Documentazione di backup e ripristino BlueXP

BlueXP backup and recovery

NetApp
April 30, 2024

Sommario

Documentazione di backup e ripristino BlueXP

Note di rilascio

Novità del backup e ripristino BlueXP

Scopri le novità di BlueXP backup e recovery.

30 aprile 2024

Capacità di abilitare o disabilitare scansioni pianificate di ransomware

In precedenza potevi abilitare o disabilitare le scansioni ransomware, ma non potevi farlo per le scansioni pianificate.

Con questa release, puoi ora abilitare o disabilitare le scansioni ransomware pianificate sull'ultima copia Snapshot utilizzando l'opzione nella pagina Advanced Settings. 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.

Fare riferimento alle seguenti informazioni per i dettagli:

- "Gestire le impostazioni di backup"
- "Gestire le policy per ONTAP Volumes"
- "Impostazioni dei criteri di backup su oggetti"

04 aprile 2024

Capacità di abilitare o disabilitare le scansioni ransomware

In precedenza, quando hai abilitato il rilevamento di ransomware in una policy di backup, si sono verificate automaticamente le scansioni al momento della creazione del primo backup e al ripristino di un backup. In precedenza, il servizio ha eseguito la scansione di tutte le copie Snapshot e non è stato possibile disattivare le scansioni.

Con questa release, puoi ora abilitare o disabilitare le scansioni ransomware sull'ultima copia Snapshot, utilizzando l'opzione nella pagina Impostazioni avanzate. Se si attiva, le scansioni vengono eseguite settimanalmente per impostazione predefinita.

Fare riferimento alle seguenti informazioni per i dettagli:

- "Gestire le impostazioni di backup"
- "Gestire le policy per ONTAP Volumes"
- "Impostazioni dei criteri di backup su oggetti"

12 marzo 2024

Possibilità di eseguire "ripristini rapidi" dai backup cloud ai volumi ONTAP on-premise

Ora puoi eseguire un *ripristino rapido* di un volume dal cloud storage a un volume di destinazione ONTAP on-premise. In precedenza era possibile eseguire un ripristino rapido solo su un sistema Cloud Volumes ONTAP. 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 è molto più veloce di un ripristino completo di volumi e ripristina i metadati da una snapshot cloud a un volume di destinazione ONTAP. L'origine potrebbe provenire da AWS S3, BLOB di Azure, Google Cloud Services o NetApp StorageGRID.

Il sistema di destinazione ONTAP on-premise deve eseguire ONTAP versione 9.14.1 o successiva.

È possibile eseguire questa operazione utilizzando il processo di ricerca e ripristino, non il processo di ricerca e ripristino.

Per ulteriori informazioni, vedere "Ripristinare i dati ONTAP dai file di backup".

Possibilità di ripristinare file e cartelle da copie Snapshot e di replica

In precedenza, potevi ripristinare file e cartelle solo dalle copie di backup in AWS, Azure e Google Cloud Services. Ora, è possibile ripristinare file e cartelle da copie Snapshot locali e da copie di replica.

È possibile eseguire questa funzione utilizzando il processo di ricerca e ripristino, non utilizzando il processo di ricerca e ripristino.

01 febbraio 2024

Miglioramenti al backup e recovery di BlueXP per Virtual Machine

- Supporta il ripristino di macchine virtuali in una posizione alternativa
- Supporto per la mancata protezione dei datastore

15 dicembre 2023

Report disponibili per le copie Snapshot locali e di replica

In precedenza, era possibile generare report solo sulle copie di backup. Adesso puoi creare report sulle copie Snapshot locali e sulle copie Snapshot di replica.

Con questi rapporti, è possibile effettuare le seguenti operazioni:

- Assicurati che i dati critici siano protetti in base alla tua politica organizzativa.
- Accertarsi che i backup siano stati eseguiti correttamente per un gruppo di volumi.
- Offri una prova della protezione sui dati di produzione.

Fare riferimento a. "Report sulla copertura per la data Protection".

Tagging personalizzato disponibile sui volumi per l'ordinamento e il filtraggio

Ora puoi aggiungere tag personalizzati ai volumi a partire da ONTAP 9.13.1 in modo da raggruppare i volumi all'interno e tra gli ambienti di lavoro. In questo modo, puoi ordinare i volumi nelle pagine dell'interfaccia utente di backup e recovery di BlueXP e filtrarli nei report.

Backup del catalogo conservati per 30 giorni

In precedenza, Catalog.zip backup venivano conservati per 7 giorni. Ora, sono conservati per 30 giorni.

Fare riferimento a. "Ripristina i dati di backup e recovery di BlueXP nei siti oscuri".

23 ottobre 2023

creazione del criterio di backup 3-2-1 durante l'attivazione del backup

In precedenza, era necessario creare criteri personalizzati prima di avviare una snapshot, una replica o un backup. Ora puoi creare una policy durante il processo di attivazione del backup utilizzando l'interfaccia utente di backup e recovery di BlueXP.

"Ulteriori informazioni sulle politiche".

Supporto del ripristino rapido on-demand dei volumi ONTAP

Il backup e recovery di BlueXP ora permette di eseguire un "ripristino rapido" di un volume dal cloud storage a un sistema Cloud Volumes ONTAP. 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 sistema di destinazione Cloud Volumes ONTAP deve eseguire ONTAP versione 9.13.0 o successiva. "Ulteriori informazioni sul ripristino dei dati".

Inoltre, il monitoraggio dei processi di backup e ripristino di BlueXP mostra informazioni sullo stato di avanzamento dei processi di ripristino rapido.

Supporto per i processi pianificati in Job Monitor

Il monitoraggio del processo di backup e recovery di BlueXP, in precedenza, ha monitorato processi di backup e ripristino pianificati da volume a archivio oggetti, ma non processi di snapshot, replica, backup e ripristino locali pianificati tramite l'interfaccia utente o l'API.

Il monitoraggio dei processi di backup e ripristino di BlueXP include ora i processi pianificati per Snapshot locali, repliche e backup sullo storage a oggetti.

"Ulteriori informazioni su Job Monitor aggiornato".

13 ottobre 2023

Miglioramenti al backup e ripristino BlueXP per le applicazioni (nativo del cloud)

- Database Microsoft SQL Server
  - Supporta backup, ripristino e recovery di database Microsoft SQL Server che risiedono in Amazon FSX per NetApp ONTAP
  - Tutte le operazioni sono supportate solo tramite API REST.
- Sistemi SAP HANA
  - Durante l'aggiornamento del sistema, il montaggio e la disinstallazione automatici dei volumi vengono eseguiti utilizzando workflow e non script
  - Supporta aggiunta, rimozione, modifica, eliminazione, manutenzione, e l'aggiornamento dell'host plug-in utilizzando l'interfaccia utente

Miglioramenti al backup e ripristino BlueXP per le applicazioni (ibrido)

- Supporto del blocco dei dati e della protezione da ransomware

- Supporta lo spostamento dei backup da StorageGRID a Tier di archiviazione
- Supporta il backup dei dati delle applicazioni MongoDB, MySQL e PostgreSQL dai sistemi ONTAP on-premise ad Amazon Web Services, Microsoft Azure, Google Cloud Platform e StorageGRID. È possibile ripristinare i dati quando necessario.

Miglioramenti al backup e recovery di BlueXP per Virtual Machine

- Supporto per il modello di distribuzione proxy del connettore

11 settembre 2023

Nuova gestione delle policy per i dati ONTAP

Questa versione include la possibilità, all'interno dell'interfaccia utente, di creare policy Snapshot personalizzate, policy di replica e policy per i backup sullo storage a oggetti per i dati ONTAP.

"Ulteriori informazioni sulle politiche".

Supporto del ripristino di file e cartelle dai volumi nello storage a oggetti ONTAP S3

In precedenza, non era possibile ripristinare file e cartelle utilizzando la funzione "Sfoglia e ripristina" quando veniva eseguito il backup dei volumi nello storage a oggetti ONTAP S3. Questa versione elimina tale restrizione.

"Ulteriori informazioni sul ripristino dei dati".

Possibilità di archiviare immediatamente i dati di backup invece della prima scrittura su storage standard

Ora puoi inviare immediatamente i file di backup allo storage di archiviazione invece di scrivere i dati su un cloud storage standard. Ciò risulta particolarmente utile per gli utenti che raramente hanno bisogno di accedere ai dati da backup del cloud o per gli utenti che stanno sostituendo un ambiente di backup su nastro.

Supporto aggiuntivo per il backup e il ripristino di volumi SnapLock

Il backup e ripristino ora può eseguire il backup dei volumi FlexVol e FlexGroup configurati utilizzando le modalità SnapLock Compliance o SnapLock Enterprise Protection. 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.

"Scopri di più sulla protezione dei dati di ONTAP".

1 agosto 2023

- A causa di un importante miglioramento della sicurezza, il connettore ora richiede l'accesso a Internet outbound a un endpoint aggiuntivo per gestire le risorse di backup e ripristino all'interno dell'ambiente cloud pubblico. Se questo endpoint non è stato aggiunto all'elenco "consentito" del firewall, nell'interfaccia utente viene visualizzato un errore relativo a "Servizio non disponibile" o "Impossibile determinare lo stato del servizio":

  https://netapp-cloud-account.auth0.com

- Quando utilizzi il pacchetto "CVO Professional" per integrare backup e recovery di Cloud Volumes ONTAP e BlueXP, è necessaria un'iscrizione PAYGO per backup e recovery. Questo non era necessario in passato. Non verranno addebitati costi per l'abbonamento di backup e recovery ai sistemi Cloud Volumes ONTAP idonei, tuttavia tali costi sono necessari durante la configurazione del backup su nuovi volumi.

È stato aggiunto il supporto per il backup dei volumi nei bucket su sistemi ONTAP S3-configurati

Ora puoi utilizzare un sistema ONTAP che è stato configurato per Simple Storage Service (S3) per eseguire il backup dei volumi nello storage a oggetti. Questo è supportato sia per i sistemi ONTAP on-premise che per i sistemi Cloud Volumes ONTAP. Questa configurazione è supportata in implementazioni cloud e in sedi interne senza accesso a Internet (distribuzione in modalità "privata").

"Scopri di più".

Ora è possibile includere le istantanee esistenti da un volume protetto nei file di backup

In passato, era possibile includere copie Snapshot esistenti dai volumi in lettura e scrittura del file di backup iniziale nello storage a oggetti (invece di iniziare con la copia Snapshot più recente). Le copie Snapshot esistenti da volumi di sola lettura (volumi di data Protection) non sono state incluse nel file di backup. Ora puoi scegliere di includere copie Snapshot meno recenti nel file di backup per i volumi "DP".

La procedura guidata di backup visualizza un prompt alla fine della procedura di backup in cui è possibile selezionare queste "istantanee esistenti".

Il backup e recovery di BlueXP non supporta più il backup automatico dei volumi aggiunti in futuro

In precedenza era possibile selezionare una casella della procedura guidata di backup per applicare il criterio di backup selezionato a tutti i volumi futuri aggiunti al cluster. Questa funzione è stata rimossa in base al feedback dell'utente e alla mancanza di utilizzo di questa funzione. Sarà necessario abilitare manualmente i backup per tutti i nuovi volumi aggiunti al cluster.

La pagina monitoraggio processi è stata aggiornata con nuove funzioni

La pagina Job Monitoring fornisce ora ulteriori informazioni relative alla strategia di backup 3-2-1. Il servizio fornisce inoltre notifiche di avviso aggiuntive relative alla strategia di backup.

Il filtro del tipo "ciclo di vita di backup" è stato rinominato "conservazione". Utilizzare questo filtro per tenere traccia del ciclo di vita del backup e per identificare la scadenza di tutte le copie di backup. Il tipo di lavoro "conservazione" acquisisce tutti i processi di eliminazione Snapshot avviati su un volume protetto dal backup e recovery di BlueXP.

"Ulteriori informazioni su Job Monitor aggiornato".

6 luglio 2023

Il backup e ripristino di BlueXP include ora la possibilità di pianificare e creare copie Snapshot e volumi replicati

Il backup e ripristino BlueXP consente ora di implementare una strategia 3-2-1 in cui è possibile avere 3 copie dei dati di origine su 2 sistemi storage diversi e 1 copia nel cloud. Dopo l'attivazione, 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

"Scopri di più sulle nuove funzionalità di backup e ripristino a spettro completo".

Questa nuova funzionalità si applica anche alle operazioni di recovery. È possibile eseguire operazioni di ripristino da una copia Snapshot, da un volume replicato o da un file di backup nel cloud. In questo modo è possibile scegliere il file di backup che soddisfa i requisiti di ripristino, inclusi costi e velocità di ripristino.

Si noti che questa nuova funzionalità e l'interfaccia utente sono supportate solo per i cluster che eseguono ONTAP 9.8 o versione successiva. Se il cluster dispone di una versione precedente del software, è possibile continuare a utilizzare la versione precedente di backup e ripristino di BlueXP. Tuttavia, si consiglia di eseguire l'aggiornamento a una versione supportata di ONTAP per ottenere le funzionalità e le funzionalità più recenti. Per continuare a utilizzare la versione precedente del software, attenersi alla seguente procedura:

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).
2. Dalla pagina *Backup Settings*, fare clic sul pulsante di opzione **Visualizza la versione precedente di backup e ripristino di BlueXP**.

   Quindi, puoi gestire i cluster meno recenti utilizzando la versione precedente del software.

Possibilità di creare un container di storage per il backup sullo storage a oggetti

Per impostazione predefinita, quando si creano file di backup nello storage a oggetti, il servizio di backup e ripristino crea i bucket nello storage a oggetti. È possibile creare autonomamente i bucket se si desidera utilizzare un determinato nome o assegnare proprietà speciali. Se si desidera creare un bucket personalizzato, è necessario crearlo prima di avviare l'attivazione guidata. "Scopri come creare i bucket di storage a oggetti".

Questa funzionalità non è attualmente supportata quando si creano file di backup su sistemi StorageGRID.

04 luglio 2023

Miglioramenti al backup e ripristino BlueXP per le applicazioni (nativo del cloud)

- Sistemi SAP HANA
  - Supporta il ripristino di connessione e copia di volumi non dati e volumi non dati globali con protezione secondaria Azure NetApp Files
- Database Oracle
  - Supporta il ripristino dei database Oracle su Azure NetApp Files in una posizione alternativa
  - Supporta la catalogazione di Oracle Recovery Manager (RMAN) dei backup dei database Oracle su Azure NetApp Files

- Consente di impostare l'host del database in modalità di manutenzione per eseguire le attività di manutenzione

Miglioramenti al backup e ripristino BlueXP per le applicazioni (ibrido)

- Supporta il ripristino in una posizione alternativa
- Consente di montare backup di database Oracle
- Supporta lo spostamento dei backup da GCP a Tier di archiviazione

Miglioramenti al backup e ripristino BlueXP per macchine virtuali (ibrido)

- Supporta la protezione di datastore di tipo NFS e VMFS
- Consente di annullare la registrazione del plug-in SnapCenter per l'host VMware vSphere
- Supporta il refresh e il rilevamento di datastore e backup più recenti

5 giugno 2023

È possibile eseguire il backup e la protezione dei volumi FlexGroup utilizzando DataLock e la protezione ransomware

I criteri di backup per i volumi FlexGroup possono ora utilizzare la protezione DataLock e ransomware quando il cluster esegue ONTAP 9.13.1 o superiore.

Nuove funzionalità di reporting

È ora disponibile una scheda Report in cui è possibile generare un report di Backup Inventory, che include tutti i backup per un account specifico, un ambiente di lavoro o un inventario SVM. È inoltre possibile creare un report Data Protection Job Activity, che fornisce informazioni sulle operazioni di Snapshot, backup, clonazione e ripristino che possono essere utili per il monitoraggio dei contratti di servizio. Fare riferimento a. "Report sulla copertura per la data Protection".

Miglioramenti di Job Monitor

È ora possibile rivedere il *ciclo di vita del backup* come tipo di lavoro nella pagina Job Monitor, per tenere traccia dell'intero ciclo di vita del backup. È inoltre possibile visualizzare i dettagli di tutte le operazioni nella timeline di BlueXP. Fare riferimento a. "Monitorare lo stato dei processi di backup e ripristino".

Avviso di notifica aggiuntivo per etichette di policy non corrispondenti

È stato aggiunto un nuovo avviso di backup: "I file di backup non sono stati creati perché le etichette dei criteri Snapshot non corrispondono". Se la *label* definita in un criterio di backup non ha un'etichetta *corrispondente* nel criterio Snapshot, non verrà creato alcun file di backup. Per aggiungere l'etichetta mancante al criterio Snapshot del volume, è necessario utilizzare Gestione di sistema o l'interfaccia utente di ONTAP.

"Esaminare tutti gli avvisi che il backup e ripristino BlueXP può inviare".

Backup automatico dei file critici di backup e ripristino BlueXP in siti bui

Quando si utilizza il backup e ripristino BlueXP in un sito senza accesso a Internet, noto come implementazione in "modalità privata", le informazioni di backup e ripristino di BlueXP vengono memorizzate solo sul sistema di connessione locale. Questa nuova funzionalità esegue automaticamente il backup dei dati critici di backup e ripristino di BlueXP su un bucket del sistema StorageGRID connesso, in modo da poter

ripristinare questi dati su un nuovo connettore, se necessario. "Scopri di più"

8 maggio 2023

Le operazioni di ripristino a livello di cartella sono ora supportate dallo storage di archiviazione e dai backup bloccati

Se un file di backup è stato configurato con la protezione DataLock & ransomware o se il file di backup risiede nello storage di archiviazione, ora le operazioni di ripristino a livello di cartella sono supportate se il cluster esegue ONTAP 9.13.1 o superiore.

Le chiavi gestite dal cliente per più aree e progetti sono supportate quando si esegue il backup dei volumi su Google Cloud

Ora puoi scegliere un bucket che si trova in un progetto diverso rispetto al progetto delle chiavi di crittografia gestite dal cliente (CMEK). "Scopri di più sulla configurazione delle tue chiavi di crittografia gestite dal cliente".

Le regioni AWS China sono ora supportate per i file di backup

Le regioni AWS China Pechino (cn-North-1) e Ningxia (cn-Nordovest-1) sono ora supportate come destinazioni per i file di backup se il cluster esegue ONTAP 9.12.1 o superiore.

Si noti che i criteri IAM assegnati al connettore BlueXP devono modificare il nome risorsa AWS "arn" in tutte le sezioni *Resource* da "aws" a "aws-cn", ad esempio "arn:aws-cn:s3:::netapp-backup-*". Vedere "Backup dei dati Cloud Volumes ONTAP su Amazon S3" e. "Backup dei dati ONTAP on-premise su Amazon S3" per ulteriori informazioni.

Miglioramenti di Job Monitor

I processi avviati dal sistema, come le operazioni di backup in corso, sono ora disponibili nella scheda **monitoraggio del processo** per i sistemi ONTAP on-premise che eseguono ONTAP 9.13.1 o versione successiva. Le versioni precedenti di ONTAP visualizzano solo i processi avviati dall'utente.

14 aprile 2023

Miglioramenti al backup e ripristino BlueXP per le applicazioni (nativo del cloud)

- Database SAP HANA
  - Supporta l'aggiornamento del sistema basato su script
  - Supporta Single-file-Snapshot-Restore se è configurato il backup Azure NetApp Files
  - Supporta l'upgrade del plug-in
- Database Oracle
  - Miglioramenti all'implementazione del plug-in attraverso la semplificazione della configurazione utente sudo non root
  - Supporta l'upgrade del plug-in
  - Supporta il rilevamento automatico e la protezione basata su policy dei database Oracle su Azure NetApp Files
  - Supporta il ripristino del database Oracle nella posizione originale con ripristino granulare

Miglioramenti al backup e ripristino BlueXP per le applicazioni (ibrido)

- Il backup e ripristino BlueXP per le applicazioni (ibrido) è basato sul piano di controllo SaaS
- Sono state modificate le API REST ibride per allinearle alle API native del cloud.
- Supporta la notifica via email

4 aprile 2023

Possibilità di eseguire il backup dei dati nel cloud dai sistemi Cloud Volumes ONTAP in modalità "limitata"

Ora è possibile eseguire il backup dei dati dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali AWS, Azure e GCP in "modalità limitata". Ciò richiede l'installazione del connettore nella regione commerciale "limitata". "Scopri di più sulle modalità di implementazione di BlueXP". Vedere "Backup dei dati Cloud Volumes ONTAP su Amazon S3" e. "Backup dei dati Cloud Volumes ONTAP in Azure Blob".

Possibilità di eseguire il backup dei volumi ONTAP on-premise su ONTAP S3 utilizzando l'API

Le nuove funzionalità delle API consentono di eseguire il backup delle snapshot dei volumi in ONTAP S3 utilizzando il backup e ripristino BlueXP. Questa funzionalità è attualmente disponibile solo per i sistemi ONTAP on-premise. Per istruzioni dettagliate, consulta il blog "Integrazione con ONTAP S3 come destinazione".

Possibilità di modificare l'aspetto della ridondanza di zona dell'account di storage Azure da LRS a ZRS

Quando si creano backup dai sistemi Cloud Volumes ONTAP allo storage Azure, 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) se si desidera che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modifica della modalità di replica dell'account storage".

Miglioramenti di Job Monitor

- Sia le operazioni di backup e ripristino avviate dall'utente dall'interfaccia utente e dall'API di backup e ripristino di BlueXP, sia i processi avviati dal sistema, come le operazioni di backup in corso, sono ora disponibili nella scheda **monitoraggio del processo** per i sistemi Cloud Volumes ONTAP che eseguono ONTAP 9.13.0 o versione successiva. Le versioni precedenti di ONTAP visualizzano solo i processi avviati dall'utente.
- Oltre a poter scaricare un file CSV per la creazione di report su tutti i lavori, ora è possibile scaricare un file JSON per un singolo lavoro e visualizzarne i dettagli. "Scopri di più".
- Sono stati aggiunti due nuovi avvisi relativi al processo di backup: "Errore del processo pianificato" e "il processo di ripristino viene completato ma con avvisi". "Esaminare tutti gli avvisi che il backup e ripristino BlueXP può inviare".

9 marzo 2023

Le operazioni di ripristino a livello di cartella ora includono tutte le sottocartelle e i file

In passato, quando si ripristinava una cartella, venivano ripristinati solo i file di tale cartella, senza alcuna sottocartella o file di sottocartelle. Ora, se si utilizza ONTAP 9.13.0 o versione successiva, vengono ripristinate tutte le sottocartelle e i file nella cartella selezionata. Ciò consente di risparmiare molto tempo e denaro nei casi in cui si dispone di più cartelle nidificate in una cartella di primo livello.

Capacità di eseguire il backup dei dati dai sistemi Cloud Volumes ONTAP nei siti con una connettività in uscita limitata

Ora puoi eseguire il backup dei dati dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali di AWS e Azure su Amazon S3 o Azure Blob. Questo richiede che il connettore venga installato in "modalità limitata" su un host Linux nella regione commerciale e che venga installato anche il sistema Cloud Volumes ONTAP. Vedere "Backup dei dati Cloud Volumes ONTAP su Amazon S3" e. "Backup dei dati Cloud Volumes ONTAP in Azure Blob".

Miglioramenti multipli di Job Monitor

- La pagina Job Monitoring ha aggiunto un filtro avanzato che consente di cercare i processi di backup e ripristino in base al tempo, al carico di lavoro (volumi, applicazioni, macchine virtuali o Kubernetes), Tipo di lavoro, stato, ambiente di lavoro e VM di storage. È anche possibile inserire testo libero per cercare qualsiasi risorsa, ad esempio "application_3". "Scopri come utilizzare i filtri avanzati".
- Sia le operazioni di backup e ripristino avviate dall'utente dall'interfaccia utente e dall'API di backup e ripristino di BlueXP, sia i processi avviati dal sistema, come le operazioni di backup in corso, sono ora disponibili nella scheda **monitoraggio del processo** per i sistemi Cloud Volumes ONTAP che eseguono ONTAP 9.13.0 o versione successiva. Le versioni precedenti dei sistemi Cloud Volumes ONTAP e dei sistemi ONTAP on-premise visualizzano solo i processi avviati dall'utente.

6 febbraio 2023

Possibilità di spostare i file di backup meno recenti nello storage di archiviazione Azure dai sistemi StorageGRID

Ora puoi eseguire il tiering dei file di backup più vecchi dai sistemi StorageGRID allo storage di archiviazione in Azure. Ciò consente di liberare spazio sui sistemi StorageGRID e di risparmiare denaro utilizzando una classe di storage economica per i file di backup meno recenti.

Questa funzionalità è disponibile se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza 11.4 o versione successiva. "Scopri di più qui".

La protezione DataLock e ransomware può essere configurata per i file di backup in Azure Blob

DataLock e ransomware Protection sono ora supportati per i file di backup memorizzati in Azure Blob. Se il sistema Cloud Volumes ONTAP o on-premise ONTAP utilizza ONTAP 9.12.1 o versione successiva, è ora possibile bloccare i file di backup ed eseguirne la scansione per rilevare eventuali ransomware. "Scopri di più su come proteggere i backup utilizzando DataLock e la protezione ransomware".

Miglioramenti del volume FlexGroup di backup e ripristino

- È ora possibile scegliere più aggregati durante il ripristino di un volume FlexGroup. Nell'ultima release è possibile selezionare solo un singolo aggregato.
- Il ripristino del volume FlexGroup è ora supportato sui sistemi Cloud Volumes ONTAP. Nell'ultima release è possibile eseguire il ripristino solo su sistemi ONTAP on-premise.

I sistemi Cloud Volumes ONTAP possono spostare i backup meno recenti nello storage di Google Archives

I file di backup vengono creati inizialmente nella classe di storage Google Standard. Ora è possibile utilizzare il backup e il ripristino BlueXP per eseguire il tiering dei backup più vecchi sullo storage Google Archive per un'ulteriore ottimizzazione dei costi. L'ultima release supportava questa funzionalità solo con cluster ONTAP on-premise, ora sono supportati i sistemi Cloud Volumes ONTAP implementati in Google Cloud.

Le operazioni di ripristino del volume consentono ora di selezionare la SVM in cui si desidera ripristinare i dati del volume

Ora ripristini i dati dei volumi su diverse macchine virtuali dello storage nei cluster ONTAP. In passato non era possibile scegliere la VM di storage.

Supporto migliorato per i volumi nelle configurazioni MetroCluster

Quando si utilizza ONTAP 9.12.1 GA o superiore, il backup è ora supportato quando si è connessi al sistema primario in una configurazione MetroCluster. L'intera configurazione di backup viene trasferita al sistema secondario in modo che i backup nel cloud continuino automaticamente dopo lo switchover.

"Per ulteriori informazioni, vedere limitazioni del backup".

9 gennaio 2023

Possibilità di spostare i file di backup meno recenti nello storage di archiviazione AWS S3 dai sistemi StorageGRID

Ora è possibile eseguire il tiering dei file di backup più vecchi dai sistemi StorageGRID allo storage di archiviazione in AWS S3. Ciò consente di liberare spazio sui sistemi StorageGRID e di risparmiare denaro utilizzando una classe di storage economica per i file di backup meno recenti. È possibile scegliere di eseguire il Tier dei backup nello storage AWS S3 Glacier o S3 Glacier Deep Archive.

Questa funzionalità è disponibile se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza 11.3 o versione successiva. "Scopri di più qui".

Possibilità di selezionare le chiavi gestite dal cliente per la crittografia dei dati su Google Cloud

Quando si esegue il backup dei dati dai sistemi ONTAP su Google Cloud Storage, è ora possibile selezionare 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 Google. Devi solo configurare le chiavi di crittografia gestite dal cliente in Google, quindi inserire i dettagli durante l'attivazione del backup e ripristino BlueXP.

Il ruolo "Storage Admin" non è più necessario per l'account del servizio per creare backup in Google Cloud Storage

Nelle versioni precedenti, il ruolo "Storage Admin" era richiesto per l'account del servizio che consente il backup e il ripristino BlueXP per accedere ai bucket di storage Google Cloud. Ora è possibile creare un ruolo personalizzato con un set ridotto di autorizzazioni da assegnare all'account del servizio. "Scopri come preparare il tuo Google Cloud Storage per i backup".

È stato aggiunto il supporto per il ripristino dei dati utilizzando Search & Restore nei siti senza accesso a Internet

Se si esegue il backup dei dati da un cluster ONTAP on-premise a StorageGRID in un sito senza accesso a Internet, noto anche come sito oscuro o offline, è ora possibile utilizzare l'opzione Cerca e ripristina per ripristinare i dati, se necessario. Questa funzionalità richiede l'implementazione di BlueXP Connector (versione 3.9.25 o superiore) nel sito offline.

"Scopri come ripristinare i dati ONTAP utilizzando Cerca Ripristina".
"Scopri come installare il connettore nel tuo sito offline".

Possibilità di scaricare la pagina dei risultati di Job Monitoring come report .csv

Dopo aver filtrato la pagina Job Monitoring per visualizzare i lavori e le azioni a cui si è interessati, è possibile generare e scaricare un file .csv di tali dati. Quindi, è possibile analizzare le informazioni o inviare il report ad altre persone della propria organizzazione. "Scopri come generare un report di monitoraggio dei processi".

19 dicembre 2022

Miglioramenti al Cloud Backup per le applicazioni

- Database SAP HANA
  - Supporta il backup e il ripristino basati su policy dei database SAP HANA residenti su Azure NetApp Files
  - Supporta policy personalizzate
- Database Oracle
  - Aggiungere host e implementare il plug-in automaticamente
  - Supporta policy personalizzate
  - Supporta backup, ripristino e clone basati su policy di database Oracle residenti su Cloud Volumes ONTAP
  - Supporta il backup e il ripristino basati su policy dei database Oracle residenti su Amazon FSX per NetApp ONTAP
  - Supporta il ripristino dei database Oracle utilizzando il metodo Connect-and-copy
  - Supporta Oracle 21c
  - Supporta la clonazione del database Oracle nativo nel cloud

Miglioramenti al Cloud Backup per macchine virtuali

- Macchine virtuali
  - Eseguire il backup delle macchine virtuali dallo storage secondario on-premise
  - Supporta policy personalizzate
  - Supporta Google Cloud Platform (GCP) per il backup di uno o più datastore
  - Supporta lo storage cloud a basso costo come Glacier, Deep Glacier e Azure Archive

6 dicembre 2022

Modifiche richieste all'endpoint di accesso a Internet in uscita del connettore

A causa di una modifica nel Cloud Backup, è necessario modificare i seguenti endpoint del connettore per un'operazione di backup cloud corretta:

Vecchio endpoint	Nuovo endpoint
https://cloudmanager.cloud.netapp.com	https://api.bluexp.netapp.com
https://*.cloudmanager.cloud.netapp.com	https://*.api.bluexp.netapp.com

Consulta l'elenco completo degli endpoint per il "AWS", "Google Cloud", o. "Azure" ambiente cloud.

Supporto per la selezione della classe di storage Google Archival nell'interfaccia utente

I file di backup vengono creati inizialmente nella classe di storage Google Standard. Ora puoi utilizzare l'interfaccia utente di Cloud Backup per eseguire il tiering dei backup più vecchi sullo storage di Google Archive dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi.

Questa funzionalità è attualmente supportata per i cluster ONTAP on-premise che utilizzano ONTAP 9.12.1 o versione successiva. Attualmente non è disponibile per i sistemi Cloud Volumes ONTAP.

Supporto per FlexGroup Volumes

Cloud Backup ora supporta il backup e il ripristino dei volumi FlexGroup. Quando utilizzi ONTAP 9.12.1 o superiore, puoi eseguire il backup dei volumi FlexGroup su cloud storage pubblico e privato. Se si dispone di ambienti di lavoro che includono volumi FlexVol e FlexGroup, una volta aggiornato il software ONTAP, è possibile eseguire il backup di qualsiasi volume FlexGroup su tali sistemi.

"Consulta l'elenco completo dei tipi di volume supportati".

Possibilità di ripristinare i dati dai backup su un aggregato specifico nei sistemi Cloud Volumes ONTAP

Nelle versioni precedenti era possibile selezionare l'aggregato solo quando si ripristinano i dati su sistemi ONTAP on-premise. Questa funzionalità ora funziona quando si ripristinano i dati sui sistemi Cloud Volumes ONTAP.

2 novembre 2022

Possibilità di esportare copie Snapshot meno recenti nei file di backup di riferimento

Se nell'ambiente di lavoro sono presenti copie Snapshot locali per volumi che corrispondono alle etichette della pianificazione di backup (ad esempio, giornaliere, settimanali, ecc.), è possibile esportare tali snapshot cronologici nello storage a 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.

Questa opzione è disponibile quando si attiva Cloud Backup per gli ambienti di lavoro. Questa impostazione può essere modificata anche in un secondo momento in "Pagina Advanced Settings (Impostazioni avanzate)".

Cloud Backup può ora essere utilizzato per l'archiviazione di volumi non più necessari sul sistema di origine

Ora è possibile eliminare la relazione di backup per un volume. Questo offre un meccanismo di archiviazione se si desidera interrompere la creazione di nuovi file di backup ed eliminare il volume di origine, conservando 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. "Scopri come".

È stato aggiunto il supporto per ricevere gli avvisi Cloud Backup tramite e-mail e nel Centro notifiche

Cloud Backup è stato integrato nel servizio di notifica BlueXP. È possibile visualizzare le notifiche di Cloud Backup facendo clic sulla campana di notifica nella barra dei menu di BlueXP. È inoltre possibile configurare BlueXP per inviare notifiche via email come avvisi, in modo da essere informati di importanti attività del sistema anche quando non si è connessi al sistema. L'e-mail può essere inviata a tutti i destinatari che devono essere a conoscenza dell'attività di backup e ripristino. "Scopri come".

La nuova pagina Advanced Settings (Impostazioni avanzate) consente di modificare le impostazioni di backup a livello di cluster

Questa nuova pagina consente di modificare molte impostazioni di backup a livello di cluster impostate durante l'attivazione del backup cloud per ciascun sistema ONTAP. È inoltre possibile modificare alcune impostazioni applicate come impostazioni di backup predefinite. Il set completo di impostazioni di backup che è possibile modificare comprende:

- Le chiavi di storage che danno al sistema ONTAP l'autorizzazione ad accedere allo storage a oggetti
- Larghezza di banda della rete allocata per caricare i backup nello storage a oggetti
- L'impostazione (e il criterio) di backup automatico per i volumi futuri
- Classe di storage di archiviazione (solo AWS)
- Se le copie Snapshot storiche sono incluse nei file di backup di riferimento iniziali
- Se le istantanee "annuali" vengono rimosse dal sistema di origine
- Spazio IP ONTAP connesso allo storage a oggetti (in caso di selezione errata durante l'attivazione)

"Scopri di più sulla gestione delle impostazioni di backup a livello di cluster".

Ora è possibile ripristinare i file di backup utilizzando Search & Restore quando si utilizza un connettore on-premise

Nella release precedente, è stato aggiunto il supporto per la creazione di file di backup nel cloud pubblico quando il connettore viene distribuito nelle vostre sedi. In questa versione, il supporto è stato continuato per consentire l'utilizzo di Search & Restore per ripristinare i backup da Amazon S3 o Azure Blob quando il connettore viene distribuito nella tua sede. Search & Restore supporta anche il ripristino dei backup dai sistemi StorageGRID ai sistemi ONTAP on-premise.

A questo punto, il connettore deve essere implementato nella piattaforma Google Cloud quando si utilizza Search & Restore per ripristinare i backup da Google Cloud Storage.

La pagina Job Monitoring è stata aggiornata

Sono stati apportati i seguenti aggiornamenti a "Pagina Job Monitoring":

- È disponibile una colonna per "workload", che consente di filtrare la pagina per visualizzare i job per i seguenti servizi di backup: Volumi, applicazioni, macchine virtuali e Kubernetes.
- È possibile aggiungere nuove colonne per "Nome utente" e "tipo di lavoro" se si desidera visualizzare questi dettagli per un processo di backup specifico.
- La pagina Dettagli lavoro visualizza tutti i lavori secondari in esecuzione per completare il lavoro principale.
- La pagina viene aggiornata automaticamente ogni 15 minuti in modo da visualizzare sempre i risultati più recenti dello stato del lavoro. E fare clic sul pulsante **Refresh** (Aggiorna) per aggiornare immediatamente la pagina.

Miglioramenti del backup multiaccount AWS

Se si desidera utilizzare un account AWS diverso da quello utilizzato per i volumi di origine per i backup Cloud Volumes ONTAP, 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. In passato, era necessario configurare molte impostazioni nella console AWS, ma non è più necessario farlo.

28 settembre 2022

Miglioramenti al Cloud Backup per le applicazioni

- Supporta Google Cloud Platform (GCP) e StorageGRID per il backup di snapshot coerenti con l'applicazione
- Creare policy personalizzate
- Supporta lo storage di archiviazione
- Eseguire il backup delle applicazioni SAP HANA
- Eseguire il backup delle applicazioni Oracle e SQL presenti nell'ambiente VMware
- Eseguire il backup delle applicazioni dallo storage secondario on-premise
- Disattivare i backup
- Annullare la registrazione del server SnapCenter

Miglioramenti al Cloud Backup per macchine virtuali

- Supporta StorageGRID per il backup di uno o più datastore
- Creare policy personalizzate

19 settembre 2022

È possibile configurare la protezione DataLock e ransomware per i file di backup nei sistemi StorageGRID

L'ultima release ha introdotto *DataLock e ransomware Protection* per i backup memorizzati nei bucket Amazon S3. Questa release estende il supporto ai file di backup memorizzati nei sistemi StorageGRID. Se il cluster utilizza ONTAP 9.11.1 o versione successiva e il sistema StorageGRID esegue la versione 11.6.0.3 o successiva, questa nuova opzione dei criteri di backup è disponibile. "Scopri di più su come utilizzare DataLock e la protezione ransomware per proteggere i tuoi backup".

Tenere presente che è necessario eseguire un connettore con la versione 3.9.22 o superiore del software. Il connettore deve essere installato in sede e può essere installato in un sito con o senza accesso a Internet.

Il ripristino a livello di cartella è ora disponibile dai file di backup

Ora è possibile ripristinare una cartella da un file di backup se si ha bisogno di accedere a tutti i file in tale cartella (directory o condivisione). Il ripristino di una cartella è molto più efficiente del ripristino di un intero volume. Questa funzionalità è disponibile per le operazioni di ripristino utilizzando sia il metodo Browse & Restore che il metodo Search & Restore quando si utilizza ONTAP 9.11.1 o versione successiva. In questo momento è possibile selezionare e ripristinare solo una singola cartella e ripristinare solo i file di tale cartella. Non vengono ripristinate sottocartelle o file di sottocartelle.

Il ripristino a livello di file è ora disponibile dai backup spostati nello storage di archiviazione

In passato era possibile ripristinare solo i volumi dai file di backup spostati nello storage di archiviazione (solo AWS e Azure). Ora è possibile ripristinare singoli file da questi file di backup archiviati. Questa funzionalità è disponibile per le operazioni di ripristino utilizzando sia il metodo Browse & Restore che il metodo Search & Restore quando si utilizza ONTAP 9.11.1 o versione successiva.

Il ripristino a livello di file consente ora di sovrascrivere il file di origine originale

In passato, un file ripristinato nel volume originale veniva sempre ripristinato come nuovo file con il prefisso "Restore_<file_name>". È ora possibile scegliere di sovrascrivere il file di origine originale quando si ripristina il file nella posizione originale sul volume. Questa funzionalità è disponibile per le operazioni di ripristino utilizzando sia il metodo Browse & Restore che il metodo Search & Restore.

Trascinare e rilasciare per abilitare il backup cloud sui sistemi StorageGRID

Se il "StorageGRID" La destinazione dei backup esiste come ambiente di lavoro su Canvas. È possibile trascinare l'ambiente di lavoro ONTAP on-premise sulla destinazione per avviare l'installazione guidata del backup cloud.

Limitazioni note

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

Limitazioni di backup e ripristino per ONTAP Volumes

Limitazioni della replica

- 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 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.
- 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.

Ripristinare le limitazioni

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 sui backup dei volumi FlexGroup.
- 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.
- 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.

Inizia subito

Informazioni su backup e ripristino BlueXP

Il servizio di backup e ripristino BlueXP offre una protezione dei dati efficiente, sicura e conveniente per i dati NetApp ONTAP, Kubernetes volumi persistenti, database e macchine virtuali, sia on-premise che nel cloud. I backup vengono generati e memorizzati automaticamente in un archivio di oggetti nel tuo account di cloud pubblico o privato.

Il servizio esegue una replica incrementale a livello di blocco e per sempre e preserva tutte le efficienze dello storage, riducendo in modo significativo la quantità di dati replicati e memorizzati. Inoltre, pagherai solo ciò che è protetto e utilizzi i Tier di storage più economici disponibili, rendendo il backup e ripristino BlueXP molto conveniente.

Se necessario, è possibile ripristinare un intero *volume* da un backup nello stesso ambiente di lavoro o in un ambiente di lavoro diverso. Quando si esegue il backup dei dati ONTAP, è anche possibile scegliere di ripristinare una cartella o uno o più *file* da un backup nello stesso ambiente di lavoro o in un altro ambiente di lavoro.

"Scopri di più sul backup e ripristino BlueXP".

Il backup e il ripristino possono essere utilizzati per:

- Backup e ripristino dei dati dei volumi ONTAP da sistemi Cloud Volumes ONTAP e ONTAP on-premise. "Scopri le funzionalità dettagliate qui".
- Eseguire il backup e il ripristino dei volumi persistenti di Kubernetes. "Scopri le funzionalità dettagliate qui".
- Eseguire il backup delle istantanee coerenti con l'applicazione dai sistemi ONTAP on-premise utilizzando il backup e il ripristino BlueXP per le applicazioni. "Scopri le funzionalità dettagliate qui".
- Eseguire il backup dei datastore nel cloud e ripristinare le macchine virtuali nel vCenter on-premise utilizzando il backup e ripristino BlueXP per VMware. "Scopri le funzionalità dettagliate qui".

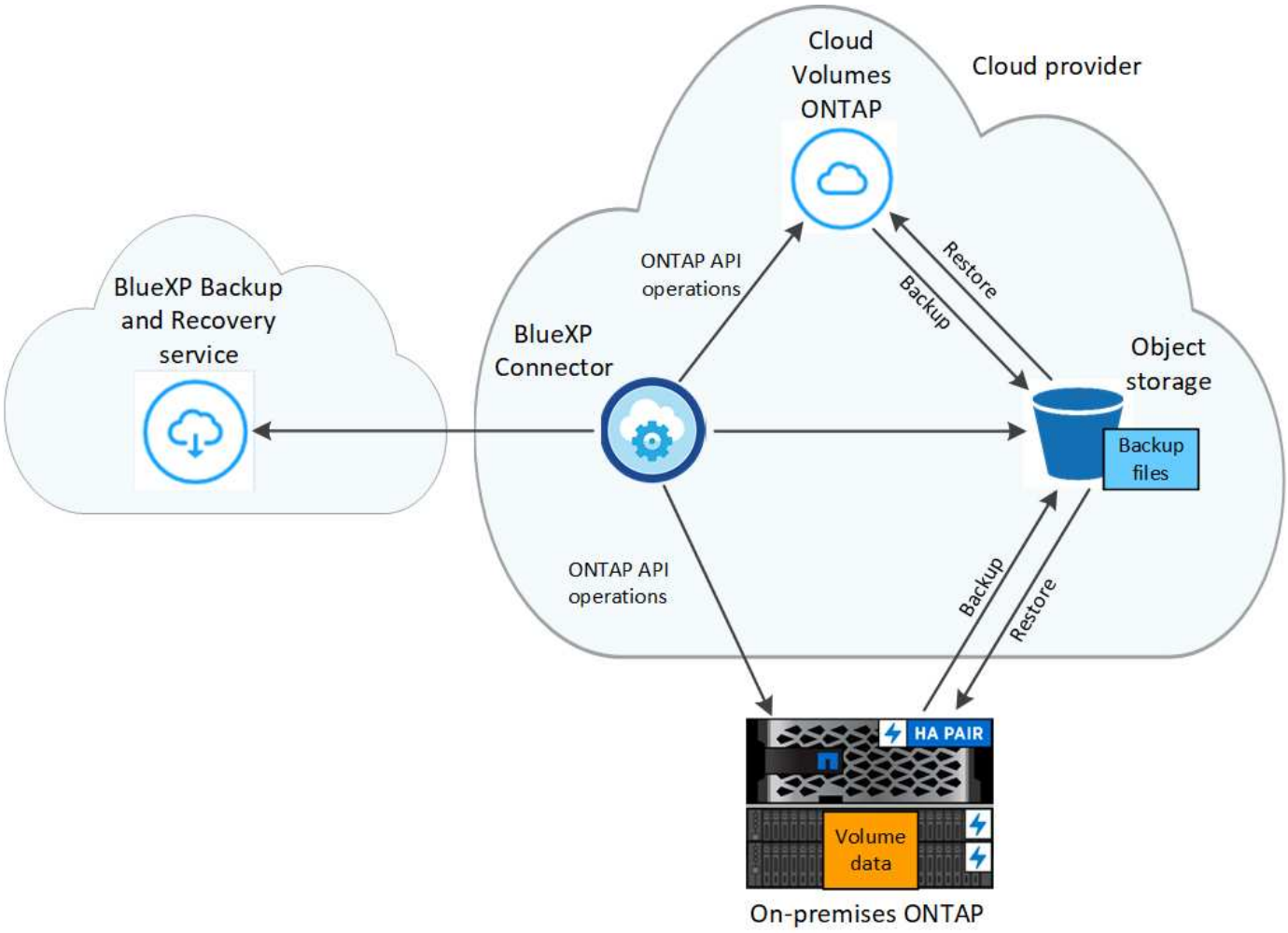
"Guarda una rapida demo"

> Quando BlueXP Connector viene implementato in un'area governativa nel cloud o in un sito senza accesso a Internet (un sito oscuro), il backup e ripristino BlueXP supporta solo le operazioni di backup e ripristino dai sistemi ONTAP. Quando si utilizzano questi metodi di implementazione, il backup e ripristino BlueXP non supporta le operazioni di backup e ripristino da cluster, applicazioni o macchine virtuali Kubernetes.

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. Le snapshot dei volumi non sono incluse nell'immagine di backup. 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.

La seguente immagine mostra la relazione tra i componenti:



Dove risiedono i backup

Le copie di backup vengono memorizzate in un archivio di oggetti creato da BlueXP nel tuo account cloud. Esiste un archivio di oggetti per cluster/ambiente di lavoro e BlueXP nomina l'archivio di oggetti come segue: `netapp-backup-clusteruuid`. 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 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.

Quando vengono eseguiti i backup

- I backup orari iniziano 5 minuti dopo l'ora, ogni ora.
- I backup giornalieri iniziano ogni giorno dopo la mezzanotte.
- I backup settimanali iniziano subito dopo la mezzanotte di domenica mattina.
- I backup mensili iniziano appena dopo la mezzanotte del primo giorno di ogni mese.

- I backup annuali iniziano appena dopo la mezzanotte del primo giorno dell'anno.

L'ora di inizio si basa sul fuso orario impostato su ciascun sistema ONTAP di origine. Non è possibile pianificare le operazioni di backup a un orario specificato dall'utente dall'interfaccia utente. Per ulteriori informazioni, contattare il tecnico di sistema.

Le copie di backup sono associate al tuo account NetApp

Le copie di backup sono associate a "Account NetApp" In cui si trova il connettore BlueXP.

Se si dispone di più connettori nello stesso account NetApp, ciascun connettore visualizza lo stesso elenco di backup. Che include i backup associati a Cloud Volumes ONTAP e alle istanze di ONTAP on-premise di altri connettori.

Impostare le licenze per il backup e ripristino BlueXP

Puoi concedere in licenza il backup e il ripristino BlueXP acquistando un abbonamento al mercato annuale o pay-as-you-go (PAYGO) dal tuo cloud provider oppure acquistando una licenza Bring-Your-Own (BYOL) 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.
- La licenza BYOL (Bring-Your-Own-License) di backup e ripristino BlueXP è una licenza mobile che è possibile utilizzare in tutti i sistemi associati all'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

Se ti iscrivi a un abbonamento pay-as-you-go nel marketplace del tuo cloud provider, è disponibile una prova gratuita di 30 giorni di backup e recovery BlueXP. 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 backup e il ripristino BlueXP, basta "Annullare la registrazione del backup e ripristino BlueXP dall'ambiente di lavoro" prima della fine della prova, non ti verrà addebitato alcun costo.

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 anche se si dispone di una versione di prova gratuita o se si porta la 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.

- Un pacchetto "CVO Edge cache" ha le stesse funzionalità del pacchetto "CVO Professional", ma include anche il supporto per "Caching edge BlueXP" servizio. Hai diritto a implementare un sistema edge caching BlueXP per ogni 3 TIB di capacità fornita sul sistema Cloud Volumes ONTAP. Questa opzione è disponibile nei mercati Azure e Google e non consente di eseguire il backup dei dati ONTAP on-premise.

"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 informazioni sui prezzi, consulta l'offerta BlueXP Marketplace".
- Azure: "Per informazioni sui prezzi, consulta l'offerta BlueXP Marketplace".
- Google Cloud: "Per informazioni sui prezzi, consulta l'offerta BlueXP Marketplace".

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 i 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 si desidera utilizzare questa opzione, è possibile impostare il contratto annuale quando si crea un ambiente di lavoro Cloud Volumes ONTAP e BlueXP richiede di iscriversi al marketplace AWS.

Quando si utilizza Azure, sono disponibili due contratti annuali da "Pagina del marketplace di Azure" Per i 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 vuoi utilizzare questa opzione, puoi impostare un contratto annuale quando crei un ambiente di lavoro Cloud Volumes ONTAP e BlueXP ti richiede di iscriverti ad Azure Marketplace.

Quando si utilizza GCP, contattare il rappresentante commerciale NetApp per acquistare un contratto annuale. Il contratto è disponibile come offerta privata in Google Cloud Marketplace.

Una volta che NetApp condivide l'offerta privata con te, puoi selezionare il piano annuale quando ti iscrivi da Google Cloud Marketplace durante l'attivazione del backup e ripristino BlueXP.

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 ripristino BYOL BlueXP è una licenza mobile in cui la capacità totale è condivisa tra tutti i sistemi associati all'account BlueXP. Per i sistemi ONTAP, è possibile ottenere una stima approssimativa della

capacità necessaria eseguendo il comando CLI `volume show -fields logical-used-by-afs` per i volumi di cui si intende eseguire 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.

Ottenere il file di licenza per il backup e ripristino BlueXP

Dopo aver acquistato la licenza di backup e recovery BlueXP (backup cloud), attiva la licenza in BlueXP inserendo il numero di serie di backup e recovery di BlueXP e l'account NSS (NetApp Support Site), oppure caricando il file di licenza NetApp (NLF). Se si prevede di utilizzare questo metodo, la procedura riportata di seguito mostra come ottenere il file di licenza NLF.

Se esegui backup e recovery di BlueXP in un sito on-premise che non dispone di accesso a Internet, significa che hai implementato il connettore BlueXP in "modalità privata", è necessario ottenere il file di licenza da un sistema connesso a internet. L'attivazione della licenza tramite il numero di serie e l'account del sito di supporto NetApp non è disponibile per le installazioni in modalità privata.

Prima di iniziare

Prima di iniziare, è necessario disporre delle seguenti informazioni:

- Numero di serie di backup e recovery di BlueXP

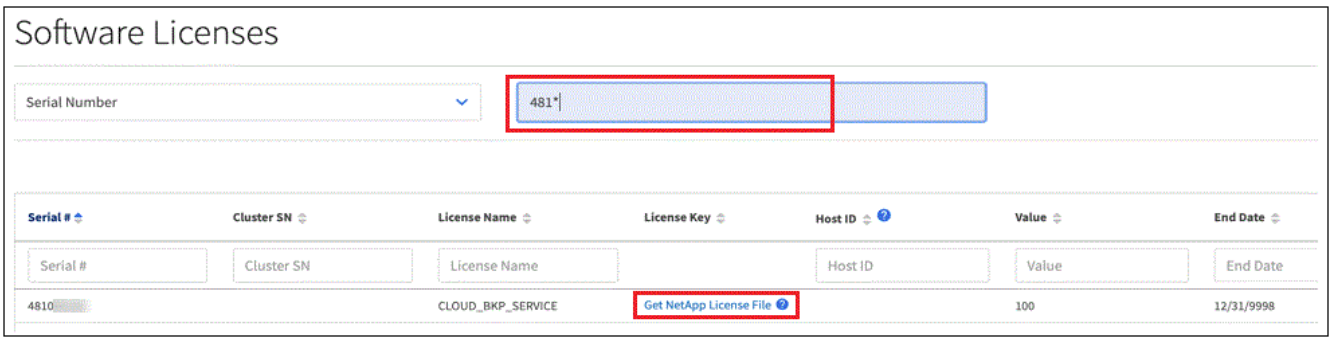
  Individua questo numero nell'ordine di vendita o contatta l'account team per ottenere queste informazioni.

- ID account BlueXP

  Puoi trovare il tuo ID account BlueXP selezionando l'elenco a discesa **account** nella parte superiore di BlueXP, quindi facendo clic su **Gestisci account** accanto all'account. L'ID account si trova nella scheda Panoramica. Per il sito in modalità privata senza accesso a Internet, utilizzare **account-DARKSITE1**.

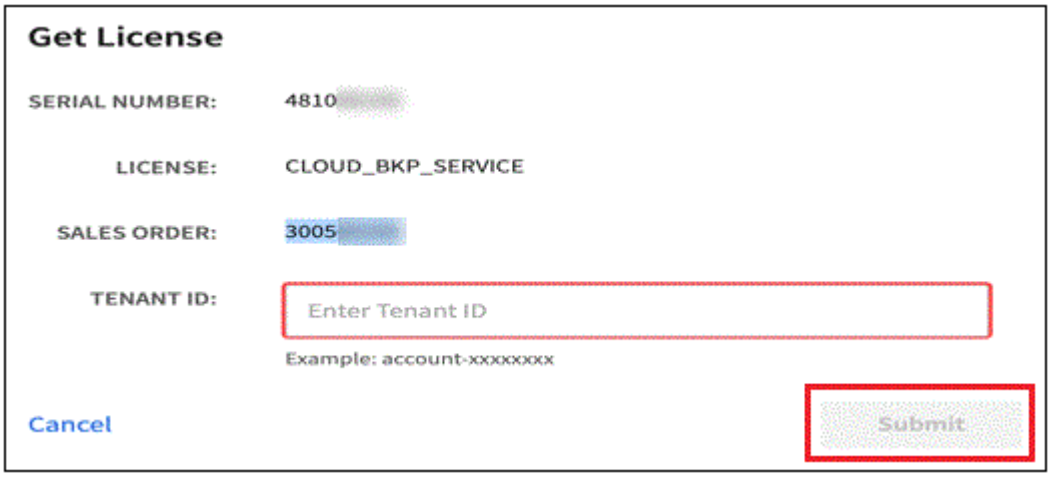
Fasi

1. Accedere a "Sito di supporto NetApp" E fare clic su **sistemi > licenze software**.
2. Inserire il numero di serie della licenza di backup e ripristino BlueXP.



3. Nella colonna **chiave di licenza**, fare clic su **Ottieni file di licenza NetApp**.

4. Inserire l'ID account BlueXP (chiamato ID tenant sul sito di supporto) e fare clic su **Submit** (Invia) per scaricare il file di licenza.



Aggiungere al proprio account le licenze BYOL di backup e ripristino BlueXP

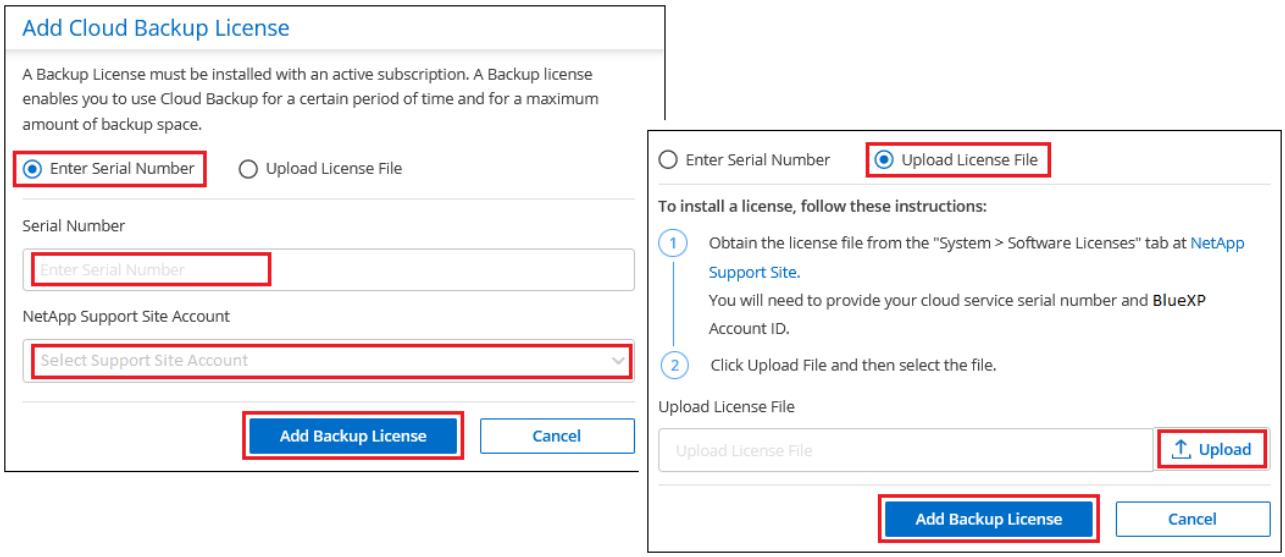
Dopo aver acquistato una licenza di backup e ripristino BlueXP per il tuo account NetApp, devi aggiungere la licenza a BlueXP.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Digital wallet**, quindi selezionare la scheda **licenze servizi dati**.
2. Fare clic su **Aggiungi licenza**.
3. Nella finestra di dialogo *Add License*, inserire le informazioni sulla licenza e fare clic su **Add License**:
   - Se si dispone del numero di serie della licenza di backup e si conosce l'account NSS, selezionare l'opzione **inserire il numero di serie** e immettere le informazioni desiderate.

     Se il tuo account NetApp Support Site non è disponibile nell'elenco a discesa, "Aggiungere l'account NSS a BlueXP".

   - Se si dispone del file di licenza di backup (richiesto se installato in un sito buio), selezionare l'opzione **Upload License file** (carica file di licenza) e seguire le istruzioni per allegare il file.

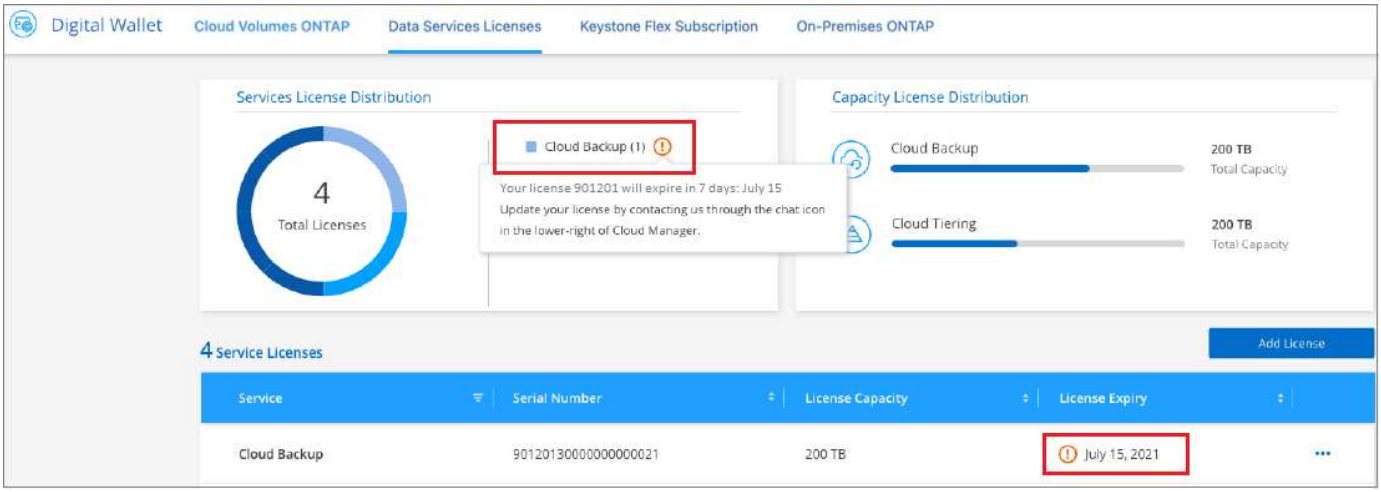


Risultato

BlueXP aggiunge la licenza in modo che il backup e ripristino BlueXP sia attivo.

Aggiornare una licenza BYOL di backup e ripristino BlueXP

Se la durata della licenza è prossima alla data di scadenza, o se la capacità concessa in licenza sta raggiungendo il limite, l'utente verrà avvisato nell'interfaccia utente di backup. Questo stato viene visualizzato anche nella pagina del portafoglio digitale BlueXP e in "Notifiche".



È possibile aggiornare la licenza di backup e ripristino BlueXP prima della scadenza, in modo da non interrompere la capacità di backup e ripristino dei dati.

Fasi

1. Fare clic sull'icona della chat in basso a destra in BlueXP oppure contattare il supporto per richiedere un'estensione del termine o una capacità aggiuntiva alla licenza di backup e ripristino BlueXP per il numero di serie specifico.

   Dopo aver pagato la licenza e averla registrata nel NetApp Support Site, BlueXP aggiorna automaticamente la licenza nel portafoglio digitale BlueXP e la pagina licenze servizi dati rifletterà la modifica tra 5 e 10 minuti.

2. Se BlueXP non riesce ad aggiornare automaticamente la licenza (ad esempio, se installata in un sito buio), sarà necessario caricare manualmente il file di licenza.
   a. È possibile Ottenere il file di licenza dal NetApp Support Site.
   b. Nella scheda *licenze servizi dati* della pagina del portafoglio digitale BlueXP, fare clic su ••• Per il numero di serie del servizio che si sta aggiornando, fare clic su **Aggiorna licenza**.

c. Nella pagina *Update License*, caricare il file di licenza e fare clic su **Update License** (Aggiorna licenza).

Risultato

BlueXP aggiorna la licenza in modo che il backup e il ripristino di BlueXP continuino ad essere attivi.

Considerazioni sulla licenza BYOL

Quando si utilizza una licenza BYOL di backup e ripristino BlueXP, nell'interfaccia utente di BlueXP viene visualizzato un avviso quando la dimensione di tutti i dati di cui si esegue il backup è prossima al limite di capacità o alla data di scadenza della licenza. Riceverai questi avvisi:

- Quando i backup hanno raggiunto il 80% della capacità concessa in licenza, e ancora una volta quando hai raggiunto il limite
- 30 giorni prima della scadenza di una licenza e di nuovo alla scadenza della stessa

Utilizzare l'icona chat in basso a destra dell'interfaccia BlueXP per rinnovare la licenza quando vengono visualizzati questi avvisi.

Due cose possono accadere alla scadenza della licenza BYOL:

- Se l'account che stai utilizzando ha un account Marketplace PAYGO, il servizio di backup continua a funzionare, ma si passa a un modello di licenza PAYGO. La capacità utilizzata dai backup viene addebitata.
- Se l'account in uso non dispone di un account Marketplace, il servizio di backup continua a essere in esecuzione, ma verranno visualizzati gli avvisi.

Una volta rinnovato l'abbonamento BYOL, BlueXP aggiorna automaticamente la licenza. Se BlueXP non riesce ad accedere al file di licenza tramite una connessione Internet sicura (ad esempio, se installato in un sito buio), è possibile ottenere il file da soli e caricarlo manualmente su BlueXP. Per istruzioni, vedere "Come aggiornare una licenza di backup e ripristino BlueXP".

I sistemi trasferiti a UNA licenza PAYGO vengono restituiti automaticamente alla licenza BYOL. E i sistemi che erano in esecuzione senza una licenza non vedranno più gli avvisi.

Monitorare la protezione dei dati

Report sulla copertura per la data Protection

Con i report di backup e ripristino BlueXP, puoi garantire che i dati critici siano protetti in base alle policy definite dalla tua organizzazione e fornire audit per le esigenze di conformità.

I report di backup e ripristino di BlueXP consentono di ottenere i seguenti risultati:

- **Visibilità delle operazioni**: Monitorate i vostri contratti di livello di servizio per quanto riguarda la protezione dei dati, il tasso di successo del backup e l'allineamento delle finestre di backup alle esigenze aziendali.
- **Compliance e auditing**: Utilizza report operativi e di inventario nei tuoi processi di audit interni ed esterni per il monitoraggio continuo della conformità.

> Le attività dei report vengono monitorate nel registro Job Monitoring in modo da poter controllare tutte le attività. "Scopri di più sul monitoraggio dei processi".

Ambito dei report

I report di backup e ripristino di BlueXP forniscono informazioni sui seguenti aspetti:

- **Posizione del connettore**: On-premise o nel cloud
- **Origine**: Volumi Cloud Volumes ONTAP, volumi ONTAP on-premise, applicazioni o volumi persistenti Kubernetes
- **Destinazione**: Qualsiasi provider cloud, NetApp StorageGRID o ONTAP S3
- **Versioni ONTAP**: 9.13.0

Creare un report sull'inventario di backup

Dalla scheda Backup and Recovery Reports di BlueXP, è possibile creare il report Backup Inventory e filtrarne il contenuto. Con il report Backup Inventory, puoi visualizzare tutti i backup relativi a un account specifico, un ambiente di lavoro o un inventario SVM.

Il report Backup Inventory mostra le seguenti informazioni e molto altro ancora:

- Account, ambiente di lavoro e SVM
- Volumi protetti e non protetti
- Destinazione del backup
- Policy di backup applicata
- Stile di crittografia (chiave gestita dal provider o chiave gestita dall'utente)
- Stato di protezione di DataLock e ransomware (governance, compliance o nessuno)
- Stato di archiviazione abilitato
- Numero di copie di backup
- Tipo di backup (backup ad hoc pianificato o avviato dall'utente)

- Classe di storage
- Etichetta Snapshot

> Il report Backup Inventory non include informazioni di backup scadute o non riuscite.

La parte superiore del report include un grafico che mostra le seguenti informazioni:

- Numero di volumi nell'ambito con almeno un backup
- Totale di volumi inattivi più volumi attivi

Il report Backup Inventory mostra i seguenti grafici:

- **Volume backup status** (Stato backup volume): Mostra i volumi protetti rispetto ai volumi non protetti per l'ambito selezionato.
- **Volumi per numero di backup**: Raggruppa i volumi in base al numero di copie di backup disponibili per questo volume.

Fasi

1. Dal menu in alto, selezionare **Report**.
2. Selezionare **Backup Inventory**.
3. Selezionare **Crea report**.
4. Selezionare l'account, l'ambiente di lavoro e SVM.

   > È possibile selezionare più ambienti di lavoro e SVM.

5. Selezionare l'intervallo di tempo: Ultime 24 ore, settimana o mese.
6. Esaminare le sezioni del report (Snapshot Policy, Replication Policy o Backup Policy), a seconda delle selezioni del report.
7. (Facoltativo) Filtra i risultati in base allo stato del lavoro.
8. (Facoltativo) esportare il contenuto del report in formato .CSV selezionando **Download CSV**.

Creare un report attività processo protezione dati

Il monitoraggio proattivo può ridurre gli sforzi necessari per monitorare tutte le risorse del tuo ecosistema. A partire da ONTAP 9.13.0, il report attività di protezione dei dati fornisce informazioni sulle operazioni di snapshot, backup, cloning e ripristino che è possibile utilizzare con il monitoraggio SLA e con i tassi di backup e ripristino.

Il report si applica alle operazioni di backup e recovery di BlueXP per Cloud Volumes ONTAP, on-premise, applicazioni e dati Kubernetes.

Il report Data Protection Job Activity mostra le seguenti informazioni e molto altro ancora:

- Account, ambiente di lavoro e SVM
- Tipo di lavoro (backup o ripristino)
- Nome risorsa (volume o applicazione)
- Stato del lavoro

- Orari e durata di inizio e fine
- Nome del criterio per i processi di backup
- Etichetta Snapshot per i processi di backup

I grafici nella parte superiore della pagina mostrano le seguenti informazioni:

- Lavori per tipo
  - Numero di processi di backup e ripristino dei volumi ONTAP
  - Numero di processi di backup e ripristino delle applicazioni
  - Numero di processi di backup e ripristino delle macchine virtuali
  - Numero di processi di backup e ripristino Kubernetes
- Attività lavorativa giornaliera

Fasi

1. Dal menu in alto, selezionare **Report**.
2. Selezionare **attività di lavoro Data Protection**.
3. Selezionare **Crea report**.
4. Selezionare l'account, l'ambiente di lavoro e SVM.
5. Selezionare l'intervallo di tempo: Ultime 24 ore, settimana o mese.
6. (Facoltativo) filtrare i risultati in base allo stato del lavoro, ai tipi di lavoro (backup o ripristino) e alle risorse.
7. (Facoltativo) esportare il contenuto del report in formato .CSV selezionando **Download CSV**.

Monitorare lo stato dei processi di backup e ripristino

È possibile monitorare lo stato di istantanee locali, repliche e backup dei processi di archiviazione a oggetti avviati e 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.

Visualizzare lo stato del lavoro in Job Monitor

È possibile visualizzare un elenco di tutte le operazioni di istantanea, replica, backup nell'archiviazione a oggetti e ripristino e il relativo stato corrente nella scheda **monitoraggio processi**. Ciò include operazioni da Cloud Volumes ONTAP, ONTAP on-premise, applicazioni, macchine virtuali e sistemi Kubernetes. Ogni operazione, o lavoro, ha un ID univoco e uno stato.

Lo stato può essere:

- Successo
- In corso
- In coda

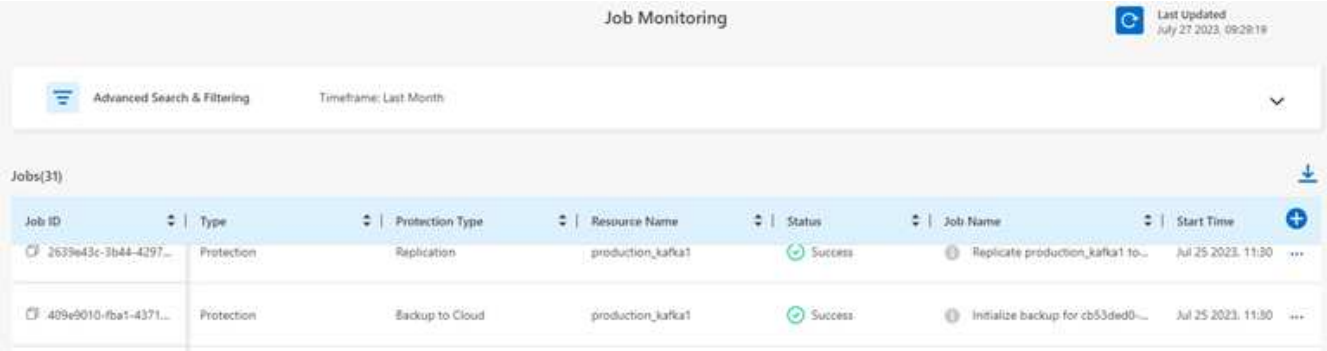
- Attenzione
- Non riuscito

Snapshot, repliche, backup sullo storage a oggetti e operazioni di ripristino avviate dall'interfaccia utente e dall'API di backup e recovery di BlueXP sono disponibili nella scheda Job Monitoring.

> 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, selezionare **protezione > Backup e ripristino**.
2. Selezionare la scheda **Job Monitoring**.



   Questa schermata mostra le intestazioni di colonna predefinite.

3. La visualizzazione di colonne aggiuntive (ambiente di lavoro, SVM, nome utente, carico di lavoro, nome policy, etichetta istantanea), selezionare ⊕.

Cercare e filtrare l'elenco dei job

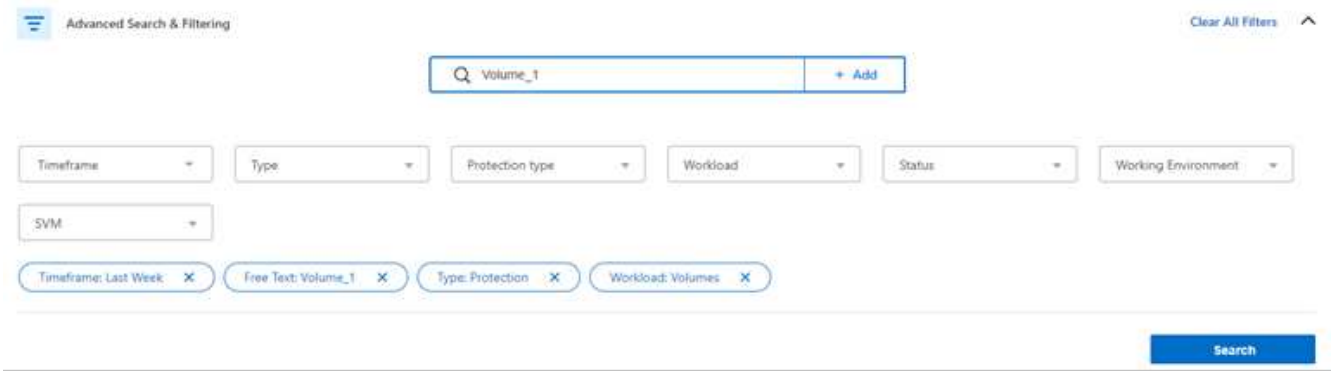
È possibile filtrare le operazioni nella pagina monitoraggio lavoro utilizzando diversi filtri, ad esempio criteri, etichette Snapshot, tipo di operazione (protezione, ripristino, conservazione o altro) e tipo di protezione (istantanea locale, replica o backup nel cloud).

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. Selezionare la scheda **Job Monitoring**.
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.



Questa schermata mostra come cercare tutti i processi "Backup" del "Volume" per i volumi denominati "Volume_1" nella "settimana precedente".

La maggior parte dei filtri sono intuitivi. Il filtro per "carico di lavoro" consente di visualizzare i lavori nelle seguenti categorie:

- Volumi (Cloud Volumes ONTAP e ONTAP Volumes on-premise)
- Applicazioni
- 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

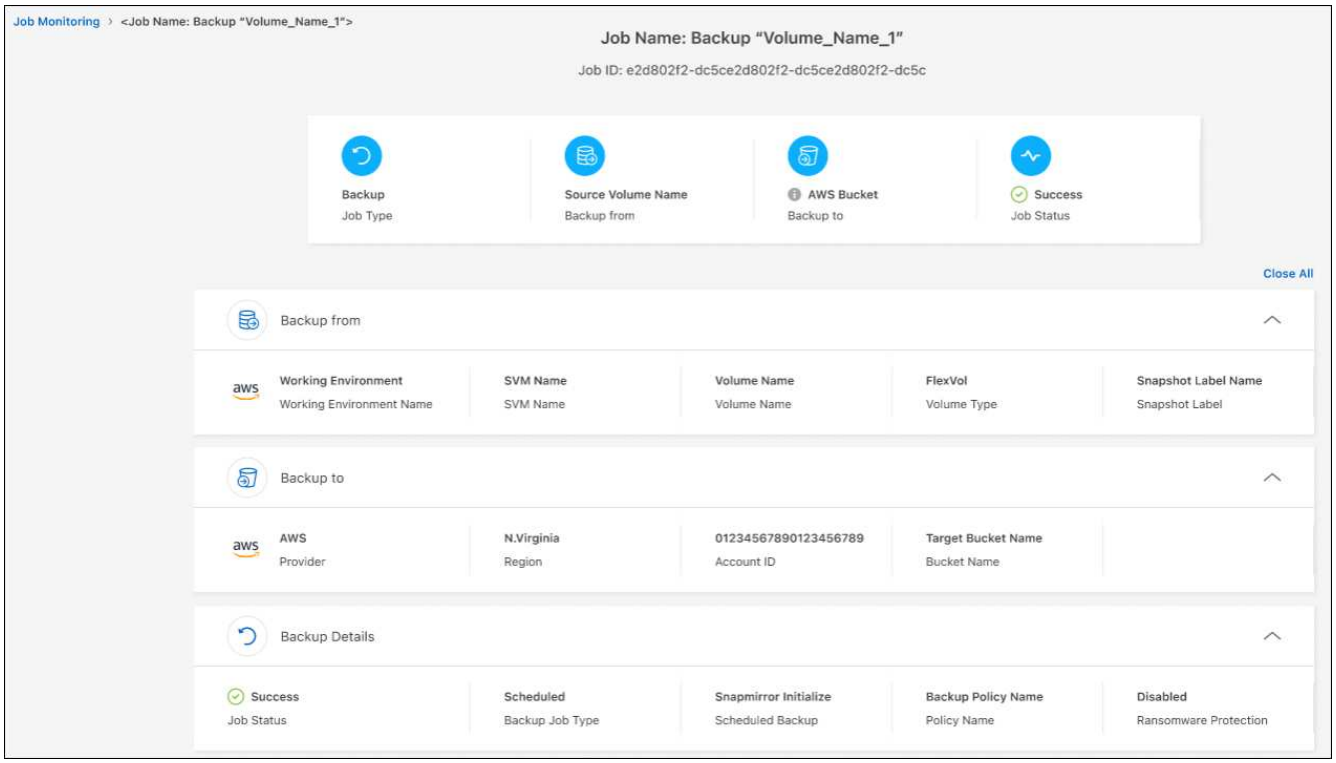
È possibile visualizzare i dettagli corrispondenti a un lavoro completato specifico. È possibile esportare i dettagli di un determinato lavoro in formato JSON.

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 job di ripristino mostrano dettagli come provider di destinazione per il backup (Amazon Web Services, Microsoft Azure, Google Cloud, on-premise), nome del bucket S3, Nome SVM, nome del volume di origine, volume di destinazione, etichetta Snapshot, numero di oggetti recuperati, nomi dei file, dimensioni dei file, data dell'ultima modifica e percorso completo dei file.

Fasi

1. Selezionare la scheda **Job Monitoring**.
2. Selezionare il nome del lavoro.
3. Selezionare il menu Actions (azioni) ••• E selezionare **Visualizza dettagli**.



Job Name: Backup "Volume_Name_1"

Job ID: e2d802f2-dc5ce2d802f2-dc5ce2d802f2-dc5c

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. Selezionare la scheda **Job Monitoring**.
2. Per scaricare un file CSV per tutti i lavori, selezionare ↓ e individuare 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. Selezionare la scheda **Job Monitoring**.
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
Snapshot locale	Errore del processo di creazione di snapshot ad-hoc di backup e recovery di BlueXP	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	Guasto al lavoro di freno di replica del backup e recovery di 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 account Admins di BlueXP ricevono e-mail per tutti gli avvisi "critici" e "raccomandati". 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".

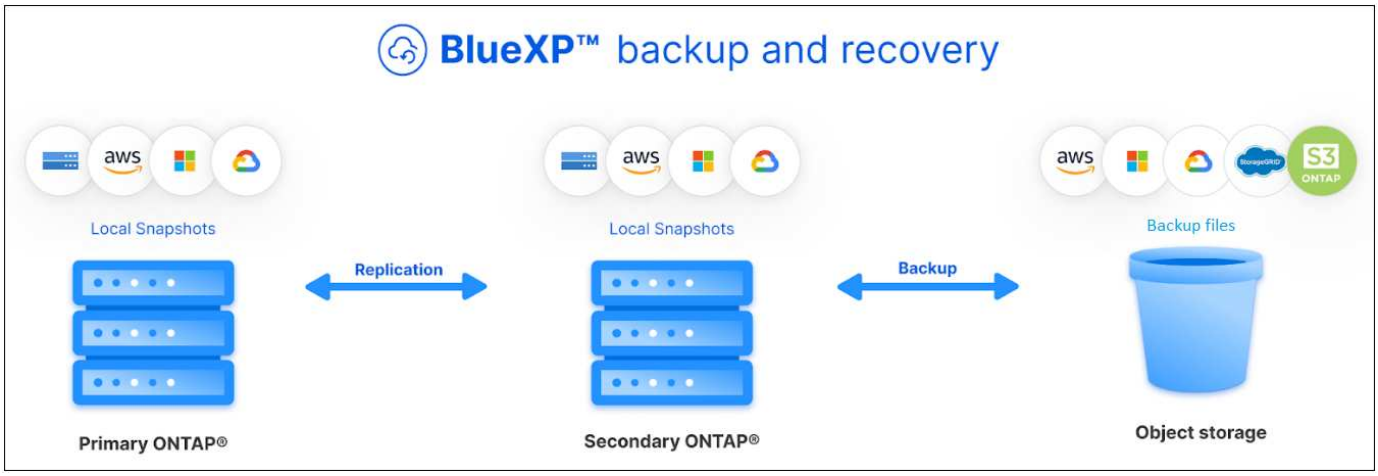
Backup e ripristino dei dati ONTAP

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.

