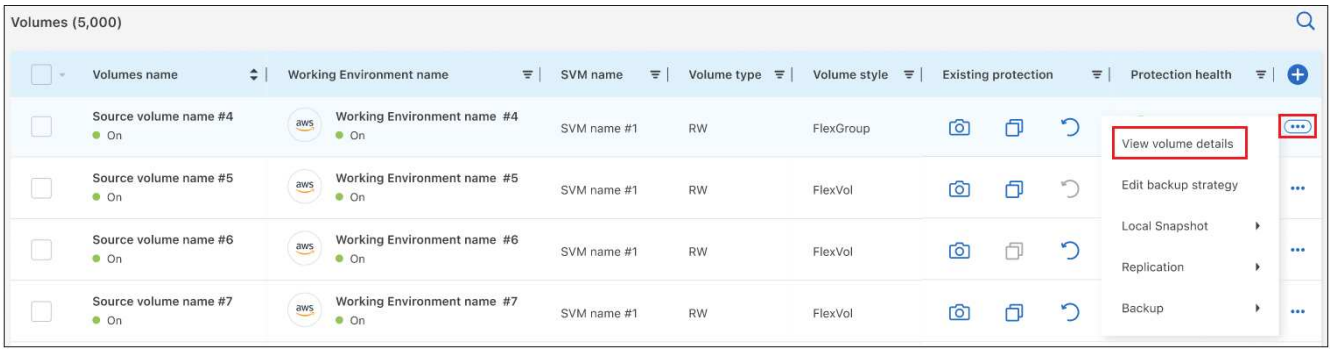
Eliminare un singolo file di backup per un volume

Se non è più necessario, è possibile eliminare un singolo file di backup. Ciò include l'eliminazione di un singolo backup di una copia Snapshot di un volume o di un backup nello storage a oggetti.

Non è possibile eliminare i volumi replicati (volumi di protezione dei dati).

Fasi

1. Dalla scheda **Volumi**, seleziona ••• per il volume sorgente e selezionare **Visualizza dettagli volume**.



Vengono visualizzati i dettagli del volume ed è possibile selezionare **Snapshot**, **Replication** o **Backup** per visualizzare l'elenco di tutti i file di backup del volume. Per impostazione predefinita, vengono visualizzate le copie snapshot disponibili.

2. Selezionare **Snapshot** o **Backup** per visualizzare il tipo di file di backup che si desidera eliminare.
3. Selezionare ••• per il file di backup del volume che vuoi eliminare e seleziona **Elimina**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina**.

Eliminare le relazioni di backup del volume

L'eliminazione della relazione di backup per un volume fornisce un meccanismo di archiviazione se si desidera interrompere la creazione di nuovi file di backup ed eliminare il volume di origine, mantenendo tutti i file di backup esistenti. Ciò consente di ripristinare il volume dal file di backup in futuro, se necessario, liberando spazio dal sistema di storage di origine.

Non è necessario eliminare il volume di origine. È possibile eliminare la relazione di backup per un volume e conservare il volume di origine. In questo caso, è possibile "attivare" il backup sul volume in un secondo momento. In questo caso, la copia di backup di riferimento originale continua ad essere utilizzata: Una nuova copia di backup di riferimento non viene creata ed esportata nel cloud. Se si riattiva una relazione di backup, al volume viene assegnato il criterio di backup predefinito.

Questa funzione è disponibile solo se nel sistema è in esecuzione ONTAP 9.12.1 o versione successiva.

Non è possibile eliminare il volume di origine dall'interfaccia utente di backup e ripristino di BlueXP. Tuttavia, è possibile aprire la pagina Volume Details (Dettagli volume) in Canvas, e. "eliminare il volume da lì".

Una volta eliminata la relazione, non è possibile eliminare i singoli file di backup dei volumi. È tuttavia possibile eliminare tutti i backup del volume.

Fasi

1. Dalla scheda **Volumi**, seleziona ••• per il volume di origine e selezionare **Backup** > **Elimina relazione**.

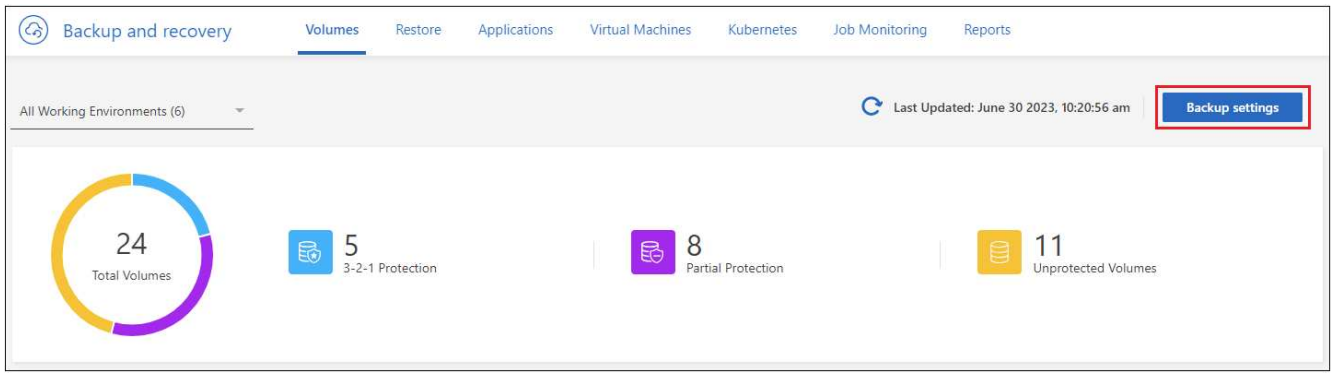
Disattivare il backup e ripristino BlueXP per un ambiente di lavoro

La disattivazione del backup e ripristino BlueXP per un ambiente di lavoro disattiva i backup di ciascun volume sul sistema e disattiva anche la possibilità di ripristinare un volume. I backup esistenti non verranno eliminati. In questo modo non si annulla la registrazione del servizio di backup da questo ambiente di lavoro, ma è possibile sospendere tutte le attività di backup e ripristino per un determinato periodo di tempo.

Tieni presente che il tuo cloud provider continuerà a addebitare i costi dello storage a oggetti per la capacità utilizzata dai backup, a meno che tu non lo utilizzi eliminare i backup.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Dalla pagina *Impostazioni di backup*, seleziona ••• per l'ambiente di lavoro in cui si desidera disattivare i backup e selezionare **Disattiva backup**.
3. Nella finestra di dialogo di conferma, seleziona **Disattiva**.

Quando il backup è disattivato, viene visualizzato il pulsante **Activate Backup** (attiva backup) per quell'ambiente di lavoro. È possibile selezionare questo pulsante quando si desidera riattivare la funzionalità di backup per quell'ambiente di lavoro.

Annullare la registrazione del backup e ripristino BlueXP per un ambiente di lavoro

È possibile annullare la registrazione di backup e ripristino BlueXP per un ambiente di lavoro se non si desidera più utilizzare la funzionalità di backup e si desidera smettere di pagare per i backup in tale ambiente di lavoro. In genere, questa funzione viene utilizzata quando si intende eliminare un ambiente di lavoro e si desidera annullare il servizio di backup.

È inoltre possibile utilizzare questa funzione se si desidera modificare l'archivio di oggetti di destinazione in cui vengono memorizzati i backup del cluster. Dopo aver disregistrato il backup e il ripristino BlueXP per l'ambiente di lavoro, è possibile attivare il backup e il ripristino BlueXP per quel cluster utilizzando le informazioni del nuovo provider di cloud.

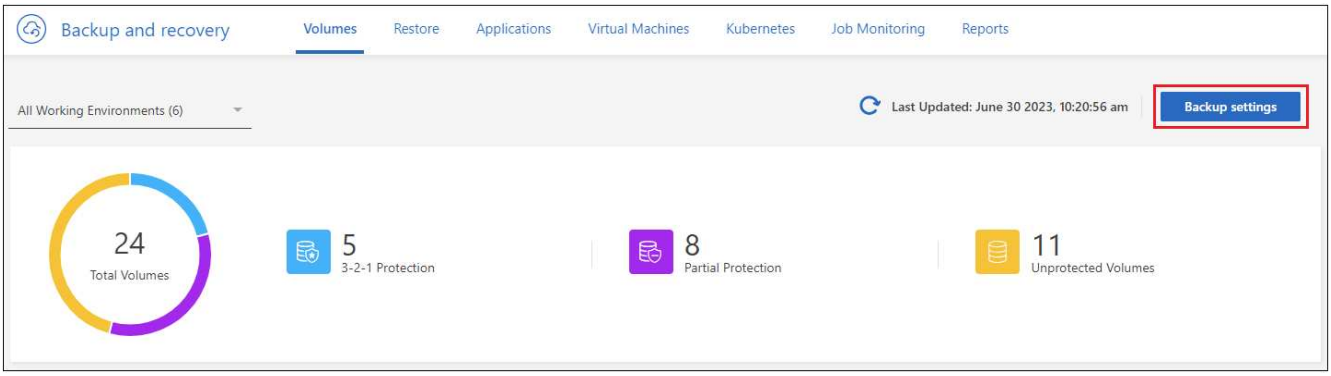
Prima di annullare la registrazione di backup e ripristino BlueXP, è necessario eseguire le seguenti operazioni, nell'ordine indicato:

- Disattivare il backup e ripristino BlueXP per l'ambiente di lavoro
- Eliminare tutti i backup per l'ambiente di lavoro

L'opzione di annullamento della registrazione non è disponibile fino al completamento di queste due azioni.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Dalla pagina *Impostazioni di backup*, seleziona ••• per l'ambiente di lavoro in cui si desidera annullare la registrazione del servizio di backup e selezionare **Annulla registrazione**.
3. Nella finestra di dialogo di conferma, seleziona **Annulla registrazione**.

Ripristina i dati ONTAP dai file di backup con il backup e il ripristino BlueXP

I backup dei dati del volume ONTAP sono disponibili dalle posizioni in cui sono stati creati i backup: Copie Snapshot, volumi replicati e backup memorizzati nello storage a oggetti. È possibile ripristinare i dati da un punto specifico in una qualsiasi di queste posizioni di backup. Con il backup e il ripristino di BlueXP è possibile ripristinare un intero volume ONTAP da un file di backup oppure, se è necessario ripristinare solo alcuni file, ripristinare una cartella o singoli file.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

- È possibile ripristinare un **volume** (come nuovo volume) nell'ambiente di lavoro originale, in un ambiente di lavoro diverso che utilizza lo stesso account cloud o in un sistema ONTAP on-premise.
- È possibile ripristinare una **cartella** in un volume nell'ambiente di lavoro originale, in un volume in un ambiente di lavoro diverso che utilizza lo stesso account cloud o in un volume su un sistema ONTAP on-premise.
- È possibile ripristinare **file** in un volume nell'ambiente di lavoro originale, in un volume in un ambiente di lavoro diverso che utilizza lo stesso account cloud o in un volume su un sistema ONTAP on-premise.

Per ripristinare i dati dai file di backup a un sistema di produzione, è necessaria una licenza di backup e ripristino BlueXP valida.

In sintesi, questi sono i flussi validi che è possibile utilizzare per ripristinare i dati dei volumi in un ambiente di lavoro ONTAP:

- File di backup → volume ripristinato
- Volume replicato → volume ripristinato
- Copia Snapshot → Volume ripristinato

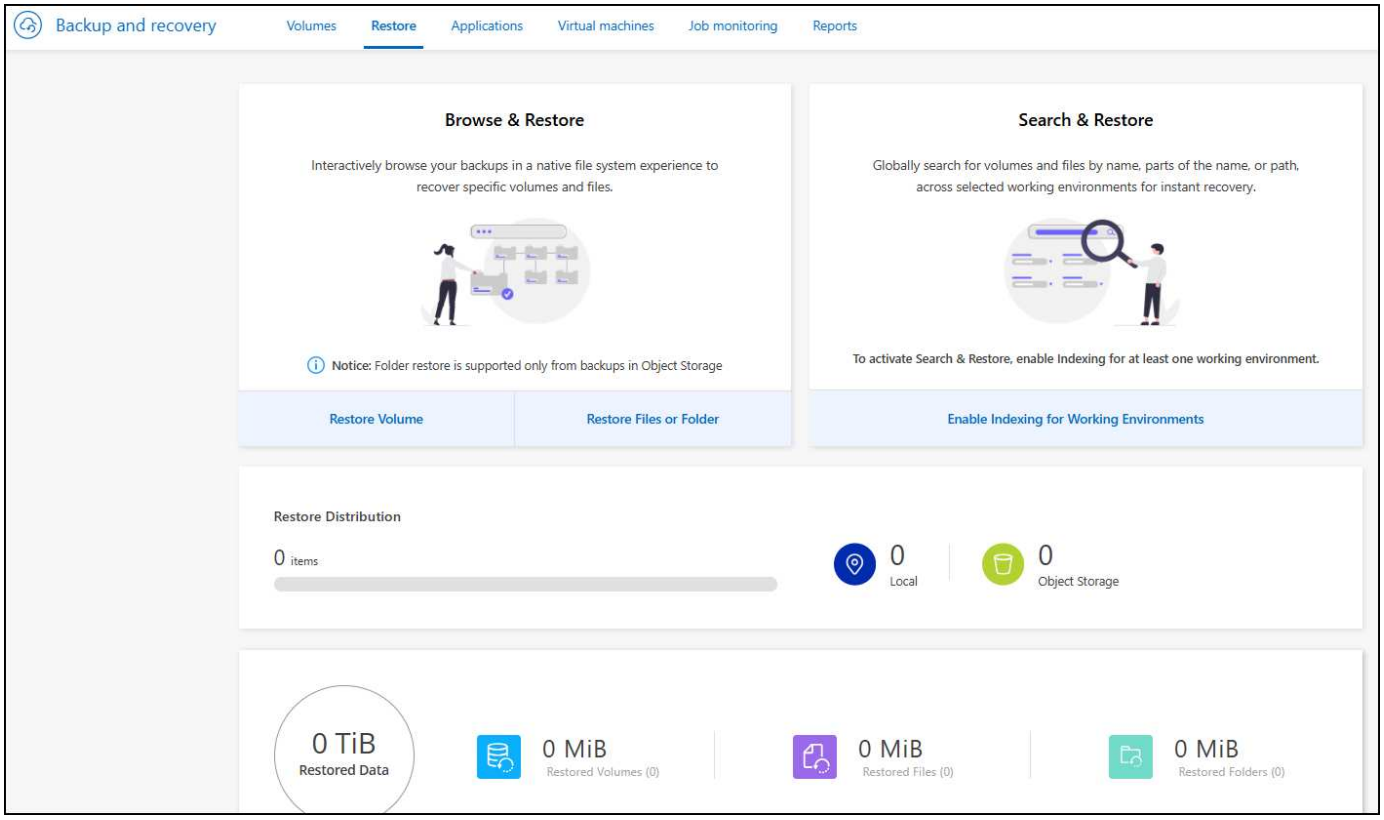
Se l'operazione di ripristino non viene completata, non tentare di eseguire nuovamente il processo di ripristino finché Job Monitor non indica che l'operazione di ripristino non è riuscita. Se si tenta di eseguire nuovamente il processo di ripristino prima che Job Monitor indichi che l'operazione di ripristino non è riuscita, l'operazione di ripristino non verrà eseguita nuovamente. Quando lo stato di Job Monitor viene visualizzato come "Failed" (non riuscito), è possibile provare nuovamente il processo di ripristino.

Per le limitazioni relative al ripristino dei dati ONTAP, vedere "Limitazioni di backup e ripristino per ONTAP Volumes".

La dashboard di ripristino

La dashboard di ripristino consente di eseguire operazioni di ripristino di volumi, cartelle e file. Per accedere alla dashboard di ripristino, fare clic su **Backup and Recovery** dal menu BlueXP, quindi fare clic sulla scheda **Restore**. Puoi anche cliccare > **Visualizza la dashboard di ripristino** dal servizio di backup e ripristino dal pannello Servizi.

Il backup e il ripristino di BlueXP devono essere già attivati per almeno un ambiente di lavoro e devono esistere file di backup iniziali.



Come puoi vedere, la dashboard di ripristino offre due modi diversi per ripristinare i dati dai file di backup: **Sfoglia e ripristina** e **Cerca e ripristina**.

Confronto tra Browse & Restore e Search & Restore

In termini generali, *Browse & Restore* è in genere migliore quando è necessario ripristinare un volume, una cartella o un file specifico dell'ultima settimana o mese, e si conoscono il nome e la posizione del file e la data

dell'ultima volta in buone condizioni. La funzione *Search & Restore* è generalmente migliore quando è necessario ripristinare un volume, una cartella o un file, ma non si ricorda il nome esatto, il volume in cui risiede o la data in cui si trovava l'ultima volta.

Questa tabella fornisce un confronto delle caratteristiche dei due metodi.

Sfoglia e ripristina	**Ricerca e ripristino**
Sfogliare una struttura in stile cartella per trovare il volume, la cartella o il file all'interno di un singolo file di backup.	Cercare un volume, una cartella o un file in **tutti i file di backup** per nome di volume parziale o completo, nome di cartella o file completo, intervallo di dimensioni e filtri di ricerca aggiuntivi.
Non gestisce il ripristino del file se il file è stato cancellato o rinominato e l'utente non conosce il nome del file originale	Gestisce le directory appena create/eliminate/rinominate e i file appena creati/cancellati/rinominati
Non sono richieste risorse aggiuntive per i cloud provider	Quando effettui il ripristino dal cloud, sono necessarie risorse aggiuntive nel bucket e nel provider di cloud pubblico per account.
Non sono richiesti costi aggiuntivi per i cloud provider	Quando esegui il ripristino dal cloud, sono necessari costi aggiuntivi per la scansione dei backup e dei volumi per i risultati di ricerca.
Il ripristino rapido è supportato.	Il ripristino rapido non è supportato.

Questa tabella fornisce un elenco di operazioni di ripristino valide in base alla posizione in cui si trovano i file di backup.

Tipo di backup	**Sfoglia e ripristina**			**Ricerca e ripristino**		
	Volume di ripristino	**Ripristinare i file**	**Cartella di ripristino**	**Volume di ripristino**	**Ripristinare i file**	**Cartella di ripristino**
Copia Snapshot	Sì	No	No	Sì	Sì	Sì
Volume replicato	Sì	No	No	Sì	Sì	Sì
File di backup	Sì	Sì	Sì	Sì	Sì	Sì

Prima di utilizzare uno dei due metodi di ripristino, assicurarsi di aver configurato l'ambiente in base ai requisiti delle risorse univoci. Tali requisiti sono descritti nelle sezioni seguenti.

Consultare i requisiti e le procedure di ripristino per il tipo di operazione di ripristino che si desidera utilizzare:

- <<Ripristinare i volumi utilizzando Sfoglia Ripristina,Ripristinare i volumi utilizzando Sfoglia Ripristina
- <<Ripristinare cartelle e file utilizzando Sfoglia Ripristina,Ripristinare cartelle e file utilizzando Sfoglia Ripristina
- <<restore-ontap-data-using-search-restore,Ripristinare volumi, cartelle e file utilizzando Search Restore

Ripristinare i dati ONTAP utilizzando Sfoglia e ripristina

Prima di iniziare il ripristino di un volume, di una cartella o di un file, è necessario conoscere il nome del volume da cui si desidera eseguire il ripristino, il nome dell'ambiente di lavoro, la SVM in cui si trova il volume e la data approssimativa del file di backup da cui si desidera eseguire il ripristino. È possibile ripristinare i dati ONTAP da una copia Snapshot, un volume replicato o da backup memorizzati nello storage a oggetti.

Nota: se il file di backup contenente i dati che si desidera ripristinare risiede nello storage cloud di archiviazione (a partire da ONTAP 9.10.1), l'operazione di ripristino richiederà più tempo e comporterà un costo. Inoltre, il cluster di destinazione deve eseguire ONTAP 9.10.1 o superiore per il ripristino del volume, 9.11.1 per il ripristino dei file, 9.12.1 per Google Archive e StorageGRID e 9.13.1 per il ripristino delle cartelle.

"Scopri di più sul ripristino dallo storage di archiviazione AWS".

"Scopri di più sul ripristino dallo storage di archivio Azure".

"Scopri di più sul ripristino dallo storage di archiviazione di Google".

La priorità alta non è supportata quando si ripristinano i dati dallo storage di archivio Azure ai sistemi StorageGRID.

Sfoglia e ripristina gli ambienti di lavoro supportati e i provider di storage a oggetti

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un ambiente di lavoro secondario (un volume replicato) o nello storage a oggetti (un file di backup) nei seguenti ambienti di lavoro. Le copie Snapshot risiedono nell'ambiente di lavoro di origine e possono essere ripristinate solo sullo stesso sistema.

Nota: è possibile ripristinare un volume da qualsiasi tipo di file di backup, ma è possibile ripristinare una cartella o singoli file solo da un file di backup nello storage a oggetti in questo momento.

Da archivio oggetti (backup)	Da primario (istantanea)	Dal sistema secondario (replica)	A ambiente di lavoro di destinazione
Amazon S3	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise ifdef::azure[]	Azure Blob
Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise	Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise ifdef::gcp[]	Storage Google Cloud	Cloud Volumes ONTAP in Google Sistema ONTAP on-premise

Da archivio oggetti (backup)	Da primario (istantanea)	Dal sistema secondario (replica)	A ambiente di lavoro di destinazione
Cloud Volumes ONTAP in Google on-premise ONTAP system endif::gcp[]	NetApp StorageGRID	Sistema ONTAP on-premise	Sistema ONTAP on-premise Cloud Volumes ONTAP
Al sistema ONTAP on-premise	ONTAP S3	Sistema ONTAP on-premise	Sistema ONTAP on-premise Cloud Volumes ONTAP

Per Browse & Restore, il connettore può essere installato nei seguenti percorsi:

- Per Amazon S3, il connettore può essere implementato in AWS o in sede
- Per Azure Blob, il connettore può essere implementato in Azure o nelle vostre sedi
- Per Google Cloud Storage, il connettore deve essere implementato nel VPC della piattaforma Google Cloud
- Per StorageGRID, il connettore deve essere implementato in sede, con o senza accesso a Internet
- Per ONTAP S3, il connettore può essere implementato in sede (con o senza accesso a Internet) o in un ambiente cloud provider

Si noti che i riferimenti ai "sistemi ONTAP on-premise" includono i sistemi FAS, AFF e ONTAP Select.

Se la versione di ONTAP sul sistema è inferiore alla 9.13.1, non è possibile ripristinare cartelle o file se il file di backup è stato configurato con DataLock & ransomware. In questo caso, è possibile ripristinare l'intero volume dal file di backup e quindi accedere ai file necessari.

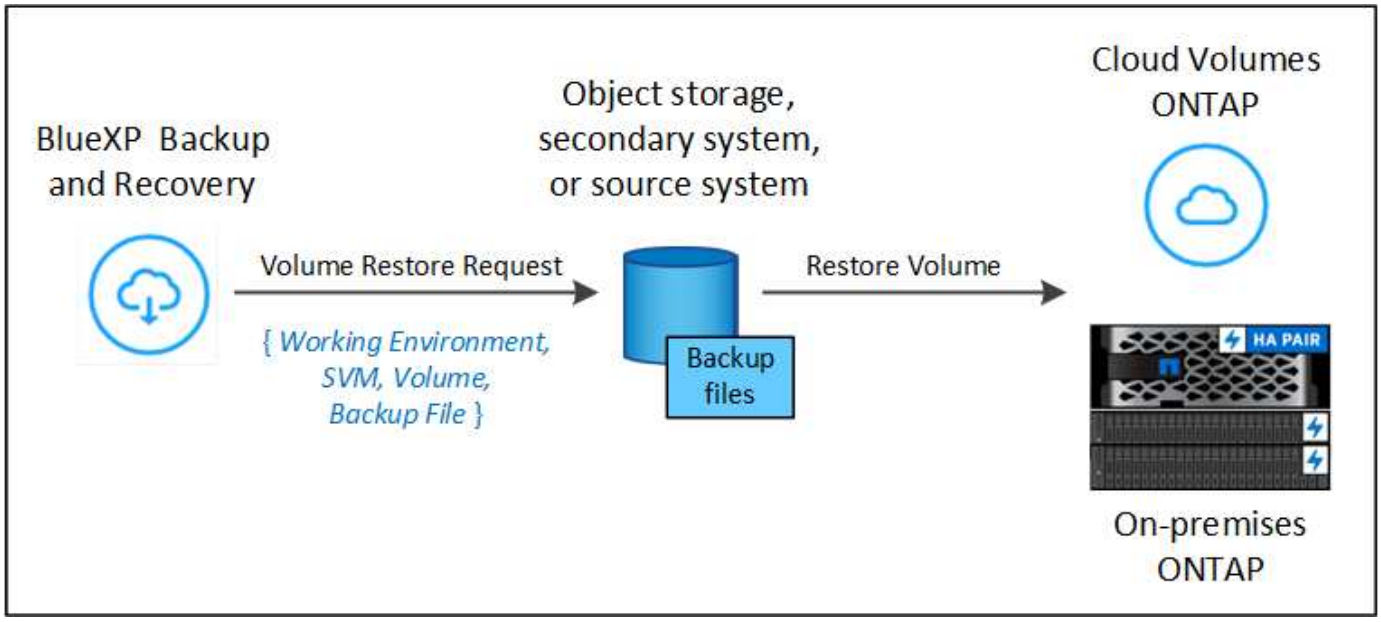
Ripristinare i volumi utilizzando Sfoglia & Ripristina

Quando si ripristina un volume da un file di backup, il backup e ripristino di BlueXP crea un *nuovo* volume utilizzando i dati del backup. Quando utilizzi un backup dallo storage a oggetti, puoi ripristinare i dati su un volume dell'ambiente di lavoro originale, in un ambiente di lavoro diverso che si trova nello stesso account cloud dell'ambiente di lavoro di origine o in un sistema ONTAP on-premise.

Quando si ripristina un backup cloud su un sistema Cloud Volumes ONTAP con ONTAP 9.13.0 o versione successiva o su un sistema ONTAP on-premise che esegue ONTAP 9.14.1, è possibile eseguire un'operazione di *ripristino rapido*. Il ripristino rapido è ideale per le situazioni di disaster recovery in cui è necessario fornire accesso a un volume il prima possibile. Un ripristino rapido ripristina i metadati dal file di backup a un volume invece di ripristinare l'intero file di backup. Il ripristino rapido non è consigliato per le applicazioni sensibili alle prestazioni o alla latenza e non è supportato con i backup nello storage archiviato.

Il ripristino rapido è supportato per i volumi FlexGroup solo se il sistema di origine da cui è stato creato il backup cloud eseguiva ONTAP 9.12.1 o versioni successive. Inoltre, è supportato per i volumi SnapLock solo se il sistema di origine esegue ONTAP 9.11.0 o superiore.

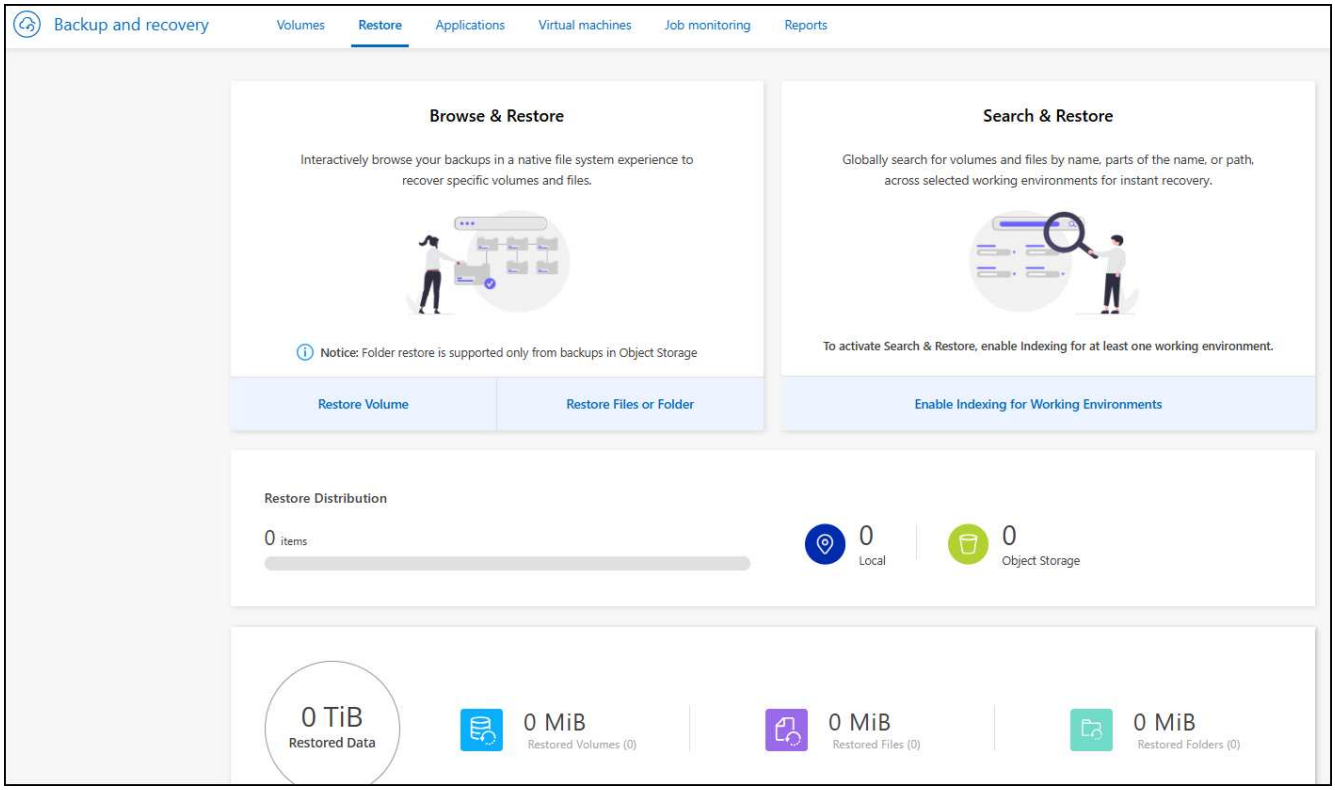
Quando si esegue il ripristino da un volume replicato, è possibile ripristinare il volume nell'ambiente di lavoro originale o in un sistema Cloud Volumes ONTAP o ONTAP on-premise.



Come si può vedere, è necessario conoscere il nome dell'ambiente di lavoro di origine, la VM di storage, il nome del volume e la data del file di backup per eseguire un ripristino del volume.

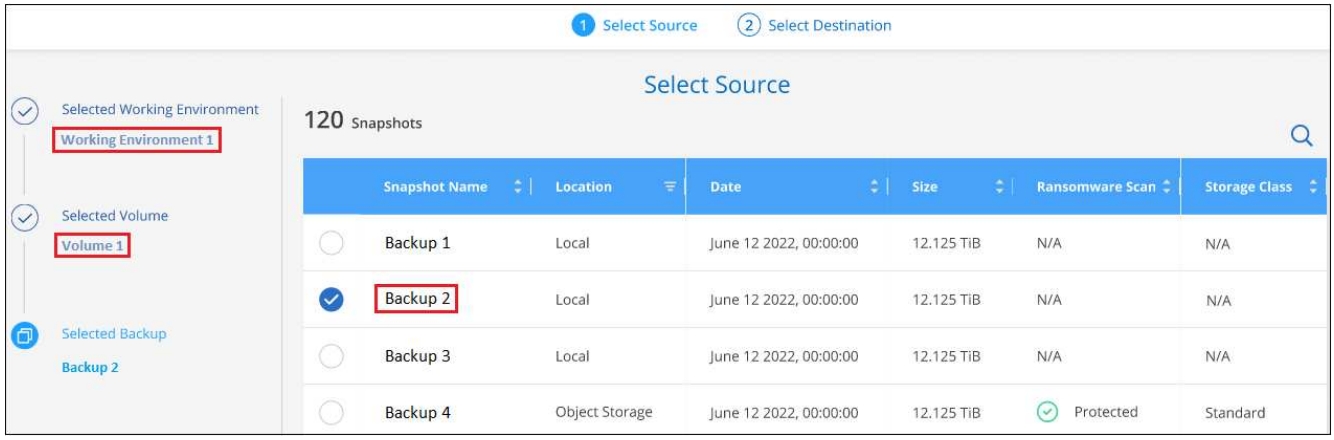
Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** per visualizzare la Dashboard di ripristino.
3. Dalla sezione *Sfoglia e ripristina*, seleziona **Ripristina volume**.



4. Nella pagina *Select Source*, accedere al file di backup del volume che si desidera ripristinare. Selezionare il file **Working Environment** (ambiente di lavoro), **Volume** (Volume) e **Backup** con la data e l'ora da cui si desidera eseguire il ripristino.

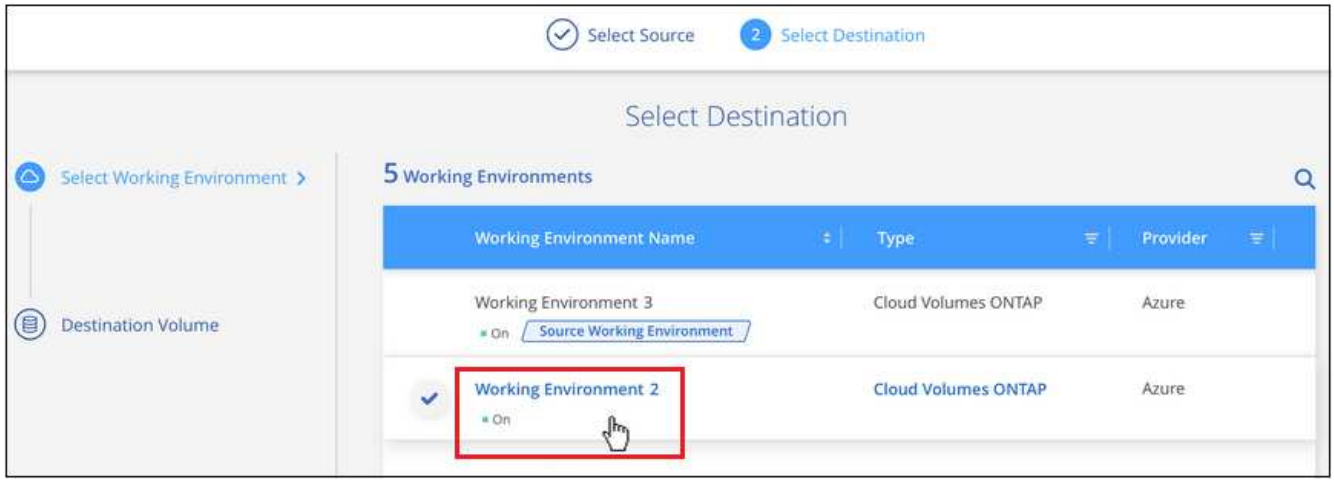
La colonna **percorso** indica se il file di backup (Snapshot) è **locale** (una copia Snapshot sul sistema di origine), **secondario** (un volume replicato su un sistema ONTAP secondario) o **archiviazione oggetto** (un file di backup nello storage a oggetti). Scegliere il file che si desidera ripristinare.



5. Selezionare **Avanti**.

   Si noti che se si seleziona un file di backup nello storage a oggetti e la protezione ransomware è attiva per tale backup (se sono stati attivati DataLock e ransomware Protection nel criterio di backup), viene richiesto di eseguire un'ulteriore scansione ransomware sul file di backup prima di ripristinare i dati. Si consiglia di eseguire la scansione del file di backup per il ransomware. (Saranno necessari costi di uscita extra da parte del cloud provider per accedere ai contenuti del file di backup).

6. Nella pagina *Select Destination*, selezionare **Working Environment** (ambiente di lavoro) in cui si desidera ripristinare il volume.

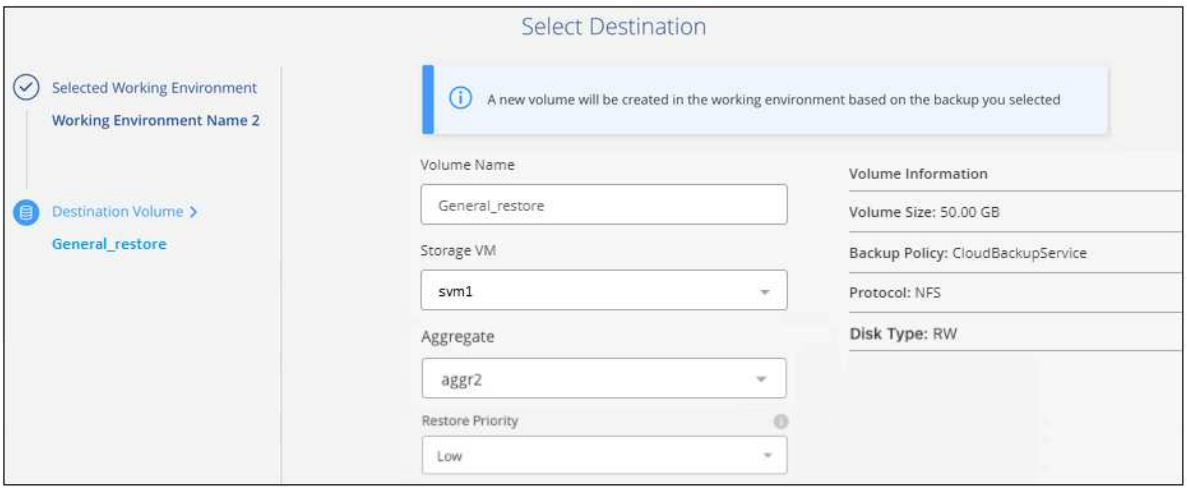


7. Quando si ripristina un file di backup dallo storage a oggetti, se si seleziona un sistema ONTAP on-premise e non si è ancora configurata la connessione del cluster allo storage a oggetti, vengono richieste ulteriori informazioni:
   - Quando si esegue il ripristino da Amazon S3, selezionare IPSpace nel cluster ONTAP in cui si trova il volume di destinazione, immettere la chiave di accesso e la chiave segreta per l'utente creato per consentire al cluster ONTAP di accedere al bucket S3, E, se lo si desidera, scegliere un endpoint VPC privato per il trasferimento sicuro dei dati.
     - Quando si esegue il ripristino da Azure Blob, selezionare IPSpace nel cluster ONTAP in cui si trova il volume di destinazione, scegliere l'abbonamento Azure per accedere allo storage a oggetti e, facoltativamente, scegliere un endpoint privato per il trasferimento sicuro dei dati selezionando

VNET e Subnet.

- Quando si esegue il ripristino da Google Cloud Storage, selezionare il progetto Google Cloud e la chiave di accesso e la chiave segreta per accedere allo storage a oggetti, alla regione in cui sono memorizzati i backup e a IPSpace nel cluster ONTAP in cui si trova il volume di destinazione.
- Quando si esegue il ripristino da StorageGRID, immettere l'FQDN del server StorageGRID e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID, selezionare la chiave di accesso e la chiave segreta necessarie per accedere allo storage a oggetti e l'IPSpace nel cluster ONTAP in cui risiede il volume di destinazione.
- Quando si esegue il ripristino da ONTAP S3, immettere l'FQDN del server ONTAP S3 e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con ONTAP S3, selezionare la chiave di accesso e la chiave segreta necessarie per accedere all'archivio oggetti, e l'IPSpace nel cluster ONTAP in cui risiede il volume di destinazione.

a. Immettere il nome da utilizzare per il volume ripristinato e selezionare Storage VM (VM di archiviazione) e aggregate (aggregato) in cui si trova il volume. Quando si ripristina un volume FlexGroup, è necessario selezionare più aggregati. Per impostazione predefinita, il nome del volume è **<source_volume_name>_restore**.



Quando ripristini un backup dallo storage a oggetti a un sistema Cloud Volumes ONTAP usando ONTAP 9.13.0 o versione successiva o su un sistema ONTAP on-premise che esegue ONTAP 9.14.1, potrai eseguire un'operazione di *ripristino rapido*.

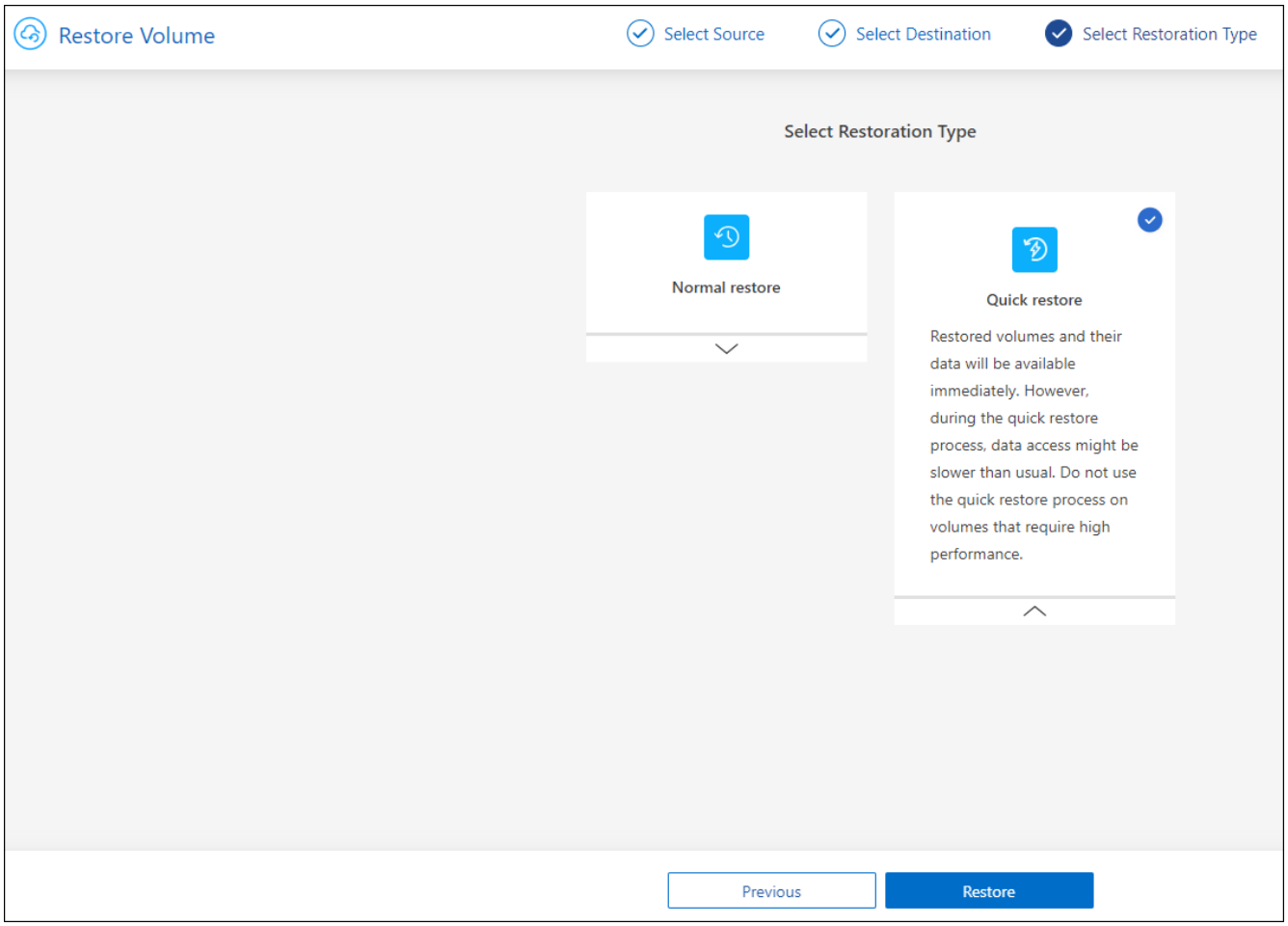
Se si sta ripristinando il volume da un file di backup che risiede in un Tier di storage di archiviazione (disponibile a partire da ONTAP 9.10.1), è possibile selezionare la priorità di ripristino.

"Scopri di più sul ripristino dallo storage di archiviazione AWS".

"Scopri di più sul ripristino dallo storage di archivio Azure".

"Scopri di più sul ripristino dallo storage di archiviazione di Google". I file di backup nel Tier di storage di Google Archive vengono ripristinati quasi immediatamente e non richiedono alcuna priorità di ripristino.

1. Selezionare **Avanti** per scegliere se si desidera eseguire un ripristino normale o un ripristino rapido:



- **Ripristino normale**: Utilizzare il ripristino normale su volumi che richiedono prestazioni elevate. I volumi non saranno disponibili fino al completamento del processo di ripristino.
- **Ripristino rapido**: I volumi e i dati ripristinati saranno immediatamente disponibili. Non utilizzare questa opzione sui volumi che richiedono prestazioni elevate, poiché durante il processo di ripristino rapido l'accesso ai dati potrebbe essere più lento del solito.

2. Selezionando **Ripristina** si torna alla Dashboard di ripristino, dove è possibile esaminare l'avanzamento dell'operazione di ripristino.

Risultato

Il backup e ripristino BlueXP crea un nuovo volume in base al backup selezionato.

Il ripristino di un volume da un file di backup che risiede nello storage di archiviazione può richiedere molti minuti o ore, a seconda del livello di archiviazione e della priorità di ripristino. È possibile selezionare la scheda **Monitoraggio processi** per visualizzare l'avanzamento del ripristino.

Ripristinare cartelle e file utilizzando Sfoglia & Ripristina

Se hai bisogno di ripristinare solo pochi file da un backup di un volume ONTAP, puoi scegliere di ripristinare una cartella o singoli file invece di ripristinare l'intero volume. È possibile ripristinare cartelle e file in un volume esistente nell'ambiente di lavoro originale o in un ambiente di lavoro diverso che utilizza lo stesso account cloud. È inoltre possibile ripristinare cartelle e file in un volume su un sistema ONTAP on-premise.

Al momento, è possibile ripristinare una cartella o singoli file solo da un file di backup nello storage a oggetti. Il ripristino di file e cartelle non è attualmente supportato da una copia snapshot locale o da un file di backup residente in un ambiente di lavoro secondario (un volume replicato).

Se si selezionano più file, tutti i file vengono ripristinati nello stesso volume di destinazione scelto. Quindi, se si desidera ripristinare i file in volumi diversi, è necessario eseguire il processo di ripristino più volte.

Quando si utilizza ONTAP 9.13.0 o versione successiva, è possibile ripristinare una cartella insieme a tutti i file e le sottocartelle all'interno di essa. Quando si utilizza una versione di ONTAP precedente alla 9.13.0, vengono ripristinati solo i file di tale cartella, non vengono ripristinate sottocartelle o file in sottocartelle.

- Se il file di backup è stato configurato con la protezione DataLock & ransomware, il ripristino a livello di cartella è supportato solo se la versione di ONTAP è 9.13.1 o superiore. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare l'intero volume dal file di backup e accedere alla cartella e ai file necessari.
- Se il file di backup risiede nello storage di archiviazione, il ripristino a livello di cartella è supportato solo se la versione di ONTAP è 9.13.1 o superiore. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare la cartella da un file di backup più recente che non è stato archiviato oppure è possibile ripristinare l'intero volume dal backup archiviato e quindi accedere alla cartella e ai file necessari.
- Con ONTAP 9.15.1, è possibile ripristinare le cartelle di FlexGroup utilizzando l'opzione "Sfoglia e ripristina". Questa funzione è in modalità Anteprima tecnologica.

  È possibile testarlo utilizzando un flag speciale descritto nella "Backup e recovery di BlueXP - blog sulla release di luglio 2024".

Prerequisiti

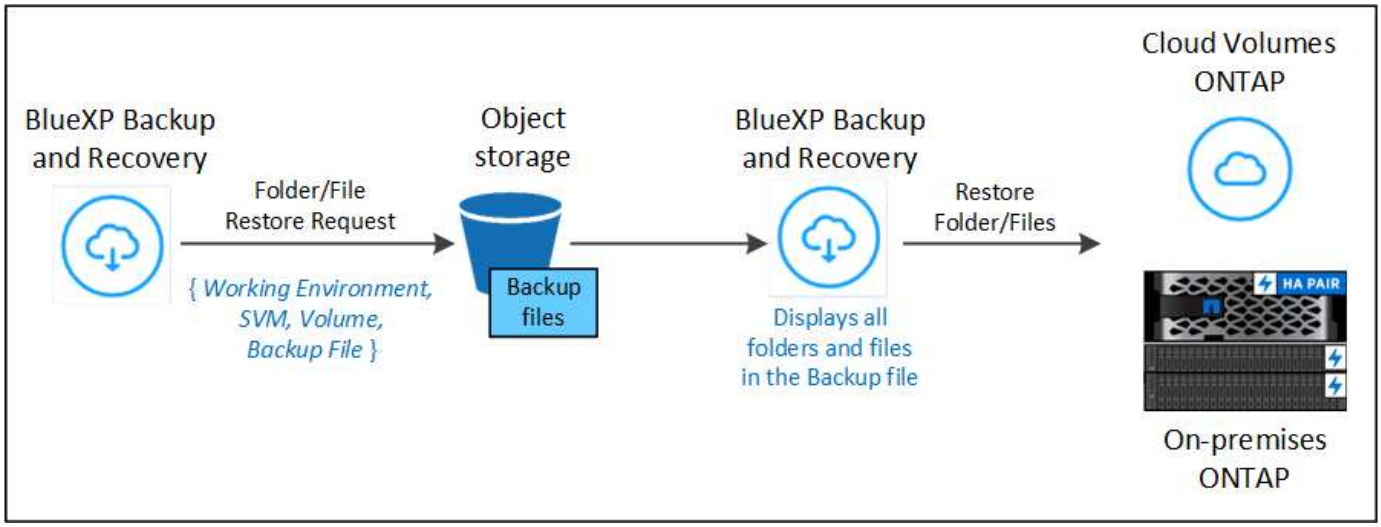
- La versione di ONTAP deve essere 9.6 o superiore per eseguire le operazioni di ripristino di *file*.
- La versione di ONTAP deve essere 9.11.1 o superiore per eseguire le operazioni di ripristino della *cartella*. ONTAP versione 9.13.1 è richiesto se i dati si trovano nello storage di archiviazione o se il file di backup utilizza DataLock e la protezione ransomware.
- La versione di ONTAP deve essere 9.15.1 P2 o superiore per ripristinare le directory FlexGroup utilizzando l'opzione Sfoglia e ripristina.

Processo di ripristino di cartelle e file

Il processo è simile al seguente:

1. Per ripristinare una cartella o uno o più file da un backup di volume, fare clic sulla scheda **Restore** (Ripristina) e fare clic su **Restore Files or Folder** (Ripristina file o cartella) in *Browse & Restore* (Sfoglia e ripristina).
2. Selezionare l'ambiente di lavoro di origine, il volume e il file di backup in cui risiedono le cartelle o i file.
3. BlueXP backup and recovery (Backup e ripristino BlueXP): Visualizza le cartelle e i file presenti nel file di backup selezionato.
4. Selezionare la cartella o i file che si desidera ripristinare dal backup.
5. Selezionare il percorso di destinazione in cui si desidera ripristinare la cartella o i file (ambiente di lavoro, volume e cartella) e fare clic su **Restore** (Ripristina).

6. I file vengono ripristinati.



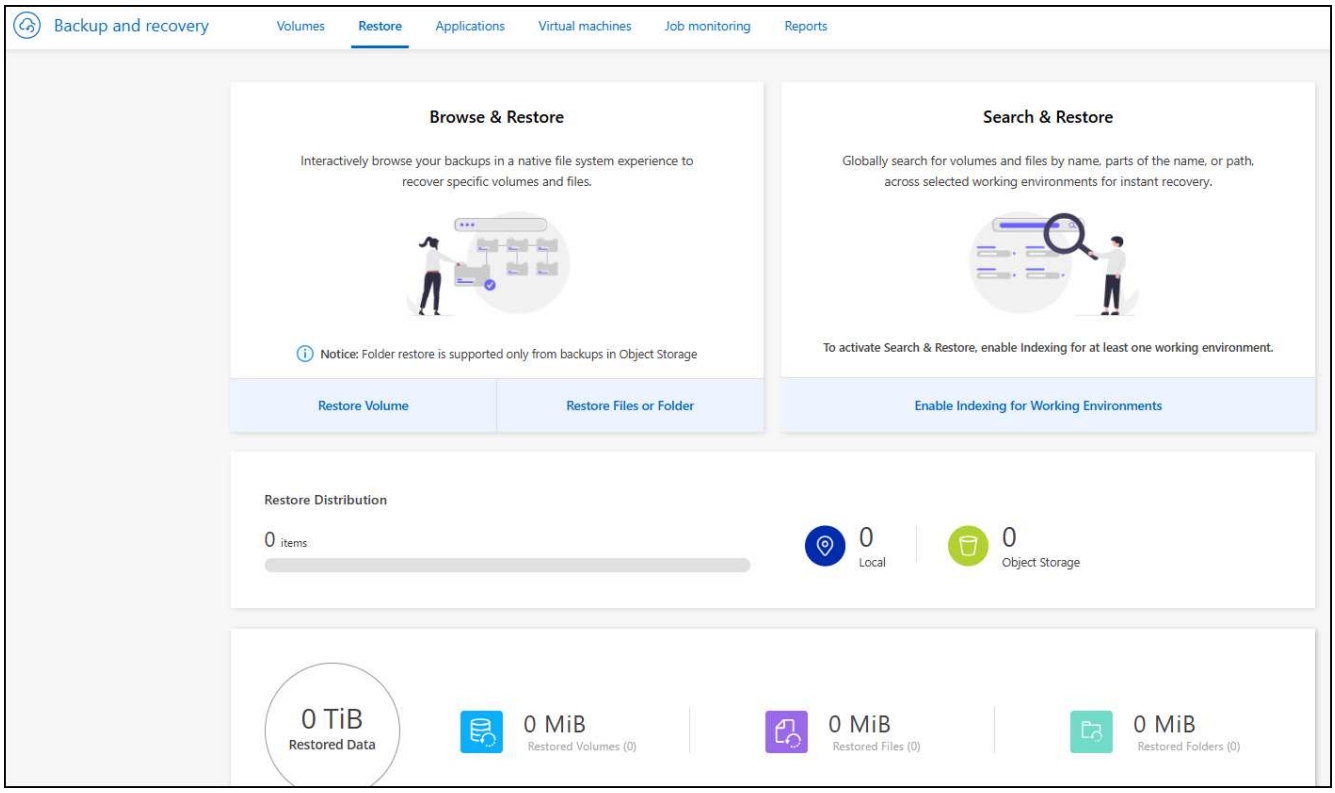
Come si può vedere, è necessario conoscere il nome dell'ambiente di lavoro, il nome del volume, la data del file di backup e il nome della cartella/file per eseguire il ripristino di una cartella o di un file.

Ripristinare cartelle e file

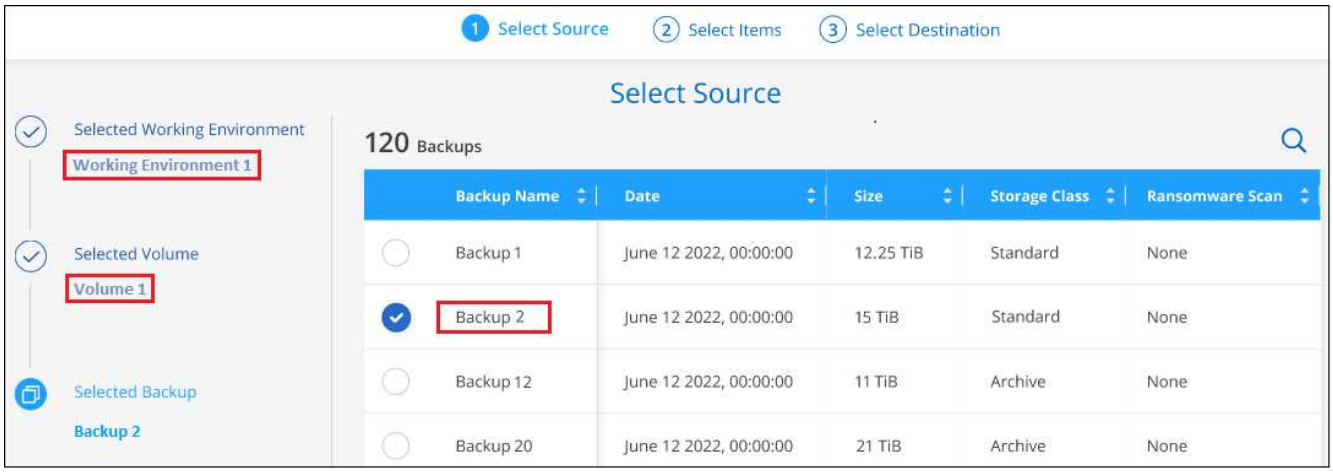
Per ripristinare cartelle o file su un volume da un backup di un volume ONTAP, procedere come segue. È necessario conoscere il nome del volume e la data del file di backup che si desidera utilizzare per ripristinare la cartella o i file. Questa funzionalità utilizza la funzione Live Browsing per visualizzare l'elenco delle directory e dei file all'interno di ciascun file di backup.

Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** per visualizzare la Dashboard di ripristino.
3. Dalla sezione *Sfoglia e ripristina*, seleziona **Ripristina file o cartella**.



4. Nella pagina *Select Source*, accedere al file di backup del volume che contiene la cartella o i file da ripristinare. Selezionare l'opzione **Working Environment** (ambiente di lavoro), **Volume** (Volume) e **Backup** con la data/ora da cui si desidera ripristinare i file.



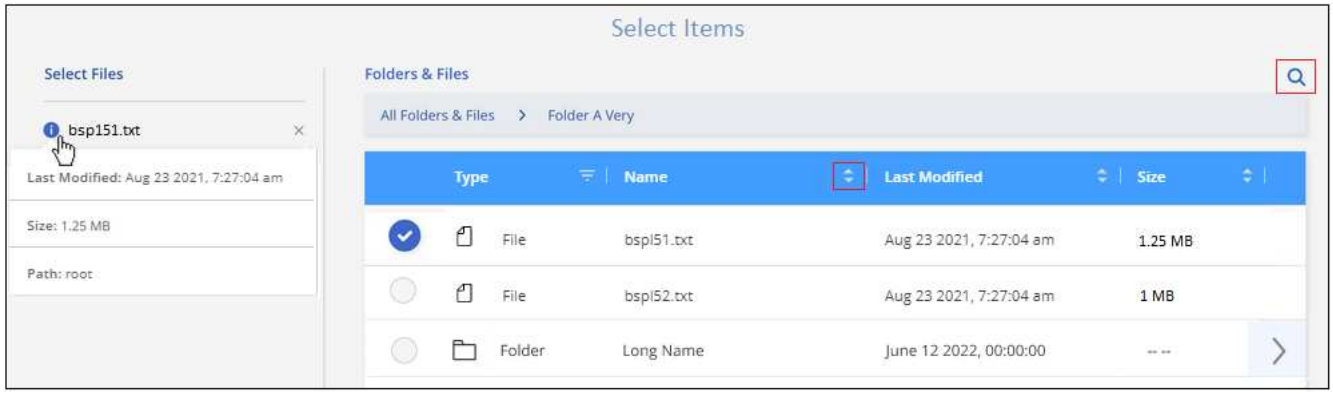
5. Selezionare **Avanti** per visualizzare l'elenco delle cartelle e dei file del backup del volume.

   Se si ripristinano cartelle o file da un file di backup che risiede in un livello di storage di archiviazione, è possibile selezionare la priorità di ripristino.

   "Scopri di più sul ripristino dallo storage di archiviazione AWS". "Scopri di più sul ripristino dallo storage di archivio Azure". "Scopri di più sul ripristino dallo storage di archiviazione di Google". I file di backup nel Tier di storage di Google Archive vengono ripristinati quasi immediatamente e non richiedono alcuna priorità di ripristino.

   E se la protezione dal ransomware è attiva per il file di backup (se hai abilitato DataLock e protezione dal ransomware nella policy di backup), ti viene richiesto di eseguire un'ulteriore scansione dal ransomware

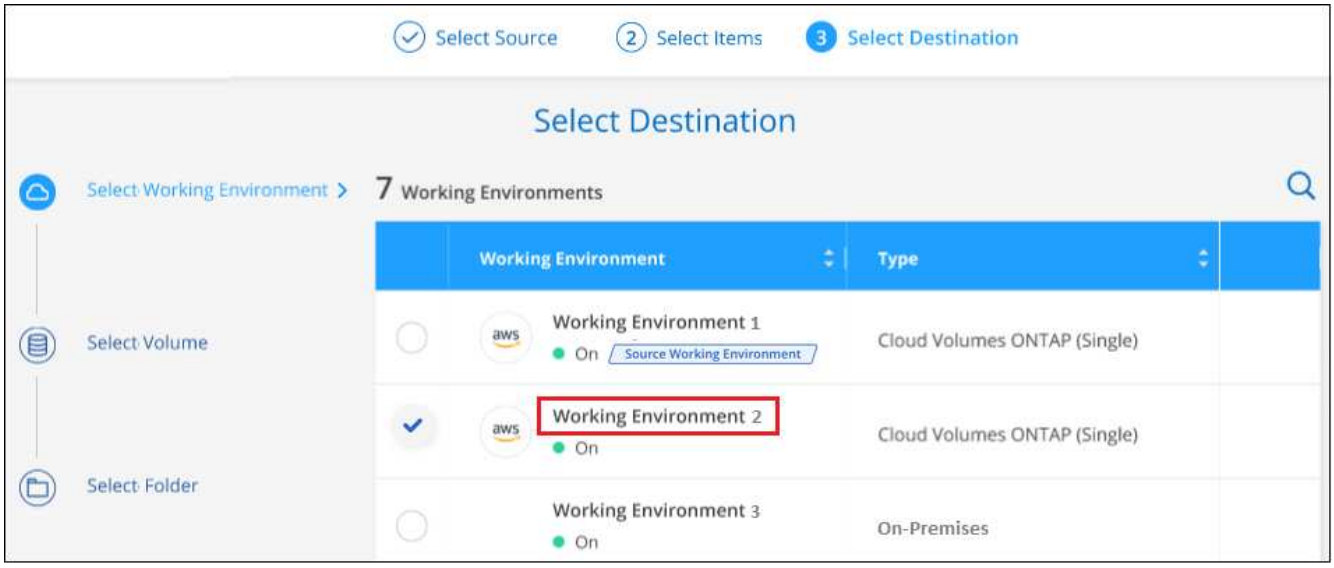
sul file di backup prima di ripristinare i dati. Si consiglia di eseguire la scansione del file di backup per il ransomware. (Saranno necessari costi di uscita extra da parte del cloud provider per accedere ai contenuti del file di backup).



6. Nella pagina *Seleziona elementi*, seleziona la cartella o i file che desideri ripristinare e seleziona **Continua**. Per assistenza nella ricerca dell'elemento:
   - Puoi selezionare il nome della cartella o del file, se lo vedi.
   - È possibile selezionare l'icona di ricerca e immettere il nome della cartella o del file per passare direttamente all'elemento.
   - È possibile scorrere i livelli delle cartelle utilizzando la freccia giù alla fine della riga per trovare file specifici.

     Quando si selezionano i file, questi vengono aggiunti alla parte sinistra della pagina in modo da visualizzare i file già selezionati. Se necessario, puoi rimuovere un file da questo elenco selezionando la **x** accanto al nome del file.

7. Nella pagina *Select Destination* (Seleziona destinazione), selezionare **Working Environment** (ambiente di lavoro) in cui si desidera ripristinare gli elementi.



Se si seleziona un cluster on-premise e non si è ancora configurata la connessione del cluster allo storage a oggetti, vengono richieste ulteriori informazioni:

   - Quando si esegue il ripristino da Amazon S3, inserire IPSpace nel cluster ONTAP in cui si trova il volume di destinazione e la chiave di accesso AWS e la chiave segreta necessarie per accedere allo

storage a oggetti. È inoltre possibile selezionare una configurazione di collegamento privato per la connessione al cluster.

- Quando si esegue il ripristino da Azure Blob, inserire IPSpace nel cluster ONTAP in cui si trova il volume di destinazione. È inoltre possibile selezionare una configurazione di endpoint privato per la connessione al cluster.
- Quando si esegue il ripristino da Google Cloud Storage, inserire IPSpace nel cluster ONTAP in cui risiedono i volumi di destinazione e la chiave di accesso e la chiave segreta necessarie per accedere allo storage a oggetti.
- Quando si esegue il ripristino da StorageGRID, immettere l'FQDN del server StorageGRID e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID, immettere la chiave di accesso e la chiave segreta necessarie per accedere allo storage a oggetti e l'IPSpace nel cluster ONTAP in cui risiede il volume di destinazione.

  a. Quindi selezionare il **Volume** e la **cartella** in cui si desidera ripristinare la cartella o i file.

     Sono disponibili alcune opzioni per la posizione durante il ripristino di cartelle e file.

- Una volta selezionato **Select Target Folder** (Seleziona cartella di destinazione), come mostrato sopra:

◦ È possibile selezionare qualsiasi cartella.

◦ È possibile passare il mouse su una cartella e fare clic alla fine della riga per visualizzare in dettaglio le sottocartelle, quindi selezionare una cartella.

- Se sono stati selezionati lo stesso ambiente di lavoro di destinazione e lo stesso volume in cui si trovava la cartella o il file di origine, è possibile selezionare **Mantieni percorso cartella di origine** per ripristinare la cartella o i file nella stessa cartella in cui erano presenti nella struttura di origine. Tutte le stesse cartelle e sottocartelle devono già esistere; le cartelle non vengono create. Quando si ripristinano i file nella posizione originale, è possibile scegliere di sovrascrivere i file di origine o di creare nuovi file.

  a. Selezionando **Ripristina** verrai reindirizzato alla Dashboard di ripristino, dove potrai esaminare l'avanzamento dell'operazione di ripristino. È inoltre possibile fare clic sulla scheda **Job Monitoring** per visualizzare l'avanzamento del ripristino.

Ripristinare i dati ONTAP utilizzando Ricerca e ripristino

È possibile ripristinare un volume, una cartella o file da un file di backup di ONTAP utilizzando Ricerca e ripristino. Search & Restore (Ricerca e ripristino) consente di cercare un volume, una cartella o un file specifico da tutti i backup, quindi di eseguire un ripristino. Non è necessario conoscere il nome esatto dell'ambiente di lavoro, il nome del volume o il nome del file: La ricerca esamina tutti i file di backup dei volumi.

L'operazione di ricerca esamina tutte le copie snapshot locali esistenti per i volumi ONTAP , tutti i volumi replicati sui sistemi di archiviazione secondaria e tutti i file di backup esistenti nell'archiviazione di oggetti. Poiché il ripristino dei dati da una copia Snapshot locale o da un volume replicato può essere più rapido e meno costoso del ripristino da un file di backup nello storage a oggetti, è possibile ripristinare i dati da queste altre posizioni.

Quando ripristini un *volume completo* da un file di backup, il backup e il recovery di BlueXP crea un volume *nuovo* utilizzando i dati del backup. Puoi ripristinare i dati come volume nell'ambiente di lavoro originale, in un ambiente di lavoro diverso che si trova nello stesso account cloud dell'ambiente di lavoro di origine o in un sistema ONTAP on-premise.

È possibile ripristinare *cartelle o file* nella posizione originale del volume, in un volume diverso nello stesso ambiente di lavoro, in un ambiente di lavoro diverso che utilizza lo stesso account cloud o in un volume su un

sistema ONTAP on-premise.

Quando si utilizza ONTAP 9.13.0 o versione successiva, è possibile ripristinare una cartella insieme a tutti i file e le sottocartelle all'interno di essa. Quando si utilizza una versione di ONTAP precedente alla 9.13.0, vengono ripristinati solo i file di tale cartella, non vengono ripristinate sottocartelle o file in sottocartelle.

Se il file di backup per il volume che si desidera ripristinare risiede nello storage di archiviazione (disponibile a partire da ONTAP 9.10.1), l'operazione di ripristino richiederà più tempo e comporterà costi aggiuntivi. Tenere presente che il cluster di destinazione deve eseguire anche ONTAP 9.10.1 o versione successiva per il ripristino del volume, 9.11.1 per il ripristino dei file, 9.12.1 per Google Archive e StorageGRID e 9.13.1 per il ripristino delle cartelle.

"Scopri di più sul ripristino dallo storage di archiviazione AWS".

"Scopri di più sul ripristino dallo storage di archivio Azure".

"Scopri di più sul ripristino dallo storage di archiviazione di Google".

- Se il file di backup nello storage a oggetti è stato configurato con la protezione DataLock e ransomware, il ripristino a livello di cartella è supportato solo se la versione di ONTAP è 9.13.1 o superiore. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare l'intero volume dal file di backup e accedere alla cartella e ai file necessari.
- Se il file di backup nello storage a oggetti risiede nello storage di archiviazione, il ripristino a livello di cartella è supportato solo se la versione di ONTAP è 9.13.1 o superiore. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare la cartella da un file di backup più recente che non è stato archiviato oppure è possibile ripristinare l'intero volume dal backup archiviato e quindi accedere alla cartella e ai file necessari.
- La priorità di ripristino "alta" non è supportata quando si ripristinano i dati dallo storage di archivio Azure ai sistemi StorageGRID.
- Il ripristino delle cartelle non è attualmente supportato dai volumi nello storage a oggetti ONTAP S3.

Prima di iniziare, si dovrebbe avere un'idea del nome o della posizione del volume o del file che si desidera ripristinare.

Search & Restore ambienti di lavoro supportati e provider di storage a oggetti

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un ambiente di lavoro secondario (un volume replicato) o nello storage a oggetti (un file di backup) nei seguenti ambienti di lavoro. Le copie Snapshot risiedono nell'ambiente di lavoro di origine e possono essere ripristinate solo sullo stesso sistema.

Nota: è possibile ripristinare volumi e file da qualsiasi tipo di file di backup, ma è possibile ripristinare una cartella solo dai file di backup nello storage a oggetti in questo momento.

Percorso del file di backup		**Ambiente di lavoro di destinazione**
Archivio oggetti (backup)	**Sistema secondario (replica)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise	Cloud Volumes ONTAP in AWS on-premise ONTAP system endif::aws[] ifdef::Azure[]

Percorso del file di backup		Ambiente di lavoro di destinazione
Azure Blob	Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise	Cloud Volumes ONTAP in Azure on-premise ONTAP system endif::Azure[] ifdef::gcp[]
Storage Google Cloud	Cloud Volumes ONTAP in Google Sistema ONTAP on-premise	Cloud Volumes ONTAP in Google on-premise ONTAP system endif::gcp[]
NetApp StorageGRID	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP on-premise
ONTAP S3	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP on-premise

Per Search & Restore, il connettore può essere installato nelle seguenti posizioni:

- Per Amazon S3, il connettore può essere implementato in AWS o in sede
- Per Azure Blob, il connettore può essere implementato in Azure o nelle vostre sedi
- Per Google Cloud Storage, il connettore deve essere implementato nel VPC della piattaforma Google Cloud
- Per StorageGRID, il connettore deve essere implementato in sede, con o senza accesso a Internet
- Per ONTAP S3, il connettore può essere implementato in sede (con o senza accesso a Internet) o in un ambiente cloud provider

Si noti che i riferimenti ai "sistemi ONTAP on-premise" includono i sistemi FAS, AFF e ONTAP Select.

Prerequisiti

- Requisiti del cluster:
  - La versione di ONTAP deve essere 9.8 o superiore.
  - La VM di storage (SVM) su cui risiede il volume deve avere una LIF di dati configurata.
  - NFS deve essere attivato sul volume (sono supportati sia i volumi NFS che SMB/CIFS).
  - SnapDiff RPC Server deve essere attivato su SVM. BlueXP esegue questa operazione automaticamente quando si attiva l'indicizzazione nell'ambiente di lavoro. (SnapDiff è la tecnologia che identifica rapidamente le differenze di file e directory tra le copie Snapshot).
- Requisiti AWS:
  - Le autorizzazioni specifiche di Amazon Athena, AWS Glue e AWS S3 devono essere aggiunte al ruolo utente che fornisce a BlueXP le autorizzazioni necessarie. "Assicurarsi che tutte le autorizzazioni siano configurate correttamente".

    Se si utilizzava già il backup e ripristino BlueXP con un connettore configurato in passato, è necessario aggiungere ora le autorizzazioni Athena e Glue al ruolo utente BlueXP. Sono necessari per la ricerca e il ripristino.
- Requisiti di Azure:
  - È necessario registrare Azure Synapse Analytics Resource Provider (chiamato "Microsoft.Synapse") con l'abbonamento. "Scopri come registrare questo provider di risorse per l'abbonamento". Per registrare il provider di risorse, è necessario essere il proprietario dell'abbonamento* o il collaboratore*.

- Le autorizzazioni specifiche di Azure Synapse Workspace e di Data Lake Storage account devono essere aggiunte al ruolo utente che fornisce a BlueXP le autorizzazioni. "Assicurarsi che tutte le autorizzazioni siano configurate correttamente".

  Nota: Se si utilizzava già il backup e ripristino BlueXP con un connettore configurato in passato, è necessario aggiungere le autorizzazioni Azure Synapse Workspace e Data Lake Storage account al ruolo utente BlueXP. Sono necessari per la ricerca e il ripristino.

- Il connettore deve essere configurato **senza** un server proxy per la comunicazione HTTP a Internet. Se hai configurato un server proxy HTTP per il tuo connettore, non puoi utilizzare la funzionalità Cerca e ripristina.

- Requisiti di Google Cloud:
  - Le autorizzazioni specifiche di Google BigQuery devono essere aggiunte al ruolo utente che fornisce a BlueXP le autorizzazioni necessarie. "Assicurarsi che tutte le autorizzazioni siano configurate correttamente".

    Se utilizzavi già il BlueXP backup and recovery con un connettore configurato in passato, ora dovrai aggiungere le autorizzazioni BigQuery al ruolo utente BlueXP . Sono necessari per la ricerca e il ripristino.

- Requisiti StorageGRID e ONTAP S3:

  A seconda della configurazione, sono disponibili 2 modi per implementare Search & Restore:

  - Se non sono presenti credenziali del provider cloud nell'account, le informazioni del catalogo indicizzate vengono memorizzate nel connettore.

    Per informazioni sul catalogo indicizzato v2, vedere la sezione seguente su come abilitare il catalogo indicizzato.

  - Se si utilizza un connettore in un sito privato (scuro), le informazioni del catalogo indicizzate vengono memorizzate nel connettore (richiede la versione 3.9.25 o superiore del connettore).
  - Se lo hai fatto "Credenziali AWS" oppure "Credenziali Azure" Nell'account, il catalogo indicizzato viene memorizzato presso il cloud provider, proprio come con un connettore implementato nel cloud. (Se si dispone di entrambe le credenziali, AWS è selezionato per impostazione predefinita).

    Anche se si utilizza un connettore on-premise, i requisiti del cloud provider devono essere soddisfatti sia per le autorizzazioni dei connettori che per le risorse del cloud provider. Per l'utilizzo di questa implementazione, vedere i requisiti AWS e Azure riportati sopra.

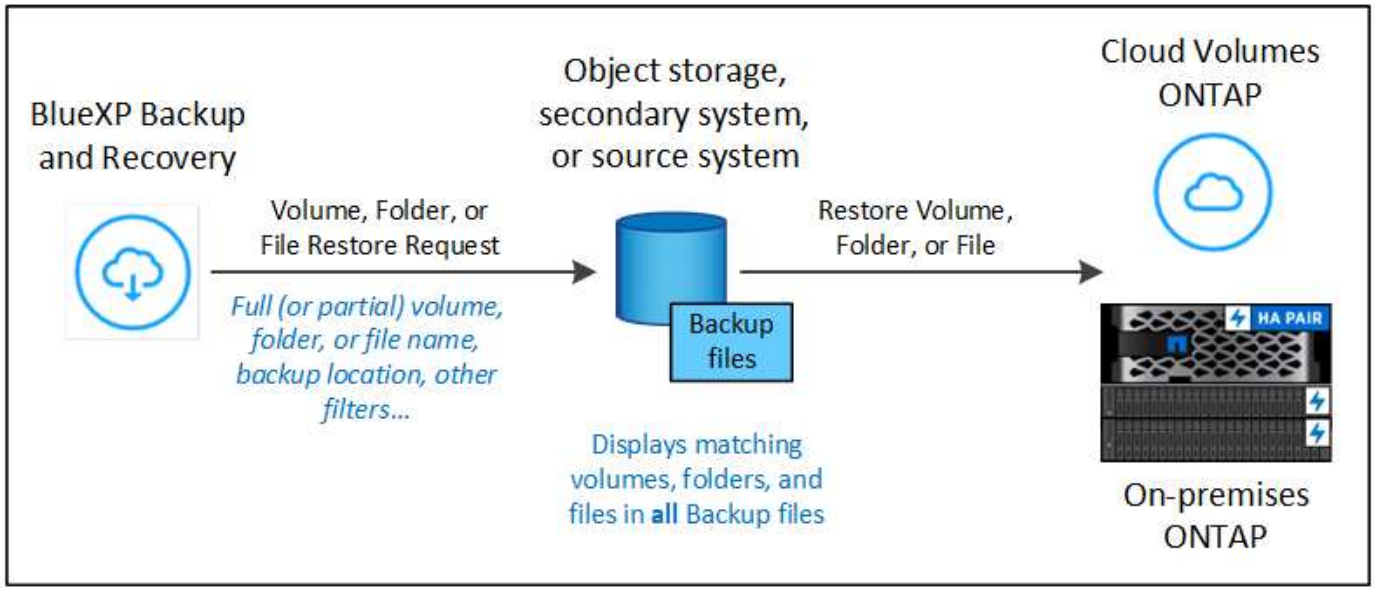
Processo di ricerca e ripristino

Il processo è simile al seguente:

1. Prima di utilizzare Search & Restore, è necessario attivare l'indicizzazione su ogni ambiente di lavoro di origine da cui si desidera ripristinare i dati dei volumi. Questo consente al catalogo indicizzato di tenere traccia dei file di backup per ogni volume.
2. Per ripristinare un volume o dei file da un backup del volume, in *Cerca e ripristina*, selezionare **Cerca e ripristina**.
3. Immettere i criteri di ricerca per un volume, una cartella o un file in base al nome parziale o completo del volume, al nome parziale o completo del file, alla posizione del backup, all'intervallo di dimensioni, all'intervallo di date di creazione, ad altri filtri di ricerca e selezionare **Cerca**.

La pagina risultati ricerca visualizza tutte le posizioni in cui è presente un file o un volume corrispondente ai criteri di ricerca.

4. Selezionare **Visualizza tutti i backup** per la posizione in cui si desidera ripristinare il volume o il file, quindi selezionare **Ripristina** sul file di backup effettivo che si desidera utilizzare.
5. Selezionare la posizione in cui si desidera ripristinare il volume, la cartella o i file e selezionare **Ripristina**.
6. Il volume, la cartella o i file vengono ripristinati.



Come si può vedere, è sufficiente conoscere un nome parziale e le ricerche di backup e ripristino di BlueXP attraverso tutti i file di backup che corrispondono alla ricerca.

Abilitare il catalogo indicizzato per ogni ambiente di lavoro

Prima di utilizzare Search & Restore, è necessario attivare l'indicizzazione su ogni ambiente di lavoro di origine da cui si intende ripristinare volumi o file. Questo consente al catalogo indicizzato di tenere traccia di ogni volume e di ogni file di backup, rendendo le ricerche molto rapide ed efficienti.

Il catalogo indicizzato è un database che memorizza i metadati relativi a tutti i volumi e i file di backup nell'ambiente di lavoro. Viene utilizzato dalla funzionalità Cerca e ripristina per trovare rapidamente i file di backup che contengono i dati che si desidera ripristinare.

Funzionalità del catalogo indicizzato v2

L'Indexed Catalog v2, rilasciato a febbraio 2025 e aggiornato a giugno 2025, include funzionalità che lo rendono più efficiente e facile da usare. Questa versione ha un significativo miglioramento delle prestazioni ed è abilitata per impostazione predefinita per tutti i nuovi clienti.

Fare riferimento alle seguenti considerazioni relative a v2:

- Il catalogo indicizzato v2 è disponibile in modalità anteprima.
- Se si è già clienti e si desidera utilizzare il catalogo v2, è necessario riindicizzare completamente l'ambiente.
- Il Catalogo v2 indicizza solo gli snapshot che hanno un'etichetta snapshot.
- Il backup e ripristino di BlueXP non indicizza le snapshot con etichette SnapMirror "orarie". Se si desidera indicizzare le istantanee con l'etichetta SnapMirror "oraria", è necessario attivarla manualmente mentre v2

è in modalità anteprima.

- Il backup e ripristino BlueXP indicizzerà i volumi e le snapshot associati agli ambienti di lavoro protetti dal backup e ripristino BlueXP solo con il catalogo v2. Gli altri ambienti di lavoro rilevati sulla piattaforma BlueXP non verranno indicizzati.
- L'indicizzazione dei dati con Catalog v2 avviene negli ambienti on-premise e negli ambienti Amazon Web Services, Microsoft Azure e Google Cloud Platform (GCP).

Il catalogo indicizzato v2 supporta quanto segue:

- Efficienza della ricerca globale in meno di 3 minuti
- Fino a 5 miliardi di file
- Fino a 5000 volumi per cluster
- Fino a 100K snapshot per volume
- Il tempo massimo per l'indicizzazione della linea di base è inferiore a 7 giorni. Il tempo effettivo varia a seconda dell'ambiente.

Abilitazione del catalogo indicizzato per un ambiente di lavoro

Il servizio non esegue il provisioning di un bucket separato quando si utilizza il Catalogo indicizzato v2. Invece, per i backup archiviati in AWS, Azure, Google Cloud Platform, StorageGRID o ONTAP S3, il servizio esegue il provisioning dello spazio sul connettore o nell'ambiente del provider cloud.

Se hai abilitato il catalogo indicizzato prima della versione v2, con gli ambienti di lavoro si verifica quanto segue:

- Per i backup memorizzati in AWS, fornisce un nuovo bucket S3 e il "Servizio di query interattiva Amazon Athena" e. "Servizio di integrazione dei dati senza server AWS Glue".
- Per i backup memorizzati in Azure, il sistema fornisce un'area di lavoro di Azure Synapse e un file system di Data Lake come contenitore per memorizzare i dati dell'area di lavoro.
- Per i backup memorizzati in Google Cloud, fornisce un nuovo bucket e il "Servizi Google Cloud BigQuery" sono forniti a livello di account/progetto.
- Per i backup archiviati in StorageGRID o ONTAP S3, offre spazio sul connettore o sull'ambiente cloud provider.

Se l'indicizzazione è già stata attivata per l'ambiente di lavoro, passare alla sezione successiva per ripristinare i dati.

Procedura per attivare l'indicizzazione per un ambiente di lavoro:

1. Effettuare una delle seguenti operazioni:
    - Se non sono stati indicizzati ambienti di lavoro, nella dashboard di ripristino in *Search & Restore*, selezionare **Enable Indexing for Working Environments** (Abilita indicizzazione per ambienti di lavoro).
    - Se almeno un ambiente di lavoro è già stato indicizzato, nella dashboard di ripristino in *Cerca e ripristina*, seleziona **Impostazioni di indicizzazione**.
2. Selezionare **Abilita indicizzazione** per l'ambiente di lavoro.

Risultato

Una volta eseguito il provisioning di tutti i servizi e attivato il catalogo indicizzato, l'ambiente di lavoro viene visualizzato come "attivo".

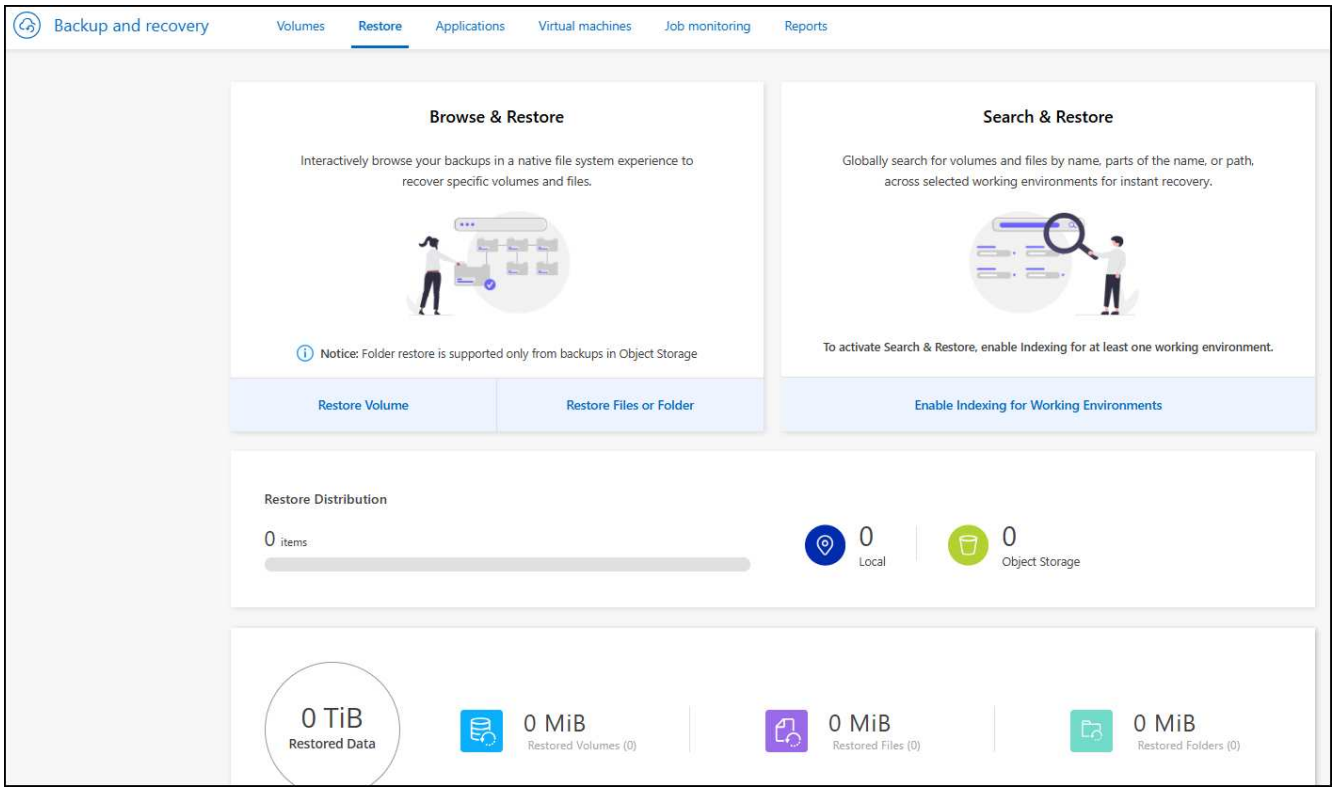
A seconda delle dimensioni dei volumi nell'ambiente di lavoro e del numero di file di backup in tutte e 3 le posizioni di backup, il processo di indicizzazione iniziale potrebbe richiedere fino a un'ora. Successivamente, viene aggiornato in modo trasparente ogni ora con modifiche incrementali per rimanere aggiornato.

Ripristinare volumi, cartelle e file utilizzando Search & Restore

Dopo di che Indicizzazione abilitata per l'ambiente di lavoro, È possibile ripristinare volumi, cartelle e file utilizzando Search & Restore. In questo modo, è possibile utilizzare un'ampia gamma di filtri per individuare il file o il volume esatto che si desidera ripristinare da tutti i file di backup.

Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** per visualizzare la Dashboard di ripristino.
3. Dalla sezione *Cerca e ripristina*, seleziona **Cerca e ripristina**.
4. Dalla sezione *Cerca e ripristina*, seleziona **Cerca e ripristina**.



5. Dalla pagina Cerca e ripristina:
   a. Nella *barra di ricerca*, immettere un nome completo o parziale del volume, del nome della cartella o del file.
   b. Selezionare il tipo di risorsa: **Volumi**, **file**, **cartelle** o **tutto**.
   c. Nell'area *Filtra per*, selezionare i criteri di filtro. Ad esempio, è possibile selezionare l'ambiente di lavoro in cui risiedono i dati e il tipo di file, ad esempio un file .JPEG. In alternativa, è possibile selezionare il tipo di percorso di backup se si desidera cercare i risultati solo all'interno delle copie Snapshot o dei file di backup disponibili nello storage a oggetti.
6. Selezionando **Cerca**, nell'area Risultati della ricerca verranno visualizzate tutte le risorse che contengono un file, una cartella o un volume che corrisponde alla tua ricerca.
7. Individua la risorsa contenente i dati che desideri ripristinare e seleziona **Visualizza tutti i backup** per

visualizzare tutti i file di backup che contengono il volume, la cartella o il file corrispondente.

8. Individua il file di backup che vuoi utilizzare per ripristinare i dati e seleziona **Ripristina**.

   I risultati identificano le copie Snapshot dei volumi locali e i volumi replicati remoti che contengono il file nella ricerca. Puoi scegliere di eseguire il ripristino dal file di backup nel cloud, dalla copia Snapshot o dal volume replicato.

9. Selezionare la posizione di destinazione in cui si desidera ripristinare il volume, la cartella o i file e selezionare **Ripristina**.
   - Per i volumi, è possibile selezionare l'ambiente di lavoro di destinazione originale oppure un ambiente di lavoro alternativo. Durante il ripristino di un volume FlexGroup, dovrai scegliere più aggregati.
   - Per le cartelle, è possibile ripristinare la posizione originale oppure selezionare una posizione alternativa, inclusi ambiente di lavoro, volume e cartella.
   - Per i file, è possibile ripristinare la posizione originale oppure selezionare una posizione alternativa, inclusi ambiente di lavoro, volume e cartella. Quando si seleziona la posizione originale, è possibile scegliere di sovrascrivere i file di origine o di creare nuovi file.

     Se si seleziona un sistema ONTAP on-premise e non è già stata configurata la connessione del cluster allo storage a oggetti, vengono richieste ulteriori informazioni:

     - Quando si esegue il ripristino da Amazon S3, selezionare IPSpace nel cluster ONTAP in cui si trova il volume di destinazione, immettere la chiave di accesso e la chiave segreta per l'utente creato per consentire al cluster ONTAP di accedere al bucket S3, E, se lo si desidera, scegliere un endpoint VPC privato per il trasferimento sicuro dei dati. "Consulta i dettagli su questi requisiti".
     - Quando si esegue il ripristino da Azure Blob, selezionare IPSpace nel cluster ONTAP in cui si trova il volume di destinazione e, se si desidera, scegliere un endpoint privato per il trasferimento sicuro dei dati selezionando VNET e Subnet. "Consulta i dettagli su questi requisiti".
     - Quando si esegue il ripristino da Google Cloud Storage, selezionare IPSpace nel cluster ONTAP in cui si trova il volume di destinazione e la chiave di accesso e la chiave segreta per accedere allo storage a oggetti. "Consulta i dettagli su questi requisiti".
     - Quando si esegue il ripristino da StorageGRID, immettere l'FQDN del server StorageGRID e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID, immettere la chiave di accesso e la chiave segreta necessarie per accedere allo storage a oggetti e l'IPSpace nel cluster ONTAP in cui risiede il volume di destinazione. "Consulta i dettagli su questi requisiti".
     - Quando si esegue il ripristino da ONTAP S3, immettere l'FQDN del server ONTAP S3 e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con ONTAP S3, selezionare la chiave di accesso e la chiave segreta necessarie per accedere all'archivio oggetti, e l'IPSpace nel cluster ONTAP in cui risiede il volume di destinazione. "Consulta i dettagli su questi requisiti".

Risultati

Il volume, la cartella o i file vengono ripristinati e si torna alla dashboard di ripristino, in modo da poter esaminare l'avanzamento dell'operazione di ripristino. È anche possibile selezionare la scheda **Monitoraggio processi** per visualizzare l'avanzamento del ripristino. Vedere "Pagina di monitoraggio dei lavori".

Proteggere i carichi di lavoro di Microsoft SQL Server

Panoramica sulla protezione dei carichi di lavoro Microsoft SQL con BlueXP backup and recovery

Proteggi i dati delle tue applicazioni Microsoft SQL Server dai sistemi ONTAP on-premise ad Amazon Web Services, Microsoft Azure o StorageGRID utilizzando il BlueXP backup and recovery. I backup vengono generati automaticamente e archiviati in un archivio oggetti nel tuo account cloud pubblico o privato, in base alle policy che crei. Puoi implementare una strategia 3-2-1, in cui hai 3 copie dei dati di origine su 2 sistemi di storage diversi e 1 copia nel cloud.

I vantaggi dell'approccio 3-2-1 includono:

- Copie multiple dei dati offrono protezione multi-layer contro le minacce interne (interne) e esterne alla cybersicurezza.
- Diversi tipi di supporti garantiscono la fattibilità del failover in caso di guasto fisico o logico di un tipo di supporto.
- La copia in loco agevola i ripristini rapidi, mentre le copie fuori sede sono disponibili nel caso in cui la copia in loco sia compromessa.

Il BlueXP backup and recovery sfruttano la tecnologia di replicazione dei dati NetApp SnapMirror per garantire che tutti i backup siano completamente sincronizzati creando copie snapshot e trasferendole nelle posizioni di backup.

È possibile raggiungere i seguenti obiettivi di protezione:

- "Configurare elementi aggiuntivi se si importa da SnapCenter"
- "Scopri i carichi di lavoro di Microsoft SQL Server e, facoltativamente, importa le risorse SnapCenter"
- "Eseguire il backup dei carichi di lavoro con snapshot locali sullo storage primario ONTAP locale"
- "Replicare i carichi di lavoro sullo storage secondario ONTAP"
- "Eseguire il backup dei carichi di lavoro in una posizione di archiviazione oggetti"
- "Esegui subito il backup dei carichi di lavoro"
- "Ripristinare i carichi di lavoro"
- "Clonare i carichi di lavoro"
- "Gestire l'inventario dei carichi di lavoro"
- "Gestione delle snapshot"

Per eseguire il backup dei carichi di lavoro, in genere si creano policy che regolano le operazioni di backup e ripristino. Per ulteriori informazioni, vedere "Creare policy" .

Destinazioni di backup supportate

Il BlueXP backup and recovery consentono di eseguire il backup di istanze e database di Microsoft SQL Server dai seguenti ambienti di lavoro di origine ai seguenti ambienti di lavoro secondari e all'archiviazione di oggetti nei provider di cloud pubblici e privati. Le copie Snapshot risiedono nell'ambiente di lavoro di origine.

Ambiente di lavoro di origine	Ambiente di lavoro secondario (replica)	Archivio oggetti di destinazione (backup)
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise	Amazon S3 ONTAP S3
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise	Azure Blob ONTAP S3
Sistema ONTAP on-premise	Cloud Volumes ONTAP Sistema ONTAP on-premise	Blob di Azure Amazon S3 NetApp StorageGRID ONTAP S3
Amazon FSX per NetApp ONTAP	Amazon FSX per NetApp ONTAP	NA ifdef::gcp[] endif::gcp[] ifdef::gcp[] endif::gcp[]

Destinazioni di ripristino supportate

È possibile ripristinare istanze e database di Microsoft SQL Server da un backup residente nell'archivio primario o in un ambiente di lavoro secondario (un volume replicato) o nell'archivio oggetti (un file di backup) nei seguenti ambienti di lavoro. Le copie Snapshot risiedono nell'ambiente di lavoro di origine e possono essere ripristinate solo sullo stesso sistema.

Dalla posizione del file di backup		A ambiente di lavoro di destinazione
Archivio oggetti (backup)	**Sistema secondario (replica)**	
Amazon S3	Cloud Volumes ONTAP in AWS Sistema ONTAP on-premise	Cloud Volumes nel sistema ONTAP locale AWS ONTAP S3
Azure Blob	Cloud Volumes ONTAP in Azure Sistema ONTAP on-premise	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure ONTAP S3 ifdef::gcp[] endif::gcp[]
StorageGRID	Cloud Volumes ONTAP Sistema ONTAP on-premise	Sistema ONTAP on-premise ONTAP S3
Amazon FSX per NetApp ONTAP	Amazon FSX per NetApp ONTAP	N / A

I riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS e AFF .

Prerequisiti per l'importazione dal servizio Plug-in nel BlueXP backup and recovery

Se si desidera importare risorse dal servizio plug-in SnapCenter per Microsoft SQL Server nel BlueXP backup and recovery, sarà necessario configurare alcuni altri elementi.

Crea prima gli ambienti di lavoro in BlueXP Canvas

Se si desidera importare risorse da SnapCenter, è consigliabile creare ambienti di lavoro in BlueXP Canvas per tutti gli storage del cluster SnapCenter locale prima di importare da SnapCenter. Ciò garantisce che le risorse host possano essere rilevate e importate correttamente.

Verificare i requisiti dell'host per installare il plug-in SnapCenter

Per importare risorse dal plug-in SnapCenter per Microsoft SQL Server, assicurarsi che siano soddisfatti i requisiti host per l'installazione del plug-in SnapCenter per Microsoft SQL Server.

Controllare specificamente i requisiti SnapCenter in "Prerequisiti per il BlueXP backup and recovery" .

Disabilitare le restrizioni remote del Controllo account utente

Prima di importare risorse da SnapCenter, disabilitare le restrizioni remote del Controllo Account Utente (UAC) sull'host Windows di SnapCenter . Disattivare UAC se si utilizza un account amministrativo locale per connettersi in remoto all'host del server SnapCenter o all'host SQL.

Considerazioni sulla sicurezza

Prima di disattivare le restrizioni remote UAC, tenere presente quanto segue:

- Rischio per la sicurezza: la disattivazione del filtraggio dei token può esporre il sistema a vulnerabilità di sicurezza, soprattutto se gli account amministrativi locali vengono compromessi da malintenzionati.
- Usare con cautela:
  - Modificare questa impostazione solo se è essenziale per le attività amministrative.
  - Assicurarsi che siano in atto password complesse e altre misure di sicurezza per proteggere gli account amministrativi.

Soluzioni alternative

- Se è richiesto l'accesso amministrativo remoto, valutare l'utilizzo di account di dominio con privilegi appropriati.
- Utilizzare strumenti di gestione remota sicuri che aderiscano alle migliori pratiche di sicurezza per ridurre al minimo i rischi.

Passaggi per disattivare le restrizioni remote del Controllo account utente

1. Modificare il `LocalAccountTokenFilterPolicy` chiave di registro sull'host Windows SnapCenter .

   Per farlo, utilizza uno dei seguenti metodi, di seguito le istruzioni:

   - Metodo 1: Editor del Registro di sistema
   - Metodo 2: script PowerShell

Metodo 1: disabilitare il controllo dell'account utente tramite l'editor del Registro di sistema

Questo è uno dei metodi che puoi utilizzare per disattivare il Controllo dell'account utente.

Fasi

1. Aprire l'Editor del Registro di sistema sull'host Windows di SnapCenter procedendo come segue:
   a. Premere `Windows+R` per aprire la finestra di dialogo Esegui.
   b. Tipo `regedit` e premere `Enter` .
2. Passare alla chiave della policy:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

3. Crea o modifica il `DWORD` valore:
   a. Individuare: `LocalAccountTokenFilterPolicy`
   b. Se non esiste, creane uno nuovo `DWORD` (32 bit) Valore denominato

`LocalAccountTokenFilterPolicy`.

4. Sono supportati i seguenti valori. Per questo scenario, impostare il valore su `1` :
   - `0` (Predefinito): le restrizioni remote UAC sono abilitate. Gli account locali hanno token filtrati quando accedono da remoto.
   - `1` : Le restrizioni remote UAC sono disabilitate. Gli account locali ignorano il filtro dei token e dispongono di privilegi amministrativi completi quando accedono da remoto.
5. Fare clic su **OK**.
6. Chiudere l'editor del Registro di sistema.
7. Riavviare l'host Windows di SnapCenter .

Esempio di modifica del registro

Questo esempio imposta LocalAccountTokenFilterPolicy su "1", disabilitando le restrizioni remote UAC.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Metodo 2: disabilitare il controllo dell'account utente tramite uno script di PowerShell

Questo è un altro metodo che puoi utilizzare per disattivare il Controllo dell'account utente.

> L'esecuzione di comandi di PowerShell con privilegi elevati può influire sulle impostazioni di sistema. Assicurarsi di comprendere i comandi e le relative implicazioni prima di eseguirli.

Fasi

1. Aprire una finestra di PowerShell con privilegi amministrativi sull'host Windows di SnapCenter :
   a. Fare clic sul menu **Start**.
   b. Cerca **PowerShell 7** o **Windows Powershell**.
   c. Fare clic con il tasto destro del mouse su tale opzione e selezionare **Esegui come amministratore**.
2. Assicurati che PowerShell sia installato sul tuo sistema. Dopo l'installazione, dovrebbe apparire nel menu **Start**.

   > PowerShell è incluso di default in Windows 7 e versioni successive.

3. Per disattivare le restrizioni remote UAC, impostare LocalAccountTokenFilterPolicy su "1" eseguendo il seguente comando:

   ```
   Set-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
   ```

4. Verificare che il valore corrente sia impostato su "1" in `LocalAccountTokenFilterPolicy` eseguendo:

```
Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"
```

- Se il valore è 1, le restrizioni remote UAC sono disabilitate.
- Se il valore è 0, le restrizioni remote UAC sono abilitate.

5. Per applicare le modifiche, riavviare il computer.

Esempi di comandi di PowerShell 7 per disabilitare le restrizioni remote UAC:

Questo esempio con il valore impostato su "1" indica che le restrizioni remote UAC sono disabilitate.

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Scopri i carichi di lavoro di Microsoft SQL Server e, facoltativamente, importali da SnapCenter nel BlueXP backup and recovery

Per poter utilizzare il servizio BlueXP backup and recovery, è necessario prima rilevare i carichi di lavoro di Microsoft SQL Server. È possibile importare dati e criteri di backup da SnapCenter , se SnapCenter è già installato.

Ruolo BlueXP obbligatorio Questa attività richiede il ruolo di super amministratore per il backup e il ripristino dei servizi dati. Scopri di più"Ruoli e privilegi dei servizi di backup e ripristino dati" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Scopri i carichi di lavoro di Microsoft SQL Server e, facoltativamente, importa le risorse SnapCenter

Durante la fase di individuazione, il BlueXP backup and recovery analizzano le istanze e i database di Microsoft SQL Server negli ambienti di lavoro all'interno della tua organizzazione.

BlueXP backup and recovery valuta le applicazioni Microsoft SQL Server. Il servizio valuta il livello di protezione esistente, inclusi i criteri di protezione dei backup, le copie snapshot e le opzioni di backup e ripristino.

La scoperta avviene nei seguenti modi:

- Se hai già SnapCenter, importa le risorse SnapCenter nel BlueXP backup and recovery utilizzando l'interfaccia utente BlueXP backup and recovery .

> Se hai già SnapCenter, verifica innanzitutto di aver soddisfatto i prerequisiti prima di importare da SnapCenter. Ad esempio, dovresti creare ambienti di lavoro in BlueXP Canvas per tutto lo storage del cluster SnapCenter locale prima di importare da SnapCenter. Vedere "Prerequisiti per l'importazione di risorse da SnapCenter".

- Se non disponi ancora SnapCenter, puoi comunque individuare i carichi di lavoro nei tuoi ambienti di lavoro aggiungendo manualmente un vCenter ed eseguendo l'individuazione.

Se SnapCenter è già installato, importare le risorse SnapCenter nel BlueXP backup and recovery

Se SnapCenter è già installato, importa le risorse SnapCenter in BlueXP backup and recovery seguendo questi passaggi. Il servizio BlueXP rileva risorse, host, credenziali e pianificazioni da SnapCenter; non è necessario ricreare tutte queste informazioni.

Puoi farlo nei seguenti modi:

- Durante l'individuazione, seleziona un'opzione per importare risorse da SnapCenter.
- Dopo l'individuazione, dalla pagina Inventario, seleziona un'opzione per importare le risorse SnapCenter .
- Dopo l'individuazione, dal menu Impostazioni, seleziona un'opzione per importare le risorse SnapCenter . Per ulteriori informazioni, vedere "Configurare il BlueXP backup and recovery".

Si tratta di un processo in due parti:

- Importare l'applicazione SnapCenter Server e le risorse host
- Gestisci le risorse host SnapCenter selezionate

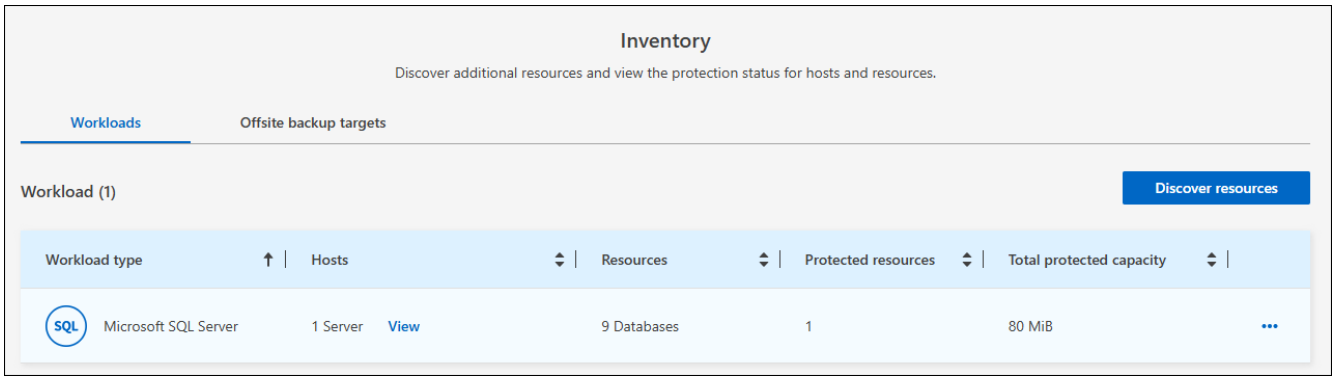
Importare l'applicazione SnapCenter Server e le risorse host

Questo primo passaggio importa le risorse host da SnapCenter e le visualizza nella pagina Inventario di BlueXP backup and recovery . A quel punto, le risorse non sono ancora gestite da BlueXP backup and recovery.