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.
  - Gestire le policy di replica

Vedere "Limitazioni della replica" Per un elenco delle funzionalità di replica non disponibili con il backup e ripristino BlueXP.

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.

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[]
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)
- Volumi conformità SnapLock (richiede ONTAP 9,14 o versione successiva)
- Volumi di destinazione SnapMirror Data Protection (DP)

Vedere le sezioni a. "Limitazioni di backup e ripristino" per ulteriori requisiti e limitazioni.

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. Leggere il Licensing per ulteriori informazioni.

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 di origine associati al "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, due contratti annuali sono disponibili per i termini a 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 si utilizza GCP, è possibile richiedere un'offerta privata da NetApp e selezionare il piano quando si effettua l'iscrizione da Google Cloud Marketplace durante l'attivazione del backup e ripristino BlueXP.

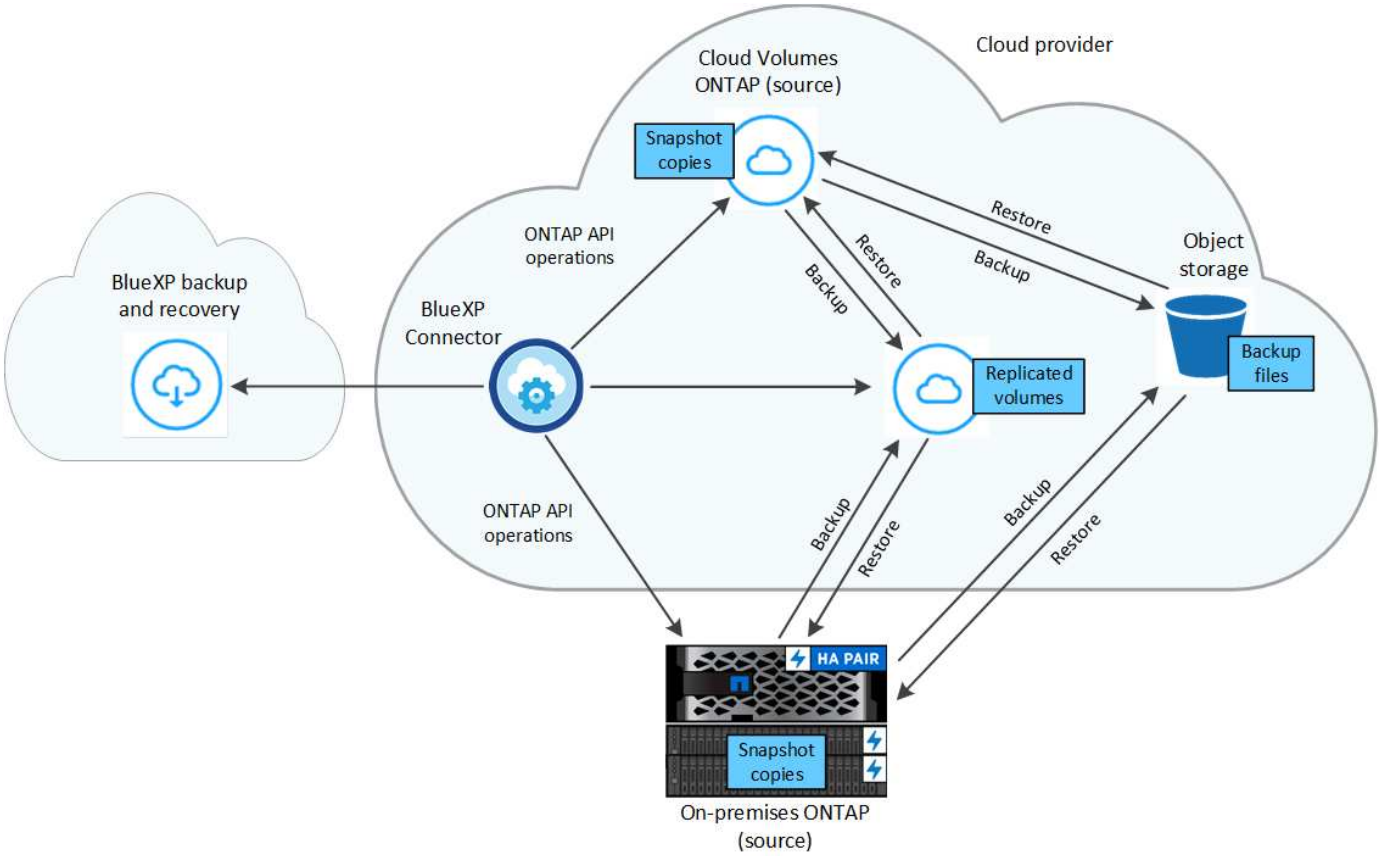
"Scopri come impostare i contratti annuali".

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 si desidera modificare l'archivio di oggetti di destinazione per un cluster in futuro, è necessario "Annullare la registrazione del backup e ripristino BlueXP per l'ambiente di lavoro", Quindi abilitare il backup e il ripristino BlueXP utilizzando le informazioni del nuovo provider di 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 intervallo, i backup meno recenti vengono rimossi in modo da avere sempre i backup più recenti (e quindi i backup obsoleti non continuano a occupare spazio).

Vedere "Pianificazioni di backup" per ulteriori informazioni sulle opzioni di pianificazione disponibili.

Nota: È possibile "creare un backup on-demand di un volume" Dalla dashboard di backup in qualsiasi momento, oltre ai file di backup creati dai backup pianificati.

> 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 del backup è lo stesso del periodo di conservazione della pianificazione del backup, più 14 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".

Vedere "Impostazioni dello storage di archiviazione" per ulteriori informazioni sull'archiviazione dei file di backup meno recenti.

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

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.

Esamineremo le seguenti opzioni:

- Quali funzionalità di protezione utilizzerai: 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)

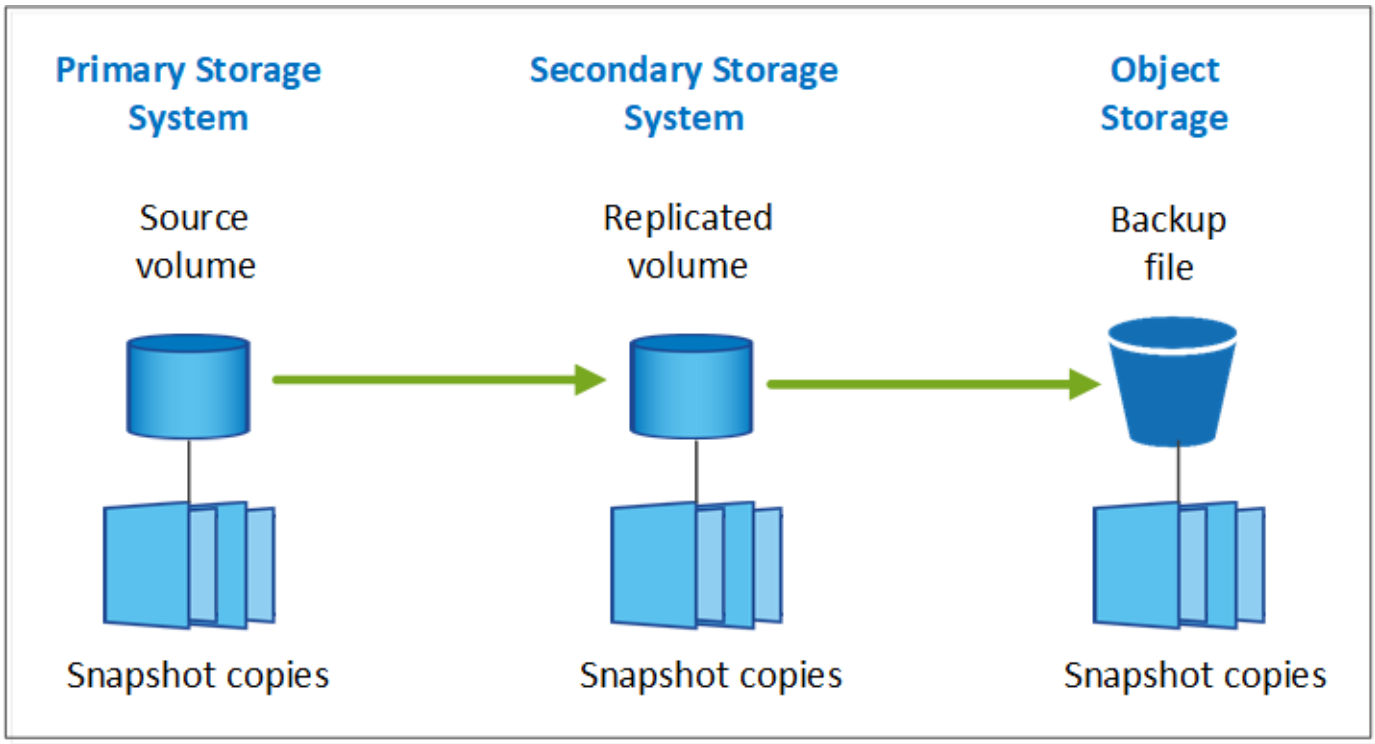
Quali funzioni di protezione utilizzerai

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	Crea un'immagine point-in-time di sola lettura di un volume all'interno del volume di origine come copia Snapshot. È possibile utilizzare la copia Snapshot per ripristinare singoli file o l'intero contenuto di un volume.

Tipo di backup	Descrizione
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 point-in-time di sola lettura di un volume. L'immagine consuma uno spazio di storage minimo e comporta un overhead delle performance trascurabile, in quanto registra solo le modifiche apportate ai file dall'ultima copia Snapshot. 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 (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.

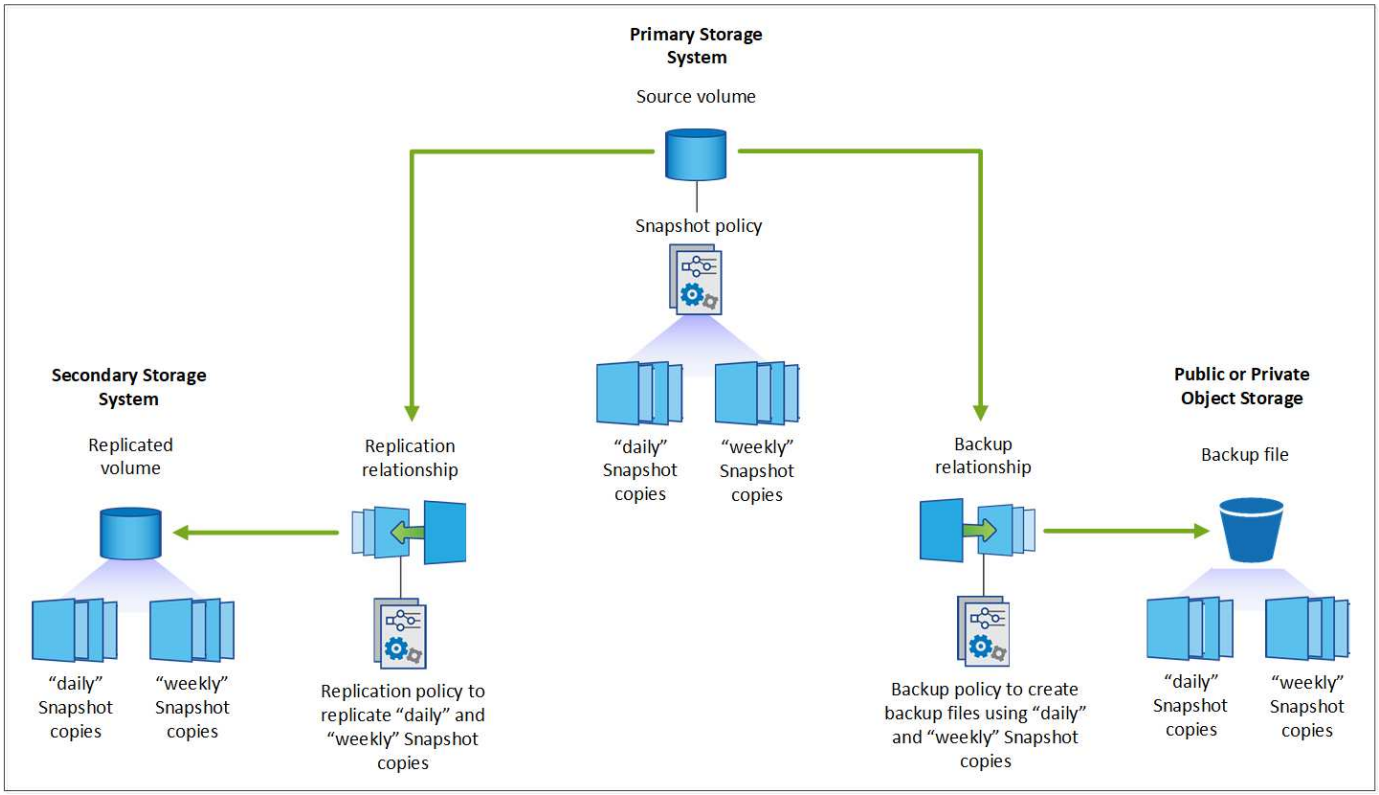
Oltre a questi criteri, lo storage cloud offre opzioni di sicurezza aggiuntive se si utilizza la funzionalità DataLock e ransomware Protection, oltre a risparmi aggiuntivi selezionando classi di storage di archiviazione per i file di backup meno recenti. "Scopri di più su DataLock e la protezione ransomware" e. "impostazioni dello storage 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
Replication	Medio	Media (spazio su disco)	Medio	Medio (rete)
Backup cloud	Basso	Basso (spazio oggetto)	Basso	Elevato (tariffe provider)

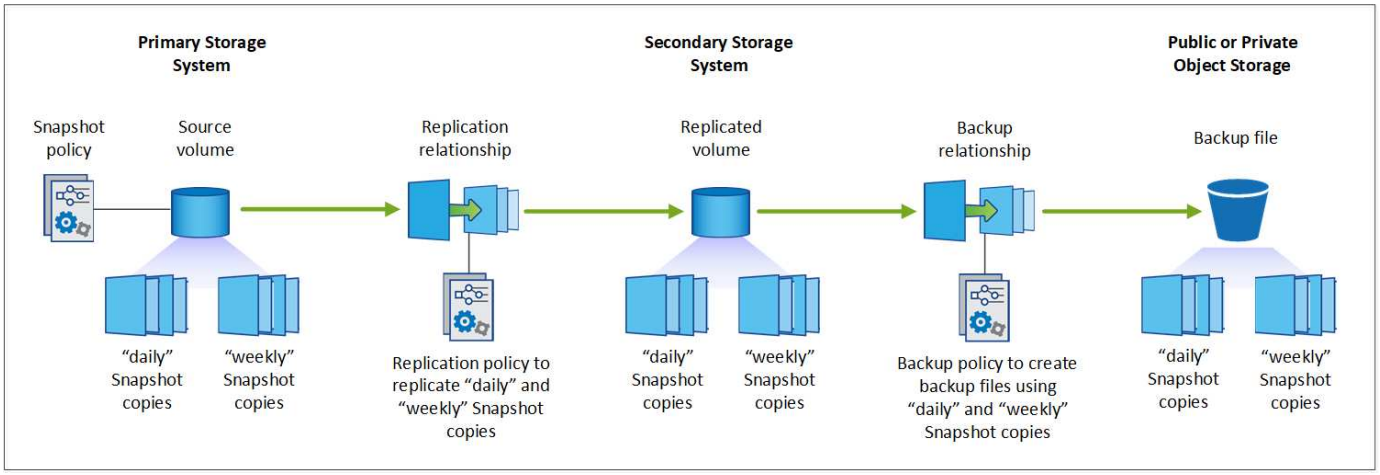
Quale architettura di backup utilizzerai

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 sia al sistema storage di destinazione che all'oggetto di backup nel cloud.



Un'architettura **Cascade** trasferisce prima la copia Snapshot al sistema di storage di destinazione, quindi il sistema trasferisce la copia all'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 performance del sistema di origine, perché invia copie Snapshot a 2 sistemi distinti	Meno effetti sulle performance del sistema storage di origine, in quanto invia la copia Snapshot una sola 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 le copie Snapshot, le repliche e i 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 policy Snapshot predefinito crea copie Snapshot ogni ora, ogni giorno e ogni settimana, conservando 6 copie Snapshot ogni ora, 2 ogni giorno e 2 ogni settimana.
- La policy di replica predefinita replica le copie Snapshot giornaliere e settimanali, conservando 7 copie Snapshot giornaliere e 52 copie Snapshot settimanali.
- La policy di backup predefinita replica le copie Snapshot giornaliere e settimanali, conservando 7 copie Snapshot giornaliere e 52 copie Snapshot 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 nelle policy Snapshot, altrimenti i volumi replicati e i file di backup non verranno creati.

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

Oltre a utilizzare l'utilizzo del recovery di backup di BlueXP per creare policy personalizzate, puoi utilizzare System Manager o l'interfaccia a riga di comando (CLI) di ONTAP.

"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 utilizzando System Manager"
"Creare un criterio di backup utilizzando l'interfaccia utente 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 esempio di ONTAP che possono essere utili se si creano criteri personalizzati. Tenere presente che è necessario utilizzare il vserver *admin* (storage VM) come `<vserver_name>` in questi comandi.

Descrizione policy	Comando
Semplice policy Snapshot	`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 container deve essere utilizzato esclusivamente per la memorizzazione dei file di backup dei volumi ONTAP e non può essere utilizzato per altri scopi. 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"

Nota: al momento non è possibile utilizzare i propri bucket S3 quando si creano backup nei sistemi StorageGRID o in ONTAP S3.

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. Per ulteriori informazioni, fai riferimento a come creare backup in AWS S3.

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 nello storage AWS quando si utilizza software ONTAP 9.11.1 o superiore sui cluster e nello storage Azure quando si utilizza software ONTAP 9.12.1 o superiore.
  - 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".
"Guarda questo video 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 ONTAP on-premise su Amazon S3"
- "Eseguire il backup dei dati Cloud Volumes ONTAP in Azure Blob"
- "Backup dei dati ONTAP on-premise su Azure Blob"
- "Eseguire il backup dei dati Cloud Volumes ONTAP su Google Cloud"
- "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, è necessario implementare BlueXP Connector nell'area limitata.

- Puoi eseguire il backup dei dati dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali di AWS su Amazon S3. "Eseguire il backup dei dati Cloud Volumes ONTAP su Amazon S3".
- È possibile eseguire il backup dei dati dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali di Azure su 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".

Gestire le policy di backup per i volumi ONTAP

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

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 sui criteri di backup predefiniti forniti, 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:

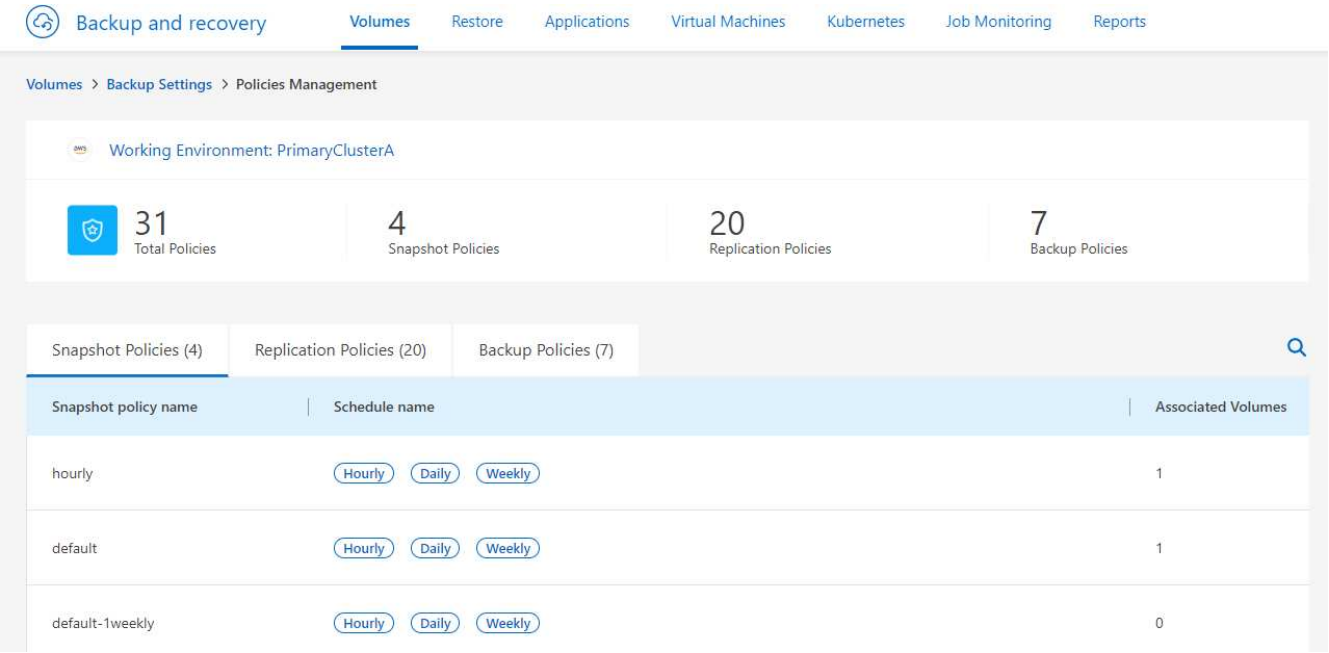
- Interfaccia utente di BlueXP
- Interfaccia utente di System Manager
- CLI ONTAP

> 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 per le copie Snapshot, le repliche e i backup sullo storage a oggetti:

- Creare un criterio 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 Snapshot prima di avviare lo Snapshot

Parte della strategia 3-2-1 prevede la creazione di una copia Snapshot del volume sul sistema di storage **primario**.

Parte del processo di creazione delle policy implica l'identificazione delle etichette di Snapshot e SnapMirror che denotano pianificazione e 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 delle istantanee. 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 dell'istantanea che indicano la pianificazione e la conservazione.
   c. Immettere la data e la frequenza di esecuzione dell'istantanea.
   d. Retention (conservazione): Immettere il numero di snapshot da conservare.
7. Selezionare **Crea**.

Esempio di criterio Snapshot utilizzando un'architettura a cascata

Questo esempio crea una policy 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 la policy Snapshot.
2. Cluster 2:
   a. Selezionare Cluster 2 nella pagina Policy.
   b. Ignorare la sezione criterio 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 una policy di backup, replica o snapshot personalizzata.

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 di policy backup su oggetti

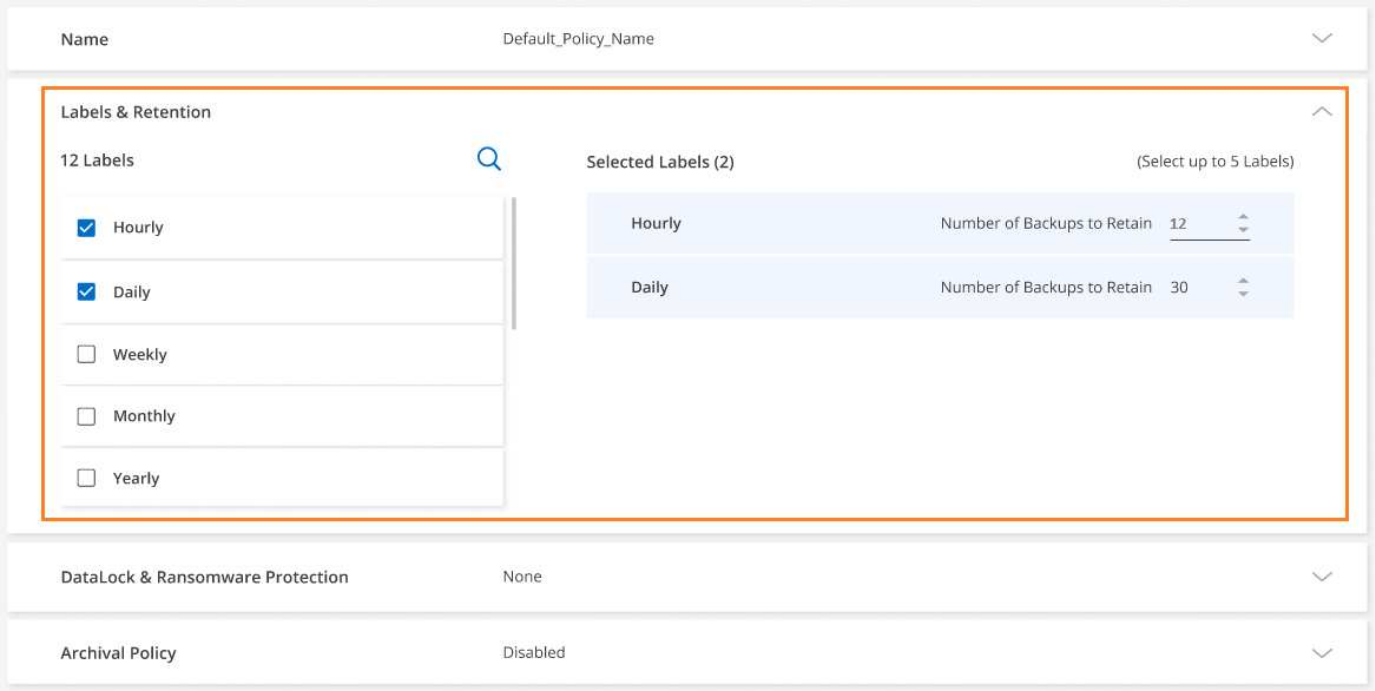
Il backup e recovery di BlueXP ti permette di creare policy di backup con una vasta gamma di impostazioni per i sistemi ONTAP e Cloud Volumes ONTAP on-premise.

> Queste impostazioni di policy sono rilevanti solo per il backup sullo storage a oggetti. Nessuna di queste impostazioni influisce sulle policy di Snapshot o di replica. Impostazioni di policy simili per snapshot e repliche verranno aggiunte in futuro.

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)

Tenere presente che i backup annaturali verranno eliminati automaticamente dal sistema di origine dopo essere stati trasferiti allo storage a oggetti. Questo comportamento predefinito può essere modificato "Nella pagina Advanced Settings (Impostazioni avanzate)" Per l'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 NetApp "Cloud Insights e Cloud Secure"o alcuni di "Protezioni anti-ransomware fornite da ONTAP" per proteggere i volumi di origine.

- 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. Puoi abilitarlo in seguito utilizzando le impostazioni avanzate di backup e recovery di BlueXP.
- DataLock e la protezione ransomware possono essere disattivati per un cluster dopo essere stati configurati per risparmiare sui costi.
- 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

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". Il periodo di tempo in cui il file di backup viene bloccato (e conservato) viene definito periodo di conservazione DataLock. E si basa sulla pianificazione dei criteri di backup e sull'impostazione di conservazione definita dall'utente, oltre a un buffer di 14 giorni. Qualsiasi policy di conservazione DataLock inferiore a 30 giorni viene arrotondata al minimo di 30 giorni.

Tenere presente che i vecchi backup vengono cancellati dopo la scadenza del periodo di conservazione DataLock, non dopo la scadenza del periodo di conservazione dei criteri di backup.

Diamo un'occhiata ad alcuni esempi di funzionamento:

- Se si crea una pianificazione di backup mensile con 12 ritentions, ogni backup viene bloccato per 12 mesi (più 14 giorni) prima dell'eliminazione.
- Se si crea una policy di backup che crea 30 backup giornalieri, 7 settimanali e 12 mensili, verranno generati tre periodi di conservazione bloccati. I backup "30 giornalieri" vengono conservati per 44 giorni (30 giorni più 14 giorni di buffer), i backup "7 settimanali" vengono conservati per 9 settimane (7 settimane più 14 giorni) e i backup "12 mensili" vengono conservati per 12 mesi (più 14 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 44 giorni (30 giorni più 14 giorni di buffer).

In quest'ultimo caso, se ogni file di backup viene bloccato per 44 giorni, si otterranno molti più file di backup di quelli che in genere vengono conservati con una policy oraria/24 ritentions. Di solito, quando il backup e ripristino di BlueXP crea il 25° file di backup, il backup più vecchio viene eliminato per mantenere le trattenute massime a 24 (in base al criterio). In questo caso, l'impostazione di conservazione DataLock sovrascrive l'impostazione di conservazione dei criteri dal criterio 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.

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 ransomware avvengono in corrispondenza dei seguenti punti del processo di backup e ripristino:

- Quando viene creato un file di backup.

  Puoi facoltativamente abilitare o disabilitare le scansioni ransomware.

  La scansione non viene eseguita sul file di backup quando viene scritto per la prima volta sullo storage cloud, ma quando viene scritto il file di backup **successivo**. Ad esempio, se si dispone di una pianificazione di backup settimanale impostata per martedì, martedì 14 viene creato un backup. Martedì 21 viene creato un altro backup. La scansione ransomware viene eseguita sul file di backup a partire dal 14.

- Quando si tenta di ripristinare i dati da un file di backup

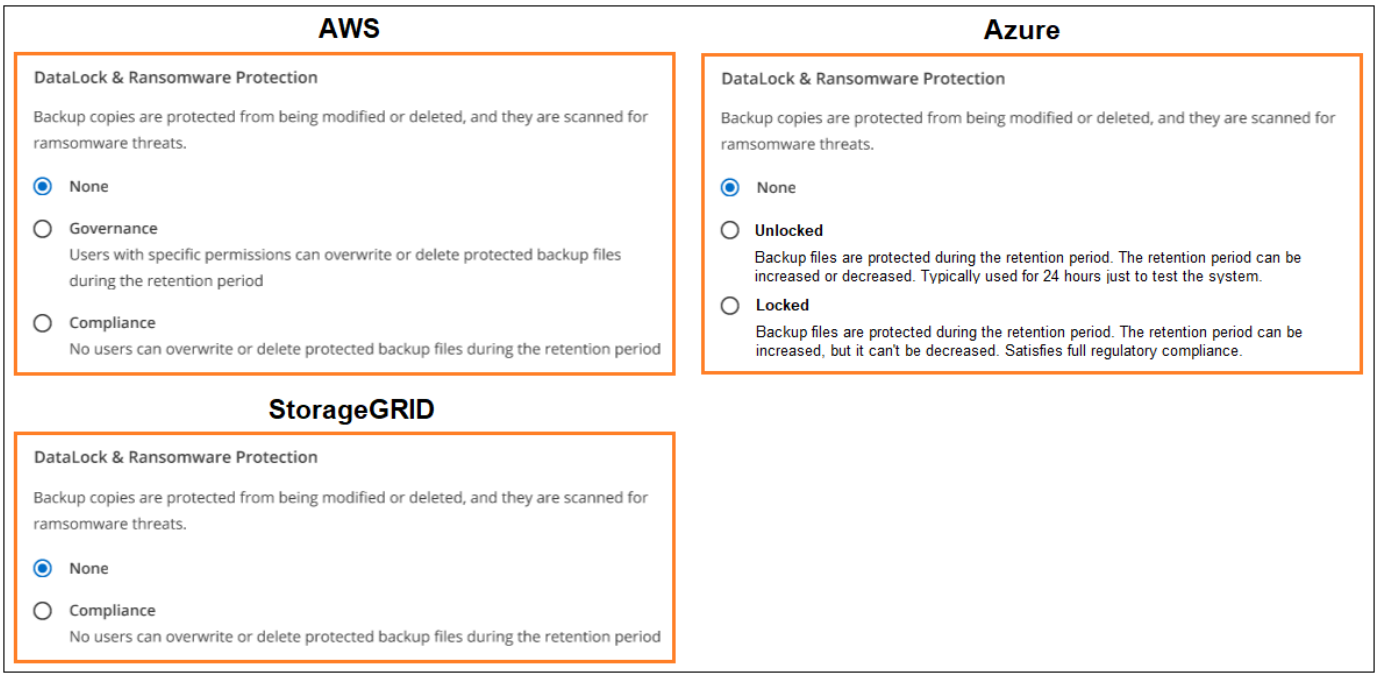
  È possibile scegliere di eseguire una scansione prima di ripristinare i dati da un file di backup oppure saltare questa scansione.

- Manualmente

  È possibile eseguire una scansione di protezione ransomware on-demand in qualsiasi momento per verificare lo stato di salute di un file di backup specifico. Questo può essere utile se si è verificato un problema ransomware su un volume specifico e si desidera verificare che i backup di quel volume non siano interessati.

Opzioni di protezione DataLock e ransomware

Ogni policy di backup fornisce una sezione per *DataLock e ransomware Protection* che è possibile applicare ai file di backup.



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 Snapshot. Puoi abilitare o disabilitare le scansioni ransomware sull'ultima copia Snapshot utilizzando l'opzione nella pagina Impostazioni avanzate. Se si attiva, le scansioni vengono eseguite ogni 7 giorni per impostazione predefinita.

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

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

È possibile scegliere tra le seguenti impostazioni per ciascun criterio di backup:

AWS

- **Nessuno** (impostazione predefinita)

  La protezione DataLock e la protezione ransomware sono disattivate.

- **Governance**

  DataLock è impostato sulla modalità *Governance* in cui gli utenti dispongono di `s3:BypassGovernanceRetention` permesso ("vedere di seguito") può sovrascrivere o eliminare i file di backup durante il periodo di conservazione. La protezione ransomware è attivata.

- **Compliance**

  DataLock è impostato sulla modalità *Compliance*, in cui nessun utente può sovrascrivere o eliminare i file di backup durante il periodo di conservazione. La protezione ransomware è attivata.

Azure

- **Nessuno** (impostazione predefinita)

  La protezione DataLock e la protezione ransomware sono disattivate.

- **Sbloccato**

  I file di backup sono protetti durante il periodo di conservazione. Il periodo di conservazione può essere aumentato o diminuito. Generalmente utilizzato per 24 ore per testare il sistema. La protezione ransomware è attivata.

- **Bloccato**

  I file di backup sono protetti durante il periodo di conservazione. Il periodo di conservazione può essere aumentato, ma non può essere diminuito. Soddisfa la piena conformità alle normative. La protezione ransomware è attivata.

StorageGRID

- **Nessuno** (impostazione predefinita)

  La protezione DataLock e la protezione ransomware sono disattivate.

- **Compliance**

  DataLock è impostato sulla modalità *Compliance*, in cui nessun utente può sovrascrivere o eliminare i file di backup durante il periodo di conservazione. La protezione ransomware è attivata.

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 attivare o disattivare questa funzione 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.

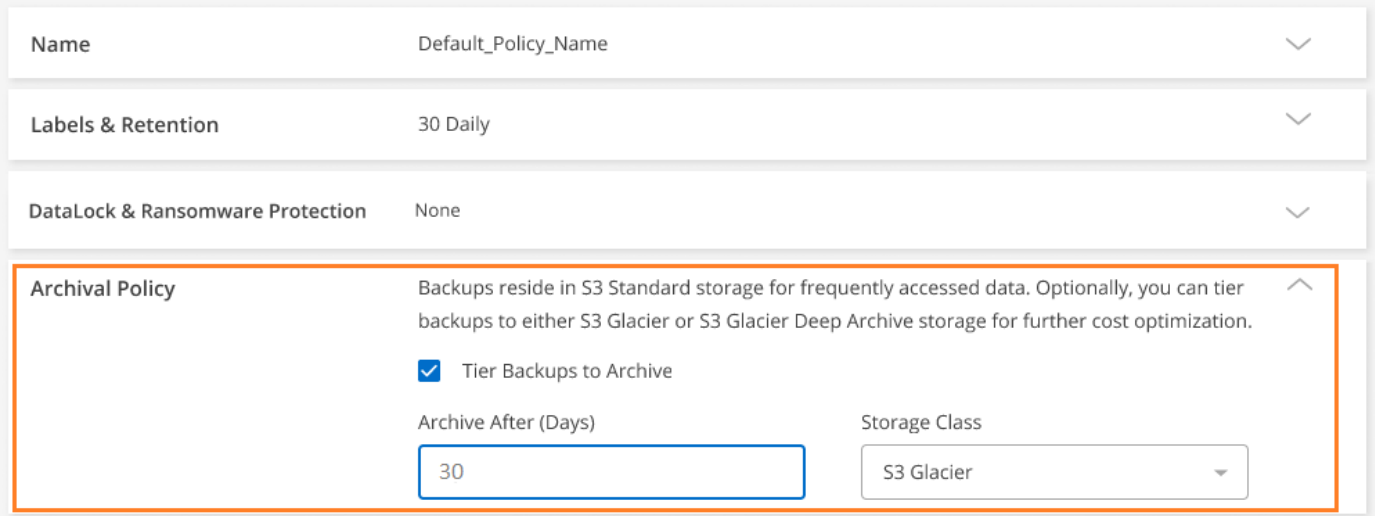
Opzioni di archiviazione

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".

+"Scopri di più sull'archiviazione dei file di backup da StorageGRID".

Gestire le opzioni di backup sullo storage a oggetti nella pagina Advanced Settings (Impostazioni avanzate)

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. In futuro verranno aggiunte impostazioni di replica simili a livello di cluster per snapshot e repliche.

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

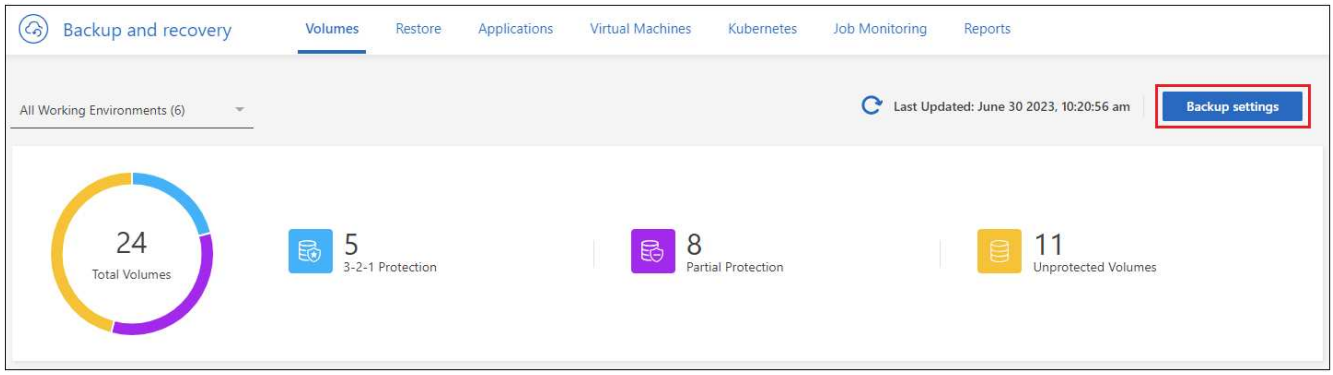
- Modifica dell'eventuale esportazione delle copie Snapshot storiche come file di backup e inclusione nei file di backup di base iniziali per volumi futuri
- Modifica della rimozione delle snapshot "annuali" dal sistema di origine
- Abilitazione o disabilitazione delle scansioni ransomware per un ambiente di lavoro, incluse le scansioni pianificate

Visualizzare le impostazioni di backup a livello di cluster

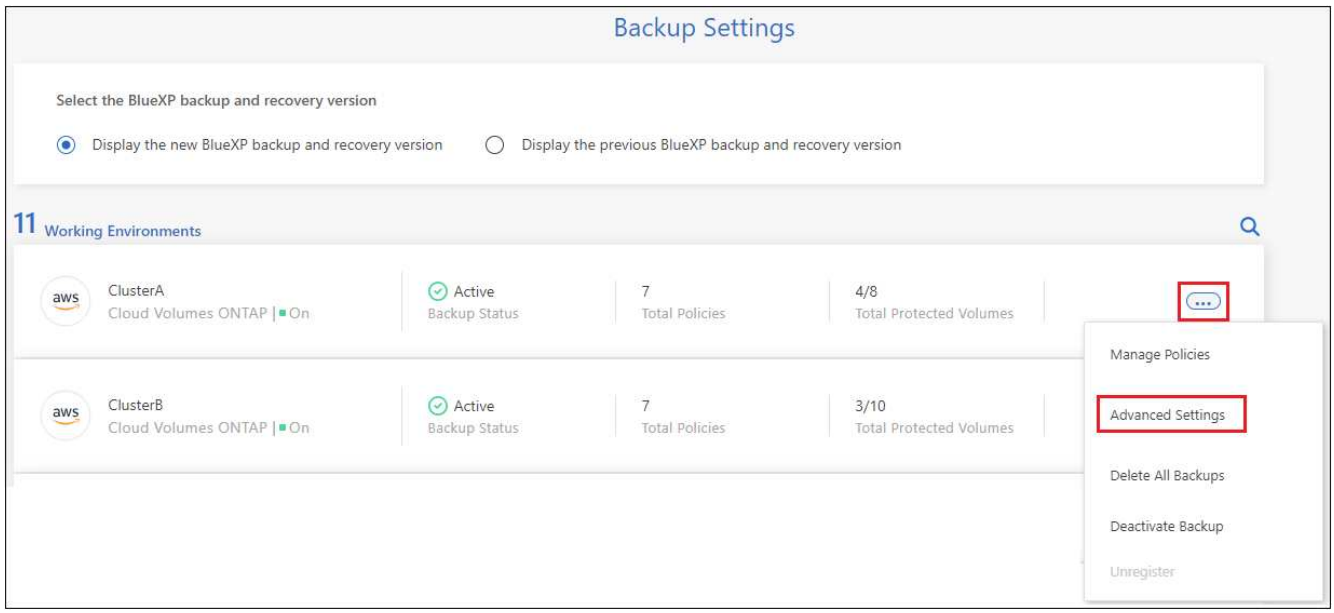
È possibile visualizzare le impostazioni di backup a livello di cluster per ciascun ambiente di lavoro.

Fasi

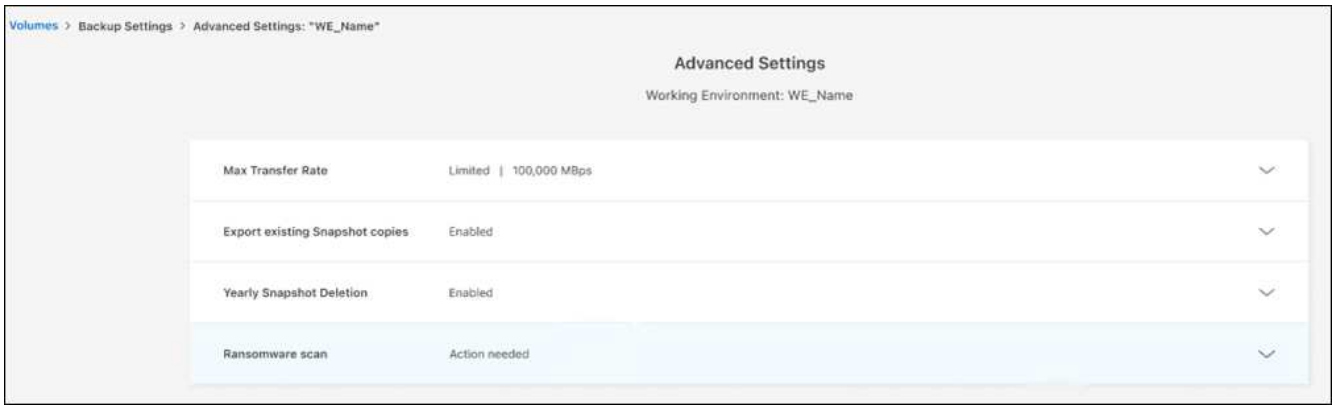
1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



3. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Advanced Settings** (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.

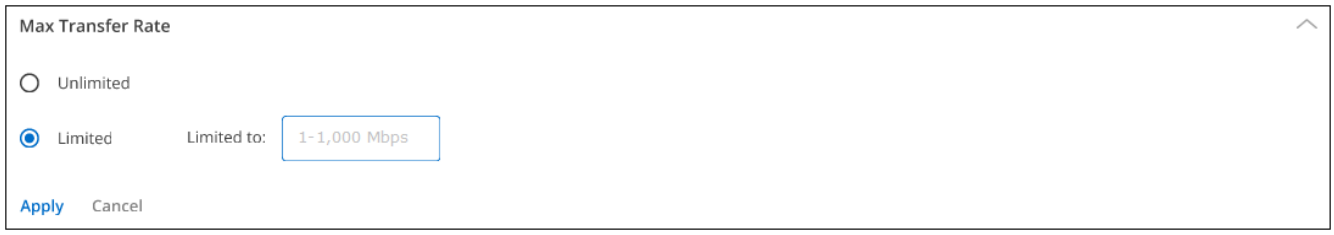
Tenere presente che alcune opzioni non sono disponibili in base alla versione di ONTAP nel cluster di origine e alla destinazione del provider cloud in cui risiedono i backup.

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 Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Advanced Settings** (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.

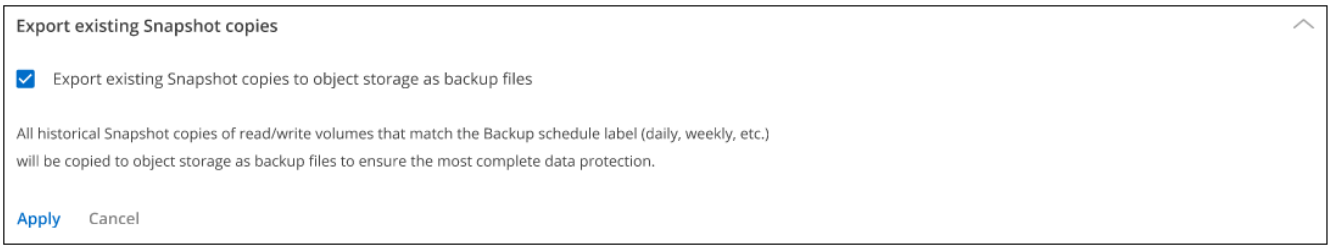
Consente di modificare se le copie Snapshot storiche vengono esportate come file di backup

Se sono presenti copie Snapshot locali per volumi che corrispondono all'etichetta della pianificazione di backup utilizzata in questo ambiente di lavoro (ad esempio, giornaliero, settimanale, ecc.), è possibile esportare tali snapshot cronologici nello storage a 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 Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Advanced Settings** (Impostazioni avanzate).
3. Nella pagina Impostazioni avanzate, espandere la sezione **Esporta copie snapshot esistenti**.



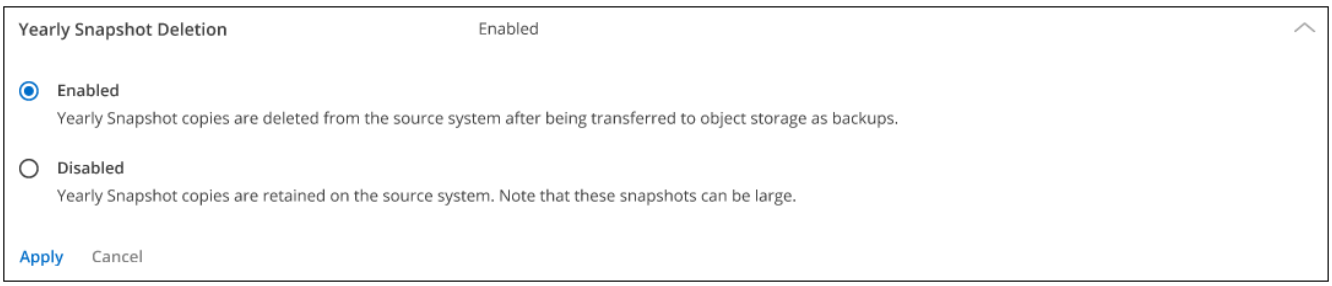
4. Selezionare se si desidera esportare le copie Snapshot esistenti.
5. Selezionare **Applica**.

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 Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Advanced Settings** (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 Snapshot. Puoi abilitare o disabilitare le scansioni ransomware sull'ultima copia Snapshot utilizzando l'opzione nella pagina Impostazioni avanzate. Se si attiva, le scansioni vengono eseguite ogni 7 giorni per impostazione predefinita.

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.

Scansioni pianificate anti-ransomware vengono eseguite solo sull'ultima copia Snapshot.

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 dettagli sulla gestione delle policy che implementano il rilevamento ransomware.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).
2. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Advanced Settings** (Impostazioni avanzate).
3. Nella pagina Impostazioni avanzate, espandere la sezione **scansione ransomware**.
4. Abilitare o disabilitare **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**.

Eseguire il backup dei dati Cloud Volumes ONTAP su Amazon S3

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dei volumi dai tuoi sistemi Cloud Volumes ONTAP su Amazon S3.

Avvio rapido

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

1 **Verificare il supporto per la configurazione**

- Cloud Volumes ONTAP 9.8 o versione successiva in AWS (si consiglia ONTAP 9.8P13 e versione successiva).

- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. "Offerta di backup di BlueXP Marketplace", an "Contratto annuale AWS", oppure è stato acquistato "e attivato" Una licenza BYOL di backup e ripristino BlueXP di NetApp.
- Hai un connettore installato in AWS:
  - Il connettore può essere installato in un sito con accesso a Internet completo ("modalità standard") o con connettività Internet limitata ("modalità limitata").
  - Il ruolo IAM che fornisce a BlueXP Connector le autorizzazioni include le autorizzazioni S3 dell'ultima versione "Policy BlueXP".

2 Preparare il connettore BlueXP

Se si dispone già di un connettore implementato in una regione AWS, tutto è impostato. In caso contrario, è necessario installare un connettore BlueXP in AWS per eseguire il backup dei dati Cloud Volumes ONTAP in AWS. Il connettore può essere installato in un sito con accesso a Internet completo ("modalità standard") o con connettività Internet limitata ("modalità limitata").

Preparare il connettore BlueXP

3 Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per AWS e BlueXP.

Verificare i requisiti di licenza.

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

Assicurarsi che i sistemi di storage primario e secondario soddisfino la versione di ONTAP e i requisiti di rete.

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

5 Abilitare il backup e ripristino BlueXP

Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra.

Abilitare il backup e ripristino BlueXP su Cloud Volumes ONTAP.

6 Attivare i backup sui volumi ONTAP

Seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

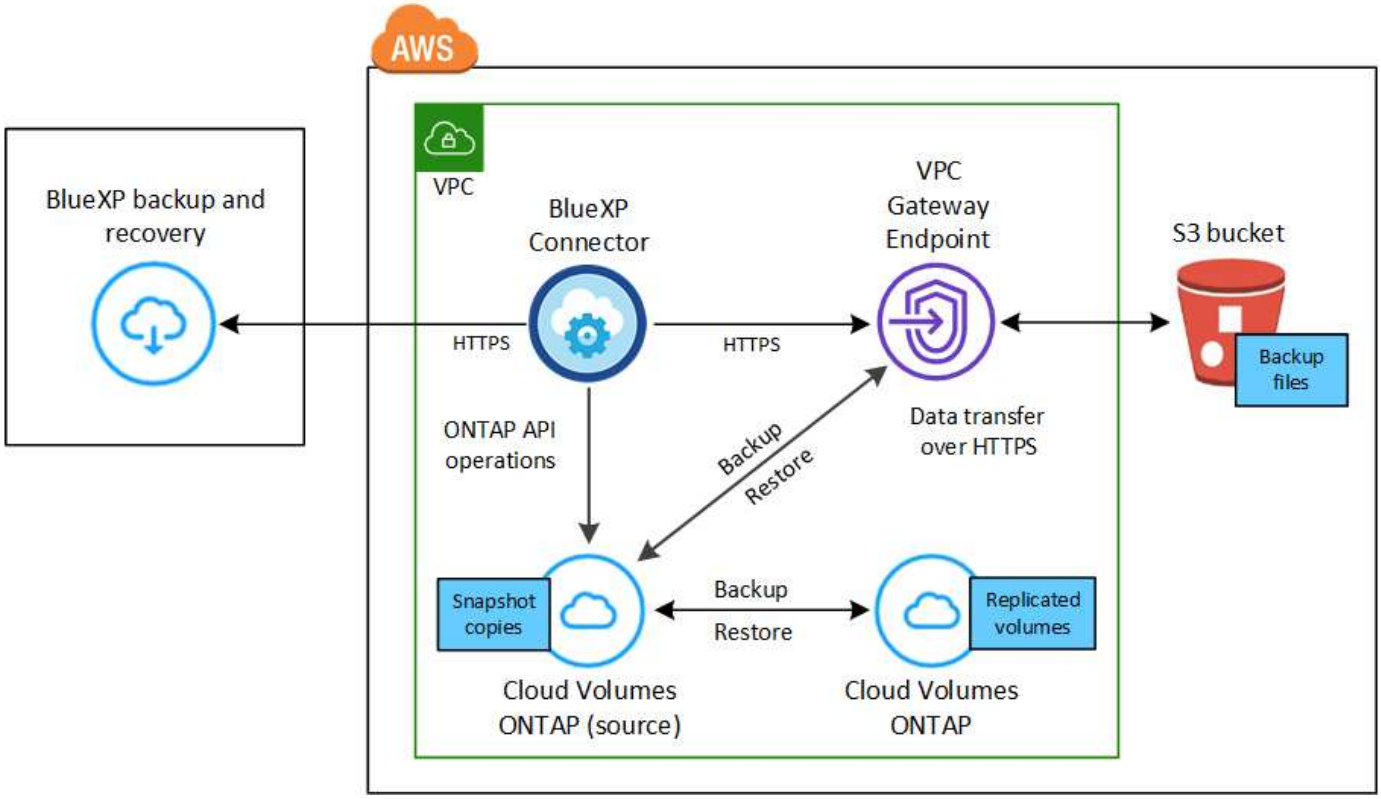
Attivare i backup sui volumi ONTAP.

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

Il ruolo IAM che fornisce a BlueXP le autorizzazioni deve includere le autorizzazioni S3 della versione più recente "Policy BlueXP". Se il criterio non contiene tutte queste autorizzazioni, consultare "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 ripristino BlueXP è supportato in tutte le regioni AWS "Dove è supportato Cloud Volumes ONTAP", Incluse le regioni di 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 i volumi su questi sistemi Cloud Volumes ONTAP, avviare il backup e ripristino BlueXP e. "attivare il backup su ciascun volume che si desidera proteggere".

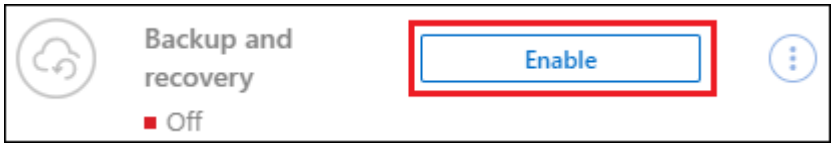
Attivare il backup e il ripristino BlueXP su un sistema esistente

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.



Per modificare le impostazioni di backup o aggiungere la replica, fare riferimento a. "Gestire i backup di 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

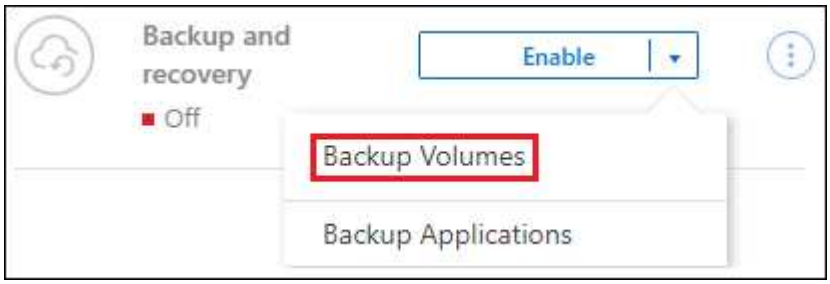
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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 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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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. (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).
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:
   - **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 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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".

3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne uno nuovo.

> Per creare un criterio personalizzato prima di attivare l'istantanea, fare riferimento alla sezione "Creare un criterio".

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

- Immettere il nome del criterio.
- Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato, fare riferimento alla sezione "Creare un criterio"..

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

- Immettere il nome del criterio.
- Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

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

  - Immettere il nome del criterio.
  - Selezionare fino a 5 programmi, generalmente di frequenze diverse.
  - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per ulteriori informazioni su DataLock e protezione dal ransomware, 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.

  i. 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 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 "Pannello Job Monitoring (monitoraggio processi)".

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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema Cloud Volumes ONTAP in AWS o a un sistema ONTAP on-premise.

Eseguire il backup dei dati Cloud Volumes ONTAP nello storage Azure Blob

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dei volumi dai tuoi sistemi Cloud Volumes ONTAP allo storage Azure Blob.

Avvio rapido

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

1 **Verificare il supporto per la configurazione**

- Cloud Volumes ONTAP 9.8 o versione successiva è in esecuzione in Azure (si consiglia ONTAP 9.8P13 e versione successiva).
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. "Offerta di backup di BlueXP Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup e ripristino BlueXP di NetApp.

2 **Preparare il connettore BlueXP**

Se disponi già di un connettore implementato in una regione Azure, sei tutto impostato. In caso contrario, è necessario installare un connettore BlueXP in Azure per eseguire il backup dei dati Cloud Volumes ONTAP nello storage Azure Blob. Il connettore può essere installato in un sito con accesso a Internet completo ("modalità standard") o con connettività Internet limitata ("modalità limitata").

Preparare il connettore BlueXP

3 **Verificare i requisiti di licenza**

È necessario verificare i requisiti di licenza per Azure e BlueXP.

Fare riferimento a. Verificare i requisiti di licenza.

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

Assicurarsi che i sistemi di origine e di destinazione soddisfino la versione di ONTAP e i requisiti di rete.

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

5 **Abilitare il backup e ripristino BlueXP**

Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra.

Abilitare il backup e ripristino BlueXP su Cloud Volumes ONTAP.

6 **Attivare i backup sui volumi ONTAP**

Seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

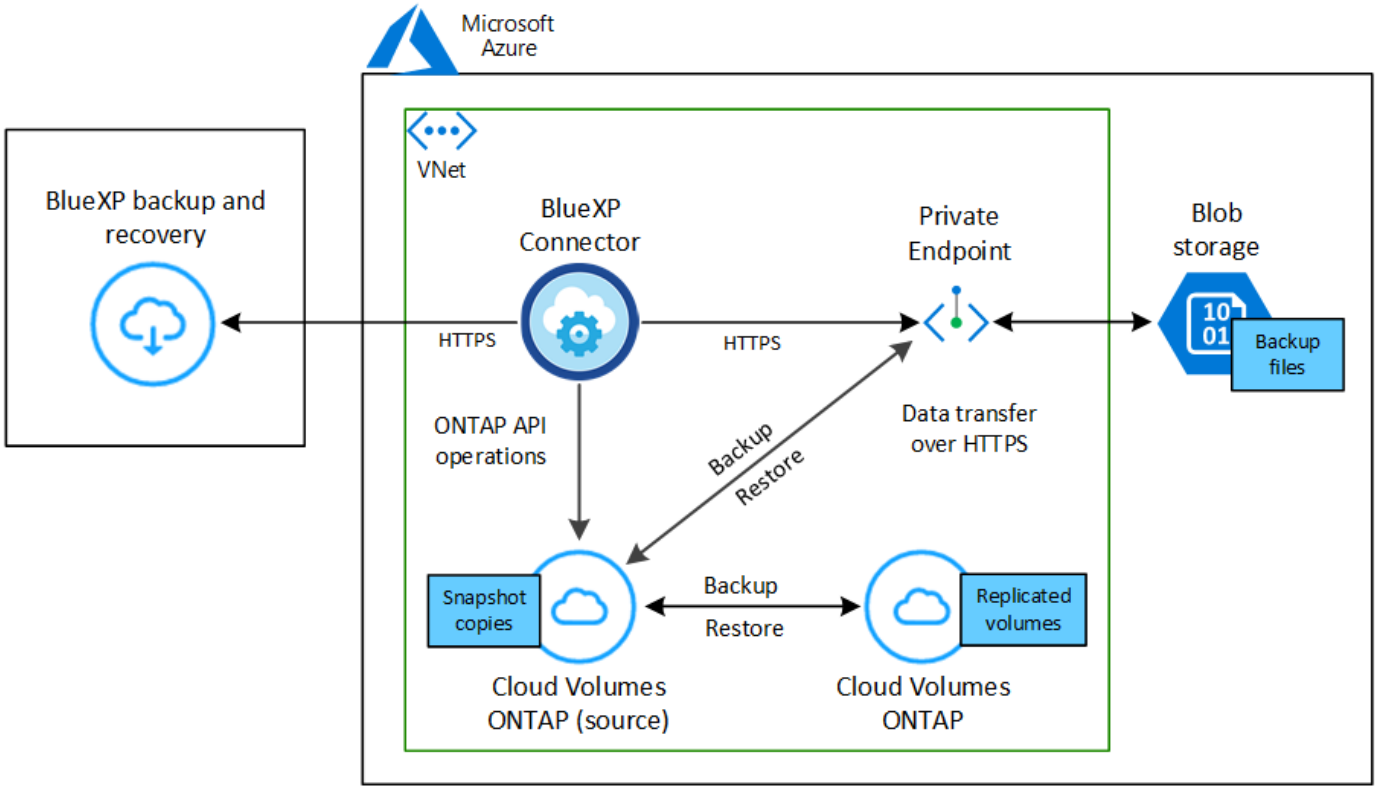
Attivare i backup sui volumi ONTAP.

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 ripristino BlueXP è supportato in tutte le regioni Azure "Dove è supportato Cloud Volumes ONTAP"; Incluse le regioni governative di Azure.

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. Se si desidera utilizzare un abbonamento Azure diverso per i backup, è necessario "Accedi al portale Azure e collega le due sottoscrizioni".

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. Fare clic su **Review + update**, quindi su **Update**.

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 *policy di accesso Azure* come modello di autorizzazione. Il modello di autorizzazione *Azure RBAC (role-based access control*) non è attualmente supportato.

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

Abilitare il backup e il ripristino di BluXP 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. Seguire la procedura per Attivazione del backup e ripristino BlueXP su un sistema esistente Per attivare il backup e il ripristino di BlueXP e scegliere il gruppo di risorse.

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 Azure, immettere il nome delle credenziali, l'ID client, il segreto client e l'ID directory, quindi fare clic su **continua**.
4. Compila la pagina Dettagli e credenziali e assicurati che sia stato sottoscritto un abbonamento a Azure Marketplace, quindi fai clic su **continua**.
5. Nella pagina servizi, lasciare attivato il servizio e fare clic su **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 i volumi su questi sistemi Cloud Volumes ONTAP, avviare il backup e ripristino BlueXP e. "attivare il backup su ciascun volume che si desidera proteggere".

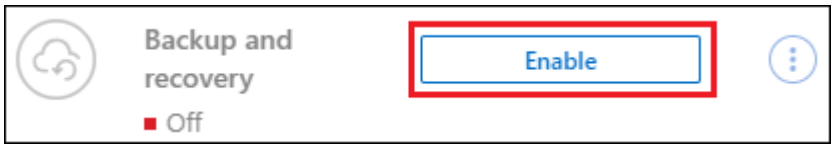
Attivare il backup e il ripristino BlueXP su un sistema esistente

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

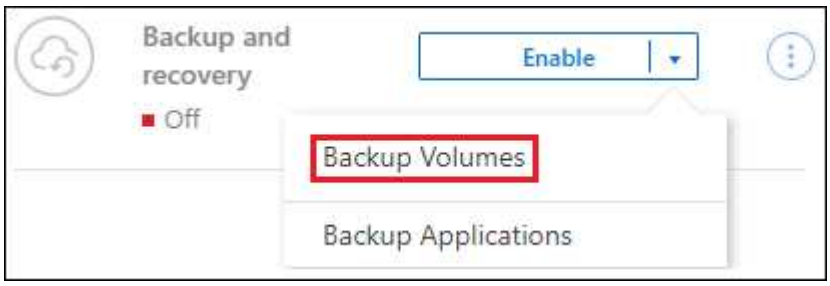
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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 All FlexVol Volumes (tutti i volumi). (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. (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).
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:
   - **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 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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".

3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne uno.

   Per creare un criterio personalizzato prima di attivare l'istantanea, fare riferimento alla sezione "Creare un criterio".

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

   - Immettere il nome del criterio.
   - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare la replica, fare riferimento alla sezione "Creare un criterio".

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

     - Immettere il nome del criterio.
     - Selezionare fino a 5 programmi, generalmente di 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. Se si desidera utilizzare un abbonamento Azure diverso per i backup, è necessario "Accedi al portale Azure e collega le due sottoscrizioni".

     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. "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. Se lo si desidera, scegliere se utilizzare un endpoint privato Azure precedentemente configurato. "Scopri come utilizzare un endpoint privato Azure".
- **Criterio di backup**: Selezionare un criterio di archiviazione backup su oggetti esistente.

  > Per creare un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "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 ulteriori informazioni su DataLock e protezione dal ransomware, fare riferimento a. "Impostazioni dei criteri di backup su oggetti".
    - Selezionare fino a 5 programmi, generalmente di 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.
  i. 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 "Pannello Job Monitoring (monitoraggio processi)".

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 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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema Cloud Volumes ONTAP in Azure o a un sistema ONTAP on-premise.

Eseguire il backup dei dati Cloud Volumes ONTAP su Google Cloud Storage

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dei volumi dai tuoi sistemi Cloud Volumes ONTAP allo storage cloud Google.

Avvio rapido

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

1 **Verificare il supporto per la configurazione**

- Si utilizza Cloud Volumes ONTAP 9.8 o versione successiva in GCP (si consiglia ONTAP 9.8P13 e versione successiva).
- Si dispone di un abbonamento GCP valido per lo spazio di storage in cui verranno collocati i backup.
- Nel progetto Google Cloud hai un account di servizio con il ruolo predefinito Storage Admin.
- Si è abbonati a. "Offerta di backup di BlueXP Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup e ripristino BlueXP di NetApp.

2 **Preparare il connettore BlueXP**

Se disponi già di un connettore implementato in un'area GCP, sei tutto impostato. In caso contrario, è necessario installare un connettore BlueXP in GCP per eseguire il backup dei dati Cloud Volumes ONTAP su Google Cloud Storage. Il connettore può essere installato in un sito con accesso a Internet completo ("modalità standard") o con connettività Internet limitata ("modalità limitata").

Preparare il connettore BlueXP

3 **Verificare i requisiti di licenza**

È necessario verificare i requisiti di licenza per Google Cloud e BlueXP.

Verificare i requisiti di licenza.

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

Assicurarsi che i sistemi di origine e di destinazione soddisfino la versione di ONTAP e i requisiti di rete.

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

5 **Abilitare il backup e ripristino BlueXP**

Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra.

Abilitare il backup e ripristino BlueXP su Cloud Volumes ONTAP.

6 **Attivare i backup sui volumi ONTAP**

Seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

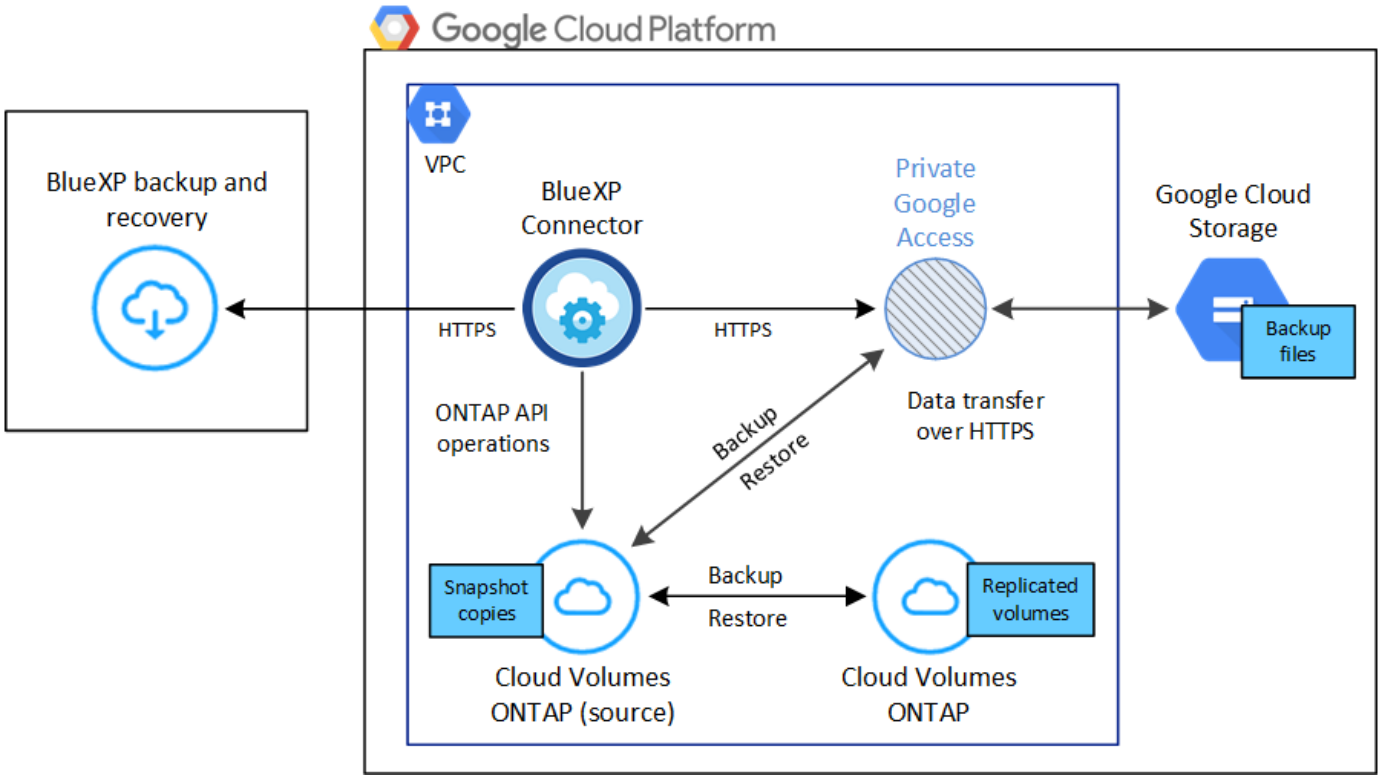
Attivare i backup sui volumi ONTAP.

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 ripristino BlueXP è supportato in tutte le regioni GCP "Dove è supportato Cloud Volumes ONTAP".

Account di servizio GCP

Devi disporre di un account di servizio nel tuo progetto Google Cloud con il ruolo predefinito Storage Admin. "Scopri come creare un account di servizio".

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. Vedere "Documentazione di Google Cloud: Abilitazione delle API" per ulteriori informazioni.

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

Abilitare il backup e il ripristino di BluXP 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

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:

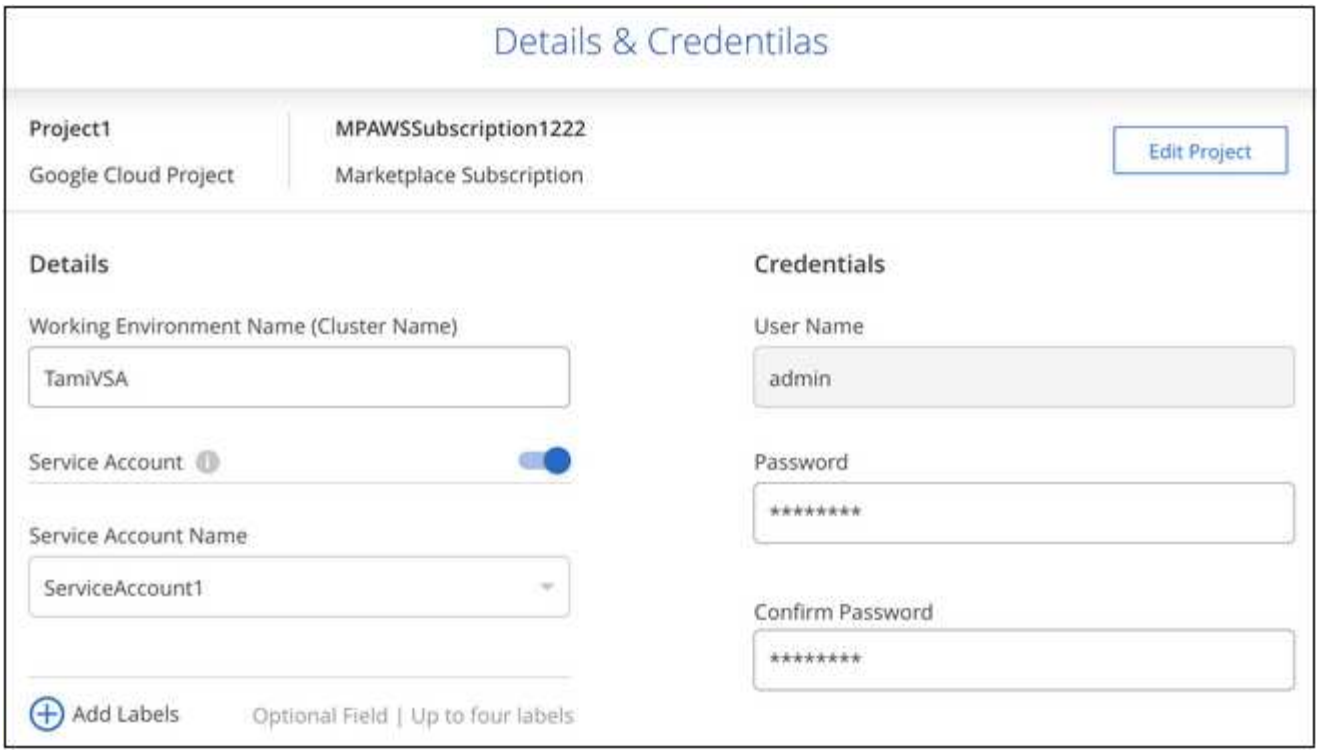
   a. Fare clic su **Edit Project** (Modifica progetto) e selezionare un nuovo progetto se quello che si desidera utilizzare è diverso dal progetto predefinito (dove si trova il connettore).

   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".

> Per modificare le impostazioni di backup o aggiungere la replica, fare riferimento a. "Gestire i backup di ONTAP".

Risultato

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

Attivare il backup e il ripristino BlueXP su un sistema esistente

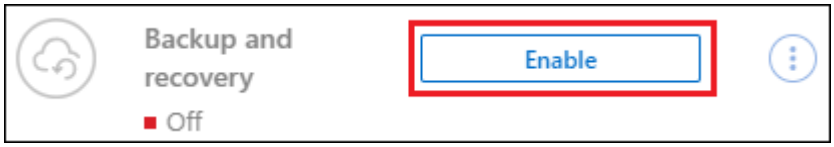
È possibile abilitare il backup e il ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro.

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.



Per modificare le impostazioni di backup o aggiungere la replica, fare riferimento a. "Gestire i backup di 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

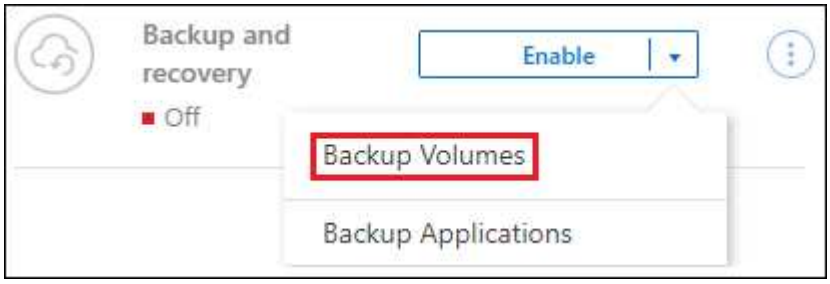
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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 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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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. (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).
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:
   - **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 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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".
3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne uno.

   Per creare un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

   Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
   - Immettere il nome del criterio.
   - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare la replica, fare riferimento alla sezione "Creare un criterio".

     Per creare un criterio, selezionare **Crea nuovo criterio** ed effettuare le seguenti operazioni:
     - Immettere il nome del criterio.
     - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

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

  - Immettere il nome del criterio.
  - Selezionare fino a 5 programmi, generalmente di 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 "Pannello Job Monitoring (monitoraggio processi)".

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 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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema Cloud Volumes ONTAP in Google o a un sistema ONTAP on-premise.

Eseguire il backup dei dati ONTAP on-premise su Amazon S3

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dei volumi dai tuoi sistemi ONTAP on-premise su un sistema di storage secondario e su uno storage cloud Amazon S3.

> I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

Avvio rapido

Inizia subito seguendo questa procedura. I dettagli di ciascuna fase sono forniti nelle sezioni seguenti di questo argomento.

1 Identificare il metodo di connessione da utilizzare

Scegliere se connettere il cluster ONTAP on-premise direttamente ad AWS S3 tramite Internet pubblico o se utilizzare una connessione diretta VPN o AWS e instradare il traffico ad AWS S3 attraverso un'interfaccia

endpoint privata VPC.

Identificare il metodo di connessione.

2 Preparare il connettore BlueXP

Se si dispone già di un connettore implementato in AWS VPC o on-premise, si è tutti pronti. In caso contrario, è necessario creare un connettore BlueXP per eseguire il backup dei dati ONTAP nello storage AWS S3. Sarà inoltre necessario personalizzare le impostazioni di rete per il connettore in modo che possa connettersi ad AWS S3.

Scopri come creare un connettore e come definire le impostazioni di rete richieste.

3 Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per AWS e BlueXP.

Fare riferimento a. Verificare i requisiti di licenza.

4 Preparare i cluster ONTAP

Individuare i cluster ONTAP in BlueXP, verificare che soddisfino i requisiti minimi e personalizzare le impostazioni di rete in modo che i cluster possano connettersi ad AWS S3.

Scopri come preparare i cluster ONTAP.

5 Preparare Amazon S3 come destinazione di backup

Impostare le autorizzazioni per il connettore per creare e gestire il bucket S3. È inoltre necessario impostare le autorizzazioni per il cluster ONTAP on-premise in modo che possa leggere e scrivere i dati nel bucket S3.

In alternativa, puoi impostare le tue chiavi personalizzate per la crittografia dei dati invece di utilizzare le chiavi di crittografia Amazon S3 predefinite. Scopri come preparare il tuo ambiente AWS S3 per ricevere backup ONTAP.

6 Attivare i backup sui volumi ONTAP

Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra. Quindi, seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

Attivare i backup sui volumi ONTAP.

Identificare il metodo di connessione

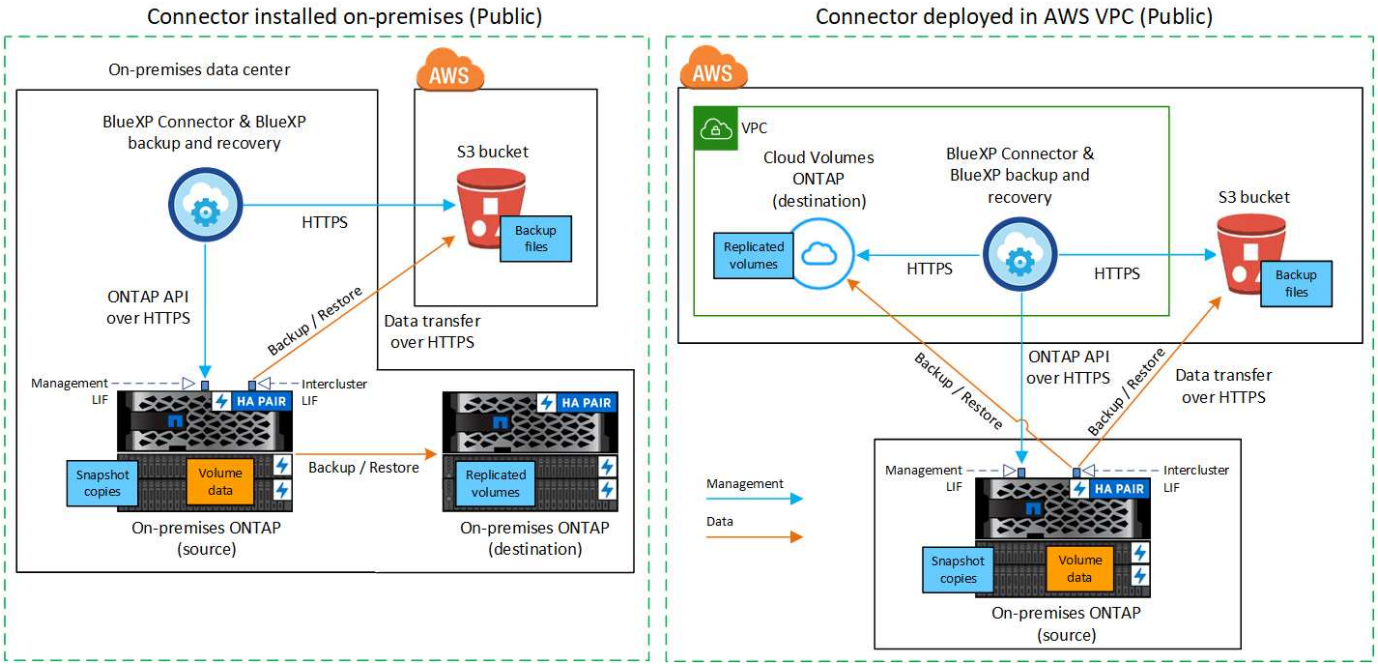
Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup da sistemi ONTAP on-premise ad AWS S3.

- **Connessione pubblica** - connette direttamente il sistema ONTAP ad AWS S3 utilizzando un endpoint pubblico S3.