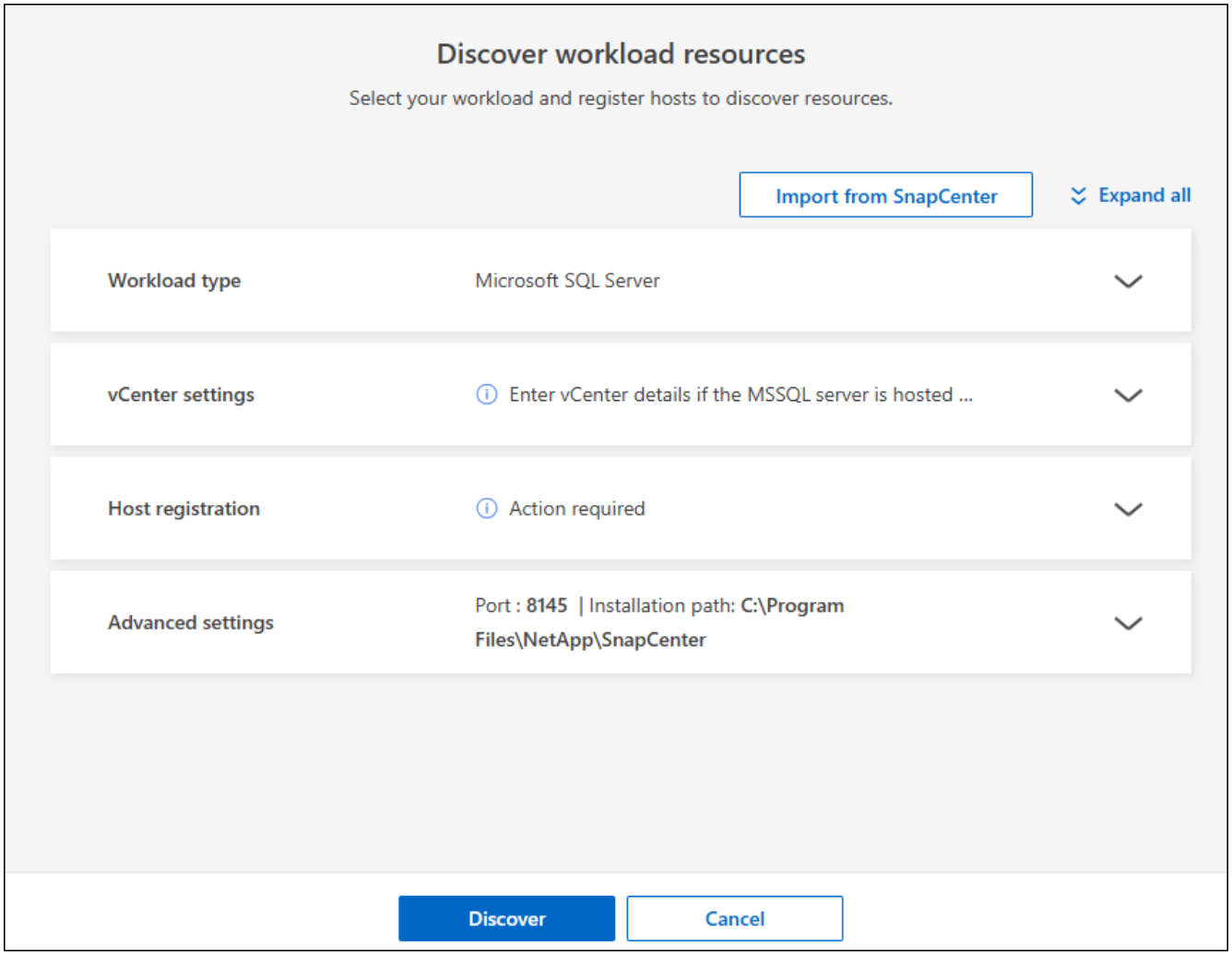
> Dopo aver importato le risorse host SnapCenter , BlueXP backup and recovery non assume automaticamente la gestione della protezione. Per farlo, è necessario selezionare esplicitamente la gestione delle risorse importate in BlueXP backup and recovery. In questo modo, si è certi di poter eseguire il backup di tali risorse da parte di BlueXP backup and recovery.

Fasi

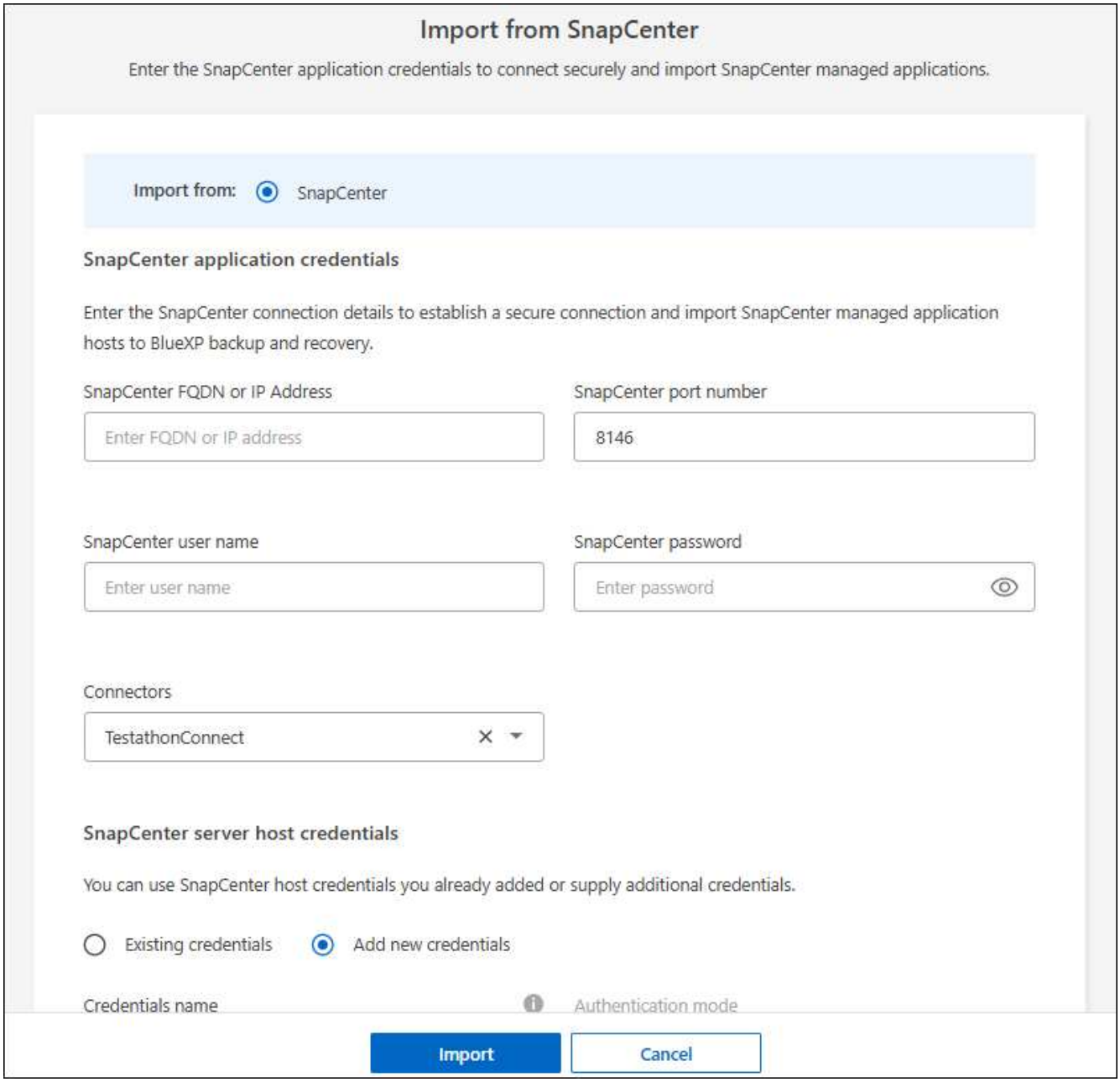
1. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.
2. Dal menu in alto, seleziona **Inventario**.



3. Dal menu in alto, seleziona **Scopri risorse**.



4. Dalla pagina delle risorse del carico di lavoro Discover BlueXP backup and recovery , seleziona **Importa da SnapCenter**.

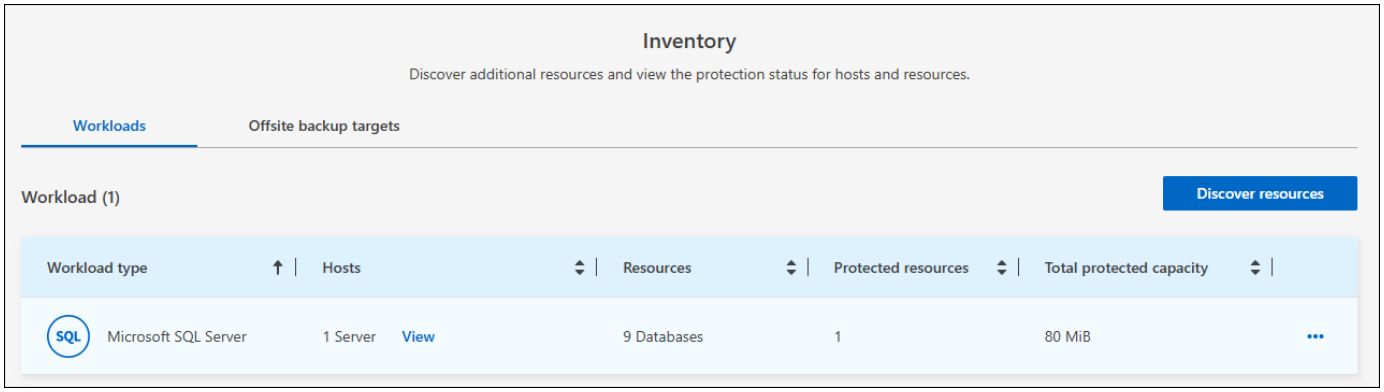


5. Inserisci * credenziali dell'applicazione SnapCenter *:
   a. * FQDN o indirizzo IP SnapCenter *: immettere l'FQDN o l'indirizzo IP dell'applicazione SnapCenter stessa.
   b. **Porta**: immettere il numero di porta per il server SnapCenter .
   c. **Nome utente** e **Password**: inserisci il nome utente e la password per SnapCenter Server.
   d. **Connettore**: seleziona il connettore BlueXP per SnapCenter.
6. Inserisci * credenziali host del server SnapCenter *:
   a. **Credenziali esistenti**: Se selezioni questa opzione, puoi utilizzare le credenziali esistenti che hai già aggiunto. Scegli il nome delle credenziali.
   b. **Aggiungi nuove credenziali**: se non disponi di credenziali host SnapCenter , puoi aggiungerne di nuove. Inserisci il nome delle credenziali, la modalità di autenticazione, il nome utente e la password.
7. Selezionare **Importa** per convalidare le voci e registrare SnapCenter Server.

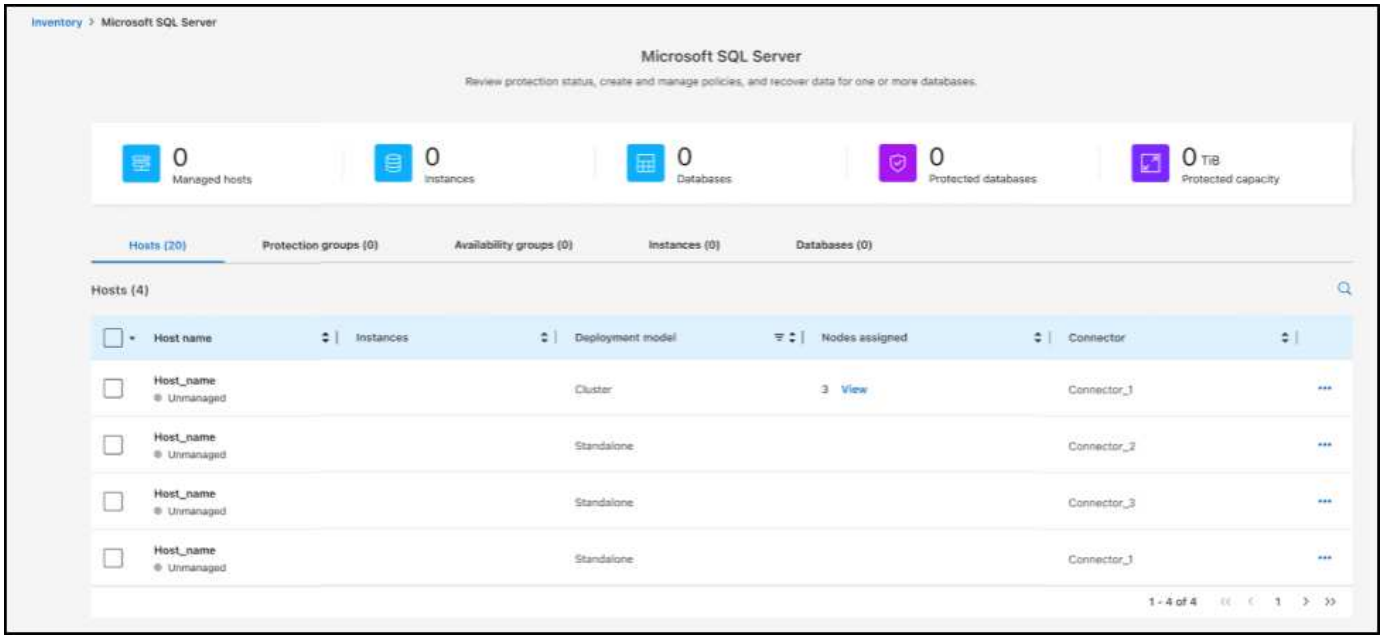
Se SnapCenter Server è già registrato, è possibile aggiornare i dettagli di registrazione esistenti.

Risultato

La pagina Inventario mostra le risorse SnapCenter importate, che includono host, istanze e database MS SQL.



Per visualizzare i dettagli delle risorse SnapCenter importate, selezionare l'opzione **Visualizza dettagli** dal menu Azioni.

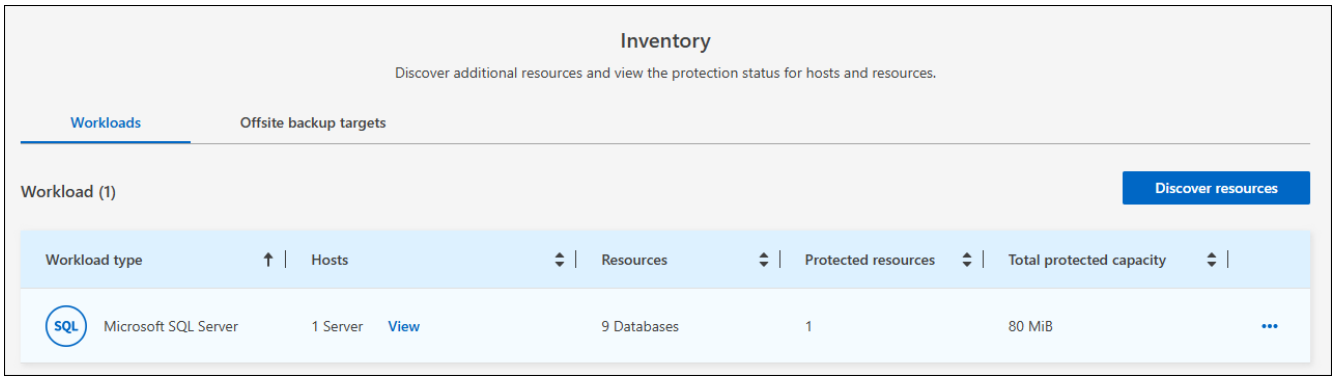


Gestire le risorse host SnapCenter

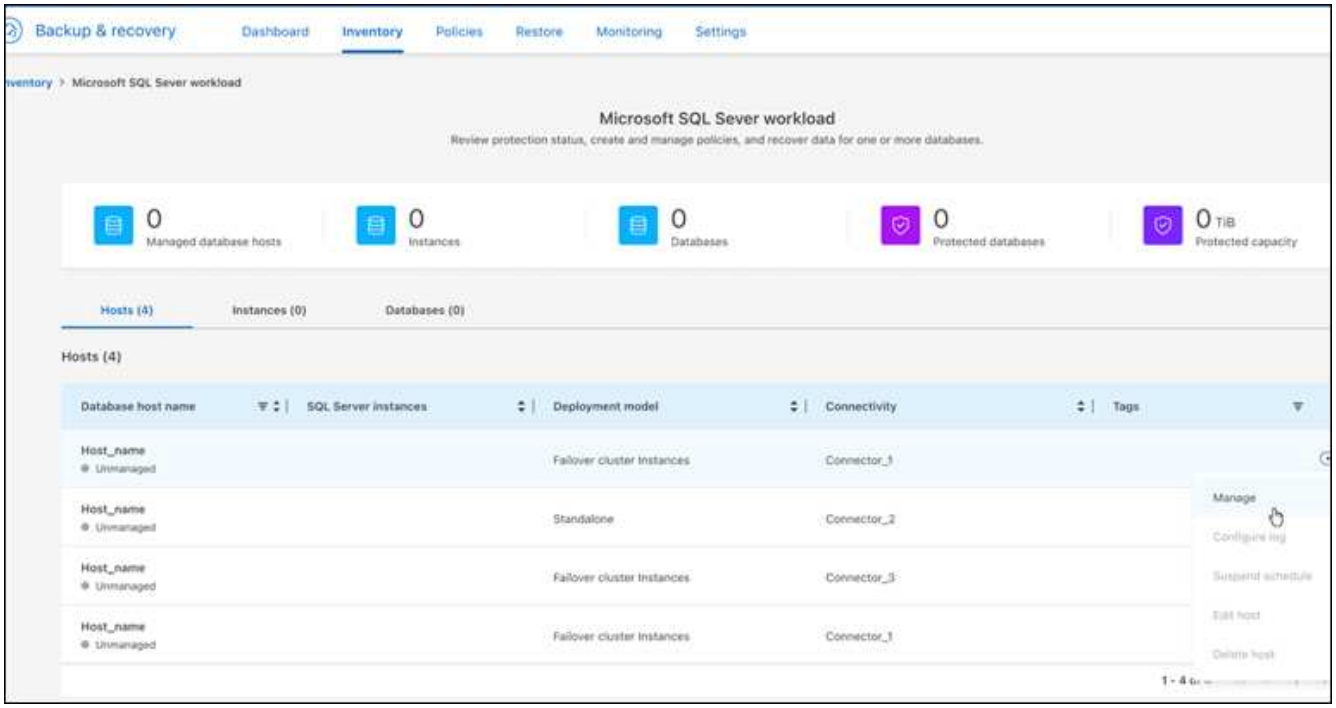
Dopo aver importato le risorse SnapCenter , gestisci tali risorse host in BlueXP backup and recovery. Dopo aver scelto di gestire tali risorse, BlueXP backup and recovery sarà in grado di eseguire il backup e il ripristino delle risorse importate da SnapCenter. Tali risorse non saranno più gestite in SnapCenter Server.

Fasi

1. Dopo aver importato le risorse SnapCenter , seleziona **Inventario** dal menu in alto.
2. Dalla pagina Inventario, seleziona l'host SnapCenter importato che da ora in poi dovrà essere gestito BlueXP backup and recovery .



3. Seleziona l'icona Azioni ••• > **Visualizza dettagli** per visualizzare i dettagli del carico di lavoro.



4. Dalla pagina Inventario > carico di lavoro, seleziona l'icona Azioni ••• > **Gestisci** per visualizzare la pagina Gestisci host.
5. Selezionare **Gestisci**.
6. Nella pagina Gestisci host, seleziona se utilizzare un vCenter esistente o aggiungerne uno nuovo.
7. Selezionare **Gestisci**.

   La pagina Inventario mostra le risorse SnapCenter appena gestite.

Facoltativamente, puoi creare un report delle risorse gestite selezionando l'opzione **Genera report** dal menu Azioni.

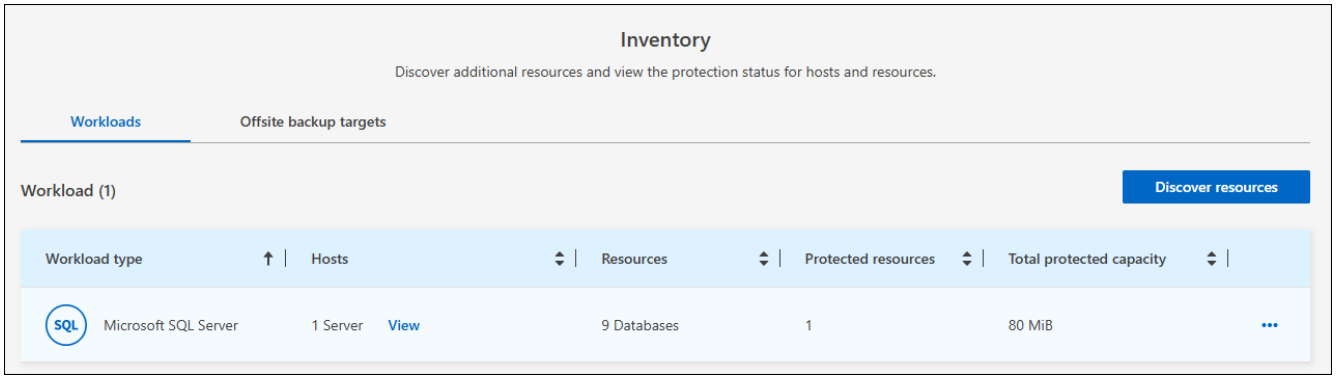
Importare le risorse SnapCenter dopo la scoperta dalla pagina Inventario

Se hai già scoperto delle risorse, puoi importare le risorse SnapCenter dalla pagina Inventario.

Fasi

1. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.

2. Dal menu in alto, seleziona **Inventario**.



3. Dalla pagina Inventario, seleziona *Importa risorse SnapCenter *.
4. Per importare le risorse SnapCenter , seguire i passaggi descritti nella sezione *Importa risorse SnapCenter * sopra.

Se SnapCenter non è installato, aggiungi un vCenter e scopri le risorse

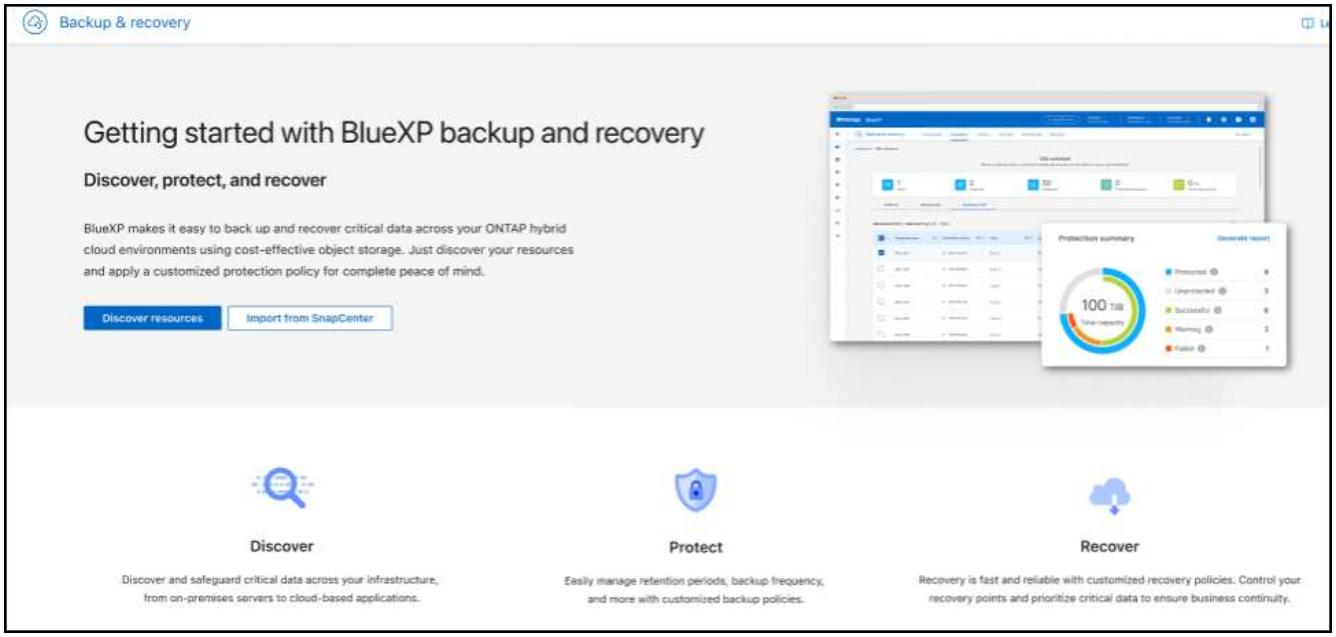
Se SnapCenter non è ancora installato, è possibile aggiungere informazioni su vCenter e fare in modo che BlueXP backup and recovery rilevi i carichi di lavoro. All'interno di ciascun BlueXP Connector, seleziona gli ambienti di lavoro in cui desideri individuare i carichi di lavoro.

Questa operazione è facoltativa se si dispone di un ambiente VMware.

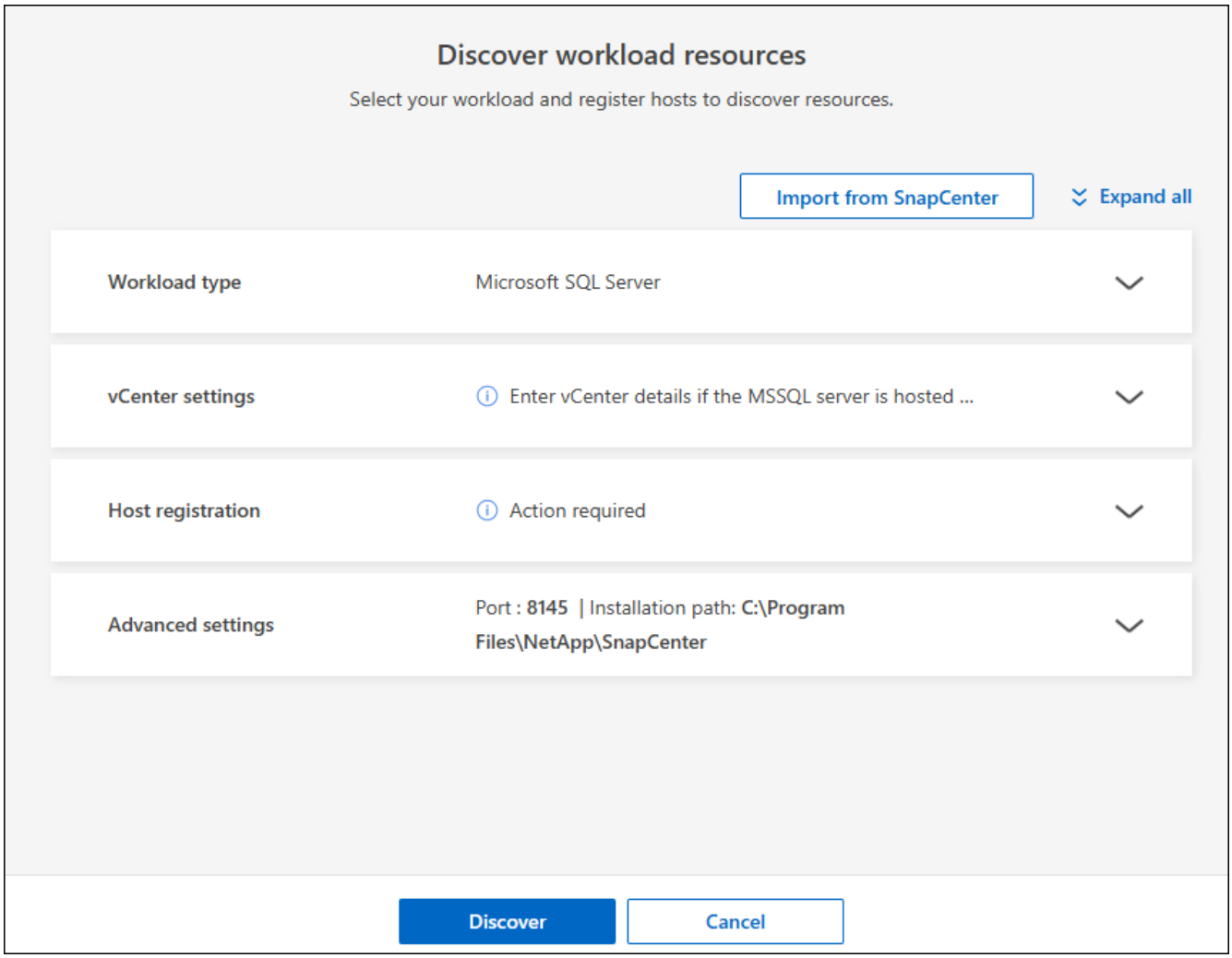
Fasi

1. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.

   Se è la prima volta che accedi a questo servizio e hai già un ambiente di lavoro in BlueXP, ma non hai scoperto alcuna risorsa, viene visualizzata la pagina di destinazione "Benvenuti nel nuovo BlueXP backup and recovery" che mostra un'opzione per **Scoprire risorse**.



2. Seleziona **Scopri risorse**.



3. Inserire le seguenti informazioni:
   a. **Tipo di carico di lavoro**: per questa versione è disponibile solo Microsoft SQL Server.
   b. **Impostazioni vCenter**: seleziona un vCenter esistente o aggiungine uno nuovo. Per aggiungere un nuovo vCenter, inserisci il nome di dominio completo (FQDN) o l'indirizzo IP del vCenter, il nome utente, la password, la porta e il protocollo.

      Se si inseriscono informazioni su vCenter, inserire le informazioni sia per le impostazioni di vCenter che per la registrazione dell'host. Se si sono aggiunte o inserite informazioni su vCenter qui, è necessario aggiungere anche le informazioni sui plugin nelle Impostazioni avanzate.

   c. **Registrazione host**: seleziona **Aggiungi credenziali** e inserisci le informazioni sugli host che contengono i carichi di lavoro che vuoi scoprire.

      Se si aggiunge un server autonomo e non un server vCenter, immettere solo le informazioni sull'host.

4. Selezionare **Discover**.

   Questo processo potrebbe richiedere alcuni minuti.

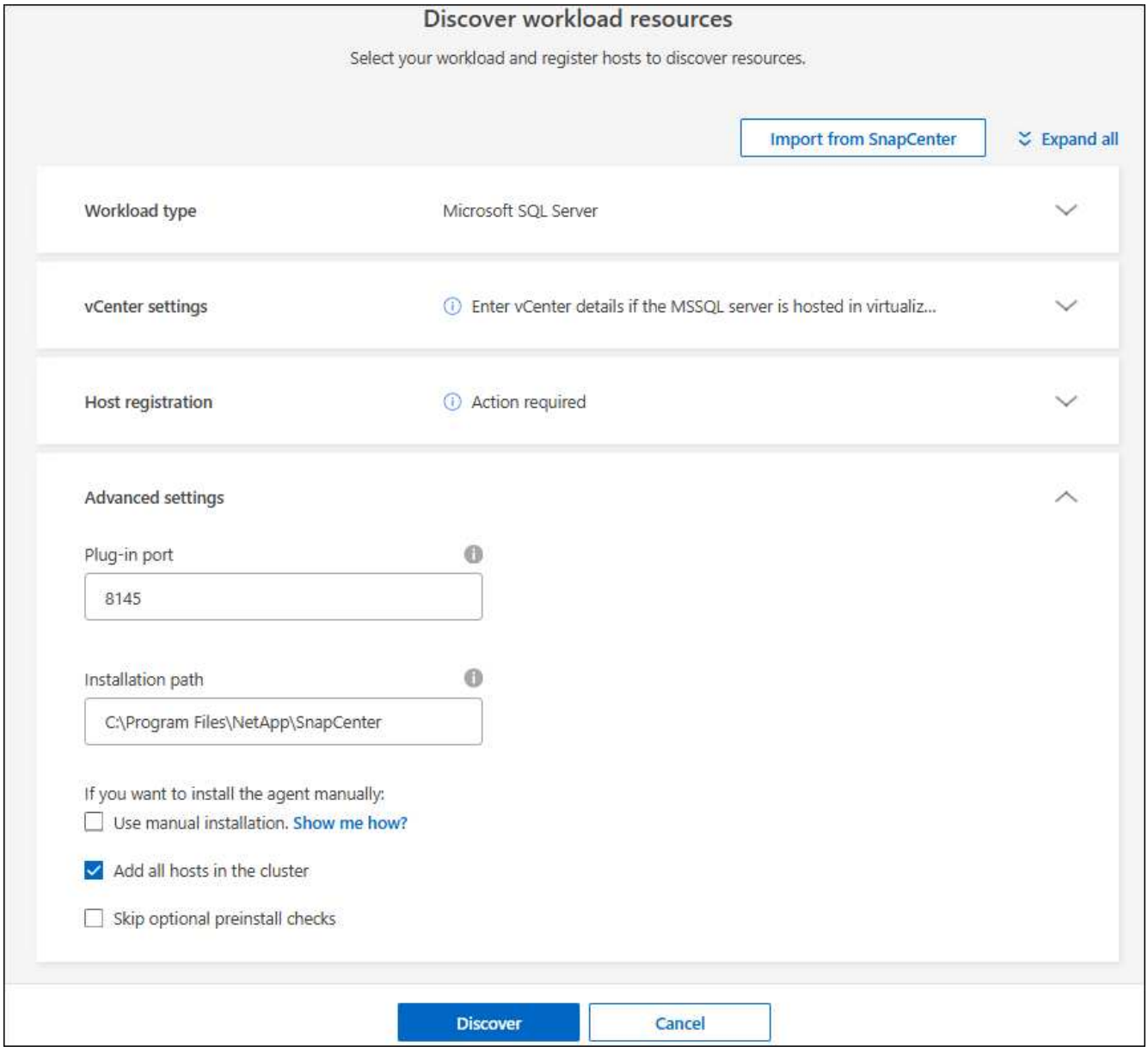
5. Continua con Impostazioni avanzate.

Imposta le opzioni delle impostazioni avanzate durante la scoperta e installa il plug-in

Con le Impostazioni Avanzate, è possibile installare manualmente l'agente del plugin su tutti i server registrati. Ciò consente di importare tutti i carichi di lavoro SnapCenter in BlueXP backup and recovery, in modo da poter gestire backup e ripristini da lì. BlueXP backup and recovery mostra i passaggi necessari per installare il plugin.

Fasi

1. Dalla pagina Scopri risorse, vai alle Impostazioni avanzate cliccando sulla freccia rivolta verso il basso a destra.

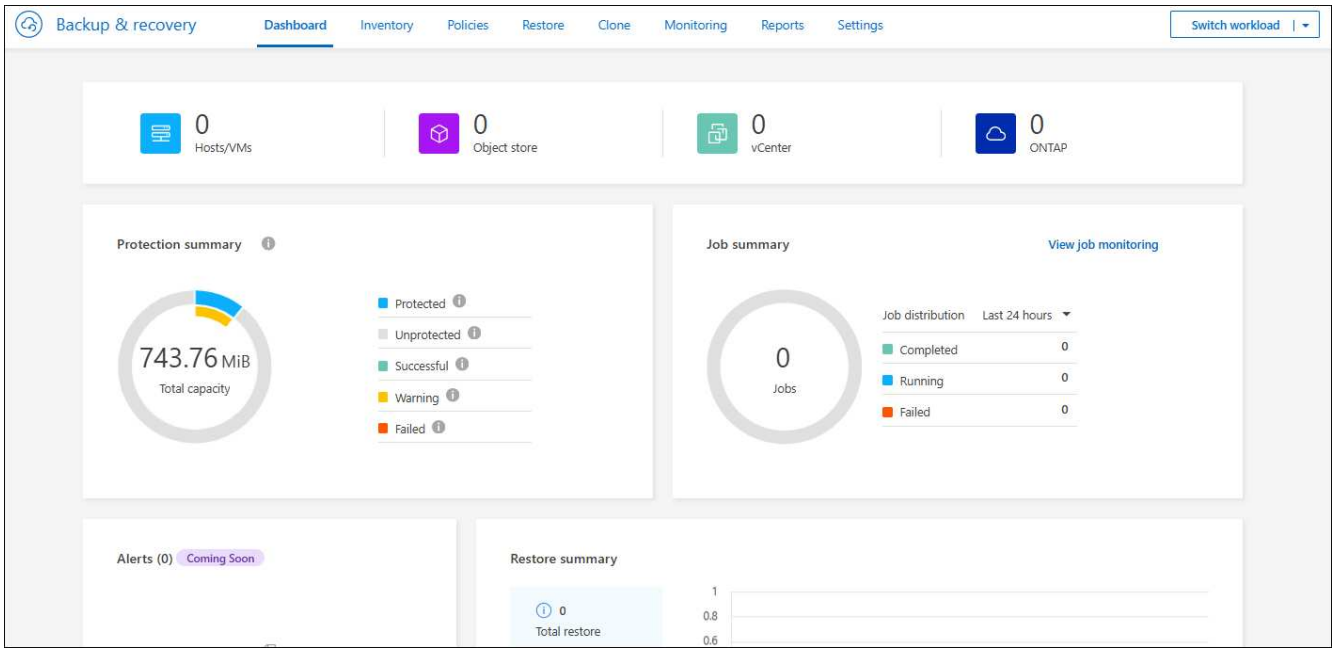


2. Nella pagina Scopri le risorse del carico di lavoro, immetti le seguenti informazioni.
   - **Inserisci il numero di porta del plug-in**: Inserisci il numero di porta utilizzato dal plug-in.
   - **Percorso di installazione**: Inserisci il percorso in cui verrà installato il plugin.

3. Se si desidera installare manualmente l'agente SnapCenter , selezionare le caselle relative alle seguenti opzioni:
   - **Usa installazione manuale**: seleziona questa casella per installare manualmente il plugin.
   - **Aggiungi tutti gli host nel cluster**: seleziona questa casella per aggiungere tutti gli host nel cluster al BlueXP backup and recovery durante l'individuazione.
   - **Salta i controlli pre-installazione facoltativi**: seleziona questa casella per saltare i controlli pre-installazione facoltativi. Potresti volerlo fare, ad esempio, se sai che le considerazioni sulla memoria o sullo spazio cambieranno a breve e desideri installare il plugin ora.
4. Selezionare **Discover**.

Vai alla dashboard BlueXP backup and recovery

1. Per visualizzare la Dashboard BlueXP backup and recovery , dal menu in alto, seleziona **Dashboard**.
2. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai nuovi carichi di lavoro scoperti, protetti e sottoposti a backup.



"Scopri cosa ti mostra la Dashboard".

Esegui il backup dei carichi di lavoro di Microsoft SQL Server con il BlueXP backup and recovery

Esegui il backup dei dati delle applicazioni Microsoft SQL Server dai sistemi ONTAP locali ad Amazon Web Services, Microsoft Azure e StorageGRID per garantire la protezione dei dati. I backup vengono generati e memorizzati automaticamente in un archivio di oggetti nel tuo account di cloud pubblico o privato.

- Per eseguire il backup dei carichi di lavoro in base a una pianificazione, creare criteri che governino le operazioni di backup e ripristino. Vedere "Creare policy" per istruzioni.
- Configurare la directory dei registri per gli host rilevati prima di avviare un backup.

- Esegui subito il backup dei carichi di lavoro (crea subito un backup su richiesta).

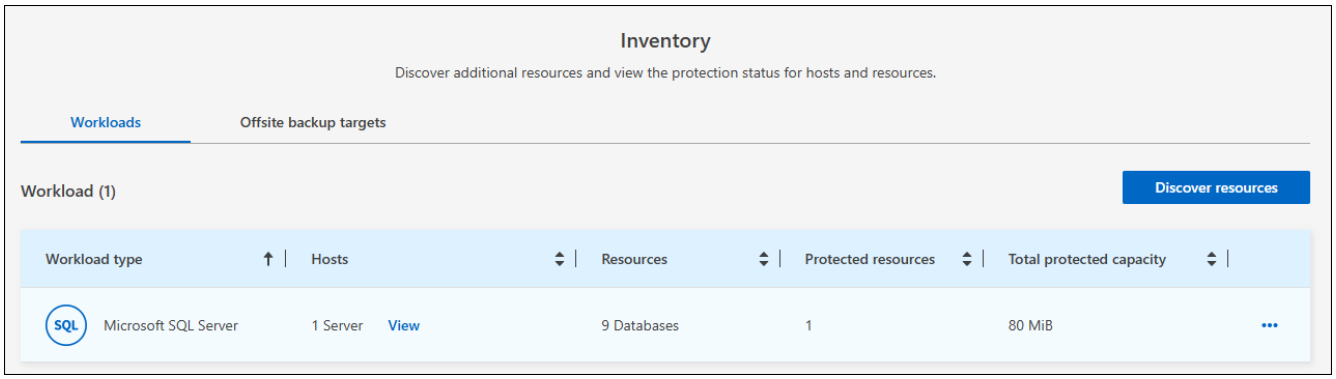
Visualizza lo stato di protezione del carico di lavoro

Prima di avviare un backup, visualizza lo stato di protezione dei tuoi carichi di lavoro.

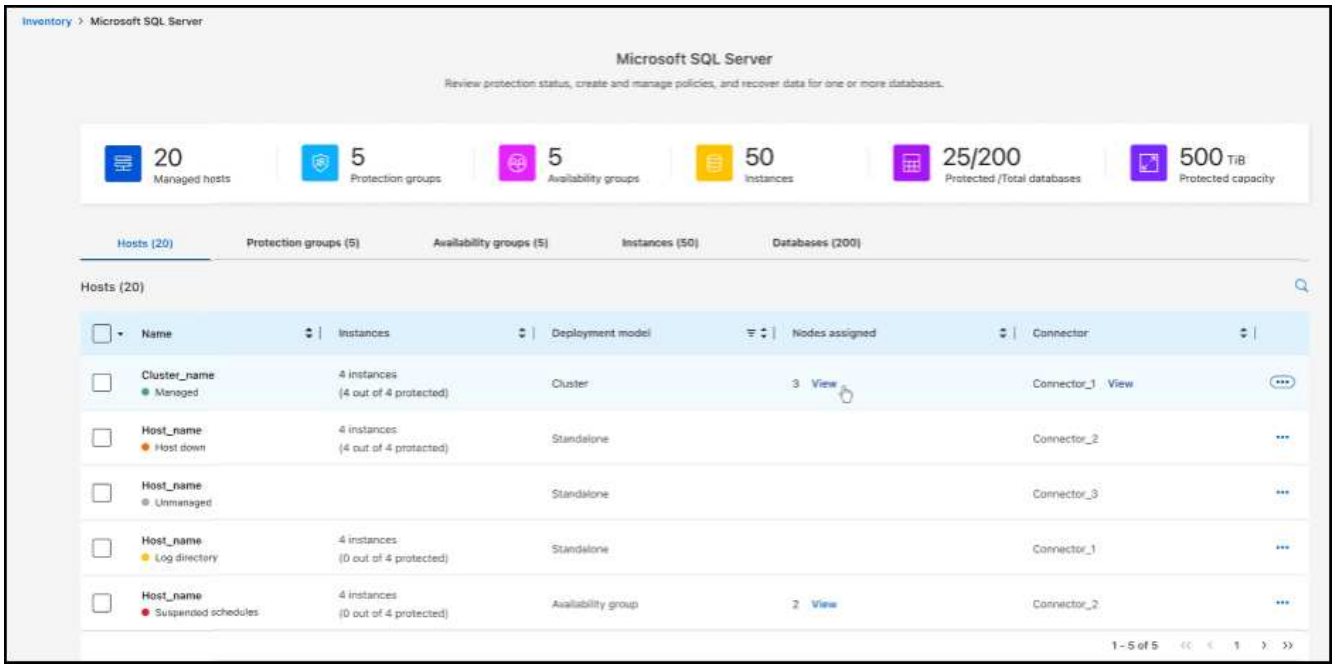
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di Backup e ripristino, Amministratore di backup di Backup e ripristino, Amministratore di ripristino di Backup e ripristino, Amministratore di clonazione di Backup e ripristino o Ruolo di visualizzatore di Backup e ripristino. Scopri di più su "Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.



4. Esaminare i dettagli nelle schede Host, Gruppi di protezione, Gruppi di disponibilità, Istanze e Database.

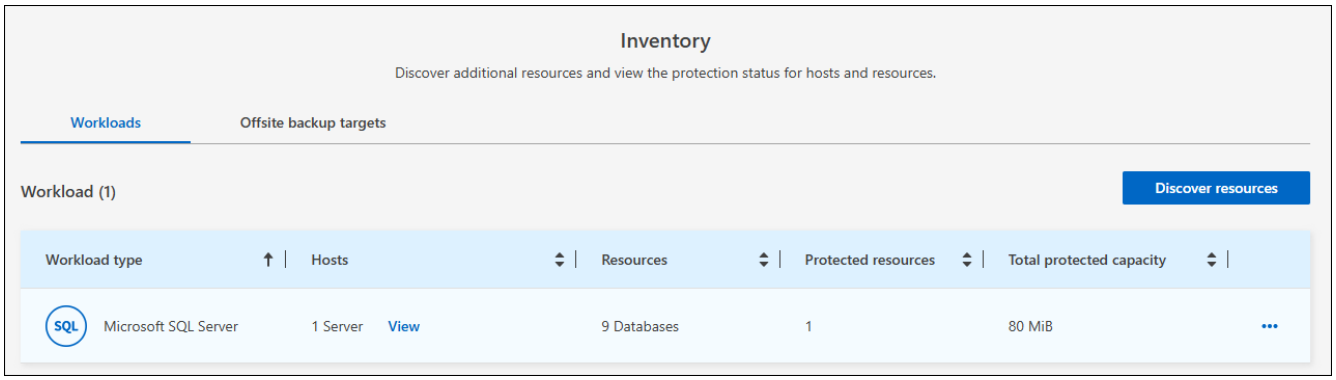
Configurare la directory dei registri per gli host rilevati

Prima di eseguire il backup dei carichi di lavoro, imposta il percorso per i log delle attività per gli host rilevati. Questo ti aiuterà a monitorare lo stato delle operazioni.

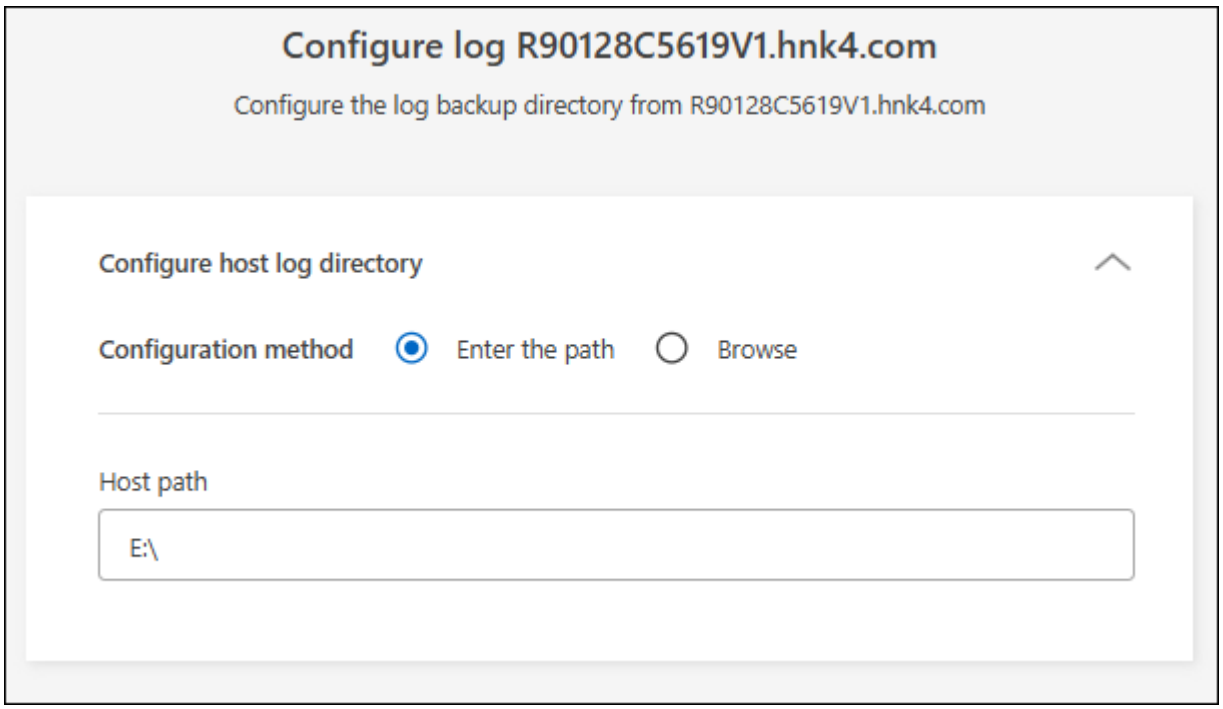
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di Backup e ripristino, amministratore di backup di Backup e ripristino o amministratore di ripristino di Backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare un host.
5. Seleziona l'icona Azioni ••• > **Configura directory registro**.



6. Specificare il percorso host o sfogliare un elenco di host o nodi host sull'host per individuare dove si desidera archiviare il registro host.

7. Selezionare quelli su cui si desidera memorizzare i registri.

> I campi visualizzati variano a seconda del modello di distribuzione selezionato, ad esempio istanza del cluster di failover o autonoma.

8. Selezionare **Salva**.

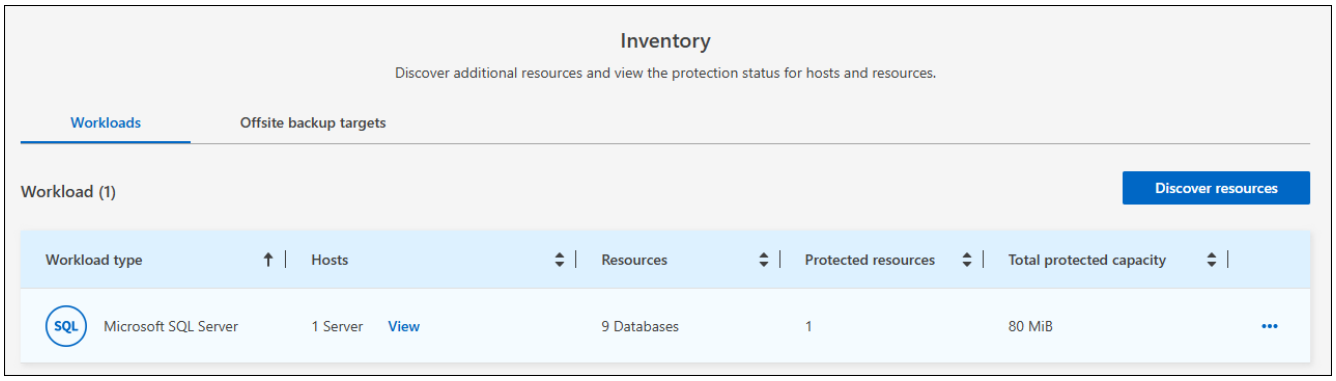
Crea un gruppo di protezione

È possibile creare un gruppo di protezione per gestire le operazioni di backup e ripristino per un set di carichi di lavoro. Un gruppo di protezione è un raggruppamento logico di carichi di lavoro che si desidera proteggere insieme.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Specificare un nome per il gruppo di protezione.
7. Selezionare le istanze o i database che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.
9. Selezionare il **Criterio di backup** che si desidera applicare al gruppo di protezione.

   Se si desidera creare una policy, selezionare **Crea nuova policy** e seguire le istruzioni per creare una policy. Per ulteriori informazioni, vedere "Creare policy" .

10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

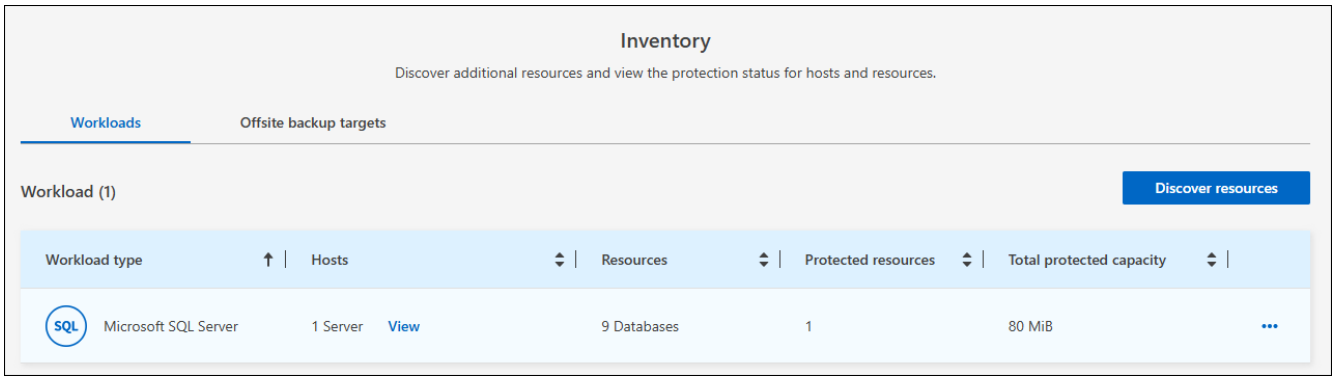
Esegui subito il backup dei carichi di lavoro con un backup on-demand

Crea immediatamente un backup on-demand. Potresti voler eseguire un backup on-demand se stai per apportare modifiche al tuo sistema e vuoi assicurarti di avere un backup prima di iniziare.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu, seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppo di protezione**, **Istanze** o **Database**.
5. Seleziona l'istanza o il database di cui vuoi eseguire il backup.
6. Seleziona l'icona Azioni ••• > **Esegui il backup adesso**.
7. Selezionare il criterio che si desidera applicare al backup.
8. Selezionare il livello di pianificazione.
9. Seleziona **Esegui backup adesso**.