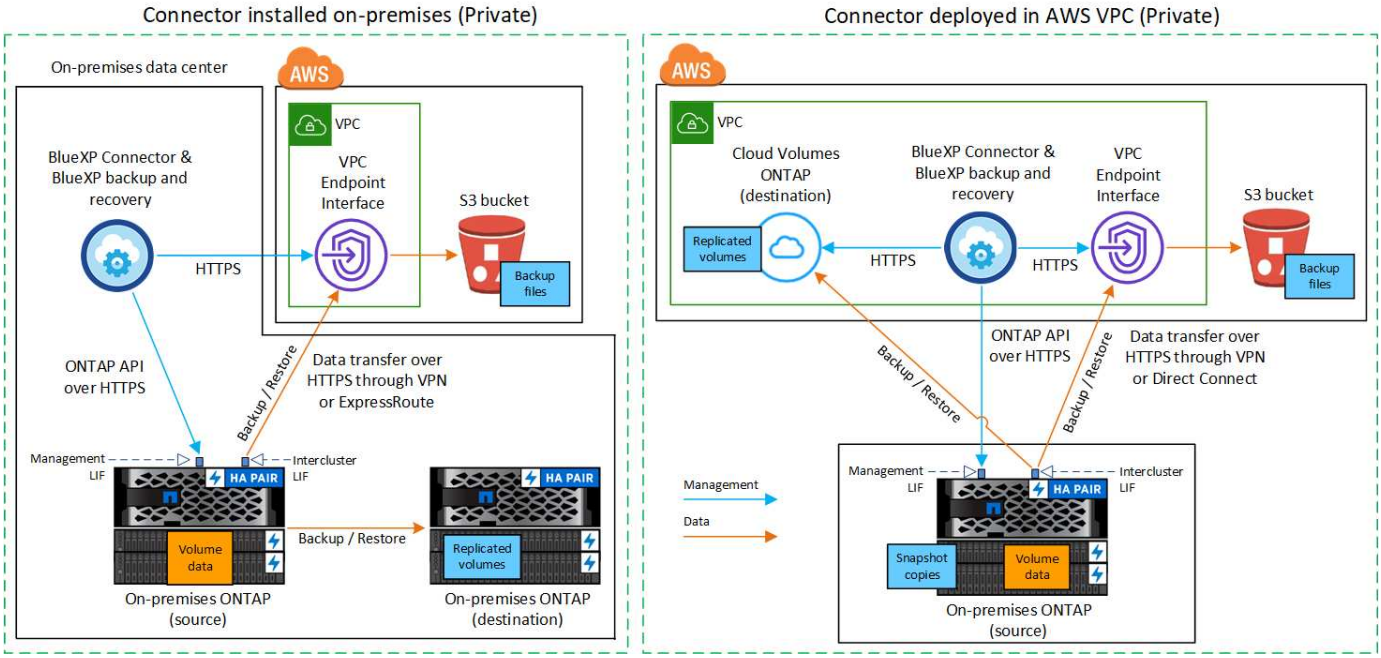
- **Connessione privata** - utilizza una connessione VPN o AWS Direct e instrada il traffico attraverso un'interfaccia endpoint VPC che utilizza un indirizzo IP privato.

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.
- "Assicurarsi che il connettore disponga delle autorizzazioni per gestire il bucket S3".
- 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. Scopri come configurare 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. "Scopri come gestire le tue licenze BYOL".

- È necessario disporre di un abbonamento AWS per lo spazio di storage a oggetti in cui verranno collocati i backup.