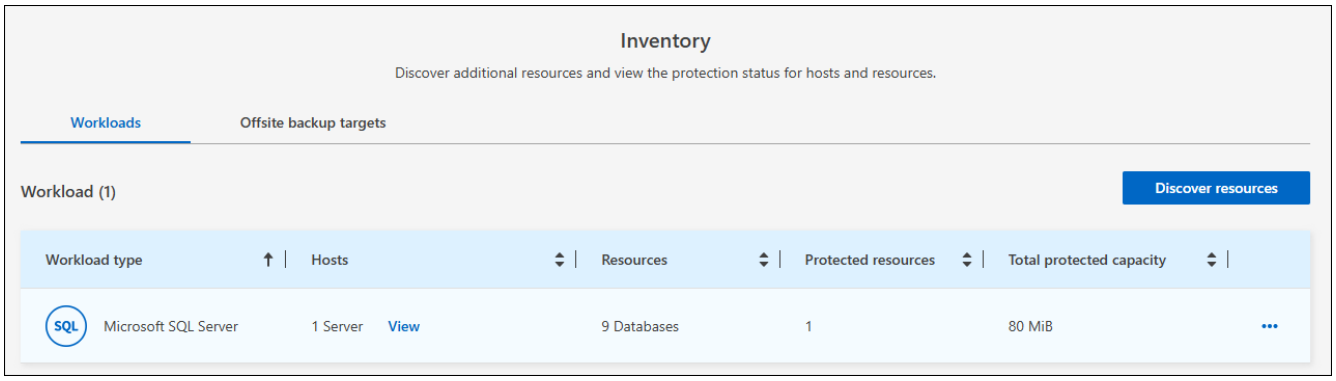
Sospendi la pianificazione del backup

La sospensione della pianificazione impedisce temporaneamente l'esecuzione del backup all'orario pianificato. Potrebbe essere necessario farlo se si sta eseguendo la manutenzione del sistema o se si verificano problemi con il backup.

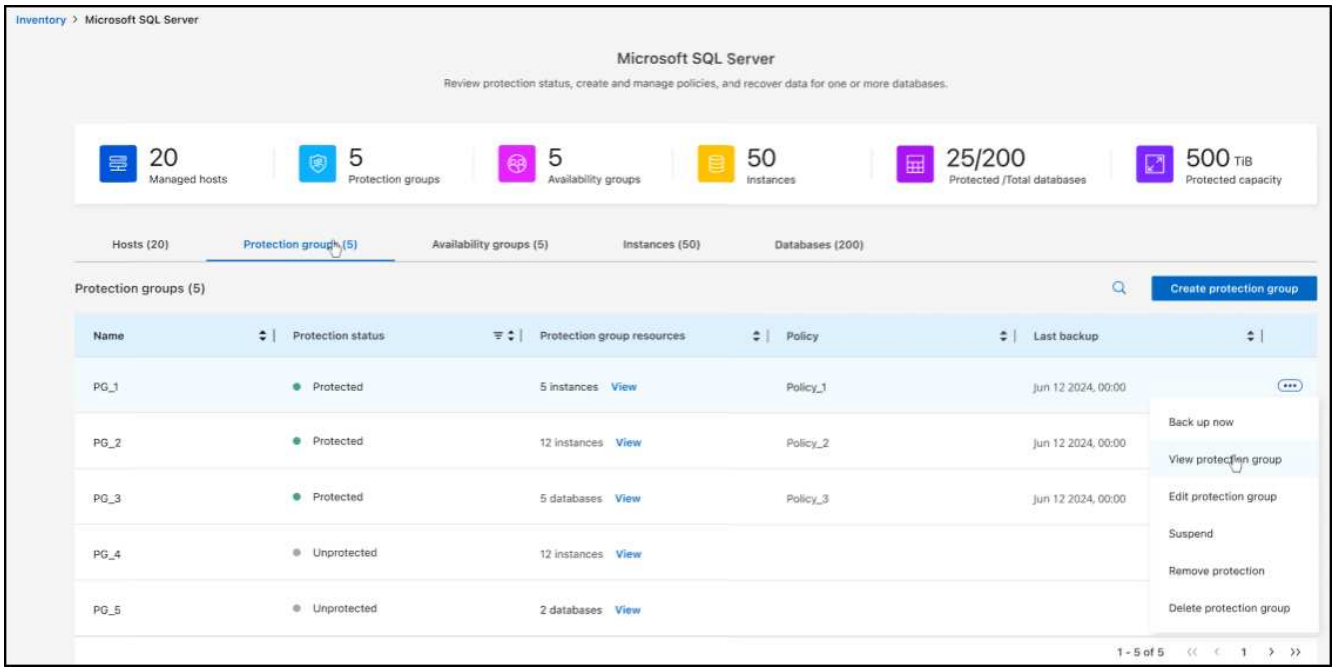
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di Backup e ripristino, amministratore di backup di Backup e ripristino, amministratore di ripristino di Backup e ripristino o amministratore di clonazione di Backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppo di protezione**, **Istanze** o **Database**.
5. Selezionare il gruppo di protezione, l'istanza o il database che si desidera sospendere.



6. Seleziona l'icona Azioni ••• > **Sospendi**.

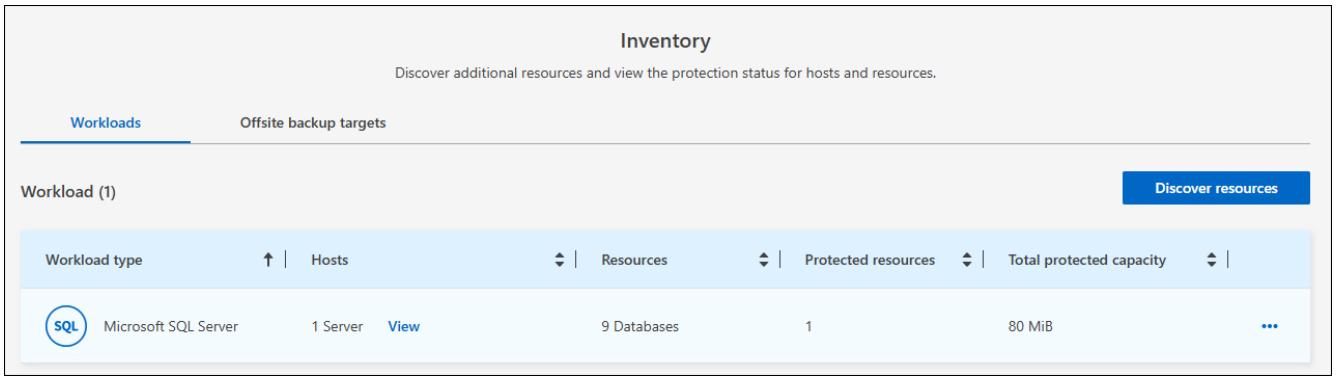
Elimina un gruppo di protezione

È possibile creare un gruppo di protezione per gestire le operazioni di backup e ripristino per un set di carichi di lavoro. Un gruppo di protezione è un raggruppamento logico di carichi di lavoro che si desidera proteggere insieme.

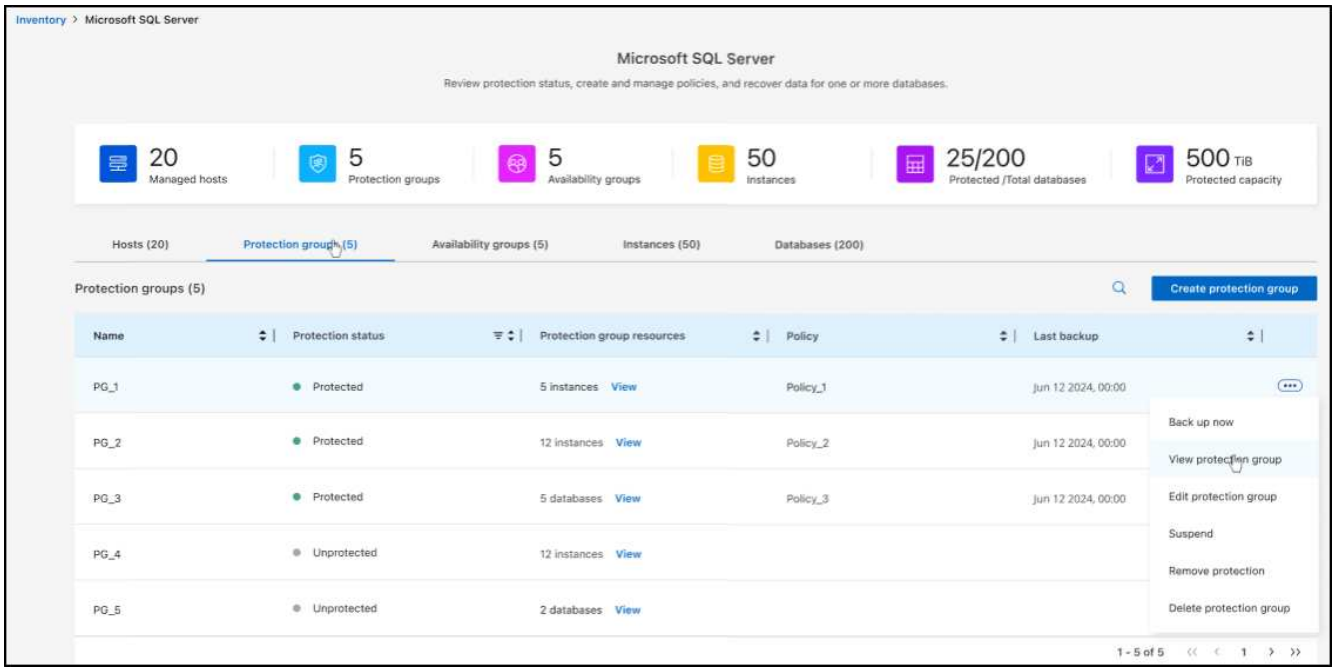
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Seleziona l'icona Azioni ••• > **Elimina gruppo di protezione**.



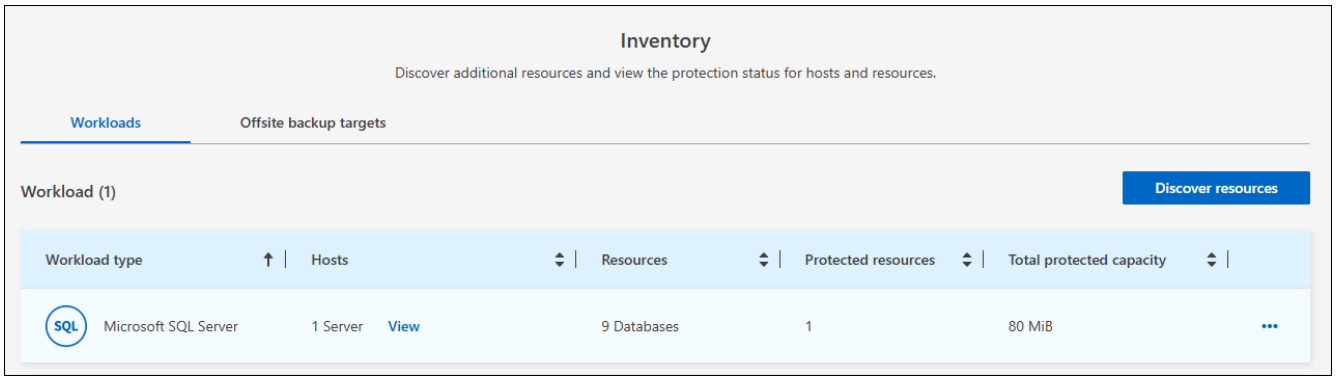
Rimuovere la protezione da un carico di lavoro

È possibile rimuovere la protezione da un carico di lavoro se non si desidera più eseguirne il backup o se si desidera interromperne la gestione nel BlueXP backup and recovery.

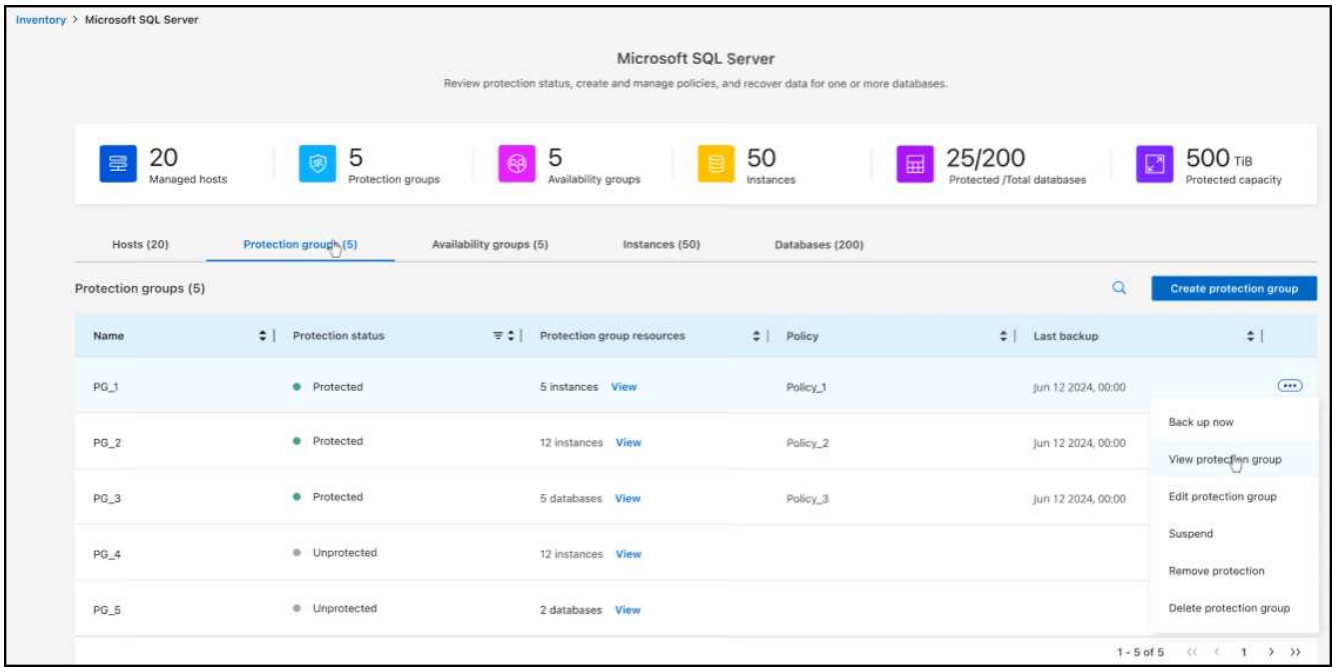
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppo di protezione**, **Istanze** o **Database**.
5. Selezionare il gruppo di protezione, l'istanza o il database.



6. Seleziona l'icona Azioni ••• > **Rimuovi protezione**.
7. Nella finestra di dialogo Rimuovi protezione, seleziona se desideri conservare i backup e i metadati oppure eliminarli.
8. Selezionare **Rimuovi** per confermare l'azione.

Ripristina i carichi di lavoro di Microsoft SQL Server con il BlueXP backup and recovery

Ripristina i carichi di lavoro di Microsoft SQL Server da copie snapshot, da un backup del carico di lavoro replicato su storage secondario o da backup archiviati in storage a oggetti utilizzando il BlueXP backup and recovery. Puoi ripristinare un carico di lavoro nell'ambiente di lavoro originale, in un ambiente di lavoro diverso che utilizza lo stesso account cloud o in un sistema ONTAP locale.

Ripristina da queste posizioni

È possibile ripristinare i carichi di lavoro da diverse posizioni di partenza:

- Ripristina da una posizione primaria
- Ripristina da una risorsa replicata
- Ripristina da un backup dell'archivio oggetti

Ripristinare questi punti

È possibile ripristinare i dati all'ultimo snapshot o a questi punti:

- Ripristina da snapshot
- Ripristina fino a un punto specifico nel tempo. Questo è utile se si conoscono il nome e la posizione del file, nonché la data dell'ultima volta in cui era in buone condizioni.
- Ripristina l'ultimo backup

Considerazioni sul ripristino da storage di oggetti

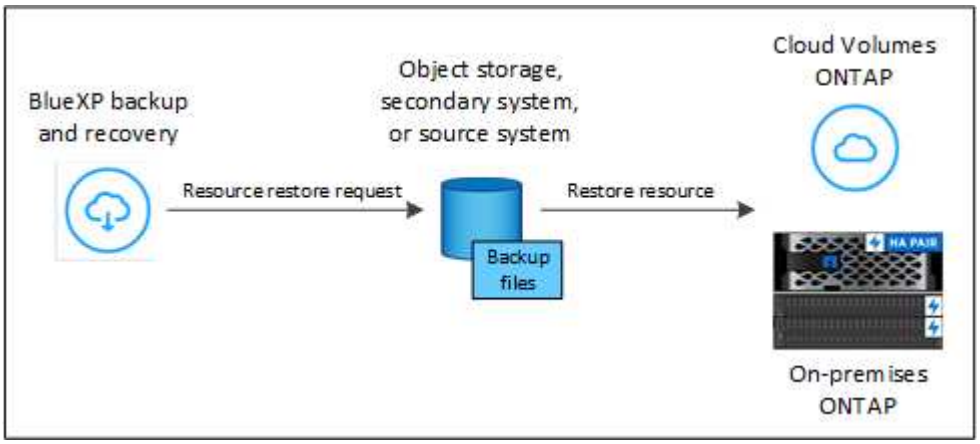
Se selezioni un file di backup nell'archivio oggetti e la protezione ransomware è attiva per quel backup (se hai abilitato DataLock e la protezione ransomware nella policy di backup), ti verrà richiesto di eseguire un ulteriore controllo di integrità sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione.

Per accedere al contenuto del file di backup, ti verranno addebitati costi di uscita aggiuntivi dal tuo provider cloud.

Come funziona il ripristino dei carichi di lavoro

Quando si ripristinano i carichi di lavoro, si verifica quanto segue:

- Quando si ripristina un carico di lavoro da un file di backup, BlueXP backup and recovery crea una *nuova* risorsa utilizzando i dati del backup.
- Quando si esegue il ripristino da un carico di lavoro replicato, è possibile ripristinare il carico di lavoro nell'ambiente di lavoro originale o in un sistema ONTAP locale.



- Quando si ripristina un backup da un archivio di oggetti, è possibile ripristinare i dati nell'ambiente di lavoro originale o in un sistema ONTAP locale.

Metodi di ripristino

È possibile ripristinare i carichi di lavoro utilizzando uno dei seguenti metodi. In genere, è consigliabile scegliere uno dei seguenti metodi in base alle proprie esigenze di ripristino:

- **Dalla pagina Ripristina**: usa questa opzione quando devi ripristinare una risorsa, ma non ricordi il nome esatto, la posizione in cui si trova o la data dell'ultima volta in cui era in buone condizioni. Puoi cercare lo snapshot utilizzando i filtri.
- **Dalla pagina Inventario**: Usalo quando devi ripristinare una risorsa specifica dell'ultima settimana o mese, di cui conosci il nome, la posizione e la data dell'ultima volta in cui era in buone condizioni. Puoi scorrere un elenco di risorse per trovare quella che desideri ripristinare.

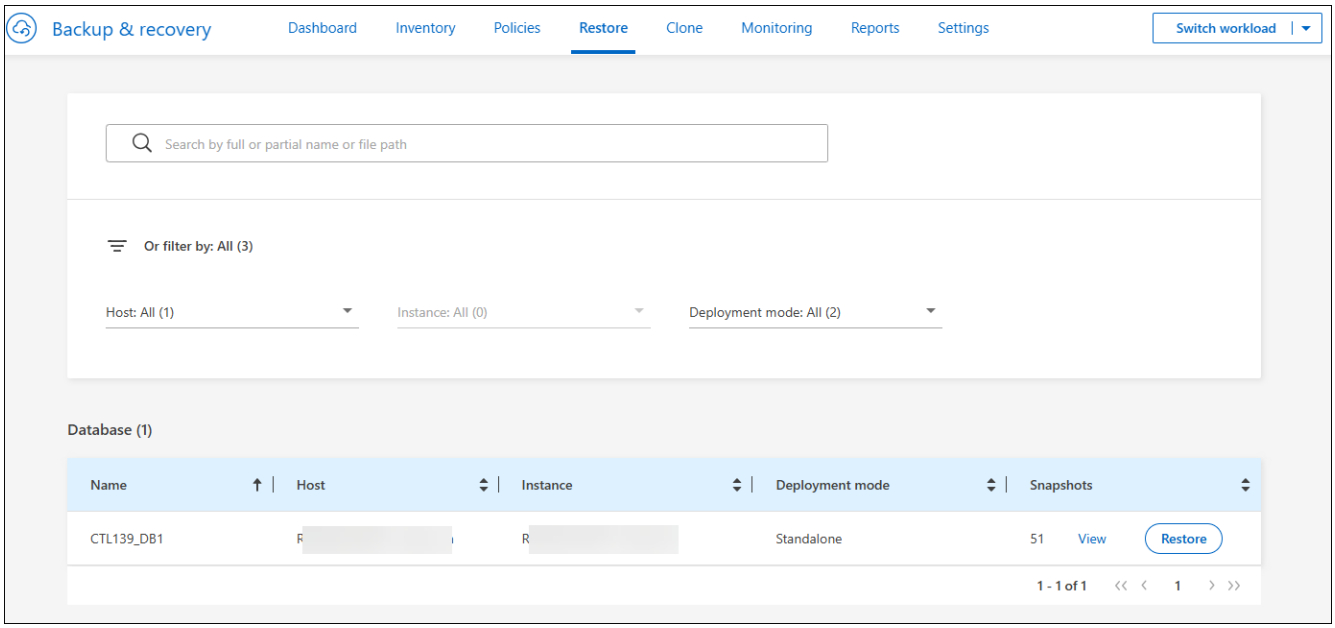
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Amministratore di ripristino di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Ripristina i dati del carico di lavoro dall'opzione Ripristina

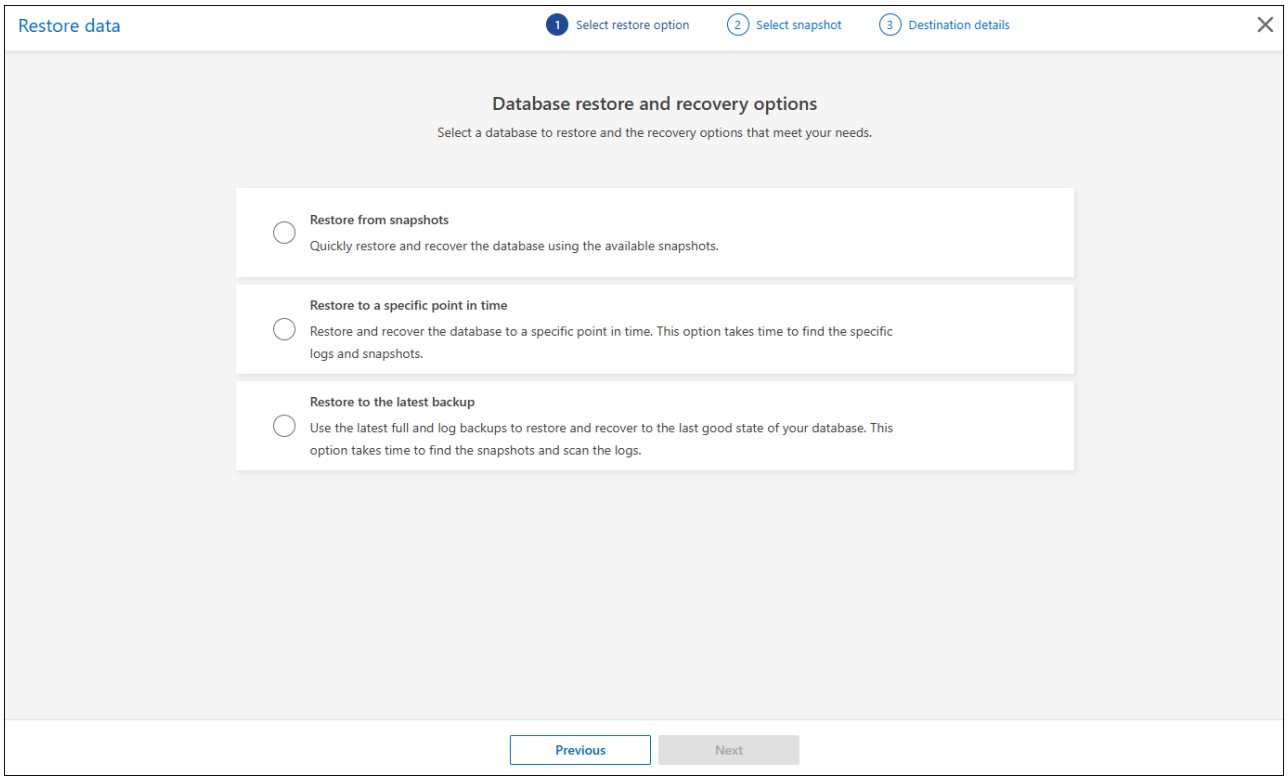
Ripristinare i carichi di lavoro del database utilizzando l'opzione Ripristina.

Fasi

1. Dal menu di backup e ripristino BlueXP , seleziona **Ripristina**.



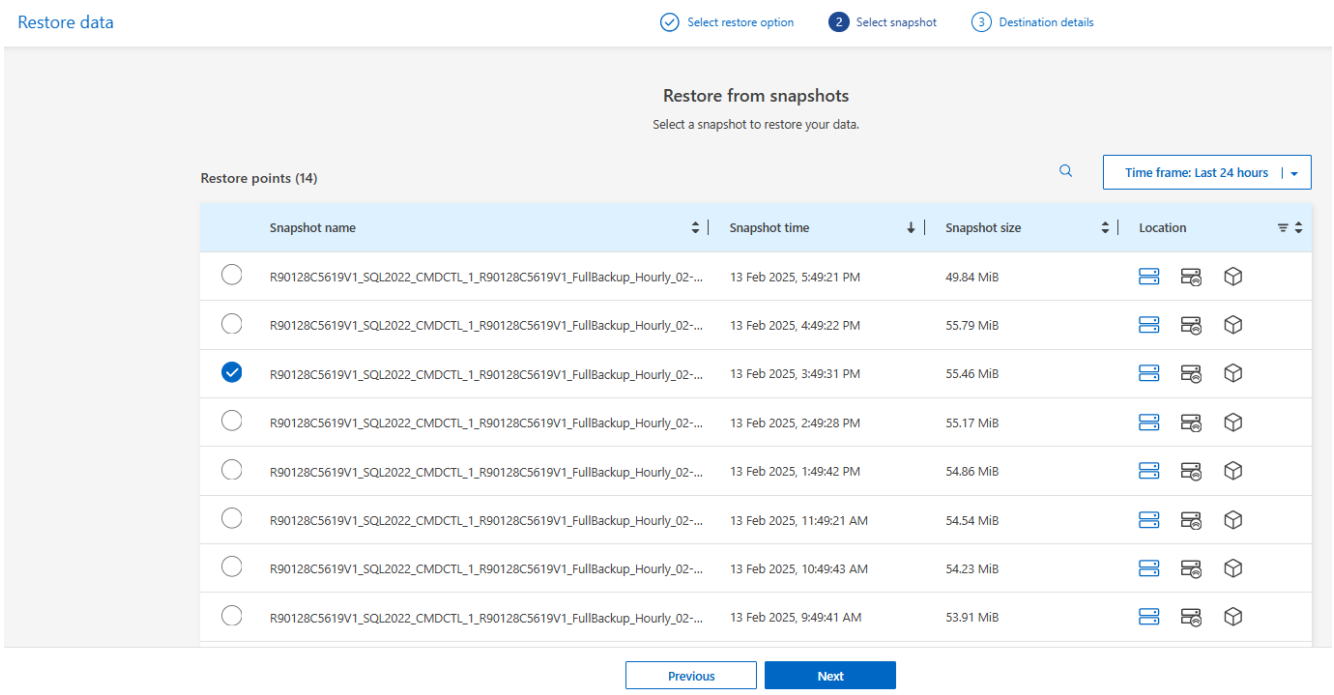
2. Seleziona il database che desideri ripristinare. Utilizza i filtri per la ricerca.
3. Selezionare l'opzione di ripristino:
   - Ripristina da snapshot
   - Ripristina fino a un punto specifico nel tempo. Questo è utile se si conoscono il nome e la posizione del file, nonché la data dell'ultima volta in cui era in buone condizioni.
   - Ripristina l'ultimo backup



Ripristinare i carichi di lavoro dagli snapshot

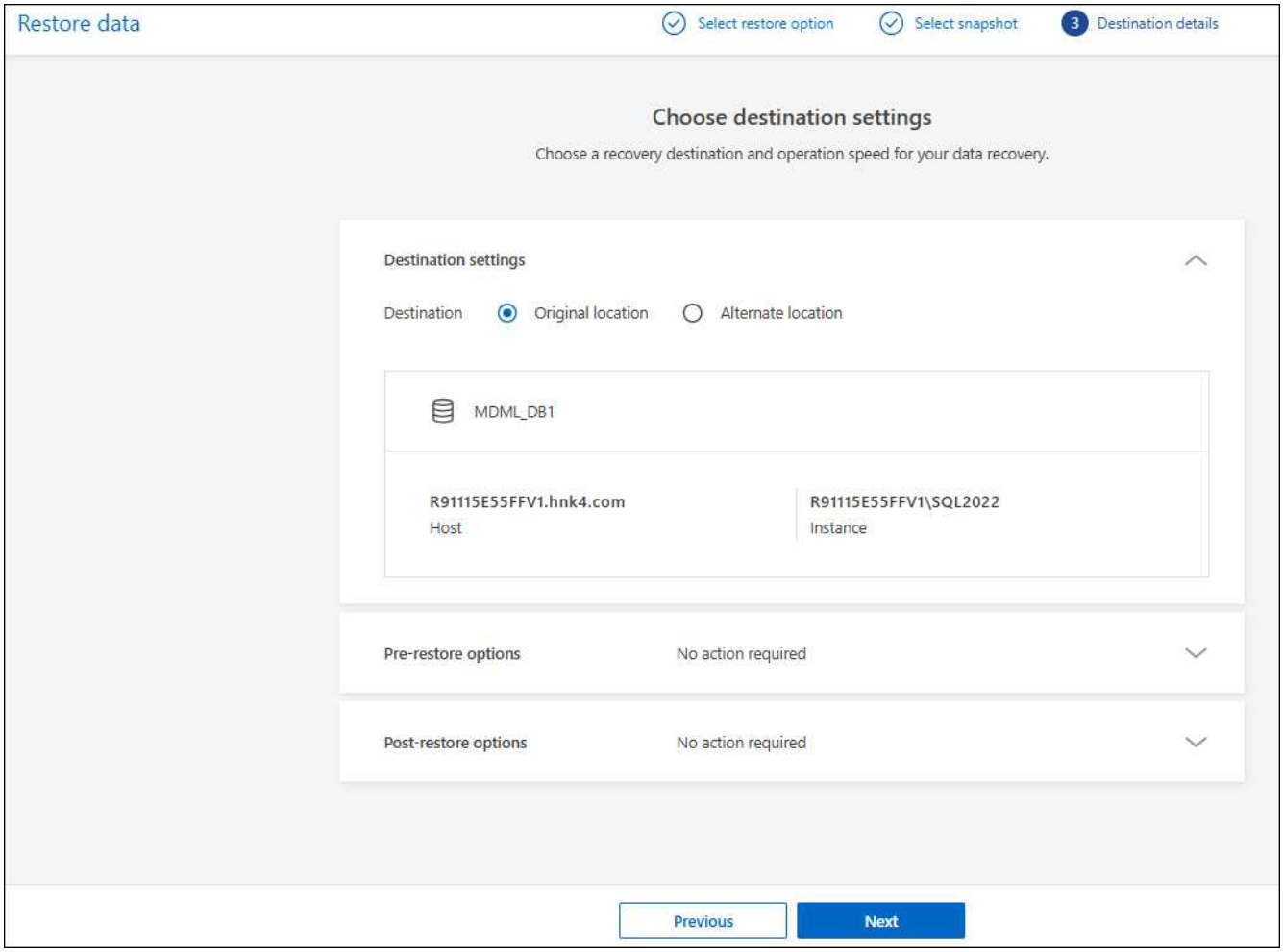
1. Proseguendo dalla pagina Opzioni di ripristino, seleziona **Ripristina da snapshot**.

   Viene visualizzato un elenco di istantanee.



2. Selezionare lo snapshot che si desidera ripristinare.
3. Selezionare **Avanti**.

Successivamente vedrai le opzioni di destinazione.



4. Nella pagina Dettagli destinazione, inserisci le seguenti informazioni:
   - **Impostazioni di destinazione**: scegli se desideri ripristinare i dati nella posizione originale o in una posizione alternativa. Per una posizione alternativa, seleziona il nome host e l'istanza, inserisci il nome del database e il percorso di destinazione in cui desideri ripristinare lo snapshot.
   - **Opzioni pre-ripristino**:
     - **Sovrascrivi il database con lo stesso nome durante il ripristino**: durante il ripristino, il nome originale del database viene mantenuto.
     - **Mantieni impostazioni di replicazione del database SQL**: conserva le impostazioni di replicazione per il database SQL dopo l'operazione di ripristino.
     - **Crea backup del registro delle transazioni prima del ripristino**: Crea un backup del registro delle transazioni prima dell'operazione di ripristino.*** Esci dal ripristino se il backup del registro delle transazioni prima del ripristino fallisce**: Interrompe l'operazione di ripristino se il backup del registro delle transazioni non riesce.
     - **Prescript**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino, tutti gli argomenti richiesti dallo script e il tempo di attesa per il completamento dello script.
   - **Opzioni post-ripristino**:
     - **Operativo**, ma non disponibile per il ripristino di ulteriori log delle transazioni. Questo ripristina il database online dopo l'applicazione dei backup dei log delle transazioni.

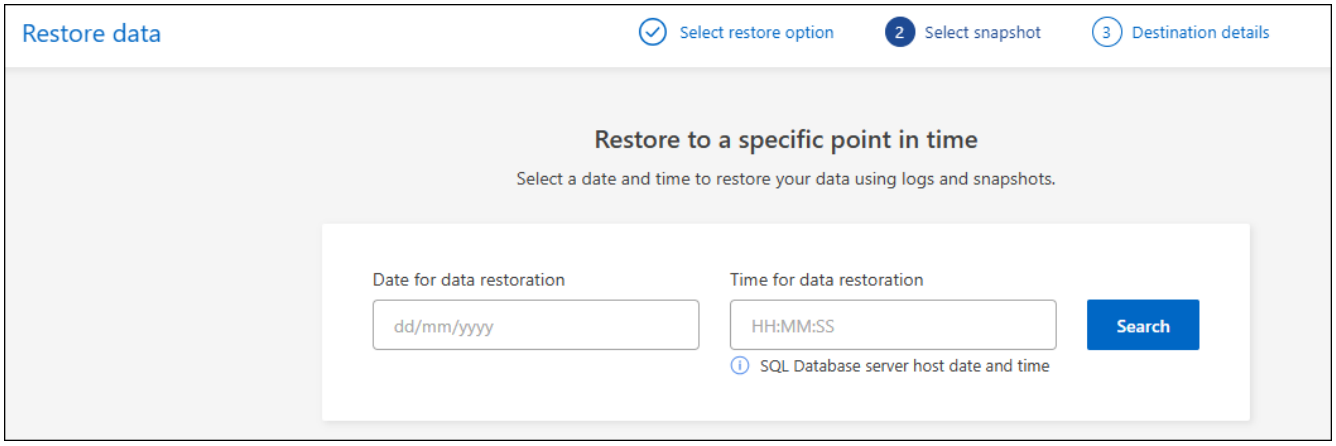
- **Non operativo**, ma disponibile per il ripristino di ulteriori log delle transazioni. Mantiene il database in uno stato non operativo dopo l'operazione di ripristino durante il ripristino dei backup dei log delle transazioni. Questa opzione è utile per il ripristino di ulteriori log delle transazioni.
- **Modalità di sola lettura** disponibile per il ripristino di ulteriori log delle transazioni. Ripristina il database in modalità di sola lettura e applica i backup dei log delle transazioni.
- **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.

5. Selezionare **Restore** (Ripristina).

Ripristinare un punto specifico nel tempo

Il BlueXP backup and recovery utilizzano i registri e gli snapshot più recenti per creare un ripristino puntuale dei dati.

1. Proseguendo dalla pagina Opzioni di ripristino, seleziona **Ripristina in un momento specifico**.
2. Selezionare **Avanti**.



3. Nella pagina Ripristina a un punto specifico nel tempo, immetti le seguenti informazioni:
   - **Data e ora del ripristino dei dati**: Inserisci la data e l'ora esatte dei dati che desideri ripristinare. Questa data e ora provengono dall'host del database Microsoft SQL Server.
4. Selezionare **Cerca**.
5. Seleziona lo snapshot che vuoi ripristinare.
6. Selezionare **Avanti**.
7. Nella pagina Dettagli destinazione, inserisci le seguenti informazioni:
   - **Impostazioni di destinazione**: scegli se desideri ripristinare i dati nella posizione originale o in una posizione alternativa. Per una posizione alternativa, seleziona il nome host e l'istanza, inserisci il nome del database e il percorso di destinazione.
   - **Opzioni pre-ripristino**:
     - **Mantieni il nome originale del database**: durante il ripristino, il nome originale del database viene mantenuto.
     - **Mantieni impostazioni di replicazione del database SQL**: conserva le impostazioni di replicazione per il database SQL dopo l'operazione di ripristino.
     - **Prescript**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino, tutti gli argomenti richiesti dallo script e il tempo di attesa per il

completamento dello script.

- **Opzioni post-ripristino**:
  - **Operativo**, ma non disponibile per il ripristino di ulteriori log delle transazioni. Questo ripristina il database online dopo l'applicazione dei backup dei log delle transazioni.
  - **Non operativo**, ma disponibile per il ripristino di ulteriori log delle transazioni. Mantiene il database in uno stato non operativo dopo l'operazione di ripristino durante il ripristino dei backup dei log delle transazioni. Questa opzione è utile per il ripristino di ulteriori log delle transazioni.
  - **Modalità di sola lettura** disponibile per il ripristino di ulteriori log delle transazioni. Ripristina il database in modalità di sola lettura e applica i backup dei log delle transazioni.
  - **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.

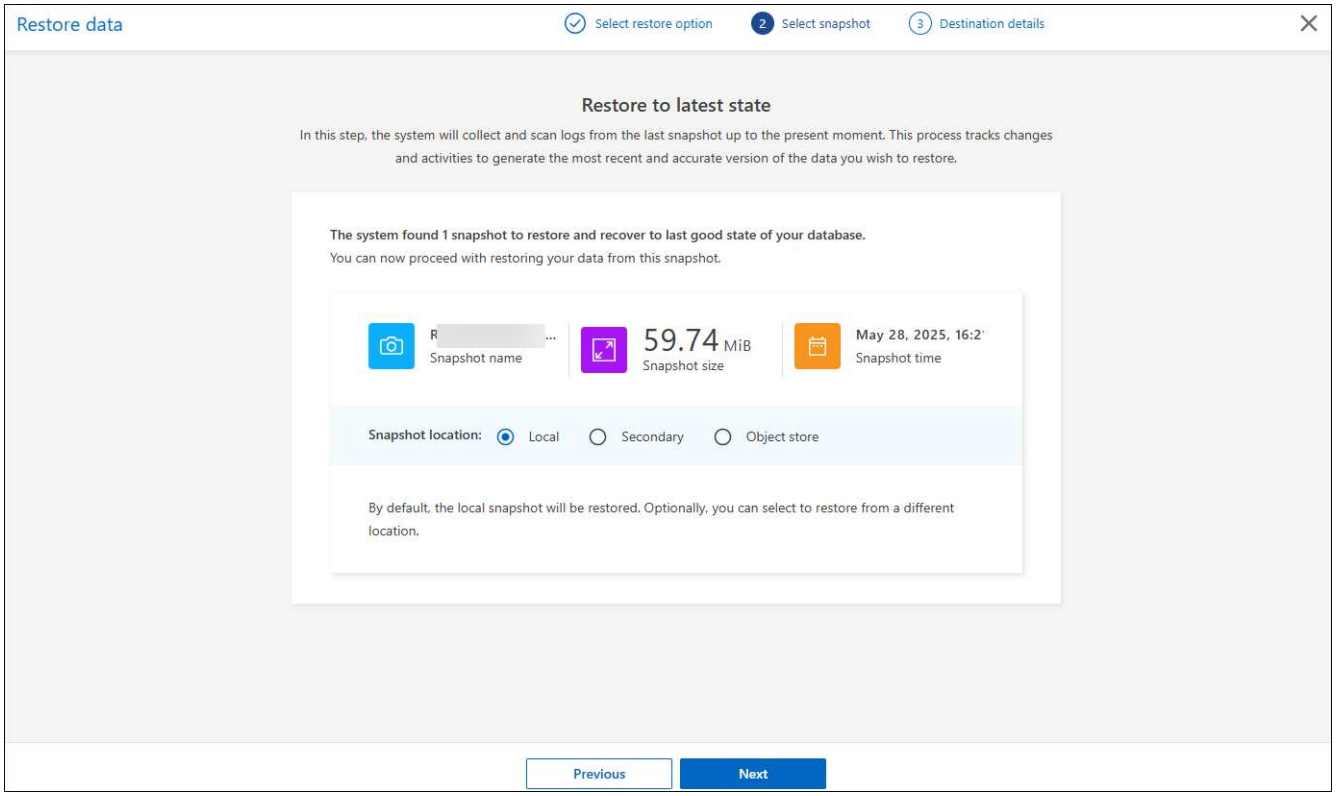
8. Selezionare **Restore** (Ripristina).

Ripristina l'ultimo backup

Questa opzione utilizza i backup completi e di registro più recenti per ripristinare i dati all'ultimo stato funzionante. Il sistema analizza i registri dall'ultimo snapshot fino a oggi. Il processo tiene traccia delle modifiche e delle attività per ripristinare la versione più recente e accurata dei dati.

1. Proseguendo dalla pagina Opzioni di ripristino, seleziona **Ripristina all'ultimo backup**.

   BlueXP backup and recovery mostra gli snapshot disponibili per l'operazione di ripristino.



2. Nella pagina Ripristina allo stato più recente, seleziona la posizione dello snapshot dell'archiviazione locale, secondaria o dell'archiviazione degli oggetti.
3. Selezionare **Avanti**.
4. Nella pagina Dettagli destinazione, inserisci le seguenti informazioni:

- **Impostazioni di destinazione**: scegli se desideri ripristinare i dati nella posizione originale o in una posizione alternativa. Per una posizione alternativa, seleziona il nome host e l'istanza, inserisci il nome del database e il percorso di destinazione.
- **Opzioni pre-ripristino**:
  - **Sovrascrivi il database con lo stesso nome durante il ripristino**: durante il ripristino, il nome originale del database viene mantenuto.
  - **Mantieni impostazioni di replicazione del database SQL**: conserva le impostazioni di replicazione per il database SQL dopo l'operazione di ripristino.
  - **Crea backup del registro delle transazioni prima del ripristino**: crea un backup del registro delle transazioni prima dell'operazione di ripristino.
  - **Esci dal ripristino se il backup del registro delle transazioni prima del ripristino fallisce**: interrompe l'operazione di ripristino se il backup del registro delle transazioni fallisce.
  - **Prescript**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino, tutti gli argomenti richiesti dallo script e il tempo di attesa per il completamento dello script.
- **Opzioni post-ripristino**:
  - **Operativo**, ma non disponibile per il ripristino di ulteriori log delle transazioni. Questo ripristina il database online dopo l'applicazione dei backup dei log delle transazioni.
  - **Non operativo**, ma disponibile per il ripristino di ulteriori log delle transazioni. Mantiene il database in uno stato non operativo dopo l'operazione di ripristino durante il ripristino dei backup dei log delle transazioni. Questa opzione è utile per il ripristino di ulteriori log delle transazioni.
  - **Modalità di sola lettura** disponibile per il ripristino di ulteriori log delle transazioni. Ripristina il database in modalità di sola lettura e applica i backup dei log delle transazioni.
  - **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.

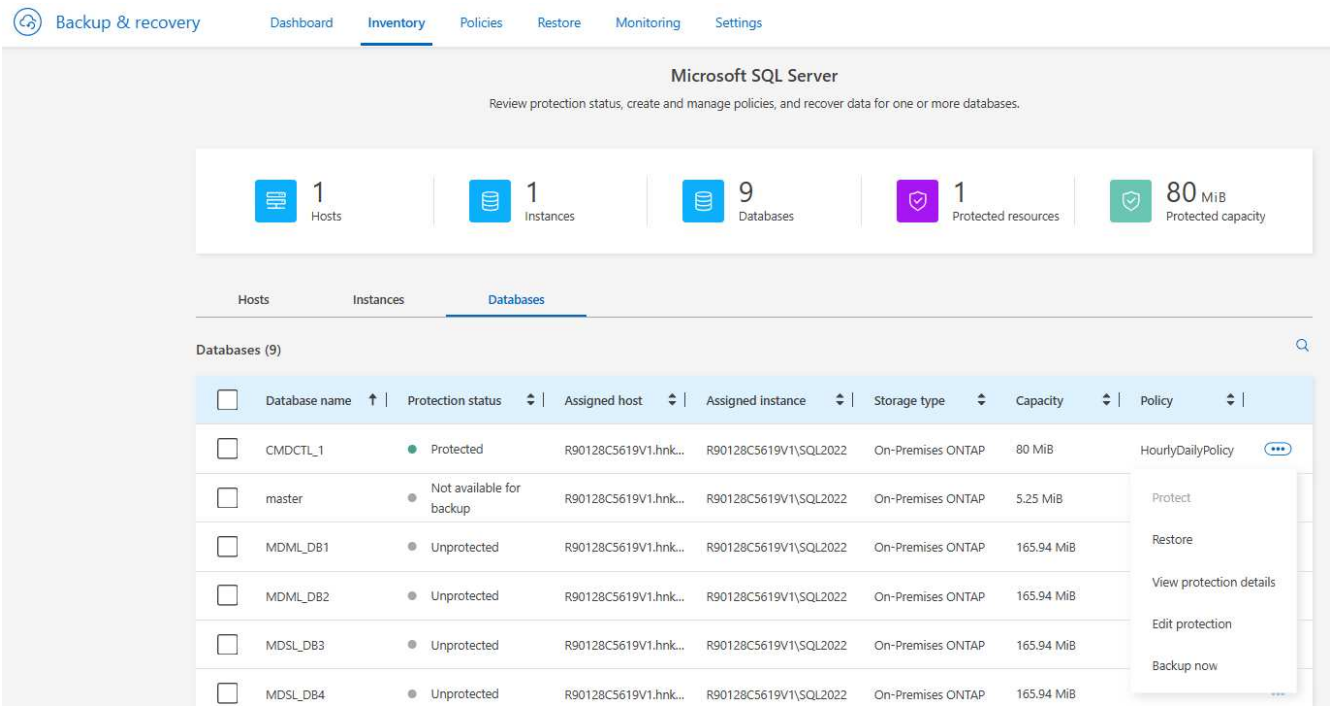
5. Selezionare **Restore** (Ripristina).

Ripristina i dati del carico di lavoro dall'opzione Inventario

Ripristina i carichi di lavoro del database dalla pagina Inventario. Utilizzando l'opzione Inventario, è possibile ripristinare solo i database, non le istanze.

Fasi

1. Dal menu di backup e ripristino BlueXP , seleziona **Inventario**.
2. Seleziona l'host in cui si trova la risorsa che desideri ripristinare.
3. Seleziona **Azioni** ••• icona e seleziona **Visualizza dettagli**.
4. Nella pagina Microsoft SQL Server, selezionare la scheda **Database**.
5. Nella scheda Database, seleziona il database che mostra lo stato "Protetto", a indicare che è presente un backup che puoi ripristinare.

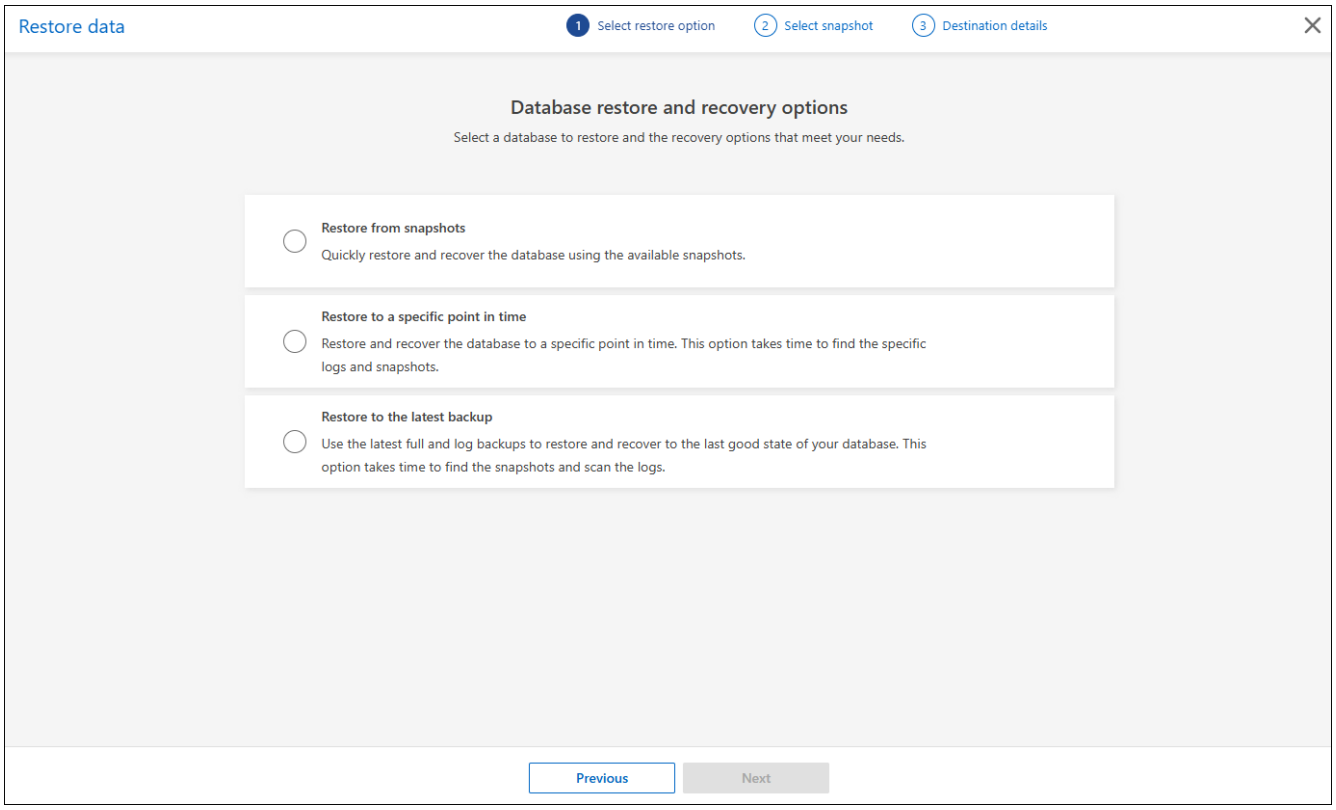


6. Seleziona **Azioni** ••• icona e seleziona **Ripristina**.

   Vengono visualizzate le stesse tre opzioni presenti quando si esegue il ripristino dalla pagina Ripristina:

   - Ripristina da snapshot
   - Ripristinare un punto specifico nel tempo
   - Ripristina l'ultimo backup

7. Continuare con gli stessi passaggi per l'opzione di ripristino dalla pagina Ripristina



Clona i carichi di lavoro di Microsoft SQL Server con BlueXP backup and recovery

Clona i dati delle applicazioni Microsoft SQL Server sulla stessa macchina virtuale o su una diversa per scopi di sviluppo, test o protezione utilizzando il BlueXP backup and recovery. Puoi creare cloni da snapshot istantanei o snapshot esistenti dei tuoi carichi di lavoro Microsoft SQL Server.

Scegli tra i seguenti tipi di cloni:

- **Snapshot e clone istantanei**: puoi creare un clone dei tuoi carichi di lavoro Microsoft SQL Server da uno snapshot istantaneo. Uno snapshot istantaneo è una copia puntuale dei dati di origine creata da un backup. Il clone viene archiviato in un archivio oggetti nel tuo account cloud pubblico o privato. Puoi utilizzare il clone per ripristinare i tuoi carichi di lavoro in caso di perdita o danneggiamento dei dati.
- **Clona da uno snapshot esistente**: puoi scegliere uno snapshot esistente da un elenco di snapshot disponibili per il carico di lavoro. Questa opzione è utile se desideri creare un clone da un momento specifico. Puoi clonare su storage primario o secondario.