Regioni supportate

Puoi creare backup da sistemi on-premise ad Amazon S3 in tutte le regioni "Dove è supportato Cloud Volumes ONTAP"; Incluse le regioni di 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. Scopri come configurare un'interfaccia endpoint VPC e caricare il certificato S3.
- "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. Confermare che le seguenti autorizzazioni S3 (dall'ultima "Policy BlueXP") Fanno parte del ruolo IAM che fornisce al connettore le autorizzazioni necessarie. In caso contrario, consultare "Documentazione AWS: Modifica delle policy IAM".

```
{
            "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-*`.

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. "Fare riferimento a come utilizzare le proprie chiavi".

Configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC

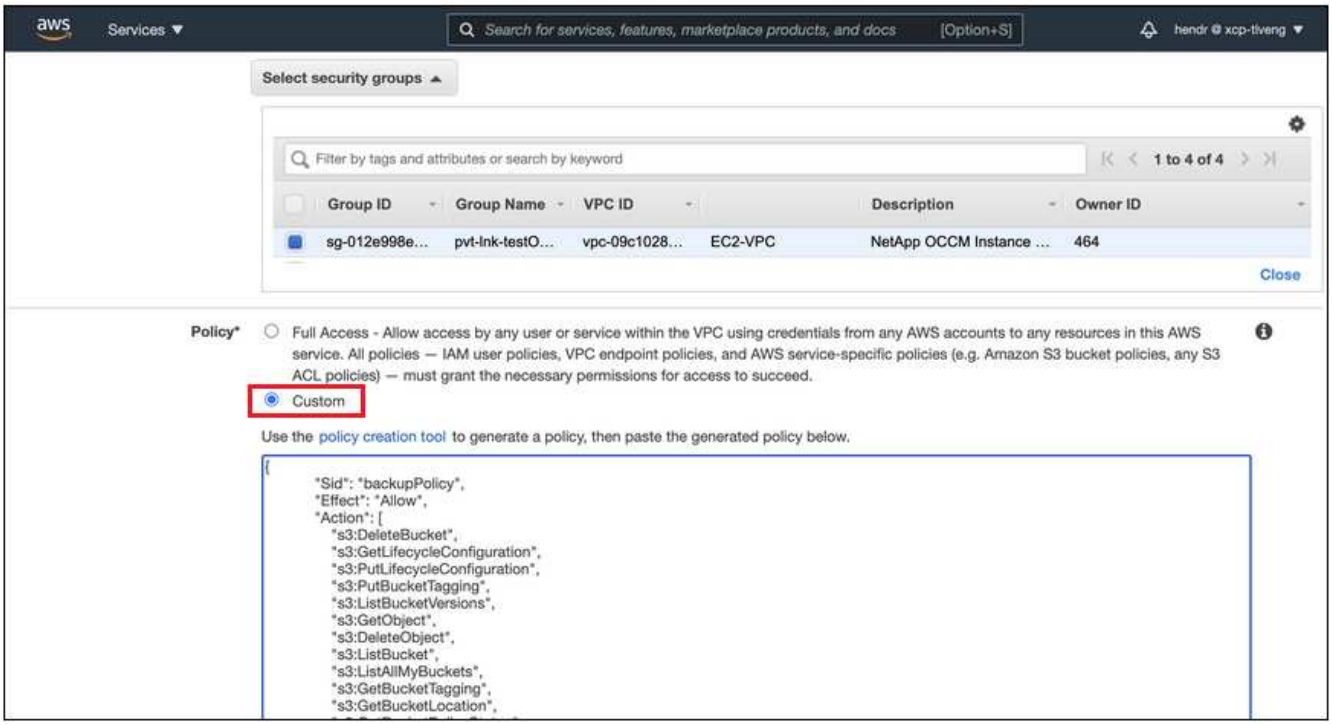
Se si desidera utilizzare una connessione Internet pubblica standard, tutte le autorizzazioni vengono impostate dal connettore e non è necessario eseguire altre operazioni. Questo tipo di connessione viene mostrato nella "primo diagramma".

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. Questo tipo di connessione viene mostrato nella "secondo diagramma".

Fasi

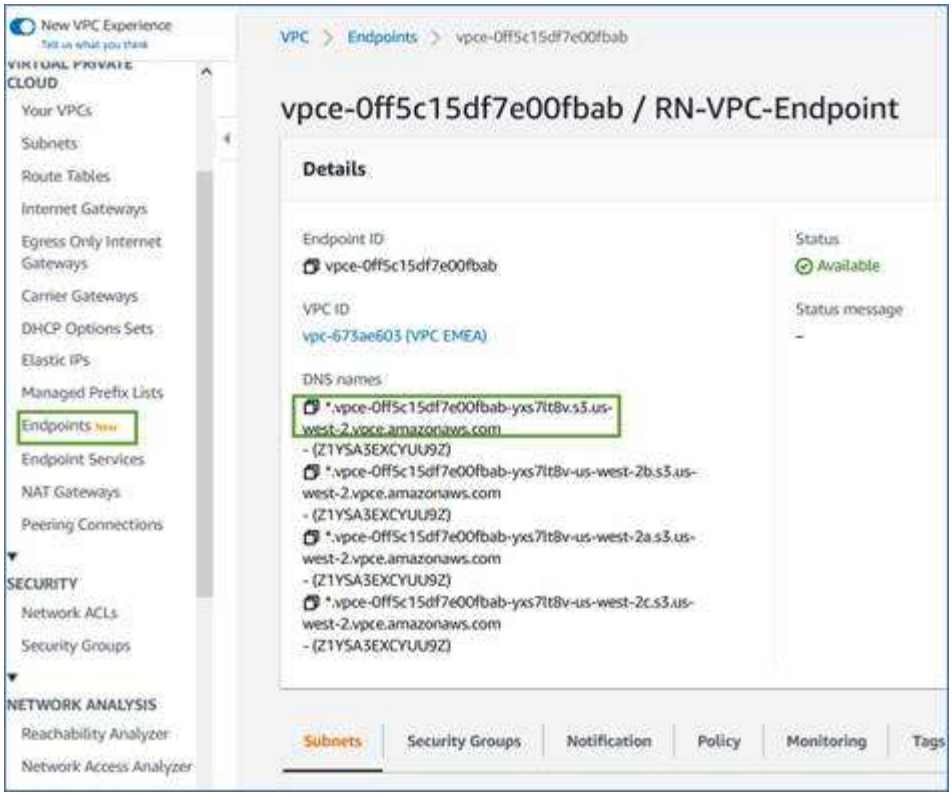
1. Creare una configurazione dell'endpoint dell'interfaccia utilizzando la console Amazon VPC o la riga di comando. "Consulta i dettagli sull'utilizzo di AWS PrivateLink per Amazon S3".
2. Modificare la configurazione del gruppo di protezione associata a BlueXP Connector. È necessario modificare la policy 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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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. (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).
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:
   - **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 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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".

3. **Istantanea locale**: Scegliere un criterio istantanea esistente o creare un criterio.

   Per creare un criterio personalizzato prima di attivare l'istantanea, fare riferimento alla sezione "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 5 programmi, generalmente di frequenze diverse.
     - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per ulteriori informazioni su DataLock e protezione dal ransomware, 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 un criterio personalizzato prima di attivare la replica, fare riferimento alla sezione "Creare un criterio".

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

     - Immettere il nome del criterio.
     - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

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

  - Immettere il nome del criterio.
  - Selezionare fino a 5 programmi, generalmente di 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.

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 "Pannello Job Monitoring (monitoraggio processi)".

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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema Cloud Volumes ONTAP in AWS o a un sistema ONTAP on-premise.

Eseguire il backup dei dati ONTAP on-premise nello storage Azure Blob

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dei volumi dai sistemi ONTAP on-premise a un sistema di storage secondario e a Azure Blob Storage.

> I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

Avvio rapido

Inizia subito seguendo questa procedura. I dettagli di ciascuna fase sono forniti nelle sezioni seguenti di questo argomento.

1 Identificare il metodo di connessione da utilizzare

Scegli se connettere il tuo cluster ONTAP on-premise direttamente ad Azure tramite Internet pubblico o se utilizzerai una VPN o Azure ExpressRoute e instraderai il traffico attraverso un'interfaccia endpoint VPC privata ad Azure.

Identificare il metodo di connessione.

2 Preparare il connettore BlueXP

Se hai già un connettore implementato in Azure VNET o on-premise, allora sei tutto impostato. In caso contrario, è necessario creare un connettore BlueXP per eseguire il backup dei dati ONTAP nello storage Azure Blob. Sarà inoltre necessario personalizzare le impostazioni di rete per il connettore in modo che possa connettersi ad Azure.

Scopri come creare un connettore e come definire le impostazioni di rete richieste.

3 Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per Azure e BlueXP.

Fare riferimento a. Verificare i requisiti di licenza.

4 Preparare i cluster ONTAP

Scopri i cluster ONTAP in BlueXP, verifica che soddisfino i requisiti minimi e personalizza le impostazioni di rete in modo che i cluster possano connettersi ad Azure.

Scopri come preparare i cluster ONTAP.

5 Preparare Azure Blob come destinazione di backup

Impostare le autorizzazioni per il connettore per creare e gestire il bucket Azure. È inoltre necessario impostare le autorizzazioni per il cluster ONTAP on-premise in modo che possa leggere e scrivere i dati nel bucket Azure.

In alternativa, è possibile impostare chiavi personalizzate per la crittografia dei dati invece di utilizzare le chiavi di crittografia predefinite di Azure. Scopri come preparare il tuo ambiente Azure per ricevere i backup di ONTAP.

6 Attivare i backup sui volumi ONTAP

Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra. Quindi, seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

Attivare i backup sui volumi ONTAP.

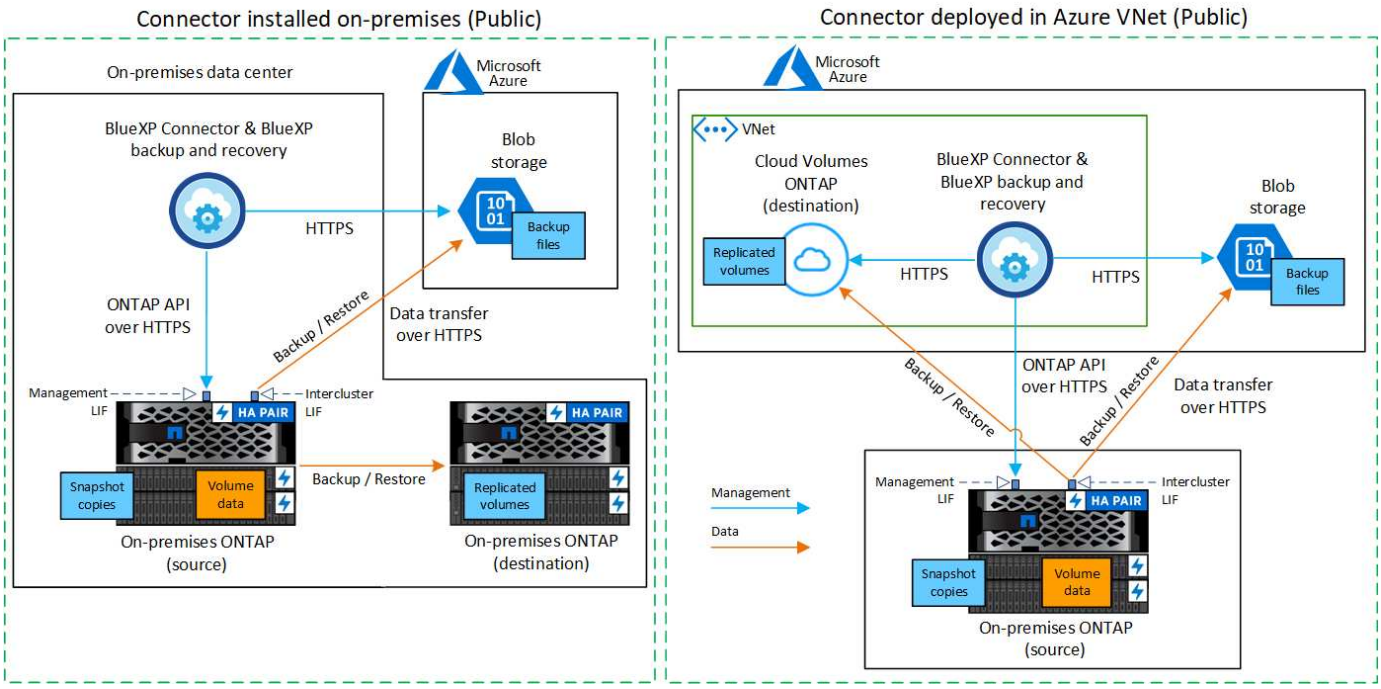
Identificare il metodo di connessione

Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup da sistemi ONTAP on-premise a Azure Blob.

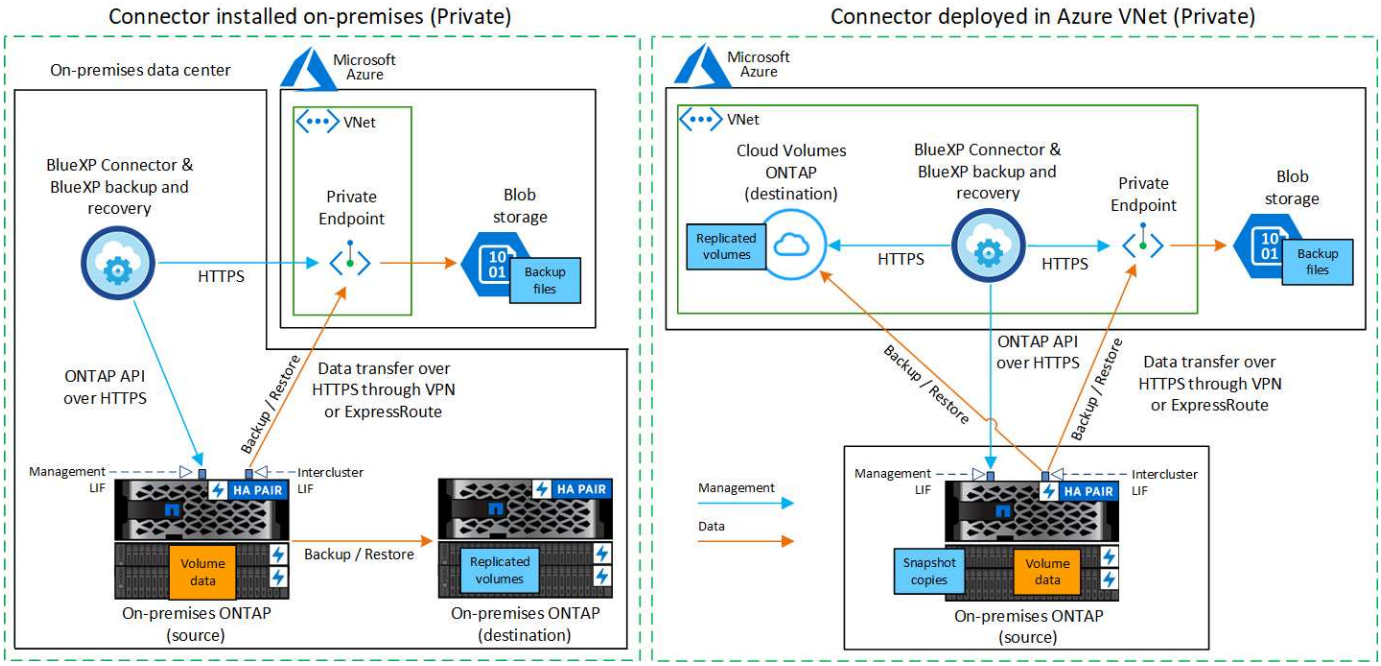
- **Connessione pubblica** - connette direttamente il sistema ONTAP allo storage Azure Blob utilizzando un endpoint Azure pubblico.
- **Connessione privata** - utilizza una VPN o ExpressRoute e instrada il traffico attraverso un VNET Private Endpoint che utilizza un indirizzo IP privato.

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 da sistemi on-premise a Azure Blob in tutte le regioni "Dove è supportato Cloud Volumes ONTAP"; Incluse le regioni governative di Azure. 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:

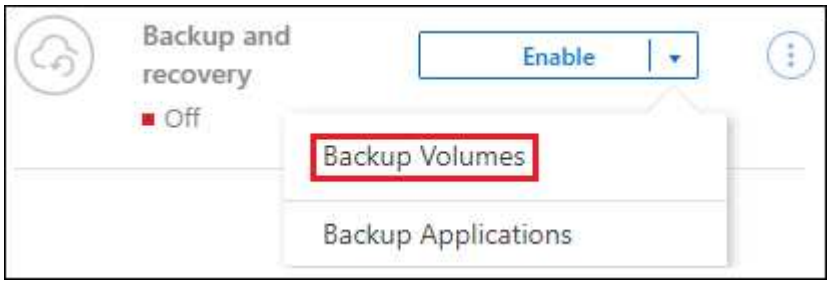
- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

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. (I volumi con la modalità conformità SnapLock non sono attualmente supportati richiedono ONTAP 9,14 o versioni successive).

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. (☑ Volume Name).
- Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).

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:
   - **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 dallo storage secondario allo storage a oggetti.
   - **Fan out**: I flussi di informazioni dal primario al secondario *e* dallo storage primario a oggetti.

     Per ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".
3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne uno nuovo.

   > Per creare un criterio personalizzato prima di attivare l'istantanea, fare riferimento alla sezione "Creare un criterio".

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

   - Immettere il nome del criterio.
   - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare la replica, fare riferimento alla sezione "Creare un criterio".

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

     - Immettere il nome del criterio.
     - Selezionare fino a 5 programmi, generalmente di 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. Se lo si desidera, scegliere se utilizzare un endpoint privato Azure precedentemente configurato. "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 un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

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

  - Immettere il nome del criterio.
  - Selezionare fino a 5 programmi, generalmente di frequenze diverse.
  - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per ulteriori informazioni su DataLock e protezione dal ransomware, 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 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 "Pannello Job Monitoring (monitoraggio processi)".

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 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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema Cloud Volumes ONTAP in Azure o a un sistema ONTAP on-premise.

Eseguire il backup dei dati ONTAP on-premise su Google Cloud Storage

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dei volumi dai tuoi sistemi ONTAP primari on-premise su un sistema di storage secondario e su Google Cloud Storage.

> I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

Avvio rapido

Inizia subito seguendo questa procedura. I dettagli di ciascuna fase sono forniti nelle sezioni seguenti di questo argomento.

1 Identificare il metodo di connessione da utilizzare

Scegli se connettere il tuo cluster ONTAP on-premise direttamente allo storage cloud di Google tramite Internet pubblico o se utilizzerai una VPN o un'interconnessione cloud di Google e instraderai il traffico attraverso un'interfaccia privata di Google Access che utilizza un indirizzo IP privato.

Identificare il metodo di connessione.

2 Preparare il connettore BlueXP

Se hai già un connettore implementato nel tuo VPC Google Cloud Platform, allora sei tutto impostato. In caso contrario, è necessario creare un connettore BlueXP per eseguire il backup dei dati ONTAP sullo storage Google Cloud. Sarà inoltre necessario personalizzare le impostazioni di rete per il connettore in modo che

possa connettersi a Google Cloud.

Scopri come creare un connettore e come definire le impostazioni di rete richieste.

3 Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per Google Cloud e BlueXP.

Fare riferimento a. Verificare i requisiti di licenza.

4 Preparare i cluster ONTAP

Scopri i tuoi cluster ONTAP in BlueXP, verifica che soddisfino i requisiti minimi e personalizza le impostazioni di rete in modo che i cluster possano connettersi a Google Cloud.

Scopri come preparare i cluster ONTAP.

5 Prepara Google Cloud come destinazione per il backup

Impostare le autorizzazioni per il connettore per creare e gestire il bucket Google Cloud. Dovrai anche impostare le autorizzazioni per il cluster ONTAP on-premise in modo che possa leggere e scrivere i dati nel bucket di Google Cloud.

In alternativa, è possibile impostare chiavi personalizzate per la crittografia dei dati invece di utilizzare le chiavi di crittografia predefinite di Google Cloud. Scopri come preparare il tuo ambiente Google Cloud per ricevere i backup di ONTAP.

6 Attivare i backup sui volumi ONTAP

Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra. Quindi, seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

Attivare i backup sui volumi ONTAP.

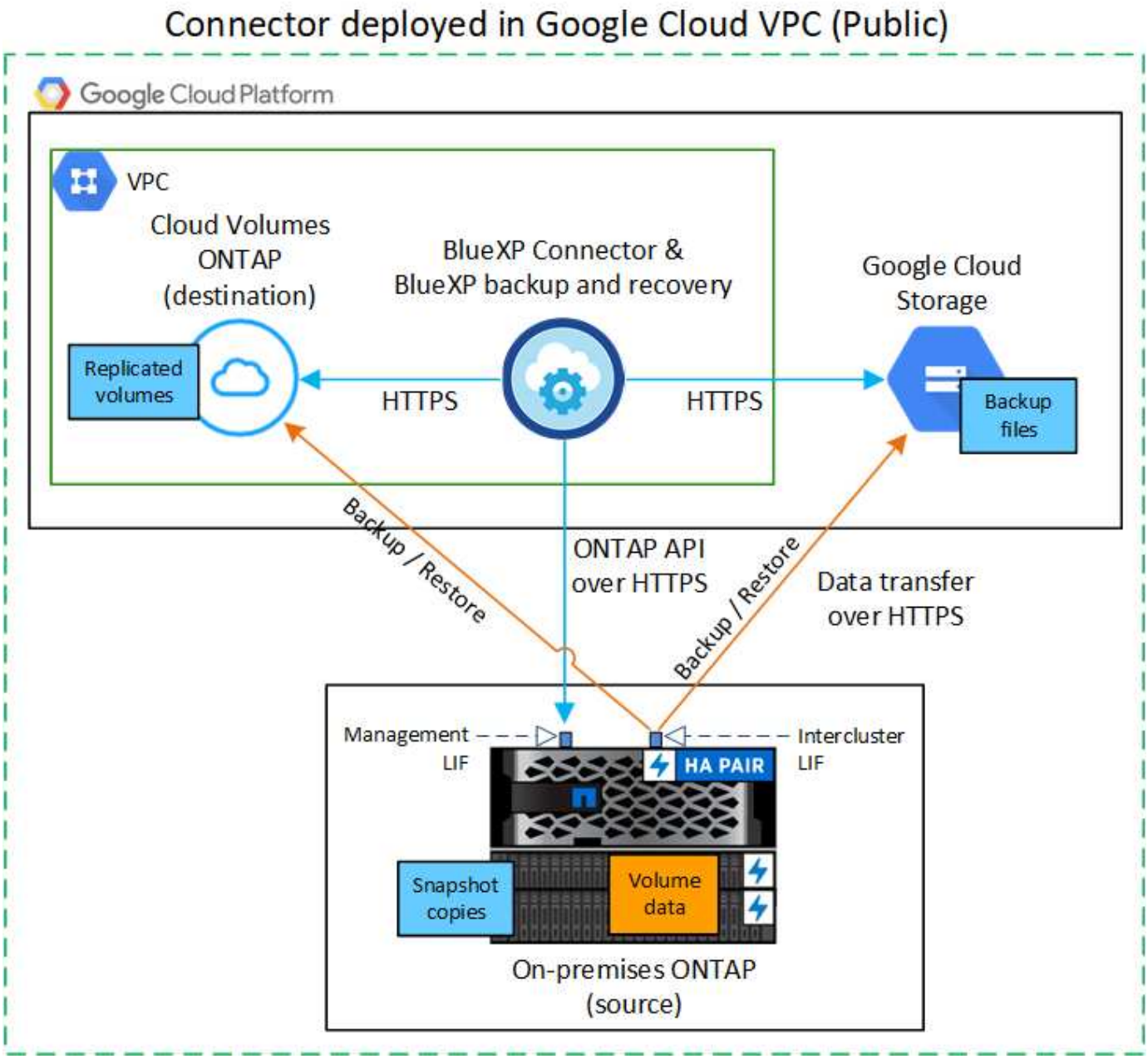
Identificare il metodo di connessione

Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup dai sistemi ONTAP on-premise allo storage cloud Google.

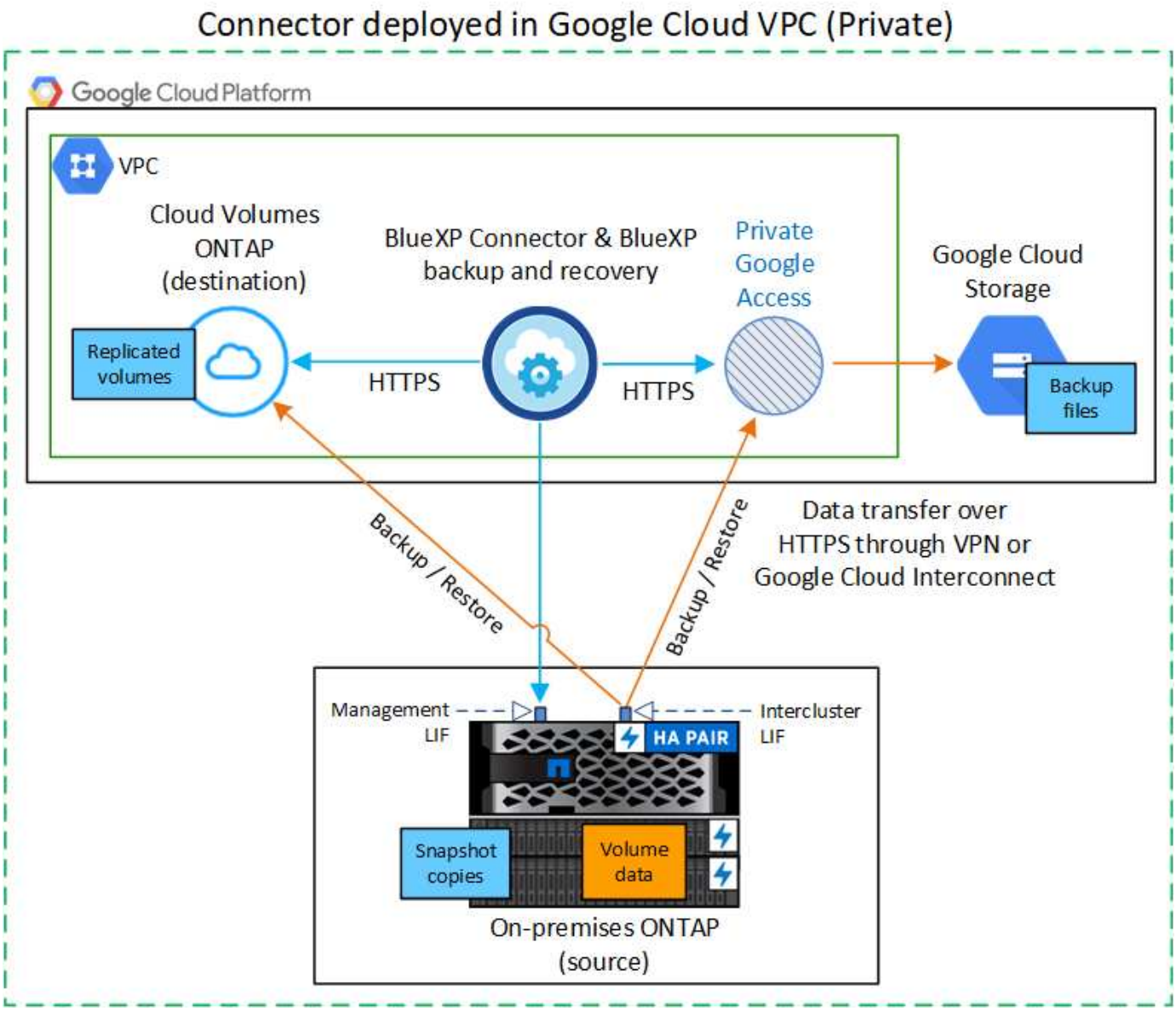
- **Connessione pubblica** - consente di connettere direttamente il sistema ONTAP allo storage cloud di Google utilizzando un endpoint pubblico di Google.
- **Connessione privata** - utilizza una VPN o Google Cloud Interconnect e instrada il traffico attraverso un'interfaccia privata di Google Access 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

Puoi creare backup da sistemi on-premise a Google Cloud Storage in tutte le regioni "Dove è supportato Cloud Volumes ONTAP". 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

Quando si imposta il backup, è necessario fornire chiavi di accesso allo storage per un account di servizio che dispone di autorizzazioni specifiche. 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. Vedere "Documentazione di Google Cloud: Abilitazione delle API" per ulteriori informazioni.

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

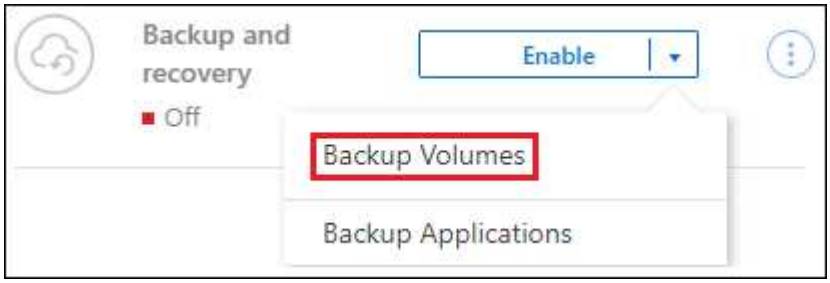
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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. (Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (Volume_1).
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:
   - **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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".

3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne uno nuovo.

   Per creare un criterio personalizzato prima di attivare l'istantanea, fare riferimento alla sezione "Creare un criterio".

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

   - Immettere il nome del criterio.
   - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare la replica, fare riferimento alla sezione "Creare un criterio".

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

     - Immettere il nome del criterio.
     - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

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

  - Immettere il nome del criterio.
  - Selezionare fino a 5 programmi, generalmente di 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 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 "Pannello Job Monitoring (monitoraggio processi)".

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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema Cloud Volumes ONTAP in Google o a un sistema ONTAP on-premise.

Effettua il backup dei dati ONTAP on-premise su ONTAP S3

Completa alcuni passaggi per iniziare il backup dei dati dei volumi dai sistemi ONTAP on-premise primari. 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).

Avvio rapido

Inizia subito seguendo questa procedura. I dettagli di ciascuna fase sono forniti nelle sezioni seguenti di questo argomento.

1 **Identificare il metodo di connessione da utilizzare**

Rivedere le modalità di connessione del cluster ONTAP primario on-premise al cluster ONTAP secondario per la replica e al cluster ONTAP configurato come server S3 per il backup nello storage a oggetti.

Identificare il metodo di connessione.

2 Preparare il connettore BlueXP

Se hai già implementato un connettore BlueXP, sai tutto. In caso contrario, dovrai creare un connettore BlueXP per eseguire il backup dei dati ONTAP su ONTAP S3. È inoltre necessario personalizzare le impostazioni di rete per il connettore in modo che possa connettersi a ONTAP S3.

Scopri come creare un connettore e come definire le impostazioni di rete richieste.

3 Verificare i requisiti di licenza

Dovrai controllare i requisiti di licenza per i tuoi sistemi ONTAP e per il backup e recovery di BlueXP.

Verificare i requisiti di licenza.

4 Preparare i cluster ONTAP

Scopri i tuoi cluster ONTAP primari e secondari in BlueXP, verifica che i cluster soddisfino i requisiti minimi e personalizza le impostazioni di rete in modo che i cluster possano connettersi allo storage a oggetti ONTAP S3.

Scopri come preparare i cluster ONTAP.

5 Preparare ONTAP S3 come destinazione di backup

Impostare le autorizzazioni per il connettore in modo che possa gestire il bucket ONTAP S3. Inoltre, dovrai impostare le autorizzazioni per il cluster ONTAP on-premise di origine in modo che possa leggere e scrivere i dati nel bucket ONTAP S3.

Scoprite come preparare il vostro ambiente ONTAP S3 a ricevere i backup ONTAP.

6 Attivare i backup sui volumi ONTAP

Selezionare l'ambiente di lavoro principale e fare clic su **Abilita > volumi di backup** accanto al servizio di backup e ripristino nel pannello a destra. Quindi, segui la procedura di installazione guidata per selezionare i volumi da sottoporre a backup e le policy snapshot, replica e backup su oggetti che utilizzerai.

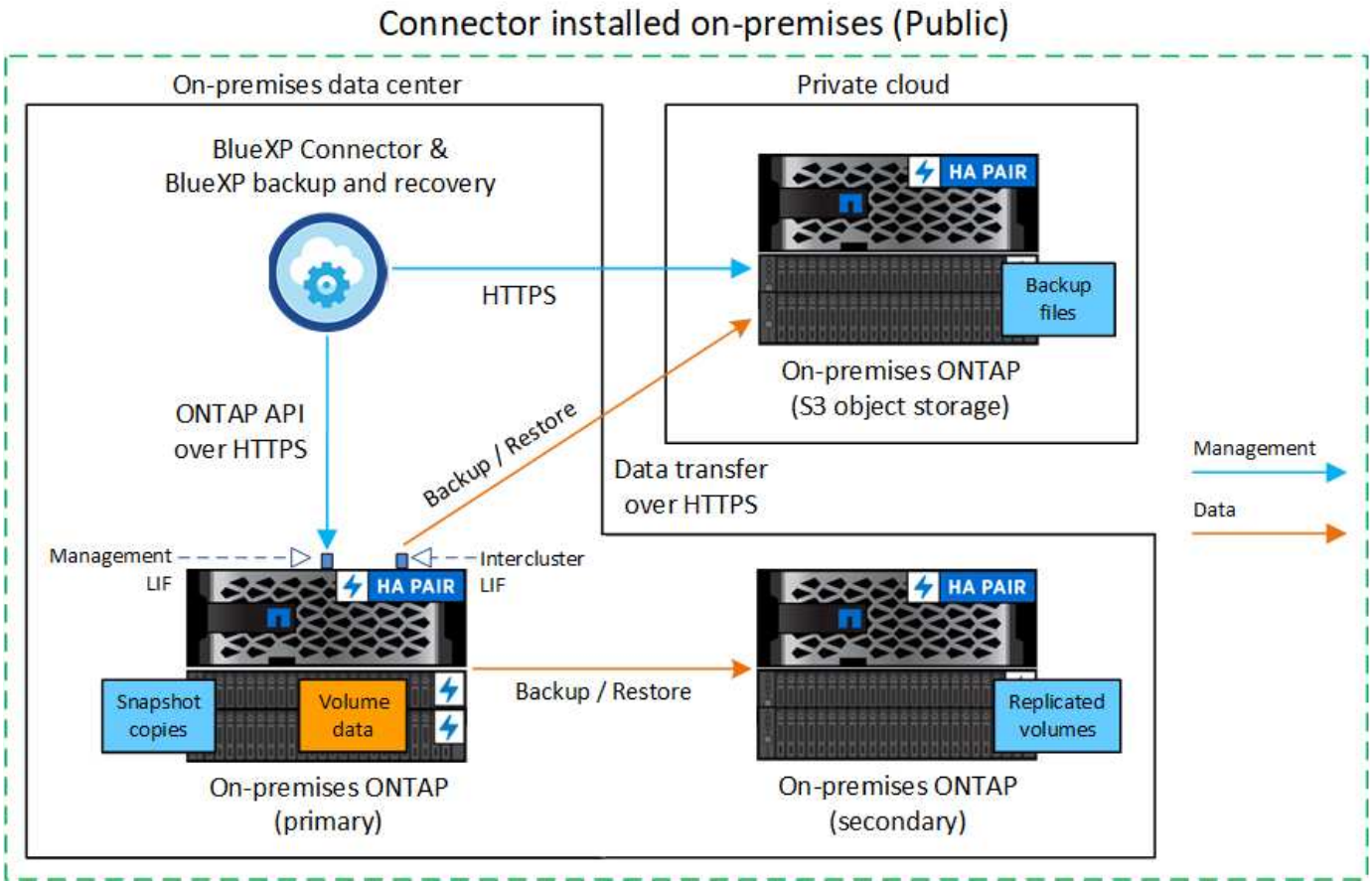
Attivare i backup sui ONTAP Volumes.

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.

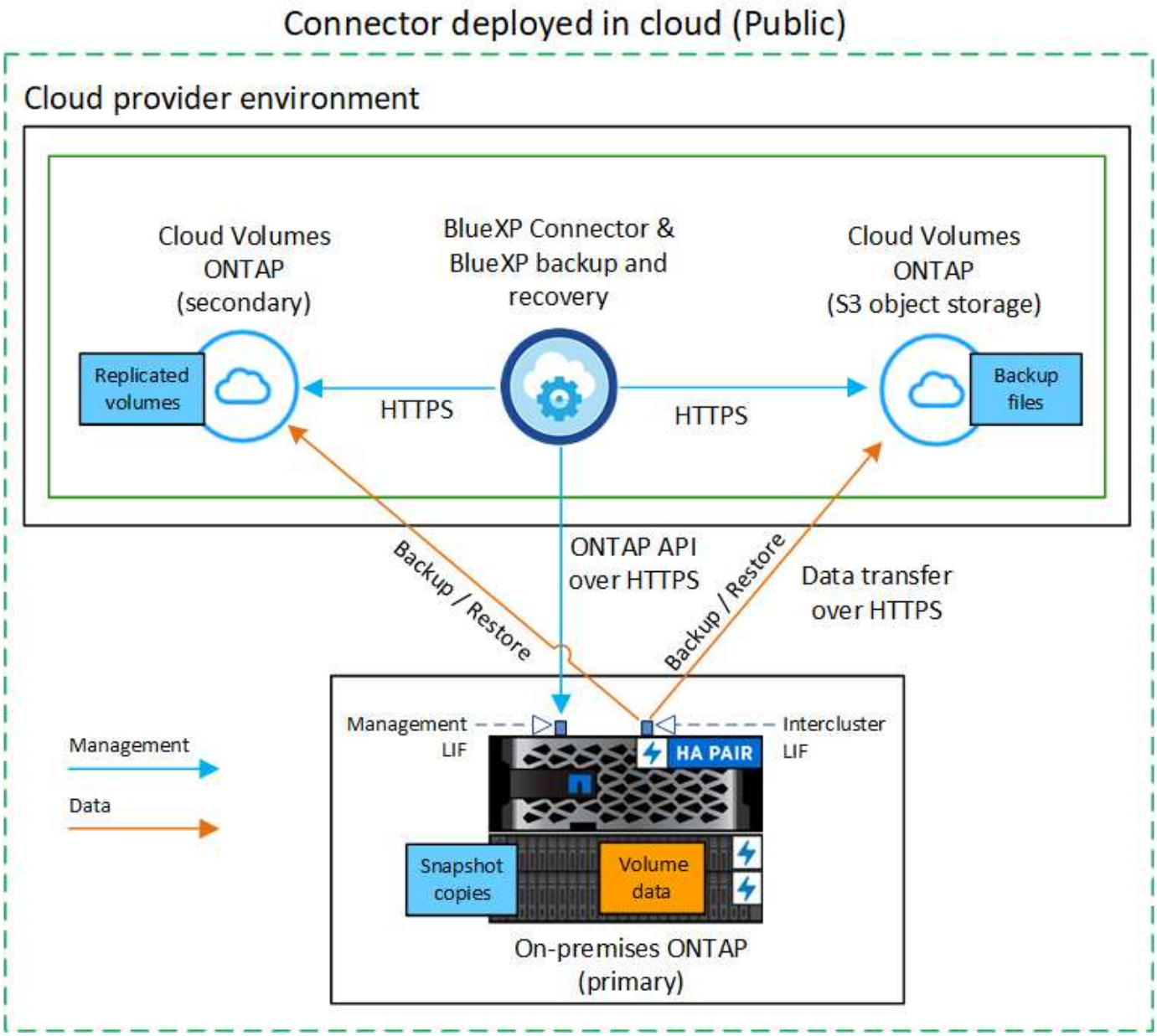
L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario on-premise su un sistema ONTAP on-premise configurato per S3 e le connessioni da preparare tra di essi. Mostra inoltre

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. Se si verifica un errore del connettore nel sito in modalità privata, è possibile "Ripristinare i dati di backup e ripristino di BlueXP su un nuovo connettore".

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).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui istantanee 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. 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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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. (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup comporta la configurazione delle seguenti opzioni:

- Opzioni di protezione: Se si desidera implementare una o tutte le opzioni di backup: Snapshot locali, replica e backup sullo storage a oggetti
- Architettura: Se vuoi utilizzare un'architettura di backup fan-out o a cascata
- Policy 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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".

3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne 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 prima di attivare l'istantanea, fare riferimento alla "Creare un criterio".

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

   - Immettere il nome del criterio.
   - Selezionare fino a 5 programmi, generalmente di 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 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare il backup utilizzando l'interfaccia utente, fare riferimento alla sezione "Creare un criterio".

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

  - Immettere il nome del criterio.
  - Selezionare fino a 5 programmi, generalmente di frequenze diverse.
  - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per ulteriori informazioni su DataLock e protezione dal ransomware, fare riferimento a. "Impostazioni dei criteri di backup su oggetti".
  - Selezionare **Crea**.

- **Esporta copie Snapshot esistenti nello storage a oggetti come file 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 (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt 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 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 "Pannello Job Monitoring (monitoraggio processi)".

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 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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema ONTAP on-premise.

Eseguire il backup dei dati ONTAP on-premise su StorageGRID

Completare alcuni passaggi per iniziare il backup dei dati dei volumi dai sistemi ONTAP primari on-premise a un sistema di storage secondario e a uno storage a oggetti nei sistemi NetApp StorageGRID.

> I "sistemi ONTAP on-premise" includono sistemi FAS, AFF e ONTAP Select.

Avvio rapido

Inizia subito seguendo questa procedura. I dettagli di ciascuna fase sono forniti nelle sezioni seguenti di questo argomento.

1 Identificare il metodo di connessione da utilizzare

Scopri come connettere il tuo cluster ONTAP on-premise direttamente a StorageGRID tramite Internet pubblico o se utilizzerai una VPN e instraderai il traffico attraverso un'interfaccia endpoint privata VPC a StorageGRID.

Identificare il metodo di connessione.

2 Preparare il connettore BlueXP

Se hai già un connettore implementato nella tua sede, allora sei tutto impostato. In caso contrario, sarà

necessario creare un connettore BlueXP per eseguire il backup dei dati ONTAP su StorageGRID. Sarà inoltre necessario personalizzare le impostazioni di rete per il connettore in modo che possa connettersi a StorageGRID.

Scopri come creare un connettore e come definire le impostazioni di rete richieste.

3 Verificare i requisiti di licenza

È necessario verificare i requisiti di licenza per StorageGRID e BlueXP.

Fare riferimento a. Verificare i requisiti di licenza.

4 Preparare i cluster ONTAP

Individuare i cluster ONTAP in BlueXP, verificare che soddisfino i requisiti minimi e personalizzare le impostazioni di rete in modo che i cluster possano connettersi a StorageGRID.

Scopri come preparare i cluster ONTAP.

5 Preparare StorageGRID come destinazione del backup

Impostare le autorizzazioni per il connettore per creare e gestire il bucket StorageGRID. È inoltre necessario impostare le autorizzazioni per il cluster ONTAP on-premise in modo che possa leggere e scrivere i dati nel bucket.

In alternativa, è possibile impostare chiavi personalizzate per la crittografia dei dati invece di utilizzare le chiavi di crittografia StorageGRID predefinite. Scopri come preparare il tuo ambiente StorageGRID per ricevere i backup di ONTAP.

6 Attivare i backup sui volumi ONTAP

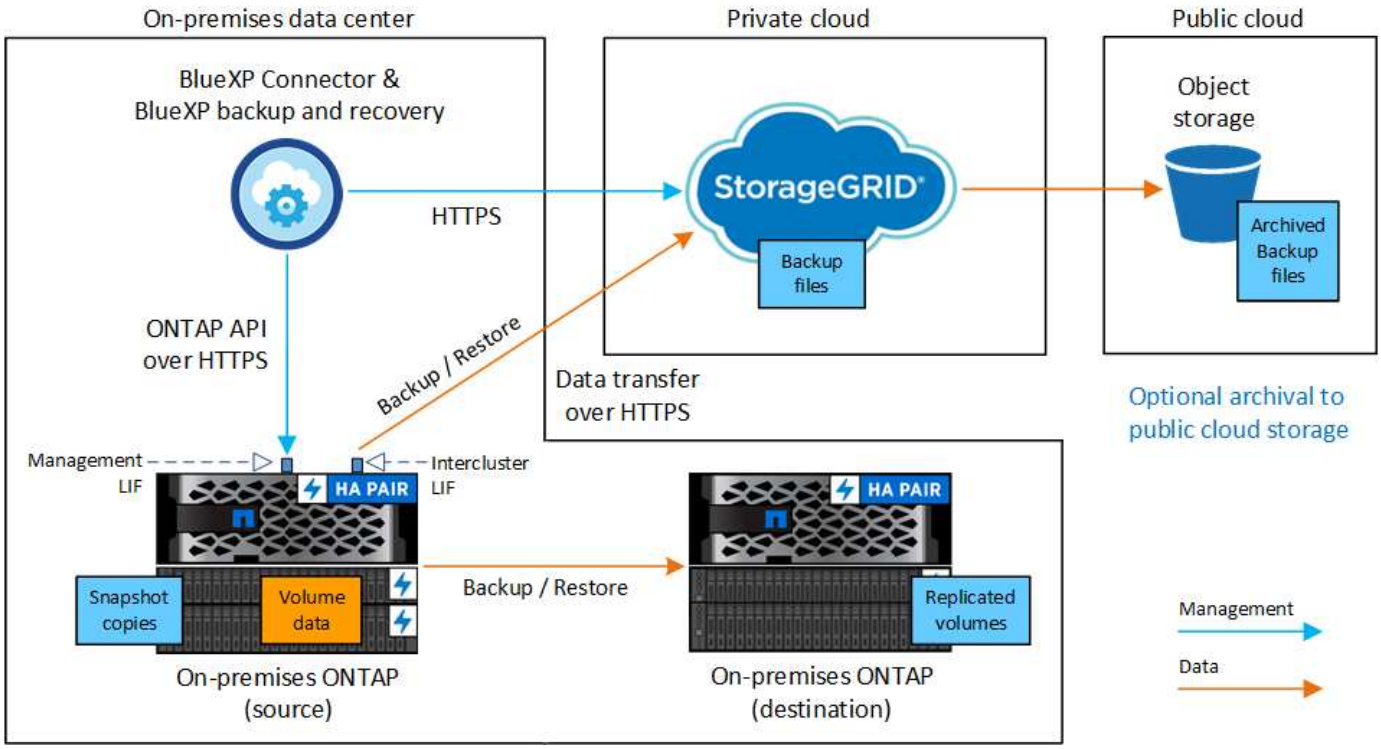
Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra. Quindi, seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui si desidera eseguire il backup.

Attivare i backup sui volumi ONTAP.

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. Se si verifica un errore del connettore nel sito in modalità privata, è possibile "Ripristinare i dati di backup e ripristino di BlueXP su un nuovo connettore".

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.

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.

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

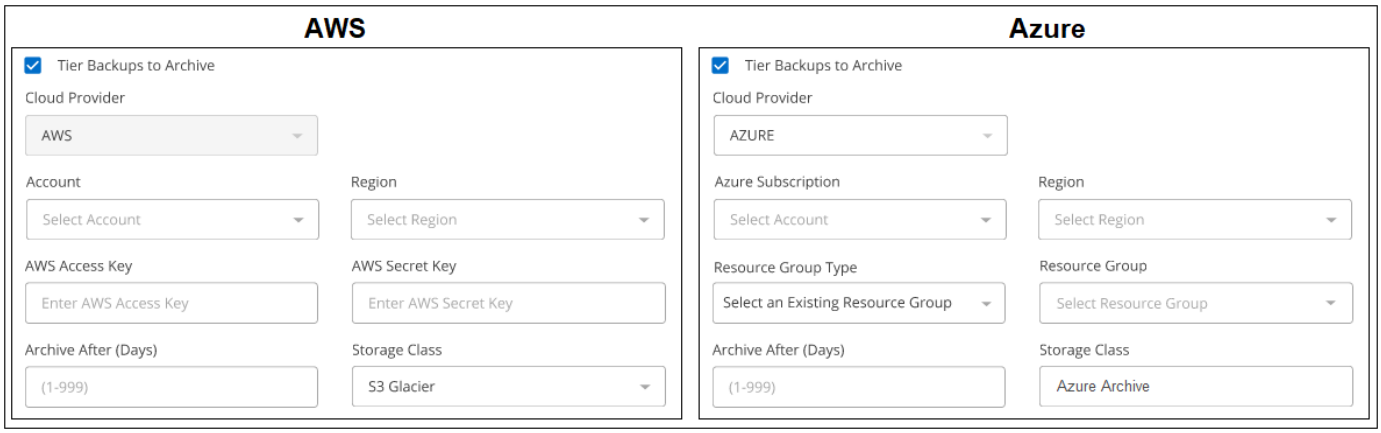
- Dovrai creare un account Amazon S3 per lo spazio di storage in cui verranno archiviati i backup.
- È possibile scegliere di eseguire il Tier dei backup nello storage AWS S3 Glacier o S3 Glacier Deep Archive. "Scopri di più sui Tier di archiviazione AWS".
- StorageGRID deve avere accesso completo al 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 ILM (Information Lifecycle Management) 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. I volumi in modalità conformità SnapLock richiedono ONTAP 9,14 o versione successiva.

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. (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).
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:
   - **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 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 ulteriori informazioni su queste architetture, fare riferimento a. "Pianifica il tuo percorso di protezione".
3. **Istantanea locale**: Scegliere un criterio istantanea esistente o crearne uno nuovo.

   > Per creare un criterio personalizzato prima di attivare l'istantanea, fare riferimento alla sezione "Creare un criterio".

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

   - Immettere il nome del criterio.
   - Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare la replica, fare riferimento alla sezione "Creare un criterio".

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

- Immettere il nome del criterio.
- Selezionare fino a 5 programmi, generalmente di 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 un criterio personalizzato prima di attivare il backup, fare riferimento alla sezione "Creare un criterio".

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

     - Immettere il nome del criterio.
     - Selezionare fino a 5 programmi, generalmente di frequenze diverse.
     - Per le policy di backup su oggetto, imposta le impostazioni DataLock e protezione dal ransomware. Per ulteriori informazioni su DataLock e protezione dal ransomware, 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 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 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 "Pannello Job Monitoring (monitoraggio processi)".

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 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 farlo "ripristinare volumi, cartelle o singoli file da un file di backup" A un sistema ONTAP on-premise.

Gestisci i backup per i tuoi sistemi ONTAP

È possibile gestire i backup per i sistemi Cloud Volumes ONTAP e ONTAP on-premise modificando la pianificazione del backup, attivando/disattivando i backup dei volumi, mettendo in pausa i backup, eliminando i backup e molto altro ancora. Sono inclusi tutti i tipi di backup, incluse le copie Snapshot, i volumi replicati e i file di backup nello storage a oggetti.

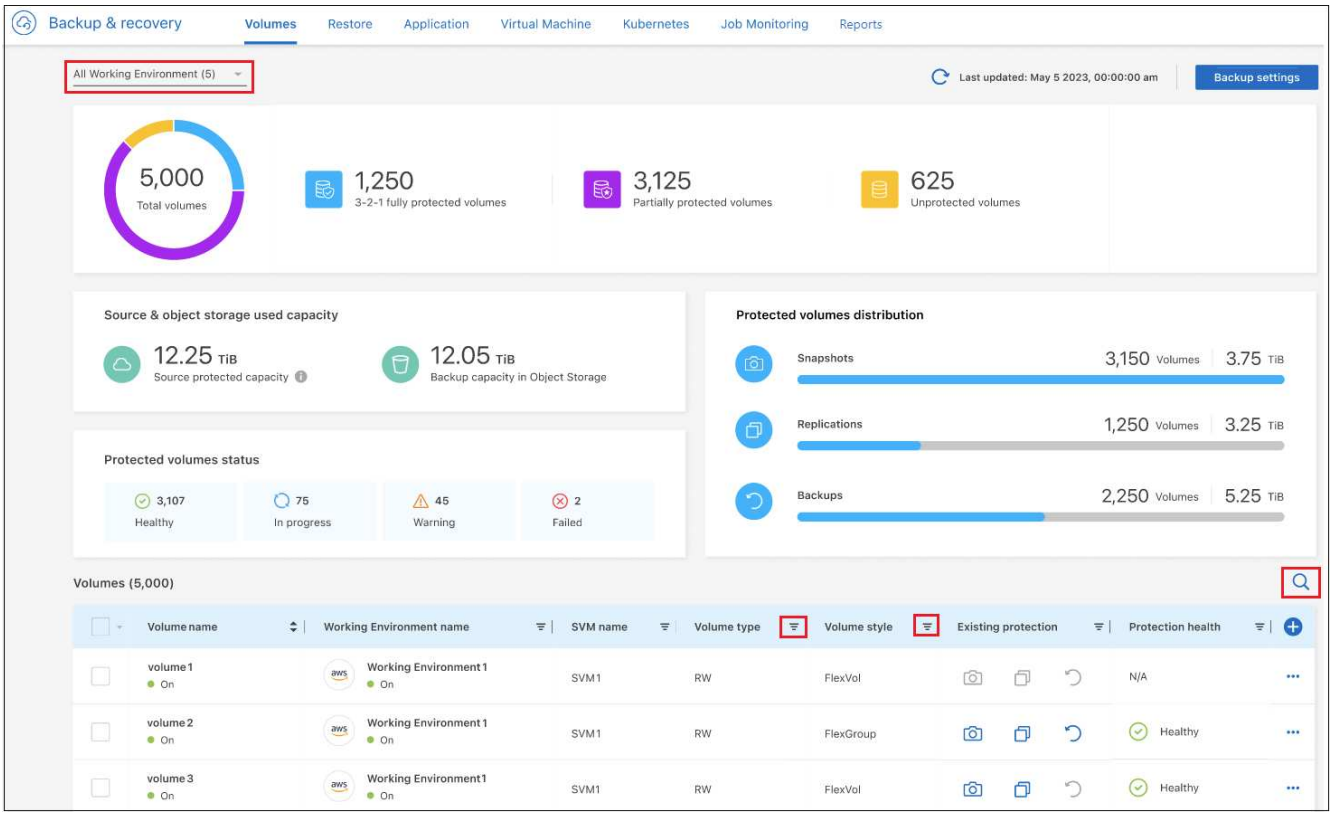
> Non gestire o modificare i file di backup direttamente sui sistemi storage o dall'ambiente del cloud provider. Questo potrebbe danneggiare i file e causare una configurazione non supportata.

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. Sono inclusi tutti i tipi di backup, incluse le copie Snapshot, i volumi replicati e i file di backup nello storage a 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. Fare clic sulla scheda **Volumes** (volumi) per visualizzare l'elenco dei volumi di backup per i sistemi Cloud Volumes ONTAP e ONTAP on-premise.



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 ulteriori colonne (aggregati, stile di protezione (Windows o UNIX), policy di snapshot, policy di replica e policy di backup), selezionare ⊕.

4. Esaminare lo stato delle opzioni di protezione nella colonna "Existing Protection" (protezione esistente). Le tre icone sono "Local Snapshot Copies" (copie Snapshot locali), "Replicated Volumes" (volumi replicati) e "Backup nello storage a oggetti".

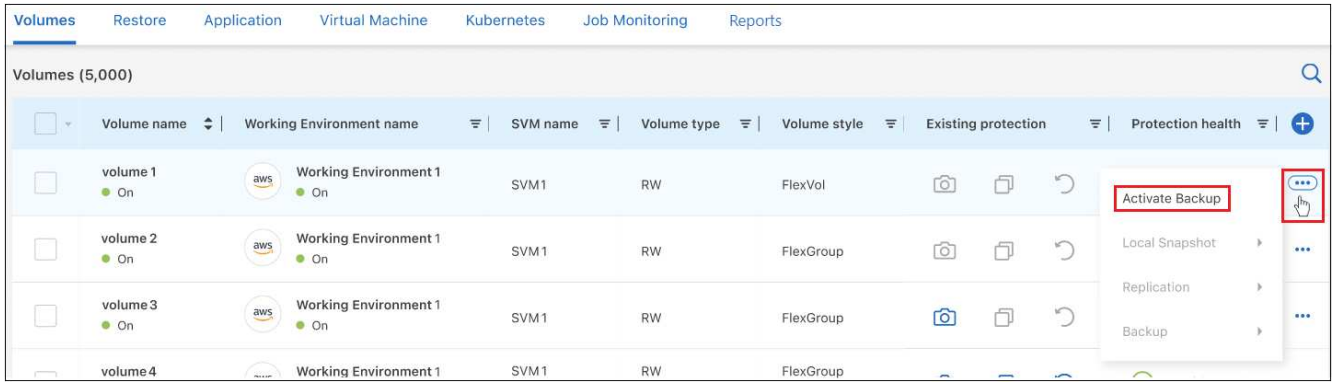
   Ogni icona è blu quando il tipo di backup è attivato e grigia quando il tipo di backup è inattivo. È possibile spostare il cursore su ciascuna icona per visualizzare la policy di backup utilizzata e altre informazioni pertinenti per ciascun tipo di backup.

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 fare clic su **Avanti**.
3. Esaminare le impostazioni di backup per questo volume, quindi fare clic su **Activate Backup** (attiva backup).

Se si desidera attivare il backup su più volumi contemporaneamente con impostazioni di backup identiche, vedere Modificare le impostazioni di backup su più volumi per ulteriori informazioni.

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 nuova policy di Snapshot, replica o backup che si desidera applicare ai volumi deve già esistere.

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*, apportare modifiche alle policy di backup esistenti per le copie Snapshot locali, i volumi replicati e i file di backup e fare clic su **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. Esaminare le impostazioni di backup per questo volume, quindi fare clic su **Activate Backup** (attiva backup).

Modificare le impostazioni di backup su più volumi

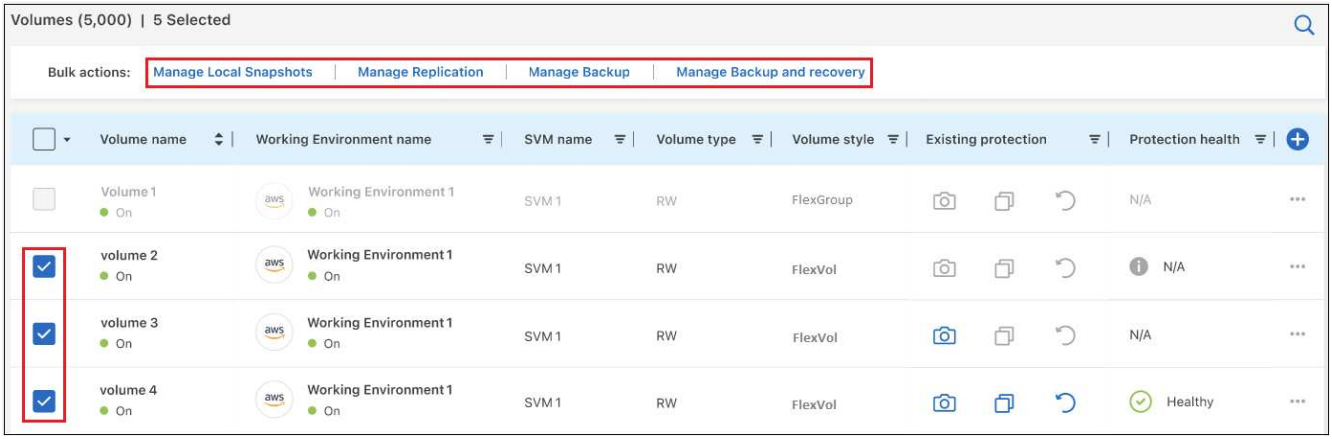
Se si desidera utilizzare le stesse impostazioni di backup su più volumi, è possibile attivare o modificare le impostazioni di backup su più volumi contemporaneamente. È possibile selezionare volumi che non dispongono di impostazioni di backup, solo di impostazioni Snapshot, solo di backup su impostazioni cloud e così via e apportare modifiche in blocco in 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)

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…	Fare clic su questo pulsante…
Gestire le impostazioni di backup di Snapshot	**Gestisci snapshot locali**
Gestire le impostazioni di backup della replica	**Gestisci replica**
Gestire le impostazioni di backup su cloud	**Gestisci backup**
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, apportare modifiche ai criteri di backup esistenti per le copie Snapshot locali, i volumi replicati o i file di backup e fare clic su **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 su un 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 creata un'istantanea sul volume di origine. Poiché questa istantanea non fa parte di una normale pianificazione Snapshot, non viene disattivata. Una volta completato il backup, è possibile eliminare manualmente questa istantanea dal volume di origine. In questo modo, i blocchi correlati a questa istantanea verranno liberati. Il nome dell'istantanea inizia 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 **Volumes** (volumi), fare clic su ••• Per il volume e selezionare **Backup** > **Crea backup ad-hoc**.

La colonna Backup Status (Stato backup) per quel volume visualizza "in corso" fino alla creazione del backup.

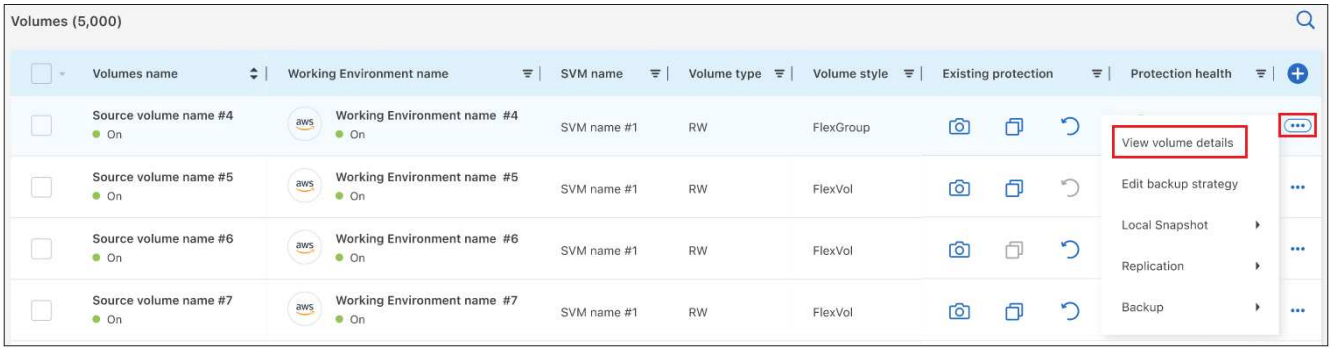
Visualizzare l'elenco dei backup per ciascun volume

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

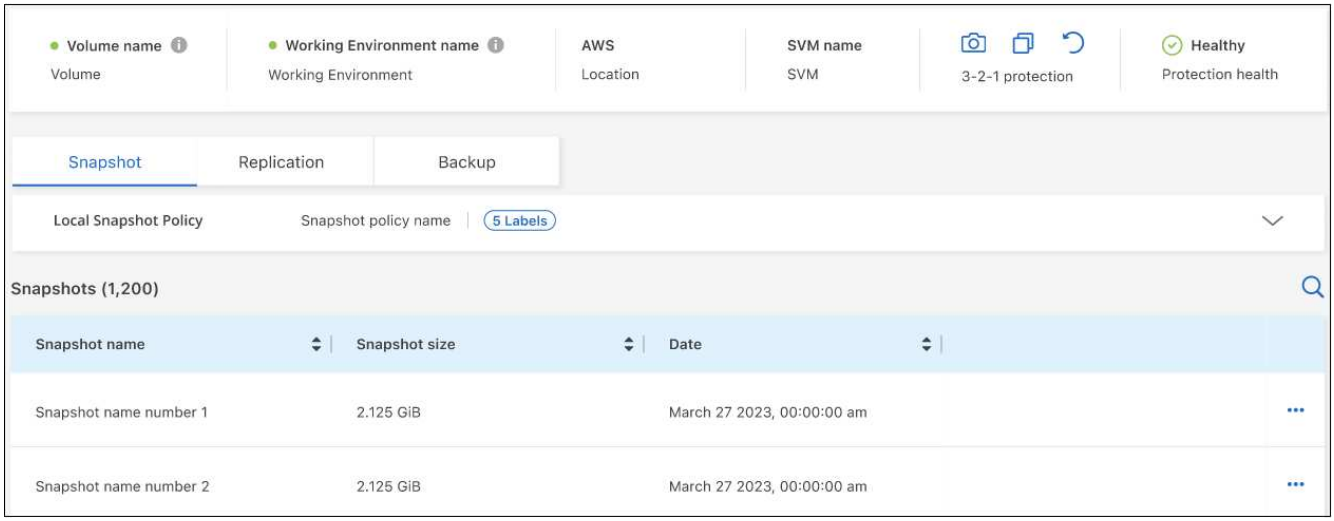
esempio l'ultimo backup eseguito, la policy di backup corrente, le dimensioni del file di backup e altro ancora.

Fasi

1. Dalla scheda **Volumes** (volumi), fare clic su ••• Per il volume di origine e selezionare **Visualizza dettagli volume**.



Per impostazione predefinita, 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

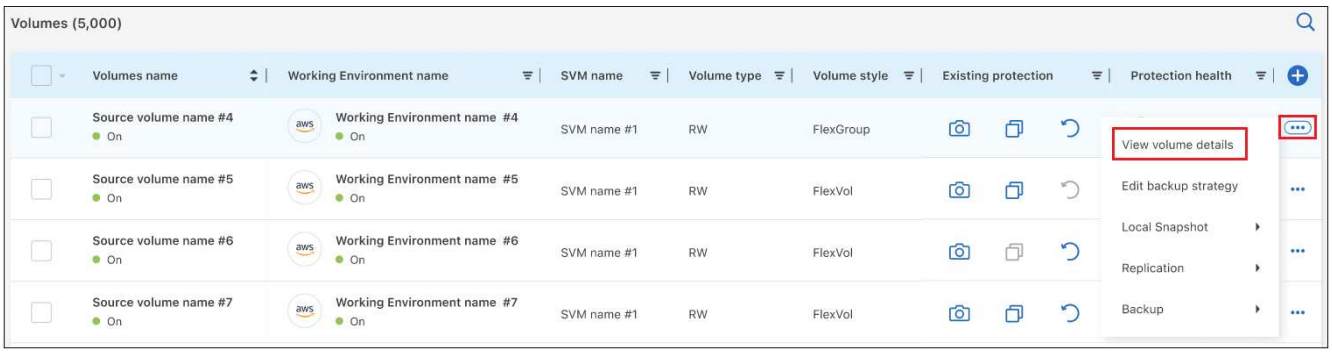
Il software di protezione ransomware di NetApp esegue la scansione dei file di backup per cercare la prova di un attacco ransomware quando viene creato un file di backup su oggetto e quando vengono ripristinati i dati di un file di backup. È inoltre possibile eseguire una scansione di protezione ransomware on-demand in qualsiasi

momento per verificare l'usabilità di uno specifico file di backup nello storage a 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.

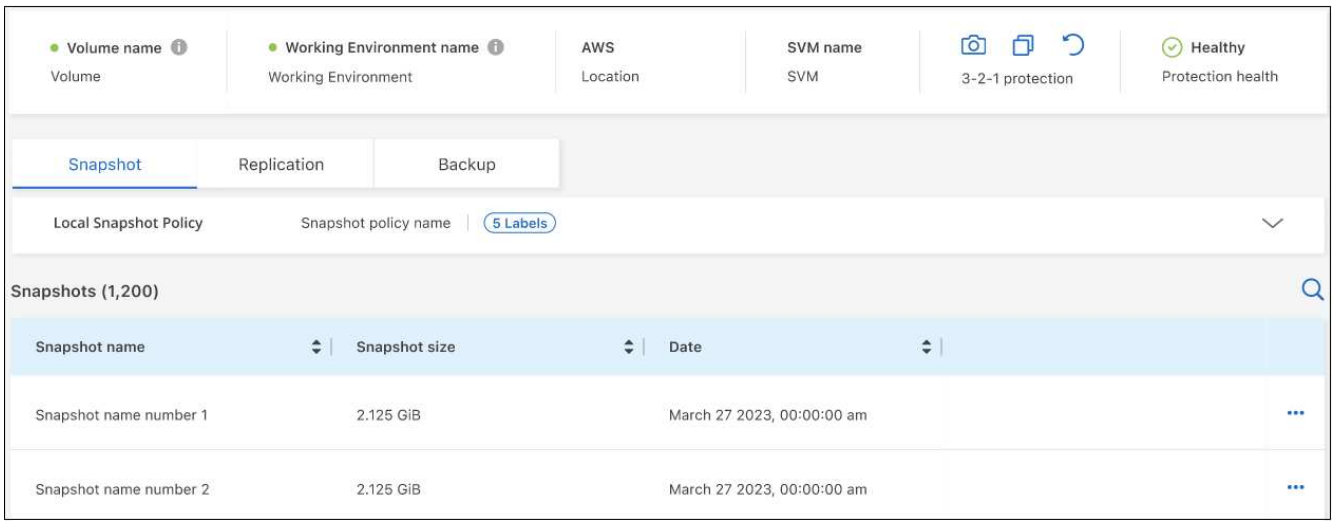
Questa funzione è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.11.1 o superiore e se sono stati attivati *DataLock e protezione ransomware* nel criterio di backup su oggetto.

Fasi

1. Dalla scheda **Volumes** (volumi), fare clic su ••• Per il volume di origine e selezionare **Visualizza dettagli volume**.

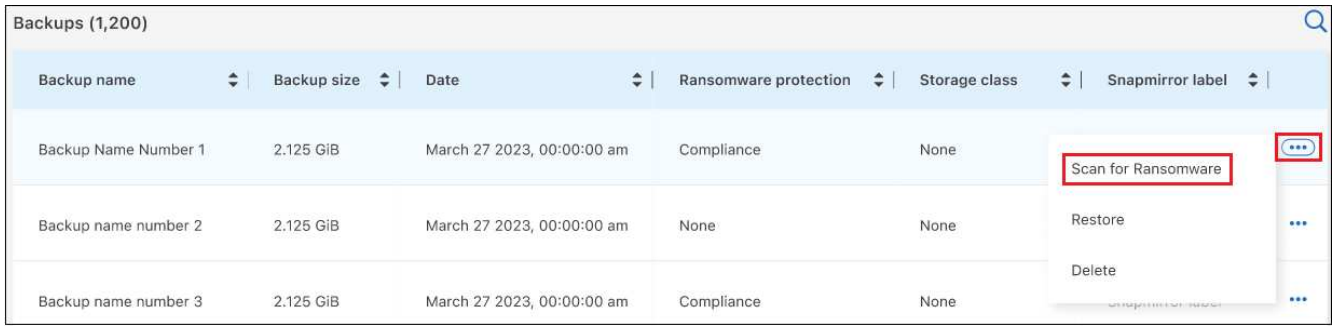


Vengono visualizzati i dettagli del volume.



2. Selezionare **Backup** per visualizzare l'elenco dei file di backup nello storage a oggetti.

3. Fare clic su ••• Per il file di backup del volume che si desidera cercare ransomware e fare clic su **Scan for ransomware**.



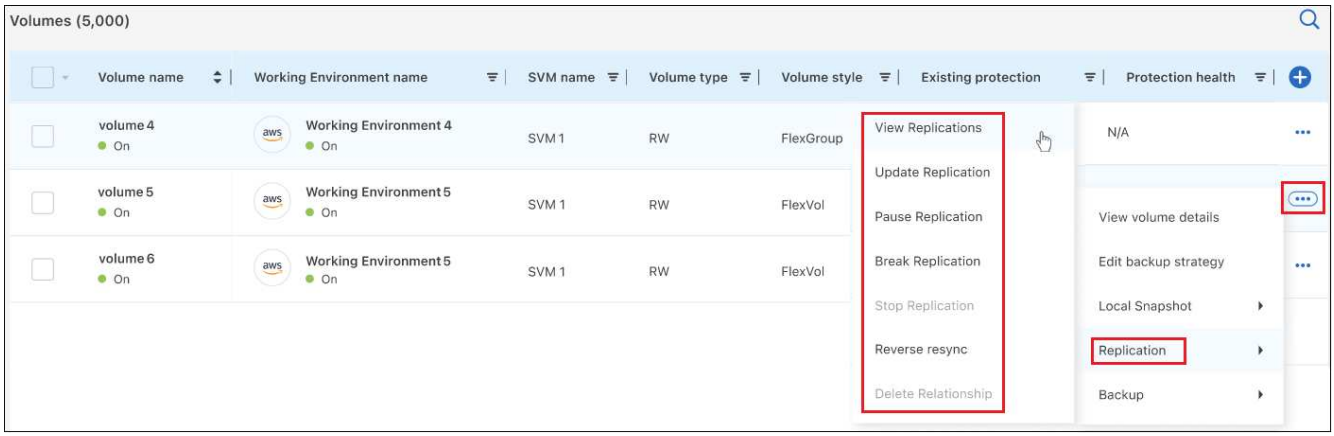
La colonna ransomware Protection (protezione ransomware) indica che la scansione è in corso.

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 **Volumes** (volumi), fare clic su ••• Per il volume di origine e selezionare l'opzione **Replication**. 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.

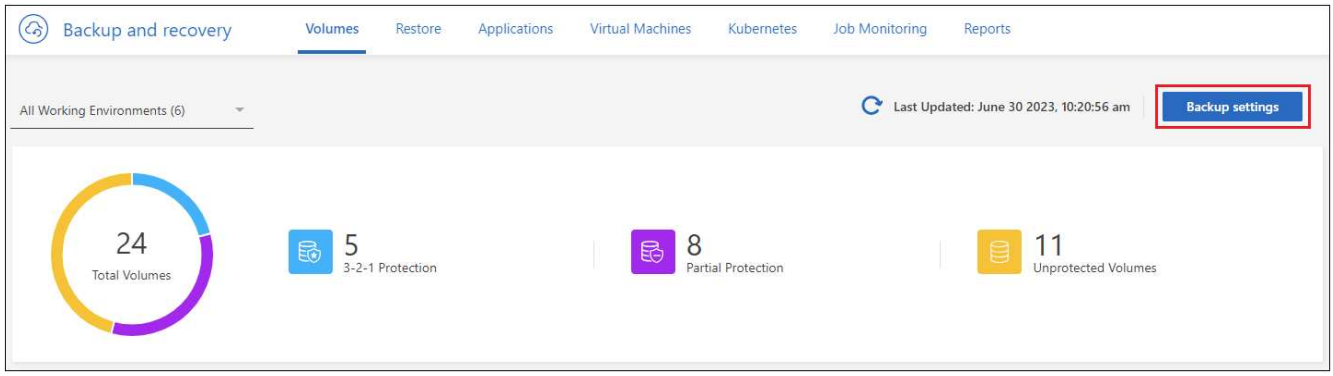
Modifica di una policy di backup nel cloud esistente

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.

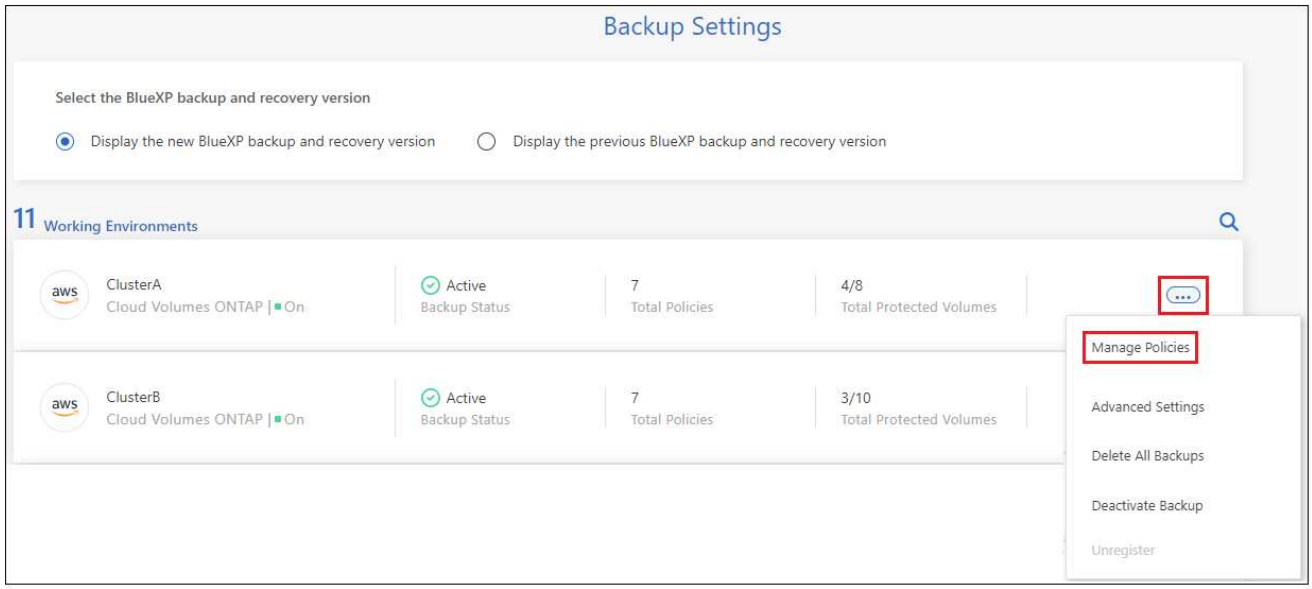
- Se sono stati attivati *DataLock e ransomware Protection* nel criterio iniziale quando si attiva il backup e il ripristino di BlueXP per questo cluster, tutti i criteri modificati devono essere configurati con la stessa impostazione DataLock (Governance o Compliance). Inoltre, se non sono stati attivati *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

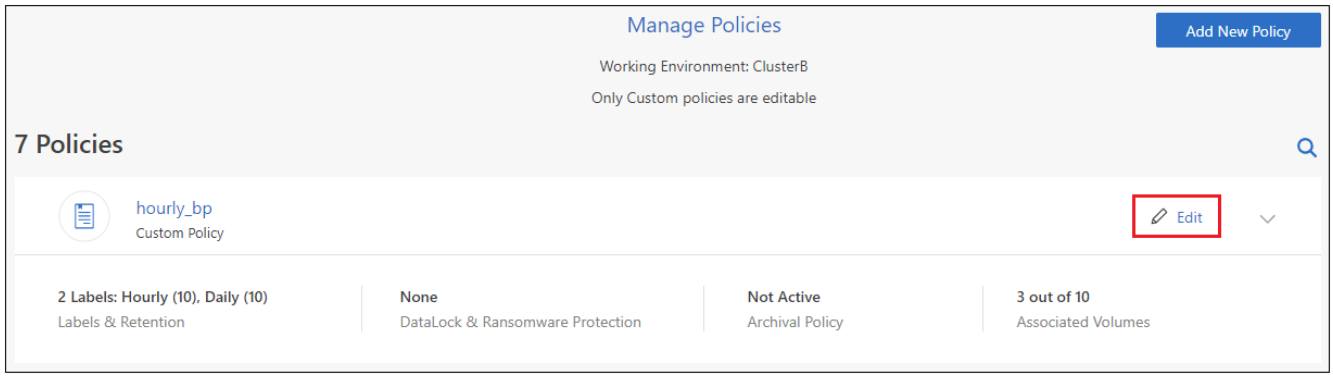
1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



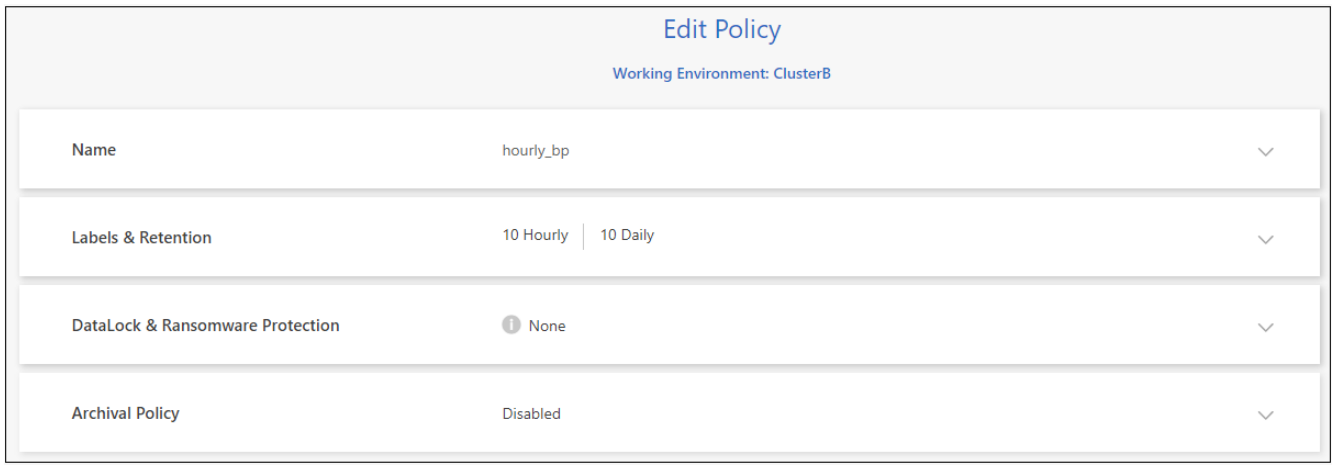
2. Nella pagina *Backup Settings*, fare clic su ••• Per l'ambiente di lavoro in cui si desidera modificare le impostazioni dei criteri e selezionare **Gestisci criteri**.



3. Dalla pagina *Manage Policies*, fare clic su **Edit** per il criterio di backup che si desidera modificare in quell'ambiente di lavoro.



4. Nella pagina *Edit Policy*, fare clic su ⌄ Per espandere la sezione *etichette e conservazione* per modificare la pianificazione e/o la conservazione del backup, quindi fare clic su **Salva**.

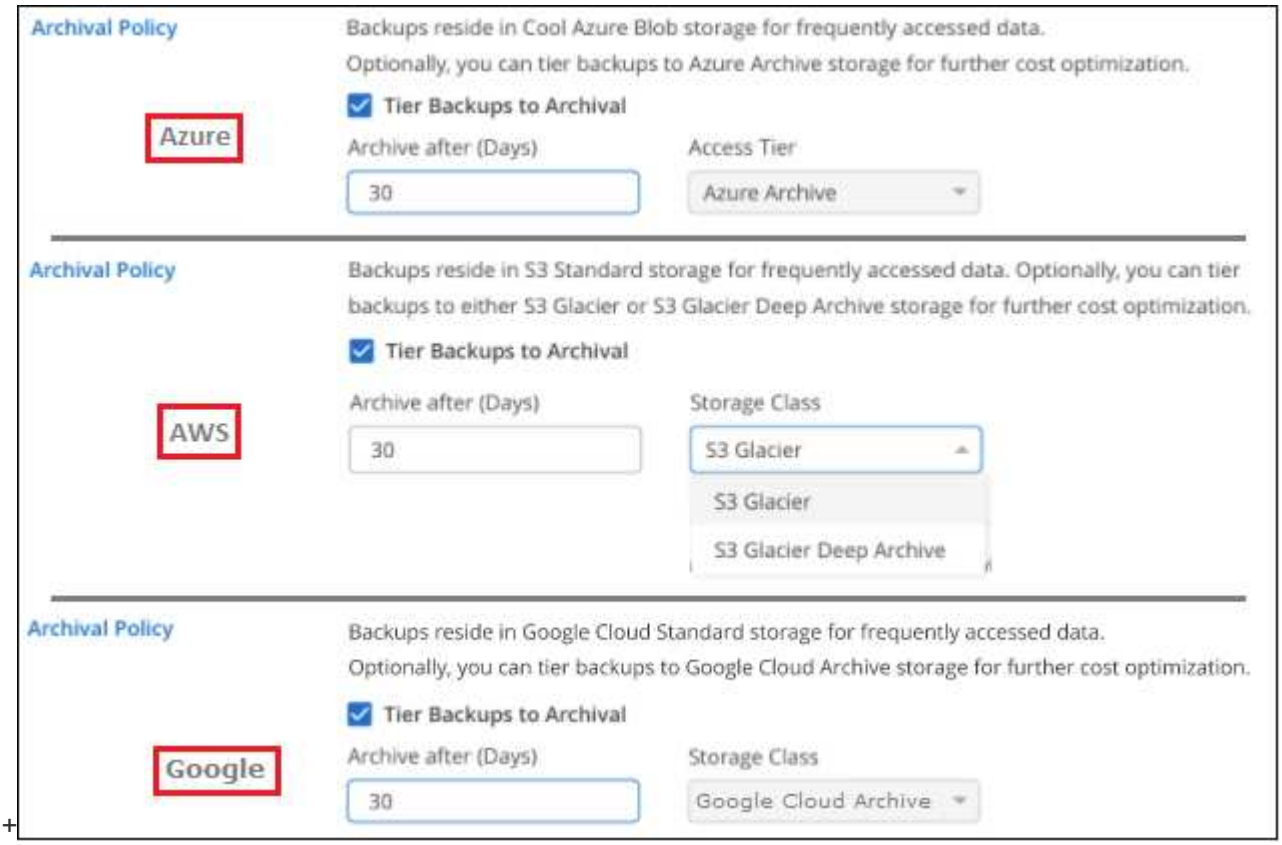


Se nel cluster è in esecuzione ONTAP 9.10.1 o versione successiva, è possibile attivare o disattivare il tiering dei backup nello storage di archiviazione dopo un certo numero di giorni.

"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

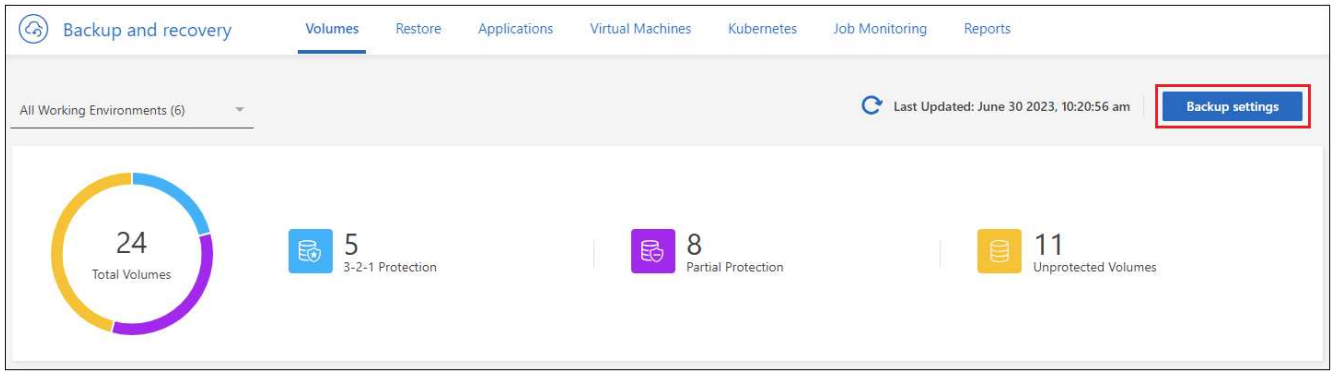
Quando si attiva il backup e il ripristino BlueXP per un ambiente di lavoro, tutti i volumi selezionati inizialmente vengono sottoposti a backup utilizzando il criterio di backup predefinito definito. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi RPO (Recovery 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.

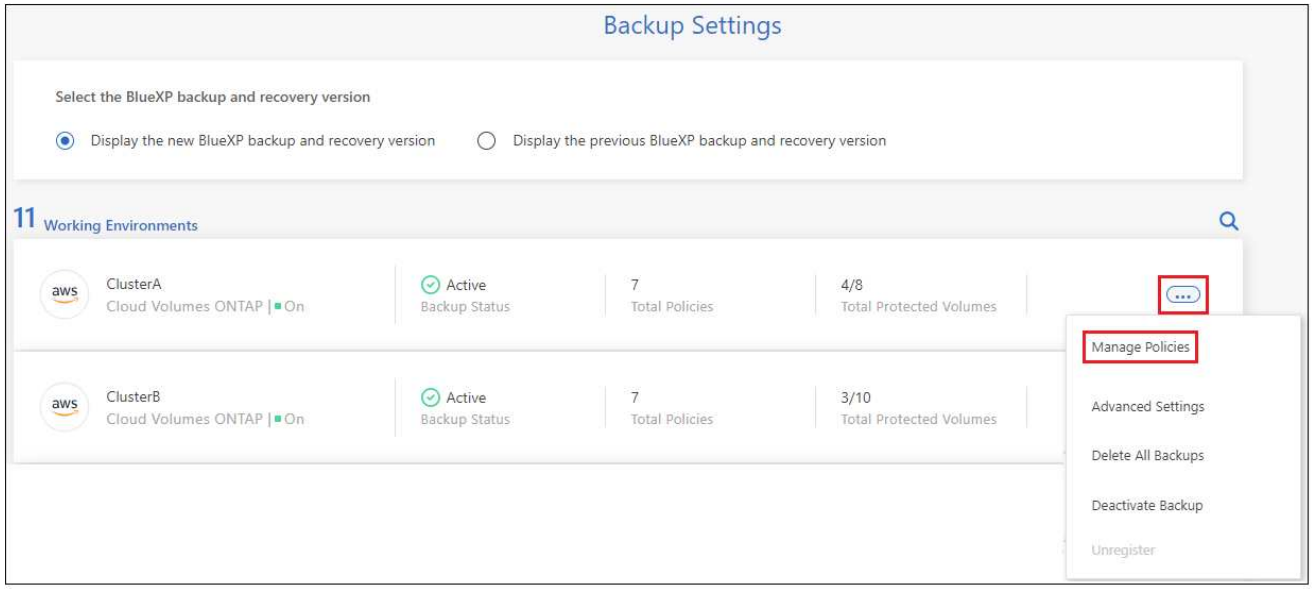
- Se sono stati attivati *DataLock e ransomware Protection* nella policy iniziale quando si attiva il backup e il ripristino di BlueXP per questo cluster, qualsiasi policy aggiuntiva creata deve essere configurata con la stessa impostazione DataLock (Governance o Compliance). Inoltre, se non sono stati 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

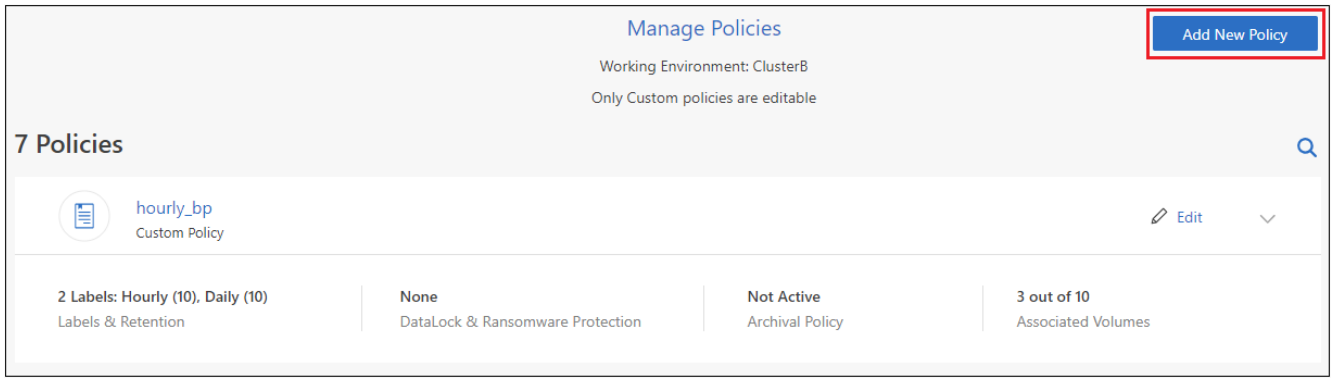
1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



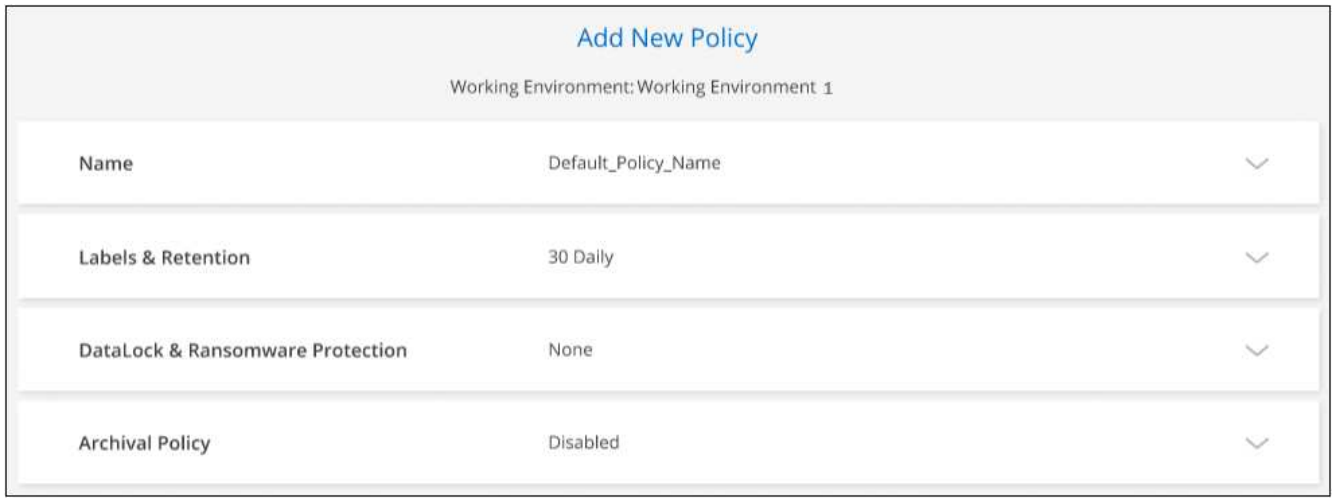
2. Nella pagina *Backup Settings*, fare clic su ••• Per l'ambiente di lavoro in cui si desidera aggiungere il nuovo criterio e selezionare **Gestisci criteri**.



3. Dalla pagina *Gestisci policy*, fare clic su **Aggiungi nuova policy**.



4. Nella pagina *Add New Policy*, fare clic su ⌄ Per espandere la sezione *etichette e conservazione* per definire la pianificazione e la conservazione del backup, quindi fare clic su **Salva**.

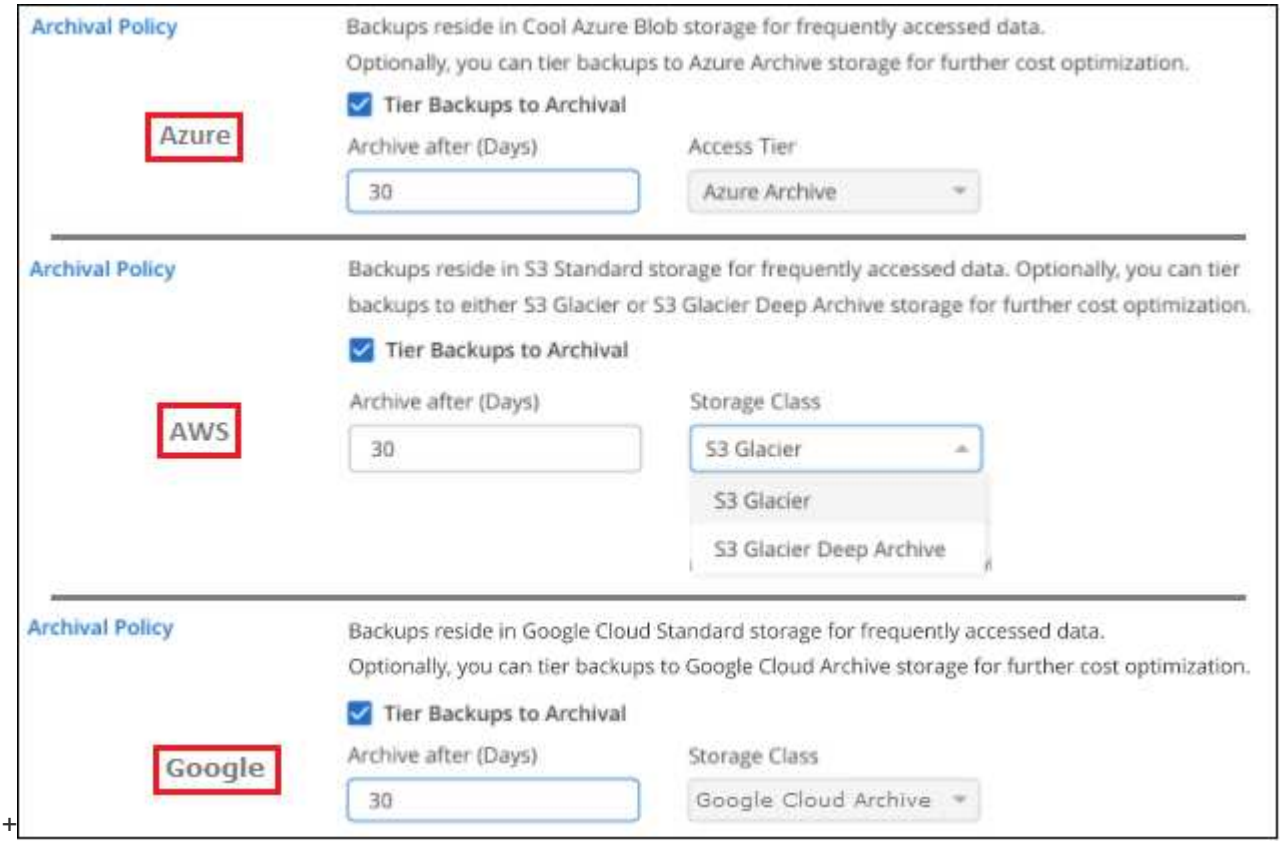


Se nel cluster è in esecuzione ONTAP 9.10.1 o versione successiva, è possibile attivare o disattivare il tiering dei backup nello storage di archiviazione dopo un certo numero di giorni.

"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.

Nota: Non è possibile eliminare i file di backup bloccati utilizzando DataLock e la protezione ransomware. L'opzione "Delete" (Elimina) non sarà disponibile dall'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

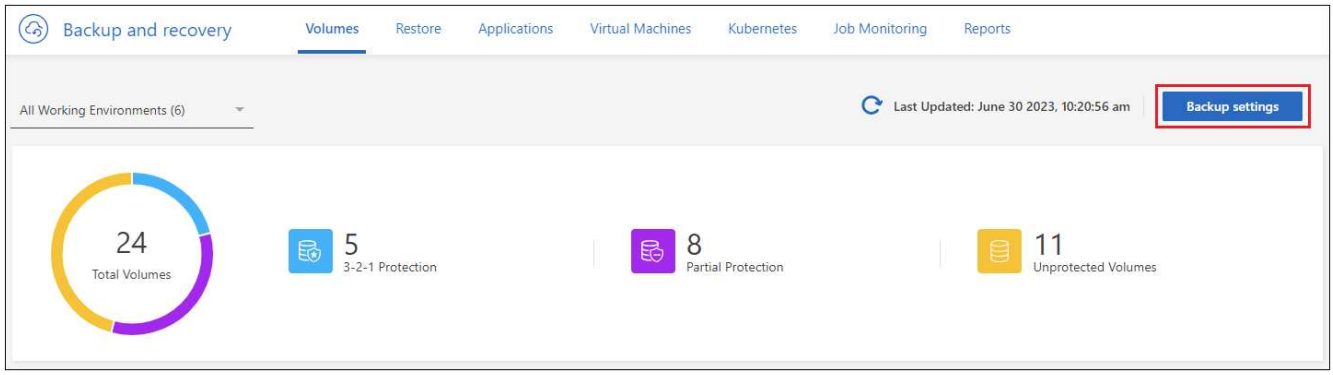
L'eliminazione di tutti i backup sullo storage a oggetti per un ambiente di lavoro non disattiva i backup futuri dei volumi in questo ambiente di lavoro. Se si desidera interrompere la creazione di backup di tutti i volumi in un ambiente di lavoro, è possibile disattivare i backup come descritto qui.

Si noti che questa azione non influisce sulle copie Snapshot o sui volumi replicati: Questi tipi di file di backup

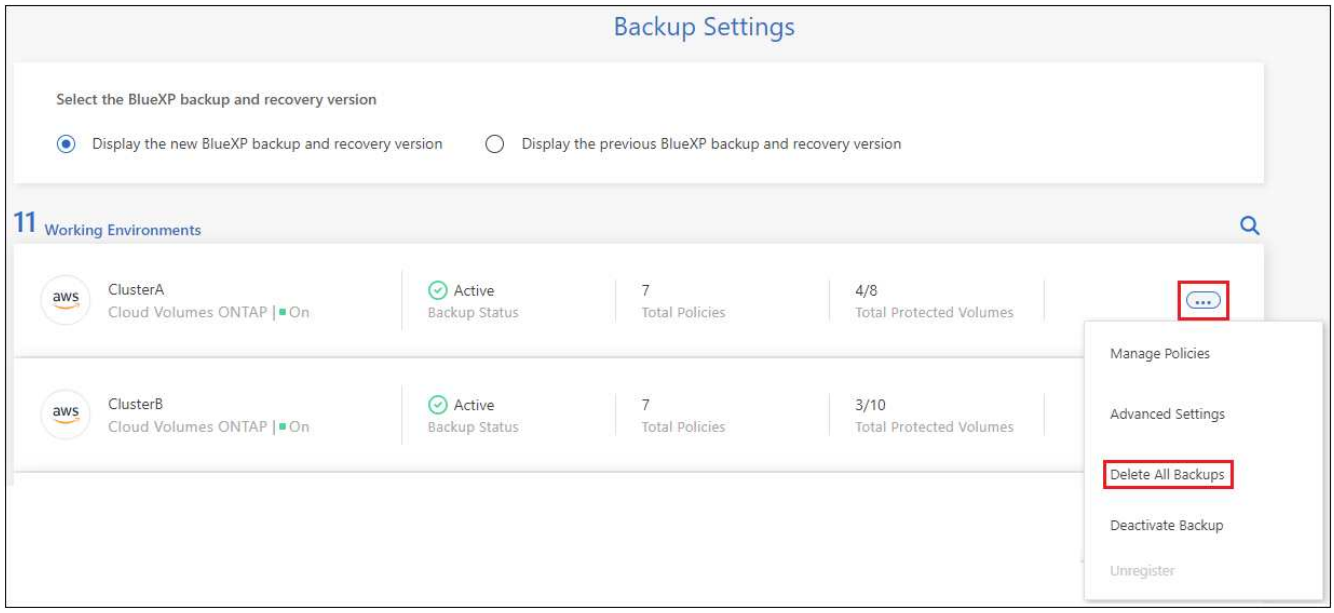
non vengono eliminati.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Fare clic su ••• 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 e fare clic su **Delete** (Elimina).

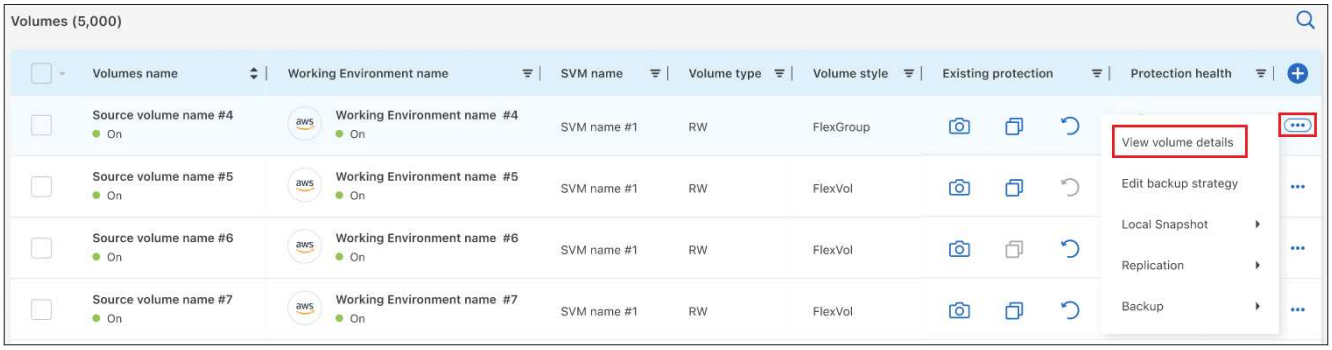
Eliminare un singolo file di backup per un volume

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.

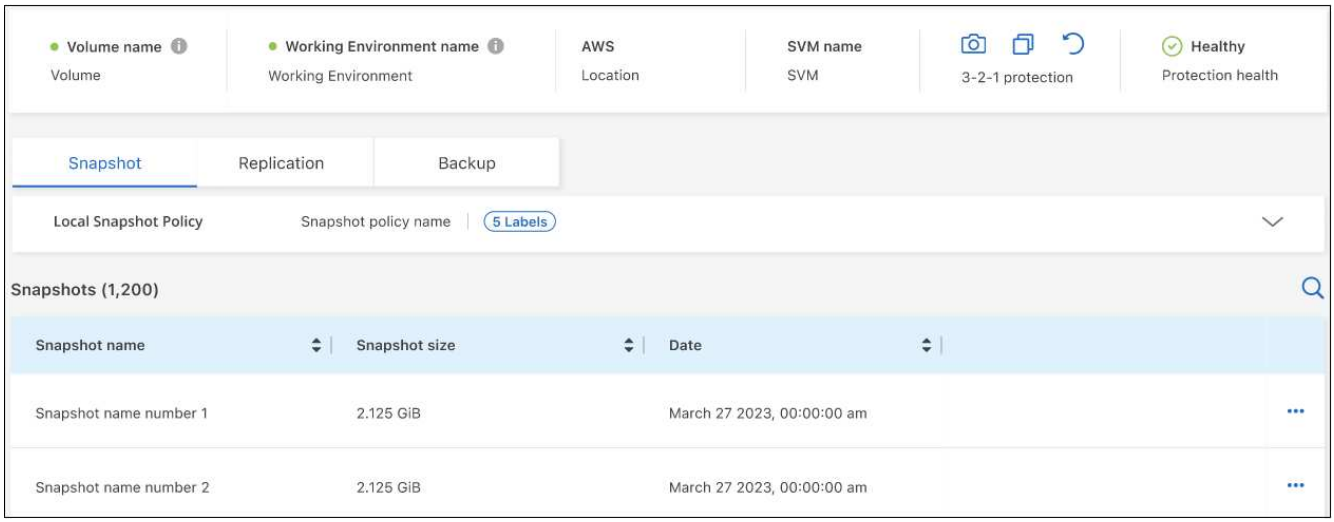
Non è possibile eliminare i volumi replicati (volumi di protezione dei dati).

Fasi

1. Dalla scheda **Volumes** (volumi), fare clic su ••• Per il volume di origine e selezionare **Visualizza dettagli volume**.

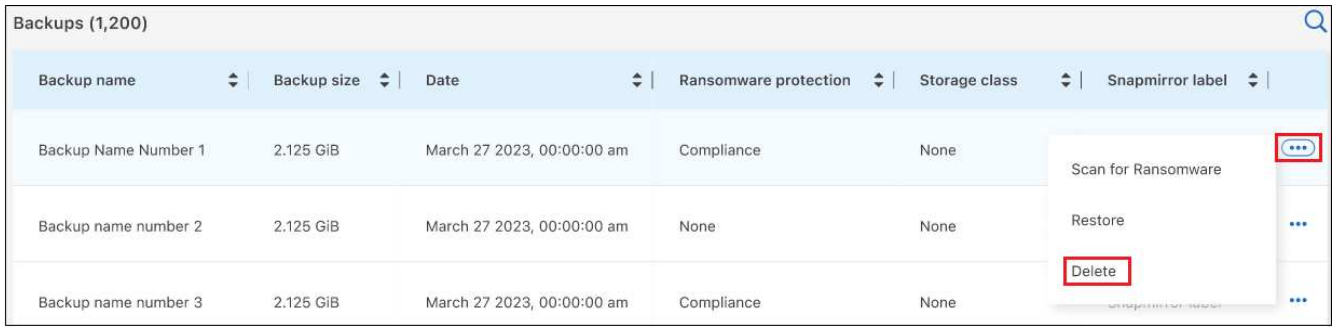


Vengono visualizzati i dettagli del volume ed è possibile selezionare **Snapshot**, **Replication** o **Backup** per visualizzare l'elenco di tutti i file di backup del volume. Per impostazione predefinita, vengono visualizzate le copie Snapshot disponibili.



2. Selezionare **Snapshot** o **Backup** per visualizzare il tipo di file di backup che si desidera eliminare.

3. Fare clic su ••• Per il file di backup del volume che si desidera eliminare e fare clic su **Delete** (Elimina). La schermata riportata di seguito si trova in un file di backup nello storage a oggetti.



4. Nella finestra di dialogo di conferma, fare clic su **Delete** (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.

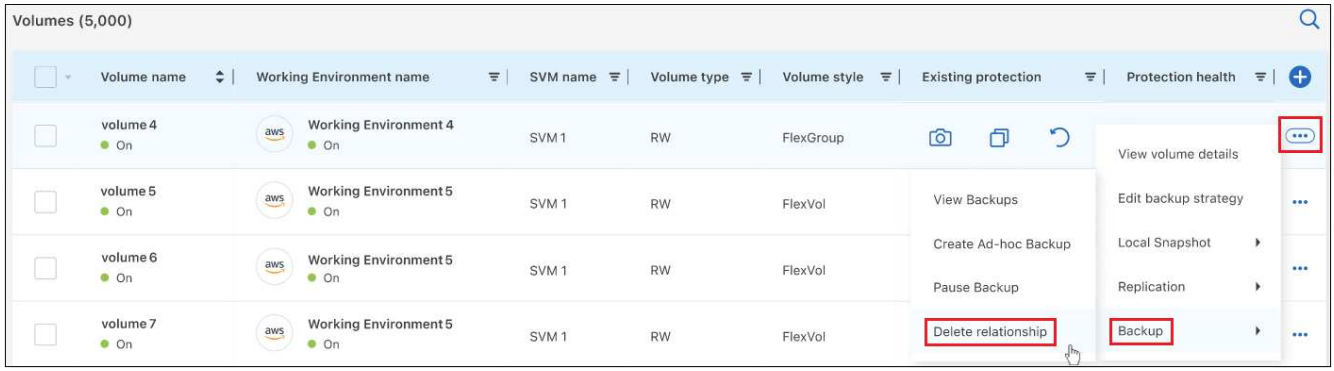
Questa funzione è disponibile solo se nel sistema è in esecuzione ONTAP 9.12.1 o versione successiva.

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. Tuttavia, è possibile "eliminare tutti i backup del volume" se si desidera rimuovere tutti i file di backup.

Fasi

1. Dalla scheda **Volumes** (volumi), fare clic su ••• Per il volume di origine e selezionare **Backup** > **Elimina relazione**.



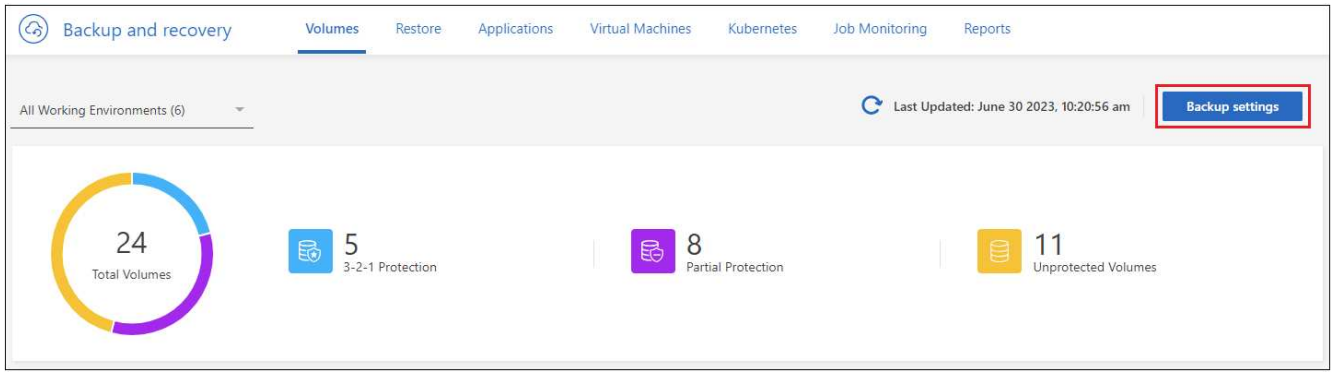
Disattivare il backup e ripristino BlueXP per un ambiente di lavoro

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.

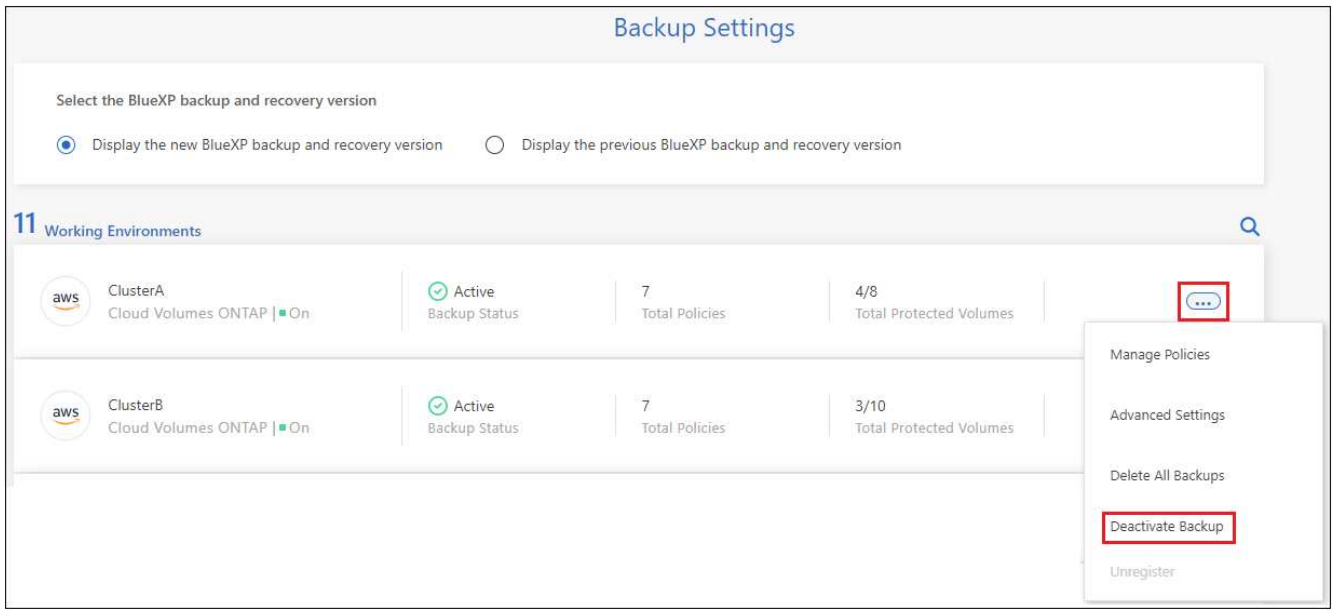
Tieni presente che il tuo cloud provider continuerà a addebitare i costi dello storage a oggetti per la capacità utilizzata dai backup, a meno che tu non lo utilizzi eliminare i backup.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro in cui si desidera disattivare i backup e selezionare **Disattiva backup**.



3. Nella finestra di dialogo di conferma, fare clic su **Disattiva**.

> Quando il backup è disattivato, viene visualizzato il pulsante **Activate Backup** (attiva backup) per quell'ambiente di lavoro. Fare clic su questo pulsante per riattivare la funzionalità di backup per l'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.

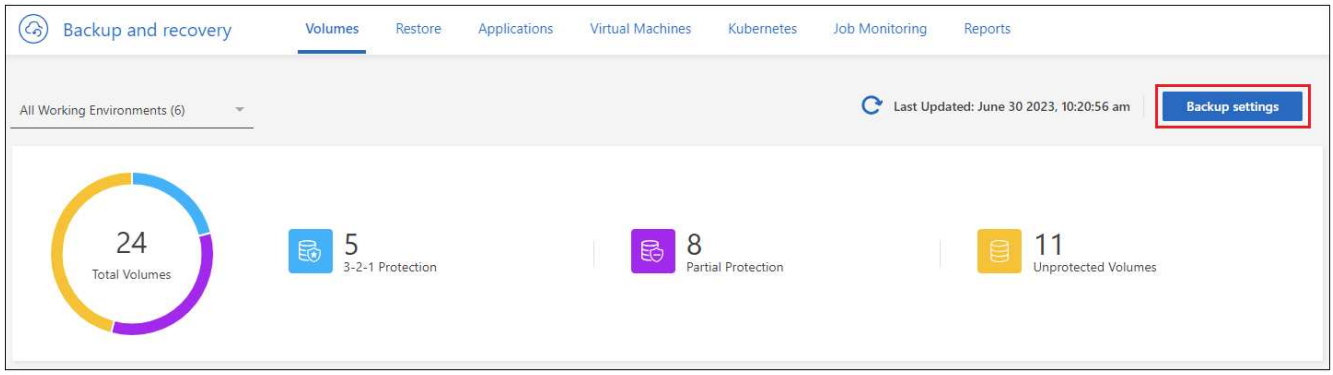
Prima di annullare la registrazione di backup e ripristino BlueXP, è necessario eseguire le seguenti operazioni, nell'ordine indicato:

- Disattivare il backup e ripristino BlueXP per l'ambiente di lavoro
- Eliminare tutti i backup per l'ambiente di lavoro

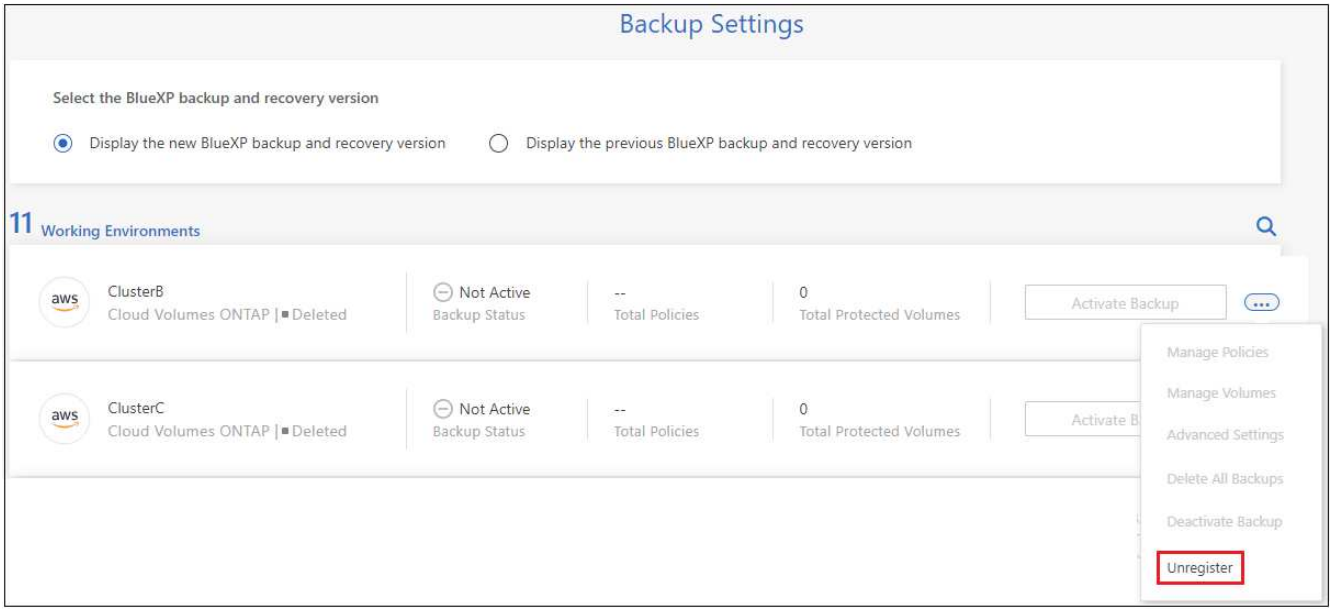
L'opzione di annullamento della registrazione non è disponibile fino al completamento di queste due azioni.

Fasi

1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



2. Dalla *pagina Backup Settings*, fare clic su ••• 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, fare clic su **Annulla registrazione**.

Ripristinare i dati ONTAP dai file di backup

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. È possibile ripristinare un intero volume ONTAP da un file di backup oppure, se è necessario ripristinare solo alcuni file, è possibile ripristinare una cartella o singoli file.

- 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:

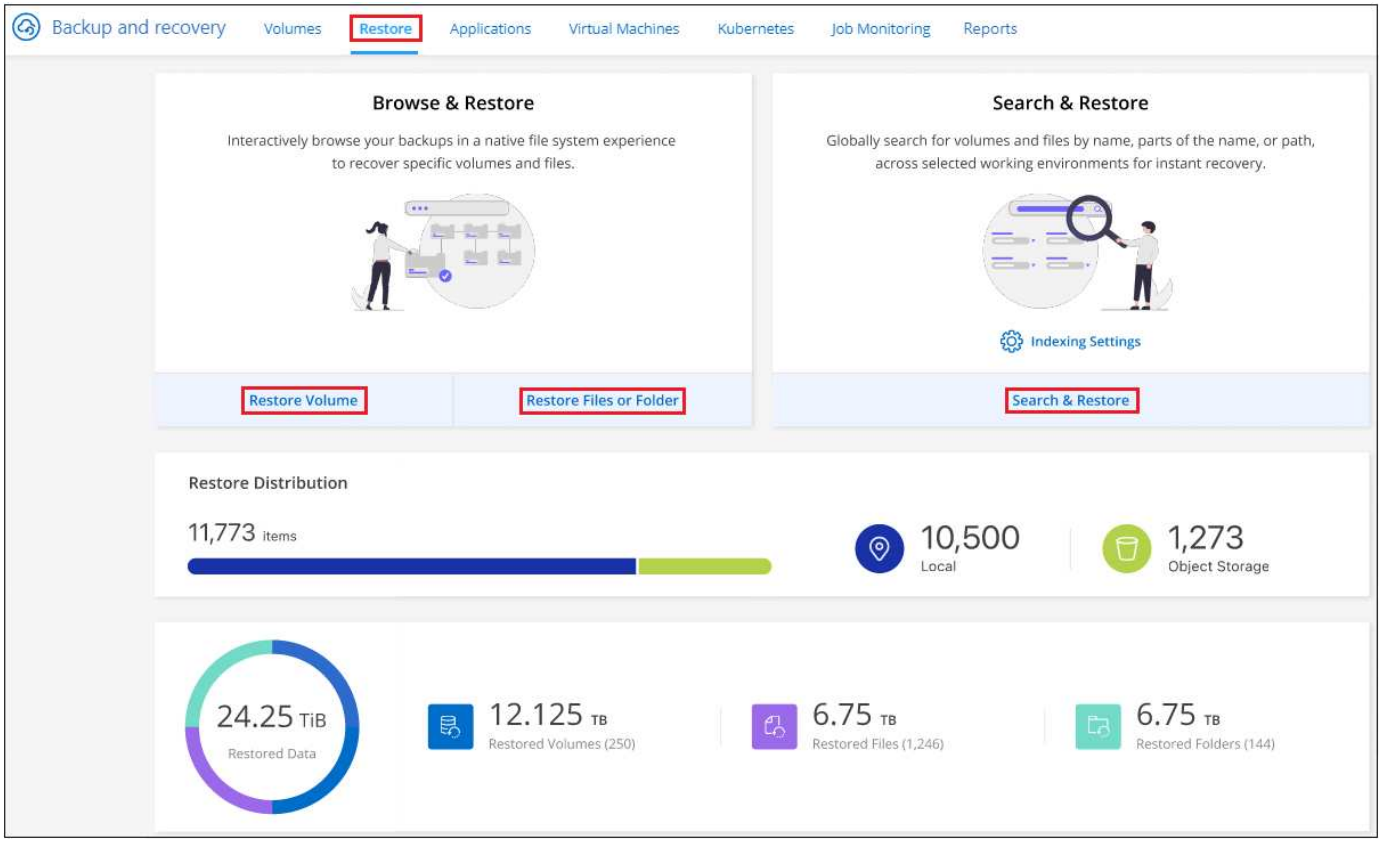
- File di backup → volume ripristinato
- Volume replicato → volume ripristinato
- Copia Snapshot → Volume ripristinato

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. È anche possibile fare clic su > **Visualizza 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 si può vedere, la dashboard di ripristino offre due diversi modi per ripristinare i dati dai file di backup: **Browse & Restore** e **Search & Restore**.

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 tra le funzionalità dei 2 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.

Sfoglia e ripristina	Ricerca e ripristino
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:

- <<Restoring volumes using Browse & Restore,Ripristinare i volumi utilizzando Sfoglia Ripristina
- <<Restoring folders and files using Browse & Restore,Ripristinare cartelle e file utilizzando Sfoglia Ripristina
- <<Restoring 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
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.

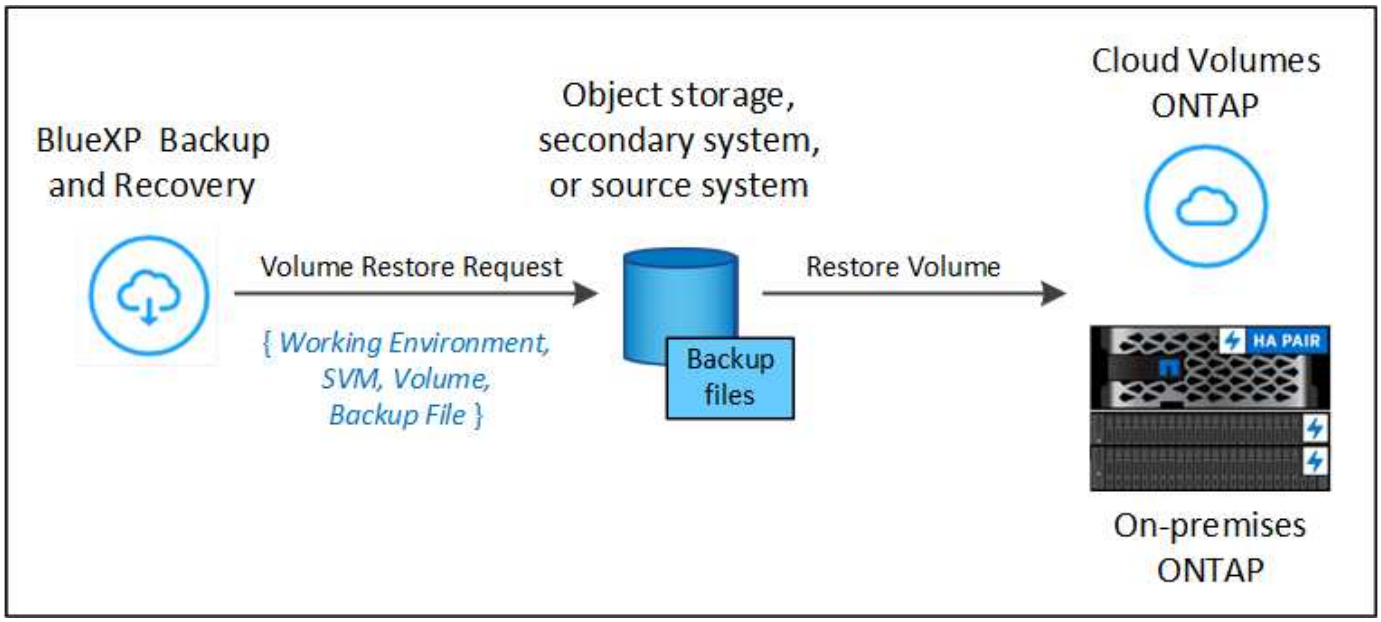
Ripristinare i volumi utilizzando Sfoglia & Ripristina

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.

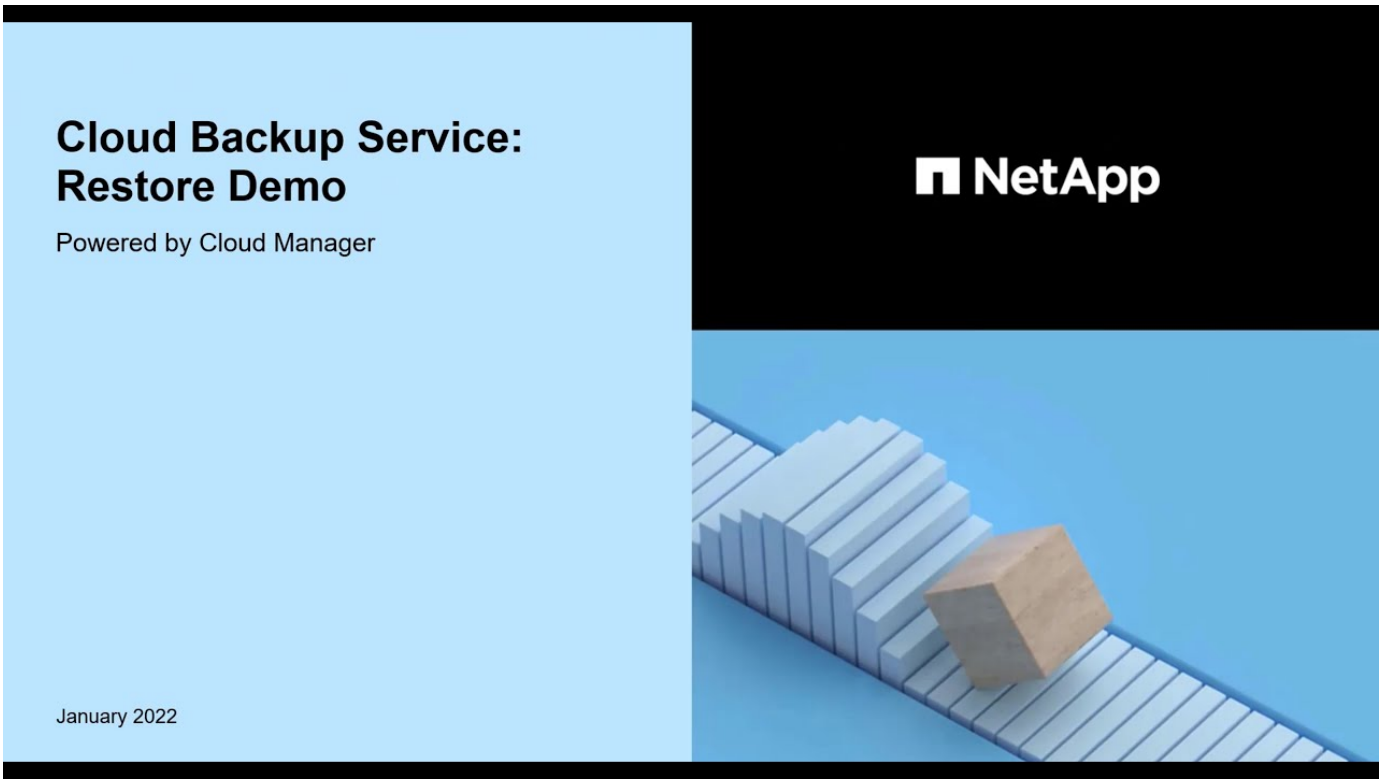
Quando si esegue il ripristino da un volume replicato, è possibile ripristinare il volume nell'ambiente di lavoro originale o in un sistema Cloud Volumes ONTAP o ONTAP on-premise.



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.

Il seguente video mostra una breve panoramica del ripristino di un volume:

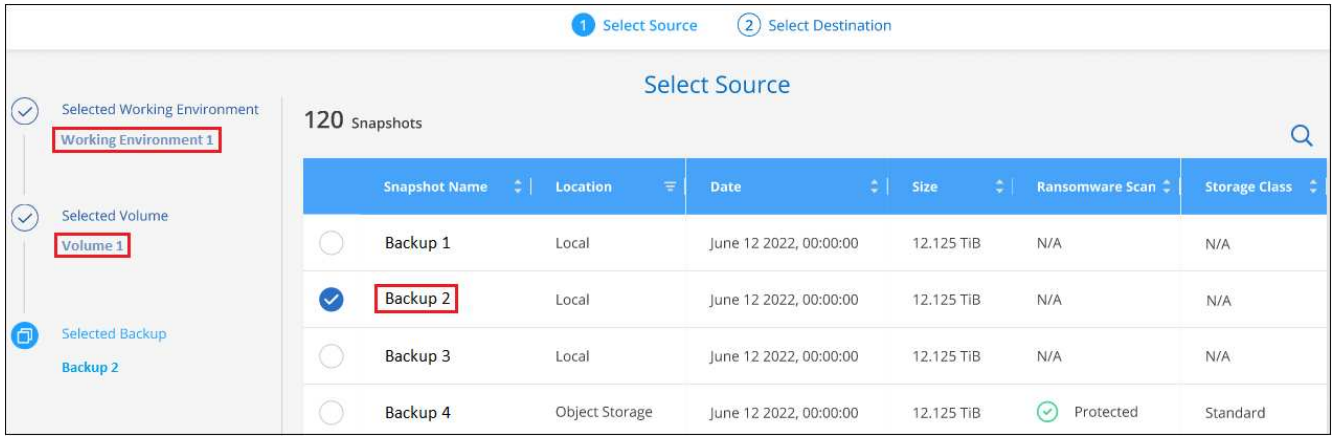


Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Fare clic sulla scheda **Restore** per visualizzare la dashboard di ripristino.
3. Nella sezione *Browse & Restore*, fare clic su **Restore Volume** (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.

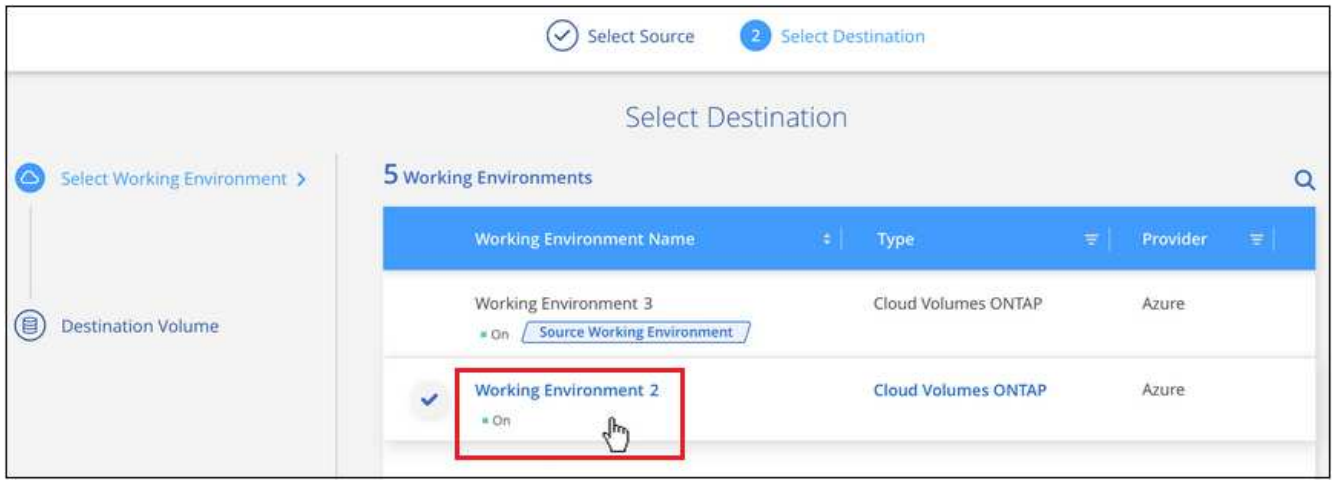
   La colonna **percorso** indica se il file di backup (Snapshot) è **locale** (una copia Snapshot sul sistema di origine), **secondario** (un volume replicato su un sistema ONTAP secondario) o **archiviazione oggetto** (un file di backup nello storage a oggetti). Scegliere il file che si desidera ripristinare.



5. Fare clic su **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).

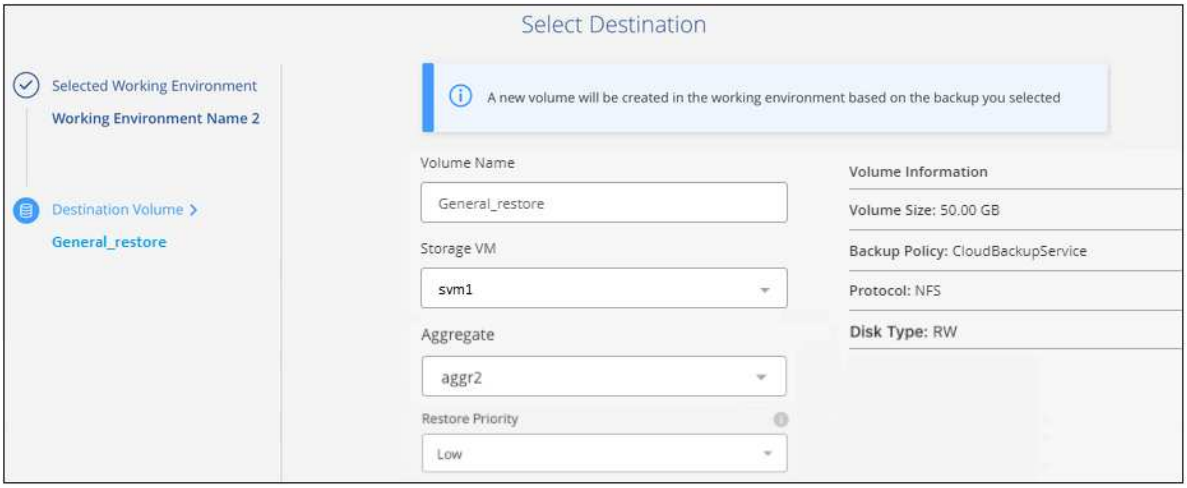
6. Nella pagina *Select Destination*, selezionare **Working Environment** (ambiente di lavoro) in cui si desidera ripristinare il volume.



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*.

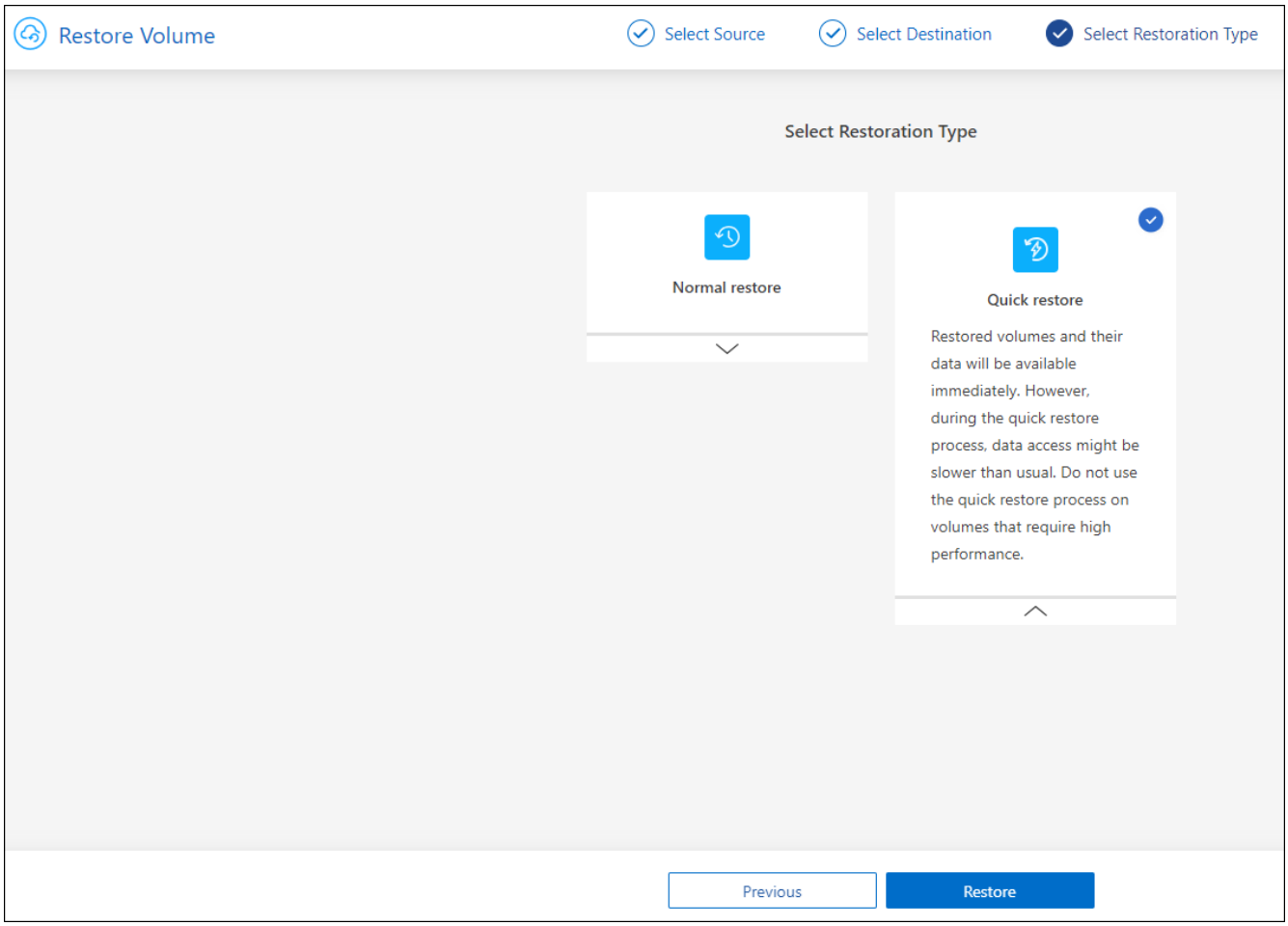
Se si sta ripristinando il volume da un file di backup che risiede in un Tier di storage di archiviazione (disponibile a partire da ONTAP 9.10.1), è possibile selezionare la priorità di ripristino.

"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. Fare clic su **Avanti** per scegliere se eseguire un ripristino normale o un processo di 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. Fare clic su **Restore** (Ripristina) per tornare alla dashboard di ripristino, in modo da 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. Fare clic sulla scheda **Job Monitoring** per visualizzare l'avanzamento del ripristino.

Ripristinare cartelle e file utilizzando Sfoglia & Ripristina

Se è necessario ripristinare solo alcuni file da un backup di un volume ONTAP, è possibile 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 che risiede 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.

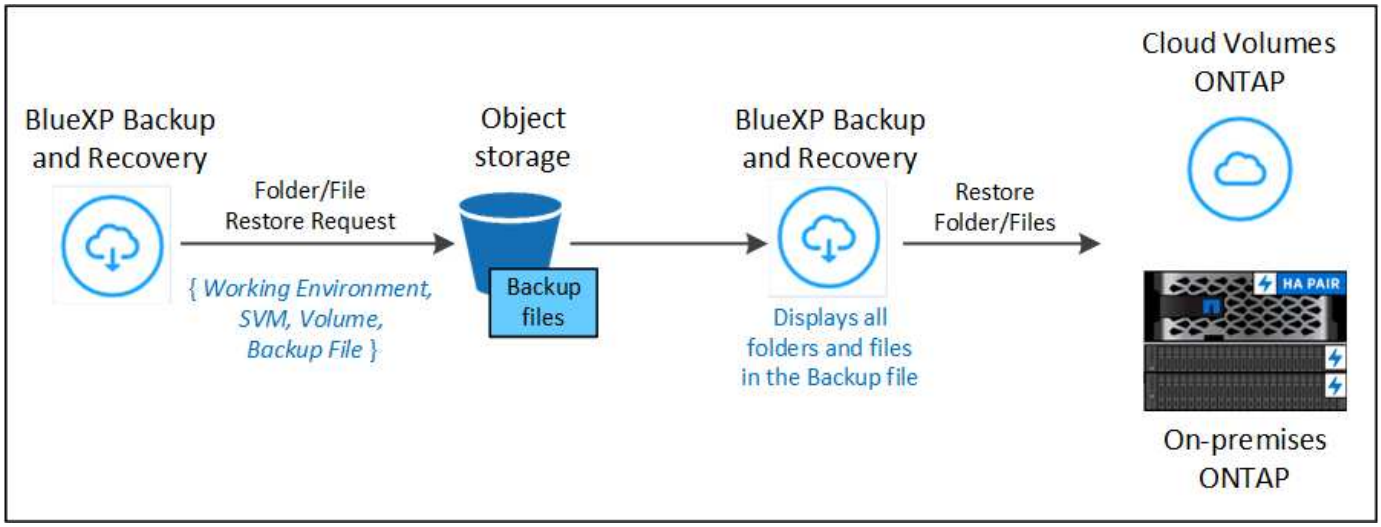
Prerequisiti

- 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.

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.

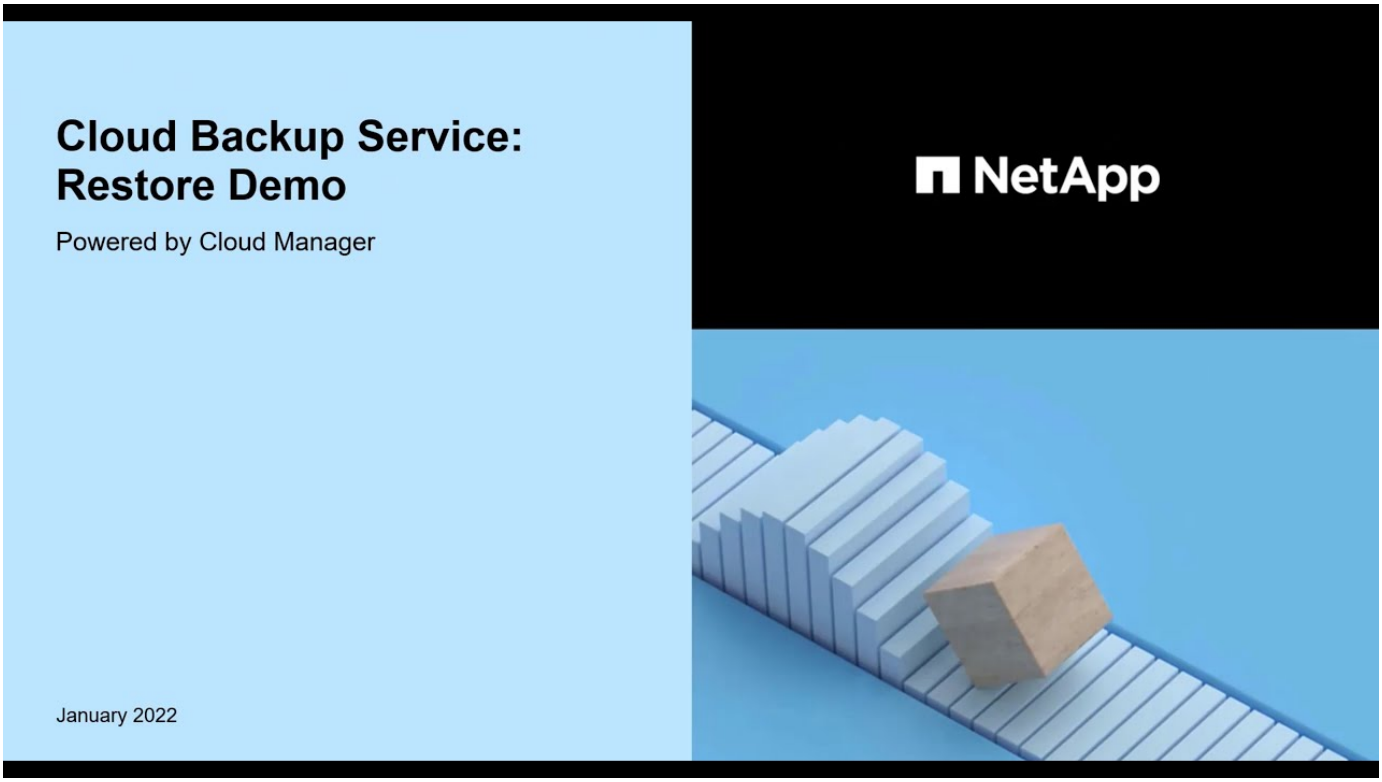


Come si può vedere, è necessario conoscere il nome dell'ambiente di lavoro, il nome del volume, la data del file di backup e il nome della cartella/file per eseguire il ripristino di una cartella o di un file.

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.

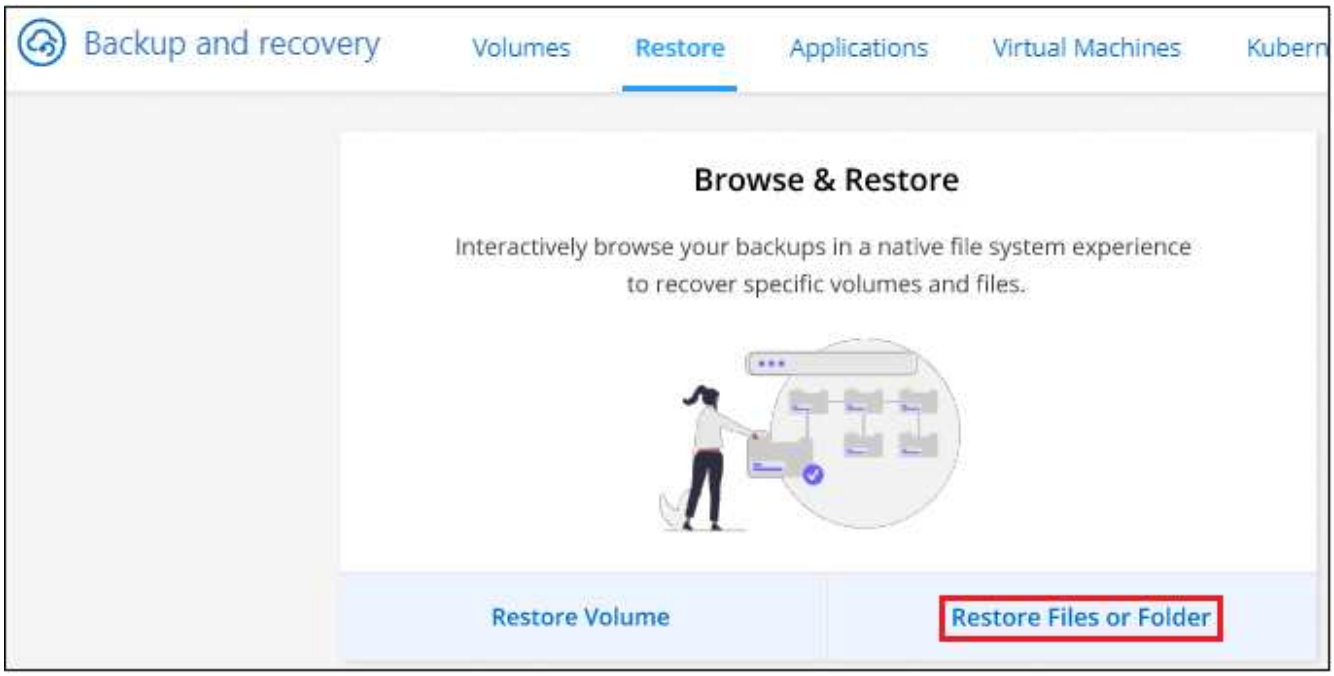
Il video seguente mostra una rapida procedura dettagliata per il ripristino di un singolo file:



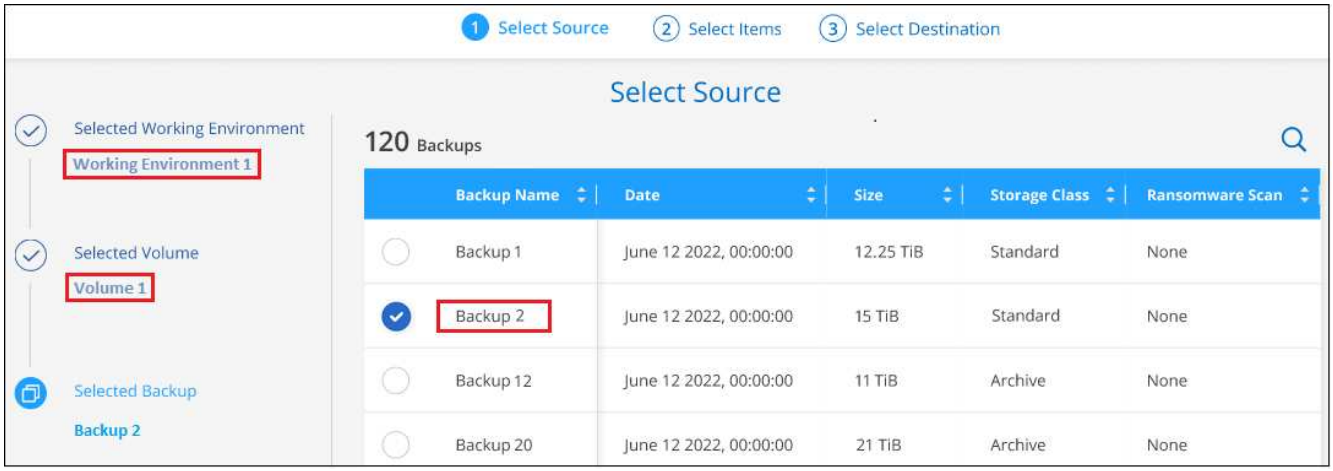
Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.

2. Fare clic sulla scheda **Restore** per visualizzare la dashboard di ripristino.
3. Nella sezione *Browse & Restore*, fare clic su **Restore Files or Folder** (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. Fare clic su **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.

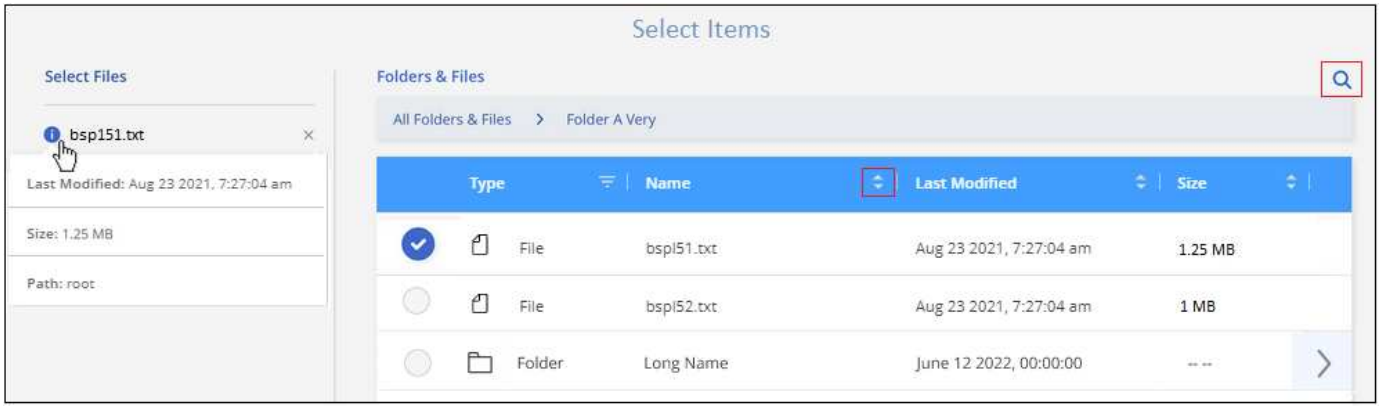
"Scopri di più sul ripristino dallo storage di archiviazione AWS".

"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).

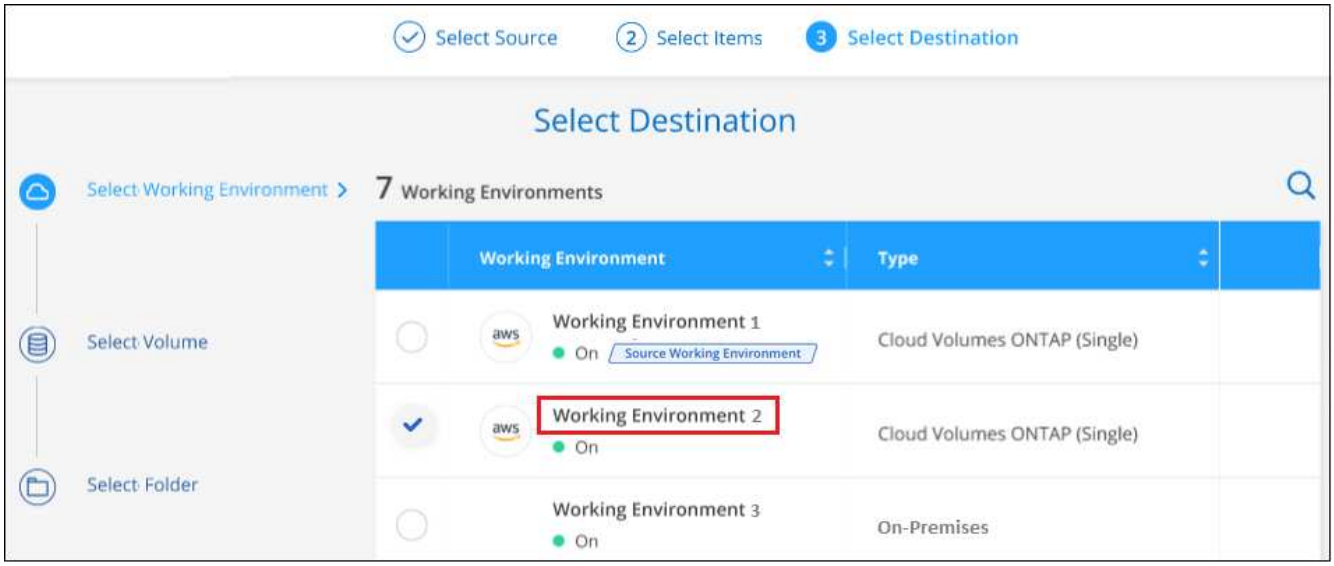
+



1. Nella pagina *Select ITEMS*, selezionare la cartella o i file che si desidera ripristinare e fare clic su **Continue** (continua). Per assistenza nella ricerca dell'elemento:
   - È possibile fare clic sul nome della cartella o del file, se visualizzato.
   - È possibile fare clic sull'icona di ricerca e immettere il nome della cartella o del file per accedere direttamente all'elemento.
   - È possibile scorrere i livelli delle cartelle in basso utilizzando › alla fine della riga per trovare file specifici.

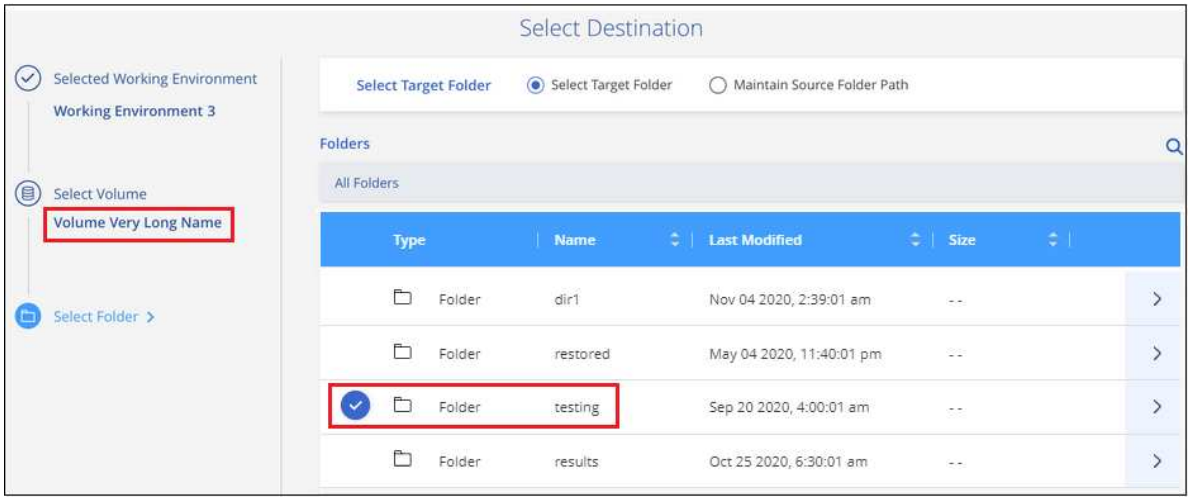
     Quando si selezionano i file, questi vengono aggiunti alla parte sinistra della pagina in modo da visualizzare i file già selezionati. Se necessario, è possibile rimuovere un file da questo elenco facendo clic sulla * x* accanto al nome del file.

2. 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 su > alla fine della riga per eseguire il drill-down nelle 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. Fare clic su **Restore** (Ripristina) per tornare alla dashboard di ripristino, in modo da esaminare l'avanzamento dell'operazione di ripristino. È inoltre possibile fare clic sulla scheda **Job Monitoring** per visualizzare l'avanzamento del ripristino.

Ripristino dei dati ONTAP mediante 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 analizza tutte le copie Snapshot locali esistenti per i volumi ONTAP, tutti i volumi replicati sui sistemi di storage secondari e tutti i file di backup presenti nello storage a 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.

Il video seguente mostra una rapida procedura dettagliata per il ripristino di un singolo file:

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[]
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 è stato configurato un server proxy HTTP per il connettore, non è possibile utilizzare la funzionalità Search & Replace.
- 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".

Nota: Se si utilizzava già il backup e ripristino BlueXP con un connettore configurato in passato, è necessario aggiungere ora 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.
  - 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.

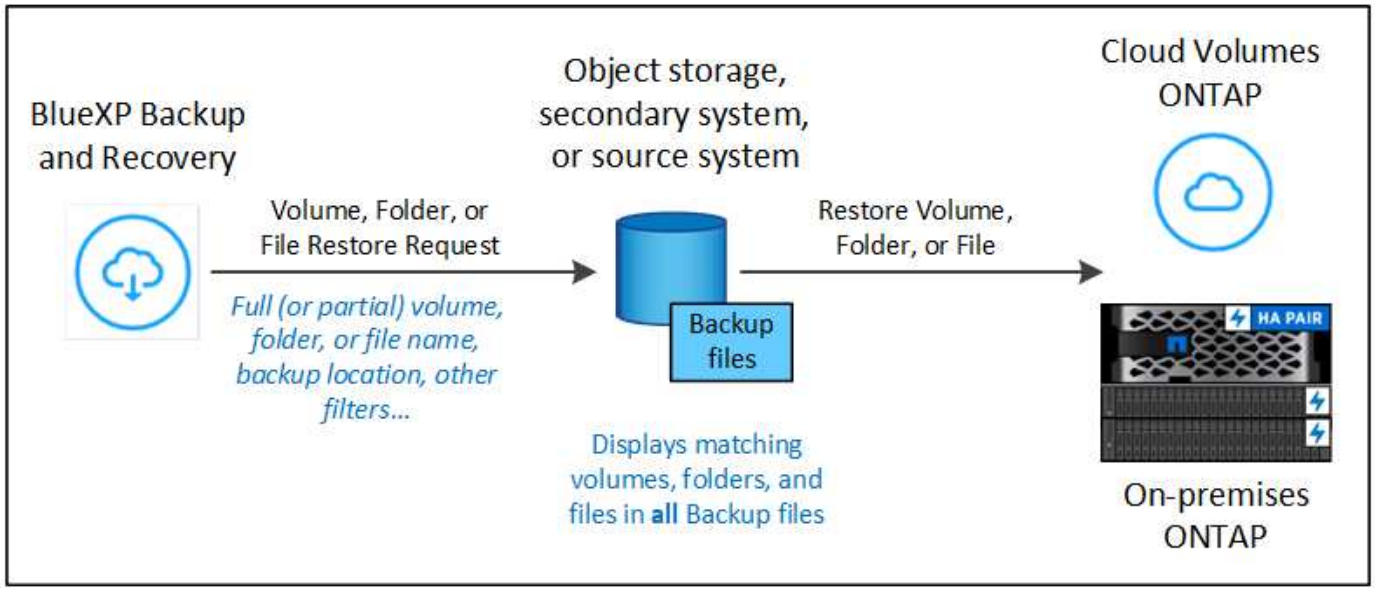
Processo di ricerca e ripristino

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. Se si desidera ripristinare uno o più file da un backup di un volume, in *Search & Restore*, fare clic su **Search & Restore** (Ricerca e ripristino).
3. Immettere i criteri di ricerca per un volume, una cartella o un file in base al nome del volume parziale o completo, al nome del file completo o parziale, alla posizione di backup, all'intervallo di dimensioni, all'intervallo di date di creazione, ad altri filtri di ricerca, E fare clic su **Cerca**.

   La pagina risultati ricerca visualizza tutte le posizioni in cui è presente un file o un volume corrispondente ai criteri di ricerca.

4. Fare clic su **View All backups** (Visualizza tutti i backup) per la posizione che si desidera utilizzare per ripristinare il volume o il file, quindi fare clic su **Restore** (Ripristina) nel 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 fare clic su **Restore** (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.

Quando si attiva questa funzionalità, il backup e ripristino di BlueXP attiva SnapDiff v3 sulla SVM per i volumi ed esegue le seguenti operazioni:

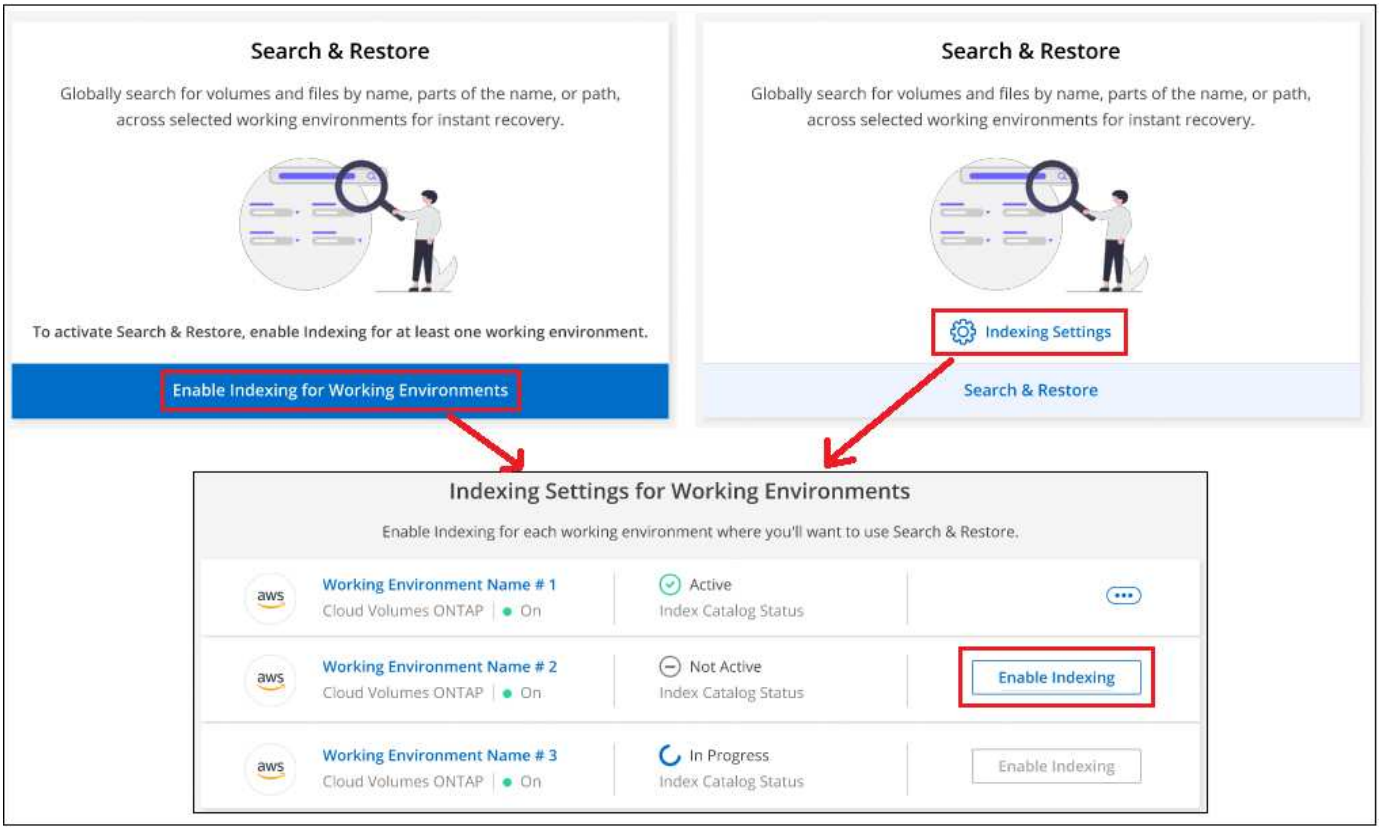
- Per i backup memorizzati in AWS, fornisce un nuovo bucket S3 e il "Servizio di query interattiva Amazon Athena" e. "Servizio di integrazione dei dati senza server AWS Glue".
- Per i backup memorizzati in Azure, il sistema fornisce un'area di lavoro di Azure Synapse e un file system di Data Lake come 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.

Per attivare l'indicizzazione per un ambiente di lavoro:

- Se non sono stati indicizzati ambienti di lavoro, nella dashboard di ripristino in *Search & Restore*, fare clic su **Enable Indexing for Working Environments** (attiva indicizzazione per ambienti di lavoro) e fare clic su **Enable Indexing** (attiva indicizzazione) per l'ambiente di lavoro.
- Se almeno un ambiente di lavoro è già stato indicizzato, nella dashboard di ripristino in *Search & Restore*, fare clic su **Indexing Settings** (Impostazioni di indicizzazione) e fare clic su **Enable Indexing** (attiva indicizzazione) per l'ambiente di lavoro.

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.

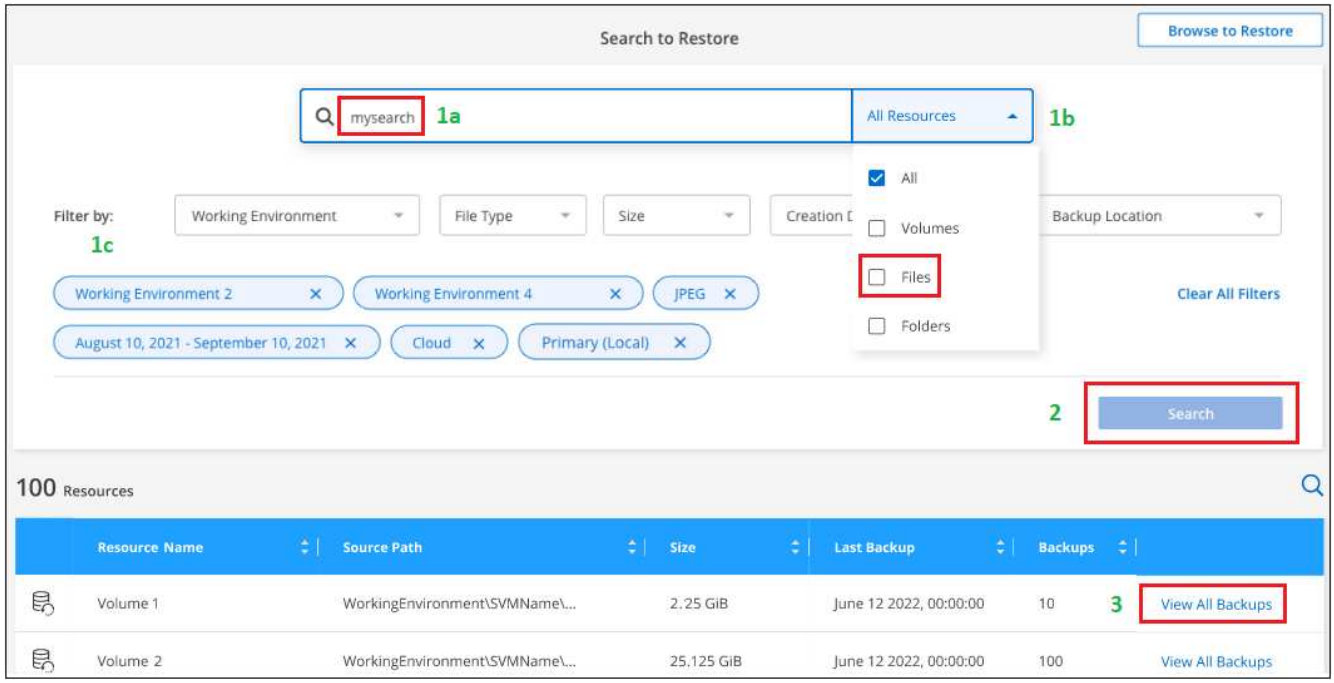
Ripristinare volumi, cartelle e file utilizzando Search & Restore

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.

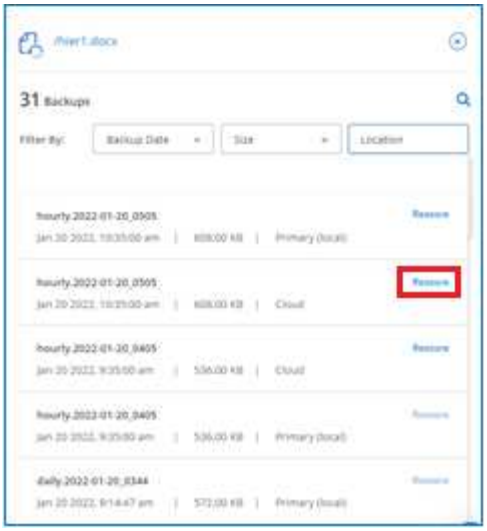
Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Fare clic sulla scheda **Restore** per visualizzare la dashboard di ripristino.
3. Nella sezione *Search & Restore*, fare clic su **Search & Restore**.

4. Dalla pagina Search to Restore (Cerca per il ripristino):
   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.
5. Fare clic su **Cerca** e nell'area risultati ricerca vengono visualizzate tutte le risorse che hanno un file, una cartella o un volume corrispondente alla ricerca.



6. Individuare la risorsa contenente i dati da ripristinare e fare clic su **View All backups** (Visualizza tutti i backup) per visualizzare tutti i file di backup che contengono il volume, la cartella o il file corrispondente.



7. Individuare il file di backup che si desidera utilizzare per ripristinare i dati e fare clic su **Restore** (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.

8. Selezionare il percorso di destinazione in cui si desidera ripristinare il volume, la cartella o i file e fare clic su **Restore** (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 inoltre possibile fare clic sulla scheda **Job Monitoring** per visualizzare l'avanzamento del ripristino.

Per i volumi ripristinati, è possibile "gestire le impostazioni di backup per questo nuovo volume" secondo necessità.

Backup e ripristino dei dati delle applicazioni on-premise

Proteggi i dati delle tue applicazioni on-premise

Il backup e ripristino BlueXP per le applicazioni offre funzionalità di protezione dei dati per snapshot coerenti con le applicazioni da ONTAP primario on-premise a cloud provider.

Puoi eseguire il backup di Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL, e PostgreSQL dai sistemi ONTAP on-premise ad Amazon Web Services, Microsoft Azure, Google Cloud Platform e StorageGRID.

Per ulteriori informazioni sul backup e ripristino BlueXP per le applicazioni, fare riferimento a:

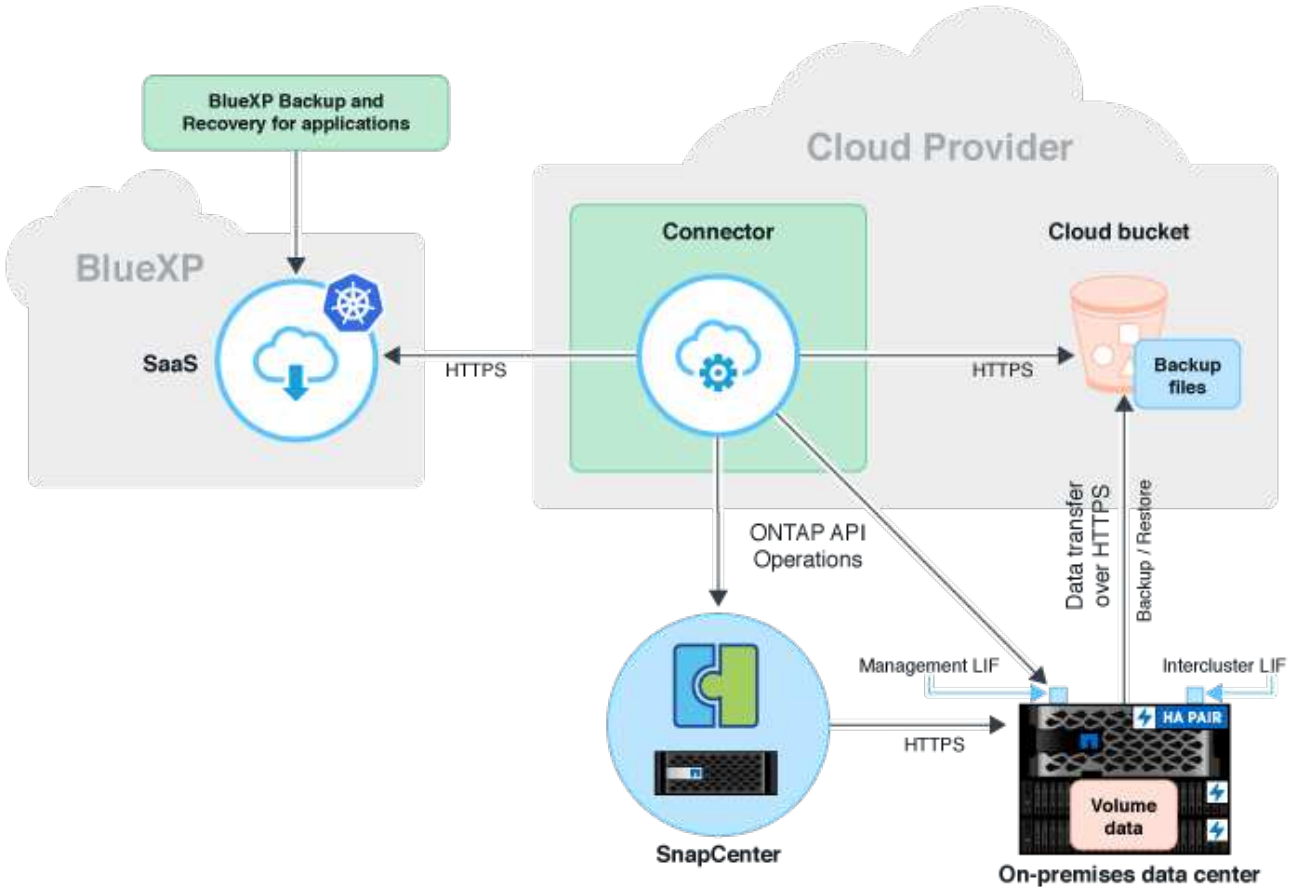
- "Backup integrato con l'applicazione con backup e ripristino BlueXP e SnapCenter"
- "Podcast su BlueXP backup e recovery per le applicazioni"

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei dati delle applicazioni nel cloud provider.

- ONTAP 9.8 o versione successiva
- BlueXP
- Server SnapCenter 4.6 o versione successiva
  - Se si desidera utilizzare le seguenti funzionalità, si consiglia di utilizzare SnapCenter Server 4.7 o versioni successive:
    - Protezione dei backup dallo storage secondario on-premise
    - Proteggere le applicazioni SAP HANA
    - Proteggere le applicazioni Oracle e SQL presenti nell'ambiente VMware
    - Esportazione dello storage di un backup
    - Disattivare i backup
    - Annullare la registrazione del server SnapCenter
  - Utilizzare SnapCenter Server 4,9 o versioni successive se si desidera utilizzare le seguenti funzioni:
    - Montare i backup del database Oracle
    - Ripristinare lo storage alternativo
  - Se si desidera proteggere le applicazioni MongoDB, MySQL e PostgreSQL, è consigliabile utilizzare SnapCenter Server 4,9P1
- Nel server SnapCenter deve essere disponibile almeno un backup per applicazione
- Almeno una policy giornaliera, settimanale o mensile in SnapCenter senza etichetta o stessa etichetta della policy in BlueXP

L'immagine seguente mostra ogni componente durante il backup nel cloud e le connessioni che è necessario preparare tra di essi:



Registrare il server SnapCenter

Solo un utente con ruolo SnapCenterAdmin può registrare l'host su cui è in esecuzione SnapCenter Server 4.6 o versione successiva. È possibile registrare più host server SnapCenter in BlueXP.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Server SnapCenter**.
3. Fare clic su **Registra server SnapCenter**.
4. Specificare i seguenti dettagli:
   a. Nel campo Server SnapCenter, specificare l'FQDN o l'indirizzo IP dell'host server SnapCenter.
   b. Nel campo porta, specificare il numero di porta su cui è in esecuzione l'host del server SnapCenter.

      Assicurarsi che la porta sia aperta per consentire la comunicazione tra il server SnapCenter e BlueXP.

   c. Nel campo Tag, specificare il nome del sito, la città o qualsiasi nome personalizzato con cui si desidera contrassegnare il server SnapCenter.

      I tag sono separati da virgole.

d. Nel campo Nome utente e Password, specificare le credenziali dell'utente con ruolo SnapCenterAdmin.

5. Selezionare il connettore dall'elenco a discesa **Connector** (connettore).
6. Fare clic su **Registra**.

Al termine

Fare clic su **Backup e ripristino** > **applicazioni** per visualizzare tutte le applicazioni protette mediante l'host del server SnapCenter registrato. Per impostazione predefinita, le applicazioni vengono rilevate automaticamente ogni giorno a mezzanotte.

Le applicazioni supportate e le relative configurazioni sono:

- Database Oracle:
  - Backup completi (dati + log) creati con almeno una pianificazione giornaliera, settimanale o mensile
  - SAN, NFS, VMDK-SAN, VMDK-NFS E RDM
- Database Microsoft SQL Server:
  - Standalone, istanze di cluster di failover e gruppi di disponibilità
  - Backup completi creati con almeno una pianificazione giornaliera, settimanale o mensile
  - SAN, VMDK-SAN, VMDK-NFS E RDM
- Database SAP HANA:
  - Container singolo 1.x
  - Contenitore di database multipli 2.x
  - Replica di sistema HANA (HSR)

    È necessario disporre di almeno un backup su siti primari e secondari. È possibile decidere di eseguire un guasto proattivo o un failover rinviato al secondario.

  - Risorse NDV (non-data Volumes) come file binari HANA, volume di log di archiviazione HANA, volume condiviso HANA e così via
- MongoDB
- MySQL
- PostgreSQL

I seguenti database non vengono visualizzati:

- Database senza backup
- Database con policy solo on-demand o orarie
- Database Oracle residenti su NVMe

Creare un criterio per il backup delle applicazioni

È necessario creare una policy per eseguire il backup dei dati dell'applicazione nel cloud.

Prima di iniziare

- Se si desidera spostare i backup dall'archivio di oggetti allo storage di archiviazione, assicurarsi di utilizzare la versione di ONTAP richiesta.

- Se utilizzi i servizi Web Amazon, dovresti utilizzare ONTAP 9.10.1 o versione successiva
- Se si utilizza Microsoft Azure, è necessario utilizzare ONTAP 9.10.1 o versione successiva
- Se utilizzi Google Cloud, dovresti utilizzare ONTAP 9.12.1 o versione successiva
- Se si utilizza StorageGRID, si consiglia di utilizzare ONTAP 9.12.1 o versione successiva

- È necessario configurare il Tier di accesso all'archivio per ciascun provider di cloud.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Dal menu a discesa Impostazioni, fare clic su **Criteri** > **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**.
7. Fare clic su **Create** (Crea).

Non è possibile modificare o eliminare un criterio associato a un'applicazione.

Eseguire il backup dei dati delle applicazioni on-premise su Amazon Web Services

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP a Amazon Web Services.

BlueXP supporta il blocco dei dati e la protezione dal ransomware. Se il cluster ONTAP è in esecuzione su ONTAP 9.11.1 o versione successiva e non hai configurato lo storage di archivio, puoi proteggere i backup dalla sovrascrittura, dall'eliminazione e dalle minacce ransomware.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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 una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   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.

Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

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

5. Selezionare **Amazon Web Services** come provider cloud.
   a. Specificare l'account AWS.
   b. Nel campo AWS Access Key (chiave di accesso AWS), specificare la chiave.
   c. Nel campo AWS Secret Key (chiave segreta AWS), specificare la password.
   d. Selezionare la regione in cui si desidera creare i backup.
   e. Specificare lo spazio IP.
   f. Selezionare il livello di archiviazione se è stato configurato lo spazio di archiviazione nel criterio.

      Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Configurare il blocco dei dati e la protezione dal ransomware.
7. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei dati delle applicazioni on-premise su Microsoft Azure

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP a Microsoft Azure.

BlueXP supporta il blocco dei dati e la protezione dal ransomware. Se il cluster ONTAP è in esecuzione su ONTAP 9.12.1 o versione successiva e non hai configurato lo storage di archivio, puoi proteggere i backup dalla sovrascrittura, dall'eliminazione e dalle minacce ransomware.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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 una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   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.

         Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

   c. Fare clic su **Aggiungi ambiente di lavoro**.
5. Selezionare **Microsoft Azure** come cloud provider.

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 lo spazio IP.
e. Selezionare il livello di archiviazione se è stato configurato lo spazio di archiviazione nel criterio.

   Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Configurare il blocco dei dati e la protezione dal ransomware.
7. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei dati delle applicazioni on-premise su Google Cloud Platform

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP alla piattaforma cloud Google.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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 una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   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.

      Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

   c. Fare clic su **Aggiungi ambiente di lavoro**.
5. Selezionare **Google Cloud Platform** come provider di cloud.
   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.
   f. Selezionare il livello di archiviazione.

Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei dati delle applicazioni on-premise su StorageGRID

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP a StorageGRID.

BlueXP supporta il blocco dei dati e la protezione dal ransomware. Se il cluster ONTAP è in esecuzione su ONTAP 9.11.1 o versione successiva, i sistemi StorageGRID sono 11.6.0.3 o versione successiva e se non hai configurato lo storage di archivio, puoi proteggere i backup da sovrascrittura, eliminazione e minacce ransomware.

Prima di iniziare

Quando si esegue il backup dei dati su StorageGRID, è necessario che sia disponibile un connettore on-premise. Sarà 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.

Per ulteriori informazioni, vedere "Creare connettori per StorageGRID".

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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 una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   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.

      Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

   c. Fare clic su **Aggiungi ambiente di lavoro**.
5. Selezionare **StorageGRID**.
   a. Specificare l'FQDN del server StorageGRID e la porta su cui viene eseguito il server StorageGRID.

      Inserire i dettagli nel formato FQDN:PORT.

   b. Nel campo Access Key (chiave di accesso), specificare la chiave.
   c. Nel campo Secret Key (chiave segreta), specificare la password.

d. Specificare lo spazio IP.

e. Specificare il livello di archiviazione se è stato configurato lo spazio di archiviazione nel criterio.

Se si seleziona…	Eseguire le seguenti operazioni…
AWS	i. Selezionare il StorageGRID dal menu a discesa o aggiungere il cluster StorageGRID. ii. Specificare l'account AWS. iii. Nel campo AWS Access Key (chiave di accesso AWS), specificare la chiave. iv. Nel campo AWS Secret Key (chiave segreta AWS), specificare la password. v. Selezionare la regione in cui si desidera creare i backup. vi. Fare clic su **Save** (Salva).
Azure	i. Selezionare il cluster StorageGRID dal menu a discesa o aggiungere il cluster. ii. Specificare l'ID dell'abbonamento Azure. iii. Selezionare la regione in cui si desidera creare i backup. iv. Creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente. v. Fare clic su **Save** (Salva).

Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Configurare il blocco dei dati e la protezione dal ransomware.
7. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Gestire la protezione delle applicazioni

È possibile gestire la protezione delle applicazioni visualizzando i criteri, visualizzando i backup, visualizzando le modifiche al layout del database, ai criteri e al gruppo di risorse e monitorando tutte le operazioni dall'interfaccia utente di BlueXP.

Visualizzare le policy

È possibile visualizzare tutte le policy. Per ciascuno di questi criteri, quando si visualizzano i dettagli vengono elencate tutte le applicazioni associate.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Criteri**.

3. Fare clic su **View Details** (Visualizza dettagli) corrispondente alla policy di cui si desidera visualizzare i dettagli.

   Vengono elencate le applicazioni associate.

   Non è possibile modificare o eliminare un criterio associato a un'applicazione.

È inoltre possibile visualizzare le policy SnapCenter estese nel cloud eseguendo `Get-SmResources` Cmdlet in SnapCenter.
Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help command name.

Visualizza i backup sul cloud

È possibile visualizzare i backup sul cloud nell'interfaccia utente di BlueXP.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **View Details** (Visualizza dettagli).

   Il tempo necessario per l'elenco dei backup dipende dalla pianificazione di replica predefinita di ONTAP.

- Per i database Oracle, vengono elencati sia i backup dei dati che dei log, il numero di modifica del sistema (SCN) per ciascun backup e la data di fine di ciascun backup. È possibile selezionare solo il backup dei dati e ripristinare il database nella posizione originale. È possibile montare il backup dei dati e il backup dei log in una posizione alternativa.
- Per i database Microsoft SQL Server, vengono elencati solo i backup completi e la data di fine di ciascun backup. È possibile selezionare il backup e ripristinare il database nella posizione originale o alternativa.
- Per l'istanza di Microsoft SQL Server, vengono elencati i backup dei database in tale istanza.
- Per i database SAP HANA, vengono elencati solo i backup dei dati e la data di fine di ciascun backup. È possibile selezionare il backup ed eseguire l'esportazione dello storage su un determinato host.
- Per MongoDB, MySQL e PostgreSQL, sono elencati solo i backup dei dati e la data finale di ciascun backup. È possibile selezionare il backup ed eseguire l'esportazione dello storage su un determinato host.

I backup creati prima di attivare la protezione cloud non sono elencati per il ripristino.

È inoltre possibile visualizzare questi backup eseguendo il `Get-SmBackup` Cmdlet in SnapCenter.
Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help command name.

Disattivare il backup

È possibile eliminare tutti i backup spostati nell'archivio di oggetti da SnapCenter e dall'archivio di oggetti.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su Disattiva backup.

Per impostazione predefinita, la casella di controllo è selezionata ed elimina tutti i backup spostati nell'archivio di oggetti da SnapCenter e dall'archivio di oggetti.

Se si deseleziona la casella di controllo, i backup vengono conservati solo nell'archivio di oggetti, ma non possono essere utilizzati per il ripristino a livello di applicazione. Successivamente, quando si attiva il backup per questa applicazione, i backup conservati nell'archivio di oggetti non vengono elencati per il ripristino.

3. Fare clic su **Disattiva backup**.

Modifica del layout del database

Quando i volumi vengono aggiunti al database, il server SnapCenter assegna automaticamente le etichette agli snapshot sui nuovi volumi in base alla policy e alla pianificazione. Questi nuovi volumi non avranno l'endpoint dell'archivio di oggetti ed è necessario aggiornare i volumi eseguendo i seguenti passaggi:

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Server SnapCenter**.
3. Fare clic su ••• Corrispondente al server SnapCenter che ospita l'applicazione e fare clic su **Aggiorna**.

   I nuovi volumi vengono scoperti.

4. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Refresh Protection** per attivare la protezione cloud per il nuovo volume.
   - Se un volume di storage viene aggiunto all'applicazione dopo la configurazione del provider cloud, il server SnapCenter etichetterà le snapshot per i nuovi backup su cui risiede l'applicazione.
   - È necessario eliminare manualmente la relazione dell'archivio di oggetti se il volume rimosso non viene utilizzato da altre applicazioni.
   - Se si aggiorna l'inventario delle applicazioni, esso conterrà il layout di storage corrente dell'applicazione.

Modifica di policy o gruppi di risorse

In caso di modifica del criterio SnapCenter o del gruppo di risorse, è necessario aggiornare la relazione di protezione.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Refresh Protection** (Aggiorna protezione).

Annullare la registrazione del server SnapCenter

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Server SnapCenter**.
3. Fare clic su ••• Corrispondente al server SnapCenter e fare clic su **Annulla registrazione**.

   Per impostazione predefinita, la casella di controllo è selezionata ed elimina tutti i backup spostati nell'archivio di oggetti da SnapCenter e dall'archivio di oggetti.

Se si deseleziona la casella di controllo, i backup vengono conservati solo nell'archivio di oggetti, ma non possono essere utilizzati per il ripristino a livello di applicazione. Successivamente, quando si attiva il backup per questa applicazione, i backup conservati nell'archivio di oggetti non vengono elencati per il ripristino.

Monitorare i lavori

I job vengono creati per tutte le operazioni di Cloud Backup. È possibile monitorare tutti i lavori e tutte le sottoattività eseguite come parte di ciascuna attività.

Fasi

1. Fare clic su **Backup and Recovery** > **Job Monitoring**.

   Quando si avvia un'operazione, viene visualizzata una finestra che indica che il processo è stato avviato. È possibile fare clic sul collegamento per monitorare il lavoro.

2. Fare clic sull'attività principale per visualizzare le attività secondarie e lo stato di ciascuna di queste attività secondarie.

Configurare i certificati CA

È possibile configurare il certificato firmato dalla CA se si desidera includere ulteriore protezione nell'ambiente.

Configurare il certificato firmato dalla CA SnapCenter in BlueXP Connector

È necessario configurare il certificato firmato dalla CA SnapCenter in BlueXP Connector in modo che il connettore possa verificare il certificato di SnapCenter.

Prima di iniziare

Eseguire il seguente comando in BlueXP Connector per ottenere *<base_mount_path>*:
```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Fasi

1. Accedere al connettore.
   ```
   cd <base_mount_path> mkdir -p server/certificate
   ```
2. Copiare i file CA principali e intermedi nella directory *<base_mount_path>/server/certificate*.

   I file CA devono essere in formato .pem.

3. Se si dispone di file CRL, attenersi alla seguente procedura:
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Copiare i file CRL nella directory *<base_mount_path>/server/crl*.
4. Connettersi a cloudmanager_snapcenter e modificare enableCACert in config.yml su true.
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert:
   false/enableCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. Riavviare il container Cloudmanager_snapcenter.
   ```
   sudo docker restart cloudmanager_snapcenter
   ```

Configurare il certificato firmato dalla CA per BlueXP Connector

Se il protocollo SSL bidirezionale è attivato in SnapCenter, attenersi alla seguente procedura sul connettore per utilizzare il certificato CA come certificato client quando il connettore si connette a SnapCenter.

Prima di iniziare

Eseguire il seguente comando per ottenere *<base_mount_path>*:

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Fasi

1. Accedere al connettore.
   ```
   cd <base_mount_path> mkdir -p client/certificate
   ```
2. Copiare il certificato e il file delle chiavi firmato dalla CA in *<base_mount_path>/client/certificate* nel connettore.

   Il nome del file deve essere certificate.pem e key.pem. Il file certificate.pem deve avere l'intera catena dei certificati, ad esempio CA intermedia e CA principale.

3. Creare il formato PKCS12 del certificato con il nome certificate.p12 e mantenere l'indirizzo *<base_mount_path>/client/certificate*.

   Esempio: openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12

4. Connettersi a cloudmanager_snapcenter e modificare sendCACert in config.yml su true.
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
   false/sendCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. Riavviare il container Cloudmanager_snapcenter.
   ```
   sudo docker restart cloudmanager_snapcenter
   ```
6. Per convalidare il certificato inviato dal connettore, eseguire le seguenti operazioni su SnapCenter.
   a. Accedere all'host del server SnapCenter.
   b. Fare clic su **Start** > **Avvia ricerca**.
   c. Digitare mmc e premere **Invio**.
   d. Fare clic su **Sì**.
   e. Nel menu file, fare clic su **Aggiungi/Rimuovi snap-in**.
   f. Fare clic su **certificati** > **Aggiungi** > **account computer** > **Avanti**.
   g. Fare clic su **computer locale** > **fine**.
   h. Se non si dispone di ulteriori snap-in da aggiungere alla console, fare clic su **OK**.
   i. Nella struttura della console, fare doppio clic su **certificati**.
   j. Fare clic con il pulsante destro del mouse sull'archivio **Trusted Root Certification Authorities**.
   k. Fare clic su **Import** (Importa) per importare i certificati e seguire la procedura descritta in **Certificate Import Wizard** (importazione guidata certificati).

Ripristinare i dati delle applicazioni on-premise

Ripristinare il database Oracle

È possibile ripristinare il database Oracle nella posizione originale o nella posizione alternativa. Per un database RAC, i dati vengono ripristinati nel nodo on-premise in cui è stato creato il backup.

È supportato solo il database completo con il ripristino del file di controllo. Se i log di archiviazione non sono presenti in AFS, specificare la posizione che contiene i log di archiviazione richiesti per il ripristino.

Single file Restore (SFR) non è supportato.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, selezionare il filtro **tipo** e dal menu a discesa selezionare **Oracle**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
4. Nella pagina delle opzioni di ripristino, specificare la posizione in cui si desidera ripristinare i file di database.

Se…	Eseguire questa operazione…
Ripristinare la posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Fare clic su **Avanti**. d. Selezionare **Database state** (Stato database) se si desidera modificare lo stato del database nello stato richiesto per eseguire le operazioni di ripristino e ripristino. I vari stati di un database, da quelli superiori a quelli inferiori, sono aperti, montati, avviati e arrestati. ◦ Se il database si trova in uno stato superiore ma lo stato deve essere modificato in uno stato inferiore per eseguire un'operazione di ripristino, selezionare questa casella di controllo. ◦ Se il database si trova in uno stato inferiore ma lo stato deve essere modificato in uno stato superiore per eseguire l'operazione di ripristino, lo stato del database viene modificato automaticamente anche se non si seleziona la casella di controllo. ◦ Se un database si trova in stato aperto e per il ripristino il database deve essere in stato montato, lo stato del database viene modificato solo se si seleziona questa casella di controllo. e. Specificare l'ambito del ripristino. ◦ Selezionare **All Logs** (tutti i registri) se si desidera ripristinare l'ultima transazione. ◦ Selezionare **fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico. ◦ Selezionare **Data e ora** se si desidera ripristinare dati e ore specifici. Specificare la data e l'ora del fuso orario dell'host del database. ◦ Selezionare **No recovery** se non si desidera eseguire il ripristino. f. Se i log di archiviazione non sono presenti nel file system attivo, specificare la posizione che contiene i log di archiviazione richiesti per il ripristino. Selezionare questa casella di controllo se si desidera aprire il database dopo il ripristino.

Se…	Eseguire questa operazione…
Ripristinare temporaneamente in un altro storage e copiare i file ripristinati nella posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. d. Fare clic su **Avanti**. e. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui i dati ripristinati dall'archivio di oggetti verranno memorizzati temporaneamente. Se si seleziona un sistema ONTAP on-premise e non si è configurata la connessione del cluster allo storage a oggetti, vengono richieste ulteriori informazioni relative all'archivio di oggetti. f. Fare clic su **Avanti**. g. Selezionare **Database state** (Stato database) se si desidera modificare lo stato del database nello stato richiesto per eseguire le operazioni di ripristino e ripristino. I vari stati di un database, da quelli superiori a quelli inferiori, sono aperti, montati, avviati e arrestati. ◦ Se il database si trova in uno stato superiore ma lo stato deve essere modificato in uno stato inferiore per eseguire un'operazione di ripristino, selezionare questa casella di controllo. ◦ Se il database si trova in uno stato inferiore ma lo stato deve essere modificato in uno stato superiore per eseguire l'operazione di ripristino, lo stato del database viene modificato automaticamente anche se non si seleziona la casella di controllo. ◦ Se un database si trova in stato aperto e per il ripristino il database deve essere in stato montato, lo stato del database viene modificato solo se si seleziona questa casella di controllo. Specificare l'ambito del ripristino. Selezionare **All Logs** (tutti i registri) se si

Se…	Eseguire questa operazione…
Ripristinare in una posizione alternativa	a. Selezionare **Ripristina in una posizione alternativa**. b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Se si desidera ripristinare lo storage alternativo, attenersi alla seguente procedura: i. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. ii. Fare clic su **Avanti**. iii. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui devono essere ripristinati i dati dell'archivio di oggetti. d. Fare clic su **Avanti**. e. Nella pagina Destination host (host di destinazione), selezionare l'host su cui verrà montato il database. i. (Facoltativo) per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti. ii. (Facoltativo) per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti. f. Fare clic su **Avanti**.

5. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

L'opzione **Restore to alternate location** (Ripristina in posizione alternativa) consente di montare il backup selezionato sull'host specificato. È necessario visualizzare manualmente il database.

Dopo aver montato il backup, non è possibile montarlo di nuovo fino a quando non viene smontato. È possibile utilizzare l'opzione **Unmount** dall'interfaccia utente per smontare il backup.

Per informazioni su come attivare il database Oracle, vedere "Articolo della Knowledge base".

Ripristinare il database di SQL Server

È possibile ripristinare il database di SQL Server nella posizione originale o nella posizione alternativa.

> Single file Restore (SFR), Recovery of log backups e reseed of Availability group non sono supportati.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, selezionare il filtro **tipo** e dal menu a discesa selezionare **SQL**.
3. Fare clic su **View Details** (Visualizza dettagli) per visualizzare tutti i backup disponibili.
4. Selezionare il backup e fare clic su **Restore** (Ripristina).
5. Nella pagina delle opzioni di ripristino, specificare la posizione in cui si desidera ripristinare i file di database.

Se…	Eseguire questa operazione…
Ripristinare la posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Fare clic su **Avanti**.
Ripristinare temporaneamente in un altro storage e copiare i file ripristinati nella posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. d. Fare clic su **Avanti**. e. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui i dati ripristinati dall'archivio di oggetti verranno memorizzati temporaneamente. f. Fare clic su **Avanti**.

Se…	Eseguire questa operazione…
Ripristinare in una posizione alternativa	a. Selezionare **Ripristina in una posizione alternativa**. b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Fare clic su **Avanti**. d. Nella pagina host di destinazione, selezionare un nome host, specificare un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino. L'estensione del file fornita nel percorso alternativo deve essere uguale all'estensione del file di database originale. e. Fare clic su **Avanti**.

Se…	Eseguire questa operazione…
Ripristinare temporaneamente in un altro storage e copiare i file ripristinati nella posizione alternativa	a. Selezionare **Ripristina in una posizione alternativa**. b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. d. Fare clic su **Avanti**. e. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui i dati ripristinati dall'archivio di oggetti verranno memorizzati temporaneamente. f. Fare clic su **Avanti**. g. Nella pagina host di destinazione, selezionare un nome host, specificare un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino. L'estensione del file fornita nel percorso alternativo deve essere uguale all'estensione del file di database originale. h. Fare clic su **Avanti**.

6. Nell'opzione **Pre-Operations**, selezionare una delle seguenti opzioni:
   - Selezionare **sovrascrivere il database con lo stesso nome durante il ripristino** per ripristinare il database con lo stesso nome.
   - Selezionare **Mantieni impostazioni di replica del database SQL** per ripristinare il database e conservare le impostazioni di replica esistenti.
7. Nella sezione **Post-Operations**, per specificare lo stato del database per il ripristino di registri transazionali aggiuntivi, selezionare una delle seguenti opzioni:
   - Selezionare **operativo, ma non disponibile** se si stanno ripristinando tutti i backup necessari.

     Questo è il comportamento predefinito, che lascia il database pronto per l'uso eseguendo il rollback delle transazioni non assegnate. Non è possibile ripristinare ulteriori registri delle transazioni fino a quando non si crea un backup.
   - Selezionare **non operativo, ma disponibile** per lasciare il database non operativo senza eseguire il rollback delle transazioni non assegnate.

È possibile ripristinare ulteriori registri delle transazioni. Non è possibile utilizzare il database fino a quando non viene ripristinato.

- Selezionare **Read-only mode (modalità di sola lettura) e Available** (disponibile) per lasciare il database in modalità di sola lettura.

  Questa opzione annulla le transazioni non assegnate, ma salva le azioni non riuscite in un file di standby in modo che gli effetti di ripristino possano essere ripristinati.

Se l'opzione Undo directory (Annulla directory) è attivata, vengono ripristinati altri log delle transazioni. Se l'operazione di ripristino del log delle transazioni non riesce, è possibile eseguire il rollback delle modifiche. La documentazione di SQL Server contiene ulteriori informazioni.

8. Fare clic su **Avanti**.
9. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Ripristinare il database SAP HANA

È possibile ripristinare il database SAP HANA su qualsiasi host.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, selezionare il filtro **tipo** e dal menu a discesa selezionare **HANA**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
4. Nella pagina delle opzioni di ripristino, specificare una delle seguenti opzioni:
   a. Per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti.
   b. Per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti.
5. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione.
6. Se lo spazio disponibile sullo storage di origine non è sufficiente o se lo storage di origine non è disponibile, selezionare **Modifica ubicazione dello storage**.

   Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione.

7. Fare clic su **Avanti**.
8. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui verranno memorizzati i dati ripristinati dall'archivio di oggetti.
9. Fare clic su **Avanti**.
10. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Questa operazione esegue solo l'esportazione dello storage del backup selezionato sull'host specificato. Si consiglia di montare manualmente il file system e di visualizzare il database. Dopo aver utilizzato il volume, l'amministratore dello storage può eliminare il volume dal cluster ONTAP.

Per informazioni su come attivare il database SAP HANA, vedere "TR-4667: Panoramica del workflow di copia del sistema SAP con SnapCenter" e. "TR-4667: Panoramica del workflow dei cloni di sistema SAP con SnapCenter".

Ripristino dei database MongoDB, MySQL e PostgreSQL

È possibile ripristinare i database MongoDB, MySQL e PostgreSQL su qualsiasi host.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, seleziona il filtro **tipo** e dal menu a discesa seleziona **MongoDB**, **MySQL** o **PostgreSQL**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
4. Nella pagina delle opzioni di ripristino, specificare una delle seguenti opzioni:
   a. Per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti.
   b. Per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti.
5. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione.
6. Se lo spazio disponibile sullo storage di origine non è sufficiente o se lo storage di origine non è disponibile, selezionare **Modifica ubicazione dello storage**.

   Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione.
7. Fare clic su **Avanti**.
8. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui verranno memorizzati i dati ripristinati dall'archivio di oggetti.
9. Fare clic su **Avanti**.
10. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Questa operazione esegue solo l'esportazione dello storage del backup selezionato sull'host specificato. Si consiglia di montare manualmente il file system e di visualizzare il database. Dopo aver utilizzato il volume, l'amministratore dello storage può eliminare il volume dal cluster ONTAP.

Backup e ripristino dei dati delle applicazioni native del cloud

Proteggi i dati delle tue applicazioni native del cloud

Il backup e ripristino BlueXP per le applicazioni offre funzionalità di protezione dei dati coerenti per le applicazioni eseguite sullo storage cloud NetApp. Il backup e ripristino BlueXP offre una protezione efficiente, coerente con l'applicazione e basata su policy delle seguenti applicazioni:

- Database Oracle residenti su Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP e Azure NetApp Files
- Sistemi SAP HANA che risiedono su Azure NetApp Files
- Database Microsoft SQL Server residenti in Amazon FSX per NetApp ONTAP

Architettura

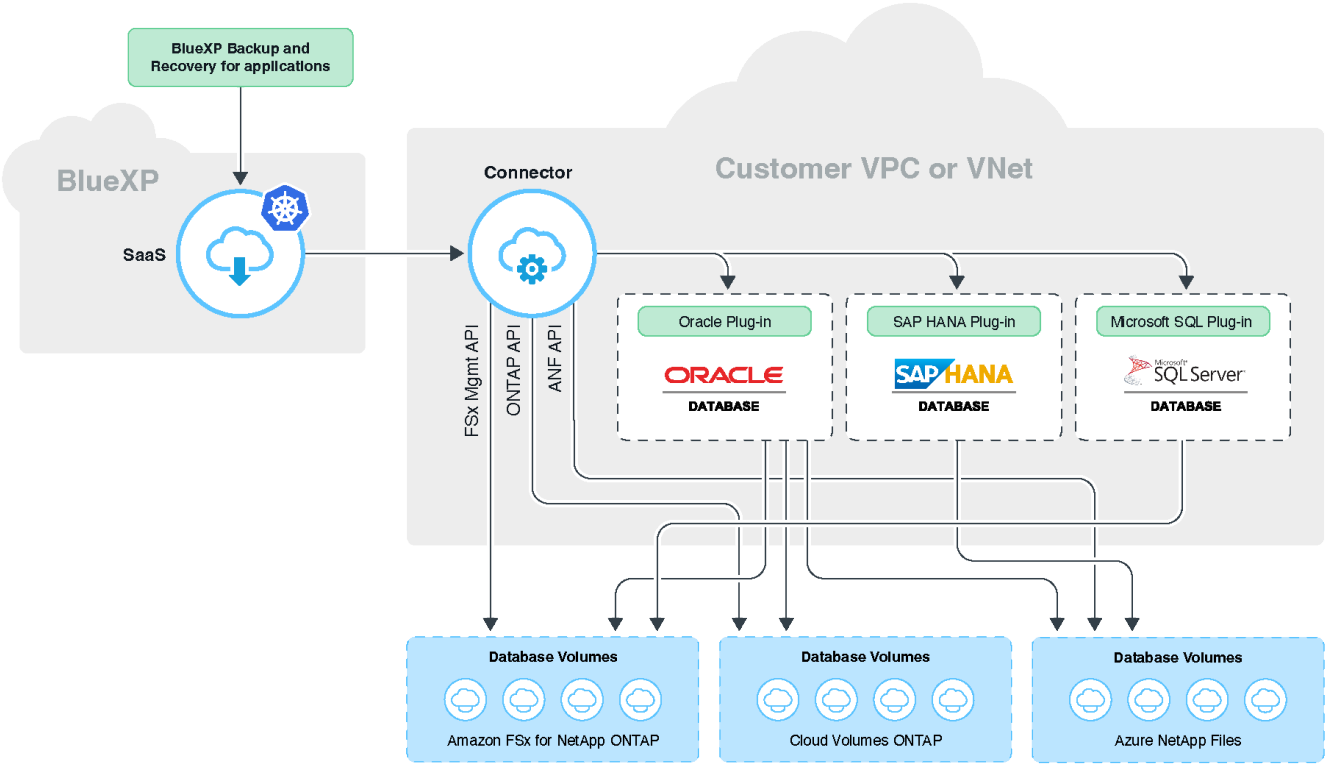
Il backup e ripristino BlueXP per l'architettura delle applicazioni include i seguenti componenti.

- Il backup e ripristino BlueXP è un insieme di servizi di protezione dei dati ospitati come servizio SaaS da NetApp e si basa sulla piattaforma BlueXP SaaS.

  Orchestrano i flussi di lavoro per la protezione dei dati per le applicazioni che risiedono su NetApp Cloud Storage.

- L'interfaccia utente di BlueXP offre funzionalità di protezione dei dati per le applicazioni ed è accessibile dall'interfaccia utente di BlueXP.
- BlueXP Connector è un componente che viene eseguito nella rete cloud e interagisce con i sistemi storage e i plug-in specifici dell'applicazione.
- Il plug-in specifico dell'applicazione è un componente che viene eseguito su ciascun host dell'applicazione e interagisce con i database in esecuzione sull'host durante le operazioni di protezione dei dati.

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



Per qualsiasi richiesta avviata dall'utente, l'interfaccia utente di BlueXP comunica con BlueXP SaaS che, dopo la convalida della richiesta, elabora lo stesso. Se la richiesta consiste nell'eseguire un flusso di lavoro, ad esempio un backup, un ripristino o un clone, il servizio SaaS avvia il flusso di lavoro e, se necessario, inoltra la chiamata a BlueXP Connector. Il connettore comunica quindi con il sistema di storage e il plug-in specifico dell'applicazione durante l'esecuzione delle attività del flusso di lavoro.

Il connettore può essere implementato nello stesso VPC o VNET delle applicazioni o in un altro. Se il connettore e le applicazioni si trovano su una rete diversa, è necessario stabilire una connettività di rete tra di essi.

> Un singolo connettore BlueXP è in grado di comunicare con più sistemi storage e plug-in di applicazioni. Per gestire le applicazioni è necessario un unico connettore, purché vi sia connettività tra il connettore e gli host delle applicazioni.

> L'infrastruttura BlueXP SaaS è resiliente ai guasti delle zone di disponibilità all'interno di una regione. Supporta i guasti regionali eseguendo il failover in una nuova regione e questo failover comporta un downtime di circa 2 ore.

Proteggere i database Oracle

Caratteristiche

- Aggiungere host e implementare il plug-in

  È possibile implementare il plug-in utilizzando l'interfaccia utente, lo script o manualmente.

- Rilevamento automatico dei database Oracle

- Backup dei database Oracle che risiedono su Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP e Azure NetApp Files
  - Backup completo (dati + controllo + file di log di archiviazione)
  - Backup on-demand
  - Backup pianificato in base ai criteri definiti dal sistema o personalizzati

    È possibile specificare diverse frequenze di pianificazione, ad esempio oraria, giornaliera, settimanale e mensile, nella policy. È inoltre possibile specificare gli script successivi che verranno eseguiti dopo il backup per copiare lo snapshot nello storage secondario.
- I backup dei database Oracle su Azure NetApp Files possono essere catalogati utilizzando Oracle RMAN
- Conservazione dei backup in base alla policy
- Ripristino dei database Oracle residenti su Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP e Azure NetApp Files
  - Ripristino del database Oracle completo (file di dati + file di controllo) dal backup specificato
  - Ripristino del database Oracle con fino a SCN, fino al momento, tutti i registri disponibili e nessuna opzione di ripristino
- Ripristino dei database Oracle su Azure NetApp Files in una posizione alternativa
- Clonazione di database Oracle residenti su Amazon FSX per NetApp ONTAP e Cloud Volumes ONTAP su host di destinazione di origine o alternativi
  - Clone di base con un click
  - Cloning avanzato con file di specifica del clone personalizzato
  - Il nome delle entità clonate può essere generato automaticamente o identico all'origine
  - Visualizzazione della gerarchia di cloni
  - Eliminazione dei database clonati
- Monitoraggio di backup, ripristino, clonazione e altri processi
- Visualizzazione del riepilogo della protezione sul dashboard
- Invio di avvisi tramite e-mail
- Aggiornare il plug-in host

Limitazioni

- Non supporta Oracle 11g
- Non supporta operazioni di montaggio, catalogo e verifica sui backup
- Non supporta Oracle su RAC e Data Guard
- Per Cloud Volumes ONTAP ha, viene utilizzato solo uno degli IP dell'interfaccia di rete. Se la connettività dell'IP non è disponibile o non è possibile accedere all'IP, le operazioni di protezione dei dati non vengono eseguite correttamente.
- Gli indirizzi IP dell'interfaccia di rete di Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP devono essere univoci nell'account e nella regione BlueXP.

Proteggere i database SAP HANA

Caratteristiche

- Aggiungere manualmente i sistemi SAP HANA
- Backup dei database SAP HANA
  - Backup on-demand (basato su file e copia Snapshot)
  - Backup pianificato in base ai criteri definiti dal sistema o personalizzati

    È possibile specificare diverse frequenze di pianificazione, ad esempio oraria, giornaliera, settimanale e mensile, nella policy.

  - Compatibile con HANA System Replication (HSR)
- Conservazione dei backup in base alla policy
- Ripristino del database SAP HANA completo dal backup specificato
- Backup e ripristino di volumi non dati HANA e volumi non dati globali
- Supporto Prescrittt e postscript utilizzando variabili ambientali per le operazioni di backup e ripristino
- Creazione di un piano d'azione per gli scenari di guasto utilizzando l'opzione pre-exit

Limitazioni

- Per la configurazione HSR, è supportato solo HSR a 2 nodi (1 primario e 1 secondario)
- La conservazione non viene attivata se il postscript non riesce durante l'operazione di ripristino

Proteggere il database di Microsoft SQL Server

Caratteristiche

- Aggiungere manualmente l'host e distribuire il plug-in
- Rilevare i database manualmente
- Eseguire il backup delle istanze di SQL Server che risiedono in Amazon FSX per NetApp ONTAP
  - Backup on-demand
  - Backup pianificato in base al criterio
  - Backup del registro dell'istanza di Microsoft SQL Server
- Ripristinare il database nella posizione originale

Limitazioni

- Il backup è supportato solo per le istanze di SQL Server
- La configurazione di istanza cluster di failover (FCI) non è supportata
- L'interfaccia utente di BlueXP non supporta operazioni specifiche del database SQL

  Tutte le operazioni specifiche dei database Microsoft SQL Server vengono eseguite tramite API REST.

- Il ripristino in una posizione alternativa non è supportato

Eseguire il backup dei database Oracle nativi del cloud

Avvio rapido

Inizia subito seguendo questa procedura.

1 Verificare il supporto per la configurazione

- Sistema operativo:
  - RHEL 7.5 o versione successiva e 8.x.
  - OL 7.5 o versione successiva e 8.x
  - SLES 15 SP4
- Cloud storage NetApp:
  - Amazon FSX per NetApp ONTAP
  - Cloud Volumes ONTAP
  - Azure NetApp Files
- Layout dello storage:
  - NFS v3 e v4.1 (incluso DNFS)
  - ISCSI con ASM (ASMFD, ASMLib e ASMUdev)

    Azure NetApp Files non supporta l'ambiente SAN.

- Layout dei database: Oracle Standard e Oracle Enterprise standalone (CDB e PDB legacy e multi-tenant)
- Versioni di database: 19c e 21c

2 Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a. "Iscriviti a BlueXP".

3 Accedere a BlueXP

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a. "Accedere a BlueXP".

4 Gestisci il tuo account BlueXP

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a. "Gestisci il tuo account BlueXP".

Configurare FSX per ONTAP

Con BlueXP è necessario creare un ambiente di lavoro FSX per ONTAP per aggiungere

e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro FSX per ONTAP

È necessario creare FSX per ambienti di lavoro ONTAP in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. "Inizia a utilizzare Amazon FSX per ONTAP" e. "Creare e gestire un ambiente di lavoro Amazon FSX per ONTAP".

È possibile creare l'ambiente di lavoro FSX per ONTAP utilizzando BlueXP o AWS. Se hai creato utilizzando AWS, dovresti scoprire FSX per i sistemi ONTAP in BlueXP.

Creare un connettore

Un account Admin deve creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. "Creazione di un connettore in AWS da BlueXP".

- È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro FSX per ONTAP che i database.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e dei database nello stesso cloud privato virtuale (VPC), è possibile implementare il connettore nello stesso VPC.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e di database in diversi VPC:
  - Se si dispone di carichi di lavoro NAS (NFS) configurati su FSX per ONTAP, è possibile creare il connettore su uno dei VPC.
  - Se si hanno solo carichi DI lavoro SAN configurati e non si intende utilizzare carichi di lavoro NAS (NFS), è necessario creare il connettore nel VPC in cui viene creato il sistema FSX per ONTAP.

> Per utilizzare i carichi di lavoro NAS (NFS), è necessario disporre di un gateway di transito tra il VPC del database e Amazon VPC. È possibile accedere all'indirizzo IP NFS, che è un indirizzo IP mobile, da un altro VPC solo attraverso il gateway di transito. Non è possibile accedere agli indirizzi IP mobili eseguendo il peering dei VPC.

Dopo aver creato il connettore, fare clic su **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni per aggiungere l'ambiente di lavoro. Assicurarsi che vi sia connettività dal connettore agli host del database Oracle e all'ambiente di lavoro FSX. Il connettore dovrebbe essere in grado di connettersi all'indirizzo IP di gestione del cluster dell'ambiente di lavoro FSX.

- Aggiungere l'ambiente di lavoro facendo clic su **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment**.

  Assicurarsi che vi sia connettività dal connettore agli host del database e all'ambiente di lavoro FSX per ONTAP. Il connettore deve connettersi all'indirizzo IP di gestione del cluster di FSX per l'ambiente di lavoro ONTAP.

- Copiare l'ID del connettore facendo clic su **Connector > Manage Connectors** (connettore > Gestisci connettori) e selezionando il nome del connettore.

Configurare Cloud Volumes ONTAP

Con BlueXP è necessario creare un ambiente di lavoro Cloud Volumes ONTAP per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore per il proprio ambiente cloud che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Cloud Volumes ONTAP

È possibile individuare e aggiungere sistemi Cloud Volumes ONTAP esistenti a BlueXP. Per ulteriori informazioni, fare riferimento a. "Aggiunta di sistemi Cloud Volumes ONTAP esistenti a BlueXP".

Creare un connettore

Puoi iniziare a utilizzare Cloud Volumes ONTAP per il tuo ambiente cloud in pochi passaggi. Per ulteriori informazioni, fare riferimento a una delle seguenti voci:

- "Avvio rapido di Cloud Volumes ONTAP in AWS"
- "Avvio rapido di Cloud Volumes ONTAP in Azure"
- "Guida rapida per Cloud Volumes ONTAP in Google Cloud"

È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro Cloud Volumes ONTAP che i database.

- Se l'ambiente di lavoro Cloud Volumes ONTAP e i database si trovano nello stesso cloud privato virtuale (VPC) o VNET, è possibile implementare il connettore nello stesso VPC o VNET.
- Se si dispone di un ambiente di lavoro Cloud Volumes ONTAP e di database in VPC o VNet diversi, assicurarsi che i VPC o VNet siano peering.

Configurare Azure NetApp Files

Con BlueXP è necessario creare un ambiente di lavoro Azure NetApp Files per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Azure NetApp Files

È necessario creare ambienti di lavoro Azure NetApp Files in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. "Scopri di più su Azure NetApp Files" e. "Creare un ambiente di lavoro Azure NetApp Files".

Creare un connettore

Un amministratore di account BlueXP dovrebbe implementare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. "Creare un connettore in Azure da BlueXP".

- Assicurarsi che vi sia connettività tra il connettore e gli host del database.

- Se si dispone dell'ambiente di lavoro e dei database Azure NetApp Files nella stessa rete virtuale (VNET), è possibile implementare il connettore nella stessa rete virtuale.
- Se si dispone di un ambiente di lavoro Azure NetApp Files e di database in reti VNet diverse e si hanno carichi di lavoro NAS (NFS) configurati su Azure NetApp Files, è possibile creare il connettore su una delle reti VNet.

Dopo aver creato il connettore, aggiungere l'ambiente di lavoro facendo clic su **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment**.

Installare il plug-in SnapCenter per Oracle e aggiungere host di database

È necessario installare il plug-in SnapCenter per Oracle su ciascuno degli host di database Oracle, aggiungere gli host di database e rilevare i database sull'host per assegnare criteri e creare backup.

- Se SSH è attivato per l'host del database, è possibile installare il plug-in utilizzando uno dei seguenti metodi:
  - Installare il plug-in e aggiungere l'host dall'interfaccia utente utilizzando l'opzione SSH. Scopri di più.
  - Installare il plug-in utilizzando lo script e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale. Scopri di più.
- Se SSH è disattivato, installare il plug-in manualmente e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale. Scopri di più.

Prerequisiti

Prima di aggiungere l'host, assicurarsi che i prerequisiti siano soddisfatti.

- L'ambiente di lavoro e il connettore dovrebbero essere stati creati.
- Assicurarsi che il connettore sia collegato agli host del database Oracle.

  Per informazioni su come risolvere il problema di connettività, fare riferimento a. "Impossibile convalidare la connettività dall'host del connettore BlueXP all'host del database dell'applicazione".

  Quando il connettore viene perso o se è stato creato un nuovo connettore, è necessario associarlo alle risorse dell'applicazione esistenti. Per istruzioni sull'aggiornamento del connettore, vedere "Aggiornare i dettagli del connettore".

- Assicurarsi che l'utente BlueXP abbia il ruolo di "account Admin".
- Assicurarsi che l'account non root (sudo) sia presente sull'host dell'applicazione per le operazioni di protezione dei dati.
- Assicurarsi che Java 11 (64-bit) Oracle Java o OpenJDK sia installato su ciascuno degli host di database Oracle e che LA variabile JAVA_HOME sia impostata correttamente.
- Se viene eseguita l'installazione basata su SSH, assicurarsi che il connettore abbia attivato la comunicazione con la porta SSH (impostazione predefinita: 22).
- Assicurarsi che il connettore abbia la comunicazione abilitata alla porta plug-in (impostazione predefinita: 8145) per il funzionamento delle operazioni di protezione dei dati.
- Assicurarsi che sia installata la versione più recente del plug-in. Per aggiornare il plug-in, fare riferimento a. Upgrade del plug-in SnapCenter per database Oracle.

Aggiungere host dall'interfaccia utente utilizzando l'opzione SSH

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.

   Se è già stato aggiunto un host e si desidera aggiungere un altro host, fare clic su **applicazioni** > **Gestisci database** > **Aggiungi**, quindi passare al punto 5.

2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

   Viene creato un account di servizio (*SnapCenter-account-<accountid>*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-<accountid>*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account** > **Gestisci account** > **membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina host details (Dettagli host), eseguire le seguenti operazioni:

   a. Selezionare **utilizzando SSH**.
   b. Specificare l'FQDN o l'indirizzo IP dell'host in cui si desidera installare il plug-in.

      Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

   c. Specificare l'utente non root(sudo) che utilizza il pacchetto del plug-in da copiare sull'host.

      L'utente root non è supportato.

   d. Specificare la porta SSH e il plug-in.

      La porta SSH predefinita è 22 e la porta plug-in è 8145.

   Dopo aver installato il plug-in, è possibile chiudere la porta SSH sull'host dell'applicazione. La porta SSH non è necessaria per le operazioni di protezione dei dati.

   a. Selezionare il connettore.
   b. (Facoltativo) se l'autenticazione senza chiave non è abilitata tra il connettore e l'host, specificare la chiave privata SSH che verrà utilizzata per comunicare con l'host.

      > La chiave privata SSH non viene memorizzata nell'applicazione e non viene utilizzata per altre operazioni.

   c. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:

   a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
   b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
   c. Creare il file */etc/sudoers.d/snapcenter* sulla macchina Linux e incollare il testo copiato.

d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.

7. Esaminare i dettagli e fare clic su **Scopri applicazioni**.
   - Una volta installato il plug-in, viene avviata l'operazione di rilevamento.
   - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a. Configurare le credenziali del database Oracle.
   - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
   - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Aggiungere host dall'interfaccia utente utilizzando l'opzione manuale e installare il plug-in utilizzando lo script

Configurare l'autenticazione basata su chiave SSH per l'account utente non root dell'host Oracle ed eseguire i seguenti passaggi per installare il plug-in.

Prima di iniziare

Assicurarsi che la connessione SSH al connettore sia attivata.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

   Viene creato un account di servizio (*SnapCenter-account-<accountid>*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-<accountid>*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account** > **Gestisci account** > **membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina host details (Dettagli host), eseguire le seguenti operazioni:
   a. Selezionare **Manuale**.
   b. Specificare l'FQDN o l'indirizzo IP dell'host in cui è installato il plug-in.

      Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

   c. Specificare la porta del plug-in.

      La porta predefinita è 8145.

   d. Specificare l'utente non root (sudo) che utilizza il pacchetto del plug-in da copiare sull'host.
   e. Selezionare il connettore.
   f. Selezionare la casella di controllo per confermare che il plug-in è installato sull'host.
   g. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:

a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.

b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.

c. Creare il file */etc/sudoers.d/snapcenter* sulla macchina Linux e incollare il testo copiato.

d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.

7. Accedere a Connector VM.

8. Installare il plug-in utilizzando lo script fornito nel connettore.

```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

Se si utilizza un connettore meno recente, eseguire il seguente comando per installare il plug-in.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Nome	Descrizione	Obbligatorio	Predefinito
plugin_host	Specifica l'host Oracle	Sì	-
nome_utente_host	Specifica l'utente SnapCenter con privilegi SSH sull'host Oracle	Sì	-
host_ssh_key	Specifica la chiave SSH dell'utente SnapCenter e viene utilizzata per connettersi all'host Oracle	Sì	-
porta_plugin	Specifica la porta utilizzata dal plug-in	No	8145
host_ssh_port	Specifica la porta SSH sull'host Oracle	No	22

Ad esempio:

- `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`
- `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. Nell'interfaccia utente di BlueXP, esaminare i dettagli e fare clic su **Scopri applicazioni**.
    - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a. Configurare le credenziali del database Oracle.
    - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
    - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Aggiungere host dall'interfaccia utente utilizzando l'opzione manuale e installare il plug-in manualmente

Se l'autenticazione basata su chiave SSH non è abilitata sull'host del database Oracle, attenersi alla seguente procedura manuale per installare il plug-in e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

   Viene creato un account di servizio (*SnapCenter-account-<accountid>*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-<accountid>*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account** > **Gestisci account** > **membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina **Dettagli host**, eseguire le seguenti operazioni:
   a. Selezionare **Manuale**.
   b. Specificare l'FQDN o l'indirizzo IP dell'host in cui è installato il plug-in.

      Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

   c. Specificare la porta del plug-in.

      La porta predefinita è 8145.

   d. Specificare l'utente sudo non-root (sudo) che utilizza il pacchetto del plug-in da copiare sull'host.
   e. Selezionare il connettore.
   f. Selezionare la casella di controllo per confermare che il plug-in è installato sull'host.
   g. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:
   a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
   b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.

c. Creare il file */etc/sudoers.d/snapcenter* sulla macchina Linux e incollare il testo copiato.

d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.

7. Accedere a Connector VM.

8. Scarica il binario del plug-in host Linux di SnapCenter.
```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

   Il binario del plug-in è disponibile all'indirizzo: *cd /var/lib/docker/Volumes/service-manager[1]-2_cloudmanager_scs_cloud_volume/_data/€(sudo docker ps|grep -po "cloudmanager_scs_cloud:.*? "|sed -e/ */"|cut -f2 -d":")/sc-linux-host-plugin*

9. Copiare *snapcenter_linux_host_plugin_scs.bin* dal percorso sopra indicato al percorso */home/<non root user (sudo)>/.sc_netapp* per ciascuno degli host di database Oracle utilizzando metodi scp o altri metodi alternativi.

10. Accedere all'host del database Oracle utilizzando l'account non root (sudo).

11. Modificare la directory in */home/<non root user>/.sc_netapp/* ed eseguire il seguente comando per abilitare le autorizzazioni di esecuzione per il file binario.
```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

12. Installare il plug-in Oracle come utente sudo SnapCenter.
```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```

13. Copiare *certificate.pem* dal percorso *<base_mount_path>/client/certificate/* del connettore VM a */var/opt/snapcenter/spl/etc/* sull'host plug-in.

14. Andare a */var/opt/snapcenter/spl/etc* ed eseguire il comando keytool per importare il file certificate.pem.
```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
-deststorepass snapcenter -noprompt
```

15. Riavviare SPL: `systemctl restart spl`

16. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.
```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
plug-in host>:<plug-in port>/PluginService/Version --cert
/config/client/certificate/certificate.pem --key
/config/client/certificate/key.pem
```

17. Nell'interfaccia utente di BlueXP, esaminare i dettagli e fare clic su **Scopri applicazioni**.
    - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a. Configurare le credenziali del database Oracle.
    - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
    - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Configurare le credenziali del database Oracle

È necessario configurare le credenziali del database utilizzate per eseguire operazioni di protezione dei dati sui database Oracle.

Fasi

1. Se l’autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per modificare l’autenticazione del database.
2. Specificare il nome utente, la password e i dettagli della porta.

   Se il database risiede in ASM, è necessario configurare anche le impostazioni ASM.

   L’utente Oracle deve disporre dei privilegi sysdba e l’utente ASM deve disporre dei privilegi sysasm.

3. Fare clic su **Configura**.

Upgrade del plug-in SnapCenter per database Oracle

È necessario aggiornare il plug-in SnapCenter per Oracle per accedere alle nuove funzionalità e ai miglioramenti più recenti. È possibile eseguire l’aggiornamento dall’interfaccia utente di BlueXP o dalla riga di comando.

Prima di iniziare

- Assicurarsi che non vi siano operazioni in esecuzione sull’host.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni** > **host**.
2. Verificare se l’aggiornamento del plug-in è disponibile per uno degli host controllando la colonna Stato generale.
3. Aggiornare il plug-in dall’interfaccia utente o utilizzando la riga di comando.

Eseguire l'aggiornamento utilizzando l'interfaccia utente	Eseguire l'aggiornamento utilizzando la riga di comando

a. Fare clic su ••• Corrispondente all'host e fare clic su **Upgrade Plug-in**.
b. Nella pagina di configurazione, eseguire le seguenti operazioni:
i. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
ii. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
iii. Modificare il file */etc/sudoers.d/snapcenter* sulla macchina Linux e incollare il testo copiato.
iv. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Upgrade** (Aggiorna).
	a. Accedere a Connector VM.
	b. Eseguire il seguente script.
	`sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`
	
	Se si utilizza un connettore meno recente, eseguire il seguente comando per aggiornare il plug-in.
	`sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`

Eseguire il backup dei database Oracle nativi del cloud

È possibile creare backup pianificati o on-demand assegnando un criterio predefinito o il criterio creato.

È inoltre possibile catalogare i backup del database Oracle utilizzando Oracle Recovery Manager (RMAN) se è stata attivata la catalogazione durante la creazione di una policy. La catalogazione (RMAN) è supportata solo per i database su Azure NetApp Files. I backup catalogati possono essere utilizzati in seguito per operazioni di ripristino a livello di blocco o tablespace point-in-time. Il database deve essere in stato montato o superiore per la catalogazione.

Creare policy per proteggere il database Oracle

È possibile creare policy se non si desidera modificare le policy predefinite.

Fasi

1. Nella pagina applicazioni, dall'elenco a discesa Impostazioni, selezionare **Criteri**.
2. Fare clic su **Crea policy**.
3. Specificare un nome di policy.

4. (Facoltativo) modificare il formato del nome del backup.
5. Specificare la pianificazione e i dettagli di conservazione.
6. Se hai selezionato *daily* e *settimanalmente* come programma e desideri attivare la catalogazione RMAN, seleziona **Catalog backup with Oracle Recovery Manager (RMAN)**.
7. (Facoltativo) inserire il percorso post-script e il valore di timeout per il post-script che verrà eseguito dopo il backup corretto, ad esempio la copia dello snapshot nello storage secondario.

   In alternativa, è possibile specificare anche gli argomenti.

   I post-script devono essere contenuti nel percorso */var/opt/snapcenter/spl/scripts*.

   Lo script post supporta un set di variabili di ambiente.

Variabile ambientale	Descrizione
SC_ORACLE_SID	Specifica il SID del database Oracle.
HOST_SC	Specifica il nome host del database
NOME_BACKUP_SC	Specifica il nome del backup. Il nome del backup dei dati e il nome del backup del registro vengono concatenati mediante delimitatori.
NOME_POLICY_BACKUP_SC	Specifica il nome del criterio utilizzato per creare il backup.
PERCORSO_COMPLETO_VOLUME_DATI_PRIMARI_SC	Specifica i percorsi dei volumi di dati concatenati utilizzando "," come delimitatore. Per i volumi Azure NetApp Files, le informazioni vengono concatenate utilizzando "/" _ /Subscriptions/{subscription_id}/resourceGroups/{resource_group}/provider/{provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumename{}_
SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH	Specifica i percorsi dei volumi del log di archiviazione concatenati utilizzando "," come delimitatore. Per i volumi Azure NetApp Files, le informazioni vengono concatenate utilizzando "/" _ /Subscriptions/{subscription_id}/resourceGroups/{resource_group}/provider/{provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumename{}_

8. Fare clic su **Create** (Crea).

Configurare il repository del catalogo RMAN

È possibile configurare il database del catalogo di ripristino come repository del catalogo RMAN. Se non si configura il repository, per impostazione predefinita, il file di controllo del database di destinazione diventa il repository del catalogo RMAN.

Prima di iniziare

Registrare manualmente il database di destinazione con il database del catalogo RMAN.

Fasi

1. Nella pagina applicazioni, fare clic su ••• > **Visualizza dettagli**.
2. Nella sezione Database details (Dettagli database), fare clic su Per configurare il repository del catalogo RMAN.
3. Specificare le credenziali per catalogare i backup con RMAN e il nome TNS (transparent Network substrate) del database di ripristino del catalogo.
4. Fare clic su **Configura**.

Creare un backup del database Oracle

È possibile assegnare un criterio predefinito o creare un criterio e assegnarlo al database. Una volta assegnato il criterio, i backup vengono creati in base alla pianificazione definita nel criterio.

> Quando si creano diskgroup ASM su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP, assicurarsi che non vi siano volumi comuni tra i diskgroup. Ogni gruppo di dischi deve disporre di volumi dedicati.

Fasi

1. Nella pagina applicazioni, se il database non è protetto mediante criteri, fare clic su **Assegna policy**.

   Se il database è protetto mediante uno o più criteri, è possibile assegnare ulteriori criteri facendo clic su ••• > **Assegna policy**.

2. Selezionare il criterio e fare clic su **Assegna**.

   I backup verranno creati in base alla pianificazione definita nella policy. Se è stato abilitato il catalogo RMAN nella policy, il backup alla fine del workflow avvierà l'operazione di catalogazione come un lavoro separato. L'avanzamento della catalogazione è visibile da Job Monitor. Una volta completata la catalogazione, **Backup Details** mostrerà lo stato del catalogo per ciascun backup.

   > L'account del servizio (*SnapCenter-account-<account_id>*) viene utilizzato per eseguire le operazioni di backup pianificate.

Creazione di backup on-demand del database Oracle

Dopo aver assegnato il criterio, è possibile creare un backup on-demand dell'applicazione.

Fasi

1. Nella pagina applicazioni, fare clic su ••• Corrispondente all'applicazione e fare clic su **Backup on-Demand**.

2. Se all'applicazione sono assegnati più criteri, selezionare il criterio, il livello di conservazione e fare clic su **Create Backup** (Crea backup).

   Se è stato abilitato il catalogo RMAN nella policy, il backup alla fine del workflow avvierà l'operazione di catalogazione come un lavoro separato. L'avanzamento della catalogazione è visibile da Job Monitor. Una volta completata la catalogazione, **Backup Details** mostrerà lo stato del catalogo per ciascun backup.

Limitazioni

- Non supporta snapshot di gruppi di coerenza per database Oracle che risiedono su più gruppi di dischi ASM con sovrapposizione di volumi FSX
- Se i database Oracle si trovano su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP e sono configurati su ASM, assicurarsi che i nomi SVM siano univoci nei sistemi FSX. Se si dispone dello stesso nome SVM nei sistemi FSX, il backup dei database Oracle che risiedono su tali SVM non è supportato.
- Dopo il ripristino di un database di grandi dimensioni (250 GB o superiore), se si esegue un backup online completo sullo stesso database, l'operazione potrebbe non riuscire e causare il seguente errore:
  ```
  failed with status code 500, error
  {\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
  snapshot. Reason: Snapshot operation not allowed due to clones backed by
  snapshots. Try again after sometime.
  ```

  Per informazioni su come risolvere questo problema, fare riferimento a: "Operazione Snapshot non consentita a causa di cloni supportati da snapshot".

Eseguire il backup dei database SAP HANA nativi del cloud

Avvio rapido

Inizia subito seguendo questa procedura.

1 **Verificare il supporto per la configurazione**

- Sistema operativo:
  - RHEL 7.6 o versione successiva
  - RHEL 8.1 o versione successiva per SAP-HANA SPS07
  - SLES 12 SP5 o versioni successive e 15 piattaforme SPX certificate da SAP HANA
- Storage cloud NetApp: Azure NetApp Files
- Layout dello storage: Per i file di dati e log, Azure supporta solo NFSv4.1.
- Layout del database:
  - SAP HANA Multitenant Database Container (MDC) 2.0SPS5, 2.0SPS6, 2.0SPS7 con tenant singoli o multipli
  - Sistema host singolo SAP HANA, sistema host multiplo SAP HANA, replica di sistema HANA
- Plug-in SAP HANA sull'host del database

2 **Iscriviti a BlueXP**

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a. "Iscriviti a BlueXP".

3 **Accedere a BlueXP**

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a. "Accedere a BlueXP".

4 **Gestisci il tuo account BlueXP**

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a. "Gestisci il tuo account BlueXP".

Configurare Azure NetApp Files

Con BlueXP è necessario creare un ambiente di lavoro Azure NetApp Files per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Azure NetApp Files

È necessario creare ambienti di lavoro Azure NetApp Files in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. "Scopri di più su Azure NetApp Files" e. "Creare un ambiente di lavoro Azure NetApp Files".

Creare un connettore

Un amministratore di account BlueXP dovrebbe implementare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. "Creare un connettore in Azure da BlueXP".

- Assicurarsi che vi sia connettività tra il connettore e gli host del database.
- Se si dispone dell'ambiente di lavoro e dei database Azure NetApp Files nella stessa rete virtuale (VNET), è possibile implementare il connettore nella stessa rete virtuale.
- Se si dispone di un ambiente di lavoro Azure NetApp Files e di database in reti VNet diverse e si hanno carichi di lavoro NAS (NFS) configurati su Azure NetApp Files, è possibile creare il connettore su una delle reti VNet.