È possibile raggiungere i seguenti obiettivi di protezione:

- Crea un clone
- Aggiornare un clone
- Separare un clone
- Elimina un clone

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di Backup e ripristino o amministratore clone di Backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

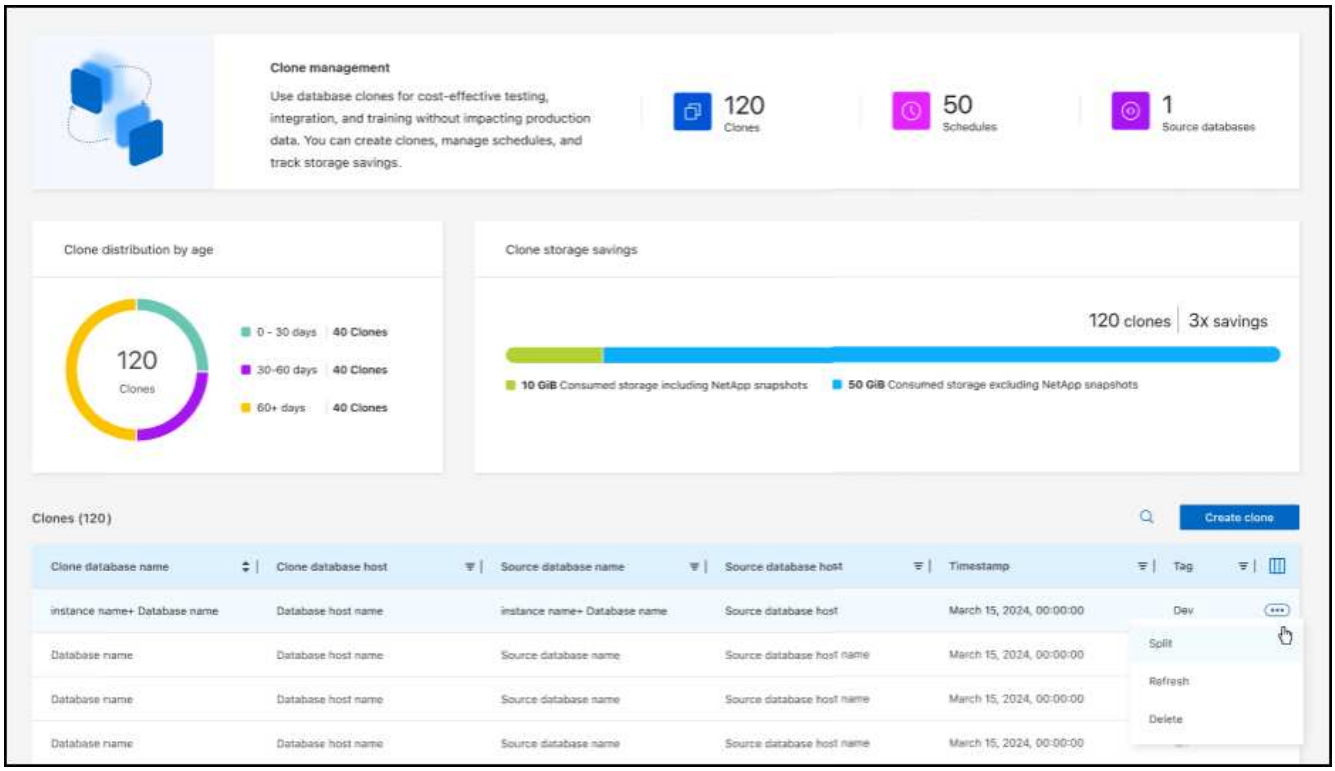
Crea un clone

Puoi creare un clone dei tuoi carichi di lavoro di Microsoft SQL Server. Un clone è una copia dei dati di origine creata da un backup. Il clone viene archiviato in un archivio oggetti nel tuo account cloud pubblico o privato. Puoi utilizzare il clone per ripristinare i tuoi carichi di lavoro in caso di perdita o danneggiamento dei dati.

È possibile creare un clone da uno snapshot esistente o da uno snapshot istantaneo. Uno snapshot istantaneo è una copia puntuale dei dati di origine creata da un backup. È possibile utilizzare il clone per ripristinare i carichi di lavoro in caso di perdita o danneggiamento dei dati.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Clona**.



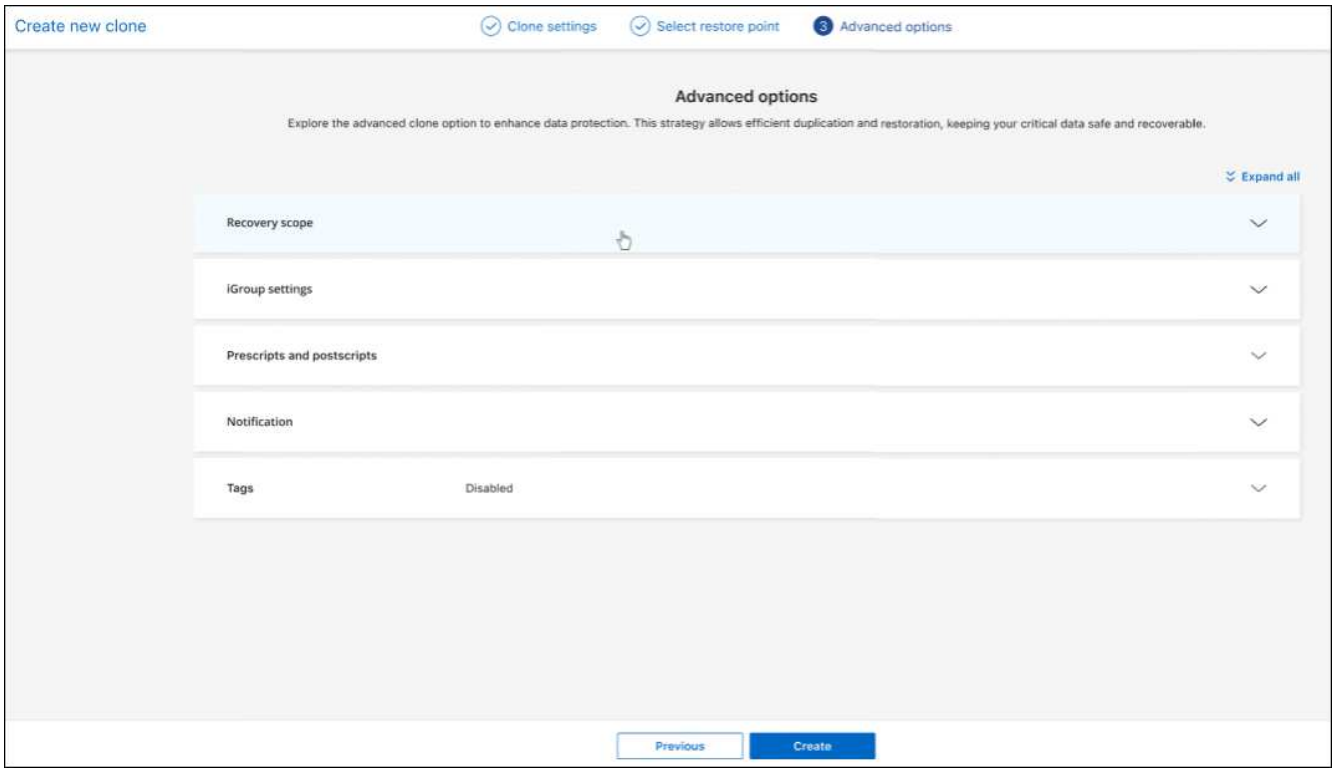
2. Seleziona **Crea nuovo clone**.
3. Seleziona il tipo di clone:
   - **Clone e aggiornamento del database da snapshot esistente**: scegli lo snapshot per il clone e configura le relative opzioni. Questa opzione è utile se desideri scegliere lo snapshot per il clone e configurare le relative opzioni.
   - **Snapshot e clone istantanei**: crea subito uno snapshot dei dati di origine e crea un clone da quello snapshot. Questa opzione è utile se desideri creare un clone dai dati più recenti nel carico di lavoro di origine.
4. Completa la sezione **Origine del database**:
   - **Clone singolo o clone in blocco**: seleziona se creare un singolo clone o più cloni. Se selezioni **Clone in blocco**, puoi creare più cloni contemporaneamente utilizzando un gruppo di protezione già creato. Questa opzione è utile se desideri creare più cloni per carichi di lavoro diversi.
   - **Host, istanza e nome del database di origine**: seleziona l'host, l'istanza e il nome del database di origine per il clone. Il database di origine è il database da cui verrà creato il clone.
5. Completare la sezione **Destinazione database**:

- **Host, istanza e nome del database di destinazione**: seleziona l'host, l'istanza e il nome del database di destinazione per il clone. Il database di destinazione è la posizione in cui verrà creato il clone.

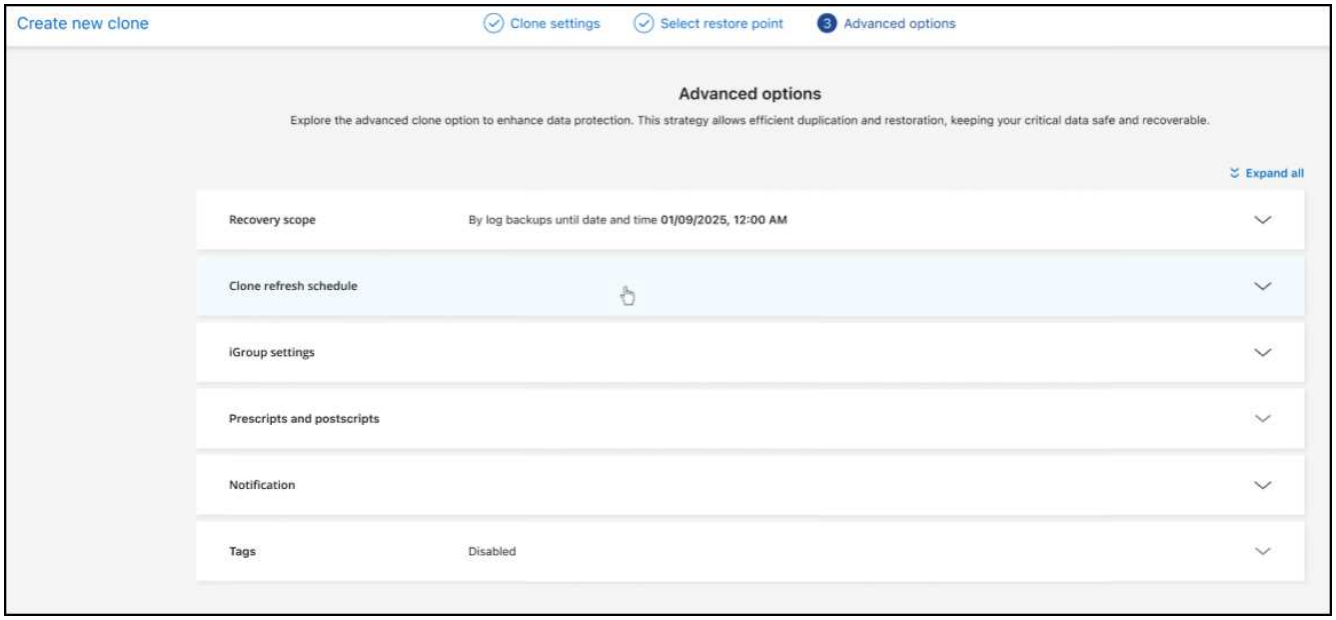
  Facoltativamente, seleziona **Suffisso** dall'elenco a discesa del nome di destinazione e aggiungi un suffisso al nome del database clonato. Se non specifichi un suffisso, il nome del database clonato sarà lo stesso del database di origine.

- **QoS (throughput massimo)**: seleziona il throughput massimo della qualità del servizio (QoS) in MBps per il clone. Il QoS definisce le caratteristiche prestazionali del clone, come il throughput massimo e gli IOPS.

6. Completa la sezione **Monte**:
   - **Assegna automaticamente punto di montaggio**: seleziona questa opzione per assegnare automaticamente un punto di montaggio al clone. Il punto di montaggio è la posizione in cui il clone verrà montato nell'archivio oggetti.
   - **Definisci percorso punto di montaggio**: Inserisci un punto di montaggio per il clone. Il punto di montaggio è la posizione in cui il clone verrà montato nell'archivio oggetti. Seleziona la lettera dell'unità, inserisci il percorso del file di dati e inserisci il percorso del file di registro.
7. Selezionare **Avanti**.
8. Seleziona il punto di ripristino:
   - **Snapshot esistenti**: seleziona uno snapshot esistente dall'elenco di snapshot disponibili per il carico di lavoro. Questa opzione è utile se desideri creare un clone da un momento specifico.
   - **Snapshot e clone istantanei**: seleziona lo snapshot più recente dall'elenco di snapshot disponibili per il carico di lavoro. Questa opzione è utile se desideri creare un clone dai dati più recenti nel carico di lavoro di origine.
9. Se hai scelto di creare **Snapshot istantaneo e clone**, seleziona la posizione di archiviazione del clone:
   - **Archiviazione locale**: Selezionare questa opzione per creare il clone nell'archiviazione locale del sistema ONTAP . L'archiviazione locale è quella direttamente collegata al sistema ONTAP .
   - **Archiviazione secondaria**: selezionare questa opzione per creare il clone nell'archiviazione secondaria del sistema ONTAP . L'archiviazione secondaria è quella utilizzata per i carichi di lavoro di backup e ripristino.
10. Selezionare la posizione di destinazione per i dati e i registri.
11. Selezionare **Avanti**.
12. Completa la sezione **Opzioni avanzate**:



13. Se hai scelto **Snapshot e clonazione istantanei**, completa le seguenti opzioni:

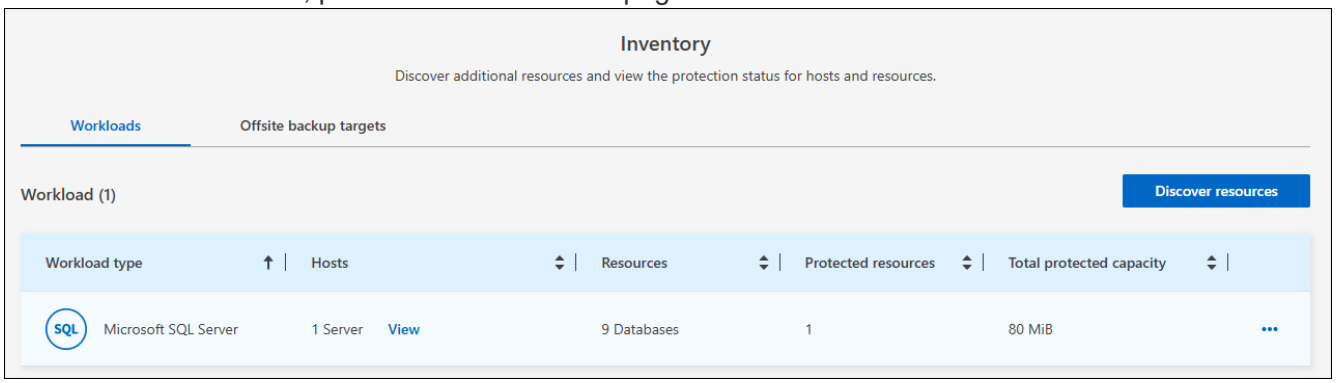


- **Pianificazione e scadenza dell'aggiornamento del clone**: se hai scelto **Clonazione istantanea**, inserisci la data di inizio dell'aggiornamento del clone. La pianificazione del clone definisce quando verrà creato il clone.
  - **Elimina il clone se la pianificazione scade**: se vuoi eliminare il clone alla data di scadenza del clone.
  - **Aggiorna clone ogni**: seleziona la frequenza con cui il clone deve essere aggiornato. Puoi scegliere di aggiornare il clone ogni ora, ogni giorno, ogni settimana, ogni mese o ogni trimestre. Questa opzione è utile se desideri mantenere il clone aggiornato con il carico di lavoro di origine.
- **Prescript e postscript**: facoltativamente, specifica gli script pre e post-clone da eseguire prima e dopo

la creazione del clone. Questi script possono essere utilizzati per eseguire attività aggiuntive, come la configurazione del clone o l'invio di notifiche.

- **Notifica**: Facoltativamente, specifica gli indirizzi email a cui ricevere notifiche sullo stato di creazione del clone insieme al report del job. Puoi anche specificare un URL webhook per ricevere notifiche sullo stato di creazione del clone. Puoi specificare se desideri ricevere notifiche di successo e fallimento oppure solo una delle due.
- **Tag**: seleziona una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse e seleziona **Applica**. Ad esempio, se aggiungi "HR" come tag a più gruppi di risorse, potrai trovare in seguito tutti i gruppi di risorse associati al tag HR.

14. Selezionare **Crea**.
15. Una volta creato il clone, potrai visualizzarlo nella pagina **Inventario**.



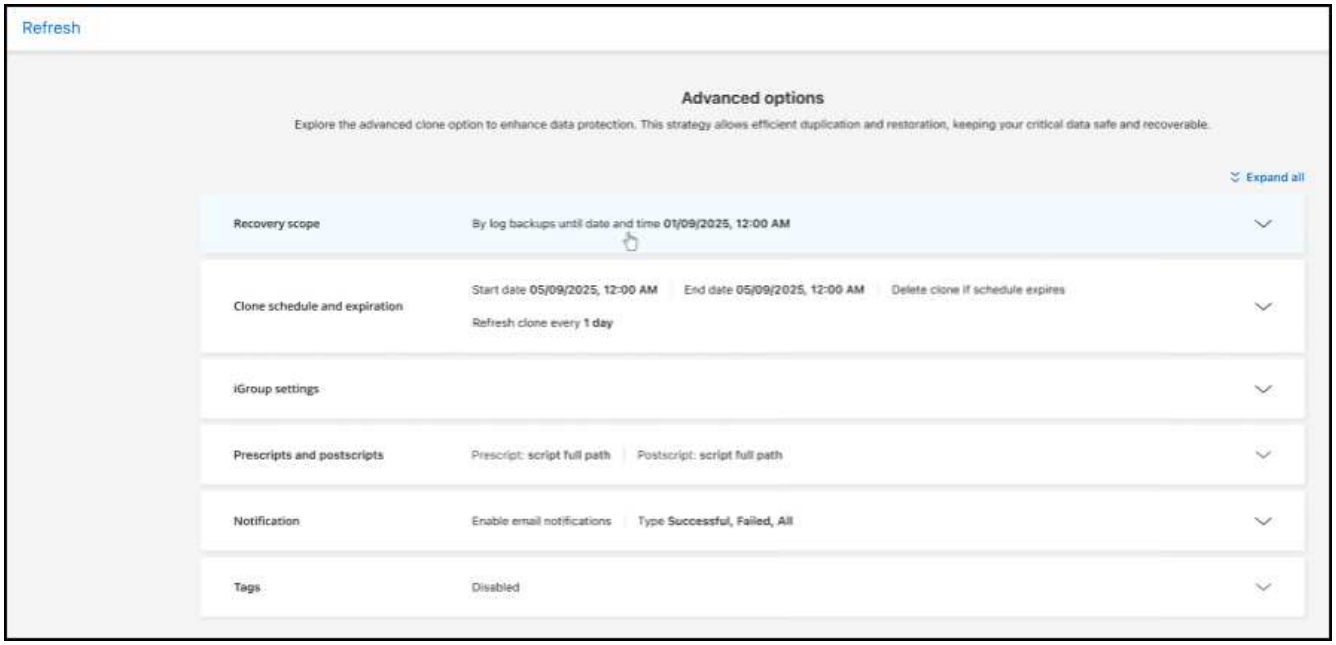
Aggiornare un clone

È possibile aggiornare un clone dei carichi di lavoro di Microsoft SQL Server. L'aggiornamento di un clone lo aggiorna con i dati più recenti del carico di lavoro di origine. Questa operazione è utile se si desidera mantenere il clone aggiornato con il carico di lavoro di origine.

È possibile modificare il nome del database, utilizzare l'ultimo snapshot istantaneo o aggiornare da uno snapshot di produzione esistente.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Clona**.
2. Seleziona il clone che vuoi aggiornare.
3. Seleziona l'icona Azioni ••• > **Aggiorna clone**.



4. Completa la sezione **Impostazioni avanzate**:
   - **Ambito di ripristino**: scegli se ripristinare tutti i backup del log o solo i backup del log fino a un momento specifico. Questa opzione è utile se desideri ripristinare il clone fino a un momento specifico.
   - **Pianificazione e scadenza dell'aggiornamento del clone**: se hai scelto **Clonazione istantanea**, inserisci la data di inizio dell'aggiornamento del clone. La pianificazione del clone definisce quando verrà creato il clone.
     - **Elimina il clone se la pianificazione scade**: se vuoi eliminare il clone alla data di scadenza del clone.
     - **Aggiorna clone ogni**: seleziona la frequenza con cui il clone deve essere aggiornato. Puoi scegliere di aggiornare il clone ogni ora, ogni giorno, ogni settimana, ogni mese o ogni trimestre. Questa opzione è utile se desideri mantenere il clone aggiornato con il carico di lavoro di origine.
   - **Impostazioni iGroup**: Selezionare l'iGroup per il clone. L'iGroup è un raggruppamento logico di iniziatori utilizzati per accedere al clone. È possibile selezionare un iGroup esistente o crearne uno nuovo. Selezionare l'iGroup dal sistema di storage ONTAP primario o secondario.
   - **Prescript e postscript**: facoltativamente, specifica gli script pre e post-clone da eseguire prima e dopo la creazione del clone. Questi script possono essere utilizzati per eseguire attività aggiuntive, come la configurazione del clone o l'invio di notifiche.
   - **Notifica**: Facoltativamente, specifica gli indirizzi email a cui ricevere notifiche sullo stato di creazione del clone insieme al report del job. Puoi anche specificare un URL webhook per ricevere notifiche sullo stato di creazione del clone. Puoi specificare se desideri ricevere notifiche di successo e fallimento oppure solo una delle due.
   - **Tag**: Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. Ad esempio, se aggiungi "HR" come tag a più gruppi di risorse, potrai trovare in seguito tutti i gruppi di risorse associati al tag HR.
5. Nella finestra di dialogo di conferma Aggiornamento, per continuare, selezionare **Aggiorna**.

Salta un aggiornamento clone

Potresti voler saltare un aggiornamento del clone se non vuoi aggiornare il clone con i dati più recenti del carico di lavoro di origine. Saltare un aggiornamento del clone ti consente di mantenere il clone così com'è senza aggiornarlo.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Clona**.
2. Seleziona il clone di cui vuoi saltare l'aggiornamento.
3. Seleziona l'icona Azioni ••• > **Salta aggiornamento**.
4. Nella finestra di dialogo di conferma "Ignora aggiornamento", procedere come segue:
   a. Per saltare solo la prossima pianificazione di aggiornamento, seleziona **Salta solo la prossima pianificazione di aggiornamento**.
   b. Per continuare, seleziona **Salta**.

Separare un clone

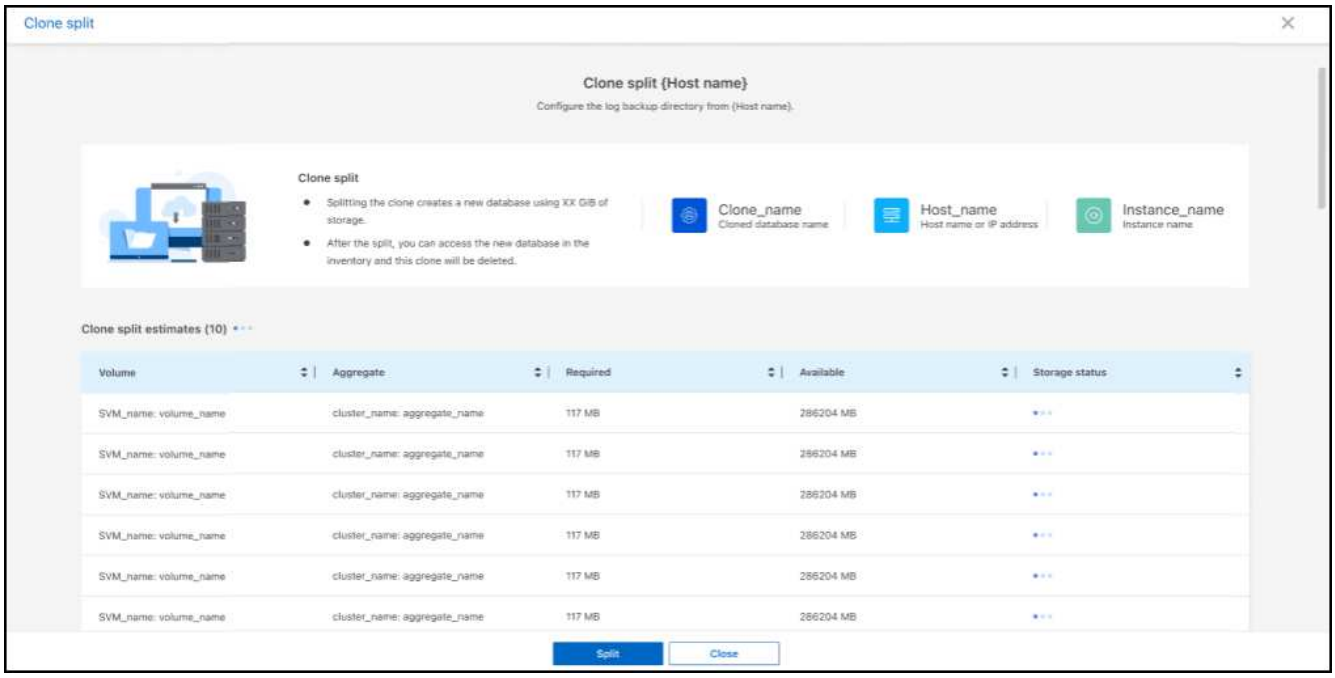
È possibile suddividere un clone dei carichi di lavoro di Microsoft SQL Server. La suddivisione di un clone crea un nuovo backup del clone. Il nuovo backup può essere utilizzato per ripristinare i carichi di lavoro.

È possibile scegliere di suddividere un clone in cloni indipendenti o a lungo termine. Una procedura guidata mostra l'elenco degli aggregati che fanno parte della SVM, le loro dimensioni e la posizione del volume clonato. BlueXP backup and recovery indica anche se lo spazio disponibile è sufficiente per suddividere il clone. Dopo la suddivisione, il clone diventa un database indipendente per la protezione.

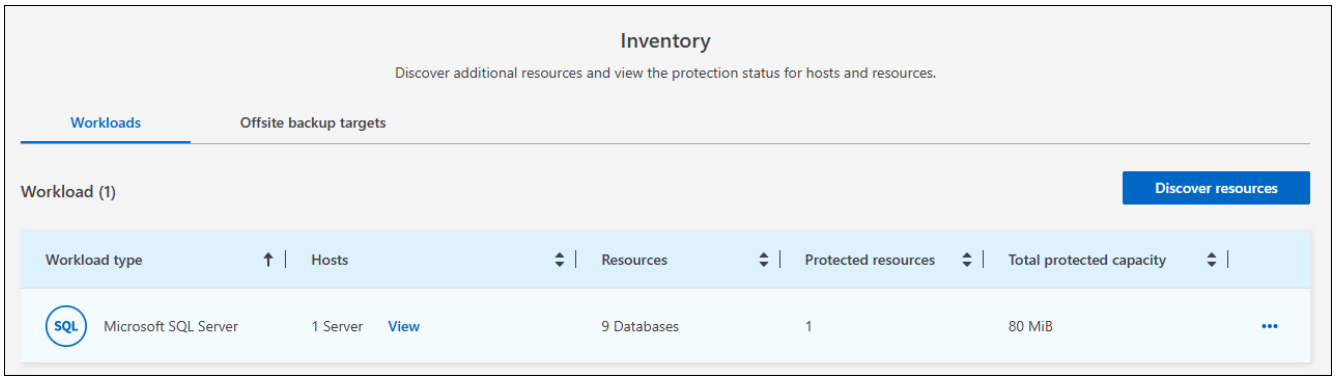
Il processo di clonazione non può essere rimosso e può essere riutilizzato per altri cloni.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Clona**.
2. Seleziona un clone.
3. Seleziona l'icona Azioni ••• > **Clonazione divisa**.



4. Rivedi i dettagli della clonazione divisa e seleziona **Dividi**.
5. Una volta creato il clone diviso, è possibile visualizzarlo nella pagina **Inventario**.



Elimina un clone

È possibile eliminare un clone dei carichi di lavoro di Microsoft SQL Server. L'eliminazione di un clone lo rimuove dall'archivio oggetti e libera spazio di archiviazione.

Se il clone è protetto da un criterio, il clone viene eliminato insieme al processo.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Clona**.
2. Seleziona un clone.
3. Seleziona l'icona Azioni ••• > **Elimina clone**.
4. Nella finestra di dialogo di conferma dell'eliminazione del clone, rivedere i dettagli dell'eliminazione.
   a. Per eliminare le risorse clonate da SnapCenter anche se i cloni o il loro archivio non sono accessibili, selezionare **Forza eliminazione**.
   b. Selezionare **Delete** (Elimina).
5. Quando il clone viene eliminato, viene rimosso dalla pagina **Inventario**.

Gestisci l'inventario di Microsoft SQL Server con il BlueXP backup and recovery

Il BlueXP backup and recovery consentono di gestire le informazioni sull'host del carico di lavoro di Microsoft SQL Server, le informazioni sul database e le informazioni sulle istanze. È possibile visualizzare, modificare ed eliminare le impostazioni di protezione del proprio inventario.

Puoi svolgere le seguenti attività relative alla gestione del tuo inventario:

- Gestire le informazioni dell'host
  - Sospendi gli orari
  - Modifica o elimina gli host
- Gestisci le informazioni sulle istanze
  - Associare le credenziali a una risorsa
  - Esegui subito il backup avviando un backup su richiesta
  - Modifica le impostazioni di protezione
- Gestire le informazioni del database
  - Proteggere i database

- Ripristinare i database
- Modifica le impostazioni di protezione
- Esegui subito il backup avviando un backup su richiesta

- Configurare la directory dei log (da Inventario > Host). Se si desidera eseguire il backup dei log per gli host del database nello snapshot, configurare prima i log in BlueXP backup and recovery. Per ulteriori informazioni, fare riferimento alla "Configurare le impostazioni BlueXP backup and recovery".

Gestire le informazioni dell'host

È possibile gestire le informazioni sugli host per garantire che siano protetti solo gli host corretti. È possibile visualizzare, modificare ed eliminare le informazioni sugli host.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di Backup e ripristino, amministratore di backup di Backup e ripristino, amministratore di ripristino di Backup e ripristino o amministratore di clonazione di Backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

- Configurare la directory dei registri. Per ulteriori informazioni, fare riferimento alla "Configurare le impostazioni BlueXP backup and recovery".
- Sospendi gli orari
- Modifica un host
- Elimina un host

Gestire gli host

Puoi gestire gli host rilevati nel tuo ambiente di lavoro, separatamente o in gruppo.

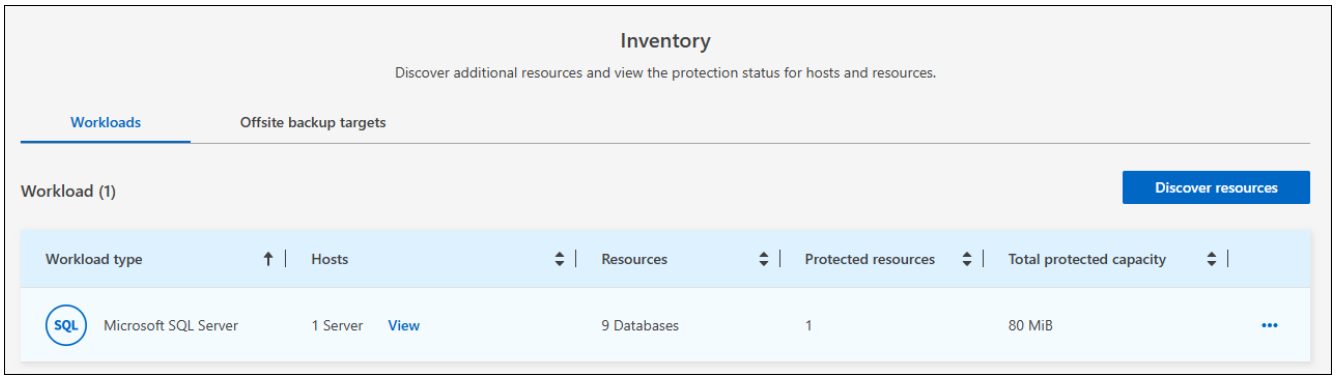
È possibile gestire solo gli host che mostrano lo stato "Non gestito" nella colonna Host. Se lo stato è "Gestito", significa che l'host è già gestito da BlueXP backup and recovery.

Dopo aver gestito gli host nel BlueXP backup and recovery, SnapCenter non gestisce più le risorse su tali host.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti oppure super amministratore di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

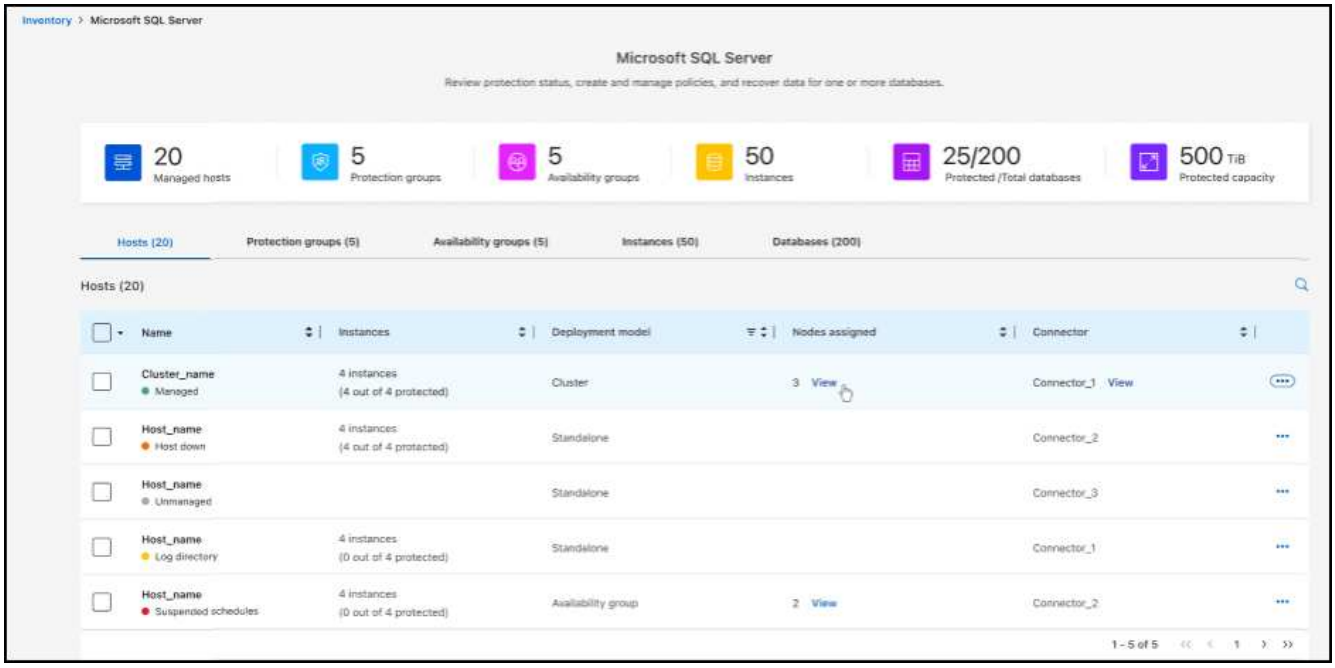
Fasi

1. Dal menu, seleziona **Inventario**.

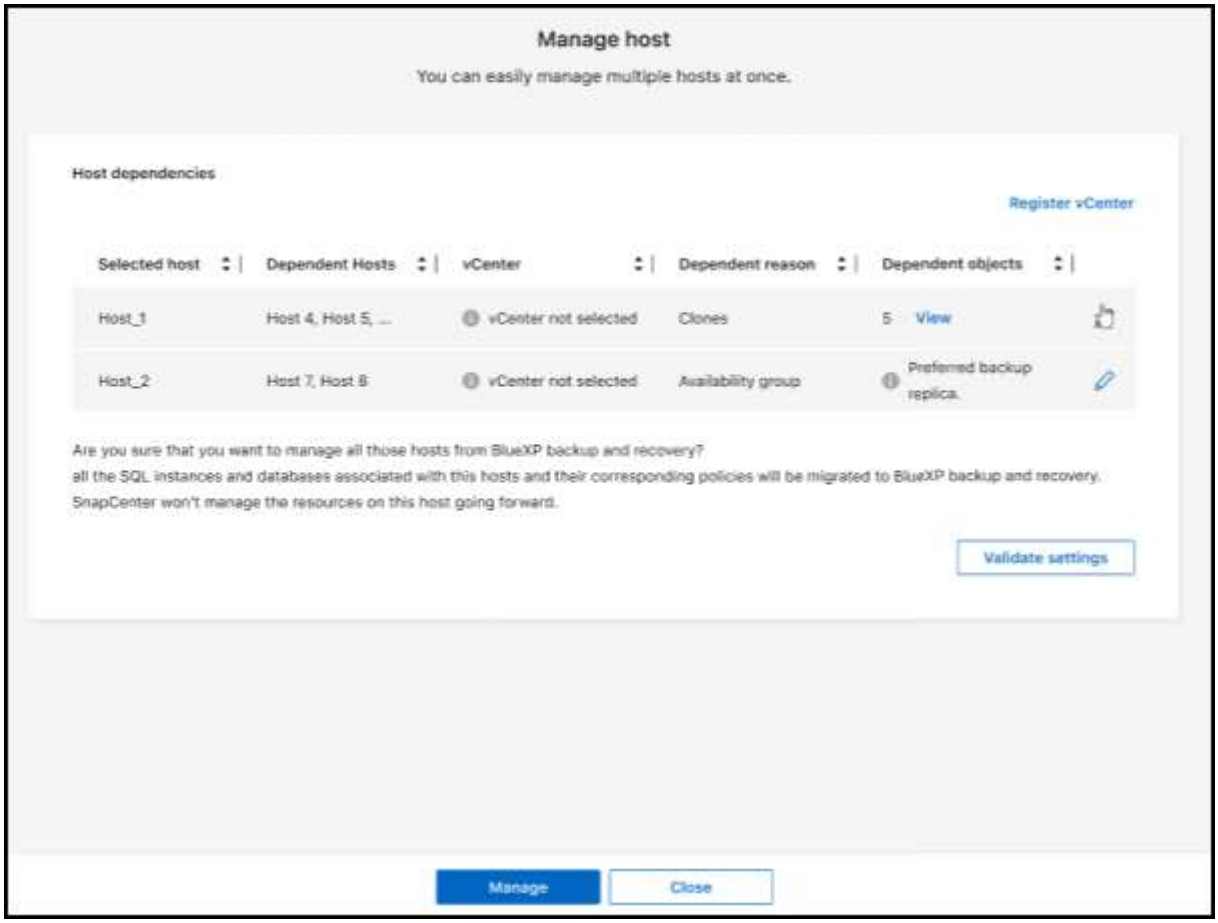


2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.

3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.



4. Selezionare la scheda **Host**.
5. Seleziona uno o più host. Se selezioni più host, verrà visualizzata l'opzione "Azioni in blocco" in cui puoi selezionare "Gestisci (fino a 5 host)".
6. Seleziona l'icona Azioni ••• > **Gestisci**.



7. Esaminare le dipendenze dell'host:
    - Se vCenter non viene visualizzato, selezionare l'icona della matita per aggiungere o modificare i dettagli di vCenter.
    - Se si aggiunge un vCenter, è necessario anche registrarlo selezionando **Registra vCenter**.
8. Seleziona **Convalida impostazioni** per testare le tue impostazioni.
9. Selezionare **Gestisci** per gestire l'host.

Sospendi gli orari

È possibile sospendere le pianificazioni per interrompere le operazioni di backup e ripristino di un host. Questa operazione potrebbe essere utile se è necessario eseguire attività di manutenzione sull'host.

Fasi

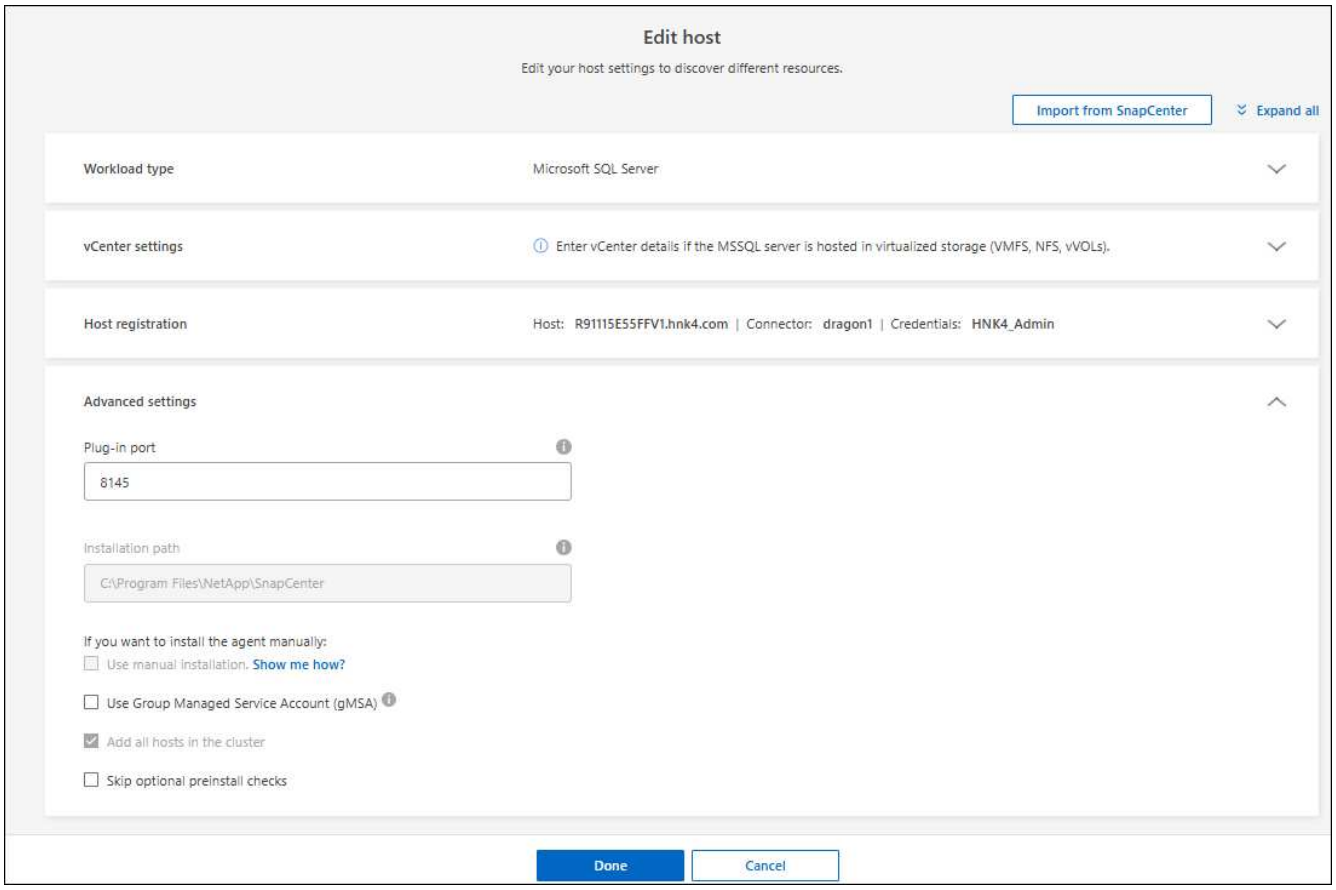
1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona l'host su cui vuoi sospendere le pianificazioni.
3. Seleziona **Azioni** ••• icona e seleziona **Sospendi pianificazioni**.
4. Nella finestra di dialogo di conferma, seleziona **Sospendi**.

Modifica un host

È possibile modificare le informazioni del server vCenter, le credenziali di registrazione dell'host e le opzioni delle impostazioni avanzate.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona l'host che vuoi modificare.
3. Seleziona **Azioni** ••• icona e seleziona **Modifica host**.



4. Modifica le informazioni dell'host.
5. Selezionare **fine**.

Elimina un host

È possibile eliminare le informazioni dell'host per interrompere gli addebiti sul servizio.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona l'host che vuoi eliminare.
3. Seleziona **Azioni** ••• icona e seleziona **Elimina host**.
4. Rivedi le informazioni di conferma e seleziona **Elimina**.

Gestisci le informazioni sulle istanze

È possibile gestire le informazioni delle istanze per garantire che le risorse dispongano delle credenziali appropriate per la protezione ed è possibile eseguire il backup delle risorse nei seguenti modi:

- Proteggere le istanze
- Credenziali associate
- Disassociare le credenziali
- Protezione dalle modifiche
- Esegui il backup adesso

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di Backup e ripristino, amministratore di backup di Backup e ripristino, amministratore di ripristino di Backup e ripristino o amministratore di clonazione di Backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Proteggere le istanze del database

È possibile assegnare una policy a un'istanza di database utilizzando policy che regolano le pianificazioni e la conservazione della protezione delle risorse.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni** ••• icona e seleziona **Proteggi**.
6. Seleziona una policy o creane una nuova.

   Per i dettagli sulla creazione di una policy, fare riferimento a "Creare un criterio" .

7. Fornire informazioni sugli script che si desidera eseguire prima e dopo il backup.
   - **Pre-script**: Inserisci il nome e il percorso del file dello script per eseguirlo automaticamente prima dell'attivazione dell'azione di protezione. Questa opzione è utile per eseguire attività o configurazioni aggiuntive che devono essere eseguite prima del flusso di lavoro di protezione.
   - **Post-script**: Inserisci il nome e il percorso del file dello script per eseguirlo automaticamente al termine dell'azione di protezione. Questa opzione è utile per eseguire attività o configurazioni aggiuntive che devono essere eseguite dopo il flusso di lavoro di protezione.
8. Fornisci informazioni su come desideri che venga verificato lo snapshot:
   - Posizione di archiviazione: seleziona la posizione in cui verrà archiviato lo snapshot di verifica.
   - Risorsa di verifica: seleziona se la risorsa che vuoi verificare si trova nello snapshot locale e nell'archiviazione secondaria ONTAP .
   - Pianificazione della verifica: seleziona la frequenza oraria, giornaliera, settimanale, mensile o annuale.

Associare le credenziali a una risorsa

È possibile associare le credenziali a una risorsa in modo che venga garantita la protezione.

Per ulteriori informazioni, vedere "Configurare le impostazioni BlueXP backup and recovery , incluse le credenziali".

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni** ••• e seleziona **Associa credenziali**.
6. Utilizza le credenziali esistenti o creane di nuove.

Modifica le impostazioni di protezione

È possibile modificare la policy, crearne una nuova, impostare una pianificazione e definire le impostazioni di conservazione.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni** ••• icona e seleziona **Modifica protezione**.

   Per i dettagli sulla creazione di una policy, fare riferimento a "Creare un criterio" .

Esegui il backup adesso

Puoi eseguire subito il backup dei tuoi dati per assicurarti che siano immediatamente protetti.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni** ••• icona e seleziona **Esegui backup adesso**.
6. Scegli il tipo di backup e imposta la pianificazione.

   Per i dettagli sulla creazione di un backup ad hoc, fare riferimento a "Creare un criterio" .

Gestire le informazioni del database

È possibile gestire le informazioni del database nei seguenti modi:

- Proteggere i database
- Ripristinare i database
- Visualizza i dettagli della protezione
- Modifica le impostazioni di protezione
- Esegui il backup adesso

Proteggere i database

È possibile modificare la policy, crearne una nuova, impostare una pianificazione e definire le impostazioni di conservazione.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Ruolo di amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database.
5. Seleziona **Azioni** ••• icona e seleziona **Proteggi**.

   Per i dettagli sulla creazione di una policy, fare riferimento a "Creare un criterio" .

Ripristinare i database

È possibile ripristinare un database per garantire la protezione dei dati.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Amministratore di ripristino di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database.
5. Seleziona **Azioni** ••• icona e seleziona **Ripristina**.

   Per informazioni sul ripristino dei carichi di lavoro, fare riferimento a "Ripristinare i carichi di lavoro" .

Modifica le impostazioni di protezione

È possibile modificare la policy, crearne una nuova, impostare una pianificazione e definire le impostazioni di conservazione.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Ruolo di amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database.
5. Seleziona **Azioni** ••• icona e seleziona **Modifica protezione**.

   Per i dettagli sulla creazione di una policy, fare riferimento a "Creare un criterio" .

Esegui il backup adesso

Puoi eseguire subito il backup delle istanze e dei database di Microsoft SQL Server per garantire la protezione immediata dei tuoi dati.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Ruolo di amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Seleziona il carico di lavoro che vuoi visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze** o **Database**.
4. Selezionare l'istanza o il database.
5. Seleziona **Azioni** ••• icona e seleziona **Esegui backup adesso**.

Gestisci gli snapshot di Microsoft SQL Server con il BlueXP backup and recovery

È possibile gestire gli snapshot di Microsoft SQL Server eliminandoli dal BlueXP backup and recovery.

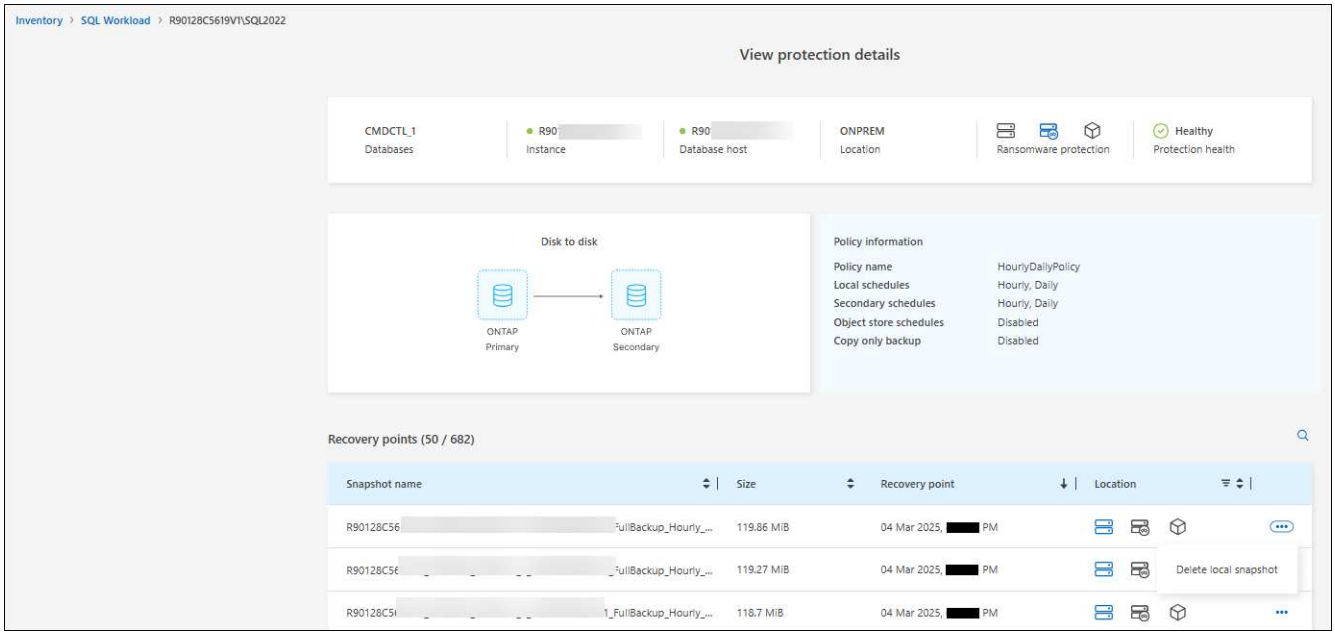
Eliminare uno snapshot

È possibile eliminare solo gli snapshot locali.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Ruolo di amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Selezionare il carico di lavoro e selezionare **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database per il quale si desidera eliminare uno snapshot.
5. Dal menu Azioni, seleziona **Visualizza dettagli protezione**.



6. Seleziona lo snapshot locale che desideri eliminare.

   L'icona dello snapshot locale nella colonna **Posizione** su quella riga deve apparire in blu.

7. Seleziona **Azioni** ••• icona e seleziona **Elimina snapshot locale**.
8. Nella finestra di dialogo di conferma, seleziona **Rimuovi**.

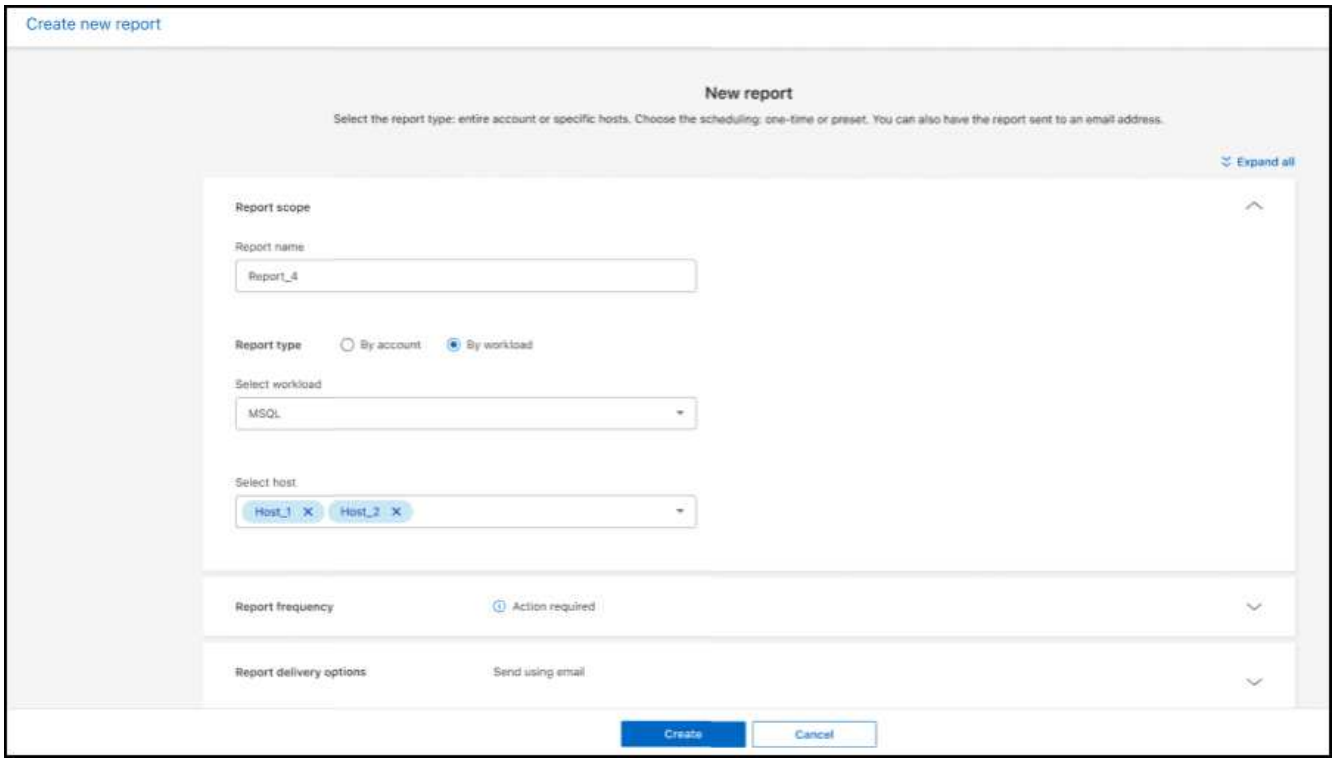
Crea report per i carichi di lavoro di Microsoft SQL Server nel BlueXP backup and recovery

In BlueXP backup and recovery, puoi creare report per i carichi di lavoro di Microsoft SQL Server per visualizzare lo stato dei backup, inclusi il numero di backup, il numero di backup riusciti e il numero di backup non riusciti. Puoi anche visualizzare i dettagli di ciascun backup, inclusi il tipo di backup, il sistema di archiviazione utilizzato e l'ora del backup.

Creare un report

Ruolo BlueXP richiesto Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di Backup e ripristino, Amministratore di backup di Backup e ripristino, Amministratore di ripristino di Backup e ripristino, Amministratore di clonazione di Backup e ripristino. Scopri di più su "Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

1. Dal menu BlueXP backup and recovery , seleziona la scheda **Report**.
2. Selezionare **Crea report**.



3. Inserisci i dettagli dell'ambito del report:
   - **Nome del report**: inserisci un nome univoco per il report.

- **Tipo di report**: scegli se desideri un report per account o per carico di lavoro (Microsoft SQL Server).
- **Seleziona host**: se hai selezionato in base al carico di lavoro, seleziona l'host per il quale desideri generare il report.
- **Seleziona contenuto**: scegli se desideri che il report includa un riepilogo di tutti i backup o i dettagli di ciascun backup. (Se hai scelto "Per account")

4. Immetti intervallo di reporting: scegli se desideri che il report includa i dati dell'ultimo giorno, degli ultimi 7 giorni, degli ultimi 30 giorni, dell'ultimo trimestre o dell'ultimo anno.
5. Inserisci i dettagli di invio del report: se desideri che il report venga inviato via email, seleziona **Invia report tramite email**. Inserisci l'indirizzo email a cui desideri che venga inviato il report.

   Configura le notifiche email nella pagina Impostazioni. Per dettagli sulla configurazione delle notifiche email, consulta "Configurare le impostazioni" .

Protezione dei carichi di lavoro VMware (anteprima senza plug-in SnapCenter per VMware)

Proteggi i carichi di lavoro VMware con la panoramica BlueXP backup and recovery

Proteggi le tue VM VMware e i tuoi datastore con il BlueXP backup and recovery. Il BlueXP backup and recovery garantiscono operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con la VM. È possibile eseguire il backup dei carichi di lavoro VMware su Amazon Web Services S3 o StorageGRID e ripristinarli su un host VMware locale.

Questa versione di BlueXP backup and recovery supporta solo VMware vCenter e non rileva vVols o VM su vVols.

Utilizza il BlueXP backup and recovery per implementare una strategia 3-2-1, in cui hai 3 copie dei tuoi dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud. I vantaggi dell'approccio 3-2-1 includono:

- Copie multiple dei dati offrono protezione multi-layer contro le minacce interne (interne) e esterne alla cybersicurezza.
- Diversi tipi di supporti garantiscono la fattibilità del failover in caso di guasto fisico o logico di un tipo di supporto.
- La copia in loco agevola i ripristini rapidi, mentre le copie fuori sede sono disponibili nel caso in cui la copia in loco sia compromessa.

NOTA Per passare da una versione all'altra dell'interfaccia utente BlueXP backup and recovery , fare riferimento a "Passa alla precedente interfaccia utente BlueXP backup and recovery" .

È possibile utilizzare il BlueXP backup and recovery per eseguire le seguenti attività relative ai carichi di lavoro VMware:

- "Scopri i carichi di lavoro VMware"
- "Crea e gestisci gruppi di protezione per carichi di lavoro VMware"

- "Eseguire il backup dei carichi di lavoro VMware"
- "Ripristinare i carichi di lavoro VMware"

Scopri i carichi di lavoro VMware con il BlueXP backup and recovery

Per poter utilizzare il servizio BlueXP backup and recovery, è necessario innanzitutto rilevare i datastore VMware e le VM in esecuzione sui sistemi ONTAP . Facoltativamente, puoi importare dati di backup e policy dal SnapCenter Plug-in for VMware vSphere se è già installato.

Ruolo BlueXP obbligatorio Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Scopri i carichi di lavoro VMware e, facoltativamente, importa le risorse SnapCenter

Durante l'individuazione, il BlueXP backup and recovery analizzano i carichi di lavoro VMware all'interno dell'organizzazione e valutano e importano le policy di protezione esistenti, le copie snapshot e le opzioni di backup e ripristino.

È possibile importare datastore e VM VMware NFS e VMFS dal SnapCenter Plug-in for VMware vSphere nell'inventario BlueXP backup and recovery .

Questa versione di BlueXP backup and recovery supporta solo VMware vCenter e non rileva vVols o VM su vVols.

Durante il processo di importazione, il BlueXP backup and recovery eseguono le seguenti attività:

- Abilita l'accesso SSH sicuro al server vCenter.
- Attiva la modalità di manutenzione su tutti i gruppi di risorse nel server vCenter.
- Prepara i metadati del vCenter e lo contrassegna come non gestito in BlueXP.
- Configura l'accesso al database.
- Rileva VMware vCenter, datastore e VM.
- Importa criteri di protezione esistenti, copie snapshot e opzioni di backup e ripristino dal SnapCenter Plug-in for VMware vSphere.
- Visualizza le risorse rilevate nella pagina Inventario BlueXP backup and recovery .

La scoperta avviene nei seguenti modi:

- Se disponi già SnapCenter Plug-in for VMware vSphere, importa le risorse SnapCenter nel BlueXP backup and recovery utilizzando l'interfaccia utente BlueXP backup and recovery .

  Se disponi già del plug-in SnapCenter , assicurati di soddisfare i prerequisiti prima di importare da SnapCenter. Ad esempio, dovresti creare ambienti di lavoro in BlueXP Canvas per tutti gli archivi cluster SnapCenter locali prima di importare da SnapCenter. Vedere "Prerequisiti per l'importazione di risorse da SnapCenter" .

- Se non disponi ancora del plug-in SnapCenter , puoi comunque individuare i carichi di lavoro nei tuoi ambienti di lavoro aggiungendo manualmente un vCenter ed eseguendo l'individuazione.

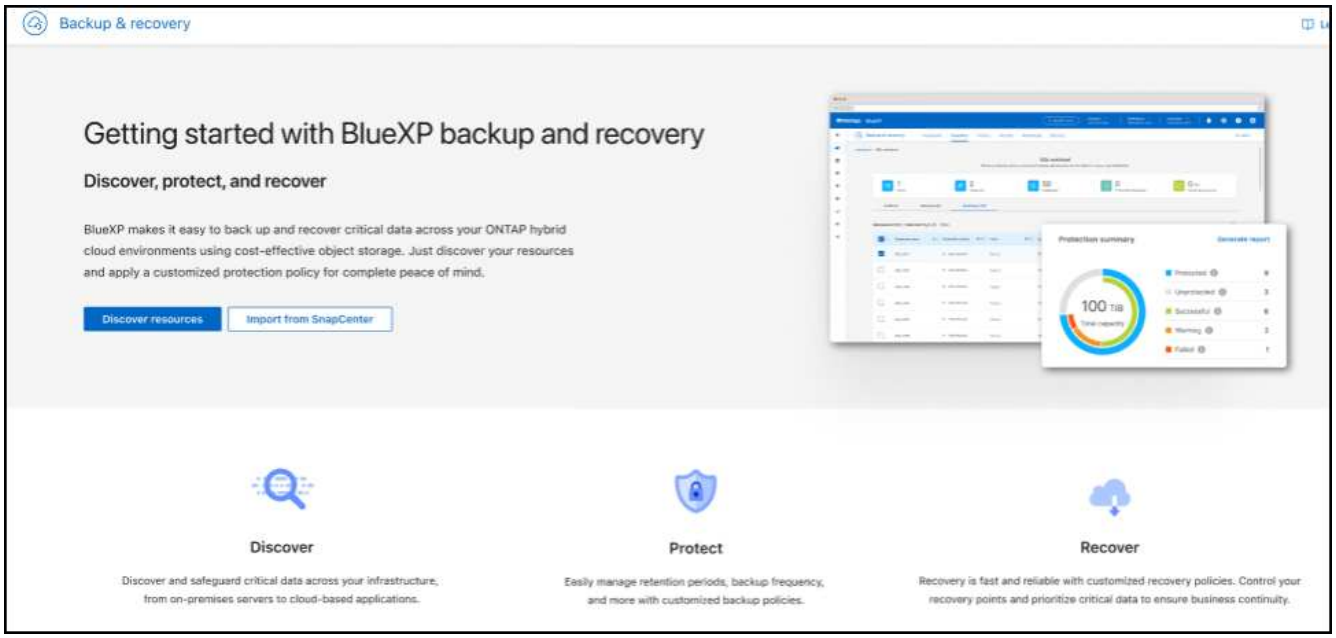
Se il plug-in SnapCenter non è già installato, aggiungi un vCenter e scopri le risorse

Se non hai ancora installato il plug-in SnapCenter per VMware, aggiungi le informazioni di vCenter e fai in modo che il BlueXP backup and recovery rilevino i carichi di lavoro. All'interno di ciascun BlueXP Connector, seleziona gli ambienti di lavoro in cui desideri individuare i carichi di lavoro.

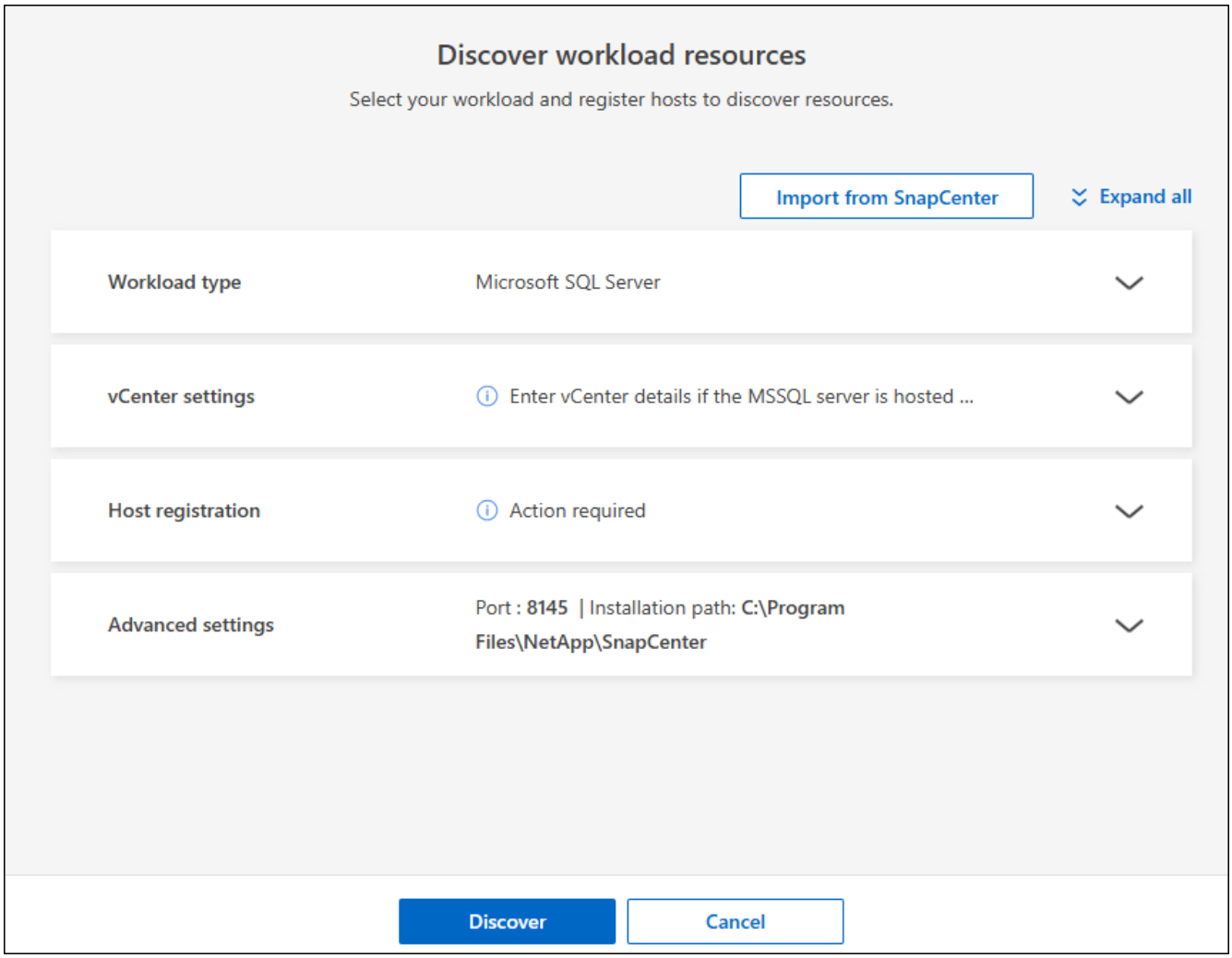
Fasi

1. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.

   Se è la prima volta che accedi a questo servizio e hai già un ambiente di lavoro in BlueXP, ma non hai scoperto alcuna risorsa, viene visualizzata la pagina di destinazione "Benvenuti nel nuovo BlueXP backup and recovery" che mostra un'opzione per **Scoprire risorse**.



2. Seleziona **Scopri risorse**.



3. Inserire le seguenti informazioni:
   a. **Tipo di carico di lavoro**: seleziona **VMware**.
   b. **Impostazioni vCenter**: aggiungi un nuovo vCenter. Per aggiungere un nuovo vCenter, immettere l'FQDN o l'indirizzo IP del vCenter, il nome utente, la password, la porta e il protocollo.

      Se si inseriscono informazioni su vCenter, inserire le informazioni sia per le impostazioni di vCenter che per la registrazione dell'host. Se si sono aggiunte o inserite informazioni su vCenter qui, è necessario aggiungere anche le informazioni sui plugin nelle Impostazioni avanzate.

   c. **Registrazione host**: non richiesta per VMware.
4. Selezionare **Discover**.

   Questo processo potrebbe richiedere alcuni minuti.

5. Continua con Impostazioni avanzate.

Se il plug-in SnapCenter è già installato, importare le risorse del plug-in SnapCenter per VMware nel BlueXP backup and recovery

Se hai già installato il plug-in SnapCenter per VMware, importa le risorse del plug-in SnapCenter nel BlueXP backup and recovery seguendo questi passaggi. Il servizio BlueXP rileva gli host ESXi, i datastore e le VM nei

vCenter e li pianifica dal plug-in; non è necessario ricreare tutte queste informazioni.

Puoi farlo nei seguenti modi:

- Durante la scoperta, seleziona un'opzione per importare le risorse dal plug-in SnapCenter .
- Dopo la scoperta, dalla pagina Inventario, seleziona un'opzione per importare le risorse del plug-in SnapCenter .
- Dopo l'individuazione, dal menu Impostazioni, seleziona un'opzione per importare le risorse del plug-in SnapCenter . Per maggiori dettagli, vedere "Configurare il BlueXP backup and recovery" . Questa funzionalità non è supportata per VMware.

Si tratta di un processo in due parti descritto in questa sezione:

1. Importa i metadati di vCenter dal plug-in SnapCenter . Le risorse vCenter importate non sono ancora gestite dal BlueXP backup and recovery.
2. Avvia la gestione di vCenter, VM e datastore selezionati nel BlueXP backup and recovery. Dopo aver avviato la gestione, BlueXP backup and recovery etichetta vCenter come "Gestito" nella pagina Inventario ed è in grado di eseguire il backup e il ripristino delle risorse importate. Dopo aver avviato la gestione nel BlueXP backup and recovery, non sarà più possibile gestire tali risorse nel plug-in SnapCenter .

Importa metadati vCenter dal plug-in SnapCenter

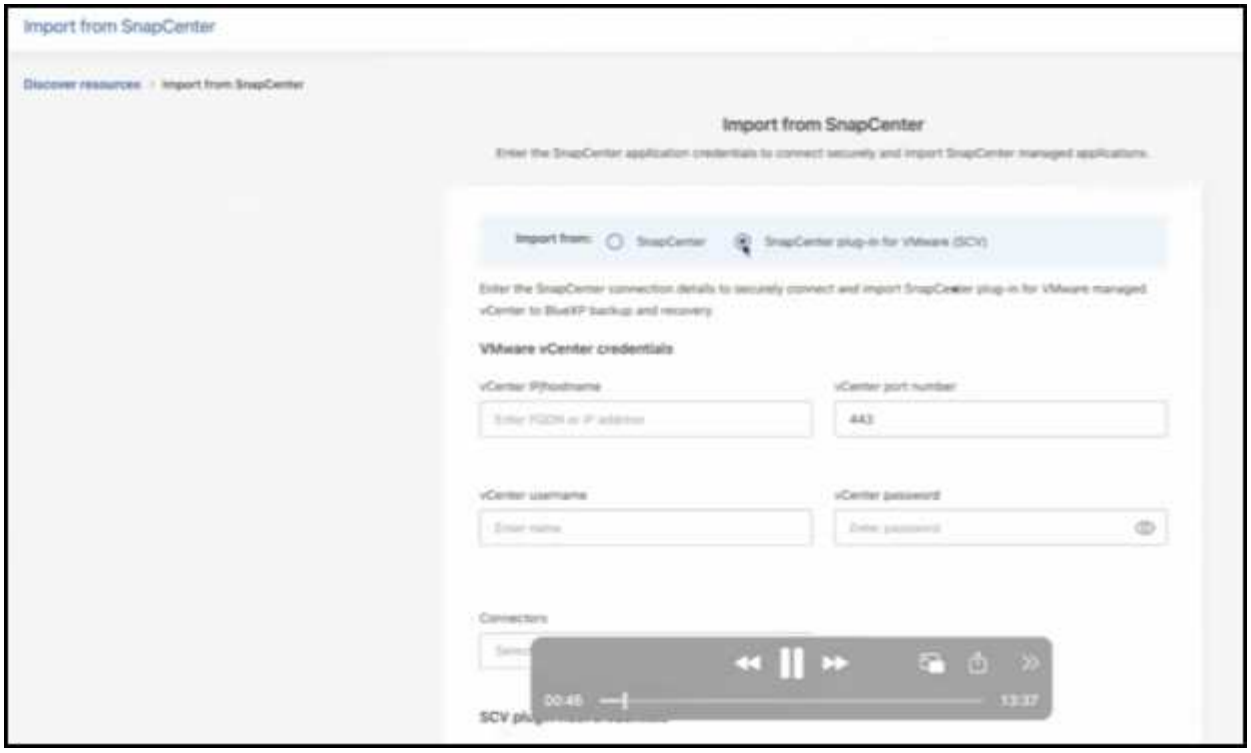
Questo primo passaggio importa i metadati di vCenter dal plug-in SnapCenter . A quel punto, le risorse non sono ancora gestite dal BlueXP backup and recovery.

Dopo aver importato i metadati di vCenter dal plug-in SnapCenter , il BlueXP backup and recovery non assumono automaticamente la gestione della protezione. Per fare ciò, è necessario selezionare esplicitamente la gestione delle risorse importate nel BlueXP backup and recovery. In questo modo sarai pronto a sottoporre tali risorse a backup tramite BlueXP backup and recovery.

Fasi

1. Dal menu di navigazione a sinistra BlueXP , seleziona **Protezione** > **Backup e ripristino**.
2. Dal menu in alto, seleziona **Inventario**.

3. Dal menu in alto nella pagina Inventario, seleziona **Scopri risorse**.
4. Dalla pagina delle risorse del carico di lavoro Discover BlueXP backup and recovery , seleziona **Importa da SnapCenter**.



5. Nel campo Importa da, seleziona * SnapCenter Plug-in per VMware*.
6. Inserisci **credenziali VMware vCenter**:
   a. **IP/nome host vCenter**: immettere l'FQDN o l'indirizzo IP del vCenter che si desidera importare in BlueXP backup and recovery.
   b. **Numero porta vCenter**: immettere il numero di porta per vCenter.
   c. **Nome utente vCenter** e **Password**: immettere il nome utente e la password per vCenter.
   d. **Connettore**: selezionare il connettore BlueXP per vCenter.
7. Inserisci * Credenziali host del plug-in SnapCenter *:
   a. **Credenziali esistenti**: Se selezioni questa opzione, puoi utilizzare le credenziali esistenti che hai già aggiunto. Scegli il nome delle credenziali.
   b. **Aggiungi nuove credenziali**: se non disponi di credenziali host per il plug-in SnapCenter , puoi aggiungerne di nuove. Immettere il nome delle credenziali, la modalità di autenticazione, il nome utente e la password.
8. Selezionare **Importa** per convalidare le voci e registrare il plug-in SnapCenter .

> Se il plug-in SnapCenter è già registrato, è possibile aggiornare i dettagli di registrazione esistenti.

Risultato

Nella pagina Inventario, vCenter viene visualizzato come non gestito nel BlueXP backup and recovery finché non si seleziona esplicitamente di gestirlo.

Gestisci le risorse importate dal plug-in SnapCenter

Dopo aver importato i metadati vCenter dal plug-in SnapCenter per VMware, gestire le risorse nel BlueXP backup and recovery. Dopo aver scelto di gestire tali risorse, BlueXP backup and recovery è in grado di eseguire il backup e il ripristino delle risorse importate. Dopo aver avviato la gestione nel BlueXP backup and recovery, non sarà più possibile gestire tali risorse nel plug-in SnapCenter .

Dopo aver scelto di gestire le risorse, le risorse, le VM e i criteri vengono importati dal plug-in SnapCenter per VMware. I gruppi di risorse, i criteri e gli snapshot vengono migrati dal plug-in e gestiti nel BlueXP backup and recovery.

Fasi

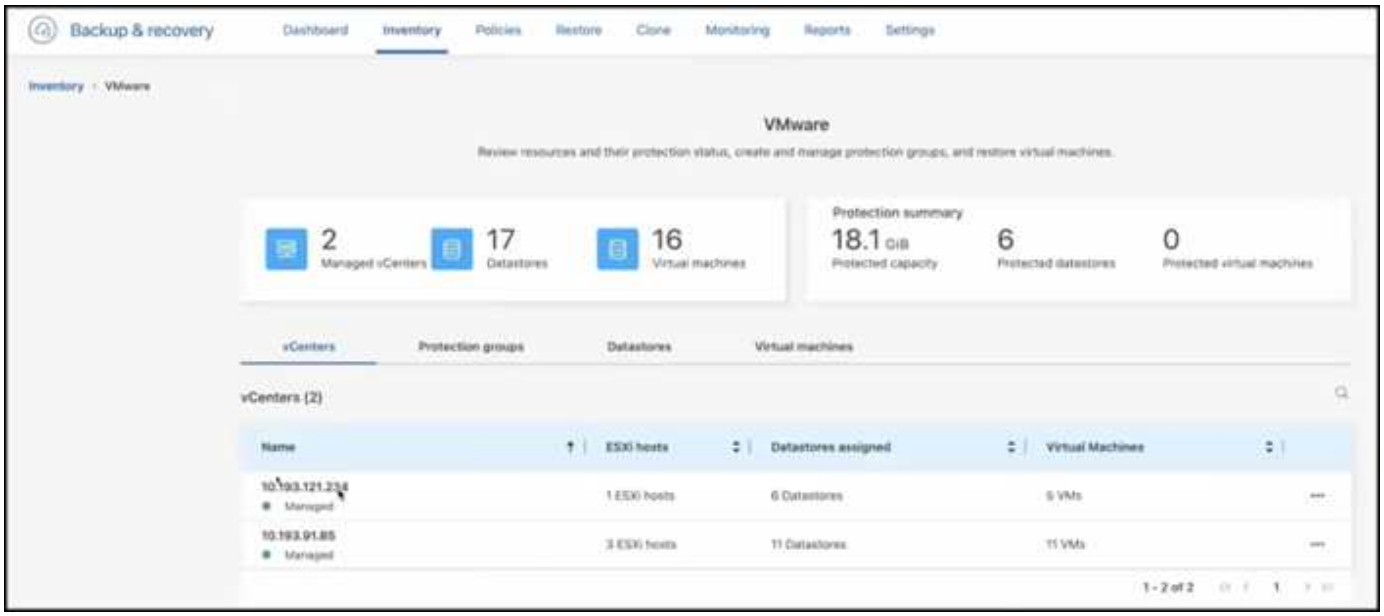
1. Dopo aver importato le risorse VMware dal plug-in SnapCenter , dal menu in alto seleziona **Inventario**.
2. Dalla pagina Inventario, seleziona il vCenter importato che da ora in poi desideri venga gestito BlueXP backup and recovery .

3. Seleziona l'icona Azioni ••• > **Visualizza dettagli** per visualizzare i dettagli del carico di lavoro.
4. Dalla pagina Inventario > carico di lavoro, seleziona l'icona Azioni ••• > **Gestisci** per visualizzare la pagina Gestisci vCenter.

5. Seleziona la casella "Vuoi continuare con la migrazione?" e seleziona **Migra**.

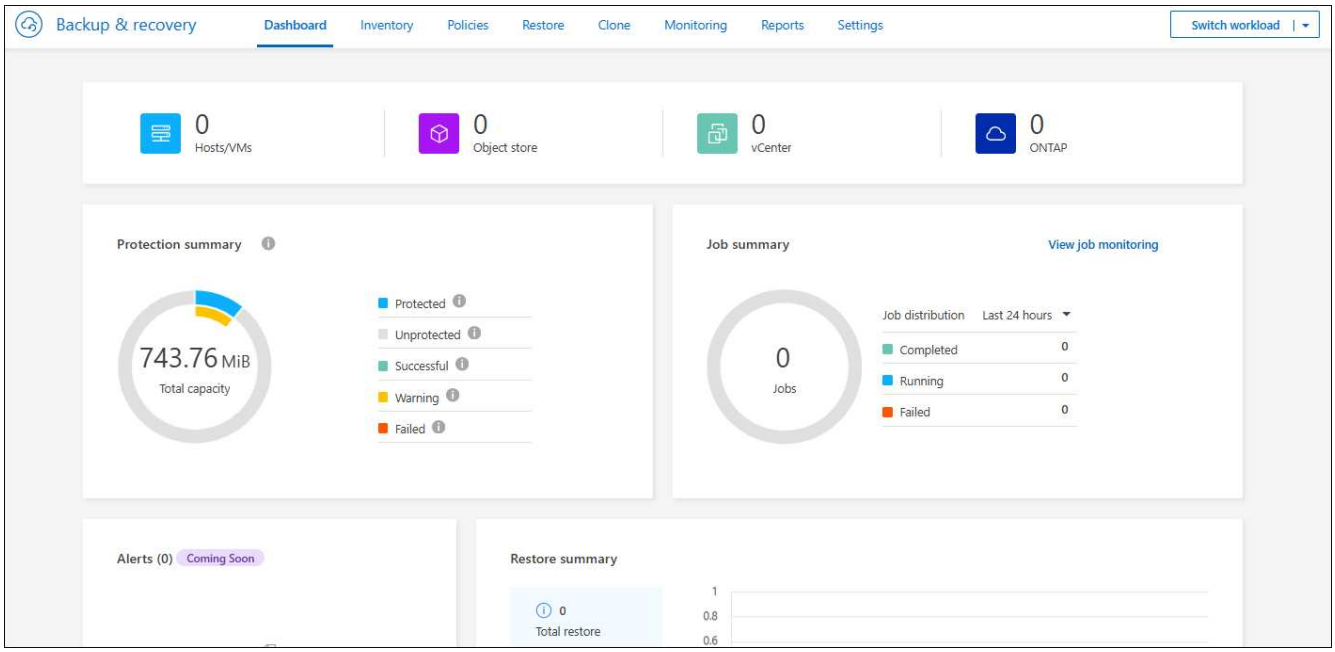
Risultato

La pagina Inventario mostra le risorse vCenter appena gestite.



Vai alla dashboard BlueXP backup and recovery

1. Per visualizzare la Dashboard BlueXP backup and recovery , dal menu in alto, seleziona **Dashboard**.
2. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai nuovi carichi di lavoro scoperti, protetti e sottoposti a backup.



"Scopri cosa ti mostra la Dashboard".

Crea e gestisci gruppi di protezione per carichi di lavoro VMware con BlueXP backup and recovery

Creare gruppi di protezione per gestire le operazioni di backup e ripristino per un set di carichi di lavoro. Un gruppo di protezione è un raggruppamento logico di risorse, quali VM e datastore, che si desidera proteggere insieme.

È possibile eseguire le seguenti attività relative ai gruppi di protezione:

- Crea un gruppo di protezione.
- Visualizza i dettagli della protezione.
- Crea subito un gruppo di protezione. Vedere "Esegui subito il backup dei carichi di lavoro VMware" .
- Sospendere e riprendere la pianificazione del backup di un gruppo di protezione.
- Elimina un gruppo di protezione.

Crea un gruppo di protezione

Raggruppa i carichi di lavoro che desideri proteggere in un gruppo di protezione. È possibile creare un gruppo di protezione per un set di carichi di lavoro di cui si desidera eseguire il backup e il ripristino insieme.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.

2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Specificare un nome per il gruppo di protezione.
7. Selezionare le VM o i database che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.
9. Selezionare il **Criterio di backup** che si desidera applicare al gruppo di protezione.

   Se si desidera creare una policy, selezionare **Crea nuova policy** e seguire le istruzioni per creare una policy. Per ulteriori informazioni, vedere "Creare policy" .

10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

Sospendere la pianificazione del backup di un gruppo di protezione

La sospensione di un gruppo di protezione interrompe i backup pianificati per il gruppo di protezione. Potrebbe essere necessario sospendere un gruppo di protezione se si desidera interrompere temporaneamente i backup per i carichi di lavoro in quel gruppo.

Quando si sospende un gruppo di protezione, lo stato di protezione cambia in "In manutenzione". È possibile riprendere la pianificazione del backup in qualsiasi momento.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.

2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.

5. Seleziona l'icona Azioni ••• > **Sospendi gruppo di protezione**.
6. Rivedi il messaggio di conferma e seleziona **Sospendi**.

Riprendi la pianificazione del backup di un gruppo di protezione

La ripresa di un gruppo di protezione sospeso riavvia i backup pianificati per il gruppo di protezione.

Lo stato di protezione cambia da "In manutenzione" quando si sospende un gruppo di protezione a "Protetto" quando lo si riprende. È possibile riprendere la pianificazione del backup in qualsiasi momento.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.

2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Seleziona l'icona Azioni ••• > **Riprendi gruppo di protezione**.
6. Rivedi il messaggio di conferma e seleziona **Riprendi**.

Risultato

Il sistema convalida le pianificazioni e modifica lo stato di protezione in "Protetto" se le pianificazioni sono valide. Se le pianificazioni non sono valide, il sistema visualizza un messaggio di errore e non riprende il gruppo di protezione.

Elimina un gruppo di protezione

L'eliminazione di un gruppo di protezione comporta la rimozione del gruppo stesso e di tutte le pianificazioni di backup associate. Potrebbe essere necessario eliminare un gruppo di protezione se non è più necessario.

Fasi

1. Dal menu BlueXP backup and recovery , seleziona **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare il gruppo di protezione che si desidera eliminare.
6. Seleziona l'icona Azioni ••• > **Elimina**.
7. Rivedere il messaggio di conferma relativo all'eliminazione dei backup associati e confermare l'eliminazione.

Esegui il backup dei carichi di lavoro VMware con il BlueXP backup and recovery

Esegui il backup delle VM VMware e degli archivi dati dai sistemi ONTAP locali ad Amazon Web Services o StorageGRID per garantire la protezione dei tuoi dati. I backup vengono generati automaticamente e archiviati in un archivio oggetti nel tuo account cloud pubblico o privato.

- Per eseguire il backup dei carichi di lavoro in base a una pianificazione, creare criteri che governino le operazioni di backup e ripristino. Vedere "Creare policy" per istruzioni.
- Creare gruppi di protezione per gestire le operazioni di backup e ripristino per un set di risorse. Vedere "Crea e gestisci gruppi di protezione per carichi di lavoro VMware con BlueXP backup and recovery" per maggiori informazioni.
- Esegui subito il backup dei carichi di lavoro (crea subito un backup su richiesta).

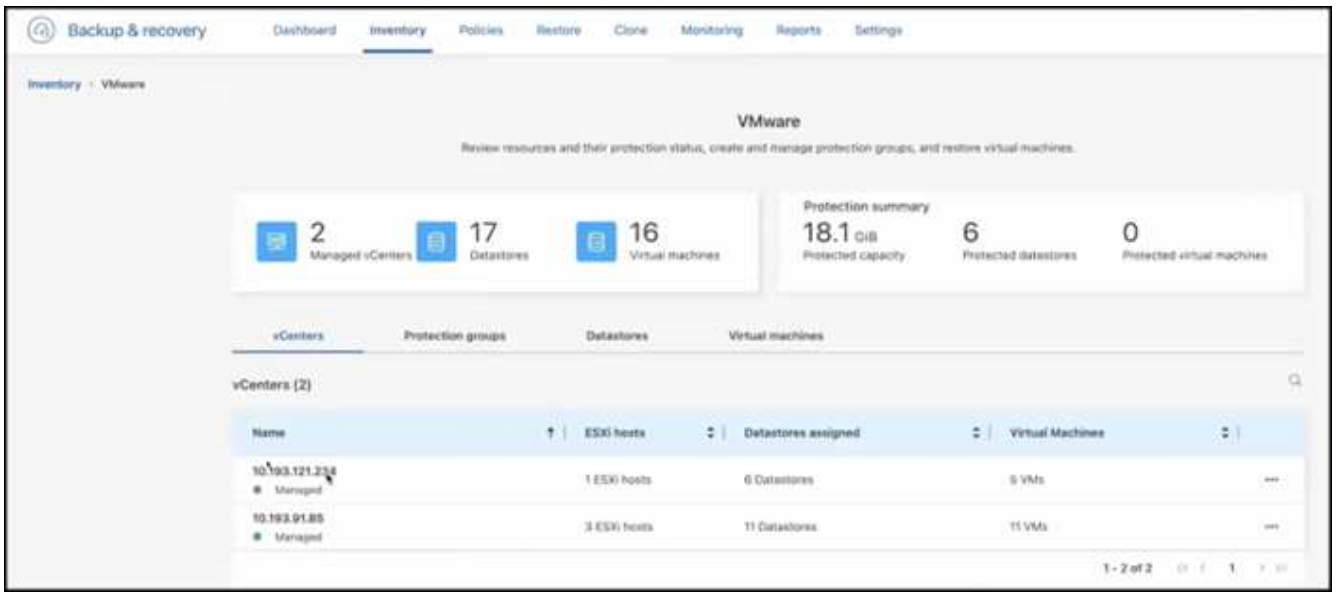
Esegui subito il backup dei carichi di lavoro con un backup on-demand

Crea immediatamente un backup on-demand. Potresti voler eseguire un backup on-demand se stai per apportare modifiche al tuo sistema e vuoi assicurarti di avere un backup prima di iniziare.

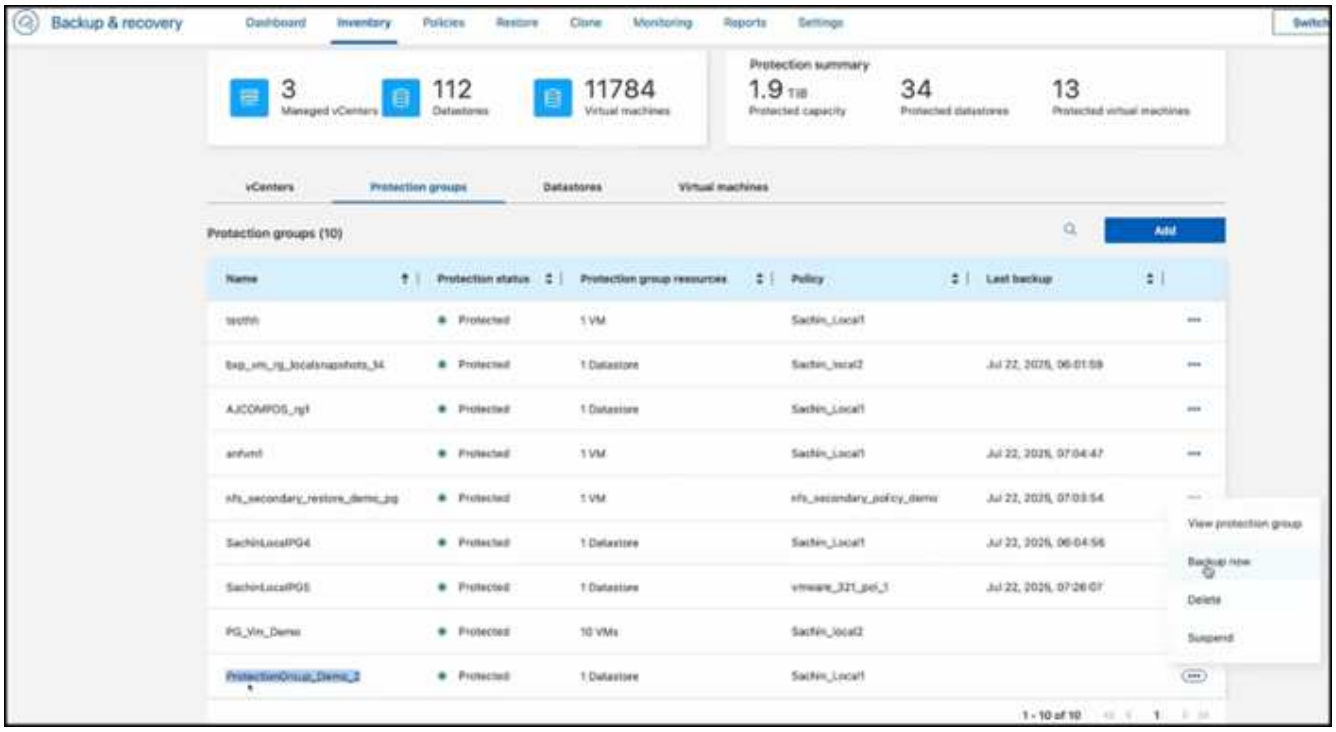
Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

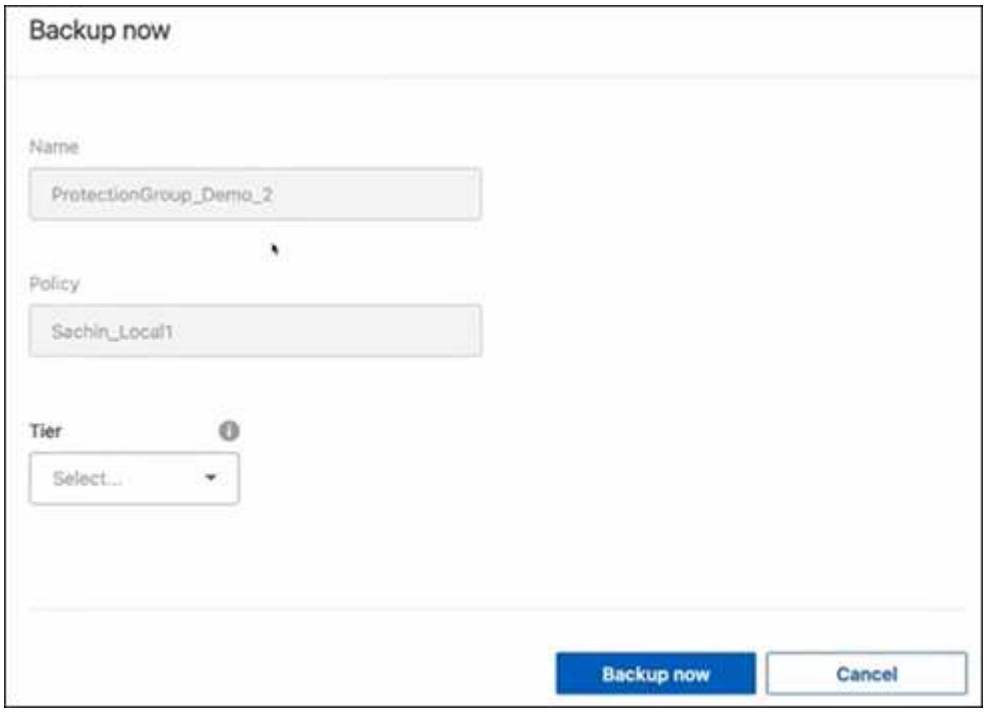
1. Dal menu, seleziona **Inventario**.



2. Selezionare un carico di lavoro per visualizzare i dettagli sulla protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**, **Datastore** o **Macchine virtuali**.



5. Selezionare il gruppo di protezione, gli archivi dati o le macchine virtuali di cui si desidera eseguire il backup.
6. Seleziona l'icona Azioni ••• > **Esegui il backup adesso**.



Il criterio applicato al backup è lo stesso criterio assegnato al gruppo di protezione, al datastore o alla macchina virtuale.

7. Selezionare il livello di pianificazione.
8. Seleziona **Esegui backup adesso**.

Ripristina i carichi di lavoro VMware con il BlueXP backup and recovery

Ripristina i carichi di lavoro VMware da copie snapshot, da un backup del carico di lavoro replicato su un archivio secondario o da backup archiviati in un archivio oggetti utilizzando il BlueXP backup and recovery.

Ripristina da queste posizioni

È possibile ripristinare i carichi di lavoro da diverse posizioni di partenza:

- Ripristina da una posizione primaria (snapshot locale)
- Ripristina da una risorsa replicata su un archivio secondario
- Ripristina da un backup di archiviazione di oggetti

Ripristinare questi punti

È possibile ripristinare i dati in questi punti:

- Ripristina la posizione originale

Considerazioni sul ripristino da storage di oggetti

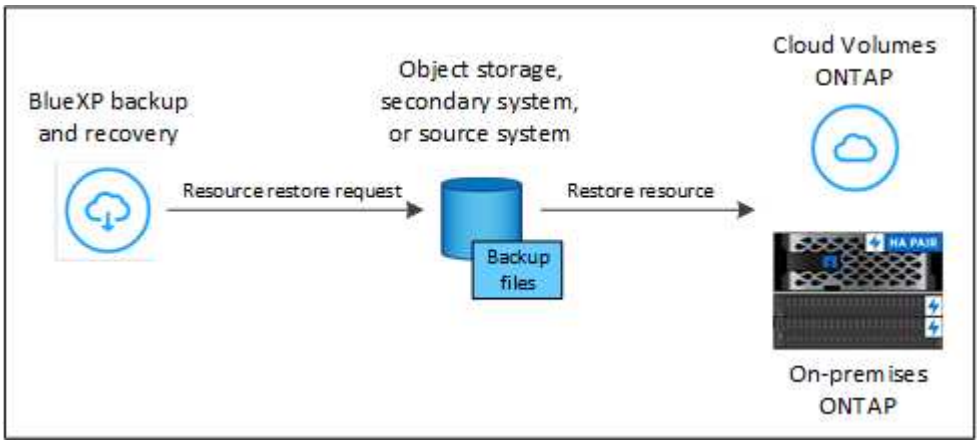
Se selezioni un file di backup nell'archivio oggetti e la protezione ransomware è attiva per quel backup (se hai abilitato DataLock e la protezione ransomware nella policy di backup), ti verrà richiesto di eseguire un ulteriore controllo di integrità sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione.

Per accedere al contenuto del file di backup, ti verranno addebitati costi di uscita aggiuntivi dal tuo provider cloud.

Come funziona il ripristino dei carichi di lavoro

Quando si ripristinano i carichi di lavoro, si verifica quanto segue:

- Quando si ripristina un carico di lavoro da un file di backup locale, il BlueXP backup and recovery creano una *nuova* risorsa utilizzando i dati del backup.
- Quando si esegue il ripristino da un carico di lavoro replicato, è possibile ripristinare il carico di lavoro nell'ambiente di lavoro originale o in un sistema ONTAP locale.



- Quando si ripristina un backup da un archivio di oggetti, è possibile ripristinare i dati nell'ambiente di lavoro originale o in un sistema ONTAP locale.

Dalla pagina Ripristina (nota anche come Cerca e ripristina)*, puoi ripristinare una risorsa anche se non ricordi il nome esatto, la posizione in cui si trova o la data dell'ultima volta in cui era in buone condizioni. È possibile cercare l'istantanea utilizzando i filtri.

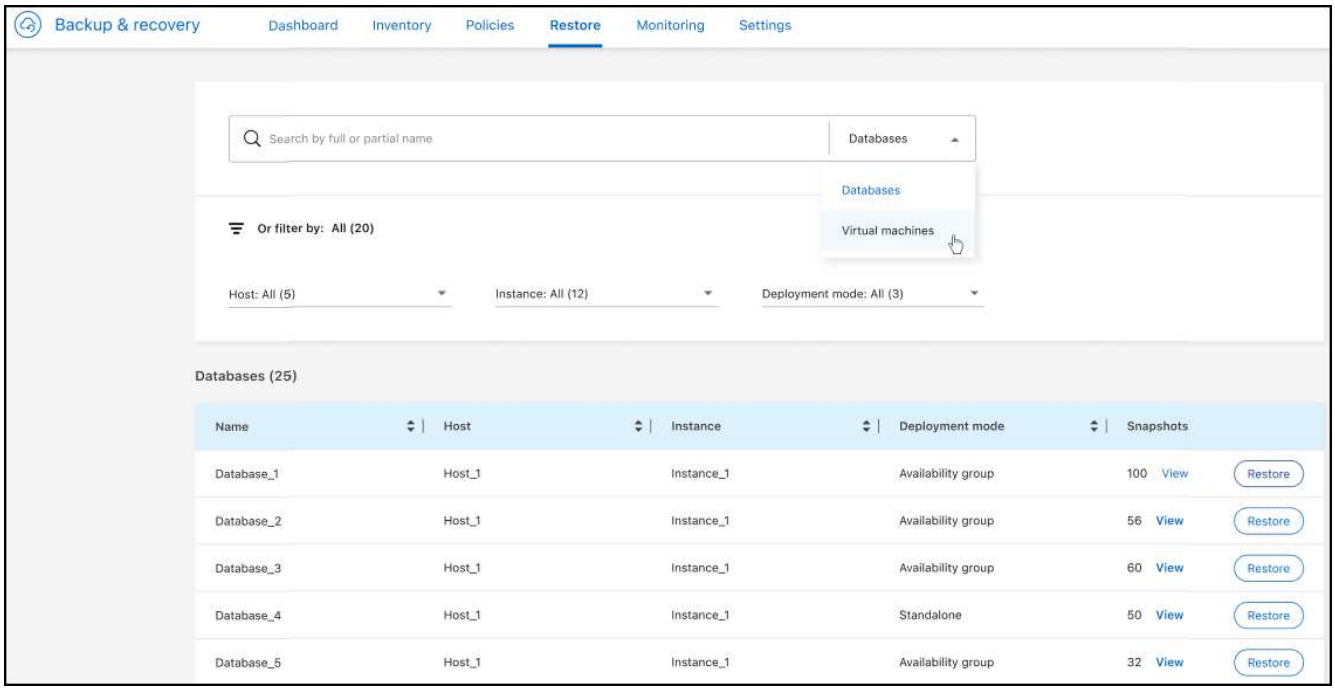
Ripristina i dati del carico di lavoro dall'opzione Ripristina (Cerca e ripristina)

Ripristina i carichi di lavoro VMware utilizzando l'opzione Ripristina. È possibile cercare l'istantanea in base al nome o utilizzando i filtri.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di backup e ripristino, Amministratore di ripristino di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

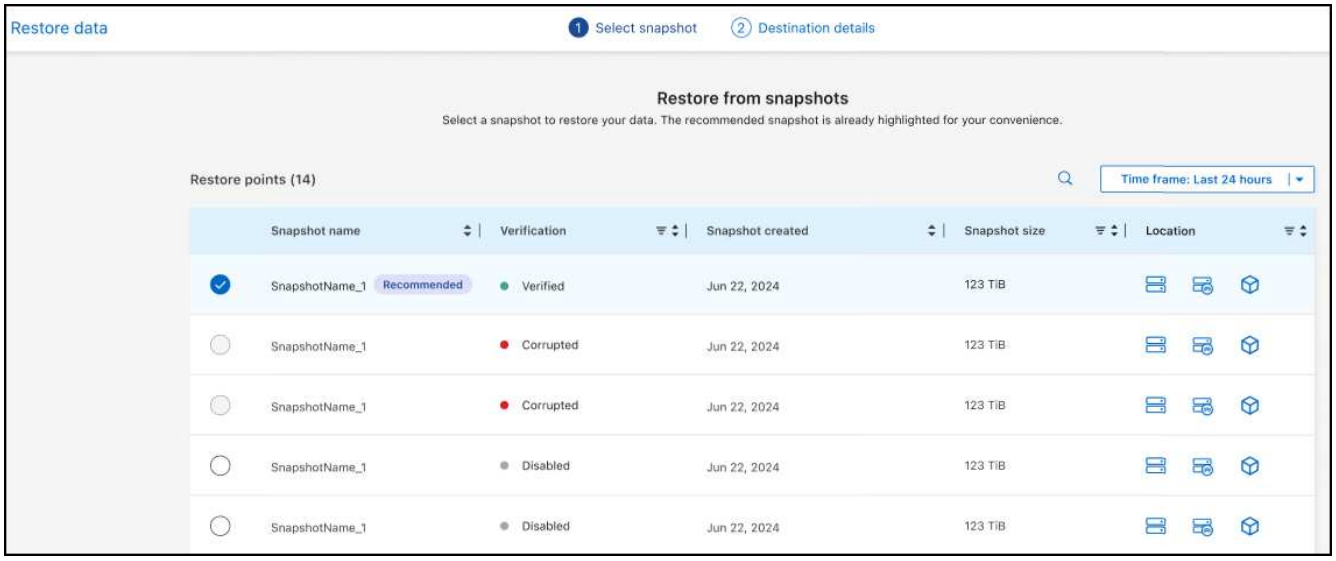
Fasi

1. Dal menu di backup e ripristino BlueXP , seleziona **Ripristina**.



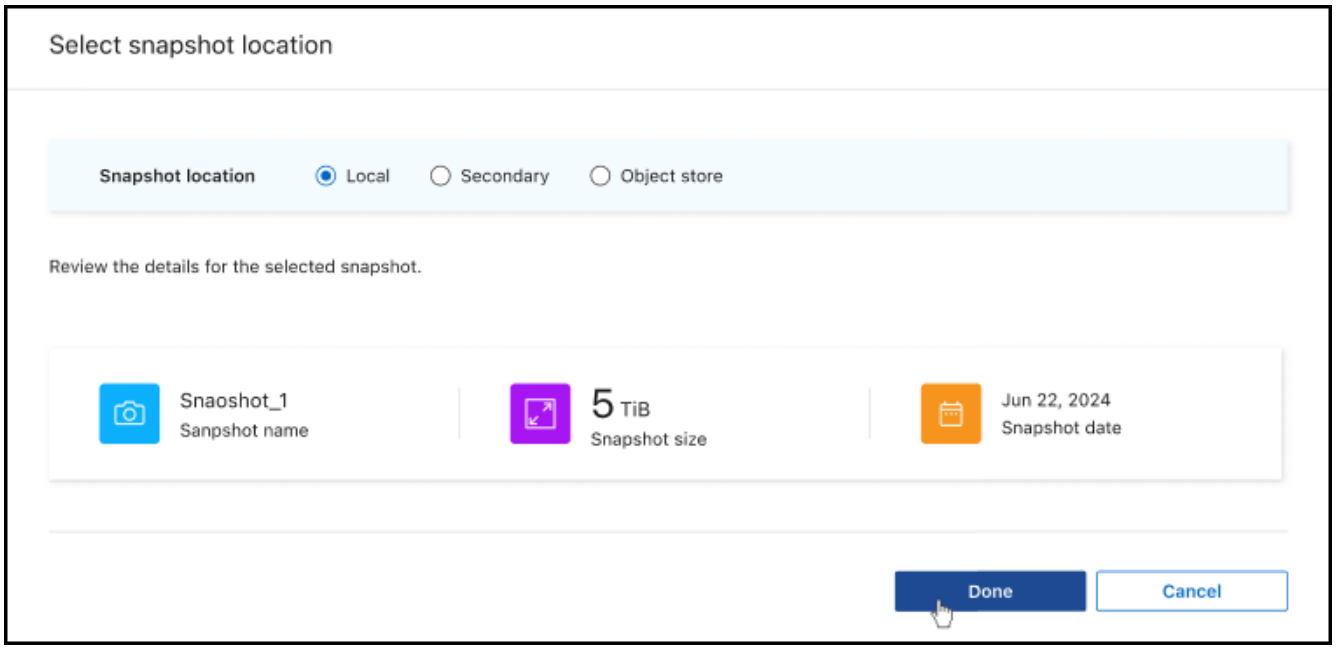
2. Dall'elenco a discesa a destra del campo di ricerca del nome, seleziona **Macchine virtuali**.
3. Immettere il nome della risorsa che si desidera ripristinare oppure filtrare in base al vCenter, al datacenter o al datastore in cui si trova la risorsa da ripristinare.