Dopo aver creato il connettore, aggiungere l'ambiente di lavoro facendo clic su **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment**.

Installare il plug-in SnapCenter per SAP HANA e aggiungere host di database

Installare il plug-in SnapCenter per SAP HANA su ciascuno degli host di database SAP HANA. A seconda che l'host SAP HANA disponga di un'autenticazione basata su chiave SSH abilitata, è possibile seguire uno dei metodi per installare il plug-in.

- Se SSH è attivato per l'host del database, è possibile installare il plug-in utilizzando l'opzione SSH. Scopri di più.
- Se SSH è disattivato, installare il plug-in manualmente. Scopri di più.

Prerequisiti

Prima di aggiungere l'host, assicurarsi che i prerequisiti siano soddisfatti.

- Assicurarsi che Java 11 (64 bit) Oracle Java o OpenJDK sia installato su ciascuno degli host di database SAP HANA.
- L'ambiente di lavoro dovrebbe essere stato aggiunto e il connettore dovrebbe essere stato creato.
- Assicurarsi che il connettore sia connesso agli host del database SAP HANA.

  Per informazioni su come risolvere il problema di connettività, fare riferimento a. "Impossibile convalidare la connettività dall'host del connettore BlueXP all'host del database dell'applicazione".

  Quando il connettore viene perso o se è stato creato un nuovo connettore, è necessario associarlo alle risorse dell'applicazione esistenti. Per istruzioni sull'aggiornamento del connettore, vedere "Aggiornare i dettagli del connettore".

- Assicurarsi che l'utente BlueXP abbia il ruolo di "account Admin".
- Si dovrebbe aver creato l'utente SnapCenter e configurato sudo per l'utente non root (sudo). Per ulteriori informazioni, fare riferimento a. "Configurare sudo per l'utente SnapCenter."
- Prima di aggiungere l'host di database, è necessario aver installato il plug-in SnapCenter per SAP HANA.
- Durante l'aggiunta degli host di database SAP HANA, è necessario aggiungere le chiavi dell'archivio utente HDB. La chiave di archivio utente sicura HDB viene utilizzata per memorizzare le informazioni di connessione degli host di database SAP HANA in modo sicuro sul client e il client HDBSQL utilizza la chiave di archivio utente sicura per connettersi all'host di database SAP HANA.
- Per la replica del sistema HANA (HSR), per proteggere i sistemi HANA, è necessario registrare manualmente i sistemi HANA primario e secondario.

  > Il nome host deve essere uguale a quello dell'host utilizzato nella replica HSR.

- Se viene eseguita l'installazione basata su SSH, assicurarsi che il connettore abbia attivato la comunicazione con la porta SSH (impostazione predefinita: 22).
- Assicurarsi che il connettore abbia la comunicazione abilitata alla porta plug-in (impostazione predefinita: 8145) per il funzionamento delle operazioni di protezione dei dati.
- Assicurarsi che sia installata la versione più recente del plug-in. Per aggiornare il plug-in, fare riferimento a. Upgrade del plug-in SnapCenter per il database SAP HANA.

Configurare sudo per l'utente SnapCenter

Creare un utente non root (sudo) per installare il plug-in.

Fasi

1. Accedere a Connector VM.
2. Scarica il binario del plug-in host Linux di SnapCenter.
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```

3. Copiare il contenuto di **sudoer.txt** situato all'indirizzo: */var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po "cloudmanager_scs_cloud:.*? "|sed -e/ */"|cut -f2 -d":")/sc-linux-host-plugin*
4. Accedere all'host di sistema SAP HANA utilizzando l'account utente root.
5. Configurare l'accesso sudo per l'utente non root copiando il testo copiato nel passaggio 3 nel file */etc/sudoers.d/snapcenter*.

   Nelle righe aggiunte al file */etc/sudoers.d/snapcenter*, sostituire *<LINUXUSER>* con l'utente non root e *<USER_HOME_DIRECTORY>* con *home/<non-root-user>*.

Installare il plug-in utilizzando lo script

Configurare l'autenticazione basata su chiave SSH per l'account utente non root dell'host SAP HANA ed eseguire i seguenti passaggi per installare il plug-in.

Prima di iniziare

Assicurarsi che la connessione SSH al connettore sia attivata.

Fasi

1. Accedere a Connector VM.
2. Installare il plug-in utilizzando lo script fornito nel connettore.
   ```
   sudo bash /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

   Se si utilizza un connettore meno recente, eseguire il seguente comando per installare il plug-in.
   ```
   sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

Nome	Descrizione	Obbligatorio	Predefinito
plugin_host	Specifica l'host SAP HANA	Sì	-
nome_utente_host	Specifica l'utente SnapCenter con privilegi SSH sull'host SAP HANA	Sì	-
host_ssh_key	Specifica la chiave SSH dell'utente SnapCenter e viene utilizzata per connettersi all'host SAP HANA	Sì	-
porta_plugin	Specifica la porta utilizzata dal plug-in	No	8145

Nome	Descrizione	Obbligatorio	Predefinito
host_ssh_port	Specifica la porta SSH sull'host SAP HANA	No	22

Ad esempio, `sudo bash /var/lib/docker/Volumes/service-manager-2_cloud_manager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --Username SnapCenter --sshkey /keys/netapp-ssh.ppk

Dopo aver installato il plug-in, è necessario Aggiunta di host di database SAP HANA.

Installare il plug-in manualmente

Se l'autenticazione basata su chiave SSH non è abilitata sull'host HANA, attenersi alla procedura manuale riportata di seguito per installare il plug-in.

Fasi

1. Accedere a Connector VM.
2. Scarica il binario del plug-in host Linux di SnapCenter.
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```
   Il binario del plug-in è disponibile all'indirizzo: *cd /var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/€(sudo docker ps|grep -po "cloudmanager_scs_cloud:.*? "|sed -e/ */"|cut -f2 -d":")/sc-linux-host-plugin*
3. Copiare *snapcenter_linux_host_plugin_scs.bin* dal percorso sopra indicato al percorso */home/<non root user (sudo)>/.sc_netapp* per ciascuno degli host di database SAP HANA utilizzando metodi SCP o altri metodi alternativi.
4. Accedere all'host del database SAP HANA utilizzando l'account non root (sudo).
5. Modificare la directory in */home/<non root user>/.sc_netapp/* ed eseguire il seguente comando per abilitare le autorizzazioni di esecuzione per il file binario.
   ```
   chmod +x snapcenter_linux_host_plugin_scs.bin
   ```
6. Installare il plug-in SAP HANA come utente sudo SnapCenter.
   ```
   ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
   ```
7. Copiare *certificate.pem* dal percorso *<base_mount_path>/client/certificate/* del connettore VM a */var/opt/snapcenter/spl/etc/* sull'host plug-in.
8. Passare a */var/opt/snapcenter/spl/etc* ed eseguire il comando keytool per importare il certificato.
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
   -deststorepass snapcenter -noprompt
   ```
9. Riavviare SPL: `systemctl restart spl`
10. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.
    ```
    docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
    plug-in host>:<plug-in port>/PluginService/Version --cert
    config/client/certificate/certificate.pem --key
    /config/client/certificate/key.pem
    ```

Dopo aver installato il plug-in, è necessario Aggiunta di host di database SAP HANA.

Upgrade del plug-in SnapCenter per il database SAP HANA

È necessario aggiornare il plug-in SnapCenter per il database SAP HANA per accedere alle nuove funzionalità e ai miglioramenti più recenti.

Prima di iniziare

- Assicurarsi che non vi siano operazioni in esecuzione sull'host.

Fasi

1. Configurare sudo per l'utente SnapCenter. Per ulteriori informazioni, vedere Configurare sudo per l'utente SnapCenter.
2. Eseguire il seguente script.
   ```
   /var/lib/docker/volumes/service-manager-
   2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
   --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
   --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
   ```

   Se si utilizza un connettore meno recente, eseguire il seguente comando per aggiornare il plug-in.
   ```
   /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
   in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
   --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   --upgrade
   ```

Aggiunta di host di database SAP HANA

È necessario aggiungere manualmente gli host di database SAP HANA per assegnare policy e creare backup. Il rilevamento automatico dell'host del database SAP HANA non è supportato.

Fasi

1. Nell'interfaccia utente **BlueXP**, selezionare **protezione** > **Backup e ripristino** > **applicazioni**.
2. Selezionare **trova applicazioni**.
3. Selezionare **Cloud Native** > **SAP HANA** e selezionare **Next**.
4. Nella pagina **applicazioni**, selezionare **Aggiungi sistema**.
5. Nella pagina **Dettagli sistema**, eseguire le seguenti operazioni:
   a. Selezionare tipo di sistema come container di database multi-tenant o volumi non dati globali.
   b. Inserire il nome del sistema SAP HANA.
   c. Specificare il SID del sistema SAP HANA.
   d. (Facoltativo) modificare l'utente OSDB.
   e. Se il sistema HANA è configurato con la replica del sistema HANA, attivare **sistema di replica del sistema HANA (HSR)**.
   f. Selezionare la casella di testo **HDB Secure User Store Keys** per aggiungere i dettagli dei tasti di memorizzazione utente.

Specificare il nome della chiave, i dettagli del sistema, il nome utente e la password e fare clic su **Aggiungi chiave**.

È possibile eliminare o modificare le chiavi dell'archivio utente.

6. Selezionare **Avanti**.
7. Nella pagina **Dettagli host**, effettuare le seguenti operazioni:
   a. Selezionare **Aggiungi nuovo host** o **Usa host esistente**.
   b. Selezionare **usando SSH** o **Manuale**.

      Per Manuale, immettere il FQDN host o IP, connettore, Nome utente, porta SSH, porta plug-in, e, facoltativamente, aggiungere e convalidare la chiave privata SSH.

   Per SSH, immettere il nome host FQDN o IP, Connector, Username e plug-in port.

   a. Selezionare **Avanti**.
8. Nella pagina **Configurazione host**, verificare se i requisiti di configurazione sono soddisfatti.

   Selezionare le caselle di controllo per confermare.

9. Selezionare **Avanti**.
10. Nella pagina **Storage Footprint**, selezionare **Aggiungi archiviazione** ed eseguire le seguenti operazioni:
    a. Selezionare l'ambiente di lavoro e specificare l'account NetApp.

       Dal riquadro di navigazione a sinistra, selezionare BlueXP **Canvas** per aggiungere un nuovo ambiente di lavoro.

    b. Selezionare i volumi richiesti.
    c. Selezionare **Aggiungi archiviazione**.
11. Controllare tutti i dettagli e selezionare **Aggiungi sistema**.

È possibile modificare o rimuovere i sistemi SAP HANA dall'interfaccia utente.

Prima di rimuovere il sistema SAP HANA, è necessario eliminare tutti i backup associati e rimuovere la protezione.

Aggiungere volumi non dati

Dopo aver aggiunto il sistema SAP HANA di tipo container di database multi-tenant, è possibile aggiungere i volumi non-Data del sistema HANA.

È possibile aggiungere queste risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database SAP HANA disponibili.

Fasi

1. Nell'interfaccia utente **BlueXP**, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** > **SAP HANA** e fare clic su **Avanti**.
4. Nella pagina **applicazioni**, fare clic su ••• Corrispondente al sistema per cui si desidera aggiungere volumi

non dati e selezionare **Manage System** (Gestisci sistema) > **non-Data Volume** (Volume non dati).

Aggiungere volumi non dati globali

Dopo aver aggiunto il sistema SAP HANA di tipo container di database multi-tenant, puoi aggiungere i Global non-Data Volumes del sistema HANA.

Fasi

1. Nell'interfaccia utente **BlueXP**, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** > **SAP HANA** e fare clic su **Avanti**.
4. Nella pagina **applicazioni**, fare clic su **Aggiungi sistema**.
5. Nella pagina **Dettagli sistema**, eseguire le seguenti operazioni:
   a. Dal menu a discesa System Type (tipo di sistema), selezionare **Global non-Data Volume** (Volume non dati globale).
   b. Inserire il nome del sistema SAP HANA.
6. . Nella pagina **Dettagli host**, effettuare le seguenti operazioni:
   a. Specificare i SID associati al sistema SAP HANA.
   b. Selezionare l'host del plug-in
   c. Fare clic su **Avanti**.
   d. Esaminare tutti i dettagli e fare clic su **Aggiungi sistema**.

Eseguire il backup dei database SAP HANA nativi del cloud

È possibile creare un backup assegnando un criterio predefinito o il criterio creato.

Creare una policy per proteggere il database SAP HANA

È possibile creare policy se non si desidera utilizzare o modificare le policy predefinite.

1. Nella pagina **applicazioni**, dall'elenco a discesa Impostazioni, selezionare **Criteri**.
2. Fare clic su **Crea policy**.
3. Specificare un nome di policy.
4. (Facoltativo) modificare il formato del nome della copia Snapshot.
5. Selezionare il tipo di policy.
6. Specificare la pianificazione e i dettagli di conservazione.
7. (Facoltativo) specificare gli script. "Prescrizioni e post-script."
8. Fare clic su **Create** (Crea).

Prescrizioni e post-script

Durante la creazione di un criterio, è possibile fornire prescritture, postscript e script di uscita. Questi script vengono eseguiti sull'host HANA durante l'operazione di protezione dei dati.

Il formato supportato per gli script è .sh, python script, perl script e così via.

Il prescrittt e il postscript devono essere registrati dall'amministratore host in `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` file.

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

Variabili ambientali

Per il flusso di lavoro di backup, le seguenti variabili ambientali sono disponibili come parte di Prespt e postscript.

Variabile ambientale	Descrizione
SID	L'identificatore di sistema del database HANA scelto per il ripristino
BackupName	Nome del backup scelto per l'operazione di ripristino
UserStoreKeyNames	Chiave userstore configurata per il database HANA
OSDBUser	Configurato OSDBUser per il database HANA
Nome criterio	Solo per backup pianificati
tipo_pianificazione	Solo per backup pianificati

Creare un backup del database SAP HANA

È possibile assegnare un criterio predefinito o creare un criterio e assegnarlo al database. Una volta assegnato il criterio, i backup vengono creati in base alla pianificazione definita nel criterio.

Prima di iniziare

Dovrebbero essere stati aggiunti gli host del database SAP HANA."Aggiunta di host di database SAP HANA"

A proposito di questa attività

Per HANA System Replication (HSR), il processo di backup pianificato viene attivato solo per il sistema HANA primario e se il sistema esegue il failover verso il sistema HANA secondario, i programmi esistenti attivano un backup sul sistema HANA primario corrente. Se il criterio non viene assegnato al sistema HANA primario e secondario, dopo il failover, le pianificazioni non avranno esito positivo.

Se ai sistemi HSR vengono assegnati criteri diversi, il backup pianificato viene attivato per i sistemi HANA primario e secondario e il backup non viene eseguito per il sistema HANA secondario.

Fasi

1. Nella pagina applicazioni, se il database non è protetto mediante criteri, fare clic su **Assegna policy**.

Sebbene il database sia protetto mediante uno o più criteri, se necessario, è possibile continuare ad assegnare ulteriori criteri facendo clic su ••• > **Assegna policy**.

2. Selezionare il criterio e fare clic su **Assegna**.

   I backup vengono creati in base alla pianificazione definita nel criterio.

   > L'account del servizio (*SnapCenter-account-<account_id>*) viene utilizzato per eseguire le operazioni di backup pianificate.

Creazione di backup on-demand del database SAP HANA

Dopo aver assegnato il criterio, è possibile creare un backup on-demand dell'applicazione.

Fasi

1. Nella pagina **applicazioni**, fare clic su ••• Corrispondente all'applicazione e fare clic su **Backup on-Demand**.
2. Selezionare il tipo di backup on-demand.
3. Per il backup basato su policy, selezionare il criterio, il livello di conservazione e fare clic su **Create Backup** (Crea backup).
4. Per una volta, selezionare Snapshot copy based (basato su copia Snapshot) o file based (basato su file), attenersi alla seguente procedura:
   a. Selezionare il valore di conservazione e specificare il nome del backup.
   b. (Facoltativo) specificare gli script e il percorso per gli script.

      Per ulteriori informazioni, vedere "Prescritture e postscript"

   c. Fare clic su **Create Backup** (Crea backup).

Eseguire il backup di database SQL Server nativi per il cloud utilizzando le API REST

Avvio rapido

Inizia subito seguendo questa procedura.

1 **Verificare il supporto per la configurazione**

- Sistema operativo:
  - Windows 2016
  - Windows 2019
  - Windows 2022
- Cloud storage NetApp: Amazon FSX per NetApp ONTAP
- Layout dello storage: SAN (ISCSI)

  La configurazione NAS non è supportata.

- Versioni database:
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2022
- Configurazione database:
  - Standalone

2 Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a. "Iscriviti a BlueXP".

3 Accedere a BlueXP

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a. "Accedere a BlueXP".

4 Gestisci il tuo account BlueXP

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a. "Gestisci il tuo account BlueXP".

Configurare FSX per ONTAP

Con BlueXP è necessario creare un ambiente di lavoro FSX per ONTAP per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro FSX per ONTAP

È necessario creare FSX per ambienti di lavoro ONTAP in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. "Inizia a utilizzare Amazon FSX per ONTAP" e. "Creare e gestire un ambiente di lavoro Amazon FSX per ONTAP".

È possibile creare l'ambiente di lavoro FSX per ONTAP utilizzando BlueXP o AWS. Se hai creato utilizzando AWS, dovresti scoprire FSX per i sistemi ONTAP in BlueXP.

Creare un connettore

Un account Admin deve creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. "Creazione di un connettore in AWS da BlueXP".

- È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro FSX per ONTAP che i database.

- Se si dispone dell'ambiente di lavoro FSX per ONTAP e dei database nello stesso cloud privato virtuale (VPC), è possibile implementare il connettore nello stesso VPC.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e di database in diversi VPC:
  - Se si dispone di carichi di lavoro NAS (NFS) configurati su FSX per ONTAP, è possibile creare il connettore su uno dei VPC.
  - Se si hanno solo carichi DI lavoro SAN configurati e non si intende utilizzare carichi di lavoro NAS (NFS), è necessario creare il connettore nel VPC in cui viene creato il sistema FSX per ONTAP.

> Per utilizzare i carichi di lavoro NAS (NFS), è necessario disporre di un gateway di transito tra il VPC del database e Amazon VPC. È possibile accedere all'indirizzo IP NFS, che è un indirizzo IP mobile, da un altro VPC solo attraverso il gateway di transito. Non è possibile accedere agli indirizzi IP mobili eseguendo il peering dei VPC.

Dopo aver creato il connettore, fare clic su **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni per aggiungere l'ambiente di lavoro. Assicurarsi che vi sia connettività dal connettore agli host del database Oracle e all'ambiente di lavoro FSX. Il connettore dovrebbe essere in grado di connettersi all'indirizzo IP di gestione del cluster dell'ambiente di lavoro FSX.

- Aggiungere l'ambiente di lavoro facendo clic su **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment**.

  Assicurarsi che vi sia connettività dal connettore agli host del database e all'ambiente di lavoro FSX per ONTAP. Il connettore deve connettersi all'indirizzo IP di gestione del cluster di FSX per l'ambiente di lavoro ONTAP.

- Copiare l'ID del connettore facendo clic su **Connector > Manage Connectors** (connettore > Gestisci connettori) e selezionando il nome del connettore.

Installare il plug-in SnapCenter per SQL Server e aggiungere host di database

È necessario installare il plug-in di SnapCenter per SQL Server su ciascuno degli host del database SQL, aggiungere gli host del database, rilevare le istanze del database e configurare le credenziali per le istanze del database.

Installare il plug-in SnapCenter per SQL Server

È necessario scaricare il plug-in **snapcenter_service_Windows_host_plugin.exe** e quindi eseguire il comando silent installer per installare il plug-in sull'host del database.

Prima di iniziare

- È necessario verificare che siano soddisfatti i seguenti prerequisiti.
  - È installato .Net 4.7.2
  - Viene installato PowerShell 4,0
  - È disponibile uno spazio minimo su disco di 5 GB
  - È disponibile una dimensione minima di 4 GB di RAM
- È necessario eseguire l'API per completare l'assunzione del cliente. Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Tenant%20Registration/createTenant

Fasi

1. Scaricare il plug-in eseguendo l'API dall'host del connettore.
   ```
   docker exec -it cloudmanager_scs_cloud curl
   'http://127.0.0.1/api/v2/pluginpackage/windows'
   ```

   La posizione del file è */var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/<agent_version>/sc-Windows-host-plugin/snapcenter_service_Windows_host_plugin.exe*.

2. Copiare *snapcenter_service_Windows_host_plugin.exe* dal connettore a ciascuno degli host del database MSSQL Server utilizzando SCP o altri metodi alternativi.
3. Installare il plug-in.
   '"C://<install_folder>/snapcenter_service_Windows_host_plugin.exe"/silent/debuglog "C://<install_folder>/ha_Suite_Silent_Install_SCSQL_FRESH.log" /log"C://install_folder/" BI_SNAPCENTER_PORT=8145 ISFeatureInstall=SCSQL'
4. Copiare il certificato autofirmato da */var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/client/certificate/certificate.pem* negli host del database di MSSQL Server.

   È inoltre possibile generare un certificato autofirmato o un certificato CA firmato se non si utilizza quello predefinito.

5. Convertire il certificato dal formato .pem al formato .crt nell'host del connettore.
   'openssl x509 -outform der -in certificate.pem -out certificate.crt'
6. Fare doppio clic sul certificato per aggiungerlo all'archivio **Personal** e **Trusted Root Certification Authority**.

Aggiungere l'host del database SQL Server

È necessario aggiungere l'host del database MSSQL utilizzando l'FQDN host.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/AddHosts

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
addr	stringa	Vero
id_connettore	stringa	Vero
plugin_type	stringa	Vero
metodo_installazione	stringa	Vero

Nome	Tipo	Obbligatorio
porta_plugin	numero	Vero
nome utente	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Visualizzare gli host del database SQL Server aggiunti

È possibile eseguire questa API per visualizzare tutti gli host di database SQL Server aggiunti.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/GetHosts

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```
{
  "num_records": 1,
    "total_records": 1,
    "records": [
        {
            "id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "addr": "scspa2722211001.rtp.openenglab.netapp.com",
            "status": "Running",
            "connector_id": "fBf8Iwbp4BscBfD02qBwWm6I03gGAesRclients",
            "plugin_port": 8145,
            "plugins": [
                {
                    "type": "mssql"
                }
            ],
            "os_type": "windows",
            "platform": "onprem",
            "username": "administrator",
            "operating_mode": "production"
        }
    ],
    "_links": {
        "next": {}
    }
}
```


Rilevare le istanze del database

È possibile eseguire questa API e immettere l'ID host per rilevare tutte le istanze MSSQL.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/MSSQLInstancesDiscoveryRequest

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametro

Nome	Tipo	Obbligatorio
host_id	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Visualizzare le istanze del database rilevate

È possibile eseguire questa API per visualizzare tutte le istanze del database rilevate.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/GetMSSQLInstancesRequest

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```
{
    "num_records": 2,
    "total_records": 2,
    "records": [
        {
            "id": "953e66de-10d9-4fd9-bdf2-bf4b0eaabfd7",
            "name": "scspa2722211001\\NAMEDINSTANCE1",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Running",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        },
        {
            "id": "18e1b586-4c89-45bd-99c8-26268def787c",
            "name": "scspa2722211001",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Stopped",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        }
    ],
    "_links": {
        "next": {}
    }
}
```


Configurare le credenziali dell’istanza del database

È possibile eseguire questa API per convalidare e impostare le credenziali per le istanze del database.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/ConfigureCredentialRequest

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell’interfaccia utente di BlueXP.

Parametro

Nome	Tipo	Obbligatorio
host_id	stringa	Vero
id_istanza	stringa	Vero
nome utente	stringa	Vero
password	stringa	Vero
auth_mode	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Eseguire il backup di database Microsoft SQL Server nativi per il cloud

È possibile creare backup pianificati o su richiesta assegnando i criteri creati.

Creare un criterio di backup

È possibile eseguire questa API per creare il criterio di backup.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService_CreateMSSQLBackupPolicy

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
nome	stringa	Vero
tipo_backup	stringa	Vero
copia_solo_backup	stringa	Falso
è_definito_sistema	stringa	Falso
formato_nome_backup	stringa	Vero
tipo_pianificazione	stringa	Vero
ora_inizio	numero	Vero
hours_interval	numero	Vero
minuti_intervallo	numero	Vero
retention_type	stringa	Vero
retention_count	numero	Vero
ora_fine	numero	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 201.

Esempio:

```
{
    "_links": {
    "self": {
        "href": "/api/resourcelink"
      }
    }
}
```

Assegnare il criterio all'istanza del database SQL

È possibile eseguire questa API per assegnare i criteri all'istanza del database SQL.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/{id}/policy-assignment'

Dove *id* è l'ID istanza MSSQL ottenuto eseguendo l'API dell'istanza del database Discover. Per ulteriori informazioni, fare riferimento a. "Rilevare le istanze del database".

Array di ID è l'input qui. Ad esempio:

```
[
  "c9f3e68d-1f9c-44dc-b9af-72a9dfc54320"
]
```

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Policy%20Assignment/PostMSSQLInstanceAssignPolicyRequest

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Crea un backup su richiesta

Puoi eseguire questa API per creare un backup on-demand.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/CreateMSSQLBackupRequest

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
id Questo è l'ID dell'istanza del database MSSQL.	stringa	Vero
tipo_risorsa	stringa	Vero
policy_id	stringa	Vero
tipo_pianificazione	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Visualizzare i backup

È possibile eseguire queste API per visualizzare l'elenco di tutti i backup e per visualizzare i dettagli di un particolare backup.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups'

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups/{id}'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/MSSQLGetBackupsRequest

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```
{
    "total_records": 1,
    "num_records": 1,
    "records": [
        {
            "backup_id": "602d7796-8074-43fc-a178-eee8c78566ac",
            "resource_id": "a779578d-cf78-46f3-923d-b9223255938c",
            "backup_name":
"Hourly_policy2_scspa2722211001_NAMEDINSTANCE1_2023_08_08_07_02_01_81269_0
",
            "policy_name": "policy2",
            "schedule_type": "Hourly",
            "start_time": "2023-08-08T07:02:10.203Z",
            "end_time": "0001-01-01T00:00:00Z",
            "backup_status": "success",
            "backup_type": "FullBackup"
        }
    ],
    "_links": {
        "next": {}
    }
}
```


Ripristinare i database Oracle nativi del cloud

Ripristinare i database Oracle nativi del cloud nella posizione originale

In caso di perdita di dati, è possibile ripristinare i file di dati, i file di controllo o entrambi nella posizione originale e quindi ripristinare il database.

Prima di iniziare

Se il database Oracle 21c è IN stato AVVIATO, l'operazione di ripristino non riesce. Eseguire il seguente comando per ripristinare correttamente il database.

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
/opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
```

Fasi

1. Fare clic su ••• Corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
2. Selezionare il punto di ripristino in cui ripristinare il database e fare clic su **Restore to original location** (Ripristina posizione originale).
3. Nella sezione ambito ripristino, eseguire le seguenti operazioni:

Se…	Eseguire questa operazione…
Ripristinare solo i file di dati	Selezionare **tutti i file di dati**.

Se…	Eseguire questa operazione…
Ripristinare solo i file di controllo	Selezionare **file di controllo**
Ripristinare sia i file di dati che i file di controllo	Selezionare **tutti i file di dati** e **file di controllo**.

È inoltre possibile selezionare la casella di controllo **Imponi ripristino in-place**.

Nel layout di Amazon FSX per NetApp ONTAP o SAN Cloud Volumes ONTAP, se il plug-in SnapCenter per Oracle trova file esterni diversi dai file di dati Oracle sul gruppo di dischi ASM, viene eseguito il metodo di ripristino connessione e copia. I file esterni possono essere di uno o più dei seguenti tipi:

- Parametro
- Password
- log di archiviazione
- log online
- File dei parametri ASM.

  L'opzione **Imponi ripristino in-place** sovrascrive i file esterni di tipo parametro, password e log di archiviazione. Utilizzare il backup più recente quando è selezionata l'opzione **Force in-place restore** (forza ripristino in-place).

4. Nella sezione ambito ripristino, eseguire le seguenti operazioni:

Se…	Eseguire questa operazione…
Ripristinare l'ultima transazione	Selezionare **tutti i registri**.
Ripristinare un numero SCN (System Change Number) specifico	Selezionare **fino a SCN** e specificare il numero SCN.
Ripristinare una data e un'ora specifiche	Selezionare **Data e ora**.
Non si desidera eseguire il ripristino	Selezionare **Nessun ripristino**.

   Per l'ambito di ripristino selezionato, nel campo **Archive Log Files Locations** (posizioni file registro archivio) è possibile specificare la posizione che contiene i registri di archiviazione richiesti per il ripristino.

   Selezionare questa casella di controllo se si desidera aprire il database in modalità DI LETTURA/SCRITTURA dopo il ripristino.

5. Fare clic su **Avanti** e rivedere i dettagli.
6. Fare clic su **Restore** (Ripristina).

Ripristinare i database Oracle nativi del cloud in una posizione alternativa

In caso di perdita di dati, è possibile ripristinare il database Oracle in una posizione alternativa solo su Azure NetApp Files. La posizione alternativa può trovarsi su un host

diverso o sullo stesso host.

Prima di iniziare

- Se il database Oracle 21c è IN stato AVVIATO, l'operazione di ripristino non riesce. Eseguire il seguente comando per ripristinare correttamente il database.
  ```
  cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
  /opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
  ```
- Assicurarsi che la versione di Oracle sull'host alternativo sia uguale a quella dell'host originale.

A proposito di questa attività

Durante l'avvio dell'operazione di ripristino, non è consentito modificare le configurazioni ad eccezione di Oracle home, throughput massimo del volume, SID Oracle e credenziali del database.

Il ripristino completo è attivato per impostazione predefinita con l'opzione *until CANCEL* impostata su true.

Per impostazione predefinita, la modalità di registro archivio è disattivata per il database ripristinato. Se necessario, è possibile attivare la modalità di registrazione dell'archivio e mantenere i registri di archiviazione sul volume NetApp.

Fasi

1. Fare clic su ••• Corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
2. Selezionare il punto di ripristino in cui ripristinare il database e fare clic su **Restore to alternate location** > **Next**.
3. Nella pagina Configuration (Configurazione), specificare i dettagli relativi a posizione alternativa, SID, Oracle_Home, credenziali del database e throughput dello storage.

   Per la credenziale del database, se l'autenticazione utente del sistema operativo è disattivata, è necessario fornire una password per consentire all'utente sys di connettersi al database ripristinato sullo stesso host o su quello di destinazione.

4. Fare clic su **Avanti**, rivedere i dettagli e fare clic su **Ripristina**.

   L'avanzamento dell'operazione di ripristino può essere visualizzato nella pagina Job Monitor. Una volta completato il processo, fare clic su **Refresh Discovery** (Aggiorna rilevamento) per visualizzare il database ripristinato. Tuttavia, non è possibile proteggere il database ripristinato in una posizione alternativa.

Ripristinare i database SAP HANA nativi del cloud

In caso di perdita di dati, è possibile ripristinare i file di dati e non, quindi ripristinare il database.

Prima di iniziare

- Il sistema SAP HANA deve essere in stato di arresto.
- Se il sistema SAP HANA è attivo e in esecuzione, è possibile fornire una prescrizione per arrestare il sistema.

A proposito di questa attività

- Se si abilitano i backup ANF su un volume, viene eseguita l'operazione Single file SnapRestore.

- Per volumi non dati e volumi non dati globali, viene eseguita l'operazione di ripristino della connessione e della copia.
  - I valori QoS (Quality of Service) per le operazioni di connessione e ripristino delle copie vengono rilevati dai volumi di origine di volumi non dati o volumi non dati globali.

> QoS è applicabile solo per pool di capacità di tipo "Manuale".

Fasi

1. Fare clic su ••• Corrispondente al database che si desidera ripristinare e fare clic su **View Details** (Visualizza dettagli).
2. Fare clic su ••• Corrispondente al backup dei dati che si desidera ripristinare e fare clic su **Restore** (Ripristina).
3. Nella pagina **Restore System**, inserire gli script. "Prescrizioni e post-script."

   Per il flusso di lavoro di ripristino, le seguenti variabili ambientali sono disponibili come parte di Prespt e postscript.

Variabile ambientale	Descrizione
SID	L'identificatore di sistema del database HANA scelto per il ripristino
BackupName	Nome del backup scelto per l'operazione di ripristino
UserStoreKeyNames	Chiave userstore configurata per il database HANA
OSDBUser	Configurato OSDBUser per il database HANA

4. Fare clic su **Restore** (Ripristina).

Cosa c'è di nuovo

Dopo il ripristino, ripristinare manualmente il sistema SAP HANA o fornire un postscript, che esegue il ripristino del sistema SAP HANA.

Ripristina volume non dati

A proposito di questa attività

Per l'operazione di connessione e ripristino delle copie, accedere al portale Microsoft Azure, selezionare il volume, fare clic su **Edit** e attivare **Hide snapshot path**.

Fasi

1. Nella pagina **applicazioni**, selezionare Volume non dati dalla casella a discesa.
2. Fare clic su ••• Corrispondente al backup che si desidera ripristinare e fare clic su **Restore** (Ripristina).

Ripristinare il volume globale non dati

A proposito di questa attività

Per l'operazione di connessione e ripristino delle copie, accedere al portale Microsoft Azure, selezionare il volume, fare clic su **Edit** e attivare **Hide snapshot path**.

Fasi

1. Nella pagina **applicazioni**, fare clic sul Global non-Data Volume che si desidera ripristinare.
2. Fare clic su ••• Corrispondente al volume non dati globale che si desidera ripristinare e fare clic su **Restore** (Ripristina).

Ripristinare il database Microsoft SQL Server

È possibile ripristinare il database Microsoft SQL Server sullo stesso host. È necessario prima ottenere l'elenco dei database e poi ripristinare il database.

Visualizzare l'elenco dei database

È possibile eseguire questa API per visualizzare l'elenco dei database.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases'

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Databases/GetMSSQLDatabasesRequest

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```
{
    "num_records": 3,
    "total_records": 3,
    "records": [
        {
            "id": "348901e5-aeaa-419f-88b1-80240de3b1fe",
            "name": "DB4",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "c79d33ab-7322-4ed6-92f5-51ad7a6944e0",
            "name": "DB5",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "40d6f35a-f4fb-48bc-8e0a-0ac93ddf0888",
            "name": "model",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.015625,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "System",
            "recovery_mode": "Full"
        }
    ],
    "_links": {
        "next": {}
    }
}
```

Ripristinare e ripristinare il database MSSQL

È possibile eseguire questa API per ripristinare il database MSSQL.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases/{id}/restore'

Dove *id* è l'ID del database MSSQL ottenuto eseguendo l'API del database di visualizzazione. Per ulteriori informazioni, fare riferimento a. Visualizzare l'elenco dei database.

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Database%20Restore/RestoreMSSQLDatabaseRequest

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
id_backup	stringa	Vero
sovrascrivi_database	bool	Vero
retain_replication_settings	bool	Falso
modalità_ripristino	stringa Le stringhe supportate da 3 sono *Operational*, *nonoperational* e *ReadOnly*.	Vero
annulla_directory_file	stringa	Vero
restore_type	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Clonare i database Oracle nativi del cloud

Clonare concetti e requisiti

È possibile clonare un database Oracle residente su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP utilizzando il backup del database sull'host del database di origine o su un host alternativo. È possibile clonare il backup dai sistemi di storage primari.

Prima di clonare il database, è necessario comprendere i concetti dei cloni e assicurarsi che tutti i requisiti siano soddisfatti.

Requisiti per la clonazione di un database Oracle

Prima di clonare un database Oracle, è necessario assicurarsi che i prerequisiti siano stati completati.

- Dovrebbe essere stato creato un backup del database. La creazione dei dati online e il backup dei log dovrebbero essere stati effettuati correttamente per consentire l'esecuzione dell'operazione di cloning.
- Nel parametro asm_diskstring, configurare:
  - AFD:* se si utilizza ASMFD
  - ORCL:* se si utilizza ASMLIB
  - /Dev/<exact_device_location> se si utilizza ASMUDEV
- Se si crea il clone su un host alternativo, l'host alternativo deve soddisfare i seguenti requisiti:
  - Il plug-in deve essere installato sull'host alternativo.
  - Il software Oracle deve essere installato sull'host alternativo.
  - L'host clone dovrebbe essere in grado di rilevare LUN dallo storage se si clonano database che risiedono su storage SAN iSCSI. Se si esegue la clonazione su un host alternativo, assicurarsi che sia stata stabilita una sessione iSCSI tra lo storage e l'host alternativo.
  - Se il database di origine è un database ASM:
    - L'istanza di ASM deve essere attiva e in esecuzione sull'host in cui verrà eseguito il clone.
    - Il provisioning del gruppo di dischi ASM deve essere eseguito prima dell'operazione di clonazione se si desidera inserire i file di log di archiviazione del database clonato in un gruppo di dischi ASM dedicato.

- Il nome del gruppo di dischi dati può essere configurato, ma assicurarsi che il nome non sia utilizzato da altri gruppi di dischi ASM sull'host in cui verrà eseguito il clone.
- I file di dati che risiedono sul gruppo di dischi ASM vengono forniti come parte del flusso di lavoro dei cloni.

Limitazioni

- La clonazione dei database residenti su Azure NetApp Files non è supportata.
- La clonazione dei database residenti su Qtree non è supportata.
- Il backup di un database clonato non è supportato.
- Se su Amazon FSX per NetApp ONTAP sono attivati backup automatici giornalieri, i volumi clonati su Amazon FSX per NetApp ONTAP non possono essere cancellati dall'interfaccia utente di BlueXP perché FSX avrebbe creato backup sui volumi clonati.
  È necessario eliminare i volumi clonati dopo aver eliminato tutti i backup del volume dall'interfaccia utente FSX e quindi eliminare i cloni dall'interfaccia utente BlueXP utilizzando l'opzione force.

Metodi di clonazione

È possibile creare un clone utilizzando il metodo di base o il file di specifica del clone.

Clonare utilizzando il metodo di base

È possibile creare il clone con le configurazioni predefinite in base al database di origine e al backup selezionato.

- I parametri del database, home e utente del sistema operativo vengono impostati per impostazione predefinita sul database di origine.
- I percorsi dei file di dati vengono denominati in base allo schema di denominazione selezionato.
- Non è possibile specificare le istruzioni pre-script, post-script e SQL.
- Per impostazione predefinita, l'opzione di ripristino è **fino all'annullamento** e utilizza il backup del registro associato al backup dei dati per il ripristino

Clonare utilizzando il file delle specifiche

È possibile definire le configurazioni nel file di specifica del clone e utilizzarlo per clonare il database. È possibile scaricare il file delle specifiche, modificarlo in base alle proprie esigenze e quindi caricarlo. "Scopri di più".

I diversi parametri definiti nel file delle specifiche e modificabili sono i seguenti:

Parametro	Descrizione
control_files	Posizione dei file di controllo per il database clone. Il numero di file di controllo sarà lo stesso del database di origine. Se si desidera eseguire l'override del percorso del file di controllo, è possibile specificare un percorso diverso del file di controllo. Il file system o il gruppo di dischi ASM dovrebbe esistere sull'host.

Parametro	Descrizione
redo_logs	Posizione, dimensione, numero di gruppi di ripristino dei log di ripristino. Per clonare il database sono necessari almeno due gruppi di log di ripristino. Se si desidera eseguire l'override del percorso del file di log di ripristino, è possibile personalizzare il percorso del file di log di ripristino in un file system diverso da quello del database di origine.il file system o il gruppo di dischi ASM dovrebbe esistere sull'host.
versione_oracle	Versione di Oracle sull'host di destinazione.
oracle_home	Oracle home sull'host di destinazione.
enable_archive_log_mode	Controlla la modalità del log di archiviazione per il database clone
parametri_database	Parametri del database per il database clonato
istruzioni_sql	Le istruzioni SQL da eseguire sul database dopo la clonazione
os_user_detail	Utente del sistema operativo Oracle nel database dei cloni di destinazione
porta_database	Porta utilizzata per comunicare con il database se l'autenticazione del sistema operativo è disattivata sull'host.
porta_asm	Porta utilizzata per la comunicazione con il database ASM se le credenziali sono fornite nell'input create clone.
skip_recovery	Non esegue l'operazione di recovery.
fino a scn	Recupera il database fino al numero scn (System Change Number) specificato.
fino a_ora	Recupera il database fino alla data e all'ora specificate. Il formato accettato è *mm/gg/aaaa hh:mm:ss*.

Parametro	Descrizione
until_cancel	Effettua il ripristino montando il backup del log associato al backup dei dati selezionato per la clonazione. Il database clonato viene recuperato fino a quando il file di log non è mancante o corrotto.
log_paths	Posizioni aggiuntive dei percorsi dei log di archiviazione da utilizzare per il ripristino del database clonato.
source_location	Posizione del gruppo di dischi o del punto di montaggio sull'host del database di origine.
clone_location	Posizione del gruppo di dischi o del punto di montaggio che deve essere creato sull'host di destinazione corrispondente alla posizione di origine.
location_type	Può essere ASM_diskgroup o mountpoint. I valori vengono compilati automaticamente al momento del download del file. Non modificare questo parametro.
pre_script	Script da eseguire sull'host di destinazione prima di creare il clone.
post_script	Script da eseguire sull'host di destinazione dopo la creazione del clone.
percorso	Percorso assoluto dello script sull'host clone. Lo script deve essere memorizzato in /var/opt/snapcenter/spl/scripts o in qualsiasi cartella all'interno di questo percorso.
timeout	Il tempo di timeout specificato per lo script in esecuzione sull'host di destinazione.
argomenti	Argomenti specificati per gli script.

Schema di naming dei cloni

Lo schema di naming dei cloni definisce la posizione dei punti di montaggio e il nome dei diskgroup del database clonato. È possibile selezionare **identico** o **generato automaticamente**.

Schema di denominazione identico

Se si seleziona lo schema di denominazione dei cloni come **identico**, la posizione dei punti di montaggio e il nome dei diskgroup del database clonato saranno gli stessi del database di origine.

Ad esempio, se il punto di montaggio del database di origine è */netapp_sourcedb/data_1 , +DATA1_DG*, per il database clonato il punto di montaggio rimane lo stesso sia per NFS che per ASM su SAN.

- Le configurazioni come il numero e il percorso dei file di controllo e dei file di ripristino saranno le stesse dell'origine.

  > Se i log di ripristino o i percorsi dei file di controllo si trovano nei volumi non dati, l'utente deve aver eseguito il provisioning del gruppo di dischi ASM o del punto di montaggio nell'host di destinazione.

- L'utente del sistema operativo Oracle e la versione di Oracle saranno le stesse del database di origine.
- Il nome del volume di storage clone avrà il seguente formato sourceVolNameSCS_Clone_CurrentTimeStampNumber.

  Ad esempio, se il nome del volume nel database di origine è *sourceVolName*, il nome del volume clonato sarà *sourceVolNameSCS_Clone_1661420020304608825*.

  > Il campo *CurrentTimeStampNumber* fornisce l'univocità nel nome del volume.

Schema di naming generato automaticamente

Se si seleziona lo schema di cloning come **generato automaticamente**, alla posizione dei punti di montaggio e al nome dei diskgroup del database clonato verrà aggiunto un suffisso.

- Se è stato selezionato il metodo di clone di base, il suffisso sarà **Clone SID**.
- Se è stato selezionato il metodo del file delle specifiche, il suffisso sarà il suffisso **suffisso** specificato durante il download del file delle specifiche del clone.

Ad esempio, se il punto di montaggio del database di origine è */netapp_sourcedb/data_1* e il **Clone SID** o il **suffisso** è *HR*, il punto di montaggio del database clonato sarà */netapp_sourcedb/data_1_HR*.

- Il numero di file di controllo e di log di ripristino sarà uguale a quello dell'origine.
- Tutti i file di log di ripristino e i file di controllo si trovano su uno dei punti di montaggio dati clonati o su gruppi di dischi ASM di dati.
- Il nome del volume di storage clone avrà il seguente formato sourceVolNameSCS_Clone_CurrentTimeStampNumber.

  Ad esempio, se il nome del volume nel database di origine è *sourceVolName*, il nome del volume clonato sarà *sourceVolNameSCS_Clone_1661420020304608825*.

  > Il campo *CurrentTimeStampNumber* fornisce l'univocità nel nome del volume.

- Il formato del punto di montaggio NAS sarà *SourceNASMountPoint_suffix*.
- Il formato del gruppo di dischi ASM sarà *SourceDiskgroup_suffix*.

Se il numero di caratteri nel gruppo di dischi clone è maggiore di 25, il numero di caratteri nel gruppo sarà *SC_hashCode_suffix*.

Parametri del database

Il valore dei seguenti parametri di database sarà uguale a quello del database di origine, indipendentemente dallo schema di denominazione dei cloni.

- log_archive_format
- audit_trail
- processi
- destinazione_aggregato_pga
- remote_login_passwordfile
- undo_tablespace
- open_cursors
- sga_target
- db_block_size

Al valore dei seguenti parametri di database viene aggiunto un suffisso basato sul SID clone.

- audit_file_dest = {sourcedatabase_parametervalue}_suffix
- log_archive_dest_1 = {sourcedatabase_oraclehome}_suffix

Variabili di ambiente predefinite supportate per il clone specifico prespt e postscript

È possibile utilizzare le variabili di ambiente predefinite supportate quando si eseguono prespt e postscript durante la clonazione di un database.

- SC_ORIGINAL_SID specifica il SID del database di origine. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: NFSB32
- SC_ORIGINAL_HOST specifica il nome dell'host di origine. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: asmrac1.gdl.englab.netapp.com
- SC_ORACLE_HOME specifica il percorso della home directory Oracle del database di destinazione. Esempio: /Ora01/app/oracle/product/18.1.0/db_1
- SC_BACKUP_NAME specifica il nome del backup. Questo parametro verrà popolato per i volumi dell'applicazione. Esempi:
  - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Se il database è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21- 2021_12.16.48.9267_07 12.16.48.9267_22_2021
- SC_ORIGINAL_OS_USER specifica il proprietario del sistema operativo del database di origine. Esempio: oracle
- SC_ORIGINAL_OS_GROUP specifica il gruppo del sistema operativo del database di origine. Esempio: Oinstall

- SC_TARGET_SID specifica il SID del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: Clonedb
- SC_TARGET_HOST specifica il nome dell'host in cui verrà clonato il database. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: asmrac1.gdl.englab.netapp.com
- SC_TARGET_OS_USER specifica il proprietario del sistema operativo del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Esempio: oracle
- SC_TARGET_OS_GROUP specifica il gruppo di sistemi operativi del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Esempio: Oinstall
- SC_TARGET_DB_PORT specifica la porta del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Esempio: 1521

Delimitatori supportati

- @ viene utilizzato per separare i dati dal nome del database e per separare il valore dalla chiave. Esempio: DATI@RG2_scspr2417819002_07-20- 2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- | viene utilizzato per separare i dati tra due entità diverse per il parametro SC_BACKUP_NAME. Esempio: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- , viene utilizzato per separare un insieme di variabili per la stessa chiave. Esempio: DATI@RG2_scspr2417819002_07-20- 2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21-2021_12.16.48.9267_1,RG2_scspr2417819002_07-22-2021_12.16.48.9267_1

Clonare i database Oracle nativi del cloud

È possibile clonare un database Oracle residente su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP utilizzando il backup del database sull'host del database di origine o su un host alternativo.

È possibile clonare i database per i seguenti motivi:

- Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto del database corrente durante i cicli di sviluppo dell'applicazione.
- Popolare i data warehouse utilizzando strumenti di estrazione e manipolazione dei dati.
- Per ripristinare i dati cancellati o modificati per errore.

Prima di iniziare

È necessario comprendere i concetti dei cloni e assicurarsi che tutti i requisiti siano soddisfatti. "Scopri di più".

Fasi

1. Fare clic su ••• Corrispondente al database che si desidera clonare e fare clic su **View Details** (Visualizza dettagli).
2. Fare clic su ••• Corrispondente al backup dei dati e fare clic su **Clone**.
3. Nella pagina Clone Details (Dettagli clone), selezionare una delle opzioni di clonazione.
4. A seconda dell'opzione selezionata, eseguire le seguenti operazioni:

Se si seleziona…	Eseguire questa operazione…
Di base	a. Selezionare l'host clone. Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e del sistema operativo dell'host del database di origine. b. Specificare il SID del clone. c. Selezionare lo schema di denominazione dei cloni. Se il database viene clonato nell'host di origine, lo schema di denominazione dei cloni viene generato automaticamente. Se il database viene clonato in un host alternativo, lo schema di naming dei cloni sarà identico. d. Specificare il percorso principale Oracle. e. (Facoltativo) specificare le credenziali del database. ◦ Credenziale del database: Se l'autenticazione utente del sistema operativo è disattivata, è necessario fornire una password per consentire all'utente sys di connettersi al database clonato sullo stesso host o su quello di destinazione. ◦ Credenziale ASM: Se l'autenticazione dell'utente del sistema operativo è disattivata sull'host di destinazione, è necessario fornire le credenziali dell'utente con privilegi sysasm per connettersi all'istanza ASM sull'host di destinazione. ⓘ Assicurarsi che il listener sia attivo e in esecuzione sull'host di destinazione. f. Fare clic su **Avanti**. g. Fare clic su **Clone**.

Se si seleziona…	Eseguire questa operazione…
File delle specifiche	a. Fare clic su **Download file** per scaricare il file delle specifiche. b. Selezionare lo schema di denominazione dei cloni. Se si seleziona, **generato automaticamente**, specificare il suffisso. c. Modificare il file delle specifiche in base ai requisiti e caricarlo facendo clic sul pulsante **Browse** (Sfoglia). d. Selezionare l'host clone. Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e del sistema operativo dell'host del database di origine. e. Specificare il SID del clone. f. (Facoltativo) specificare le credenziali del database. ◦ Credenziale del database: Se l'autenticazione utente del sistema operativo è disattivata, è necessario fornire una password per consentire all'utente sys di connettersi al database clonato sullo stesso host o su quello di destinazione. ◦ Credenziale ASM: Se l'autenticazione dell'utente del sistema operativo è disattivata sull'host di destinazione, è necessario fornire le credenziali dell'utente con privilegi sysasm per connettersi all'istanza ASM sull'host di destinazione. Assicurarsi che il listener sia attivo e in esecuzione sull'host di destinazione. g. Fare clic su **Avanti**. h. Fare clic su **Clone**.

5. Fare clic su + Accanto a **Filtra per** e seleziona **Clona opzioni** > **cloni** per visualizzare i cloni.

Aggiornare il sistema di destinazione SAP HANA

È possibile eseguire un refresh di un sistema di destinazione SAP HANA con i dati di un

sistema di origine SAP HANA. Questo può essere utilizzato per fornire i dati di produzione correnti in un sistema di test. Il backup e recovery di BlueXP ti consente di selezionare una copia Snapshot da un sistema di origine e di creare un nuovo volume Azure NetApp Files basato sulla copia Snapshot. Sono disponibili script di esempio che consentono di eseguire le operazioni necessarie sull'host del database per ripristinare il database SAP HANA.

Prima di iniziare

- Installare il sistema di destinazione SAP HANA prima di eseguire la prima operazione di refresh.
- Dovresti aggiungere manualmente i sistemi HANA di origine e destinazione nel backup e recovery di BlueXP.
- Assicurarsi che la versione del database SAP HANA sia la stessa sul sistema di origine e di destinazione.
- Si sarebbe dovuto decidere quali script di refresh utilizzare. Gli script di refresh sono disponibili nel report tecnico della soluzione.

  "Script di esempio di automazione"

  È possibile personalizzare gli script di refresh.

- Le seguenti variabili ambientali sono disponibili come parte di Prespt e postscript:
  - CLONED_VOLUMES_MOUNT_PATH
  - <SOURCEVOLUME>_DESTINATION
  - HANA_DATABASE_TYPE
  - TENANT_DATABASE_NAMES
- È necessario aggiornare il plug-in alla versione 3,0.
- I percorsi di montaggio devono essere identici per il volume di dati sui sistemi SAP HANA di origine e di destinazione.
- Prima della prima operazione di aggiornamento, assicurarsi che il file '/etc/fstab' non contenga voci per i volumi di dati del sistema SAP HANA di destinazione.

A proposito di questa attività

- L'aggiornamento del sistema è supportato solo per il sistema HANA di container di database multi-tenant.
- I criteri esistenti saranno validi dopo l'aggiornamento del sistema.
- I nuovi volumi creati avranno la seguente convenzione di denominazione: <sourcevolumename>-<timestamp>
  - Formato timestamp: <year> <month> <day>-<hour> <minute> <second>

    Ad esempio, se il volume di origine è vol1, il nome del volume aggiornato sarà vol1-20230109-184501

> Il nuovo volume verrà inserito nello stesso pool di capacità dei volumi di destinazione.

- Il percorso di giunzione sarà lo stesso del nome del volume.
- Il "numero massimo di throughput" per il nuovo volume viene prelevato dal volume del sistema di destinazione con pool di capacità manuali Quality of Service (QoS).

Per i pool di capacità QoS automatici, il throughput è definito dalla capacità del volume di origine.

- Durante l'aggiornamento del sistema, il montaggio e la disinstallazione automatici dei volumi vengono eseguiti utilizzando workflow e non script.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nella pagina **applicazioni**, fare clic su ••• Per selezionare l'azione corrispondente al sistema che si desidera aggiornare e selezionare **System Refresh** (Aggiorna sistema).
3. Nella pagina **System Refresh**, eseguire le seguenti operazioni:
   a. Selezionare il sistema di origine e la copia Snapshot.
   b. (Facoltativo) immettere gli indirizzi di esportazione da cui è possibile accedere ai nuovi volumi.
   c. (Opzionale) immettere la massima velocità di trasmissione dello storage (MIB).
   d. Immettere prescrittt, postscript e i percorsi degli script di errore. Lo script on failure viene eseguito solo quando l'operazione di refresh del sistema non riesce.
   e. Fare clic su **Aggiorna**.

Gestire la protezione dei dati applicativi nativi del cloud

Monitorare i lavori

È possibile monitorare lo stato dei lavori avviati negli ambienti di lavoro. In questo modo è possibile visualizzare i lavori completati correttamente, quelli in corso e quelli che non sono riusciti, in modo da poter diagnosticare e risolvere eventuali problemi.

> I lavori pianificati verranno elencati nella pagina di monitoraggio dei lavori BlueXP dopo un ritardo di 5 minuti (massimo) dall'ora di completamento del lavoro.

Per ulteriori informazioni, fare riferimento a. "Monitorare lo stato del lavoro".

Manutenzione degli host di database Oracle

Un amministratore può mettere manualmente gli host del database in modalità di manutenzione per eseguire attività di manutenzione sugli host. Durante l'aggiornamento, gli host vengono automaticamente messi in modalità di manutenzione e, dopo l'aggiornamento, gli host vengono automaticamente trasferiti in modalità di produzione.

Quando gli host vengono messi in modalità di manutenzione, le operazioni on-demand non vengono eseguite e i processi pianificati vengono ignorati.

> Non è possibile verificare se sono in esecuzione lavori per le risorse sugli host prima di mettere gli host in modalità di manutenzione.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**
2. Selezionare **Oracle** come tipo di applicazione.
3. Fare clic su **Impostazioni** > **host**.

4. Eseguire una delle seguenti operazioni:

Se…	Eseguire questa operazione…
Impostare l'host in modalità di manutenzione	Fare clic su ••• Corrispondente all'host e selezionare **Enable maintenance mode** (attiva modalità di manutenzione).
Desidera portare l'host fuori dalla modalità di manutenzione	Fare clic su ••• Corrispondente all'host in manutenzione e selezionare **Disable maintenance mode** (Disattiva modalità di manutenzione).

Dati di audit

Quando si esegue direttamente un'API o si utilizza l'interfaccia utente per effettuare la chiamata API a una qualsiasi delle API esposte esternamente del backup e ripristino BlueXP per le applicazioni, la richiesta viene dettagliata come intestazioni, ruolo, corpo della richiesta, E le informazioni API verranno registrate nella tempistica di BlueXP e le voci di audit verranno conservate per sempre nella tempistica. Anche lo stato e la risposta agli errori della chiamata API vengono verificati dopo il completamento dell'operazione. Nel caso di risposte API asincrone come i job, l'id del job viene registrato anche come parte della risposta.

Il backup e ripristino BlueXP per le applicazioni registra le voci come host IP, corpo della richiesta, nome dell'operazione, chi ha attivato, alcune intestazioni, E lo stato operativo dell'API.

Visualizzare i dettagli del backup

È possibile visualizzare il numero totale di backup creati, i criteri utilizzati per la creazione dei backup, la versione del database e l'ID dell'agente.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **View Details** (Visualizza dettagli).

> L'ID dell'agente è associato al connettore. Se un connettore utilizzato durante la registrazione dell'host SAP HANA non esiste più, i backup successivi dell'applicazione non avranno esito positivo perché l'ID dell'agente del nuovo connettore è diverso. Modificare l'id del connettore nell'host. Per ulteriori informazioni, vedere Aggiornare i dettagli del connettore.

Elimina clone

Se non è più necessario, è possibile eliminare un clone.

Fasi

1. Fare clic su + Accanto a **Filtra per** e seleziona **Clona opzioni** > **Clona genitori**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **View Details** (Visualizza dettagli).
3. Nella pagina Database Details (Dettagli database), fare clic su + Accanto a **Filtra per** e selezionare **Clona**.

4. Fare clic su ••• Corrispondente al clone che si desidera eliminare e fare clic su **Delete** (Elimina).
5. (Facoltativo) selezionare la casella di controllo **forza eliminazione**.

Aggiornare i dettagli del connettore

Se il connettore utilizzato durante la registrazione dell'host dell'applicazione non esiste più o è danneggiato, è necessario implementare un nuovo connettore. Dopo aver implementato il nuovo connettore, eseguire l'API **Connector-update** per aggiornare i dettagli del connettore per tutti gli host registrati utilizzando il vecchio connettore.

Dopo aver aggiornato i dettagli del connettore per gli host Oracle o SAP HANA, eseguire le seguenti operazioni per assicurarsi che i dettagli del connettore siano stati aggiornati correttamente.

Fasi

1. Accedere a BlueXP Connector VM ed eseguire le seguenti operazioni:
   a. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.
   ```
   docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/getVersion --cert/config/client/certificate/certificate.pem --key/config/client/certificate/key.pem
   ```
   b. Ottenere il percorso di montaggio base.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
   ```
   c. Copiare certificate.pem dal percorso *<base_mount_path>/client/certificate/* del connettore VM a */var/opt/snapcenter/spl/etc/* sull'host del plug-in.
2. Accedere all'host del plug-in ed eseguire le seguenti operazioni:
   a. Passare a */var/opt/snapcenter/spl/etc* ed eseguire il comando keytool per importare il file certificate.pem.
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks -deststorepass snapcenter -noprompt
   ```
   b. Riavviare SPL: `systemctl restart spl`
   c. Eseguire una delle seguenti operazioni:

Se sei acceso…	Eseguire questa operazione…
Host del database Oracle	i. Assicurarsi che tutti i "prerequisiti" sono soddisfatti. ii. Fare clic su **Backup and Recovery** > **applicazioni** iii. Fare clic su ••• Corrispondente all'applicazione e fare clic su **View Details** (Visualizza dettagli). iv. Modificare **ID connettore**.

Se sei acceso…	Eseguire questa operazione…
Host di database SAP HANA	i. Assicurarsi che tutti i "prerequisiti" sono soddisfatti. ii. Eseguire il seguente comando: `curl --location --request PATCH 'https://snapcenter.cloudmanager.cloud.netapp.com/api/saphana/hosts/connector/update' \ --header 'x-account-id: <CM account-id>' \ --header 'Authorization: Bearer token' \ --header 'Content-Type: application/json' \ --data-raw '{ "old_connector_id": "Old connector id that no longer exists", "new_connector_id": "New connector Id"}'` I dettagli del connettore verranno aggiornati correttamente se tutti gli host hanno il plug-in SnapCenter per il servizio SAP HANA installato e in esecuzione e se sono tutti raggiungibili dal nuovo connettore.

Configurare il certificato firmato dalla CA

È possibile configurare il certificato firmato dalla CA se si desidera includere ulteriore protezione nell'ambiente.

Configurare il certificato firmato dalla CA per BlueXP Connector

Il connettore utilizza un certificato autofirmato per comunicare con il plug-in. Il certificato autofirmato viene importato nel keystore dallo script di installazione. Per sostituire il certificato autofirmato con il certificato firmato dalla CA, procedere come segue.

Fasi

1. Per utilizzare il certificato CA come certificato client quando il connettore si connette al plug-in, attenersi alla seguente procedura.
   a. Accedere a Connector.
   b. Eseguire il seguente comando per ottenere *<base_mount_path>*:
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

c. Eliminare tutti i file esistenti che si trovano in *<base_mount_path>/client/certificate* nel connettore.

d. Copiare il certificato e il file delle chiavi firmato dalla CA in *<base_mount_path>/client/certificate* nel connettore.

   Il nome del file deve essere certificate.pem e key.pem. Il file certificate.pem deve avere l'intera catena dei certificati, ad esempio CA intermedia e CA principale.

e. Creare il formato PKCS12 del certificato con il nome certificate.p12 e mantenere l'indirizzo *<base_mount_path>/client/certificate*.

   Esempio: openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12

2. Per convalidare il certificato inviato dal connettore, eseguire le seguenti operazioni sull'host del plug-in.

   a. Accedere all'host del plug-in.

   b. Copiare il certificato.pem e i certificati per tutte le CA intermedie e root dal connettore all'host plug-in in */var/opt/snapcenter/spl/etc/*.

   > Il formato della CA intermedia e del certificato della CA principale deve essere in formato .crt.

   c. Passare a */var/opt/snapcenter/spl/etc* ed eseguire il comando keytool per importare il file certificate.pem.
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore
   keystore.jks -deststorepass snapcenter -noprompt
   ```

   d. Importare la CA principale e i certificati intermedi.
   ```
   keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter
   -alias trustedca -file <certificate.crt>
   ```

   > Il certificato.crt fa riferimento ai certificati della CA principale e della CA intermedia.

   e. Riavviare SPL: `systemctl restart spl`

Configurare il certificato firmato dalla CA per il plug-in

Il certificato CA deve avere lo stesso nome registrato in Cloud Backup per l'host plug-in.

Fasi

1. Per ospitare il plug-in utilizzando il certificato CA, attenersi alla seguente procedura sull'host del plug-in.

   a. Accedere alla cartella contenente il keystore della SPL */var/opt/snapcenter/spl/etc*.

   b. Creare il formato PKCS12 del certificato con certificato e chiave con alias *splkeystore*.

   Il file certificate.pem deve avere l'intera catena dei certificati, ad esempio CA intermedia e CA principale.

Esempio: openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12 -name splkeystore

   a. Aggiungere il certificato CA creato nel passaggio precedente.
   ```
   keytool -importkeystore -srckeystore certificate.p12 -srcstoretype pkcs12
   -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore
   -destalias splkeystore -noprompt
   ```

b. Verificare i certificati.
```
keytool -list -v -keystore keystore.jks
```

c. Riavviare SPL: `systemctl restart spl`

2. Eseguire le seguenti operazioni sul connettore in modo che il connettore possa verificare il certificato del plug-in.

a. Accedere al connettore come utente non root.

b. Eseguire il seguente comando per ottenere *<base_mount_path>*:
```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs
sudo docker volume inspect | grep Mountpoint
```

c. Copiare i file della CA principale e intermedia nella directory del server.
```
cd <base_mount_path>
mkdir server
```

I file CA devono essere in formato pem.

d. Connettersi a cloud_scs_cloud e modificare **enableCACert** in *config.yml* in **true**.
```
sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert:
false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-
cloud/config/config.yml
```

e. Riavviare il container cloud_scs_cloud.
```
sudo docker restart cloudmanager_scs_cloud
```

Accedere alle API REST

Le API REST per proteggere le applicazioni nel cloud sono disponibili all'indirizzo: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/.

Per accedere alle API REST, è necessario ottenere il token utente con autenticazione federata. Per informazioni su come ottenere il token utente, fare riferimento a. "Creare un token utente con autenticazione federata".

Backup e ripristino dei dati delle macchine virtuali

Proteggi i dati delle tue macchine virtuali

Il backup e ripristino BlueXP per macchine virtuali offre funzionalità di protezione dei dati eseguendo il backup dei datastore e il ripristino delle macchine virtuali.

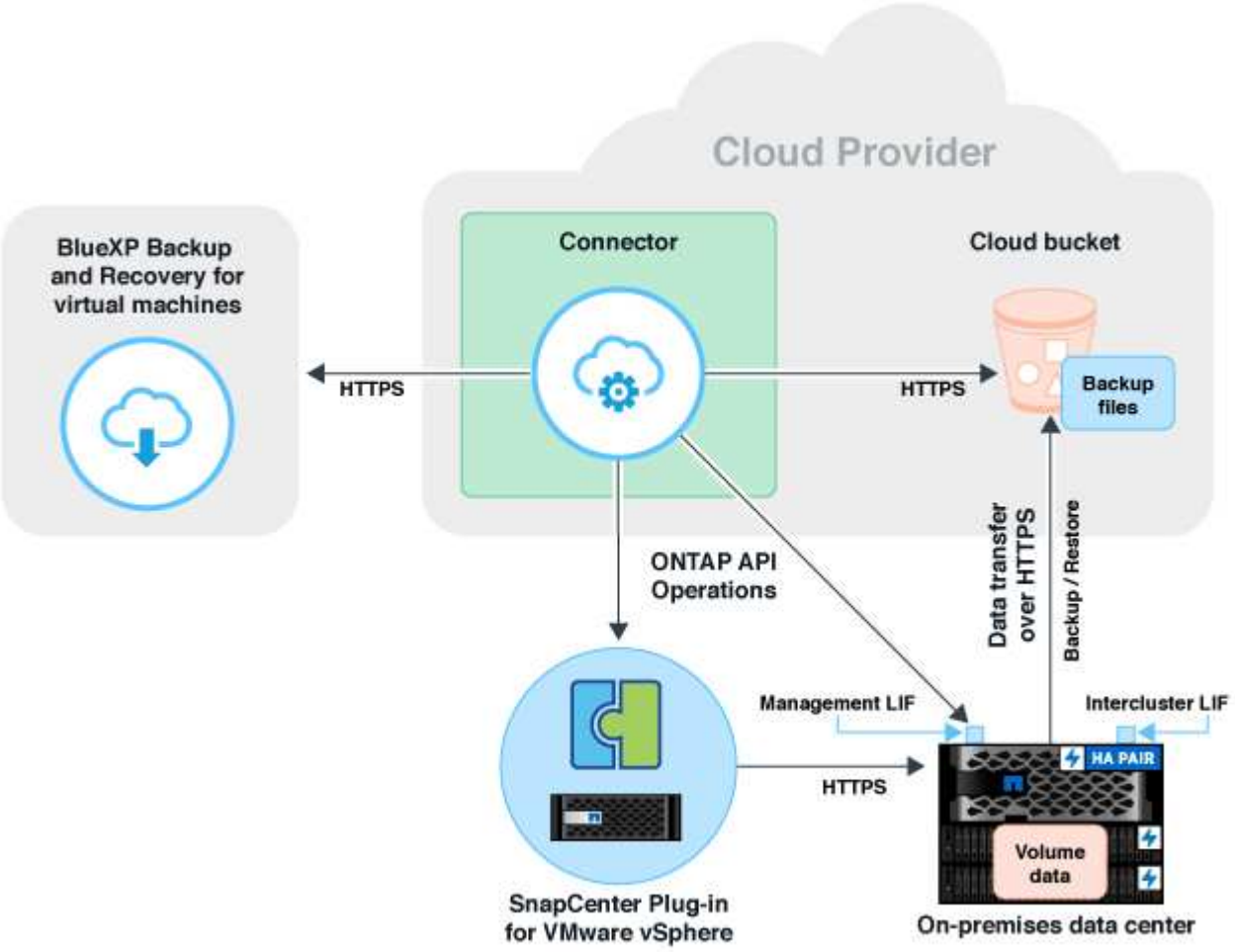
È possibile eseguire il backup dei datastore su Amazon Web Services S3, Microsoft Azure Blob, piattaforma cloud Google e StorageGRID e ripristinare le macchine virtuali nel plug-in SnapCenter on-premise per l'host VMware vSphere. Il backup e recovery di BlueXP per le macchine virtuali supporta anche il modello di implementazione di Connector proxy.

Prima di iniziare

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup di datastore e macchine virtuali su un cloud provider.

- 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 di VMFS, il plug-in SnapCenter per host VMware vSphere deve essere eseguito su 4.9 o versione 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 le policy pre-programmate, il livello di pianificazione deve essere lo stesso per il datastore nel plug-in SnapCenter per 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.

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



Registrare il plug-in SnapCenter per l'host VMware vSphere

È necessario registrare il plug-in SnapCenter per l'host VMware vSphere in BlueXP per visualizzare i datastore e le macchine virtuali. Solo un utente con accesso amministrativo può registrare il plug-in SnapCenter per l'host VMware vSphere.

> È possibile registrare più plug-in SnapCenter per gli host VMware vSphere in BlueXP. Tuttavia, una volta effettuata la registrazione, non è possibile rimuovere il plug-in SnapCenter per l'host VMware vSphere.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Dal menu a discesa **Impostazioni**, fare clic su **plug-in SnapCenter per VMware vSphere**.
3. Fare clic su **Registra il plug-in SnapCenter per 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. Fare clic su **Registra**.

Al termine

Fare clic su **Backup e ripristino** > **macchine virtuali** per visualizzare tutti i datastore e le macchine virtuali protetti mediante il plug-in SnapCenter registrato per l'host VMware vSphere.

Creare una policy per il backup dei datastore

È possibile creare un criterio o utilizzare uno dei seguenti criteri predefiniti disponibili in BlueXP.

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
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. Fare clic su **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. Fare clic su **Create** (Crea).

> Non è possibile modificare o eliminare una policy associata a un datastore.

Eseguire il backup dei datastore su Amazon Web Services

Puoi eseguire il backup e archiviare uno o più datastore su Amazon Web Services per migliorare l'efficienza dello storage 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.

Prima di iniziare

Assicurarsi di aver soddisfatto tutte le "requisiti" prima di eseguire il backup dei datastore nel cloud.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Fare clic su ••• Corrispondente all'archivio dati di cui si desidera eseguire il backup e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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. Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) corrispondente alla 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. Fare clic su **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. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei datastore su Microsoft Azure

È possibile eseguire il backup di uno o più datastore in Microsoft Azure integrando il plug-in SnapCenter per host VMware vSphere con 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.

Prima di iniziare

Assicurarsi di aver soddisfatto tutte le "requisiti" prima di eseguire il backup dei datastore nel cloud.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Fare clic su ••• Corrispondente all'archivio dati di cui si desidera eseguire il backup e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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. Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) corrispondente alla 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. Fare clic su **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 una tantum e non sarà possibile configurarla in un secondo momento.
6. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Backup dei datastore su Google Cloud Platform

È possibile eseguire il backup di uno o più datastore sulla piattaforma cloud di Google integrando il plug-in SnapCenter per host VMware vSphere con 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.

Prima di iniziare

Assicurarsi di aver soddisfatto tutte le "requisiti" prima di eseguire il backup dei datastore nel cloud.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Fare clic su ••• Corrispondente all'archivio dati di cui si desidera eseguire il backup e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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. Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) corrispondente alla 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. Fare clic su **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. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei datastore su StorageGRID

È possibile eseguire il backup di uno o più datastore su StorageGRID integrando il plug-in SnapCenter per host VMware vSphere con 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.

Prima di iniziare

Assicurarsi di aver soddisfatto tutte le "requisiti" prima di eseguire il backup dei datastore nel cloud.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Fare clic su ••• Corrispondente all'archivio dati di cui si desidera eseguire il backup e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (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. Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) corrispondente alla 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. Fare clic su **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. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Gestione della protezione dei dati di datastore e macchine virtuali

È possibile visualizzare policy, datastore 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.

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 di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Criteri**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente alla policy 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 di BlueXP, fare clic su **protezione** > **backup e ripristino** > **macchine virtuali** > **Impostazioni** > **plug-in SnapCenter per VMware vSphere**.
2. Fare clic sul plug-in SnapCenter per l'host 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 di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Virtual Machines**.
2. Fare clic su ••• Corrispondente al datastore che si desidera annullare la protezione e fare clic su **Annulla 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 di BlueXP, fare clic su **protezione** > **backup e ripristino** > **macchine virtuali** > **Impostazioni** > **plug-in SnapCenter per VMware vSphere**.
2. Fare clic su ••• E selezionare **Modifica**.
3. Modificare i dettagli come richiesto.
4. Fare clic su **Save** (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. Fare clic su **Backup and recovery** > **Virtual Machines**.
2. Dal menu a discesa **Impostazioni**, fare clic su **plug-in SnapCenter per VMware vSphere**.
3. Fare clic su ••• Corrispondente al plug-in SnapCenter per l'host VMware vSphere e fare clic su **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. Fare clic su **Backup and recovery** > **Virtual Machines**.
2. Fare clic su ••• Corrispondente al datastore e fare clic su **Refresh Protection**.

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. Fare clic su **Backup and recovery** > **Virtual Machines**.
2. Dal menu a discesa **Impostazioni**, fare clic su **plug-in SnapCenter per VMware vSphere**.
3. Fare clic su ••• Corrispondente al plug-in SnapCenter per l'host VMware vSphere e fare clic su **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. Fare clic su **Backup and Recovery** > **Job Monitoring**.

   Quando si avvia un'operazione, viene visualizzata una finestra che indica che il processo è stato avviato. È possibile fare clic sul collegamento per monitorare il lavoro.

2. Fare clic sull'attività principale per visualizzare le attività secondarie e lo stato di ciascuna di queste attività secondarie.

Ripristinare i dati delle macchine virtuali dal cloud

È possibile ripristinare i dati delle macchine virtuali dal cloud al vCenter on-premise. 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.

Prima di iniziare

- Assicurarsi di aver soddisfatto tutte le "requisiti" prima di ripristinare le macchine virtuali dal 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 di BlueXP, fare clic su **protezione** > **backup e ripristino** > **macchine virtuali** > **plug-in SnapCenter per VMware vSphere** e selezionare il plug-in SnapCenter per l'host 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. Fare clic su ••• Corrispondente all'archivio dati che si desidera ripristinare e fare clic su **View Details** (Visualizza dettagli). 2. Fare clic su **Restore** (Ripristina) corrispondente al backup che si desidera ripristinare. 3. Selezionare la macchina virtuale che si desidera ripristinare dal backup e fare clic su **Avanti**. 4. Assicurarsi che sia selezionato **originale** e fare clic su **continua**. 5. Se la macchina virtuale è protetta utilizzando un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **priorità ripristino archiviazione** e fare clic su **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. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Se si desidera ripristinare la macchina virtuale…	Eseguire questa operazione…
in una posizione alternativa dal datastore	1. Fare clic su ••• Corrispondente all'archivio dati che si desidera ripristinare e fare clic su **View Details** (Visualizza dettagli). 2. Fare clic su **Restore** (Ripristina) corrispondente al backup che si desidera ripristinare. 3. Selezionare la macchina virtuale che si desidera ripristinare dal backup e fare clic su **Avanti**. 4. Selezionare **alternativa**. 5. Selezionare vCenter Server, host ESXi, datastore e rete alternativi. 6. Fornire un nome per la macchina virtuale dopo il ripristino e fare clic su **continua**. 7. Se la macchina virtuale è protetta utilizzando un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **priorità ripristino archiviazione** e fare clic su **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. Esaminare i dettagli e fare clic su **Restore** (Ripristina).
nella posizione originale dalle macchine virtuali	1. Fare clic su ••• Corrispondente alla macchina virtuale che si desidera ripristinare e fare clic su **Restore** (Ripristina). 2. Selezionare il backup tramite il quale si desidera ripristinare la macchina virtuale. 3. Assicurarsi che sia selezionato **originale** e fare clic su **continua**. 4. Se la macchina virtuale è protetta utilizzando un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **priorità ripristino archiviazione** e fare clic su **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. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Se si desidera ripristinare la macchina virtuale…	Eseguire questa operazione…
in una posizione alternativa dalle macchine virtuali	1. Fare clic su ••• Corrispondente alla macchina virtuale che si desidera ripristinare e fare clic su **Restore** (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. Fornire un nome per la macchina virtuale dopo il ripristino e fare clic su **continua**. 6. Se la macchina virtuale è protetta utilizzando un criterio in cui sono configurate le impostazioni di archiviazione, selezionare **priorità ripristino archiviazione** e fare clic su **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. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Backup e ripristino dei dati Kubernetes

Proteggi i dati del cluster Kubernetes utilizzando il backup e ripristino BlueXP

Il backup e ripristino BlueXP offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cluster Kubernetes. I backup vengono generati e memorizzati automaticamente in un archivio di oggetti nel tuo account di cloud pubblico o privato.

Se necessario, è possibile ripristinare un intero *volume* da un backup nello stesso ambiente di lavoro o in un ambiente di lavoro diverso.

Caratteristiche

Funzionalità di backup:

- Eseguire il backup di copie indipendenti dei volumi persistenti 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.
- I dati di backup sono protetti con crittografia AES-256 bit a riposo e connessioni HTTPS TLS 1.2 in volo.
- Supporto di un massimo di 4,000 backup di un singolo volume.

Funzionalità di ripristino:

- Ripristinare i dati da un momento specifico.
- Ripristinare un volume nel sistema di origine o in un sistema diverso.
- Ripristina i dati a livello di blocco, posizionando i dati direttamente nella posizione specificata, mantenendo gli ACL originali.

Ambienti di lavoro Kubernetes supportati e provider di storage a oggetti

Il backup e ripristino BlueXP consente di eseguire il backup dei volumi Kubernetes dai seguenti ambienti di lavoro allo storage a oggetti nei seguenti provider di cloud pubblici e privati:

Ambiente di lavoro di origine	Destinazione del file di backup ifdef::aws[]
Cluster Kubernetes in AWS	Amazon S3 endif::aws[] ifdef::Azure[]
Kubernetes in Azure	Azure Blob endif::Azure[] ifdef::gcp[]
Kubernetes in Google	Google Cloud Storage endif::gcp[]

È possibile ripristinare un volume da un file di backup di Kubernetes nei seguenti ambienti di lavoro:

Percorso del file di backup	Ambiente di lavoro di destinazione ifdef::aws[]
Amazon S3	Cluster Kubernetes in AWS endif::aws[] ifdef::Azure[]
Azure Blob	Cluster Kubernetes in Azure endif::Azure[] ifdef::gcp[]

Percorso del file di backup	Ambiente di lavoro di destinazione ifdef::aws[]
Storage Google Cloud	Cluster Kubernetes in Google endif::gcp[]

Costo

L'utilizzo del backup e ripristino di BlueXP comporta due tipi di costi: Costi delle risorse e costi del servizio.

Costi delle risorse

I costi delle risorse vengono pagati al cloud provider per la capacità dello storage a oggetti nel cloud. 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).

Costi di servizio

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

Esistono due 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'acquistare le licenze direttamente da NetApp. Leggere il Licensing per ulteriori informazioni.

Licensing

Il backup e ripristino BlueXP è disponibile in due opzioni di licenza: Pay as You Go (PAYGO) e Bring Your Own License (BYOL). Se non si dispone di una licenza, è disponibile una versione di prova gratuita di 30 giorni.

Versione di prova gratuita

Quando utilizzi la versione di prova gratuita di 30 giorni, ti viene notificato il numero di giorni di prova gratuiti rimasti. Al termine della prova gratuita, i backup non vengono più creati. Per continuare a utilizzare il servizio, è necessario sottoscrivere il servizio o acquistare una licenza.

I file di backup non vengono cancellati quando il servizio viene disattivato. Il tuo cloud provider continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup, a meno che non elimini i backup.

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 attraverso il marketplace del tuo cloud provider, pagherai per GB i dati di cui hai eseguito il backup, senza alcun pagamento anticipato da parte di there. Il tuo cloud provider ti addebita la fattura mensile.

È necessario iscriversi anche se si dispone di una versione di prova gratuita o se si porta la propria licenza (BYOL):

- L'iscrizione garantisce che non vi siano interruzioni del servizio al termine della prova gratuita.

  Al termine del periodo di prova, ti verrà addebitato ogni ora in base alla quantità di dati di cui hai effettuato il backup.

- Se si esegue il backup di un numero di dati superiore a quello consentito dalla licenza BYOL, il backup dei dati prosegue con l'abbonamento pay-as-you-go.

  Ad esempio, se si dispone di una licenza BYOL da 10 TB, tutta la capacità oltre i 10 TB 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.

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

Porta la tua licenza

BYOL è basato sui termini (12, 24 o 36 mesi) *e* sulla capacità in incrementi di 1 TB. Pagherai NetApp per utilizzare il servizio per un periodo di tempo, ad esempio 1 anno, e per una capacità massima, ad esempio 10 TB.

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 di origine associati al "Account BlueXP".

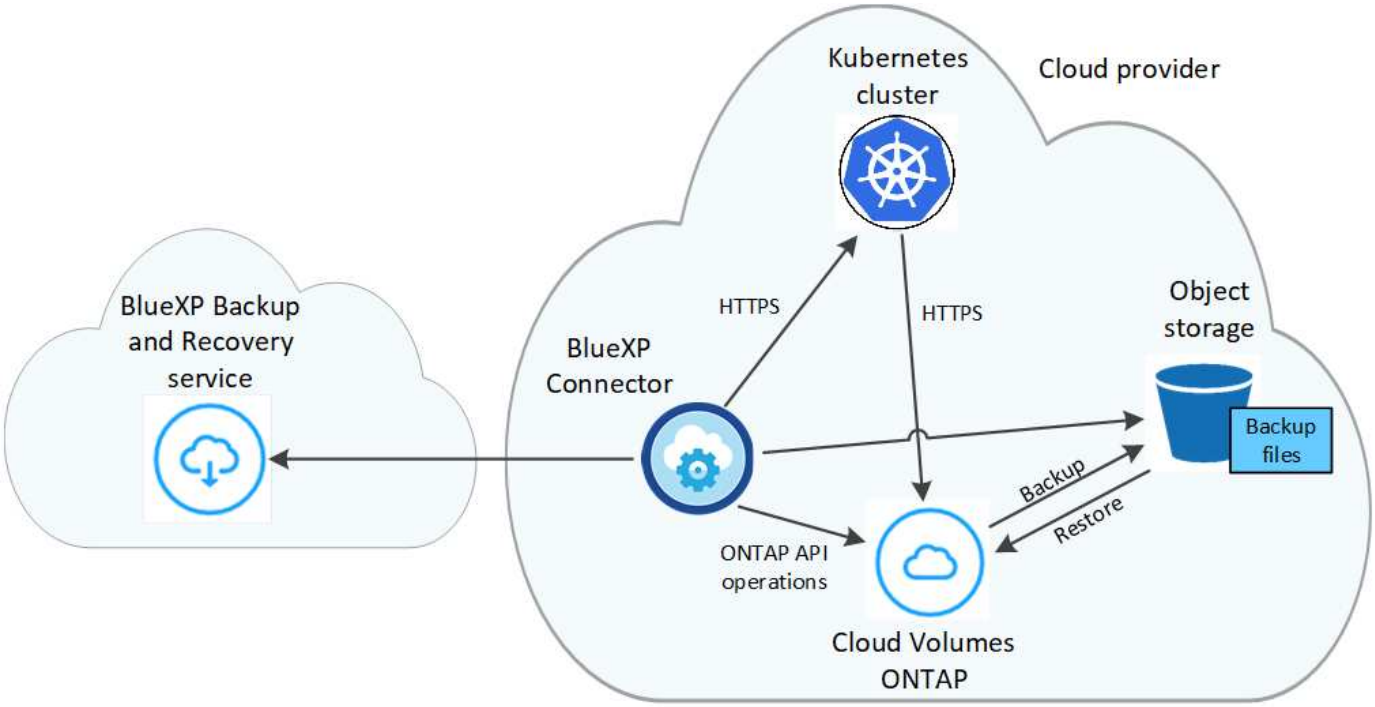
"Scopri come gestire le tue licenze BYOL".

Come funziona il backup e ripristino di BlueXP

Quando si abilita il backup e il ripristino BlueXP su un sistema Kubernetes, 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.

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

La seguente immagine mostra la relazione tra ciascun componente:



Classi di storage o livelli di accesso supportati

- In AWS, i backup iniziano nella classe di storage *Standard* e passano alla classe di storage *Standard-infrequent Access* dopo 30 giorni.
- In Azure, i backup sono associati al Tier di accesso *Cool*.
- In GCP, i backup sono associati alla classe di storage *Standard* per impostazione predefinita.

Pianificazione di backup personalizzabile e impostazioni di conservazione per cluster

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 dall'utente. 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.

È possibile scegliere una combinazione di backup orari, giornalieri, settimanali e mensili di tutti i volumi.

Una volta raggiunto il numero massimo di backup per una categoria o intervallo, i backup meno recenti vengono rimossi in modo da avere sempre i backup più aggiornati.

Volumi supportati

Il backup e ripristino BlueXP supporta i volumi persistenti (PVS).

Limitazioni

- Quando si crea o modifica un criterio di backup quando non sono assegnati volumi al criterio, il numero di backup conservati può essere massimo di 1018. Come soluzione alternativa, è possibile ridurre il numero di backup per creare il criterio. Quindi, è possibile modificare il criterio per creare fino a 4000 backup dopo aver assegnato i volumi al criterio.
- I backup dei volumi ad-hoc che utilizzano il pulsante **Backup Now** non sono supportati sui volumi Kubernetes.

Backup dei dati persistenti del volume di Kubernetes su Amazon S3

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dai volumi persistenti sui cluster EKS Kubernetes sullo storage Amazon S3.

Avvio rapido

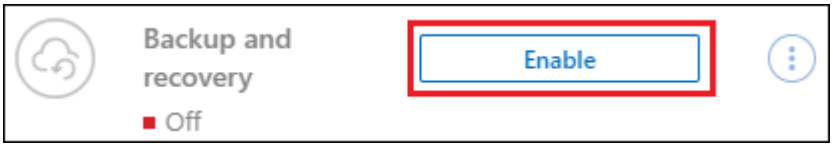
Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Esaminare i prerequisiti

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP.
  - Trident deve essere installato sul cluster e la versione di Trident deve essere 21.1 o superiore.
  - Tutti i PVC che verranno utilizzati per creare volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".
  - Il cluster deve utilizzare Cloud Volumes ONTAP su AWS per lo storage back-end.
  - Il sistema Cloud Volumes ONTAP deve eseguire ONTAP 9.7P5 o versione successiva.
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. "Offerta di backup di BlueXP Marketplace", an "Contratto annuale AWS", oppure è stato acquistato "e attivato" Una licenza BYOL di backup e ripristino BlueXP di NetApp.
- Il ruolo IAM che fornisce a BlueXP Connector le autorizzazioni include le autorizzazioni S3 dell'ultima versione "Policy BlueXP".

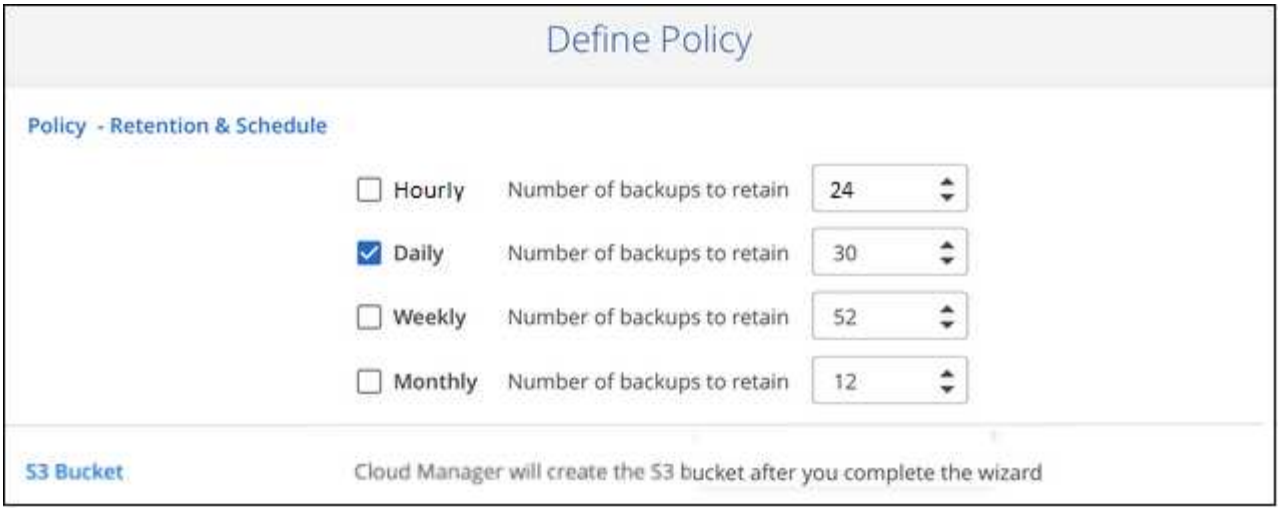
2 Abilitare il backup e il ripristino BlueXP sul cluster Kubernetes esistente

Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra, quindi seguire la procedura di installazione guidata.



3 Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup orari, giornalieri, settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca più opzioni. È inoltre possibile modificare il numero di copie di backup che si desidera conservare.



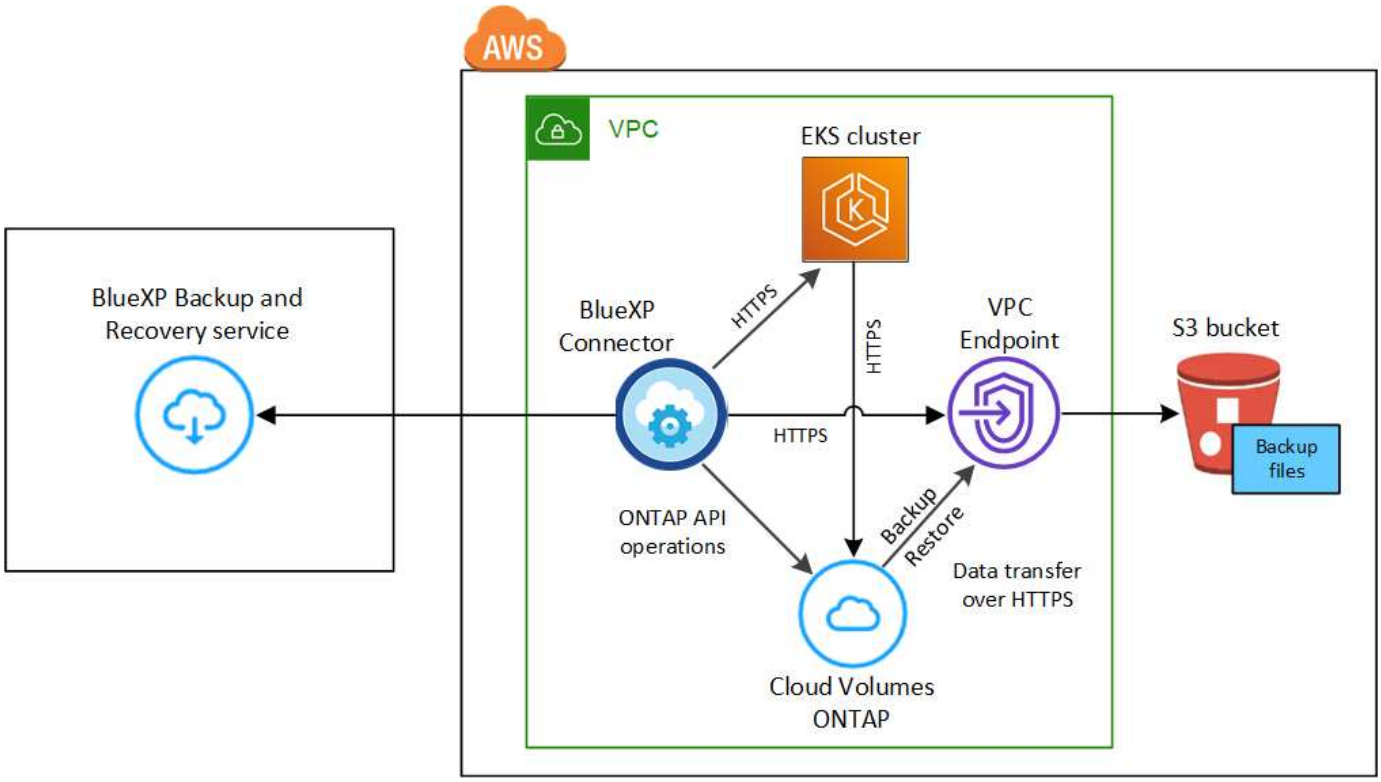
4 **Selezionare i volumi di cui si desidera eseguire il backup**

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi). Un bucket S3 viene creato automaticamente nello stesso account AWS e nella stessa regione del sistema Cloud Volumes ONTAP e i file di backup vengono memorizzati in tale area.

Requisiti

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

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



Tenere presente che l'endpoint VPC è opzionale.

Requisiti del cluster Kubernetes

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP. "Scopri come scoprire il cluster Kubernetes".
- Trident deve essere installato sul cluster e la versione di Trident deve essere almeno 21.1. Vedere "Come installare Trident" oppure "Come aggiornare la versione di Trident".
- Il cluster deve utilizzare Cloud Volumes ONTAP su AWS per lo storage back-end.
- Il sistema Cloud Volumes ONTAP deve trovarsi nella stessa regione AWS del cluster Kubernetes e deve eseguire ONTAP 9.7P5 o versioni successive (si consiglia ONTAP 9.8P11 e versioni successive).

  Si noti che i cluster Kubernetes in ubicazioni on-premise non sono supportati. Sono supportati solo i cluster Kubernetes nelle implementazioni cloud che utilizzano sistemi Cloud Volumes ONTAP.

- Tutti gli oggetti persistenti di richiesta di rimborso del volume che verranno utilizzati per creare i volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".

  È possibile eseguire questa operazione per singoli PVC aggiungendo `snapshotPolicy` in annotazioni:

  ```
  kind: PersistentVolumeClaim
  apiVersion: v1
  metadata:
    name: full
    annotations:
      trident.netapp.io/snapshotPolicy: "default"
  spec:
    accessModes:
      - ReadWriteMany
    resources:
      requests:
        storage: 1000Mi
    storageClassName: silver
  ```

  È possibile eseguire questa operazione per tutti i PVC associati a uno storage back-end specifico aggiungendo `snapshotPolicy` sotto i valori predefiniti in `backend.json` file:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

Requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è disponibile un abbonamento 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".

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

Regioni AWS supportate

Il backup e ripristino BlueXP è supportato in tutte le regioni AWS "Dove è supportato Cloud Volumes ONTAP".

Autorizzazioni di backup AWS richieste

Il ruolo IAM che fornisce a BlueXP le autorizzazioni deve includere le autorizzazioni S3 della versione più recente "Policy BlueXP".

Di seguito sono riportate le autorizzazioni S3 specifiche del criterio:

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

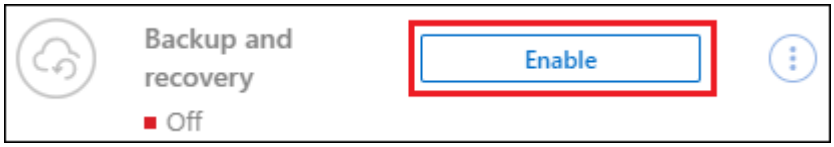
Attivazione del backup e ripristino BlueXP

Abilita backup e ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro Kubernetes.

Fasi

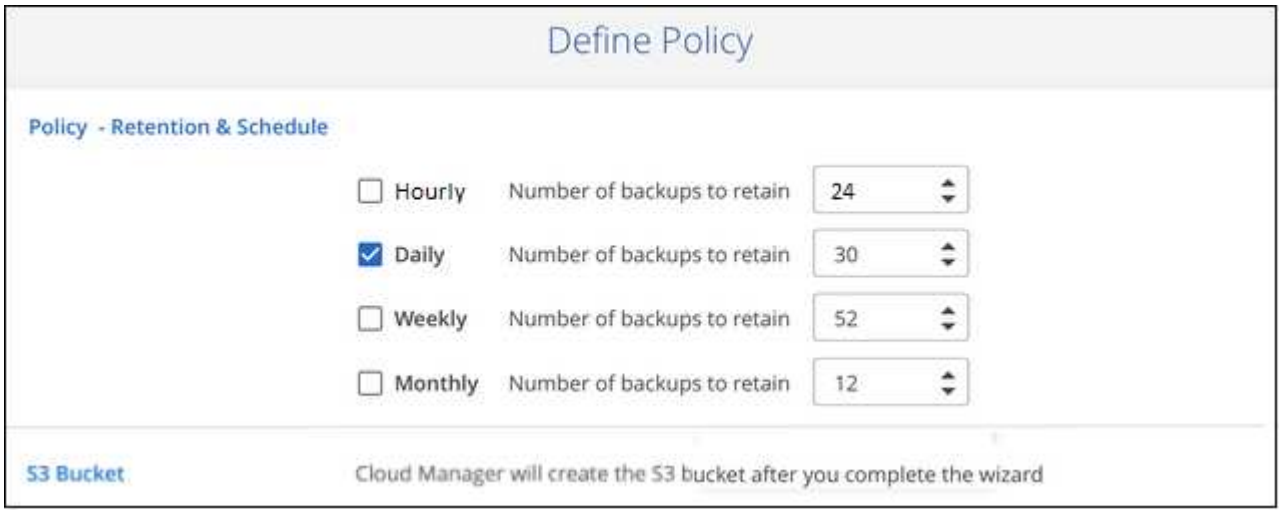
1. Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.

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

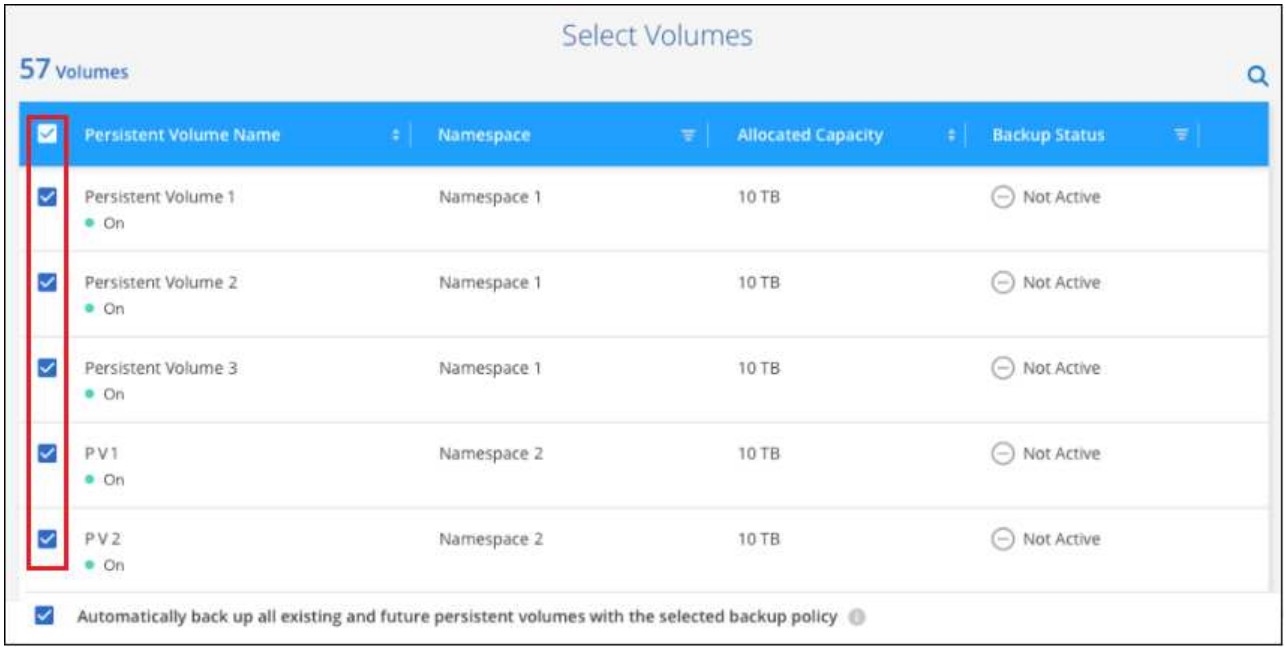


2. Inserire i dettagli del criterio di backup e fare clic su **Avanti**.

   È possibile definire la pianificazione del backup e scegliere il numero di backup da conservare.



3. Selezionare i volumi persistenti di cui si desidera eseguire il backup.
   - Per eseguire il backup di tutti i volumi, selezionare la casella nella riga del titolo (☑ Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☑ Volume_1).



4. Se si desidera che il backup di tutti i volumi correnti e futuri sia attivato, lasciare selezionata la casella di controllo "Backup automatico dei volumi futuri…". Se si disattiva questa impostazione, sarà necessario attivare manualmente i backup per i volumi futuri.
5. Fare clic su **Activate Backup** (attiva backup) per avviare il backup e il ripristino di BlueXP con i backup iniziali di ciascun volume selezionato.

Risultato

Un bucket S3 viene creato automaticamente nello stesso account AWS e nella stessa regione del sistema Cloud Volumes ONTAP e i file di backup vengono memorizzati in tale area.

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

Quali sono le prossime novità?

È possibile "avviare e arrestare i backup dei volumi o modificare la pianificazione del backup". Puoi anche farlo "ripristinare interi volumi da un file di backup" Come nuovo volume nello stesso cluster Kubernetes o in un altro cluster in AWS (nella stessa regione).

Backup di Kubernetes dati di volumi persistenti nello storage Azure Blob

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dai volumi persistenti sui cluster AKS Kubernetes nello storage Azure Blob.

Avvio rapido

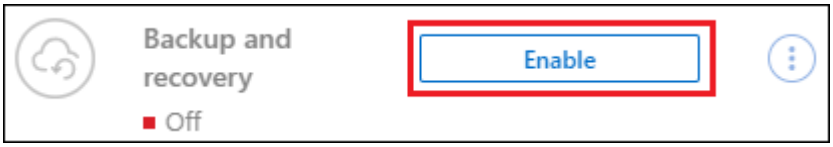
Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Esaminare i prerequisiti

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP.
  - Trident deve essere installato sul cluster e la versione di Trident deve essere 21.1 o superiore.
  - Tutti i PVC che verranno utilizzati per creare volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".
  - Il cluster deve utilizzare Cloud Volumes ONTAP su Azure per lo storage back-end.
  - Il sistema Cloud Volumes ONTAP deve eseguire ONTAP 9.7P5 o versione successiva.
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. "Offerta di backup di BlueXP Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup e ripristino BlueXP di NetApp.

2 Abilitare il backup e il ripristino BlueXP sul cluster Kubernetes esistente

Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra, quindi seguire la procedura di installazione guidata.



3 Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup orari, giornalieri, settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca più opzioni. È inoltre possibile modificare il numero di copie di backup che si desidera conservare.

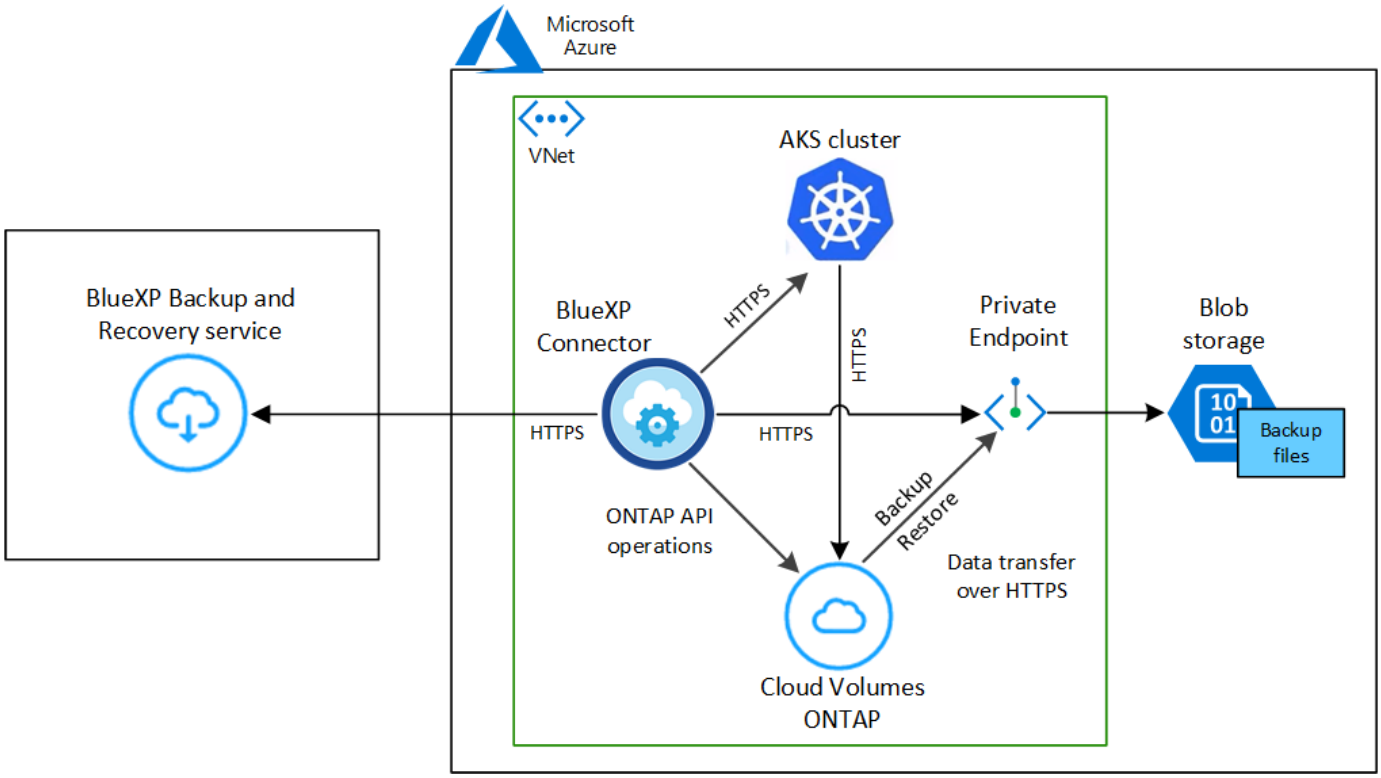
4 **Selezionare i volumi di cui si desidera eseguire il backup**

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi). I file di backup vengono memorizzati in un container Blob utilizzando la stessa sottoscrizione Azure e la stessa regione del sistema Cloud Volumes ONTAP.

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi persistenti di Kubernetes sullo storage Blob.

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



Tenere presente che l'endpoint privato è facoltativo.

Requisiti del cluster Kubernetes

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP. "Scopri come scoprire il cluster Kubernetes".
- Trident deve essere installato sul cluster e la versione di Trident deve essere almeno 21.1. Vedere "Come installare Trident" oppure "Come aggiornare la versione di Trident".
- Il cluster deve utilizzare Cloud Volumes ONTAP su Azure per lo storage back-end.
- Il sistema Cloud Volumes ONTAP deve trovarsi nella stessa regione Azure del cluster Kubernetes e deve eseguire ONTAP 9.7P5 o versioni successive (si consiglia ONTAP 9.8P11 e versioni successive).

  Si noti che i cluster Kubernetes in ubicazioni on-premise non sono supportati. Sono supportati solo i cluster Kubernetes nelle implementazioni cloud che utilizzano sistemi Cloud Volumes ONTAP.

- Tutti gli oggetti persistenti di richiesta di rimborso del volume che verranno utilizzati per creare i volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".

  È possibile eseguire questa operazione per singoli PVC aggiungendo `snapshotPolicy` in annotazioni:

  ```
  kind: PersistentVolumeClaim
  apiVersion: v1
  metadata:
    name: full
    annotations:
      trident.netapp.io/snapshotPolicy: "default"
  spec:
    accessModes:
      - ReadWriteMany
    resources:
      requests:
        storage: 1000Mi
    storageClassName: silver
  ```

  È possibile eseguire questa operazione per tutti i PVC associati a uno storage back-end specifico aggiungendo `snapshotPolicy` sotto i valori predefiniti in `backend.json` file:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

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".

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di storage in cui verranno collocati i backup.

Aree Azure supportate

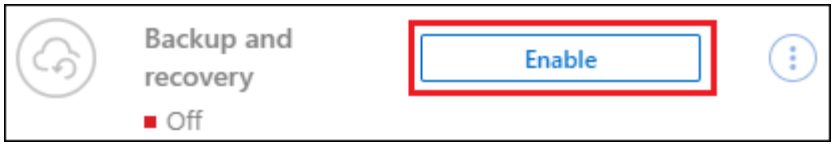
Il backup e ripristino BlueXP è supportato in tutte le regioni Azure "Dove è supportato Cloud Volumes ONTAP".

Attivazione del backup e ripristino BlueXP

Abilita backup e ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro Kubernetes.

Fasi

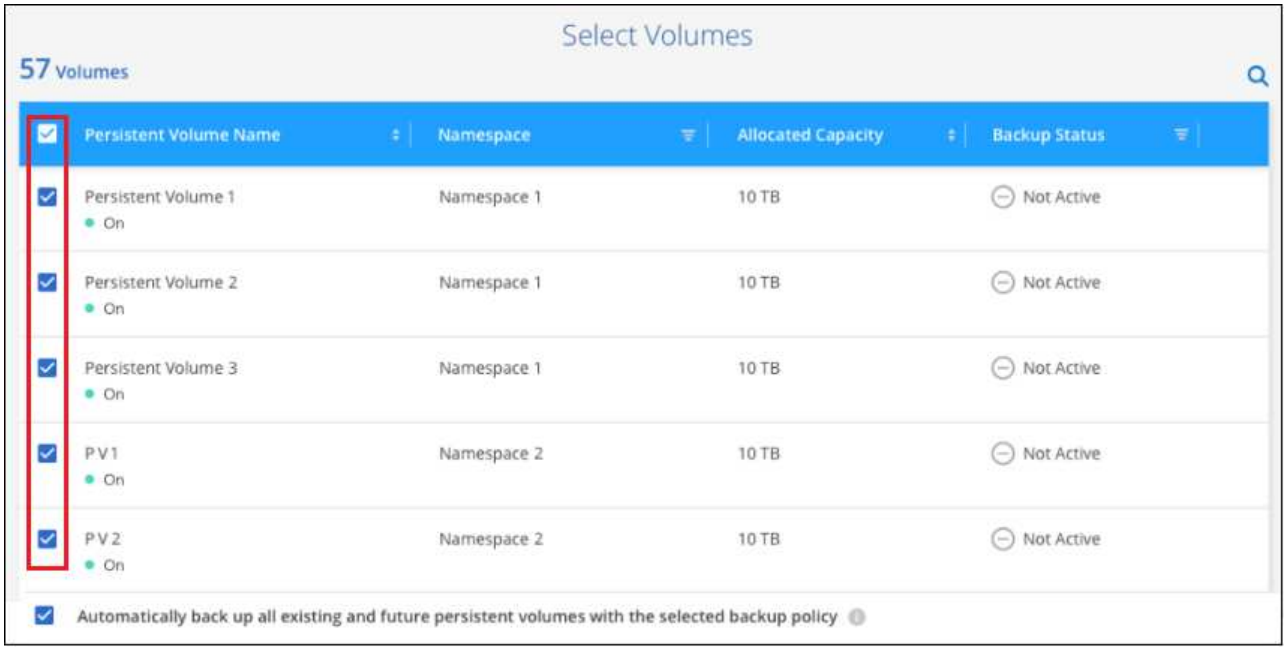
1. Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.



2. Inserire i dettagli del criterio di backup e fare clic su **Avanti**.

   È possibile definire la pianificazione del backup e scegliere il numero di backup da conservare.

3. Selezionare i volumi persistenti di cui si desidera eseguire il backup.
   - Per eseguire il backup di tutti i volumi, selezionare la casella nella riga del titolo (Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (Volume_1).



4. Se si desidera che il backup di tutti i volumi correnti e futuri sia attivato, lasciare selezionata la casella di controllo "Backup automatico dei volumi futuri…". Se si disattiva questa impostazione, sarà necessario attivare manualmente i backup per i volumi futuri.
5. Fare clic su **Activate Backup** (attiva backup) per avviare il backup e il ripristino di BlueXP con i backup iniziali di ciascun volume selezionato.

Risultato

I file di backup vengono memorizzati in un container Blob utilizzando la stessa sottoscrizione Azure e la stessa regione del sistema Cloud Volumes ONTAP.

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

Quali sono le prossime novità?

È possibile "avviare e arrestare i backup dei volumi o modificare la pianificazione del backup". Puoi anche farlo "ripristinare interi volumi da un file di backup" Come nuovo volume nello stesso cluster Kubernetes o in un altro cluster in Azure (nella stessa regione).

Backup di Kubernetes dati di volume persistenti su storage Google Cloud

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dai volumi persistenti sui cluster GKE Kubernetes sullo storage Google Cloud.

Avvio rapido

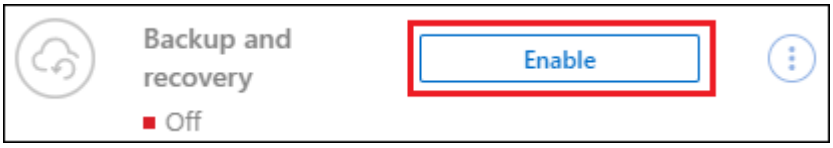
Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Esaminare i prerequisiti

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP.
  - Trident deve essere installato sul cluster e la versione di Trident deve essere 21.1 o superiore.
  - Tutti i PVC che verranno utilizzati per creare volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".
  - Il cluster deve utilizzare Cloud Volumes ONTAP su GCP per lo storage back-end.
  - Il sistema Cloud Volumes ONTAP deve eseguire ONTAP 9.7P5 o versione successiva.
- Si dispone di un abbonamento GCP valido per lo spazio di storage in cui verranno collocati i backup.
- Nel progetto Google Cloud hai un account di servizio con il ruolo predefinito Storage Admin.
- Si è abbonati a. "Offerta di backup di BlueXP Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup e ripristino BlueXP di NetApp.

2 Abilitare il backup e il ripristino BlueXP sul cluster Kubernetes esistente

Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra, quindi seguire la procedura di installazione guidata.



Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup orari, giornalieri, settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca più opzioni. È inoltre possibile modificare il numero di copie di backup che si desidera conservare.

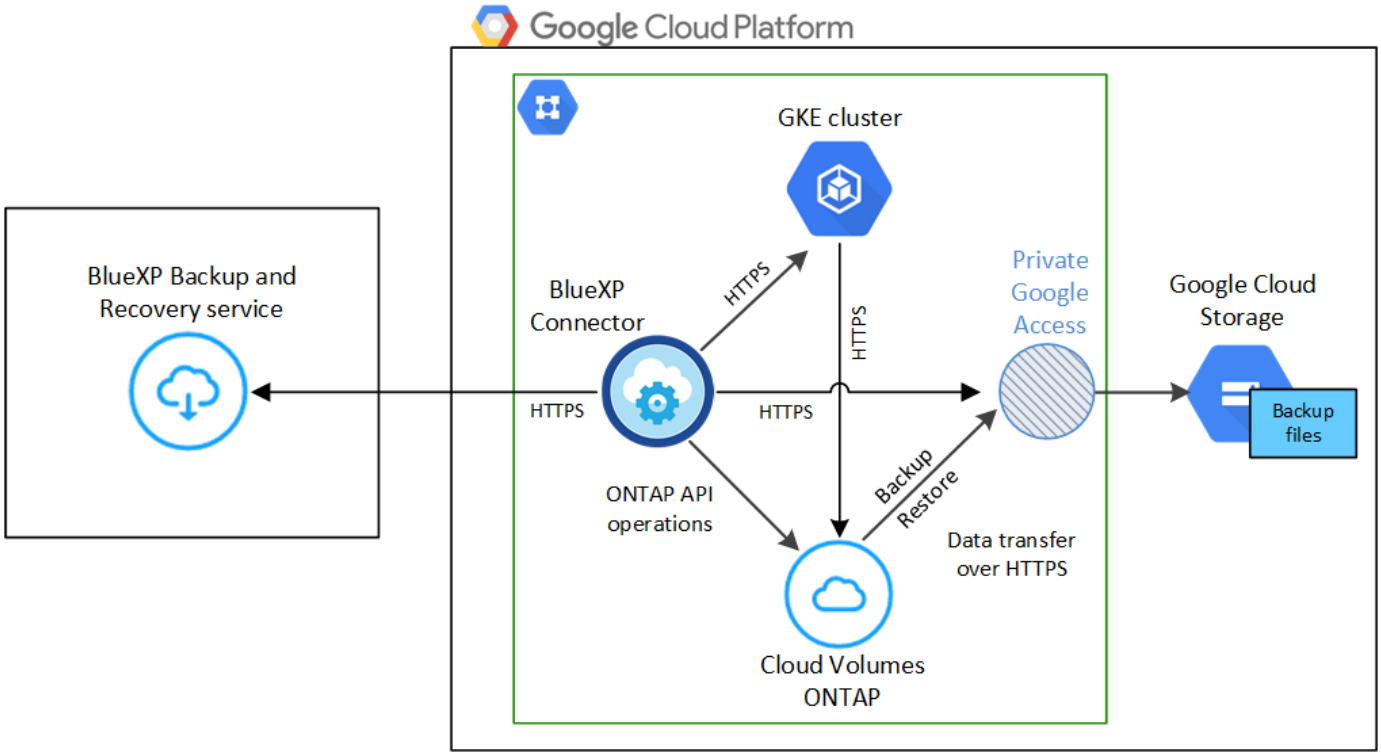
Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi). I file di backup vengono memorizzati in un bucket di storage cloud Google utilizzando la stessa sottoscrizione GCP e la stessa regione del sistema Cloud Volumes ONTAP.

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi persistenti Kubernetes sullo storage Google Cloud.

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



Tenere presente che l'endpoint privato è facoltativo.

Requisiti del cluster Kubernetes

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP. "Scopri come scoprire il cluster Kubernetes".
- Trident deve essere installato sul cluster e la versione di Trident deve essere almeno 21.1. Vedere "Come installare Trident" oppure "Come aggiornare la versione di Trident".
- Il cluster deve utilizzare Cloud Volumes ONTAP su GCP per lo storage back-end.
- Il sistema Cloud Volumes ONTAP deve trovarsi nella stessa regione GCP del cluster Kubernetes e deve eseguire ONTAP 9.7P5 o versioni successive (si consiglia ONTAP 9.8P11 e versioni successive).

  Si noti che i cluster Kubernetes in ubicazioni on-premise non sono supportati. Sono supportati solo i cluster Kubernetes nelle implementazioni cloud che utilizzano sistemi Cloud Volumes ONTAP.

- Tutti gli oggetti persistenti di richiesta di rimborso del volume che verranno utilizzati per creare i volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".

  È possibile eseguire questa operazione per singoli PVC aggiungendo `snapshotPolicy` in annotazioni:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

È possibile eseguire questa operazione per tutti i PVC associati a uno storage back-end specifico aggiungendo `snapshotPolicy` sotto i valori predefiniti in `backend.json` file:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

Regioni GCP supportate

Il backup e ripristino BlueXP è supportato in tutte le regioni GCP "Dove è supportato Cloud Volumes ONTAP".

Requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento tramite "Mercato GCP" È necessario prima di attivare il backup e il 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.

Account di servizio GCP

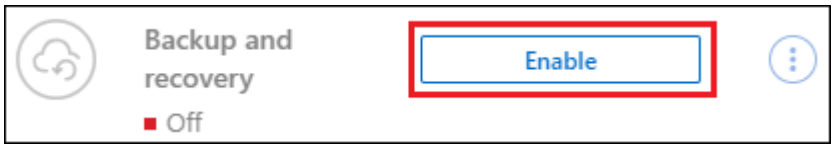
Devi disporre di un account di servizio nel tuo progetto Google Cloud con il ruolo predefinito Storage Admin. "Scopri come creare un account di servizio".

Attivazione del backup e ripristino BlueXP

Abilita backup e ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro Kubernetes.

Fasi

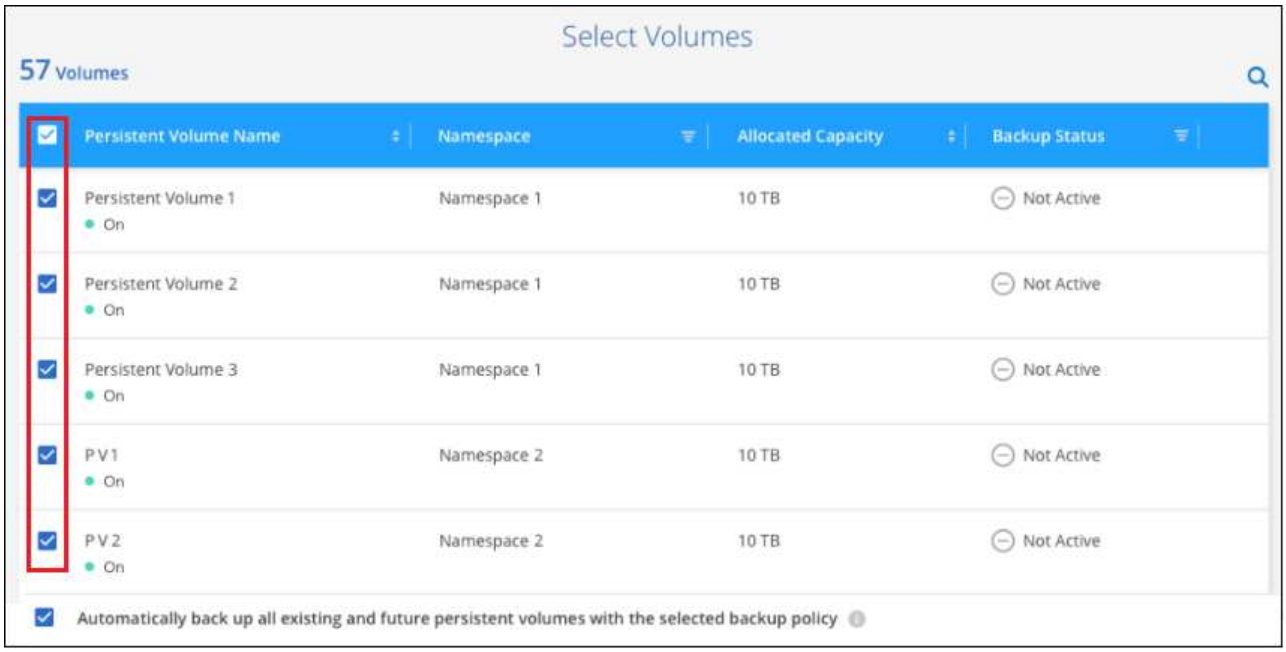
1. Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.



2. Inserire i dettagli del criterio di backup e fare clic su **Avanti**.

   È possibile definire la pianificazione del backup e scegliere il numero di backup da conservare.

3. Selezionare i volumi persistenti di cui si desidera eseguire il backup.
   - Per eseguire il backup di tutti i volumi, selezionare la casella nella riga del titolo (Volume Name).
   - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (Volume_1).



4. Se si desidera che il backup di tutti i volumi correnti e futuri sia attivato, lasciare selezionata la casella di controllo "Backup automatico dei volumi futuri…". Se si disattiva questa impostazione, sarà necessario attivare manualmente i backup per i volumi futuri.
5. Fare clic su **Activate Backup** (attiva backup) per avviare il backup e il ripristino di BlueXP con i backup iniziali di ciascun volume selezionato.

Risultato

I file di backup vengono memorizzati in un bucket di storage cloud Google utilizzando la stessa sottoscrizione GCP e la stessa regione del sistema Cloud Volumes ONTAP.

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

Quali sono le prossime novità?

È possibile "avviare e arrestare i backup dei volumi o modificare la pianificazione del backup". Puoi anche farlo "ripristinare interi volumi da un file di backup" Come nuovo volume nello stesso cluster Kubernetes o in un altro cluster in GCP (nella stessa regione).

Gestione dei backup per i sistemi Kubernetes

Puoi gestire i backup per i tuoi sistemi Kubernetes modificando la pianificazione del backup, attivando/disattivando i backup dei volumi, eliminando i backup e molto altro ancora.

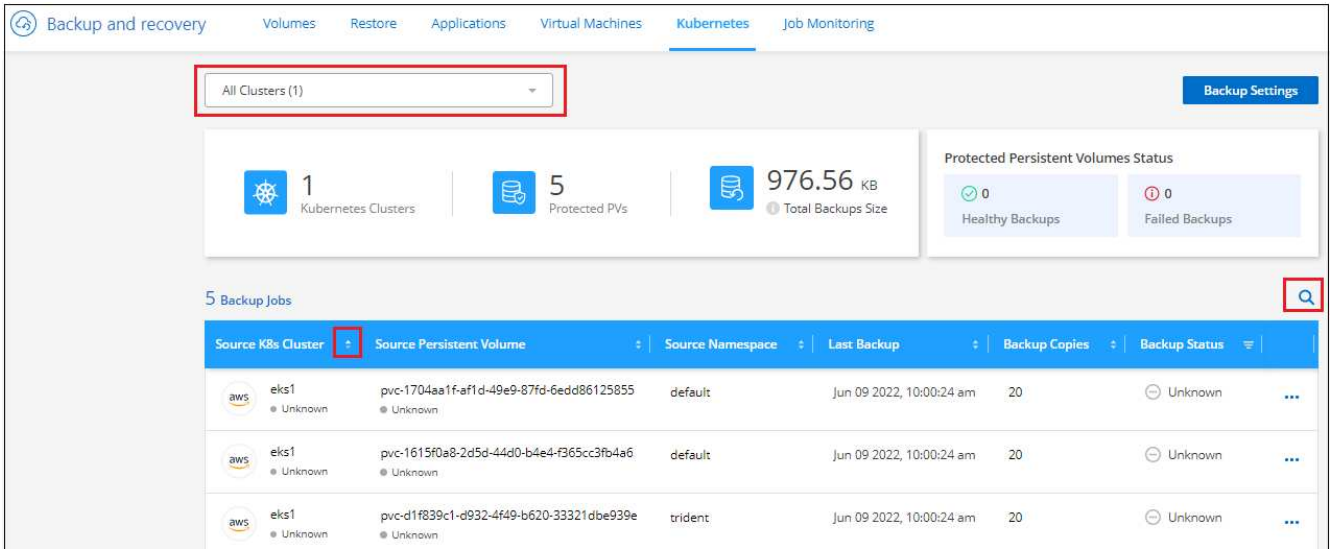
> Non gestire o modificare i file di backup direttamente dall'ambiente del cloud provider. Questo potrebbe danneggiare i file e causare una configurazione non supportata.

Visualizzazione dei volumi di cui viene eseguito il backup

È possibile visualizzare un elenco di tutti i volumi attualmente sottoposti a backup con il backup e ripristino di BlueXP.

Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Fare clic sulla scheda **Kubernetes** per visualizzare l'elenco dei volumi persistenti per i sistemi Kubernetes.



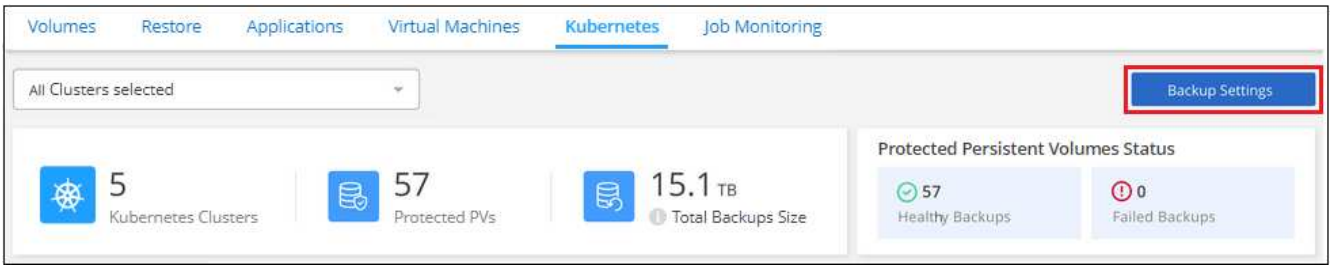
Se si cercano volumi specifici in determinati cluster, è possibile perfezionare l'elenco in base al cluster e al volume oppure utilizzare il filtro di ricerca.

Attivazione e disattivazione dei backup dei volumi

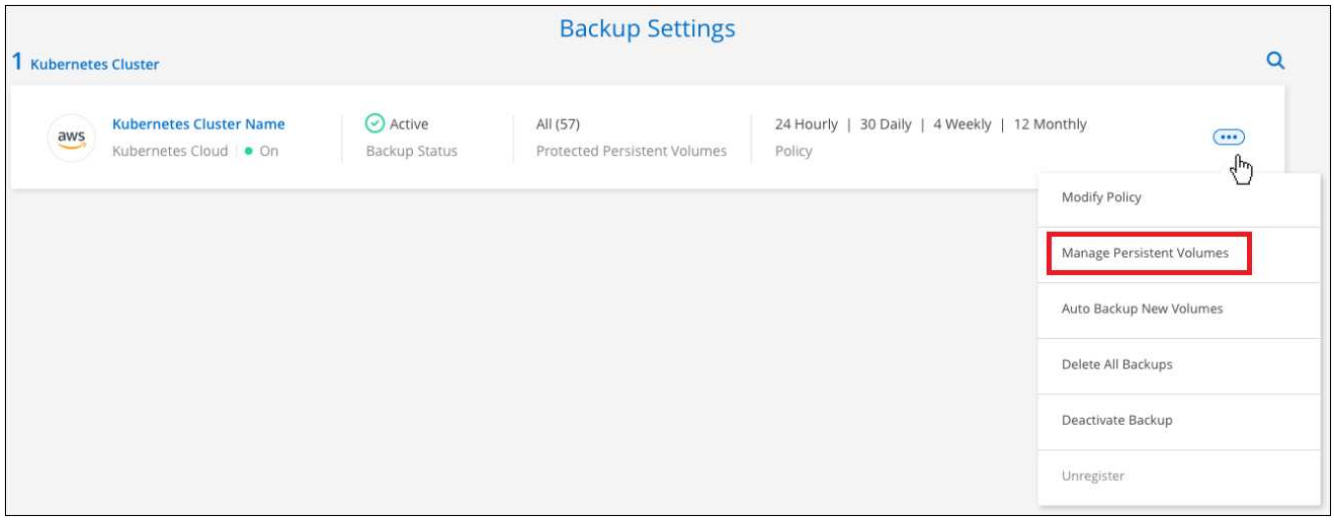
È possibile interrompere il backup di un volume se non sono necessarie copie di backup di quel volume e non si desidera pagare il costo di archiviazione dei backup. È inoltre possibile aggiungere un nuovo volume all'elenco di backup, se non viene eseguito il backup.

Fasi

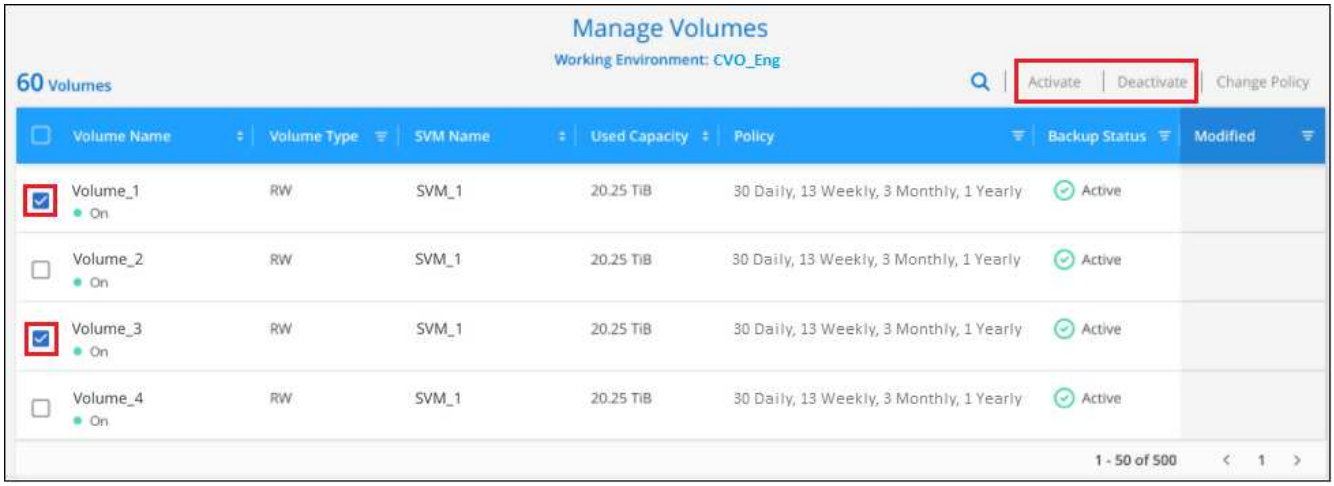
1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su ••• Per il cluster Kubernetes e selezionare **Manage Persistent Volumes** (Gestisci volumi persistenti).



3. Selezionare la casella di controllo di uno o più volumi da modificare, quindi fare clic su **Activate** o **Deactivate** (Disattiva) a seconda che si desideri avviare o interrompere i backup del volume.



4. Fare clic su **Save** (Salva) per confermare le modifiche.

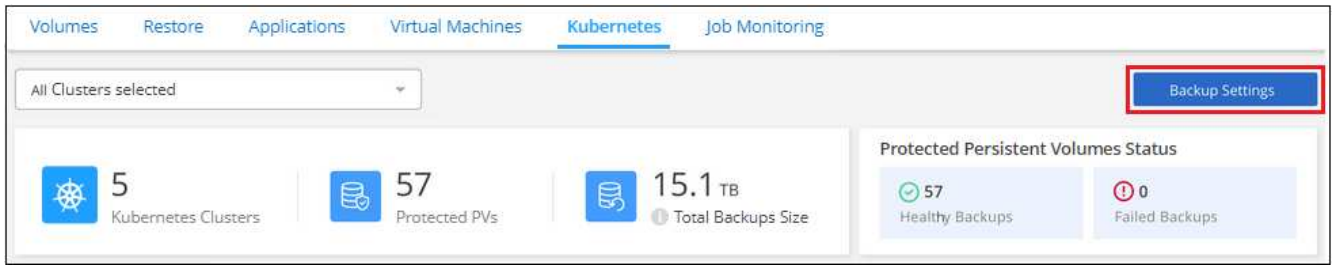
Nota: quando si interrompe il backup di un volume, il provider di cloud continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup a meno che non si utilizzi eliminare i backup.

Modifica di un criterio di backup esistente

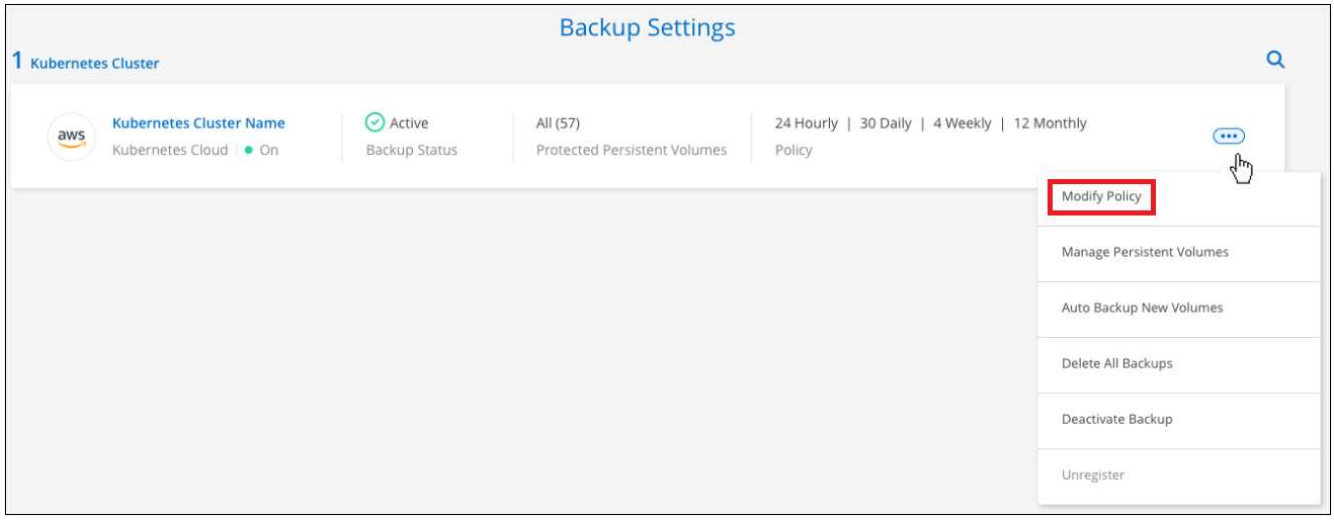
È possibile modificare gli attributi di un criterio di backup attualmente applicato ai volumi in un ambiente di lavoro. La modifica del criterio di backup influisce su tutti i volumi esistenti che utilizzano il criterio.

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.

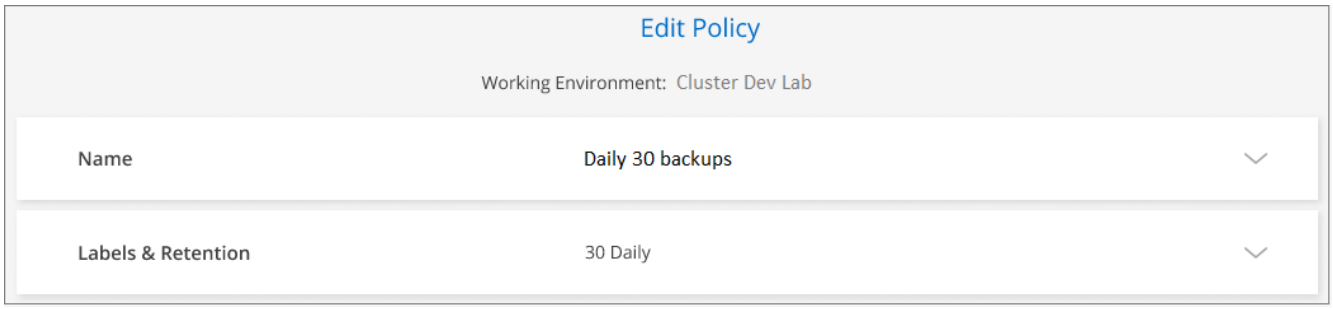


2. Nella pagina *Backup Settings*, fare clic su ••• Per l'ambiente di lavoro in cui si desidera modificare le impostazioni e selezionare **Gestisci policy**.



3. Dalla pagina *Manage Policies*, fare clic su **Edit Policy** (Modifica policy) per il criterio di backup che si desidera modificare in quell'ambiente di lavoro.

4. Dalla pagina *Edit Policy*, modificare la pianificazione e la conservazione del backup e fare clic su **Save** (Salva).



Impostazione di un criterio di backup da assegnare ai nuovi volumi

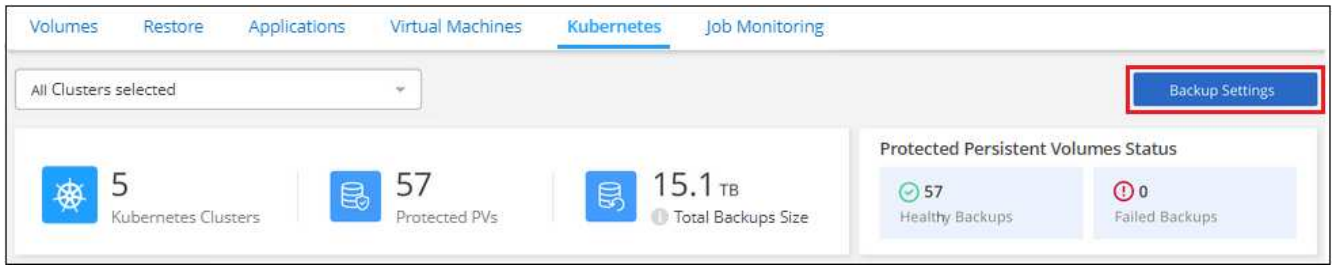
Se non è stata selezionata l'opzione che consente di assegnare automaticamente un criterio di backup ai volumi appena creati al momento dell'attivazione del backup e ripristino BlueXP sul cluster Kubernetes, è possibile scegliere questa opzione nella pagina *Backup Settings* più avanti. L'assegnazione di una policy di backup ai volumi appena creati garantisce la protezione di tutti i dati.

Tenere presente che il criterio che si desidera applicare ai volumi deve già esistere.

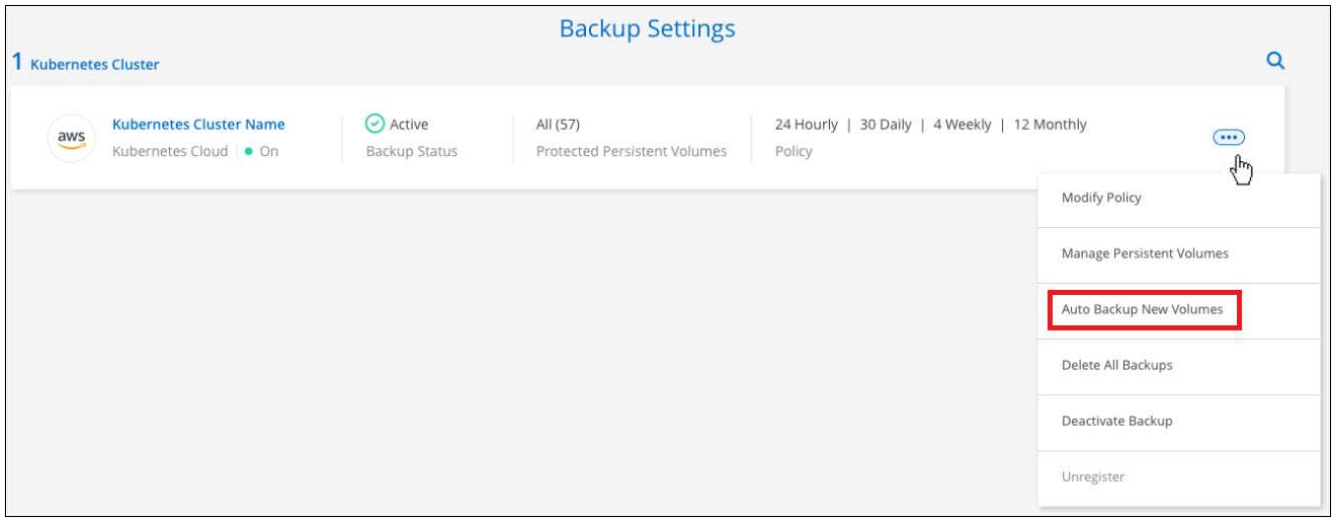
È inoltre possibile disattivare questa impostazione in modo che il backup dei volumi appena creati non venga eseguito automaticamente. In tal caso, sarà necessario attivare manualmente i backup per tutti i volumi specifici di cui si desidera eseguire il backup in futuro.

Fasi

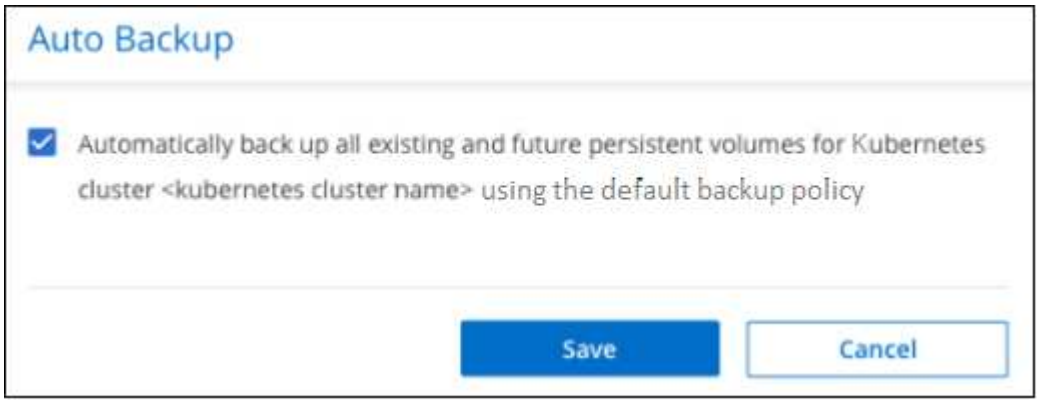
1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su ••• Per il cluster Kubernetes in cui sono presenti i volumi e selezionare **Backup automatico nuovi volumi**.



3. Selezionare la casella di controllo "Backup automatico dei volumi persistenti futuri…", scegliere il criterio di backup che si desidera applicare ai nuovi volumi e fare clic su **Salva**.



Risultato

A questo punto, questa policy di backup verrà applicata a tutti i nuovi volumi creati in questo cluster Kubernetes.

Visualizzazione dell'elenco dei backup per ciascun volume

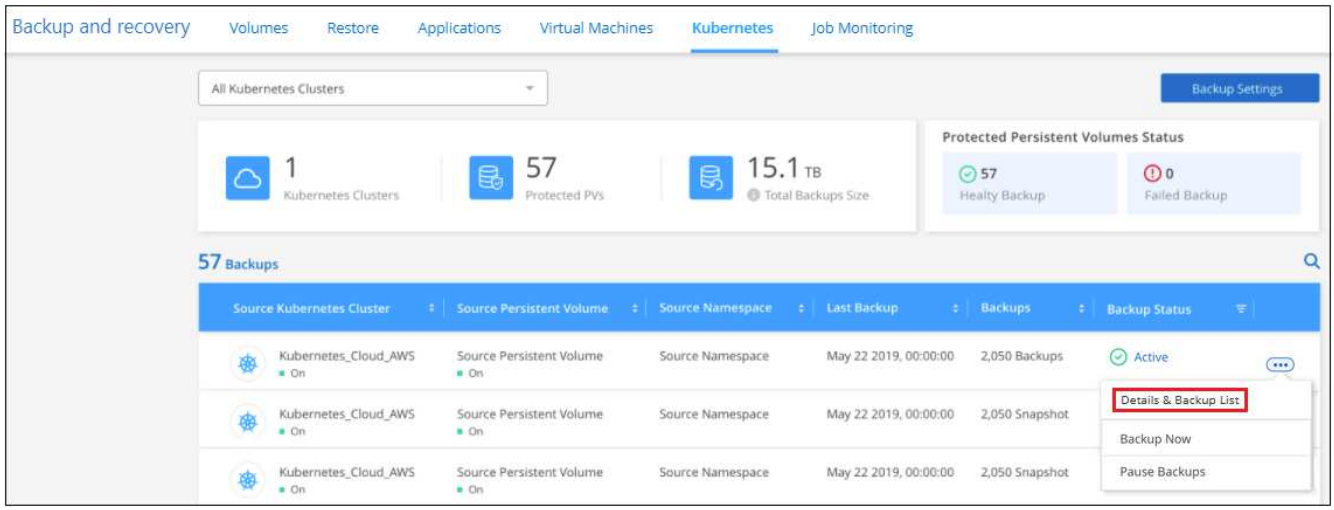
È possibile visualizzare l'elenco di tutti i file di backup esistenti per ciascun volume. In questa pagina vengono visualizzati i dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup, ad esempio l'ultimo backup eseguito, la policy di backup corrente, le dimensioni del file di backup e altro ancora.

Questa pagina consente inoltre di eseguire le seguenti operazioni:

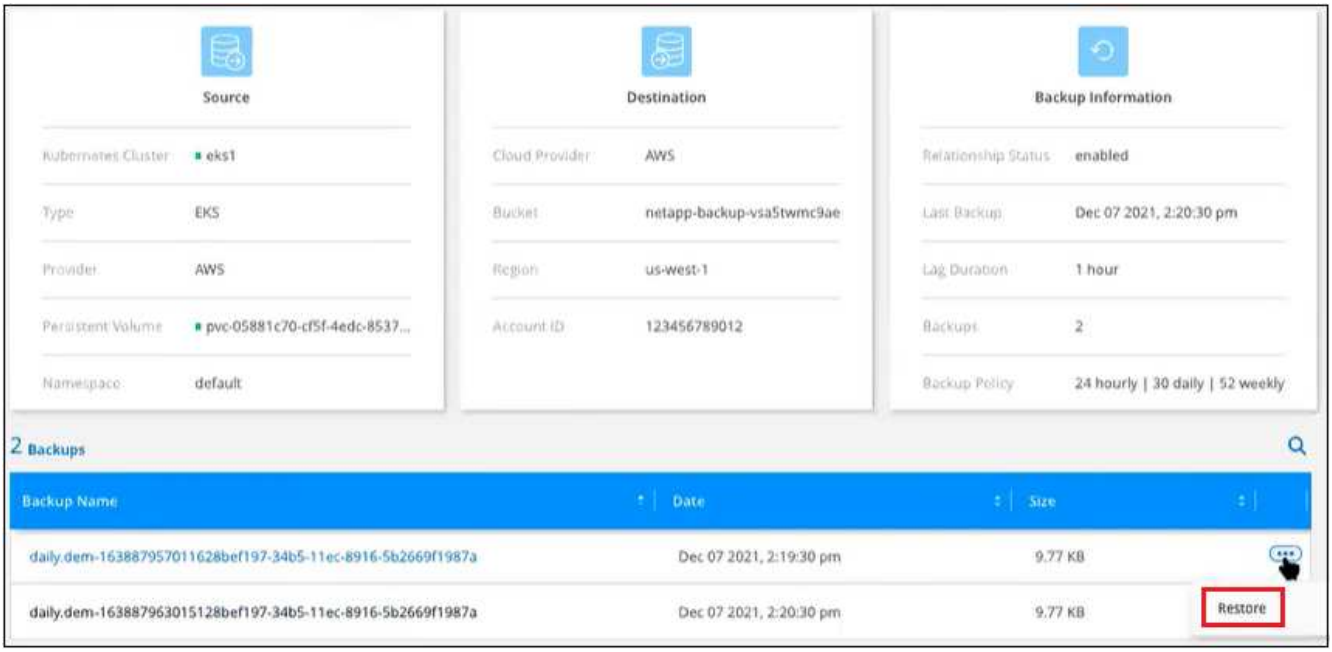
- Eliminare tutti i file di backup per il volume
- Eliminare singoli file di backup per il volume
- Scarica un report di backup per il volume

Fasi

1. Dalla scheda **Kubernetes**, fare clic su ••• Per il volume di origine e selezionare **Details & Backup List**.



   Viene visualizzato l'elenco di tutti i file di backup con i dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup.



Eliminazione dei 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 cluster Kubernetes. È possibile eliminare tutti i backup se non sono più necessari o se è stato eliminato il volume di origine e si desidera rimuovere tutti i backup.

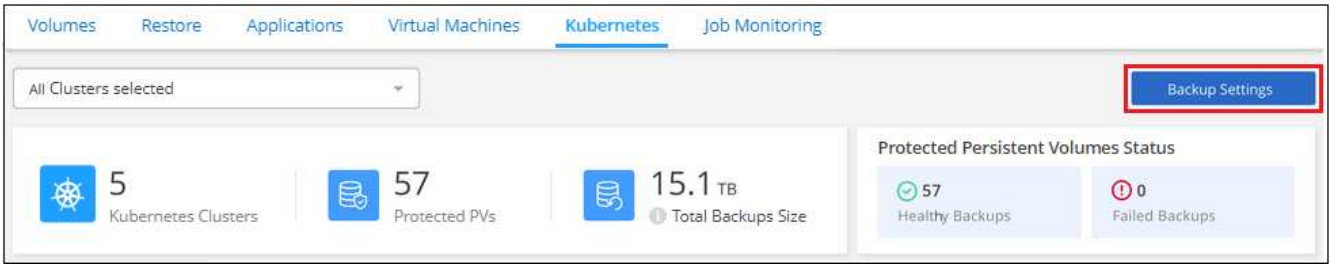
> Se si prevede di eliminare un ambiente di lavoro o un cluster con backup, è necessario eliminare i backup **prima** di eliminare il sistema. Il backup e il ripristino di BlueXP non eliminano automaticamente i backup quando si elimina un sistema e non esiste attualmente alcun supporto nell'interfaccia 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.

Eliminazione di tutti i file di backup per un ambiente di lavoro

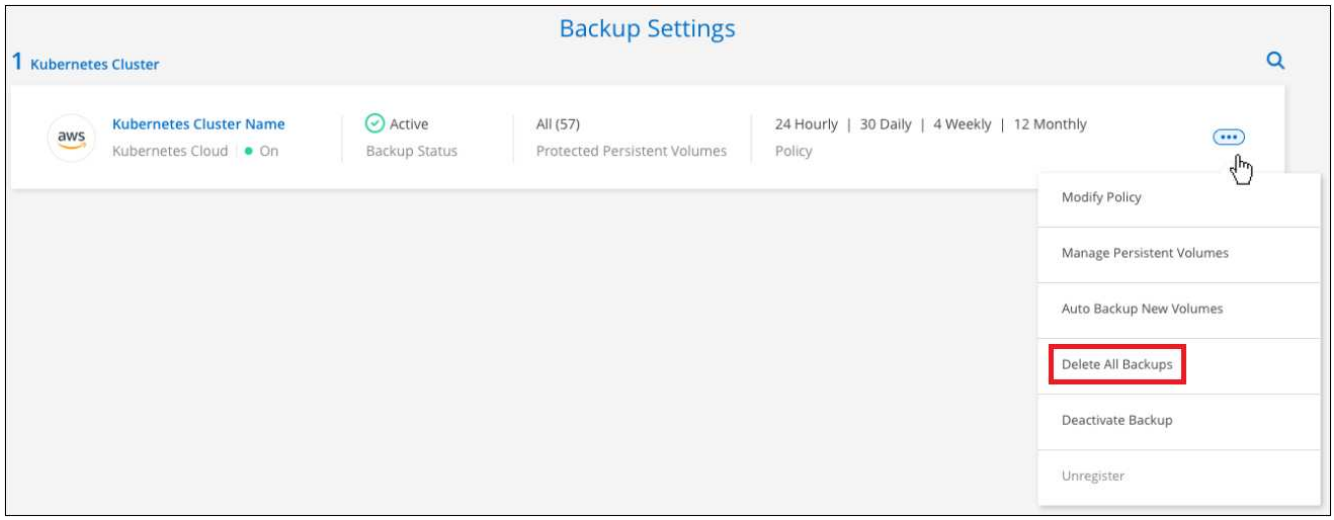
L'eliminazione di tutti i backup per un ambiente di lavoro non disattiva i backup futuri dei volumi in questo ambiente di lavoro. Se si desidera interrompere la creazione di backup di tutti i volumi in un ambiente di lavoro, è possibile disattivare i backup come descritto qui.

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Fare clic su ••• Per il cluster Kubernetes in cui si desidera eliminare tutti i backup e selezionare **Delete All backups** (Elimina tutti i backup).



3. Nella finestra di dialogo di conferma, immettere il nome dell'ambiente di lavoro e fare clic su **Delete** (Elimina).

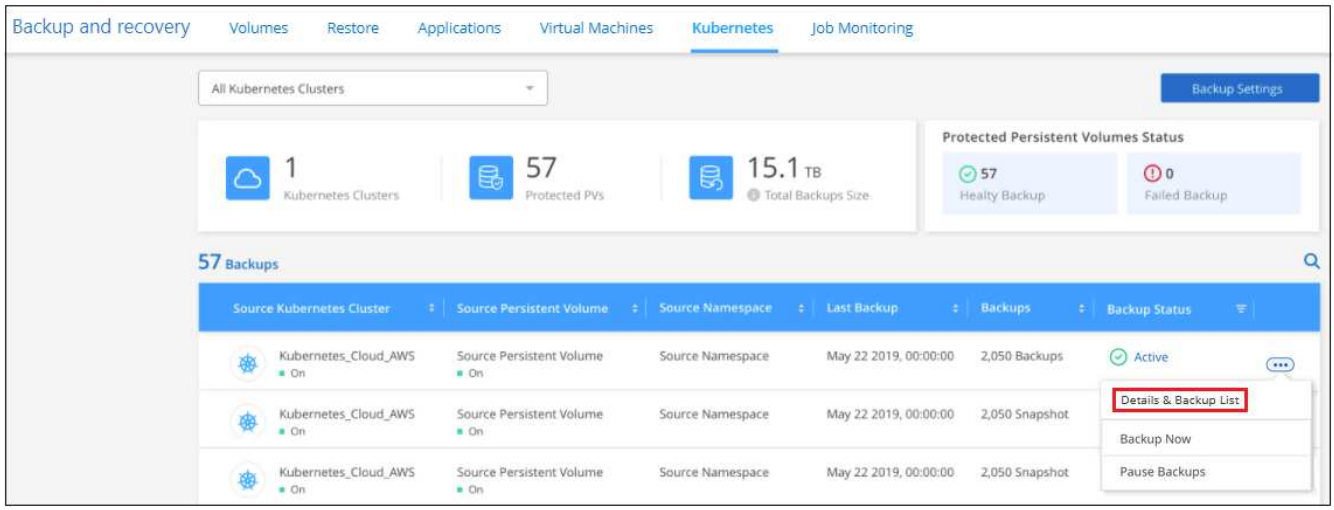
Eliminazione di tutti i file di backup di un volume

L'eliminazione di tutti i backup per un volume disattiva anche i backup futuri per quel volume.

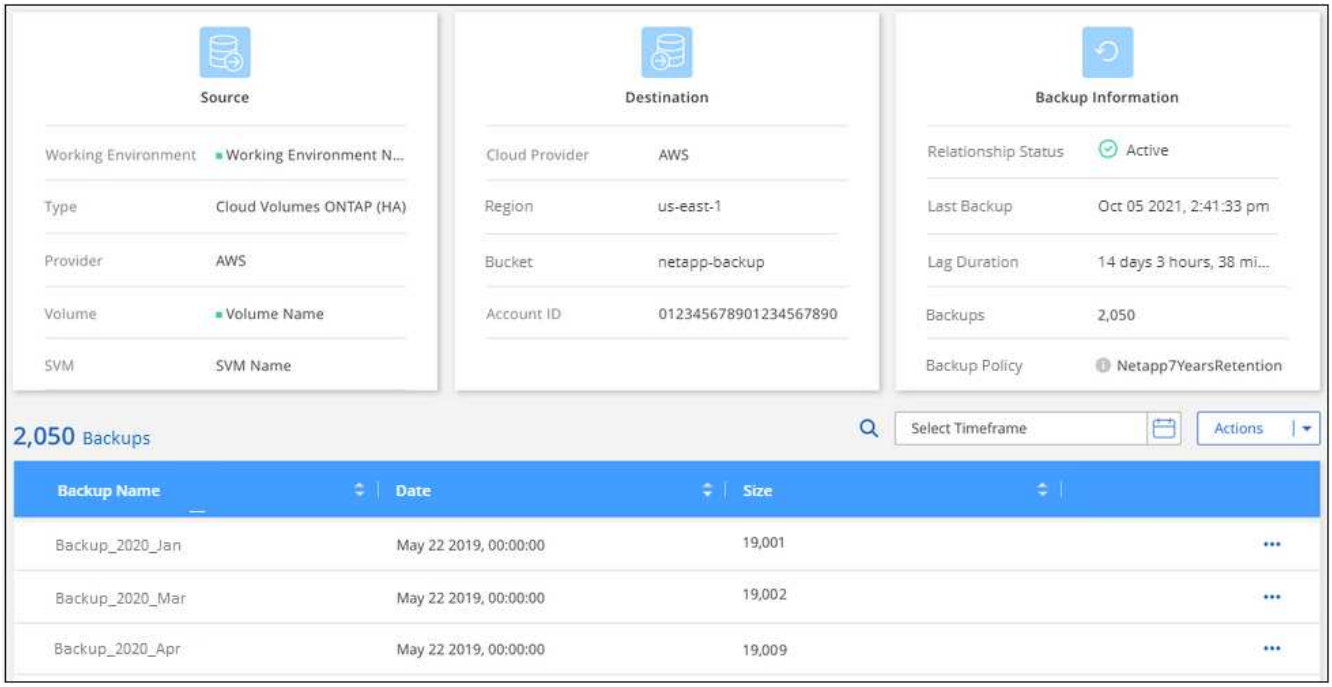
È possibile riavviare l'esecuzione dei backup per il volume In qualsiasi momento dalla pagina Gestisci backup.

Fasi

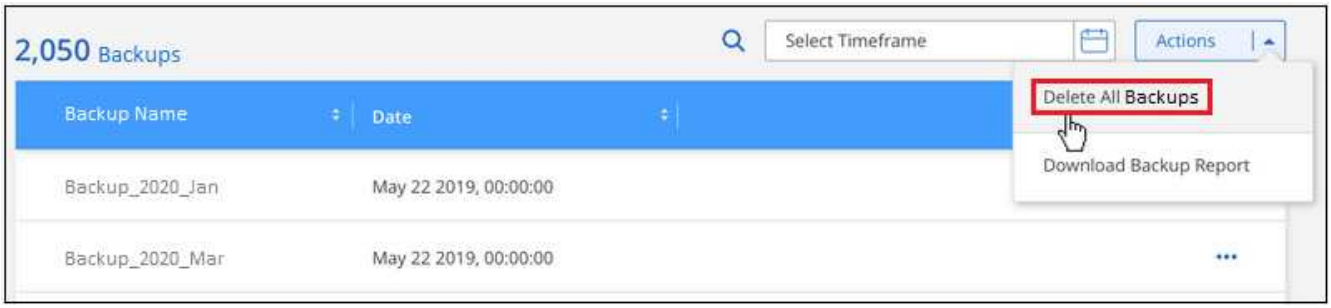
1. Dalla scheda **Kubernetes**, fare clic su ••• Per il volume di origine e selezionare **Details & Backup List**.



Viene visualizzato l'elenco di tutti i file di backup.



2. Fare clic su **azioni** > **Elimina tutti i backup**.



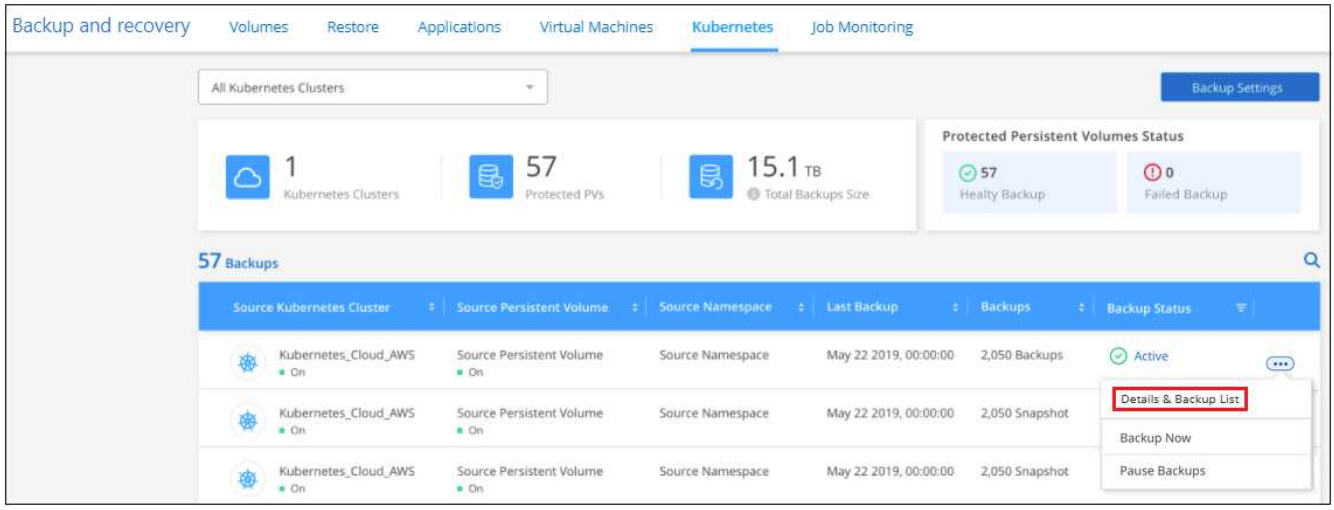
3. Nella finestra di dialogo di conferma, inserire il nome del volume e fare clic su **Delete** (Elimina).

Eliminazione di un singolo file di backup per un volume

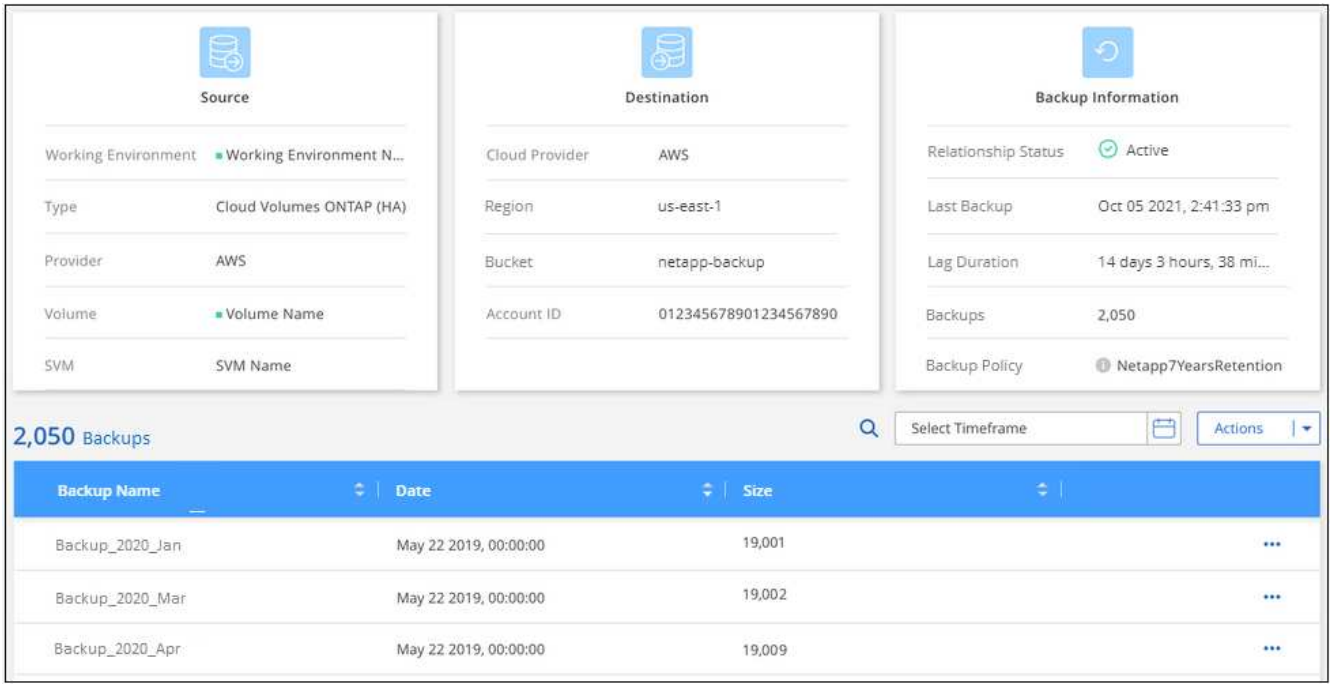
È possibile eliminare un singolo file di backup. Questa funzione è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.8 o superiore.

Fasi

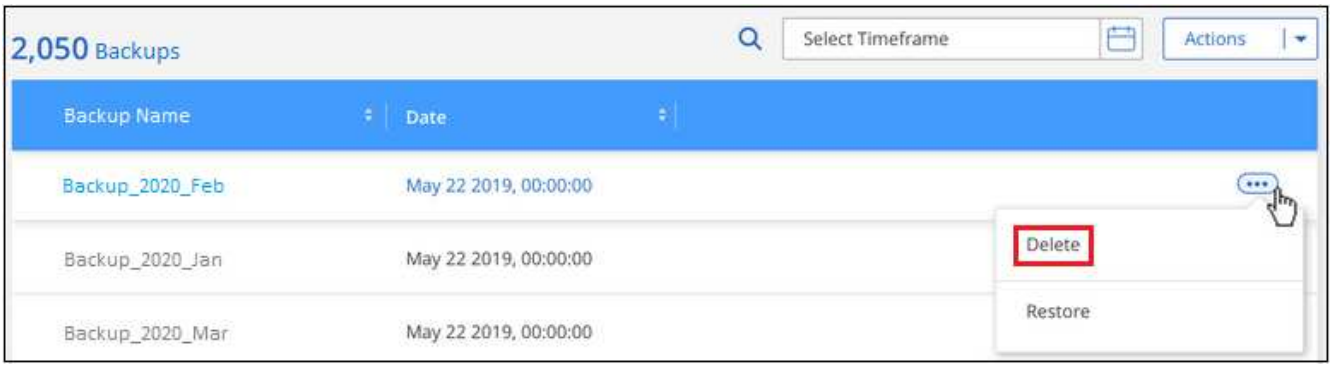
1. Dalla scheda **Kubernetes**, fare clic su ••• Per il volume di origine e selezionare **Details & Backup List**.



Viene visualizzato l'elenco di tutti i file di backup.



2. Fare clic su ••• Per il file di backup del volume che si desidera eliminare e fare clic su **Delete** (Elimina).



3. Nella finestra di dialogo di conferma, fare clic su **Delete** (Elimina).

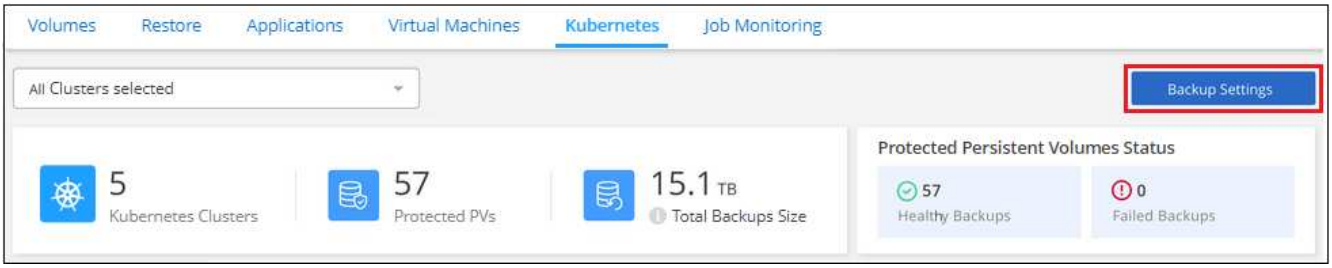
Disattivazione del backup e ripristino BlueXP per un ambiente di lavoro

La disattivazione del backup e ripristino di 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.

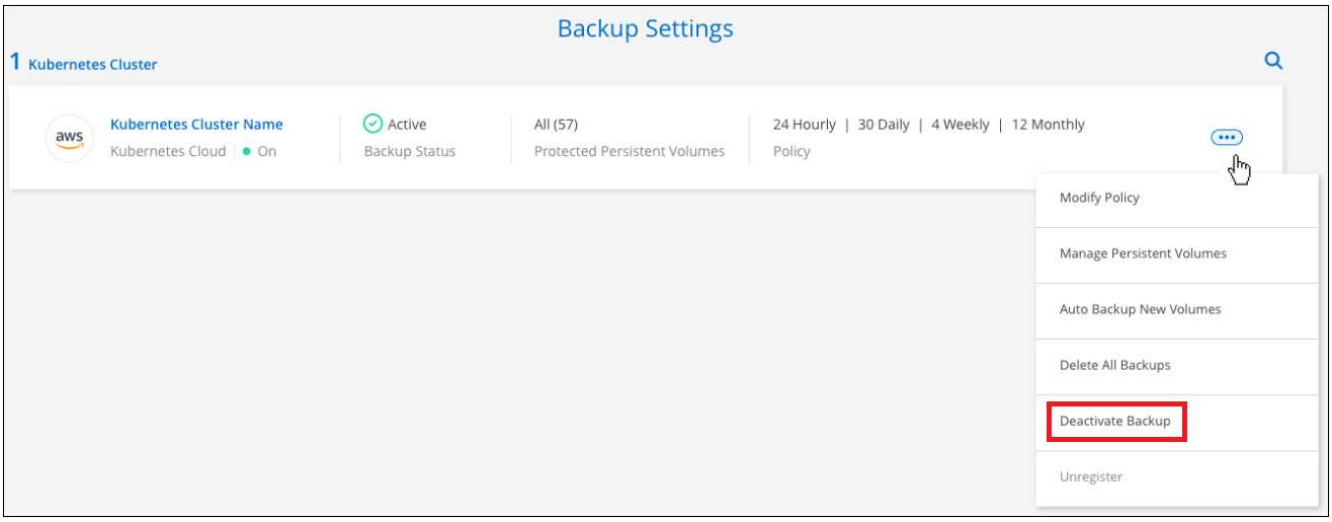
Tieni presente che il tuo cloud provider continuerà a addebitare i costi dello storage a oggetti per la capacità utilizzata dai backup, a meno che tu non lo utilizzi eliminare i backup.

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro o il cluster Kubernetes, in cui si desidera disattivare i backup e selezionare **Disattiva backup**.



3. Nella finestra di dialogo di conferma, fare clic su **Disattiva**.

> Quando il backup è disattivato, viene visualizzato il pulsante **Activate Backup** (attiva backup) per quell'ambiente di lavoro. Fare clic su questo pulsante per riattivare la funzionalità di backup per l'ambiente di lavoro.

Annullamento della registrazione di 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 funzionalità viene utilizzata quando si intende eliminare un cluster Kubernetes 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.

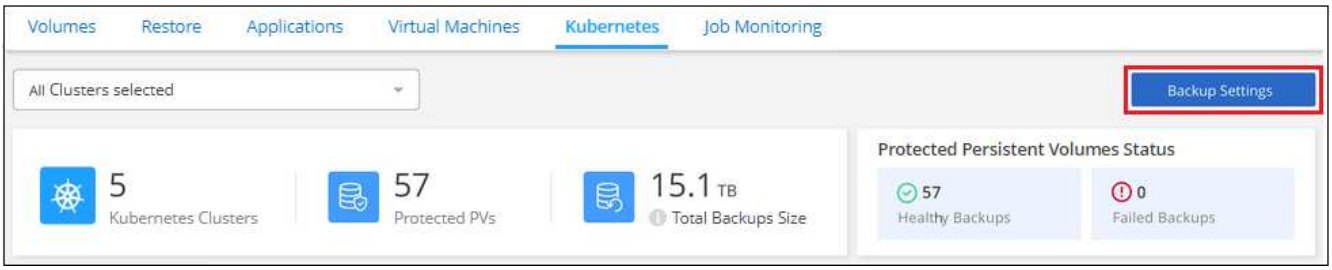
Prima di annullare la registrazione di backup e ripristino BlueXP, è necessario eseguire le seguenti operazioni, nell'ordine indicato:

- Disattivare il backup e ripristino BlueXP per l'ambiente di lavoro
- Eliminare tutti i backup per l'ambiente di lavoro

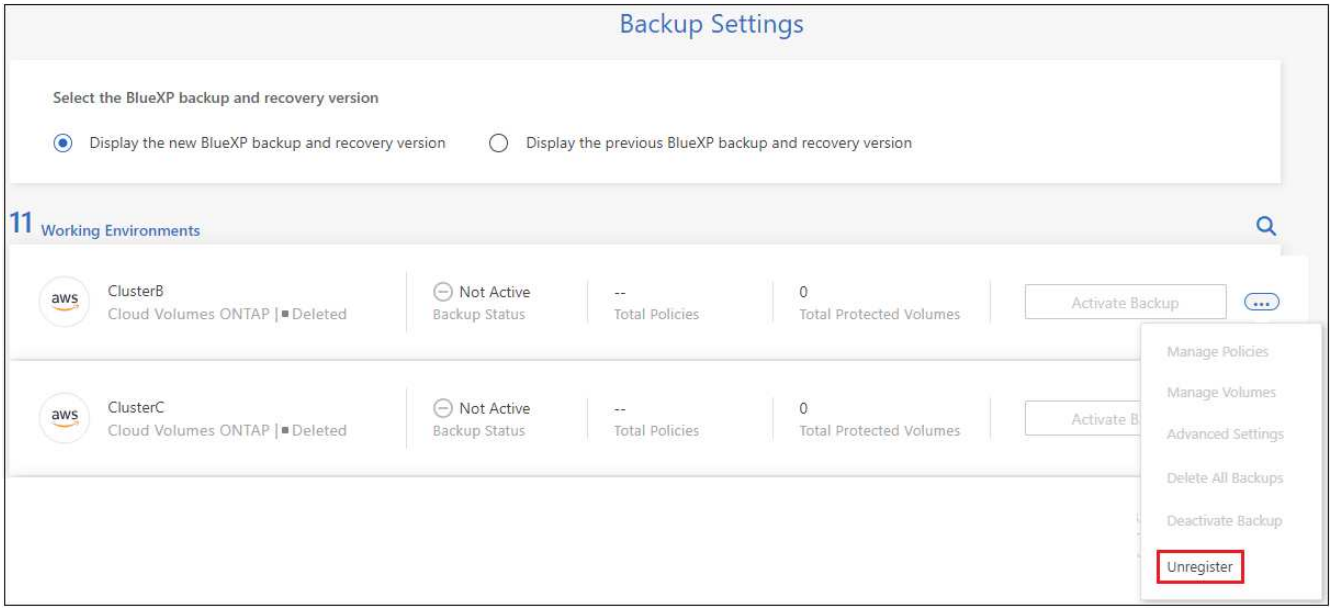
L'opzione di annullamento della registrazione non è disponibile fino al completamento di queste due azioni.

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su ••• Per il cluster Kubernetes in cui si desidera annullare la registrazione del servizio di backup e selezionare **Annulla registrazione**.



3. Nella finestra di dialogo di conferma, fare clic su **Annulla registrazione**.

Ripristino dei dati Kubernetes dai file di backup

I backup vengono memorizzati in un archivio di oggetti nel tuo account cloud in modo da poter ripristinare i dati da un punto specifico. È possibile ripristinare un intero volume

persistente Kubernetes da un file di backup salvato.

Puoi ripristinare un volume persistente (come nuovo volume) nello stesso ambiente di lavoro o in un ambiente di lavoro diverso che utilizza lo stesso account cloud.

Ambienti di lavoro supportati e provider di storage a oggetti

È possibile ripristinare un volume da un file di backup di Kubernetes nei seguenti ambienti di lavoro:

Percorso del file di backup	Ambiente di lavoro di destinazione ifdef::aws[]
Amazon S3	Cluster Kubernetes in AWS endif::aws[] ifdef::Azure[]
Azure Blob	Cluster Kubernetes in Azure endif::Azure[] ifdef::gcp[]
Storage Google Cloud	Cluster Kubernetes in Google endif::gcp[]

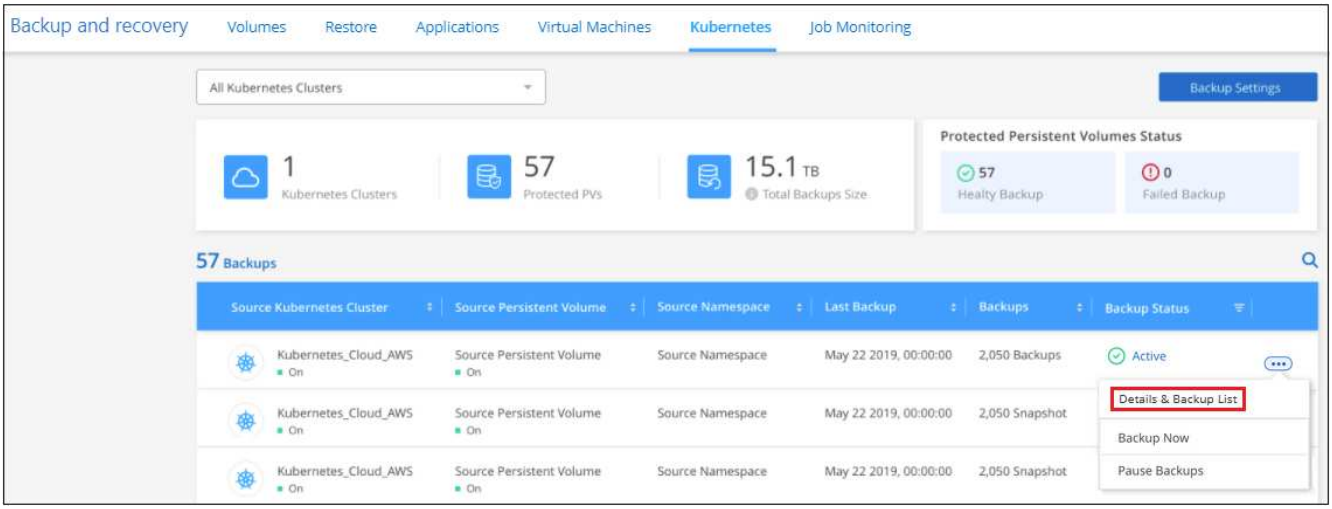
Ripristino dei volumi da un file di backup di Kubernetes

Quando si ripristina un volume persistente da un file di backup, BlueXP crea un *nuovo* volume utilizzando i dati del backup. È possibile ripristinare i dati in un volume nello stesso cluster Kubernetes o in un cluster Kubernetes diverso che si trova nello stesso account cloud del cluster Kubernetes di origine.

Prima di iniziare, è necessario conoscere il nome del volume che si desidera ripristinare e la data del file di backup che si desidera utilizzare per creare il volume appena ripristinato.

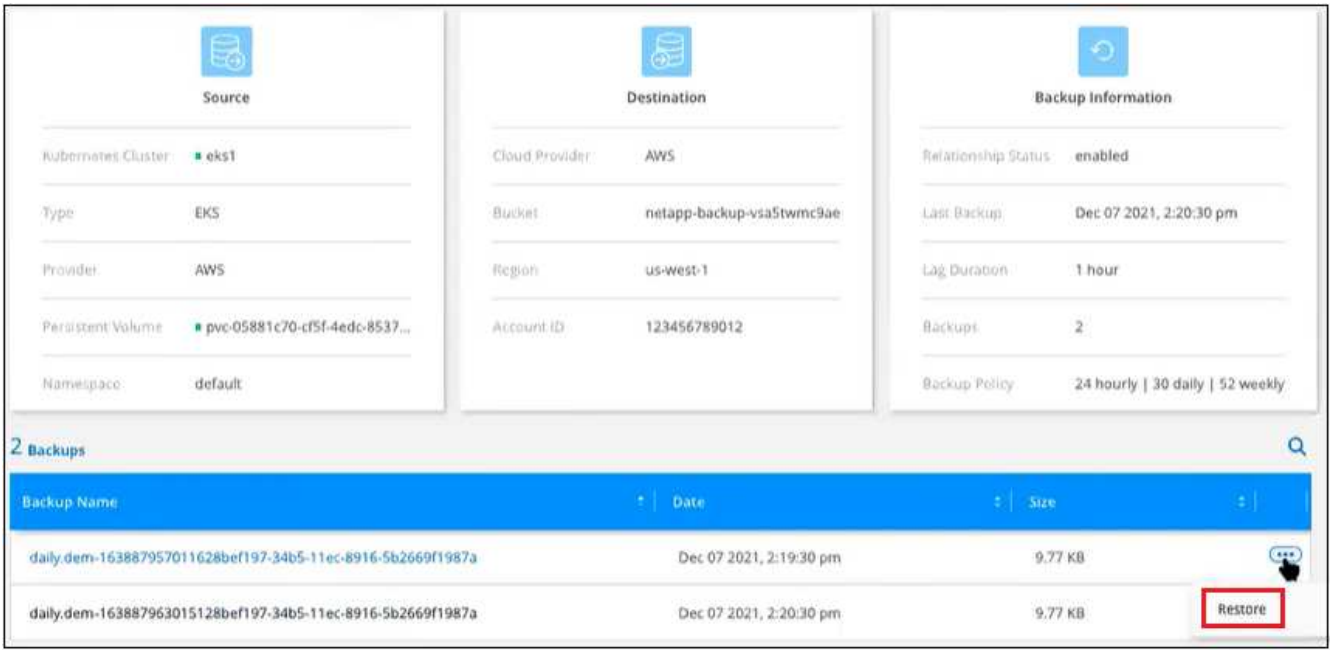
Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Fare clic sulla scheda **Kubernetes** per visualizzare la dashboard Kubernetes.



3. Individuare il volume che si desidera ripristinare, quindi fare clic su •••, Quindi fare clic su **Details & Backup List**.

   Viene visualizzato l'elenco di tutti i file di backup per quel volume, insieme ai dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup.



4. Individuare il file di backup specifico che si desidera ripristinare in base alla data/ora, quindi fare clic su •••E quindi **Restore**.
5. Nella pagina *Select Destination*, selezionare il cluster *Kubernetes* in cui si desidera ripristinare il volume, il *namespace*, la *Storage Class* e il nuovo *nome del volume persistente*.

6. Fare clic su **Restore** (Ripristina) per tornare alla dashboard di Kubernetes, in modo da esaminare l'avanzamento dell'operazione di ripristino.

Risultato

BlueXP crea un nuovo volume nel cluster Kubernetes in base al backup selezionato. È possibile "gestire le impostazioni di backup per questo nuovo volume" secondo necessità.

API di backup e ripristino BlueXP

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

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.

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…y6nyhBjwkeMwHc4ValobjUmju2x0xUH48g` 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 API

La documentazione per ciascuna API di backup e ripristino BlueXP è disponibile all'interno del sito

https://docs.netapp.com/us-en/bluexp-automation/cbs/overview.html.

Riferimento

Classi di storage di archivio AWS S3 e tempi di recupero del ripristino

Il backup e ripristino BlueXP supporta due classi di storage di archiviazione S3 e la maggior parte delle regioni.

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 relativa a. ripristino dei dati dallo storage di archiviazione.

- 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".

Ripristino dei dati dallo storage di archiviazione

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

Tier di archiviazione	Ripristinare priorità e costi		
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 archiviazione Azure e tempi di recupero del ripristino

Il backup e ripristino BlueXP supporta un unico livello di accesso per l'archiviazione Azure e la maggior parte delle regioni.

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 successiva su ripristino dei dati dallo storage di archiviazione.

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".

Ripristino dei dati dallo storage di archiviazione

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".

Classi di storage di archivio e tempi di recupero di Google

Il backup e ripristino BlueXP supporta una classe di storage di archiviazione Google e la maggior parte delle regioni.

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 relativa a. ripristino dei

dati dallo storage di archiviazione.

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".

Ripristino dei dati dallo storage di archiviazione

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.

Configurare il backup per l'accesso multi-account in Azure

Il backup e ripristino BlueXP consente di creare file di backup in un account Azure diverso da quello in cui risiedono i volumi Cloud Volumes ONTAP di origine. Entrambi gli account possono essere diversi dall'account in cui si trova BlueXP Connector.

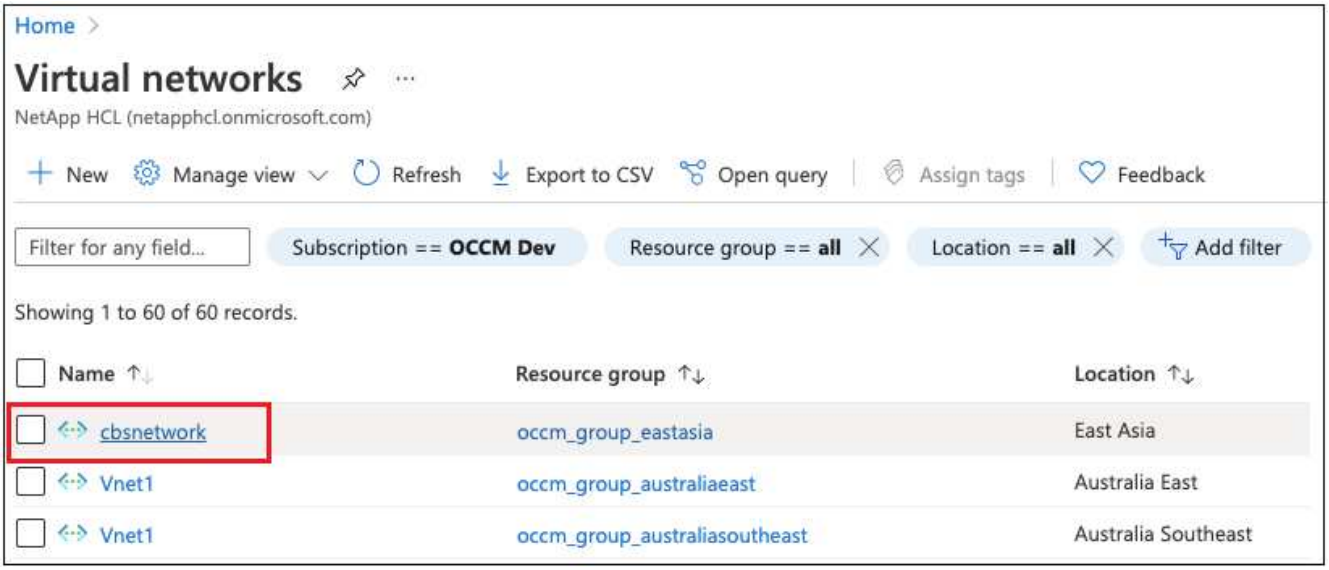
Questi passaggi sono necessari solo quando si è "Backup dei dati Cloud Volumes ONTAP nello storage Azure Blob".

Seguire i passaggi riportati di seguito per configurare la configurazione in questo modo.

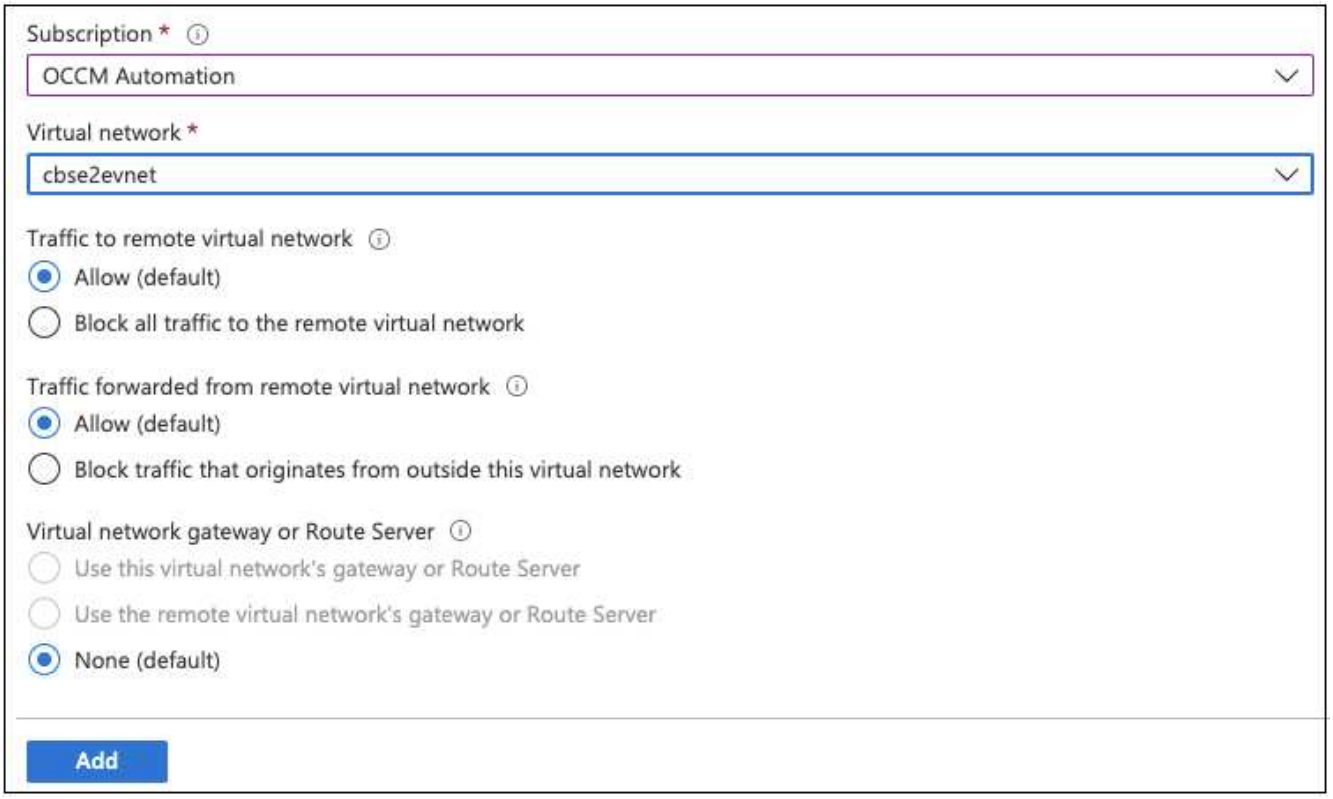
Impostare il peering VNET tra gli account

Si noti che se si desidera che BlueXP gestisca il sistema Cloud Volumes ONTAP in un account/regione differente, è necessario configurare il peering VNET. Il peering VNET non è richiesto per la connettività degli account di storage.

1. Accedere al portale Azure e da casa, selezionare Virtual Networks (reti virtuali).
2. Selezionare l'abbonamento che si sta utilizzando come abbonamento 1 e fare clic su VNET in cui si desidera impostare il peering.

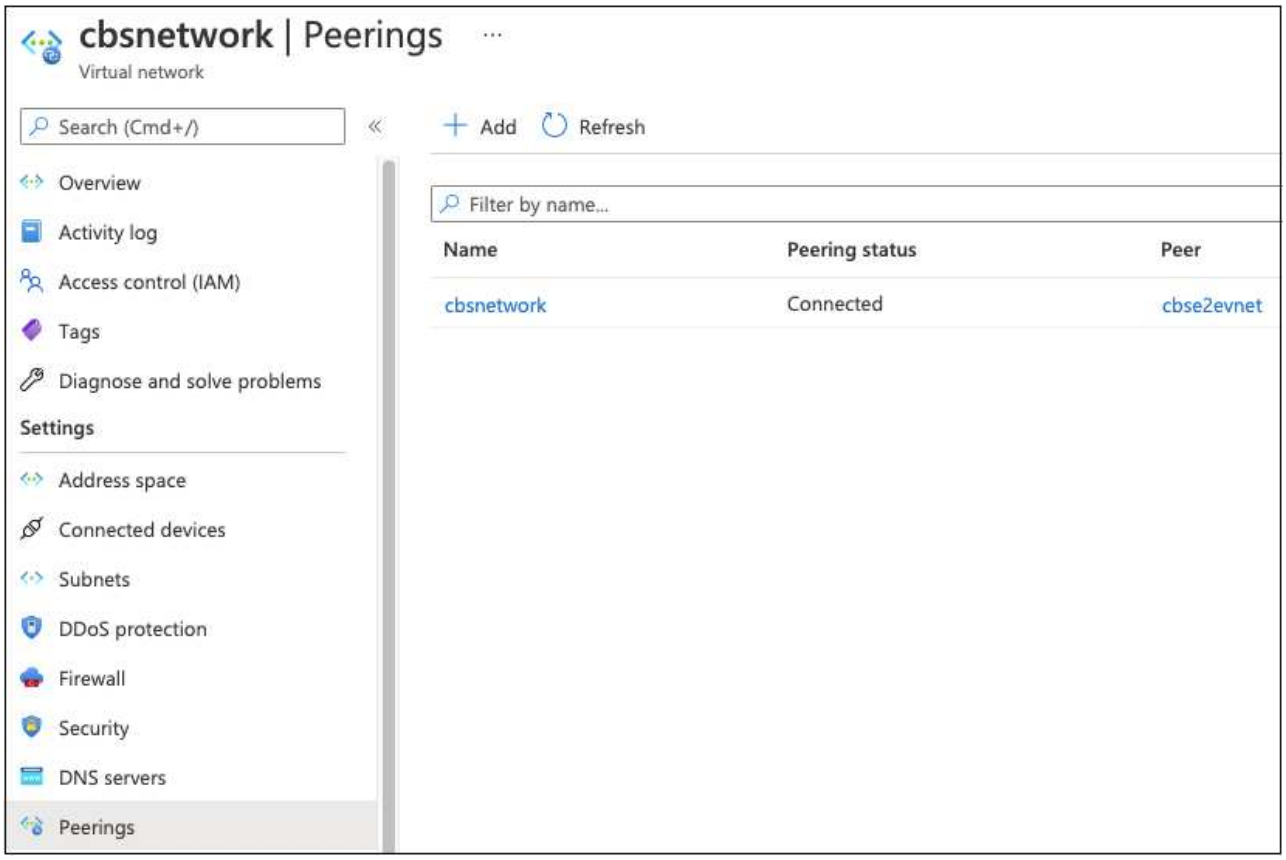


3. Selezionare **cbsnetwork** e dal pannello di sinistra, fare clic su **Peerings**, quindi fare clic su **Add**.

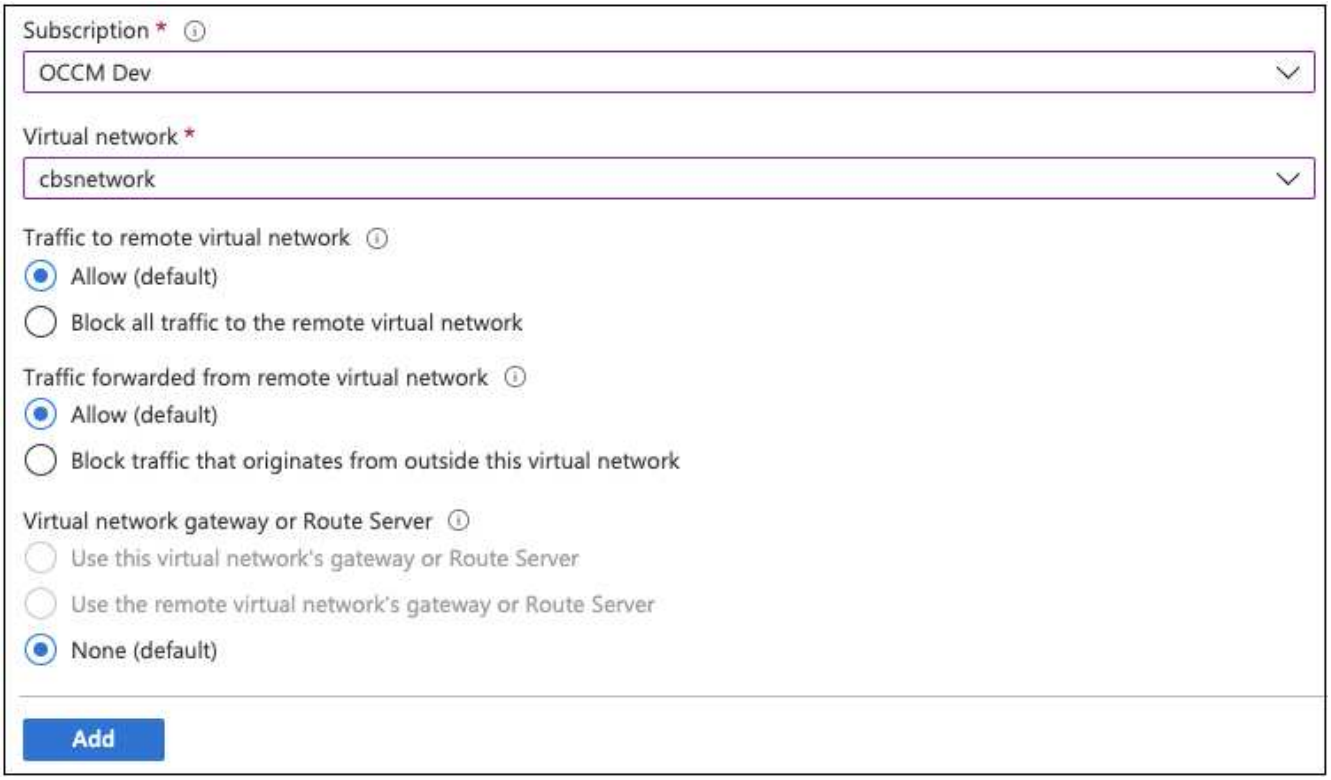


4. Inserire le seguenti informazioni nella pagina di peering, quindi fare clic su **Aggiungi**.
   - Peering link name for this network (Nome collegamento peering per questa rete): È possibile assegnare un nome qualsiasi per identificare la connessione peering.
   - Remote virtual network peering link name (Nome collegamento peering rete virtuale remota): Immettere un nome per identificare il VNET remoto.
   - Mantenere tutte le selezioni come valori predefiniti.
   - In Subscription (abbonamento), selezionare l'abbonamento 2.
   - Virtual network (rete virtuale), selezionare la rete virtuale con abbonamento 2 a cui si desidera

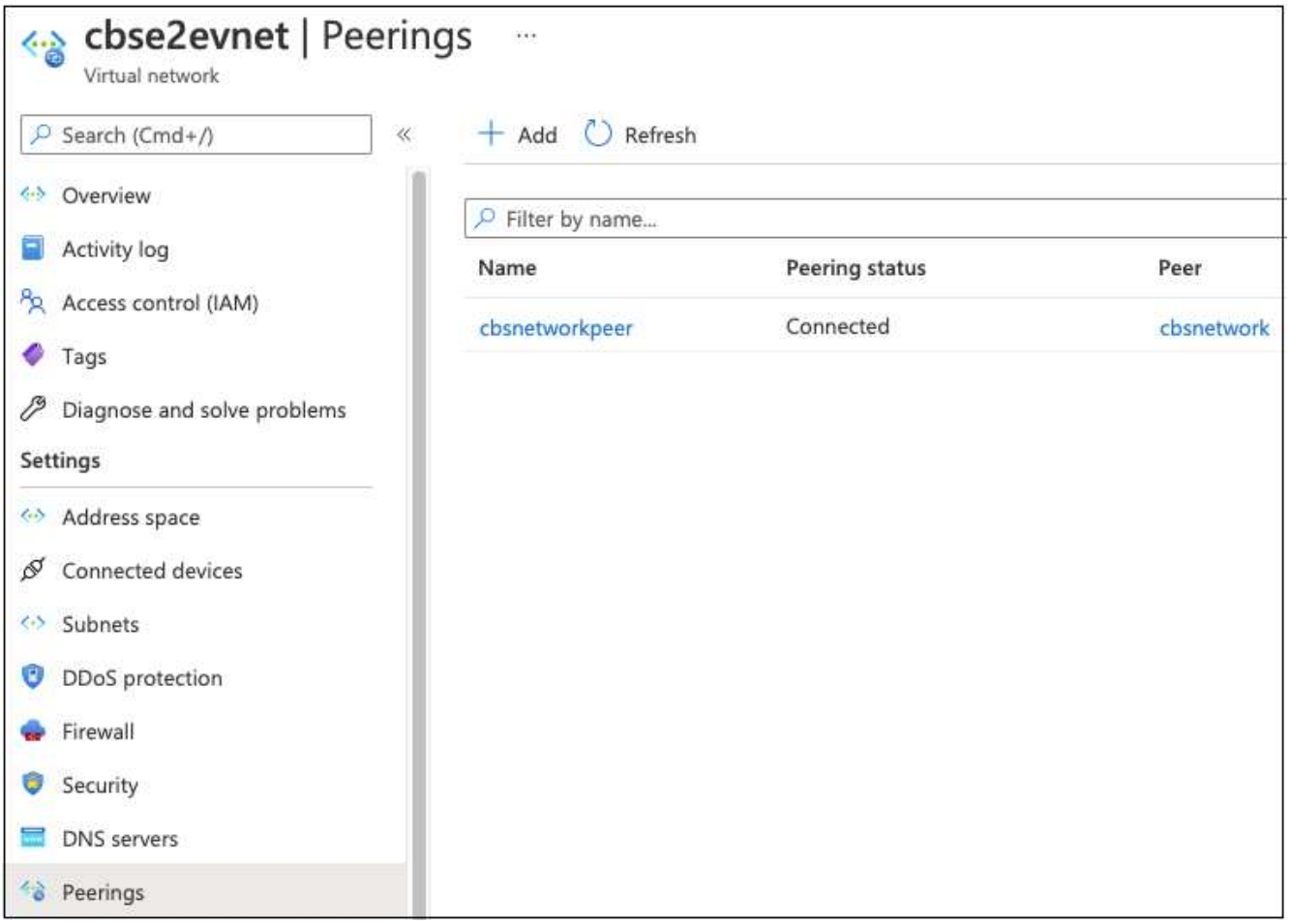
impostare il peering.



5. Eseguire le stesse operazioni in Subscription 2 VNET e specificare l'abbonamento e i dettagli VNET remoti dell'abbonamento 1.



Vengono aggiunte le impostazioni di peering.



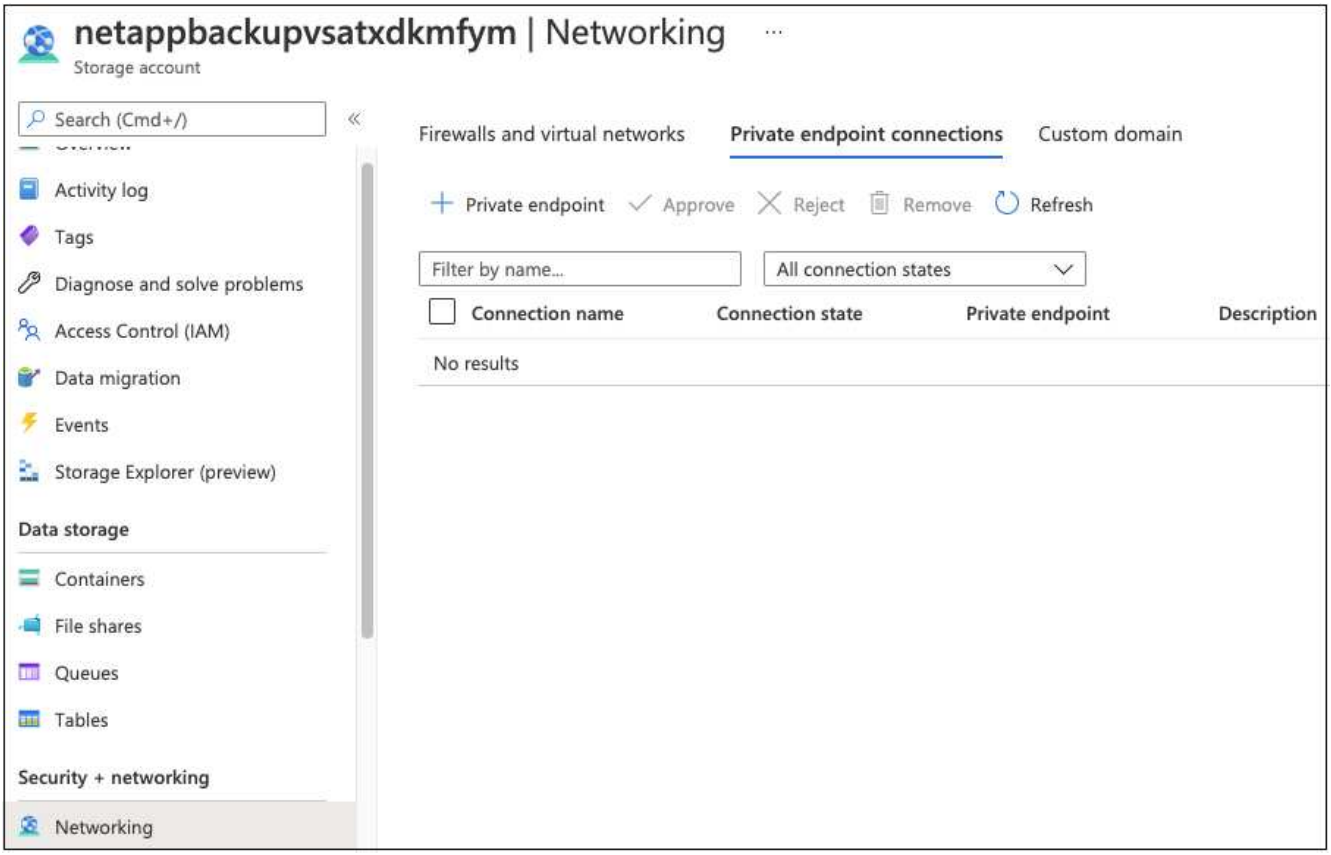
Creare un endpoint privato per l'account storage

Ora è necessario creare un endpoint privato per l'account storage. In questo esempio, l'account storage viene creato nell'abbonamento 1 e il sistema Cloud Volumes ONTAP viene eseguito nell'abbonamento 2.

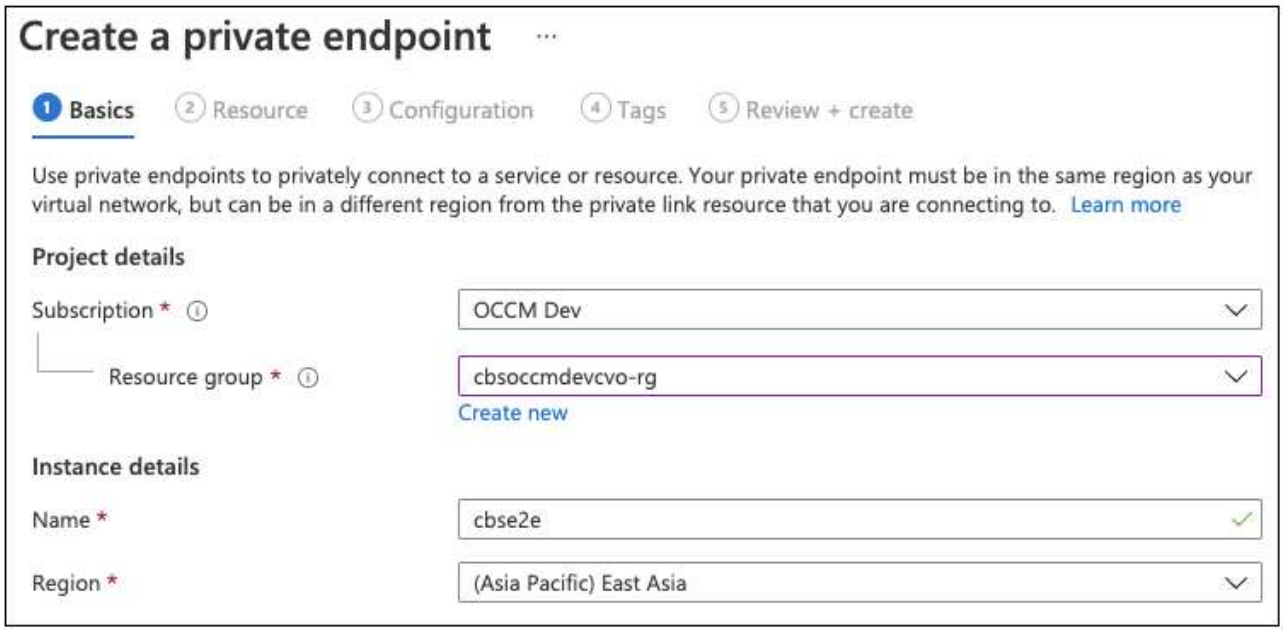
> Per eseguire la seguente azione, è necessario disporre dell'autorizzazione di un collaboratore di rete.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

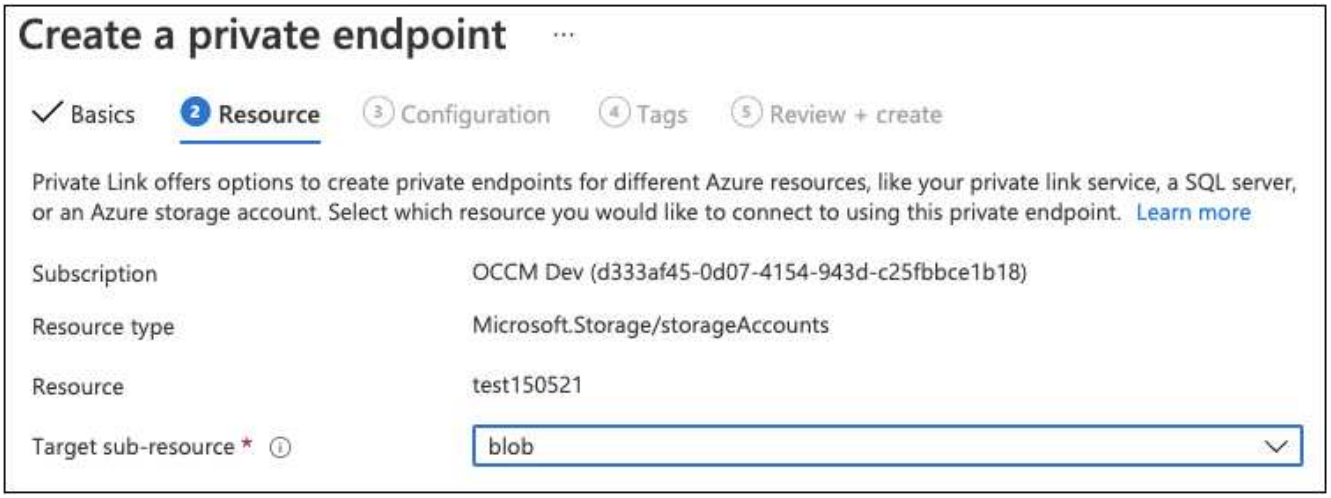
1. Accedere all'account Storage > Networking > Private endpoint Connections e fare clic su **+ Private endpoint**.



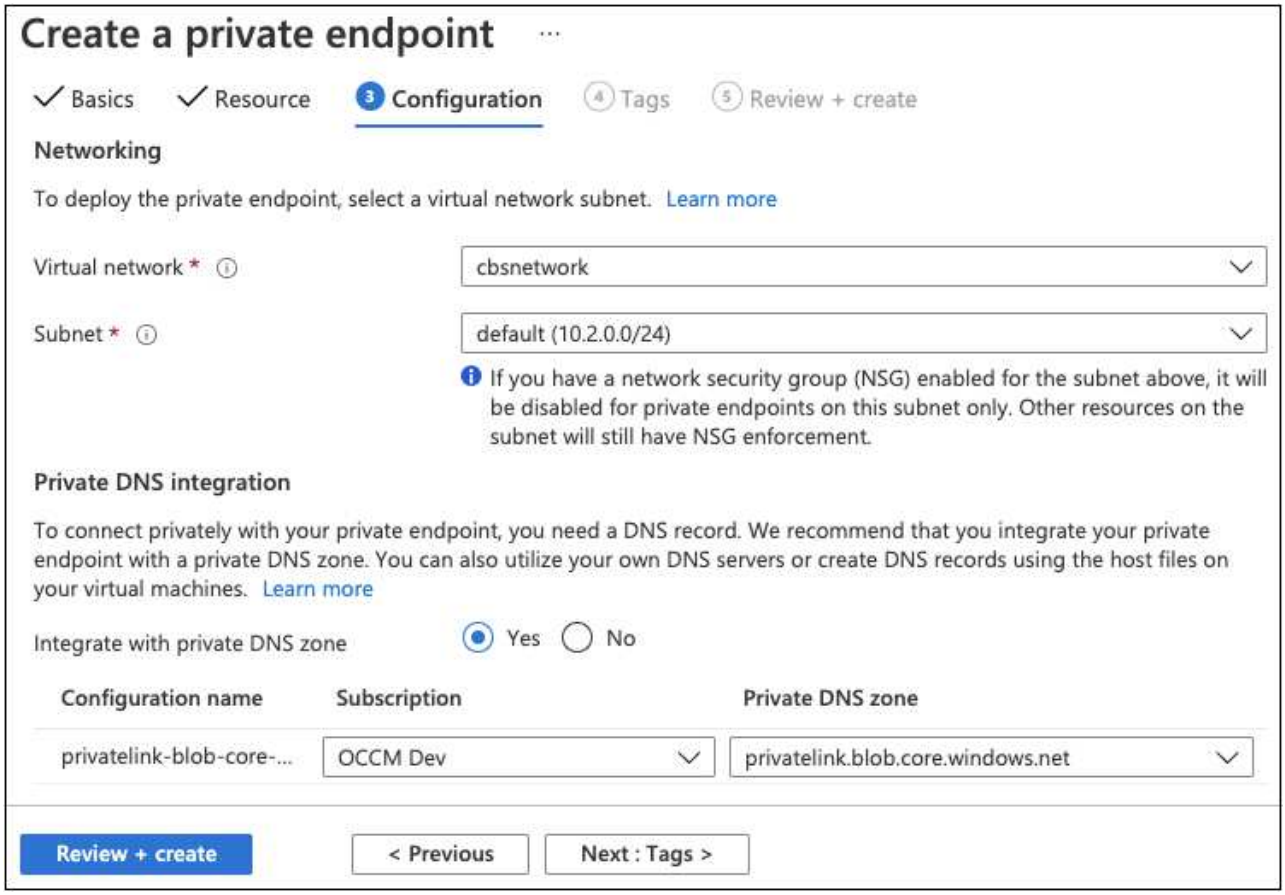
2. Nella pagina *Basics* dell'endpoint privato:
   - Selezionare Subscription 2 (abbonamento 2) (in cui vengono implementati il connettore BlueXP e il sistema Cloud Volumes ONTAP) e il gruppo di risorse.
   - Inserire un nome endpoint.
   - Selezionare la regione.



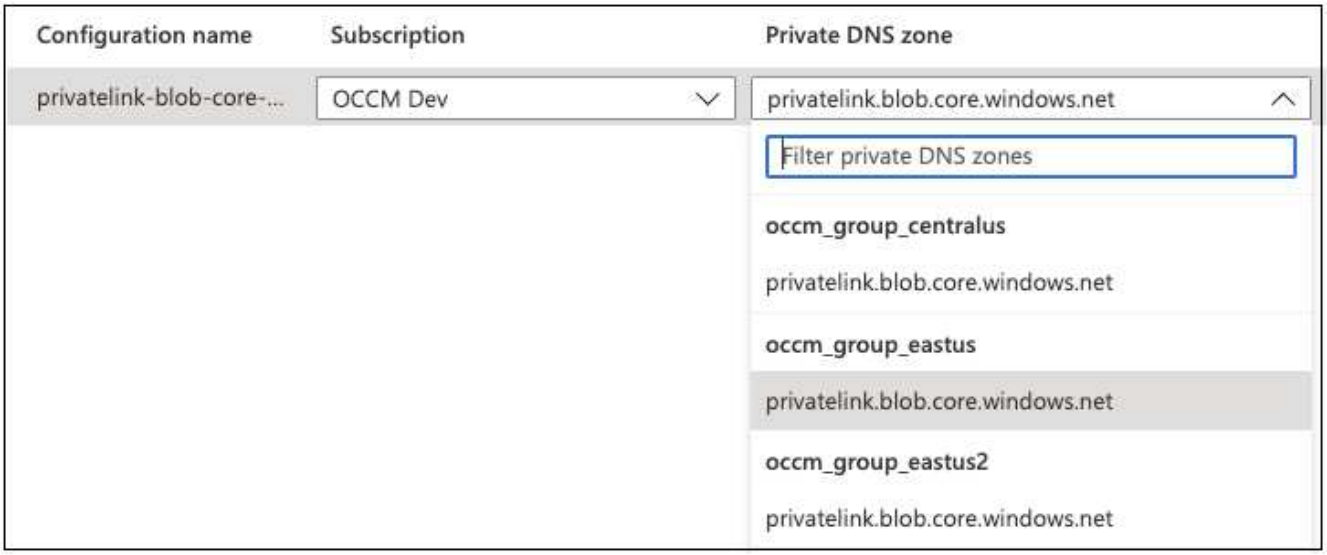
3. Nella pagina *Resource*, selezionare la sottorisorsa di destinazione come **blob**.



4. Nella pagina di configurazione:
   - Selezionare la rete virtuale e la subnet.
   - Fare clic sul pulsante di opzione **Sì** per "integrare con la zona DNS privata".



5. Nell'elenco Private DNS zone (zona DNS privata), assicurarsi che la zona privata sia selezionata dalla regione corretta e fare clic su **Review + Create** (Rivedi + Crea).



Ora l'account storage (nell'abbonamento 1) ha accesso al sistema Cloud Volumes ONTAP in esecuzione nell'abbonamento 2.

6. Riprovare ad abilitare il backup e il ripristino BlueXP sul sistema Cloud Volumes ONTAP e questa volta dovrebbe essere possibile.

Ripristinare i dati di backup e ripristino BlueXP in un sito buio

Quando utilizzi il backup e recovery di BlueXP in un sito senza accesso a Internet, noto come *modalità privata*, viene eseguito il backup dei dati di configurazione di backup e recovery di BlueXP nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host BlueXP Connector in futuro, è possibile implementare un nuovo connettore e ripristinare i dati critici di backup e ripristino di BlueXP.

Si noti che quando si utilizza il backup e ripristino BlueXP in un ambiente SaaS in cui BlueXP Connector viene implementato presso il provider cloud o sul proprio sistema host dotato di accesso a Internet, tutti i dati importanti di configurazione di backup e ripristino BlueXP vengono sottoposti a backup e protetti nel cloud. In caso di problemi con il connettore, è sufficiente creare un nuovo connettore e aggiungere gli ambienti di lavoro per ripristinare automaticamente i dettagli del backup.

Sono disponibili 2 tipi di dati di cui viene eseguito il backup:

- Database di backup e ripristino BlueXP - contiene un elenco di tutti i volumi, i file di backup, i criteri di backup e le informazioni di configurazione.
- File di catalogo indicizzati - contiene indici dettagliati utilizzati per la funzionalità di ricerca e ripristino che rendono le ricerche molto rapide ed efficienti quando si cercano i dati dei volumi che si desidera ripristinare.

Il backup di questi dati viene eseguito una volta al giorno a mezzanotte e viene conservato un massimo di 7 copie di ciascun file. Se il connettore gestisce più ambienti di lavoro ONTAP on-premise, i file di backup e ripristino BlueXP si trovano nel bucket dell'ambiente di lavoro attivato per primo.

Nessun dato di volume è mai incluso nel database di backup e ripristino BlueXP o nei file di catalogo indicizzati.

Ripristinare i dati di backup e ripristino di BlueXP su un nuovo connettore

Se il connettore on-premise presenta un guasto catastrofico, è necessario installare un nuovo connettore e ripristinare i dati di backup e ripristino di BlueXP nel nuovo connettore.

Per riportare il sistema di backup e ripristino BlueXP a uno stato operativo, è necessario eseguire 4 operazioni:

- Installare un nuovo connettore BlueXP
- Ripristinare il database di backup e ripristino BlueXP
- Ripristinare i file di catalogo indicizzati
- Riscopri tutti i tuoi sistemi ONTAP e StorageGRID on-premise nell'interfaccia utente di BlueXP

Una volta verificato il corretto funzionamento del sistema, si consiglia di creare nuovi file di backup.

Di cosa hai bisogno

È necessario accedere ai backup di database e indici più recenti dal bucket StorageGRID o ONTAP S3 in cui vengono memorizzati i file di backup:

- File di database MySQL per backup e ripristino BlueXP

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/`e viene chiamato `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 viene chiamato `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`.

Installare un nuovo connettore su un nuovo host Linux on-premise

Quando si installa un nuovo connettore BlueXP, assicurarsi di scaricare la stessa versione del software installata sul connettore originale. Le modifiche periodiche alla struttura del database di backup e ripristino di BlueXP possono rendere incompatibili le versioni software più recenti con i backup del database originali. È possibile "Aggiornare il software del connettore alla versione più recente dopo il ripristino del database di backup".

1. "Installare il connettore BlueXP su un nuovo host Linux on-premise"
2. Accedere a BlueXP utilizzando le credenziali utente amministratore appena create.

Ripristinare il database di backup e ripristino BlueXP

1. Copiare il backup MySQL dalla posizione di backup al nuovo host del connettore. Verrà utilizzato il nome del file di esempio "CBS_DB_Backup_23_05_2023.sql" riportato di seguito.
2. Copiare il backup nel contenitore MySQL docker utilizzando il seguente comando:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Inserire la shell del container MySQL usando il seguente comando:

```
docker exec -it ds_mysql_1 sh
```

4. Nella shell container, implementare "env".
5. Avrai bisogno della password MySQL DB, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il backup e ripristino di BlueXP MySQL DB utilizzando il seguente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verificare che MySQL DB di backup e ripristino BlueXP sia stato ripristinato correttamente utilizzando i seguenti comandi SQL:

```
mysql -u root -p cloud_backup
```

Inserire la password.

```
mysql> show tables;
mysql> select * from volume;
```

Verificare che i volumi visualizzati siano gli stessi dell'ambiente originale.

Ripristinare i file di catalogo indicizzati

1. Copiare il file zip di backup del catalogo indicizzato (verrà utilizzato il nome del 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 la cartella "catalogdb1" sia stata creata con le sottocartelle "Changes" e "Snapshot" sottostanti.

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti gli ambienti di lavoro ONTAP on-premise" che erano disponibili nel tuo ambiente precedente. Questo 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 agli ambienti di lavoro ONTAP così come sono stati configurati nella configurazione originale del connettore utilizzando "API BlueXP".

È necessario eseguire questa procedura per ogni sistema ONTAP 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 'User-Agent:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0'
-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":"pass
word"}
> '
```

   Questa API restituirà una risposta simile a quella riportata di seguito. 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'ID dell'agente X utilizzando l'API di tenancy/esterno/risorsa.

```
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 a quella riportata di seguito. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-Agent-id*.

3. Aggiornare il database di backup e ripristino BlueXP con i dettagli del sistema StorageGRID associato agli ambienti di lavoro. Assicurarsi di immettere il nome di dominio completo del StorageGRID, la chiave di accesso e la chiave di storage 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 di backup e ripristino di BlueXP

1. Selezionare ciascun ambiente di lavoro ONTAP e fare clic su **Visualizza backup** accanto al servizio di backup e ripristino nel pannello di destra.

   Dovrebbe essere possibile visualizzare tutti i backup creati per i volumi.

2. Dalla dashboard di ripristino, nella sezione Search & Restore (Ricerca e ripristino), fare clic su **Indexing Settings** (Impostazioni di indicizzazione).

   Assicurarsi che gli ambienti di lavoro che in precedenza avevano attivato la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Search & Restore (Ricerca e ripristino), eseguire alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato è stato completato correttamente.

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. Per riavviare il servizio, è necessario seguire diversi passaggi iniziali a seconda che il connettore sia stato implementato nel cloud o che il connettore sia stato installato manualmente su un sistema Linux.

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
Implementazione del cloud	`docker restart cloudmanager_cbs`
Installazione manuale con accesso a Internet	`docker restart cloudmanager_cbs`
Installazione manuale senza accesso a Internet	`docker restart ds_cloudmanager_cbs_1`

Conoscenza e supporto

Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione dell'abbonamento al supporto per l'ID account BlueXP (il numero di serie a 20 cifre 960xxxxxxxxx nella pagina Support Resources di BlueXP).

  Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

- Registrazione dei numeri di serie Cloud Volumes ONTAP associati a un abbonamento nel mercato del provider cloud (si tratta di numeri di serie 909201xxxxxxxx a 20 cifre).

  Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

Registrare l'account BlueXP per il supporto NetApp

Per registrarsi al supporto e attivare i diritti di supporto, un utente del proprio account BlueXP deve associare un account del sito di supporto NetApp al proprio account di accesso BlueXP. La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

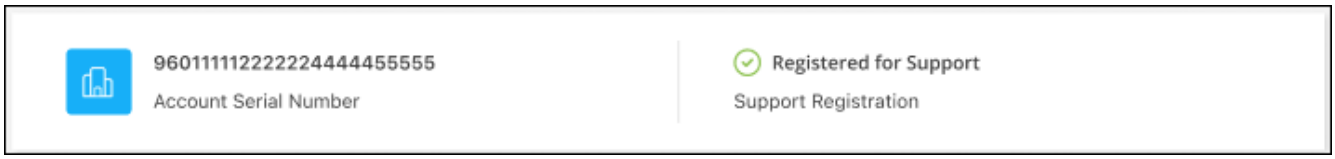
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

   La pagina **risorse** dovrebbe mostrare che il tuo account è registrato per il supporto.

   Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che il tuo account BlueXP non sia registrato per il supporto. Se un utente dell'account ha seguito questa procedura, l'account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

Fasi

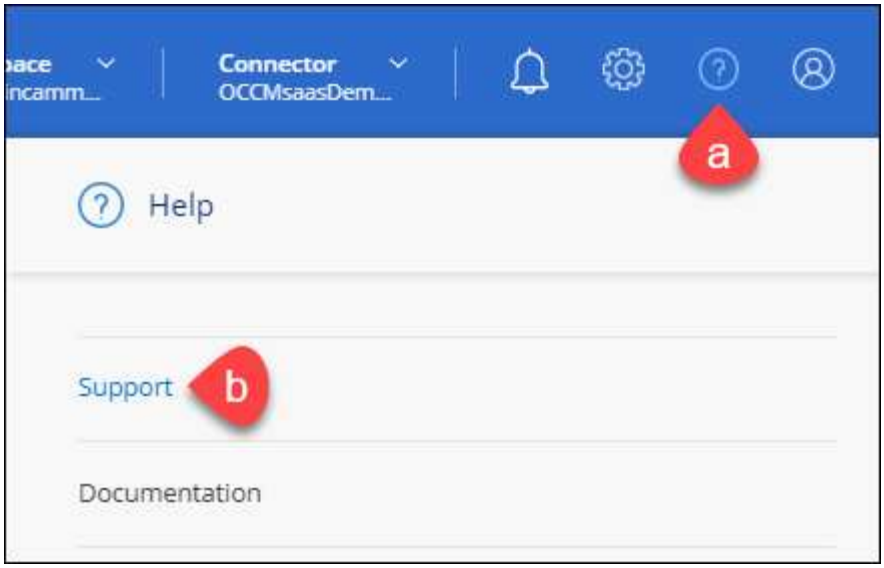
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto Cliente esistente con un account NSS.

Novità di NetApp

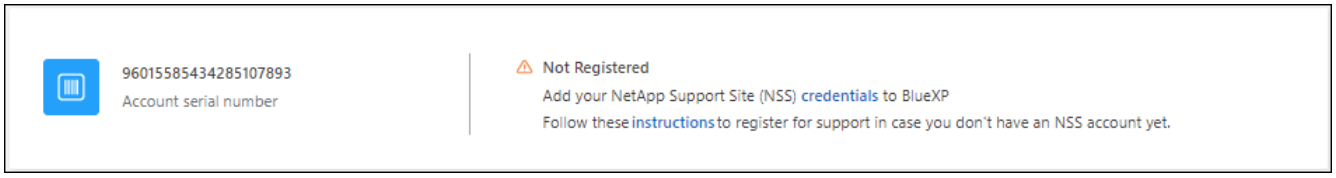
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare "Sito per la registrazione del supporto NetApp" E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

   Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

7. Confermare l'azione dall'interno dell'e-mail.

   La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

8. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.

Al termine

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di assunzione per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in Cliente esistente con un account NSS.

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

Per attivare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP, è necessario associare le credenziali del sito di supporto NetApp all'account BlueXP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

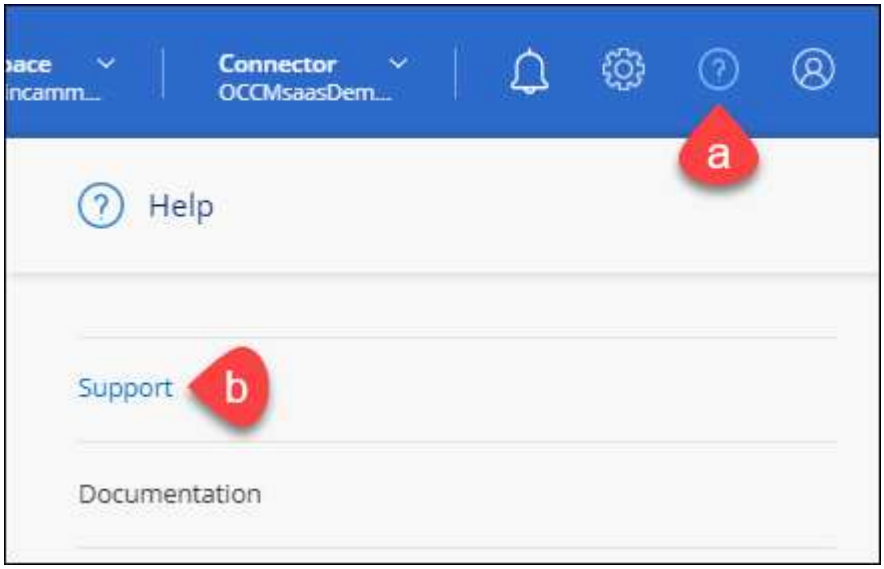
L'associazione delle credenziali NSS all'account BlueXP è diversa dall'account NSS associato a un account utente BlueXP.

Queste credenziali NSS sono associate all'ID account BlueXP specifico. Gli utenti che appartengono all'account BlueXP possono accedere a queste credenziali da **Support > NSS Management**.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include il supporto tecnico remoto via web ticketing.

Ottieni supporto per un file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

  Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- "Community"

  Unisciti alla community BlueXP per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo l'attivazione del supporto.

Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. "Scopri come gestire le credenziali associate all'accesso a BlueXP".
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:

   a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.

   b. Selezionare **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp:

      - **Servizio**: Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
      - **Ambiente di lavoro**: Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

        L'elenco degli ambienti di lavoro rientra nell'ambito dell'account, dell'area di lavoro e del connettore BlueXP selezionato nel banner superiore del servizio.

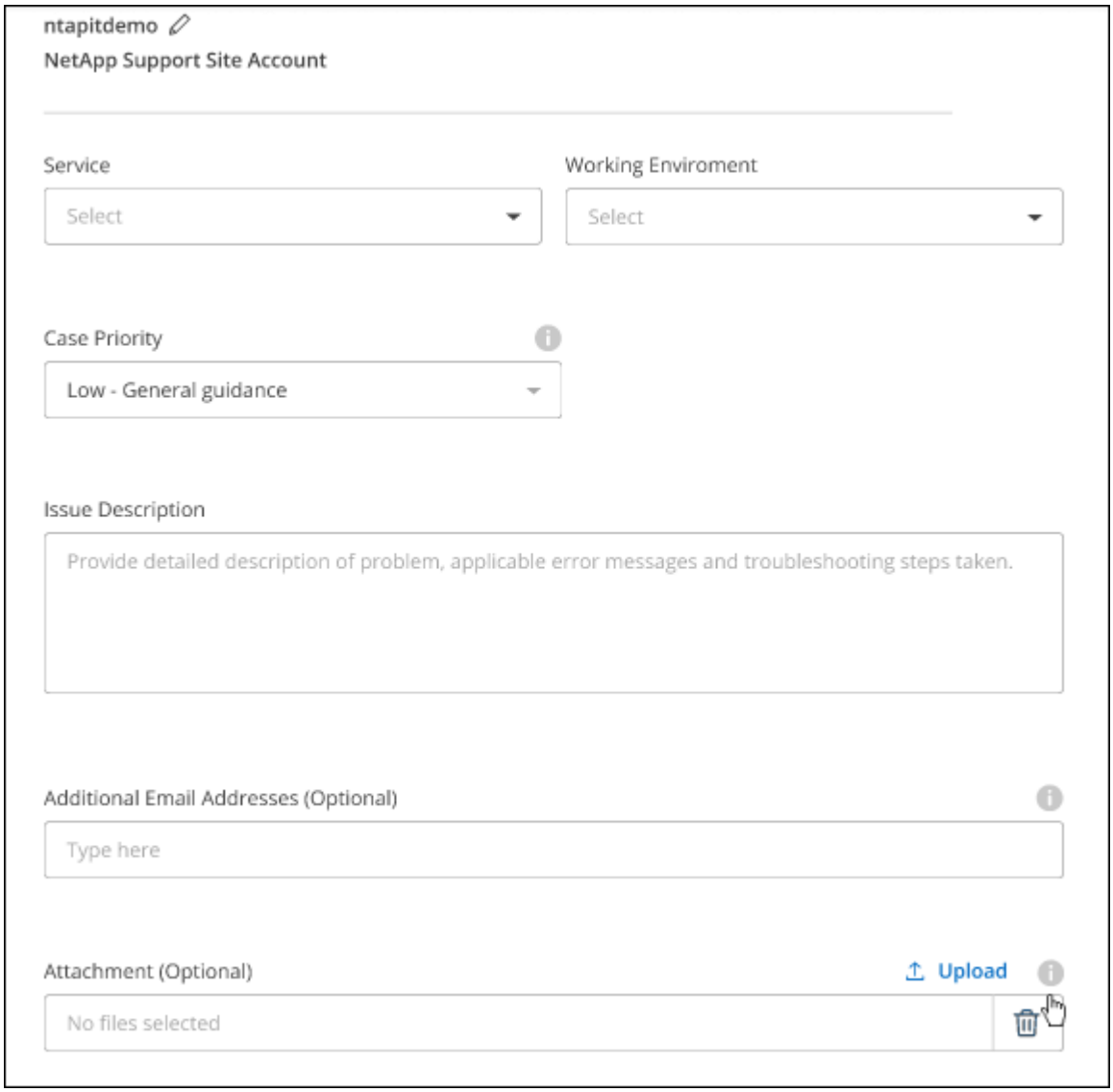
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.

      - **Descrizione del problema**: Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
      - **Indirizzi e-mail aggiuntivi**: Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale)**: Carica fino a cinque allegati, uno alla volta.

  Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo https://mysupport.netapp.com/site/help

Gestire i casi di supporto (anteprima)

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

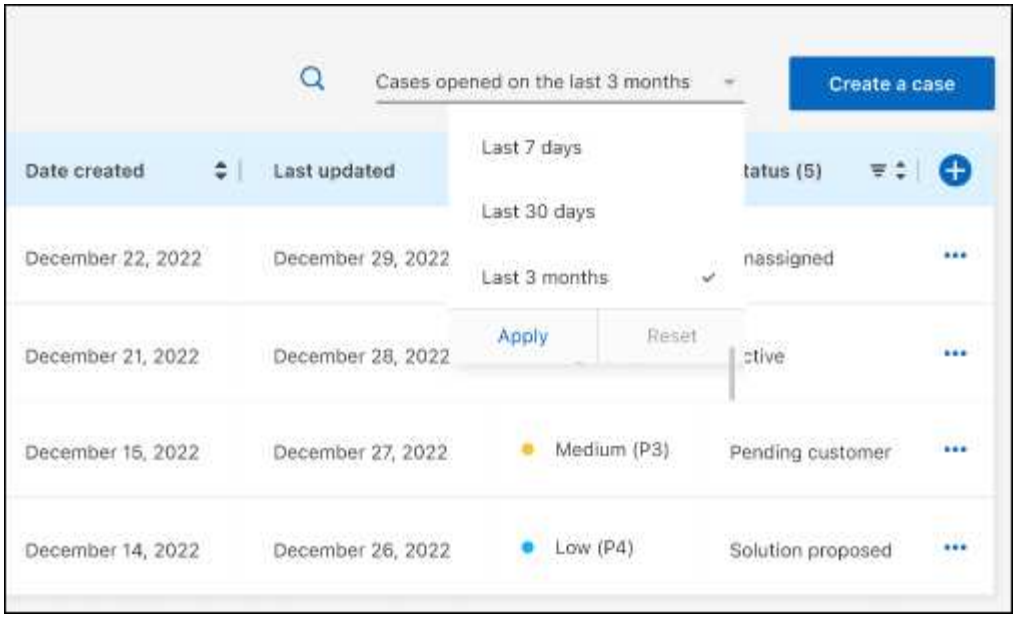
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  Per ulteriori informazioni, consulta la procedura riportata di seguito.
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

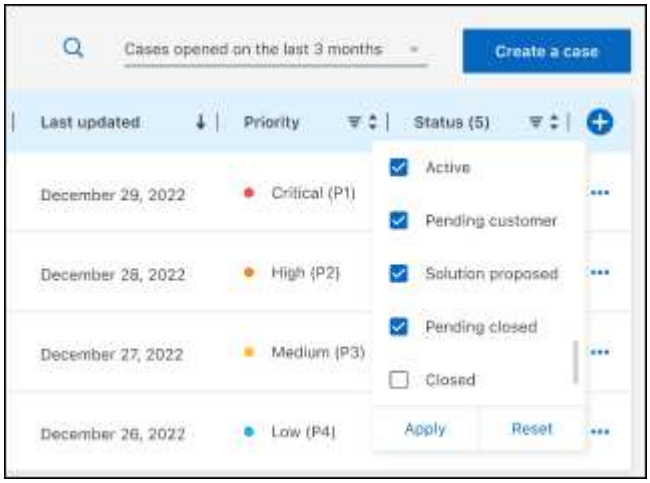
Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.

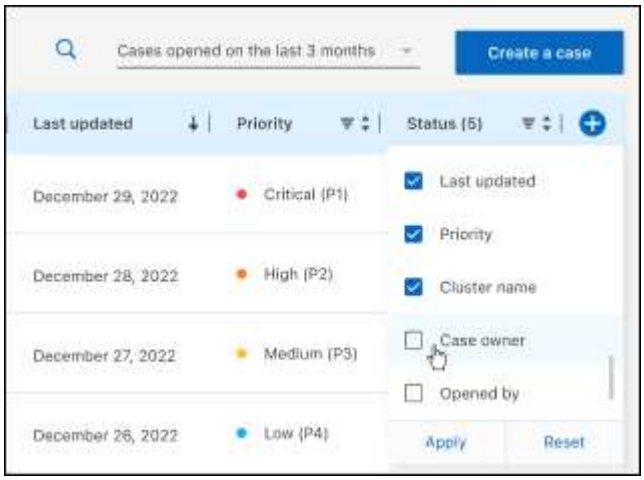
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
   - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.

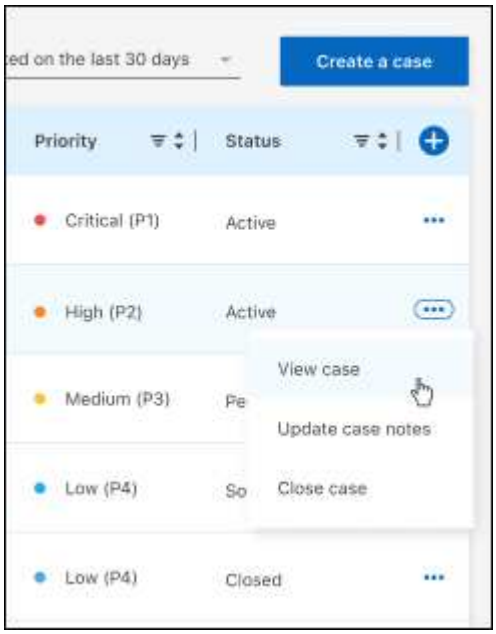


- Modificare le colonne visualizzate nella tabella selezionando e quindi scegliere le colonne che si desidera visualizzare.



4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:
    - **Visualizza caso**: Visualizza tutti i dettagli relativi a un caso specifico.
    - **Aggiorna note sul caso**: Fornisci ulteriori dettagli sul problema oppure seleziona **carica file** per allegare fino a un massimo di cinque file.

      Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
    - **Chiudi caso**: Fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.



Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per BlueXP"
- "Avviso per il backup e ripristino di BlueXP"
- "Avviso per il ripristino di un singolo file"