   Viene visualizzato un elenco di snapshot che corrispondono ai criteri di ricerca.



4. Seleziona lo snapshot che vuoi ripristinare.

   Viene visualizzato un elenco di opzioni di posizione di ripristino.



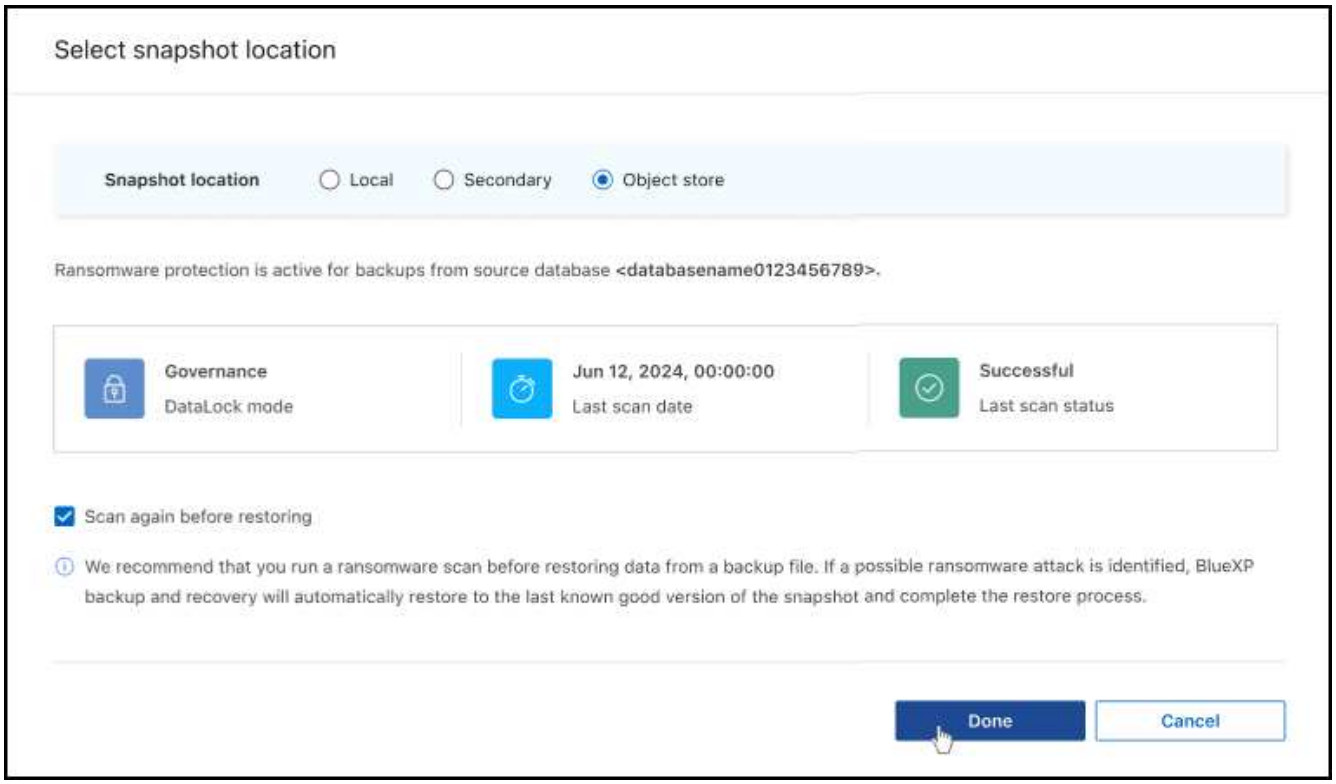
5. Selezionare la posizione di ripristino in cui si desidera ripristinare lo snapshot:

   - Locale: ripristina lo snapshot nella posizione originale.
   - Archiviazione secondaria: ripristina lo snapshot in una posizione di archiviazione secondaria.

     Se si sceglie l'archiviazione secondaria, immettere le informazioni sulla posizione di origine e di destinazione, nonché la posizione di origine e secondaria per i log.

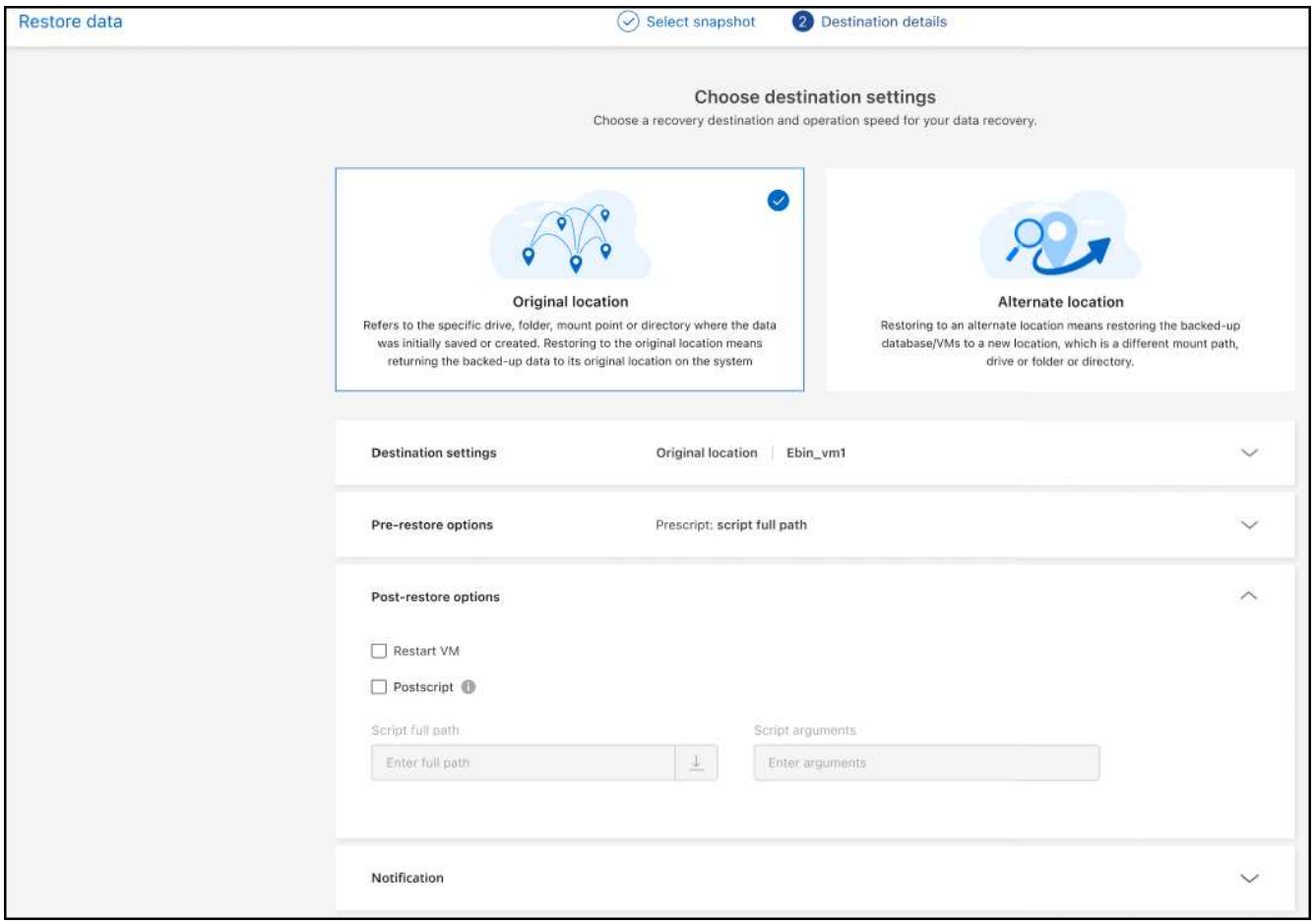
   - Archiviazione oggetti: ripristina lo snapshot in una posizione di archiviazione oggetti.

     Se si sceglie l'archiviazione di oggetti, verificare se si desidera eseguire nuovamente la scansione dello snapshot prima del ripristino.



6. Selezionare **Fine** o **Avanti** per procedere alla pagina delle impostazioni di destinazione del ripristino.

   Successivamente, puoi scegliere le impostazioni di destinazione e le opzioni pre-ripristino e post-ripristino.



Selezione della destinazione

1. Selezionare le impostazioni di destinazione e le opzioni pre-ripristino e post-ripristino.

Ripristina nella posizione originale

Nella pagina dei dettagli della destinazione di ripristino, immettere le seguenti informazioni:

1. **Abilita ripristino rapido**: seleziona questa opzione per eseguire un'operazione di ripristino rapido. I volumi e i dati ripristinati saranno disponibili immediatamente. Non utilizzare questa opzione su volumi che richiedono prestazioni elevate perché durante il processo di ripristino rapido l'accesso ai dati potrebbe essere più lento del solito.
2. **Opzioni pre-ripristino**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino e tutti gli argomenti accettati dallo script.
3. **Opzioni post-ripristino**:
   - **Riavvia VM**: selezionare questa opzione per riavviare la VM al termine dell'operazione di ripristino e dopo l'applicazione dello script post-ripristino.
   - **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.
4. Sezione **Notifiche**:
   - **Abilita notifiche e-mail**: seleziona questa opzione per ricevere notifiche e-mail sull'operazione di ripristino e indica il tipo di notifiche che desideri ricevere.
5. Selezionare **Restore** (Ripristina).

Ripristina in posizione alternativa

Non disponibile per l'anteprima VMware.

1. Selezionare **Restore** (Ripristina).

Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, super amministratore di backup e ripristino, amministratore di ripristino di backup e ripristino. "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Proteggi i carichi di lavoro VMware (con il plug-in SnapCenter per VMware)

Protezione dei carichi di lavoro delle macchine virtuali nella panoramica BlueXP backup and recovery

Proteggi i carichi di lavoro delle tue macchine virtuali con il BlueXP backup and recovery. Il BlueXP backup and recovery offrono operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con la VM per VM, datastore e VMDK.

È possibile eseguire il backup dei datastore su Amazon Web Services S3, Microsoft Azure Blob, piattaforma cloud Google e StorageGRID e ripristinare le macchine virtuali nel plug-in SnapCenter on-premise per l'host VMware vSphere.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Per istruzioni sulla protezione dei carichi di lavoro delle macchine virtuali, vedere i seguenti argomenti:

- "Creare una policy per i carichi di lavoro VMware"
- "Eseguire il backup dei datastore VMware su Amazon Web Services"
- "Eseguire il backup dei datastore VMware su Microsoft Azure"
- "Esegui il backup dei datastore VMware su Google Cloud Platform"
- "Eseguire il backup dei datastore VMware su StorageGRID"
- "Ripristinare i carichi di lavoro VMware"
- "Gestisci la protezione per i carichi di lavoro VMware"

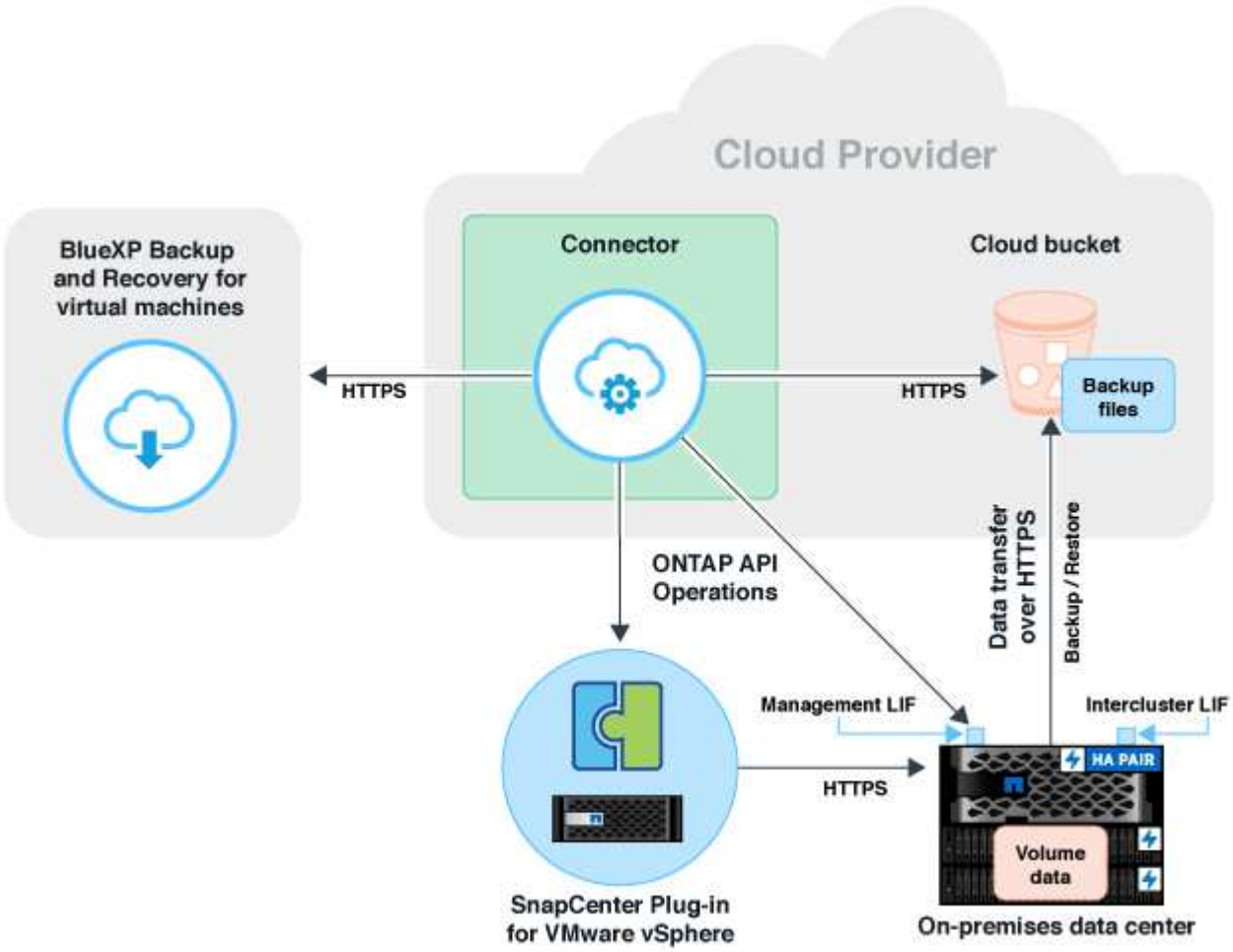
Prerequisiti per i carichi di lavoro delle macchine virtuali nel BlueXP backup and recovery

Prima di iniziare a proteggere i carichi di lavoro delle macchine virtuali con il BlueXP backup and recovery, assicurati di soddisfare i seguenti prerequisiti:

- Plug-in SnapCenter per VMware vSphere 4.6P1 o versione successiva
  - Si consiglia di utilizzare il plug-in SnapCenter per VMware vSphere 4.7P1 o versione successiva per eseguire il backup dei datastore dallo storage secondario on-premise.
- ONTAP 9.8 o versione successiva
- BlueXP
- Sono supportati gli archivi dati NFS e VMFS. I vVol non sono supportati.
- Per il supporto VMFS, il SnapCenter Plug-in for VMware vSphere deve essere in esecuzione sulla versione 4.9 o successiva. Assicurarsi di eseguire un backup del datastore VMFS se il plug-in SnapCenter per l'host VMware vSphere è stato aggiornato da una versione precedente alla release 4.9.
- Almeno un backup dovrebbe essere stato eseguito nel plug-in SnapCenter per VMware vSphere 4.6P1.
- Almeno una policy giornaliera, settimanale o mensile nel plug-in SnapCenter per VMware vSphere senza etichetta o etichetta uguale a quella della policy macchine virtuali in BlueXP.
- Per una policy predefinita, il livello di pianificazione dovrebbe essere lo stesso per il datastore nel SnapCenter Plug-in for VMware vSphere e nel cloud.
- Assicurarsi che non vi siano volumi FlexGroup nell'archivio dati perché il backup e il ripristino dei volumi FlexGroup non sono supportati.
- Disattivare "**_Recent**" sui gruppi di risorse richiesti. Se "**_Recent**" è attivato per il gruppo di risorse, i backup di tali gruppi di risorse non possono essere utilizzati per la protezione dei dati nel cloud e, successivamente, non possono essere utilizzati per l'operazione di ripristino.
- Assicurarsi che il datastore di destinazione in cui verrà ripristinata la macchina virtuale disponga di spazio sufficiente per ospitare una copia di tutti i file delle macchine virtuali, ad esempio VMDK, VMX, VMSD e così via.
- Assicurarsi che l'archivio dati di destinazione non abbia file di macchine virtuali obsoleti nel formato restore_xxx_xxxxxx_filename degli errori dell'operazione di ripristino precedente. Eliminare i file obsoleti prima di avviare un'operazione di ripristino.

- Per distribuire un connettore con proxy configurato, assicurarsi che tutte le chiamate dei connettori in uscita siano instradate attraverso il server proxy.
- Se un volume di cui è stato eseguito il backup di un datastore è già protetto dalla scheda Volumes (backup e recovery di BlueXP → Volumes), non è possibile proteggere nuovamente lo stesso datastore dalla scheda Virtual Machine (backup e recovery di BlueXP → Virtual Machine).

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



Registra il SnapCenter Plug-in for VMware vSphere da utilizzare con il BlueXP backup and recovery

È necessario registrare il plug-in SnapCenter per l'host VMware vSphere nel backup e ripristino BlueXP affinché i datastore e le macchine virtuali vengano visualizzati. Solo un utente con accesso amministrativo può registrare il plug-in SnapCenter per l'host VMware vSphere.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.
2. Dal menu a discesa **Impostazioni**, seleziona * SnapCenter Plug-in for VMware vSphere*.
3. Selezionare **Registra il SnapCenter Plug-in for VMware vSphere**.
4. Specificare i seguenti dettagli:
   a. Nel campo Plug-in SnapCenter per VMware vSphere, specificare l'FQDN o l'indirizzo IP del plug-in SnapCenter per l'host VMware vSphere.
   b. Nel campo porta, specificare il numero di porta su cui è in esecuzione il plug-in SnapCenter per l'host VMware vSphere.

      Assicurarsi che la comunicazione sia aperta tra il plug-in SnapCenter on-premise per l'host VMware vSphere in esecuzione sulla porta 8144 predefinita e l'istanza del connettore BlueXP che potrebbe essere in esecuzione in qualsiasi provider cloud (servizi Web Amazon, Microsoft Azure, piattaforma cloud Google) o on-premise.

   c. Nel campo Nome utente e Password, specificare le credenziali dell'utente vCenter con il ruolo di amministratore.
5. Selezionare **Registra**.

Al termine

Selezionare **Backup e ripristino** > **Macchine virtuali** per visualizzare tutti i datastore e le macchine virtuali protetti mediante il SnapCenter Plug-in for VMware vSphere .

Creare una policy per eseguire il backup degli archivi dati nel BlueXP backup and recovery

È possibile creare una policy o utilizzare una delle seguenti policy predefinite disponibili nel backup e ripristino di BlueXP.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

- Se non si desidera modificare i criteri predefiniti, è necessario creare dei criteri.
- Per spostare i backup dall'archivio di oggetti allo storage di archiviazione, è necessario eseguire ONTAP 9.10.1 o versione successiva e i servizi Web Amazon o Microsoft Azure devono essere il provider di cloud.
- È necessario configurare il Tier di accesso all'archivio per ciascun provider di cloud.

A proposito di questa attività

In BlueXP sono disponibili i seguenti criteri predefiniti:

Nome policy	Etichetta	Valore di conservazione
LTR giornaliero di 1 anno (conservazione a lungo termine)	Ogni giorno	366

Nome policy	Etichetta	Valore di conservazione
5 anni di LTR giornaliero	Ogni giorno	1830
LTR settimanale di 7 anni	Settimanale	370
LTR mensile di 10 anni	Mensile	120

Fasi

1. Nella pagina macchine virtuali, dall'elenco a discesa Impostazioni, selezionare **Criteri**.
2. Selezionare **Crea policy**.
3. Nella sezione Dettagli policy, specificare il nome del policy.
4. Nella sezione conservazione, selezionare uno dei tipi di conservazione e specificare il numero di backup da conservare.
5. Selezionare Primary (principale) o Secondary (secondario) come origine dello storage di backup.
6. (Facoltativo) se si desidera spostare i backup dall'archivio di oggetti allo storage di archiviazione dopo un certo numero di giorni per l'ottimizzazione dei costi, selezionare la casella di controllo **Tier backups to Archival** e immettere il numero di giorni dopo i quali il backup deve essere archiviato.
7. Selezionare **Crea**.

Non è possibile modificare o eliminare una policy associata a un datastore.

Eseguire il backup degli archivi dati su Amazon Web Services nel BlueXP backup and recovery

È possibile eseguire il backup e l'archiviazione di uno o più datastore con il backup e il ripristino di BlueXP su Amazon Web Services per migliorare l'efficienza di archiviazione e la transizione al cloud.

Se il datastore è associato a un criterio di archiviazione, è possibile selezionare il livello di archiviazione. I livelli di archiviazione supportati sono Glacier e Glacier Deep.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

Assicurati di aver soddisfatto tutti i requisiti "requisiti di protezione della macchina virtuale" prima di eseguire il backup degli archivi dati sul cloud.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.
2. Selezionare ••• corrispondente al datastore di cui si desidera effettuare il backup e fare clic su **Attiva backup**.
3. Nella pagina Assegna policy, seleziona la policy e fai clic su **Avanti**.

4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per uno dei datastore, è possibile riutilizzarlo per tutti gli altri datastore che risiedono nello stesso cluster ONTAP.

   a. Selezionare **Aggiungi ambiente di lavoro** corrispondente all'SVM.
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.
   c. Selezionare **Aggiungi ambiente di lavoro**.
5. Selezionare **Amazon Web Services** per configurarlo come provider cloud.
   a. Specificare l'account AWS.
   b. Nel campo AWS Access Key (chiave di accesso AWS), specificare la chiave per la crittografia dei dati.
   c. Nel campo AWS Secret Key (chiave segreta AWS), specificare la password per la crittografia dei dati.
   d. Selezionare la regione in cui si desidera creare i backup.
   e. Specificare gli indirizzi IP della LIF di gestione del cluster che sono stati aggiunti come ambienti di lavoro.
   f. Selezionare il livello di archiviazione.

      Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non è possibile configurarla in un secondo momento.
6. Controlla i dettagli e seleziona **Attiva backup**.

Esegui il backup degli archivi dati su Microsoft Azure con il backup e il ripristino di BlueXP

È possibile eseguire il backup di uno o più datastore su Microsoft Azure integrando il plug-in SnapCenter per l'host VMware vSphere con il backup e il ripristino di BlueXP. In questo modo, gli amministratori delle macchine virtuali potranno eseguire facilmente e rapidamente il backup e l'archiviazione dei dati per l'efficienza dello storage e accelerare la transizione al cloud.

Se il datastore è associato a un criterio di archiviazione, viene fornita un'opzione per selezionare il livello di archiviazione. Il Tier di archiviazione supportato è Azure Archive Blob Storage.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

Assicurati di aver soddisfatto tutti i requisiti "requisiti di protezione della macchina virtuale" prima di eseguire il backup degli archivi dati sul cloud.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.

2. Selezionare ••• corrispondente al datastore di cui si desidera effettuare il backup e selezionare **Attiva backup**.
3. Nella pagina Assegna policy, seleziona la policy e fai clic su **Avanti**.
4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per uno dei datastore, è possibile riutilizzarlo per tutti gli altri datastore che risiedono nello stesso cluster ONTAP.

   a. Selezionare **Aggiungi ambiente di lavoro** corrispondente all'SVM.
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.
   c. Selezionare **Aggiungi ambiente di lavoro**.
5. Selezionare **Microsoft Azure** per configurarlo come provider cloud.
   a. Specificare l'ID dell'abbonamento Azure.
   b. Selezionare la regione in cui si desidera creare i backup.
   c. Creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente.
   d. Specificare gli indirizzi IP della LIF di gestione del cluster che sono stati aggiunti come ambienti di lavoro.
   e. Selezionare il livello di archiviazione.

      Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività che si esegue una sola volta e non sarà possibile impostarla in seguito.
6. Controlla i dettagli e seleziona **Attiva backup**.

Esegui il backup degli archivi dati su Google Cloud Platform con il backup e il ripristino di BlueXP

È possibile eseguire il backup di uno o più datastore su Google Cloud Platform integrando il plug-in SnapCenter per l'host VMware vSphere con il backup e il ripristino di BlueXP. In questo modo, gli amministratori delle macchine virtuali potranno eseguire facilmente e rapidamente il backup e l'archiviazione dei dati per l'efficienza dello storage e accelerare la transizione al cloud.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

Assicurati di aver soddisfatto tutti i requisiti "requisiti di protezione della macchina virtuale" prima di eseguire il backup degli archivi dati sul cloud.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.

2. Selezionare ••• corrispondente al datastore di cui si desidera effettuare il backup e selezionare **Attiva backup**.
3. Nella pagina Assegna policy, seleziona la policy e fai clic su **Avanti**.
4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per uno dei datastore, è possibile riutilizzarlo per tutti gli altri datastore che risiedono nello stesso cluster ONTAP.

   a. Selezionare **Aggiungi ambiente di lavoro** corrispondente all'SVM.
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.
   c. Selezionare **Aggiungi ambiente di lavoro**.
5. Selezionare **Google Cloud Platform** per configurarla come cloud provider.
   a. Seleziona il progetto Google Cloud in cui desideri creare il bucket di storage Google Cloud per i backup.
   b. Nel campo Google Cloud Access Key, specificare la chiave.
   c. Nel campo Google Cloud Secret Key, specificare la password.
   d. Selezionare la regione in cui si desidera creare i backup.
   e. Specificare lo spazio IP.
6. Controlla i dettagli e seleziona **Attiva backup**.

Esegui il backup degli archivi dati su StorageGRID con il backup e il ripristino di BlueXP

È possibile eseguire il backup di uno o più datastore su StorageGRID integrando il plug-in SnapCenter per l'host VMware vSphere con il backup e il ripristino di BlueXP. In questo modo, gli amministratori delle macchine virtuali potranno eseguire facilmente e rapidamente il backup e l'archiviazione dei dati per l'efficienza dello storage e accelerare la transizione al cloud.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

Assicurati di aver soddisfatto tutti i requisiti "requisiti di protezione della macchina virtuale" prima di eseguire il backup degli archivi dati sul cloud.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.
2. Selezionare ••• corrispondente al datastore di cui si desidera effettuare il backup e fare clic su **Attiva backup**.
3. Nella pagina Assegna policy, seleziona la policy e fai clic su **Avanti**.

4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per uno dei datastore, è possibile riutilizzarlo per tutti gli altri datastore che risiedono nello stesso cluster ONTAP.

   a. Selezionare **Aggiungi ambiente di lavoro** corrispondente all'SVM.
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.
   c. Selezionare **Aggiungi ambiente di lavoro**.
5. Selezionare **StorageGRID**.
   a. Specificare l'IP dello Storage Server.
   b. Selezionare la chiave di accesso e la chiave segreta.
6. Controlla i dettagli e seleziona **Attiva backup**.

Gestisci la protezione di datastore e VM nel BlueXP backup and recovery

Con il backup e il ripristino di BlueXP è possibile visualizzare policy, archivi dati e macchine virtuali prima di eseguire il backup e il ripristino dei dati. A seconda delle modifiche apportate a database, policy o gruppi di risorse, è possibile visualizzare gli aggiornamenti dall'interfaccia utente di BlueXP.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Visualizzare le policy

È possibile visualizzare tutti i criteri predefiniti. Per ciascuno di questi criteri, quando si visualizzano i dettagli, vengono elencati tutti i criteri e le macchine virtuali associati.

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.
2. Dal menu a discesa **Impostazioni**, seleziona **Criteri**.
3. Selezionare **Visualizza dettagli** corrispondente alla polizza di cui si desidera visualizzare i dettagli.

Vengono elencati i criteri e le macchine virtuali associati.

Visualizza datastore e macchine virtuali

Vengono visualizzati i datastore e le macchine virtuali protetti mediante il plug-in SnapCenter registrato per l'host VMware vSphere.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali** > **Impostazioni** > * SnapCenter Plug-in for VMware vSphere*.
2. Selezionare il SnapCenter Plug-in for VMware vSphere per il quale si desidera visualizzare i datastore e le

macchine virtuali.

Annullare la protezione dei datastore

Puoi annullare la protezione di un datastore già protetto in precedenza. Puoi annullare la protezione di un datastore quando vuoi eliminare i backup del cloud o non eseguirne più il backup nel cloud. Dopo il successo della mancata protezione, il datastore può essere nuovamente protetto.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali**.
2. Seleziona l'icona Azioni ••• corrispondente al datastore di cui si desidera rimuovere la protezione e selezionare **Rimuovi protezione**.

Modificare il plug-in SnapCenter per l'istanza di VMware vSphere

È possibile modificare i dettagli del plug-in SnapCenter per host VMware vSphere in BlueXP.

Fasi

1. Nell'interfaccia utente BlueXP , seleziona **Protezione** > **Backup e ripristino** > **Macchine virtuali** > **Impostazioni** > * SnapCenter Plug-in for VMware vSphere*.
2. Seleziona l'icona Azioni ••• e seleziona **Modifica**.
3. Modificare i dettagli come richiesto.
4. Selezionare **Salva**.

Aggiorna risorse e backup

Se si desidera visualizzare gli ultimi datastore e backup aggiunti all'applicazione, è necessario aggiornare le risorse e i backup. In questo modo si avvia il rilevamento delle risorse e dei backup e vengono visualizzati i dettagli più recenti.

1. Selezionare **Backup e ripristino** > **Macchine virtuali**.
2. Dal menu a discesa **Impostazioni**, seleziona * SnapCenter Plug-in for VMware vSphere*.
3. Seleziona l'icona Azioni ••• corrispondente al SnapCenter Plug-in for VMware vSphere e selezionare **Aggiorna risorse e backup**.

Aggiornare il criterio o il gruppo di risorse

In caso di modifica del criterio o del gruppo di risorse, è necessario aggiornare la relazione di protezione.

1. Selezionare **Backup e ripristino** > **Macchine virtuali**.
2. Seleziona l'icona Azioni ••• corrispondente al datastore e selezionare **Aggiorna protezione**.

Annullare la registrazione del plug-in SnapCenter per l'host VMware vSphere

Tutti i datastore e le macchine virtuali associati al plug-in SnapCenter per host VMware vSphere non saranno protetti.

1. Selezionare **Backup e ripristino** > **Macchine virtuali**.
2. Dal menu a discesa **Impostazioni**, seleziona * SnapCenter Plug-in for VMware vSphere*.
3. Seleziona l'icona Azioni ••• corrispondente al SnapCenter Plug-in for VMware vSphere e selezionare

Annulla registrazione.

Monitorare i lavori

Per tutte le operazioni di backup e recovery di BlueXP vengono create delle job. È possibile monitorare tutti i lavori e tutte le sottoattività eseguite come parte di ciascuna attività.

1. Selezionare **Backup e ripristino** > **Monitoraggio processi**.

   Quando si avvia un'operazione, viene visualizzata una finestra che indica che il processo è stato avviato. È possibile selezionare il collegamento per monitorare il lavoro.

2. Selezionare l'attività principale per visualizzare le attività secondarie e lo stato di ciascuna di esse.

Ripristina i dati delle macchine virtuali con il BlueXP backup and recovery

È possibile ripristinare i dati delle macchine virtuali dal cloud al vCenter locale con il backup e il ripristino di BlueXP. È possibile ripristinare la macchina virtuale nella stessa posizione esatta da cui è stato eseguito il backup o in una posizione alternativa. Se il backup della macchina virtuale è stato eseguito utilizzando i criteri di archiviazione, è possibile impostare la priorità di ripristino dell'archivio.

Non è possibile ripristinare le macchine virtuali che si estendono tra i datastore.

NOTA Per passare da e verso i carichi di lavoro BlueXP backup and recovery , fare riferimento a "Passa a diversi carichi di lavoro BlueXP backup and recovery" .

Prima di iniziare

- Assicurati di aver soddisfatto tutti i requisiti "requisiti di protezione della macchina virtuale" prima di eseguire il backup degli archivi dati sul cloud.
- Se si esegue il ripristino in una posizione alternativa:
  - Verificare che i vCenter di origine e di destinazione siano in modalità collegata.
  - Verificare che i dettagli del cluster di origine e di destinazione siano aggiunti in BlueXP Canvas e in modalità collegata nei vCenter in entrambi i plug-in SnapCenter per l'host VMware vSphere.
  - Assicurarsi che l'ambiente di lavoro (WE) sia aggiunto in corrispondenza della posizione alternativa in BlueXP Canvas.

Fasi

1. Nell'interfaccia utente BlueXP , selezionare **Protezione** > **Backup e ripristino** > **Macchine virtuali** > * SnapCenter Plug-in for VMware vSphere* e selezionare l'host SnapCenter Plug-in for VMware vSphere .

   Se la macchina virtuale di origine viene spostata in un'altra posizione (vMotion) e l'utente attiva un ripristino della macchina virtuale da BlueXP, la macchina virtuale viene ripristinata nella posizione di origine da cui è stato eseguito il backup.

1. Puoi ripristinare la macchina virtuale nella posizione originale o in una posizione alternativa dal datastore o dalle macchine virtuali:

Se si desidera ripristinare la macchina virtuale…	Eseguire questa operazione…
nella posizione originale dal datastore	1. Seleziona l'icona Azioni ••• corrispondente al datastore che si desidera ripristinare e fare clic su **Visualizza dettagli**. 2. Selezionare **Ripristina** corrispondente al backup che si desidera ripristinare. 3. Selezionare la macchina virtuale che si desidera ripristinare dal backup e selezionare **Avanti**. 4. Assicurarsi che sia selezionato **Originale** e selezionare **Continua**. 5. Se la macchina virtuale è protetta mediante un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **Priorità di ripristino archivio** e selezionare **Avanti**. La priorità di ripristino dell'archivio supportata per Amazon Web Services è alta, standard e bassa e la priorità di ripristino dell'archivio supportata per Microsoft Azure è alta e standard. 6. Rivedi i dettagli e seleziona **Ripristina**.
in una posizione alternativa dal datastore	1. Seleziona l'icona Azioni ••• corrispondente al datastore che si desidera ripristinare e selezionare **Visualizza dettagli**. 2. Selezionare **Ripristina** corrispondente al backup che si desidera ripristinare. 3. Selezionare la macchina virtuale che si desidera ripristinare dal backup e selezionare **Avanti**. 4. Selezionare **alternativa**. 5. Selezionare vCenter Server, host ESXi, datastore e rete alternativi. 6. Dopo il ripristino, specificare un nome per la macchina virtuale e selezionare **Continua**. 7. Se la macchina virtuale è protetta mediante un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **Priorità di ripristino archivio** e selezionare **Avanti**. La priorità di ripristino dell'archivio supportata per Amazon Web Services è alta, standard e bassa e la priorità di ripristino dell'archivio supportata per Microsoft Azure è alta e standard. 8. Rivedi i dettagli e seleziona **Ripristina**.

Se si desidera ripristinare la macchina virtuale…	Eseguire questa operazione…
nella posizione originale dalle macchine virtuali	1. Seleziona l'icona Azioni ••• corrispondente alla macchina virtuale che si desidera ripristinare e selezionare **Ripristina**. 2. Selezionare il backup tramite il quale si desidera ripristinare la macchina virtuale. 3. Assicurarsi che sia selezionato **Originale** e selezionare **Continua**. 4. Se la macchina virtuale è protetta mediante un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **Priorità di ripristino archivio** e selezionare **Avanti**. La priorità di ripristino dell'archivio supportata per Amazon Web Services è alta, standard e bassa e la priorità di ripristino dell'archivio supportata per Microsoft Azure è alta e standard. 5. Rivedi i dettagli e seleziona **Ripristina**.
in una posizione alternativa dalle macchine virtuali	1. Seleziona l'icona Azioni ••• corrispondente alla macchina virtuale che si desidera ripristinare e selezionare **Ripristina**. 2. Selezionare il backup tramite il quale si desidera ripristinare la macchina virtuale. 3. Selezionare **alternativa**. 4. Selezionare vCenter Server, host ESXi, datastore e rete alternativi. 5. Dopo il ripristino, specificare un nome per la macchina virtuale e selezionare **Continua**. 6. Se la macchina virtuale è protetta mediante un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **Priorità di ripristino archivio** e selezionare **Avanti**. La priorità di ripristino dell'archivio supportata per Amazon Web Services è alta, standard e bassa e la priorità di ripristino dell'archivio supportata per Microsoft Azure è alta e standard. 7. Rivedi i dettagli e seleziona **Ripristina**.

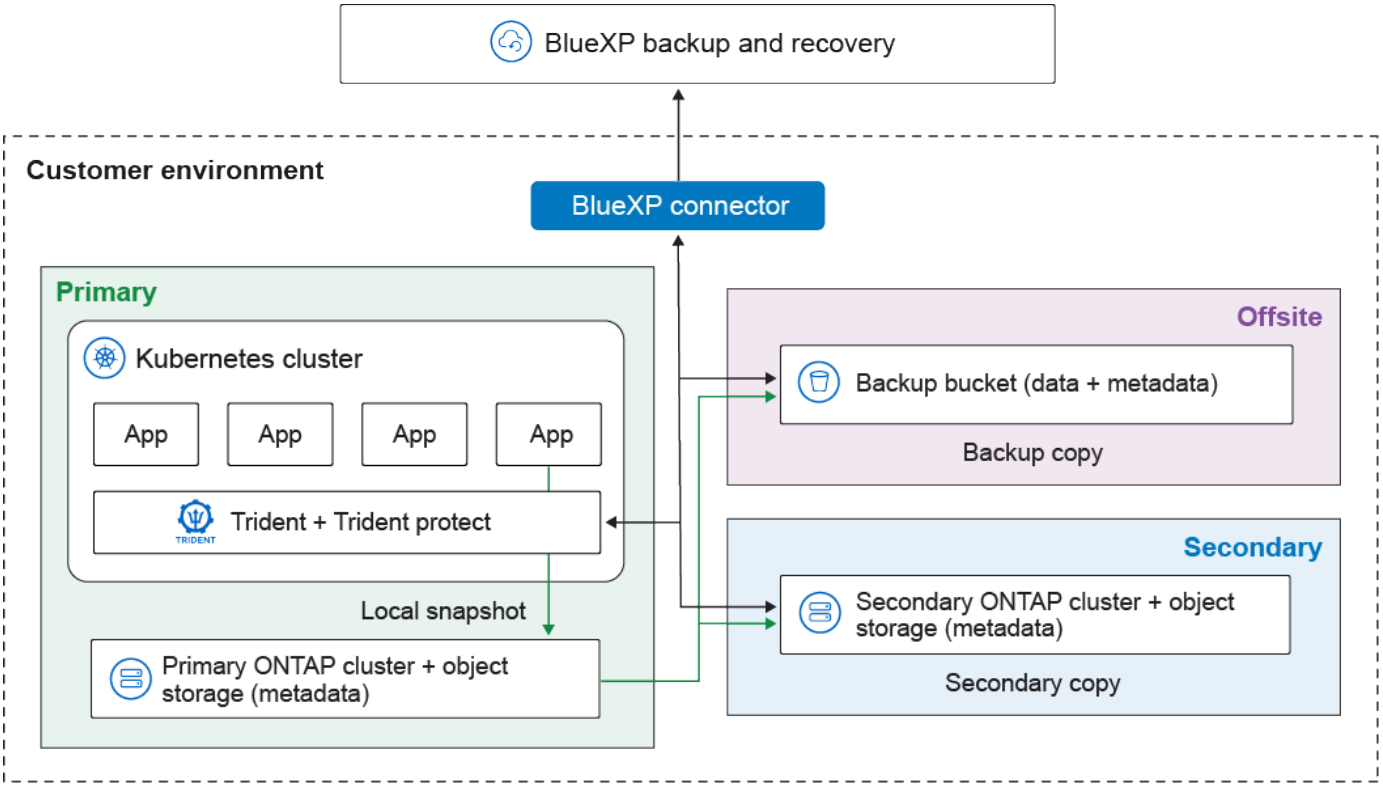
Se l'operazione di ripristino non viene completata, non tentare di eseguire nuovamente il processo di ripristino finché Job Monitor non indica che l'operazione di ripristino non è riuscita. Se si tenta di eseguire nuovamente il processo di ripristino prima che Job Monitor indichi che l'operazione di ripristino non è riuscita, l'operazione di ripristino non verrà eseguita nuovamente. Quando lo stato di Job Monitor viene visualizzato come "Failed" (non riuscito), è possibile provare nuovamente il processo di ripristino.

Proteggi i carichi di lavoro di Kubernetes (anteprima)

Panoramica sulla gestione dei carichi di lavoro Kubernetes

La gestione dei carichi di lavoro Kubernetes in BlueXP backup and recovery ti consente di individuare, gestire e proteggere i tuoi cluster e le tue applicazioni Kubernetes da un'unica posizione. Puoi gestire risorse e applicazioni ospitate sui tuoi cluster Kubernetes. Puoi anche creare e associare policy di protezione ai tuoi carichi di lavoro Kubernetes, il tutto utilizzando un'unica interfaccia.

Il diagramma seguente mostra i componenti e l'architettura di base del backup e del ripristino per i carichi di lavoro Kubernetes e come diverse copie dei dati possono essere archiviate in posizioni diverse:



Il BlueXP backup and recovery offrono i seguenti vantaggi per la gestione dei carichi di lavoro Kubernetes:

- Un unico piano di controllo per proteggere le applicazioni in esecuzione su più cluster Kubernetes. Queste applicazioni possono includere container o macchine virtuali in esecuzione sui cluster Kubernetes.
- Integrazione nativa con NetApp SnapMirror, che consente funzionalità di offload dello storage per tutti i flussi di lavoro di backup e ripristino.
- Backup incrementali permanenti per le applicazioni Kubernetes, che si traducono in Recovery Point Objectives (RPO) e Recovery Time Objectives (RTO) inferiori.

> La presente documentazione viene fornita come anteprima tecnologica. Durante l'anteprima, la funzionalità Kubernetes non è consigliata per i carichi di lavoro di produzione. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale.

È possibile eseguire le seguenti attività relative alla gestione dei carichi di lavoro di Kubernetes:

- "Scopri i carichi di lavoro di Kubernetes" .
- "Gestire i cluster Kubernetes".
- "Aggiungi e proteggi le applicazioni Kubernetes" .
- "Gestire le applicazioni Kubernetes".
- "Ripristina le applicazioni Kubernetes" .

Scopri i carichi di lavoro di Kubernetes nel BlueXP backup and recovery

Per poter utilizzare il servizio BlueXP backup and recovery, è necessario innanzitutto rilevare i carichi di lavoro di Kubernetes.

Ruolo BlueXP obbligatorio Questa attività richiede il ruolo di super amministratore per il backup e il ripristino dei servizi dati. Scopri di più"Ruoli e privilegi dei servizi di backup e ripristino dati" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Scopri i carichi di lavoro di Kubernetes

Nell'inventario di backup e ripristino, è possibile individuare i carichi di lavoro Kubernetes in esecuzione nel proprio ambiente. L'individuazione di un carico di lavoro aggiunge un cluster Kubernetes al BlueXP backup and recovery, consentendo di aggiungere applicazioni al cluster e proteggere le risorse ospitate dal cluster.

Fasi

1. Effettuare una delle seguenti operazioni:
   - Se stai rilevando carichi di lavoro Kubernetes per la prima volta, in BlueXP backup and recovery seleziona **Discover and Manage** nel tipo di carico di lavoro Kubernetes.
   - Se hai già individuato i carichi di lavoro di Kubernetes, in BlueXP backup and recovery seleziona **Inventario** > **Carichi di lavoro** e quindi seleziona **Individua risorse**.
2. Selezionare il tipo di carico di lavoro **Kubernetes**.
3. Inserisci un nome per il cluster e scegli un connettore da utilizzare con il cluster.
4. Seguire le istruzioni della riga di comando che appaiono:
   - Crea uno spazio dei nomi Trident Protect
   - Crea un segreto Kubernetes
   - Aggiungi un repository Helm
   - Installare Trident Protect e il connettore Trident Protect

     Questi passaggi garantiscono che il BlueXP backup and recovery possano interagire con il cluster.
5. Dopo aver completato i passaggi, seleziona **Scopri**.

   Il cluster viene aggiunto all'inventario.
6. Selezionare **Visualizza** nel carico di lavoro Kubernetes associato per visualizzare l'elenco di applicazioni, cluster e namespace per quel carico di lavoro.

Vai alla dashboard BlueXP backup and recovery

Per visualizzare la Dashboard BlueXP backup and recovery , seguire questi passaggi.

1. Dal menu in alto, seleziona **Dashboard**.
2. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai nuovi carichi di lavoro scoperti, protetti e sottoposti a backup.

   "Scopri cosa ti mostra la Dashboard".

Aggiungi e proteggi le applicazioni Kubernetes

Il BlueXP backup and recovery consentono di individuare facilmente i cluster Kubernetes, senza dover generare e caricare file kubeconfig. È possibile connettere i cluster Kubernetes e installare il software necessario utilizzando semplici comandi copiati dall'interfaccia utente BlueXP .

Ruolo BlueXP richiesto

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso BlueXP backup and recovery" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Aggiungi e proteggi una nuova applicazione Kubernetes

Il primo passo per proteggere le applicazioni Kubernetes è creare un'applicazione all'interno BlueXP backup and recovery. Quando si crea un'applicazione, si segnala a BlueXP l'applicazione in esecuzione sul cluster Kubernetes.

Prima di iniziare

Prima di poter aggiungere e proteggere un'applicazione Kubernetes, è necessario "scopri i carichi di lavoro di Kubernetes" .

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Selezionare **Crea applicazione**.
5. Inserisci un nome per l'applicazione.
6. Facoltativamente, seleziona uno dei seguenti campi per cercare le risorse che desideri proteggere:
   - Cluster associato
   - Spazi dei nomi associati
   - Tipi di risorse
   - Selettori di etichette
7. Facoltativamente, seleziona **Risorse con ambito cluster** per scegliere tutte le risorse con ambito a livello di cluster. Se le includi, verranno aggiunte all'applicazione al momento della creazione.
8. Facoltativamente, seleziona **Cerca** per trovare le risorse in base ai tuoi criteri di ricerca.

   BlueXP non memorizza i parametri o i risultati della ricerca; i parametri vengono utilizzati per cercare nel cluster Kubernetes selezionato le risorse che possono essere incluse nell'applicazione.

9. BlueXP visualizza un elenco di risorse che corrispondono ai criteri di ricerca.
10. Se l'elenco contiene le risorse che desideri proteggere, seleziona **Avanti**.
11. Facoltativamente, nell'area **Criterio**, seleziona un criterio di protezione esistente per proteggere l'applicazione o creane uno nuovo. Se non selezioni un criterio, l'applicazione verrà creata senza criterio di protezione. Puoi"aggiungere una politica di protezione" Dopo.
12. Nell'area **Prescript e postscript**, abilitare e configurare eventuali hook di esecuzione prescript o postscript che si desidera eseguire prima o dopo le operazioni di backup. Per abilitare prescript o postscript, è necessario aver già creato almeno uno. "modello di gancio di esecuzione" .
13. Selezionare **Crea**.

Risultato

L'applicazione viene creata e visualizzata nell'elenco delle applicazioni nella scheda **Applicazioni** dell'inventario di Kubernetes. BlueXP abilita la protezione dell'applicazione in base alle impostazioni e puoi monitorarne l'avanzamento nell'area **Monitoraggio** di backup e ripristino.

Proteggere un'applicazione Kubernetes esistente

Abilita un criterio di protezione su un'applicazione Kubernetes che hai già aggiunto.

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri proteggere e seleziona il menu Azioni associato.
5. Selezionare **Proteggi**.
6. Nell'area **Criterio**, seleziona un criterio di protezione esistente per proteggere l'applicazione oppure creane uno nuovo. Fare riferimento a"Creare un criterio" per maggiori informazioni sulla creazione di policy di protezione.
7. Nell'area **Prescript e postscript**, abilita e configura eventuali hook di esecuzione prescript o postscript che desideri eseguire prima o dopo le operazioni di backup. Puoi configurare il tipo di hook di esecuzione, il modello utilizzato, gli argomenti e i selettori di etichetta.
8. Selezionare **fine**.

Risultato

BlueXP abilita la protezione per l'applicazione in base alle impostazioni, ed è possibile monitorarne l'avanzamento nell'area **Monitoraggio** di backup e ripristino. Non appena si abilita la protezione per un'applicazione, BlueXP ne crea un backup completo. Eventuali backup incrementali futuri vengono creati in base alla pianificazione definita nella policy di protezione associata all'applicazione.

Esegui subito il backup di un'applicazione Kubernetes

Crea manualmente un backup di un'applicazione Kubernetes per stabilire una base di riferimento per backup e snapshot futuri o per garantire la protezione dei dati più recenti.

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.

3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione di cui vuoi effettuare il backup e seleziona il menu Azioni associato.
5. Selezionare **Esegui backup adesso**.
6. Assicurarsi che sia selezionato il nome corretto dell'applicazione.
7. Selezionare **Backup**.

Risultato

BlueXP crea un backup dell'applicazione e ne visualizza l'avanzamento nell'area **Monitoraggio** di backup e ripristino. Il backup viene creato in base ai criteri di protezione associati all'applicazione.

Ripristina le applicazioni Kubernetes

Il BlueXP backup and recovery consentono di ripristinare le applicazioni protette tramite una policy di protezione. Per ripristinare un'applicazione, è necessario che quest'ultima disponga di almeno un punto di ripristino. Un punto di ripristino può essere costituito dallo snapshot locale o dal backup nell'archivio oggetti (o da entrambi). È possibile ripristinare un'applicazione utilizzando l'archivio locale, secondario o dell'archivio oggetti.

Ruolo BlueXP richiesto

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso BlueXP backup and recovery" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri ripristinare e seleziona il menu Azioni associato.
5. Selezionare **Visualizza e ripristina**.

   Viene visualizzato l'elenco dei punti di ripristino.

6. Aprire il menu Azioni per il punto di ripristino che si desidera utilizzare e selezionare **Ripristina**.

Impostazioni generali

1. Selezionare l'origine da cui effettuare il ripristino (archivio locale o archivio oggetti).
2. Selezionare il cluster di destinazione dall'elenco **Cluster**.
3. Selezionare lo spazio dei nomi di destinazione del ripristino.

   È possibile ripristinare lo spazio dei nomi originale o uno nuovo.

4. Selezionare **Avanti**.

Selezione delle risorse

1. Scegli se desideri ripristinare tutte le risorse associate all'applicazione o utilizzare un filtro per selezionare

risorse specifiche da ripristinare:

Ripristina tutte le risorse

1. Selezionare **Ripristina tutte le risorse**.
2. Selezionare **Avanti**.

Ripristinare risorse specifiche

1. Seleziona **Risorse selettive**.
2. Scegli il comportamento del filtro delle risorse. Se scegli **Includi**, le risorse selezionate vengono ripristinate. Se scegli **Escludi**, le risorse selezionate non vengono ripristinate.
3. Seleziona **Aggiungi regole** per aggiungere regole che definiscano i filtri per la selezione delle risorse. È necessaria almeno una regola per filtrare le risorse.

   Ogni regola può essere filtrata in base a criteri quali lo spazio dei nomi della risorsa, le etichette, il gruppo, la versione e il tipo.
4. Selezionare **Salva** per salvare ciascuna regola.
5. Dopo aver aggiunto tutte le regole necessarie, seleziona **Cerca** per visualizzare le risorse disponibili nell'archivio di backup che corrispondono ai criteri di filtro.

   Le risorse mostrate sono le risorse attualmente presenti nel cluster.
6. Una volta soddisfatti del risultato, selezionare **Avanti**.

Impostazioni di destinazione

1. Scegliere se ripristinare la classe di archiviazione predefinita o una classe di archiviazione diversa.
2. Facoltativamente, se si sceglie di ripristinare in una classe di archiviazione diversa, selezionare una classe di archiviazione di destinazione che corrisponda a ciascuna classe di archiviazione di origine.
3. Selezionare **Restore** (Ripristina).

Gestire i cluster Kubernetes

Il BlueXP backup and recovery consentono di individuare e gestire i cluster Kubernetes in modo da proteggere le risorse ospitate dai cluster.

Ruolo BlueXP richiesto

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso BlueXP backup and recovery" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Per scoprire i cluster Kubernetes, fare riferimento a "Scopri i carichi di lavoro di Kubernetes" .

Modifica le informazioni del cluster Kubernetes

È possibile modificare un cluster se è necessario cambiarne il nome.

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario** > **Cluster**.
2. Nell'elenco dei cluster, seleziona il cluster che desideri modificare e seleziona il menu Azioni associato.
3. Selezionare **Modifica cluster**.
4. Apportare le modifiche necessarie al nome del cluster. Il nome del cluster deve corrispondere al nome utilizzato con il comando Helm durante il processo di individuazione.
5. Selezionare **fine**.

Rimuovere un cluster Kubernetes

Se non è più necessario proteggere le risorse ospitate da un cluster Kubernetes, è possibile rimuoverlo da BlueXP backup and recovery. La rimozione di un cluster non elimina il cluster stesso o le sue risorse, ma solo il cluster dall'inventario BlueXP . Prima di poter rimuovere un cluster, è necessario disabilitare la protezione ed eliminare le applicazioni associate da BlueXP backup and recovery.

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario** > **Cluster**.
2. Nell'elenco dei cluster, seleziona il cluster che desideri modificare e seleziona il menu Azioni associato.
3. Selezionare **Rimuovi cluster**.
4. Controllare le informazioni nella finestra di dialogo di conferma e selezionare **Rimuovi**.

Gestire le applicazioni Kubernetes

Il BlueXP backup and recovery consentono di rimuovere la protezione ed eliminare le applicazioni Kubernetes e le risorse associate.

Ruolo BlueXP richiesto

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso BlueXP backup and recovery" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Rimuovere la protezione da un'applicazione Kubernetes

È possibile rimuovere la protezione da un'applicazione se non si desidera più proteggerla. Quando si rimuove la protezione da un'applicazione, BlueXP backup and recovery interrompe la protezione dell'applicazione, ma conserva tutti i backup e gli snapshot associati.

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione di cui desideri rimuovere la protezione e seleziona il menu Azioni associato.
5. Selezionare **Rimuovi protezione**.
6. Leggi l'avviso e, quando sei pronto, seleziona **Rimuovi protezione**.

Elimina un'applicazione Kubernetes

Puoi eliminare un'applicazione se non ti serve più. Quando elimini un'applicazione, BlueXP backup and

recovery interrompe la protezione dell'applicazione e cancella tutti i backup e gli snapshot associati.

Fasi

1. Nel BlueXP backup and recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri eliminare e seleziona il menu Azioni associato.
5. Selezionare **Delete** (Elimina).
6. Abilita **Elimina snapshot e backup** per rimuovere tutti gli snapshot e i backup dell'applicazione.

   Non sarà più possibile ripristinare l'applicazione utilizzando questi snapshot e backup.

7. Conferma l'azione e seleziona **Elimina**.

Gestisci i modelli di hook di esecuzione BlueXP backup and recovery per i carichi di lavoro Kubernetes

Un hook di esecuzione è un'azione personalizzata che puoi configurare per essere eseguita insieme a un'operazione di protezione dei dati di un'applicazione Kubernetes gestita. Ad esempio, se si dispone di un'applicazione di database, è possibile utilizzare un gancio di esecuzione per mettere in pausa tutte le transazioni del database prima di uno snapshot e riprendere le transazioni al termine dello snapshot. Ciò garantisce snapshot coerenti con l'applicazione. Quando crei un modello di hook di esecuzione, puoi specificare il tipo di hook, lo script da eseguire e qualsiasi filtro che determini a quali contenitori applicare l'hook. Puoi quindi utilizzare il modello per associare gli hook di esecuzione alle tue applicazioni.

Ruolo BlueXP richiesto

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso BlueXP backup and recovery" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Tipi di hook di esecuzione

BlueXP backup and recovery supporta i seguenti tipi di hook di esecuzione, in base al momento in cui possono essere eseguiti:

- Pre-snapshot
- Post-snapshot
- Pre-backup
- Post-backup
- Post-ripristino

Ordine di esecuzione

Quando viene eseguita un'operazione di protezione dei dati, gli eventi hook di esecuzione hanno luogo nel seguente ordine:

1. Gli eventuali hook di esecuzione pre-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook pre-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook prima dell'operazione non è garantito né configurabile.
2. Se applicabile, si verificano blocchi del filesystem.
3. Viene eseguita l'operazione di protezione dei dati.
4. I filesystem congelati vengono scongelati, se applicabile.
5. Gli eventuali hook di esecuzione post-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook post-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook dopo l'operazione non è garantito né configurabile.

Se si creano più hook di esecuzione dello stesso tipo (ad esempio, pre-snapshot), l'ordine di esecuzione di tali hook non è garantito. Tuttavia, è garantito l'ordine di esecuzione di ganci di tipi diversi. Ad esempio, di seguito è riportato l'ordine di esecuzione di una configurazione che ha tutti i diversi tipi di ganci:

1. Hook pre-snapshot eseguiti
2. Esecuzione di hook post-snapshot
3. Hook pre-backup eseguiti
4. Hook post-backup eseguiti

> Prima di abilitarli in un ambiente di produzione, è necessario verificare sempre gli script hook di esecuzione. È possibile utilizzare il comando 'kubectl exec' per testare comodamente gli script. Dopo aver attivato gli hook di esecuzione in un ambiente di produzione, testare le snapshot e i backup risultanti per assicurarsi che siano coerenti. Per eseguire questa operazione, clonare l'applicazione in uno spazio dei nomi temporaneo, ripristinare lo snapshot o il backup e quindi testare l'applicazione.

> Se un gancio di esecuzione pre-snapshot aggiunge, modifica o rimuove le risorse Kubernetes, queste modifiche sono incluse nella snapshot o nel backup e in qualsiasi operazione di ripristino successiva.

Note importanti sugli hook di esecuzione personalizzati

Quando si pianificano gli hook di esecuzione per le applicazioni, considerare quanto segue.

- Un gancio di esecuzione deve utilizzare uno script per eseguire le azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Gli hook di esecuzione devono essere scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Le impostazioni dell'hook di esecuzione e tutti i criteri corrispondenti vengono utilizzati per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.

> Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, si consiglia di ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati. Se si avvia un'operazione di backup o snapshot con gli hook di esecuzione associati, ma poi si annulla, gli hook possono ancora essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che la logica utilizzata in un gancio di esecuzione post-backup non può presumere che il backup sia stato completato.

Esecuzione dei filtri hook

Quando si aggiunge o si modifica un gancio di esecuzione per un'applicazione, è possibile aggiungere filtri al gancio di esecuzione per gestire i contenitori corrispondenti. I filtri sono utili per le applicazioni che utilizzano la stessa immagine container su tutti i container, ma possono utilizzare ogni immagine per uno scopo diverso (ad esempio Elasticsearch). I filtri consentono di creare scenari in cui gli hook di esecuzione vengono eseguiti su alcuni container identici, ma non necessariamente su tutti. Se si creano più filtri per un singolo gancio di esecuzione, questi vengono combinati con un operatore AND logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.

Ogni filtro aggiunto a un gancio di esecuzione utilizza un'espressione regolare per far corrispondere i contenitori nel cluster. Quando un gancio corrisponde a un container, il gancio esegue lo script associato su quel container. Le espressioni regolari per i filtri utilizzano la sintassi RE2 (espressione regolare), che non supporta la creazione di un filtro che esclude i contenitori dall'elenco di corrispondenze. Per informazioni sulla sintassi supportata BlueXP backup and recovery per le espressioni regolari nei filtri di hook di esecuzione, vedere "Supporto della sintassi RE2 (Regular Expression 2)" .

> Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

Esempi di gancio di esecuzione

Visita il sito "Progetto NetApp Verda GitHub" per scaricare i veri hook di esecuzione per le app più diffuse, come Apache Cassandra ed Elasticsearch. Puoi anche vedere esempi e trovare idee per strutturare i tuoi hook di esecuzione personalizzati.

Creare un modello di hook di esecuzione

È possibile creare un modello di hook di esecuzione personalizzato da utilizzare per eseguire azioni prima o dopo un'operazione di protezione dei dati su un'applicazione.

Fasi

1. In BlueXP, vai su **Protezione** > **Backup e ripristino**.
2. Selezionare la scheda **Impostazioni**.
3. Espandi la sezione **Modello di hook di esecuzione**.
4. Selezionare **Crea modello di hook di esecuzione**.
5. Immettere un nome per l'hook di esecuzione.
6. Facoltativamente, scegli un tipo di hook. Ad esempio, un hook post-restore viene eseguito al termine dell'operazione di ripristino.
7. Nella casella di testo **Script**, inserisci lo script shell eseguibile che desideri eseguire come parte del modello di hook di esecuzione. Facoltativamente, puoi selezionare **Carica script** per caricare un file script.
8. Selezionare **Crea**.

   Il modello viene creato e appare nell'elenco dei modelli nella sezione **Modello di hook di esecuzione**.

Monitorare i lavori nel BlueXP backup and recovery

Con il BlueXP backup and recovery puoi monitorare lo stato degli snapshot locali, delle repliche e dei backup su processi di archiviazione di oggetti avviati, nonché ripristinare i processi avviati. È possibile visualizzare i lavori completati, in corso o non riusciti, in modo da poter diagnosticare e risolvere i problemi. Utilizzando BlueXP Notification Center, puoi abilitare l'invio di notifiche via email per essere informato di importanti attività del sistema anche quando non sei connesso al sistema. Utilizzando la timeline di BlueXP, è possibile visualizzare i dettagli di tutte le azioni avviate tramite l'interfaccia utente o l'API.

Il BlueXP backup and recovery conservano le informazioni sui processi per 15 giorni, dopodiché vengono eliminate e non sono più visibili in Job Monitor.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Super amministratore di Backup e ripristino, Amministratore di backup di Backup e ripristino, Amministratore di ripristino di Backup e ripristino, Amministratore di clonazione di Backup e ripristino o Ruolo di visualizzatore di Backup e ripristino. Scopri di più su "Ruoli e privilegi di backup e ripristino" . "Scopri i ruoli di accesso BlueXP per tutti i servizi" .

Visualizzare lo stato del lavoro in Job Monitor

È possibile visualizzare un elenco di tutte le operazioni di snapshot, replica, backup su storage di oggetti e ripristino, nonché il relativo stato corrente nella scheda **Monitoraggio processi**. Ciò include le operazioni di Cloud Volumes ONTAP, ONTAP on-premise, applicazioni e macchine virtuali. Ogni operazione, o lavoro, ha un ID univoco e uno stato.

Lo stato può essere:

- Successo
- In corso
- In coda
- Attenzione
- Non riuscito

Nella scheda Monitoraggio processi sono disponibili snapshot, repliche, backup su storage di oggetti e operazioni di ripristino avviate dall'interfaccia utente e dall'API BlueXP backup and recovery .

> Se i sistemi ONTAP sono stati aggiornati alla versione 9.13.x e non vengono visualizzate operazioni di backup pianificate in corso in Job Monitor, sarà necessario riavviare il servizio di backup e ripristino BlueXP. "Scopri come riavviare il backup e il ripristino di BlueXP".

Fasi

1. Dal menu BlueXP backup and recovery , selezionare la scheda **Monitoraggio**.
2. Per visualizzare colonne aggiuntive (Ambiente di lavoro, SVM, Nome utente, Carico di lavoro, Nome policy, Etichetta snapshot), selezionare il segno più.

Cercare e filtrare l'elenco dei job

È possibile filtrare le operazioni nella pagina Monitoraggio processi utilizzando diversi filtri, ad esempio criteri, etichetta snapshot, tipo di operazione (protezione, ripristino, conservazione o altro) e tipo di protezione (snapshot locale, replica o backup sul cloud).

Per impostazione predefinita, nella pagina monitoraggio processi vengono visualizzati i processi di protezione e ripristino delle ultime 24 ore. È possibile modificare l'intervallo di tempo utilizzando il filtro dell'intervallo di tempo.

Fasi

1. Dal menu BlueXP backup and recovery , selezionare la scheda **Monitoraggio**.
2. Per ordinare i risultati in modo diverso, selezionare ciascuna intestazione di colonna per ordinare in base a Stato, ora di inizio, Nome risorsa e altro ancora.
3. Se si stanno cercando lavori specifici, selezionare l'area **Ricerca avanzata e filtraggio** per aprire il pannello di ricerca.

   Utilizzare questo pannello per immettere una ricerca di testo libero per qualsiasi risorsa, ad esempio "volume 1" o "applicazione 3". È inoltre possibile filtrare l'elenco dei lavori in base alle voci dei menu a discesa.

   La maggior parte dei filtri sono intuitivi. Il filtro per "carico di lavoro" consente di visualizzare i lavori nelle seguenti categorie:

   - Volumi ONTAP (Cloud Volumes ONTAP e volumi ONTAP on-premise)
   - Microsoft SQL Server
   - Macchine virtuali
   - Kubernetes

   - È possibile cercare i dati all'interno di una specifica "SVM" solo se è stato selezionato per la prima volta un ambiente di lavoro.
   - È possibile effettuare la ricerca utilizzando il filtro "tipo di protezione" solo dopo aver selezionato il "tipo" di "protezione".

4. Per aggiornare immediatamente la pagina, selezionare  pulsante. In caso contrario, questa pagina viene aggiornata ogni 15 minuti in modo da visualizzare sempre i risultati più recenti dello stato del lavoro.

Visualizzare i dettagli del lavoro

È possibile visualizzare i dettagli corrispondenti a un lavoro completato specifico. È possibile esportare i dettagli di un determinato lavoro in formato JSON.

Puoi visualizzare dettagli come tipo di lavoro (pianificato o on-demand), tempi di inizio e fine del tipo di backup di SnapMirror (iniziale o periodico), durata, quantità di dati trasferiti dall'ambiente di lavoro allo storage a oggetti, velocità di trasferimento media, nome della policy, blocco di conservazione abilitato, scansione ransomware eseguita, dettagli sulla fonte di protezione e sul target di protezione.

I processi di ripristino mostrano dettagli quali il provider di destinazione del backup (Amazon Web Services, Microsoft Azure, Google Cloud, locale), il nome del bucket S3, il nome della SVM, il nome del volume di origine, il volume di destinazione, l'etichetta dello snapshot, il conteggio degli oggetti recuperati, i nomi dei file, le dimensioni dei file, la data dell'ultima modifica e il percorso completo del file.

Fasi

1. Dal menu BlueXP backup and recovery , selezionare la scheda **Monitoraggio**.
2. Selezionare il nome del lavoro.
3. Selezionare il menu Actions (azioni) ••• E selezionare **Visualizza dettagli**.
4. Espandere ogni sezione per visualizzare i dettagli.

Scarica i risultati di Job Monitoring come report

È possibile scaricare il contenuto della pagina principale di Job Monitoring come report dopo averlo perfezionato. Il backup e ripristino di BlueXP genera e scarica un file .CSV che è possibile rivedere e inviare ad altri gruppi in base alle necessità. Il file .CSV include fino a 10,000 righe di dati.

Dalle informazioni relative ai dettagli di monitoraggio dei processi, è possibile scaricare un file JSON contenente i dettagli di un singolo processo.

Fasi

1. Dal menu BlueXP backup and recovery , selezionare la scheda **Monitoraggio**.
2. Per scaricare un file CSV per tutti i lavori, seleziona il pulsante Scarica e individua il file nella directory di download.
3. Per scaricare un file JSON per un singolo job, selezionare il menu Actions (azioni) ••• Per il lavoro, selezionare **Download JSON file** e individuare il file nella directory di download.

Esaminare i processi di conservazione (ciclo di vita del backup)

Il monitoraggio dei flussi di conservazione (o *ciclo di vita del backup*) consente di ottenere la completezza, la responsabilità e la sicurezza dei backup durante le verifiche. Per tenere traccia del ciclo di vita del backup, è possibile identificare la scadenza di tutte le copie di backup.

Un processo di ciclo di vita di backup tiene traccia di tutte le copie Snapshot che vengono eliminate o nella coda da eliminare. A partire da ONTAP 9,13, è possibile esaminare tutti i tipi di lavoro denominati "conservazione" nella pagina monitoraggio processi.

Il tipo di lavoro "conservazione" acquisisce tutti i processi di eliminazione Snapshot avviati su un volume protetto dal backup e recovery di BlueXP.

Fasi

1. Dal menu BlueXP backup and recovery , selezionare la scheda **Monitoraggio**.
2. Selezionare l'area **Advanced Search & Filtering** (Ricerca e filtraggio avanzati) per aprire il pannello Search (Cerca).
3. Selezionare "conservazione" come tipo di lavoro.

Esaminare gli avvisi di backup e ripristino in BlueXP Notification Center

BlueXP Notification Center tiene traccia dell'avanzamento dei processi di backup e ripristino avviati, in modo da verificare se l'operazione è stata eseguita correttamente.

Oltre a visualizzare gli avvisi nel Centro notifiche, è possibile configurare BlueXP in modo che invii alcuni tipi di notifiche via email come avvisi, in modo da essere informato di importanti attività del sistema anche quando non si è connessi al sistema. "Scopri di più sul Centro notifiche e su come inviare e-mail di avviso per i processi di backup e ripristino".

Il Centro notifiche visualizza numerosi eventi di istantanea, replica, backup nel cloud e ripristino, ma solo determinati eventi attivano avvisi e-mail:

Tipo di operazione	Evento	Livello di avviso	E-mail inviata
Attivazione	Attivazione backup e ripristino non riuscita per l'ambiente di lavoro	Errore	Sì
Attivazione	La modifica di backup e ripristino non è riuscita per l'ambiente di lavoro	Errore	Sì
Istantanea locale	Errore di creazione di snapshot ad hoc BlueXP backup and recovery	Errore	Sì
Replica	Errore del processo di replica ad-hoc di backup e recovery di BlueXP	Errore	Sì
Replica	Errore del processo di pausa del backup e recovery di BlueXP	Errore	No
Replica	Errore del processo di interruzione della replica di backup e ripristino BlueXP	Errore	No
Replica	Errore del processo di risincronizzazione della replica di backup e recovery di BlueXP	Errore	No
Replica	La replica di backup e recovery di BlueXP arresta il guasto al processo	Errore	No
Replica	Errore durante la risincronizzazione inversa del processo di backup e recovery di BlueXP	Errore	Sì
Replica	La replica di backup e recovery di BlueXP elimina l'errore del processo	Errore	Sì

A partire da ONTAP 9.13.0, tutti gli avvisi vengono visualizzati per i sistemi Cloud Volumes ONTAP e ONTAP on-premise. Per i sistemi con Cloud Volumes ONTAP 9.13.0 e on-premise ONTAP, viene visualizzato solo l'avviso relativo al completamento del processo di ripristino, ma con avvisi.

Per impostazione predefinita, gli amministratori dell'organizzazione e degli account BlueXP ricevono e-mail per tutti gli avvisi "critici" e "consigliati". Per impostazione predefinita, tutti gli altri utenti e destinatari non ricevono alcuna notifica e-mail. Le e-mail possono essere inviate a qualsiasi utente BlueXP che fa parte del tuo NetApp Cloud account o a qualsiasi altro destinatario che abbia bisogno di conoscere l'attività di backup e ripristino.

Per ricevere gli avvisi e-mail di backup e ripristino di BlueXP, è necessario selezionare i tipi di severità della notifica "critico", "Avviso" e "errore" nella pagina Impostazioni avvisi e notifiche.

"Scopri come inviare e-mail di avviso per i processi di backup e ripristino".

Fasi

1. Dalla barra dei menu di BlueXP, selezionare ().
2. Esaminare le notifiche.

Esaminare l'attività operativa nella timeline di BlueXP

È possibile visualizzare i dettagli delle operazioni di backup e ripristino per ulteriori analisi nella cronologia di BlueXP. La Timeline di BlueXP fornisce informazioni dettagliate su ciascun evento, avviato dall'utente o dal sistema, e mostra le azioni avviate nell'interfaccia utente o tramite l'API.

"Scopri le differenze tra la cronologia e il centro di notifica".

Riavviare il servizio di backup e ripristino BlueXP

In alcuni casi potrebbe essere necessario riavviare il servizio di backup e ripristino BlueXP.

La funzionalità di backup e ripristino BlueXP è integrata nel connettore BlueXP.

Fasi

1. Connettersi al sistema Linux su cui è in esecuzione il connettore.

Posizione del connettore	Procedura
Implementazione del cloud	Seguire le istruzioni per "Connessione alla macchina virtuale Connector Linux" a seconda del cloud provider utilizzato.
Installazione manuale	Accedere al sistema Linux.

2. Immettere il comando per riavviare il servizio.

Posizione del connettore	Comando Docker	Comando Podman
Implementazione del cloud	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installazione manuale con accesso a Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installazione manuale senza accesso a Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`

Automatizza con le API REST BlueXP backup and recovery

Le funzionalità di backup e ripristino di BlueXP disponibili tramite l'interfaccia utente Web sono disponibili anche tramite l'API RESTful.

Nel backup e ripristino di BlueXP sono definite dieci categorie di endpoint:

- backup - gestisce le operazioni di backup del cloud e delle risorse on-premise e recupera i dettagli dei dati di backup
- catalogo - gestisce la ricerca indicizzata dei file nel catalogo in base a una query (Search & Restore)
- Cloud - recupera informazioni su varie risorse di provider cloud da BlueXP
- Job - gestisce le voci dei dettagli della commessa nel database BlueXP
- License (licenza): Recupera la validità della licenza degli ambienti di lavoro da BlueXP
- ransomware scan (scansione ransomware) - avvia una scansione ransomware su un file di backup specifico
- restore (ripristina): consente di eseguire operazioni di ripristino a livello di volume, file e cartelle
- sfr - Recupera i file da un file di backup per operazioni di ripristino a livello di file singolo (Browse & Restore)
- StorageGRID - consente di recuperare i dettagli su un server StorageGRID e di rilevare un server StorageGRID
- ambiente di lavoro - gestisce le policy di backup e configura l'archivio di oggetti di destinazione associato a un ambiente di lavoro

Riferimento API

La documentazione per ogni API BlueXP backup and recovery è disponibile da "Automazione BlueXP per il BlueXP backup and recovery" .

Per iniziare

Per iniziare a utilizzare le API di backup e ripristino di BlueXP, è necessario ottenere un token utente, l'ID account BlueXP e l'ID connettore BlueXP.

Quando si effettua una chiamata API, aggiungere il token utente nell'intestazione Authorization e l'ID del connettore BlueXP nell'intestazione x-Agent-id. È necessario utilizzare l'ID account BlueXP nelle API.

Se si utilizza un account di servizio, è necessario utilizzare il token di accesso al servizio anziché un token utente. Il valore per "client_id" ("Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC") è un valore fisso e non può essere modificato. In questo caso, segui le istruzioni qui: "Crea un token di accesso al servizio" .

Fasi

1. Ottenere un token utente dal sito Web di NetApp BlueXP.

   Assicurarsi di generare il token di refresh dal seguente collegamento: https://services.cloud.netapp.com/

refresh-token/. Il token refresh è una stringa alfanumerica che verrà utilizzata per generare un token utente.

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

Il token utente del sito Web BlueXP ha una data di scadenza. La risposta API include un campo "expires_in" che indica la scadenza del token. Per aggiornare il token, è necessario chiamare nuovamente questa API.

2. Ottenere l'ID account BlueXP.

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR……
```

Questa API restituirà una risposta simile a quella riportata di seguito. È possibile recuperare l'ID del centro di costo analizzando l'output da **[0].[accountPublicId]**.

```
 [{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}……
. Ottenere l'ID x-Agent che contiene l'ID del connettore BlueXP.
```

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5……
```

Questa API restituirà una risposta simile a quella riportata di seguito. È possibile recuperare l'id agente

analizzando l'output da **occm.[0].[Agent].[agentId]**.


```
{"occms":[{"account":"account-
OOnAR4ZS","accountName":"cbs","occm":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
"agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z","status":"ready","occmName"
:"cbsgcpdevcntsg-
asia","primaryCallbackUri":"http://34.93.197.21","manualOverrideUris":[]
,"automaticCallbackUris":["http://34.93.197.21","http://34.93.197.21/occ
mui","https://34.93.197.21","https://34.93.197.21/occmui","http://10.138
.0.16","http://10.138.0.16/occmui","https://10.138.0.16","https://10.138
.0.16/occmui","http://localhost","http://localhost/occmui","http://local
host:1337","http://localhost:1337/occmui","https://localhost","https://l
ocalhost/occmui","https://localhost:1337","https://localhost:1337/occmui
"],"createDate":"1652120369286","agent":{"useDockerInfra":true,"network"
:"default","name":"cbsgcpdevcntsg-
asia","agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients","provider":"gc
p","systemId":"a3aa3578-bfee-4d16-9e10-
```


Esempio di utilizzo delle API

Nell'esempio seguente viene illustrata una chiamata API per attivare il backup e il ripristino di BlueXP in un ambiente di lavoro con una nuova policy con etichette giornaliere, orarie e settimanali impostate, che archiviano dopo giorni impostati su 180 giorni, nella regione Est-US-2 nel cloud Azure. Si noti che questo abilita solo il backup nell'ambiente di lavoro, ma non viene eseguito il backup dei volumi.

Richiesta API

Verrà utilizzato l'ID account BlueXP `account-DpTFcxN3`, ID connettore BlueXP `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients`e token utente `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4V alobjUmju2x0xUH48g` in questo comando.

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }'
```

Response è un ID processo che è possibile monitorare.

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

Monitorare la risposta.

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Risposta.

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "PENDING",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Monitorare fino a quando lo "stato" non è "COMPLETATO".

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "COMPLETED",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Riferimento

Criteri in SnapCenter confrontati con quelli nel BlueXP backup and recovery

Esistono alcune differenze tra i criteri utilizzati in SnapCenter e quelli utilizzati nel BlueXP backup and recovery che potrebbero influire su ciò che viene visualizzato dopo l'importazione di risorse e criteri da SnapCenter.

Pianifica i livelli

SnapCenter utilizza i seguenti livelli di pianificazione:

- **Ogni ora**: più ore e minuti con qualsiasi ora (0-23) e qualsiasi minuto (0-60).
- **Giornaliero**: include un'opzione per ripetere ogni tot giorni, ad esempio ogni 3 giorni.
- **Settimanale**: da domenica a lunedì, con la possibilità di eseguire uno snapshot il primo giorno della settimana o in più giorni della settimana.
- **Mensile**: mesi da gennaio a dicembre, con la possibilità di eseguire l'operazione in giorni specifici del mese, ad esempio il 7 di ogni mese e anche in più giorni del mese.

Il BlueXP backup and recovery utilizzano i seguenti livelli di pianificazione, leggermente diversi:

- **Ogni ora**: esegue gli snapshot solo a intervalli di 15 minuti, ad esempio intervalli di 1 ora o 15 minuti inferiori a 60.
- **Giornaliero**: Ore del giorno (0-23) con orario di inizio, ad esempio, alle 10:00, con la possibilità di eseguire l'operazione ogni tot di ore.
- **Settimanale**: Giorno della settimana (da domenica a lunedì) con la possibilità di eseguire l'operazione in uno o più giorni. È lo stesso di SnapCenter.
- **Mensile**: Date del mese (0-30) con un'ora di inizio in più date del mese.
- **Annuale**: Mensile. Corrisponde al mensile di SnapCenter.

Più policy in SnapCenter con lo stesso livello di pianificazione

È possibile assegnare più policy con lo stesso livello di pianificazione a una risorsa in SnapCenter. Tuttavia, il BlueXP backup and recovery non supportano più policy su una risorsa che utilizza lo stesso livello di pianificazione.

Esempio: se si utilizzano tre policy (per dati, registro e registro degli snapshot) in SnapCenter, dopo la migrazione da SnapCenter, il BlueXP backup and recovery utilizzano una singola policy anziché tutte e tre.

Pianificazioni giornaliere SnapCenter importate

Il BlueXP backup and recovery regolano le pianificazioni SnapCenter come segue:

- Se la pianificazione SnapCenter è impostata su un intervallo inferiore o uguale a 7 giorni, BlueXP backup and recovery imposta la pianificazione su settimanale. Alcuni snapshot verranno saltati durante la settimana.

Esempio: se si dispone di una policy giornaliera SnapCenter con un intervallo di ripetizione di 3 giorni a partire da lunedì, BlueXP backup and recovery imposta la pianificazione su settimanale, ovvero lunedì, giovedì e domenica. Alcuni giorni verranno saltati perché non sono esattamente ogni 3 giorni.

- Se la pianificazione SnapCenter è impostata su un intervallo superiore a 7 giorni, BlueXP backup and recovery imposta la pianificazione su mensile. Alcuni snapshot verranno saltati durante il mese.

  Esempio: se si dispone di una policy giornaliera SnapCenter con un intervallo di ripetizione di 10 giorni a partire dal 2 del mese, il BlueXP backup and recovery (post migrazione) impostano la pianificazione su mensile il 2, il 12 e il 22 del mese. Alcuni giorni verranno saltati il mese successivo.

Pianificazioni orarie SnapCenter importate

I criteri orari SnapCenter con intervalli di ripetizione superiori a un'ora vengono convertiti in criteri giornalieri nel BlueXP backup and recovery.

Qualsiasi politica oraria con intervalli ripetuti che non siano un fattore di 24 (ad esempio 5, 7, ecc.) salterà alcuni snapshot nel corso della giornata.

Esempio: se si dispone di una policy oraria SnapCenter con un intervallo di ripetizione ogni 5 ore a partire dall'1:00, il BlueXP backup and recovery (dopo la migrazione) imposteranno la pianificazione su giornaliera con intervalli di 5 ore all'1:00, alle 6:00, alle 11:00, alle 16:00 e alle 21:00. Alcune ore verranno saltate: dopo le 21:00, la ripetizione dovrebbe essere alle 2:00 ogni 5 ore, ma sarà sempre all'1:00.

Conservazione dei registri dai criteri di SnapCenter

Se in SnapCenter è presente una risorsa con più policy, il BlueXP backup and recovery utilizzano il seguente ordine di priorità per assegnare il valore di conservazione del registro:

- Per i criteri "Backup completo con backup del registro" più i criteri "solo registro" in SnapCenter, il BlueXP backup and recovery utilizzano il valore di conservazione del criterio solo registro.
- Per i criteri "Backup completo solo con registro" e "Completo e registro" in SnapCenter, il BlueXP backup and recovery utilizzano il valore di conservazione solo registro.
- Per "Backup completo e registro" più "Backup completo" in SnapCenter, il BlueXP backup and recovery utilizzano il valore di conservazione "Backup completo e registro".
- Se in SnapCenter è presente solo un backup completo, il BlueXP backup and recovery non abilitano il backup del registro.

Conservazione del backup del registro

Con SnapCenter è possibile avere più valori di conservazione su più policy associate a una risorsa. Tuttavia, il BlueXP backup and recovery supportano solo un singolo valore di conservazione per tutti i criteri associati a una risorsa.

Conteggio della conservazione dai criteri di SnapCenter

Se si dispone di una risorsa con protezione secondaria abilitata in SnapCenter con più volumi di origine, più volumi di destinazione e più relazioni SnapMirror , il BlueXP backup and recovery utilizzano solo il conteggio di conservazione del primo criterio.

Esempio: se si dispone di una policy SnapCenter con un conteggio di conservazione pari a 5 e di un'altra policy con un conteggio di conservazione pari a 10, il BlueXP backup and recovery utilizzeranno il conteggio di

conservazione pari a 5.

Etichette SnapMirror dai criteri di SnapCenter

Le etichette SnapMirror per ogni policy in SnapCenter rimangono intatte dopo la migrazione, anche se il livello viene modificato.

Esempio: una policy oraria di SnapCenter potrebbe essere modificata in giornaliera in BlueXP backup and recovery. Tuttavia, le etichette SnapMirror rimangono invariate dopo la migrazione.

Gestione dell'identità e dell'accesso alle funzionalità BlueXP backup and recovery

Il BlueXP backup and recovery utilizzano la gestione dell'identità e dell'accesso (IAM) per gestire l'accesso di ciascun utente a specifiche funzionalità e azioni.

Il servizio utilizza i seguenti ruoli specifici per il BlueXP backup and recovery.

- **Super amministratore di backup e ripristino**: esegue qualsiasi azione nel BlueXP backup and recovery.
- **Amministratore di backup**: esegue backup su snapshot locali, replica su storage secondario ed esegue backup su azioni di storage di oggetti in BlueXP backup and recovery.
- **Ripristina amministrazione**: ripristina i carichi di lavoro utilizzando il BlueXP backup and recovery.
- **Clone admin**: clona applicazioni e dati utilizzando il BlueXP backup and recovery.
- **Visualizzatore di backup e ripristino**: visualizza le informazioni nel BlueXP backup and recovery, ma non esegue alcuna azione.

Per i dettagli su tutti i ruoli di accesso BlueXP , vedere "La documentazione di installazione e amministrazione di BlueXP" .

Nella tabella seguente sono indicate le azioni che ogni ruolo di BlueXP backup and recovery può eseguire.

Funzione e azione	Super amministratore di backup e ripristino	Amministratore del backup	Ripristina amministratore	Clona amministratore	Visualizzatore
Aggiungi, modifica o elimina host	Sì	No	No	No	No
Installa i plugin	Sì	No	No	No	No
Aggiungi credenziali (host, istanza, vCenter)	Sì	No	No	No	No
Visualizza dashboard e tutte le schede	Sì	Sì	Sì	Sì	Sì
Inizia la prova gratuita	Sì	No	No	No	No

Funzione e azione	Super amministratore di backup e ripristino	Amministratore del backup	Ripristina amministratore	Clona amministratore	Visualizzatore
Avvia il rilevamento dei carichi di lavoro	No	Sì	Sì	Sì	No
Visualizza le informazioni sulla licenza	Sì	Sì	Sì	Sì	Sì
Attiva la licenza	Sì	No	No	No	No
Visualizza gli host	Sì	Sì	Sì	Sì	Sì
Orari:					
Attivare gli orari	Sì	Sì	Sì	Sì	No
Sospendi gli orari	Sì	Sì	Sì	Sì	No
Politiche e protezione:					
Visualizza i piani di protezione	Sì	Sì	Sì	Sì	Sì
Crea, modifica o elimina la protezione	Sì	Sì	No	No	No
Ripristinare i carichi di lavoro	Sì	No	Sì	No	No
Crea un clone, dividi un clone o elimina un clone	Sì	No	No	Sì	No
Crea, modifica o elimina una policy	Sì	Sì	No	No	No
Segnalazioni:					
Visualizzare i report	Sì	Sì	Sì	Sì	Sì
Creare report	Sì	Sì	Sì	Sì	No
Eliminare i referti	Sì	No	No	No	No
Importa da SnapCenter e gestisci l'host:					
Visualizza i dati SnapCenter importati	Sì	Sì	Sì	Sì	Sì
Importa dati da SnapCenter	Sì	Sì	No	No	No

Funzione e azione	Super amministratore di backup e ripristino	Amministratore del backup	Ripristina amministratore	Clona amministratore	Visualizzatore
Gestisci (migra) l'host	Sì	Sì	No	No	No
Configura impostazioni:					
Configurare la directory del registro	Sì	Sì	Sì	No	No
Associa o rimuovi le credenziali dell'istanza	Sì	Sì	Sì	No	No
Secchi:					
Visualizza bucket	Sì	Sì	Sì	Sì	Sì
Crea, modifica o elimina bucket	Sì	Sì	No	No	No

Ripristinare i dati di configurazione BlueXP backup and recovery in un sito oscuro

Quando si utilizza il BlueXP backup and recovery in un sito senza accesso a Internet, noto come *modalità privata*, i dati di configurazione BlueXP backup and recovery vengono sottoposti a backup nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host di BlueXP Connector, è possibile distribuire un nuovo Connector e ripristinare i dati critici BlueXP backup and recovery .

Questa procedura si applica solo ai dati di volume ONTAP .

Quando si utilizza il BlueXP backup and recovery in un ambiente SaaS in cui BlueXP Connector è distribuito presso il provider cloud o sul proprio sistema host con accesso a Internet, tutti i dati importanti di configurazione BlueXP backup and recovery vengono sottoposti a backup e protetti nel cloud. Se riscontri un problema con il connettore, crea semplicemente un nuovo connettore e aggiungi i tuoi ambienti di lavoro: i dettagli del backup verranno ripristinati automaticamente.

Esistono due tipi di dati sottoposti a backup:

- Database BlueXP backup and recovery : contiene un elenco di tutti i volumi, file di backup, criteri di backup e informazioni di configurazione.
- File di catalogo indicizzati: contengono indici dettagliati utilizzati per la funzionalità di ricerca e ripristino, che rendono le ricerche molto rapide ed efficienti quando si cercano dati di volume che si desidera ripristinare.

Questi dati vengono sottoposti a backup una volta al giorno a mezzanotte e vengono conservate al massimo 7 copie di ciascun file. Se il connettore gestisce più ambienti di lavoro ONTAP locali, i file BlueXP backup and recovery saranno posizionati nel bucket dell'ambiente di lavoro attivato per primo.

Nessun dato di volume viene mai incluso nel database BlueXP backup and recovery o nei file del catalogo indicizzato.

Ripristina i dati BlueXP backup and recovery su un nuovo connettore BlueXP

Se il tuo BlueXP Connector locale subisce un errore catastrofico, dovrai installare un nuovo Connector e quindi ripristinare i dati BlueXP backup and recovery sul nuovo Connector.

Per ripristinare il funzionamento del sistema BlueXP backup and recovery, è necessario eseguire le seguenti operazioni:

- Installa un nuovo connettore BlueXP
- Ripristinare il database BlueXP backup and recovery
- Ripristina i file del catalogo indicizzato
- Riscopri tutti i tuoi sistemi ONTAP on-premise e i sistemi StorageGRID nell'interfaccia utente BlueXP

Una volta verificato che il sistema è tornato a funzionare, ti consigliamo di creare nuovi file di backup.

Cosa ti servirà

Sarà necessario accedere ai backup più recenti del database e dell'indice dal bucket StorageGRID o ONTAP S3 in cui sono archiviati i file di backup:

- File di database MySQL BlueXP backup and recovery

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/` , e si chiama `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- File zip di backup del catalogo indicizzato

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/catalog_backup/` , e si chiama `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installa un nuovo connettore su un nuovo host Linux locale

Quando installi un nuovo BlueXP Connector, assicurati di scaricare la stessa versione del software installata sul Connector originale. Le modifiche periodiche alla struttura del database BlueXP backup and recovery potrebbero rendere le nuove versioni del software incompatibili con i backup del database originali. Puoi "aggiornare il software Connector alla versione più recente dopo aver ripristinato il database di backup" .

1. "Installa BlueXP Connector su un nuovo host Linux locale"
2. Accedi a BlueXP utilizzando le credenziali utente amministratore appena create.

Ripristinare il database BlueXP backup and recovery

1. Copiare il backup MySQL dalla posizione di backup al nuovo host del connettore. Di seguito utilizzeremo il nome file di esempio "CBS_DB_Backup_23_05_2023.sql".
2. Copiare il backup nel contenitore Docker MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accedere alla shell del contenitore MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Nella shell del contenitore, distribuire "env".
5. Ti servirà la password del database MySQL, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il BlueXP backup and recovery utilizzando il seguente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verificare che il BlueXP backup and recovery siano stati ripristinati correttamente utilizzando i seguenti comandi SQL:

```
mysql -u root -p cloud_backup
```

Inserisci la password.

```
mysql> show tables;
mysql> select * from volume;
```

Controlla se i volumi mostrati sono gli stessi presenti nell'ambiente originale.

Ripristina i file del catalogo indicizzato

1. Copiare il file zip di backup del catalogo indicizzato (utilizzeremo il nome file di esempio "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") dalla posizione di backup al nuovo host del connettore nella cartella "/opt/application/netapp/cbs".
2. Decomprimere il file "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" utilizzando il seguente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Eseguire il comando **ls** per assicurarsi che sia stata creata la cartella "catalogdb1" con le sottocartelle "changes" e "snapshots".

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti gli ambienti di lavoro ONTAP on-prem"che erano disponibili nel tuo ambiente precedente. Ciò include il sistema ONTAP utilizzato come server S3.
2. "Scopri i tuoi sistemi StorageGRID" .

Impostare i dettagli dell'ambiente StorageGRID

Aggiungere i dettagli del sistema StorageGRID associato ai propri ambienti di lavoro ONTAP così come sono stati configurati nella configurazione originale del connettore utilizzando "API BlueXP" .

Le seguenti informazioni si applicano alle installazioni in modalità privata a partire da BlueXP 3.9.xx. Per le versioni precedenti, utilizzare la seguente procedura: "DarkSite Cloud Backup: backup e ripristino di MySQL e catalogo indicizzato" .

Sarà necessario eseguire questi passaggi per ogni sistema che esegue il backup dei dati su StorageGRID.

1. Estrarre il token di autorizzazione utilizzando la seguente API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d
'{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pa
ssword"}
> '
```

   Mentre l'indirizzo IP, il nome utente e le password sono valori personalizzati, il nome dell'account non lo è. Il nome dell'account è sempre "account-DARKSITE1". Inoltre, il nome utente deve essere formattato come indirizzo email.

   Questa API restituirà una risposta simile alla seguente. È possibile recuperare il token di autorizzazione come mostrato di seguito.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Estrarre l'ID dell'ambiente di lavoro e l'X-Agent-Id utilizzando l'API tenancy/external/resource.


```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```


Questa API restituirà una risposta simile alla seguente. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-agent-id*.

3. Aggiornare il database BlueXP backup and recovery con i dettagli del sistema StorageGRID associato agli ambienti di lavoro. Assicurarsi di immettere il nome di dominio completo di StorageGRID, nonché la chiave di accesso e la chiave di archiviazione come mostrato di seguito:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verificare le impostazioni BlueXP backup and recovery

1. Selezionare ciascun ambiente di lavoro ONTAP e fare clic su **Visualizza backup** accanto al servizio Backup e ripristino nel pannello di destra.

   Dovresti essere in grado di vedere tutti i backup creati per i tuoi volumi.

2. Nella Dashboard di ripristino, nella sezione Cerca e ripristina, fai clic su **Impostazioni di indicizzazione**.

   Assicurarsi che gli ambienti di lavoro in cui era precedentemente abilitata la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Cerca e ripristina, esegui alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato sia stato completato correttamente.

Livelli di archiviazione AWS supportati con BlueXP backup and recovery

Il backup e ripristino BlueXP supporta due classi di storage di archiviazione S3 e la maggior parte delle regioni.

NOTA Per passare da una versione all'altra dell'interfaccia utente BlueXP backup and recovery , fare riferimento a "Passa alla precedente interfaccia utente BlueXP backup and recovery" .

Classi di storage di archiviazione S3 supportate per backup e ripristino BlueXP

Quando i file di backup vengono creati inizialmente, vengono memorizzati nello storage S3 *Standard*. Questo Tier è ottimizzato per l'archiviazione dei dati a cui si accede raramente, ma che consente anche di accedervi immediatamente. Dopo 30 giorni, i backup passano alla classe di storage S3 *Standard-infrequent Access* per risparmiare sui costi.

Se i cluster di origine eseguono ONTAP 9.10.1 o superiore, è possibile scegliere di eseguire il Tier dei backup per lo storage *S3 Glacier* o *S3 Glacier Deep Archive* dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. È possibile impostare su "0" o su 1-999 giorni. Se si imposta su "0" giorni, non sarà possibile modificarlo successivamente a 1-999 giorni.

Non è possibile accedere immediatamente ai dati di questi livelli quando necessario e richiede un costo di recupero più elevato, quindi è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione su questa pagina relativa al ripristino dei dati dall'archivio.

- Se non si seleziona alcun livello di archiviazione nella prima policy di backup quando si attiva il backup e ripristino BlueXP, *S3 Glacier* sarà l'unica opzione di archiviazione per le policy future.
- Se si seleziona *S3 Glacier* nella prima policy di backup, è possibile passare al livello *S3 Glacier Deep Archive* per le policy di backup future per quel cluster.
- Se si seleziona *S3 Glacier Deep Archive* nella prima policy di backup, tale Tier sarà l'unico Tier di archiviazione disponibile per future policy di backup per quel cluster.

Si noti che quando si configura il backup e ripristino BlueXP con questo tipo di regola del ciclo di vita, non è necessario configurare alcuna regola del ciclo di vita quando si imposta il bucket nell'account AWS.

"Scopri le classi di storage S3".

Ripristina i dati dallo storage di archivio

Anche se la memorizzazione di file di backup meno recenti nello storage di archiviazione è molto meno costosa rispetto allo storage Standard o Standard-IA, l'accesso ai dati da un file di backup nello storage di archiviazione per le operazioni di ripristino richiederà più tempo e costerà più denaro.

Quanto costa ripristinare i dati da Amazon S3 Glacier e Amazon S3 Glacier Deep Archive?

Sono disponibili 3 priorità di ripristino per il recupero dei dati da Amazon S3 Glacier e 2 priorità di ripristino per il recupero dei dati da Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive costa meno di S3 Glacier:

Tier di archiviazione	Ripristinare priorità e costi		
	Alto	**Standard**	**Basso**
Ghiacciaio S3	Recupero più rapido, costo più elevato	Recupero più lento, costi inferiori	Recupero più lento, costo più basso
S3 Glacier Deep Archive		Recupero più rapido, costi più elevati	Recupero più lento, costo più basso

Ogni metodo ha una tariffa di recupero per GB e una tariffa per richiesta diverse. Per informazioni dettagliate sui prezzi di S3 Glacier per regione AWS, visitare il "Pagina dei prezzi di Amazon S3".

Quanto tempo ci vorrà per ripristinare gli oggetti archiviati in Amazon S3 Glacier?

Il tempo totale di ripristino è costituito da 2 parti:

- **Tempo di recupero**: Tempo necessario per recuperare il file di backup dall'archivio e collocarlo nello storage standard. Questo è talvolta chiamato tempo di "reidratazione". Il tempo di recupero varia a seconda della priorità di ripristino scelta.

Tier di archiviazione	Priorità di ripristino e tempo di recupero		
	Alto	**Standard**	**Basso**
Ghiacciaio S3	3-5 minuti	3-5 ore	5-12 ore
S3 Glacier Deep Archive		12 ore	48 ore

- **Restore Time** (tempo di ripristino): Tempo di ripristino dei dati dal file di backup nello storage standard. Questo tempo non è diverso dall'operazione di ripristino tipica direttamente dallo storage standard, quando non si utilizza un livello di archiviazione.

Per ulteriori informazioni sulle opzioni di recupero di Amazon S3 Glacier e S3 Glacier Deep Archive, fare riferimento a. "Domande frequenti su Amazon relative a queste classi di storage".

Livelli di accesso all'archivio di Azure supportati con BlueXP backup and recovery

Il backup e ripristino BlueXP supporta un unico livello di accesso per l'archiviazione Azure e la maggior parte delle regioni.

NOTA Per passare da una versione all'altra dell'interfaccia utente BlueXP backup and recovery , fare riferimento a "Passa alla precedente interfaccia utente BlueXP backup and recovery" .

Livelli di accesso Azure Blob supportati per backup e ripristino BlueXP

Quando i file di backup vengono creati inizialmente, vengono memorizzati nel Tier di accesso *Cool*. Questo Tier è ottimizzato per l'archiviazione dei dati a cui si accede raramente, ma quando necessario, è possibile accedervi immediatamente.

Se i cluster di origine eseguono ONTAP 9.10.1 o versione successiva, è possibile scegliere di eseguire il tiering dei backup dallo storage *Cool* allo storage *Azure Archive* dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. Non è possibile accedere immediatamente ai dati di questo Tier quando necessario e richiede un costo di recupero più elevato, quindi è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione su questa pagina relativa al ripristino dei dati dall'archivio.

Si noti che quando si configura il backup e ripristino di BlueXP con questo tipo di regola del ciclo di vita, non è necessario configurare alcuna regola del ciclo di vita quando si imposta il container nell'account Azure.

"Scopri i Tier di accesso di Azure Blob".

Ripristina i dati dallo storage di archivio

Sebbene l'archiviazione di file di backup meno recenti nello storage di archiviazione sia molto meno costosa rispetto allo storage Cool, l'accesso ai dati da un file di backup in Azure Archive per le operazioni di ripristino richiederà più tempo e costerà più denaro.

Quanto costa ripristinare i dati da Azure Archive?

Quando si recuperano i dati da Azure Archive, è possibile scegliere due priorità di ripristino:

- **Alta**: Recupero più rapido, costi più elevati
- **Standard**: Recupero più lento, costi inferiori

Ogni metodo ha una tariffa di recupero per GB e una tariffa per richiesta diverse. Per informazioni dettagliate sui prezzi di Azure Archive per regione Azure, visitare il "Pagina dei prezzi di Azure".

La priorità alta non è supportata quando si ripristinano i dati da Azure ai sistemi StorageGRID.

Quanto tempo ci vorrà per ripristinare i dati archiviati in Azure Archive?

Il tempo di ripristino è costituito da 2 parti:

- **Tempo di recupero**: Il tempo necessario per recuperare il file di backup archiviato da Azure Archive e collocarlo in Cool Storage. Questo è talvolta chiamato tempo di "reidratazione". Il tempo di recupero varia a seconda della priorità di ripristino scelta:
  - **Alto**: < 1 ora
  - **Standard**: < 15 ore
- **Restore Time** (tempo di ripristino): Il tempo necessario per ripristinare i dati dal file di backup in Cool Storage. Questo tempo non è diverso dalla tipica operazione di ripristino direttamente da Cool storage, quando non si utilizza un Tier di archiviazione.

Per ulteriori informazioni sulle opzioni di recupero di Azure Archive, fare riferimento a. "Domande frequenti su Azure".

Livelli di archiviazione di Google supportati con BlueXP backup and recovery

Il backup e ripristino BlueXP supporta una classe di storage di archiviazione Google e la maggior parte delle regioni.

NOTA Per passare da una versione all'altra dell'interfaccia utente BlueXP backup and recovery , fare riferimento a "Passa alla precedente interfaccia utente BlueXP backup and recovery" .

Classi di storage di archivio supportate da Google per backup e ripristino BlueXP

Quando i file di backup vengono creati inizialmente, vengono memorizzati nello storage *Standard*. Questo Tier è ottimizzato per l'archiviazione dei dati a cui si accede raramente, ma che consente anche di accedervi immediatamente.

Se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di raggruppare i

backup più vecchi in storage *Archive* nell'interfaccia utente di backup e ripristino BlueXP dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. I dati in questo Tier richiederanno un costo di recupero più elevato, pertanto è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione su questa pagina relativa al ripristino dei dati dall'archivio.

Si noti che quando si configura il backup e ripristino di BlueXP con questo tipo di regola del ciclo di vita, non è necessario configurare alcuna regola del ciclo di vita quando si imposta il bucket nell'account Google.

"Scopri le classi di storage di Google".

Ripristina i dati dallo storage di archivio

Sebbene la memorizzazione di file di backup meno recenti nello storage di archiviazione sia molto meno costosa rispetto allo storage standard, l'accesso ai dati da un file di backup nello storage di archiviazione per le operazioni di ripristino richiederà un tempo leggermente più lungo e costerà più denaro.

Quanto costa ripristinare i dati da Google Archive?

Per informazioni dettagliate sui prezzi di Google Cloud Storage per regione, visita il "Pagina dei prezzi di Google Cloud Storage".

Quanto tempo ci vorrà per ripristinare gli oggetti archiviati in Google Archive?

Il tempo totale di ripristino è costituito da 2 parti:

- **Tempo di recupero**: Tempo necessario per recuperare il file di backup dall'archivio e collocarlo nello storage standard. Questo è talvolta chiamato tempo di "reidratazione". A differenza delle soluzioni di storage più "fredde" fornite da altri cloud provider, i tuoi dati sono accessibili in pochi millisecondi.
- **Restore Time** (tempo di ripristino): Tempo di ripristino dei dati dal file di backup nello storage standard. Questo tempo non è diverso dall'operazione di ripristino tipica direttamente dallo storage standard, quando non si utilizza un livello di archiviazione.

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 il backup e ripristino di BlueXP"
- "Avviso per il ripristino di un singolo file"