Backup e ripristino dei dati ONTAP

BlueXP backup and recovery

NetApp
April 18, 2024

Sommario

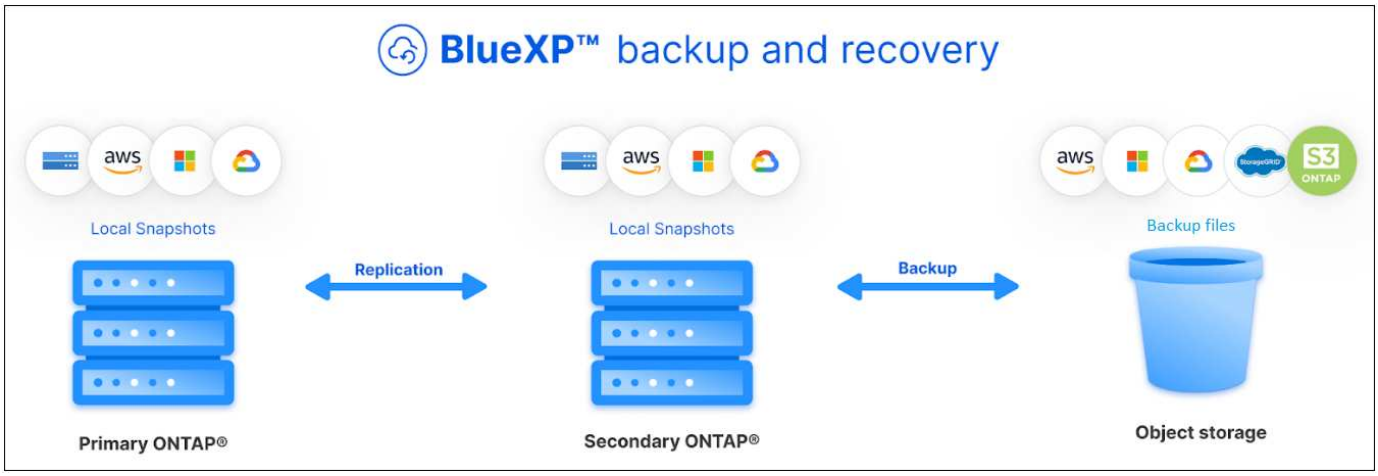
Backup e ripristino dei dati ONTAP

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.

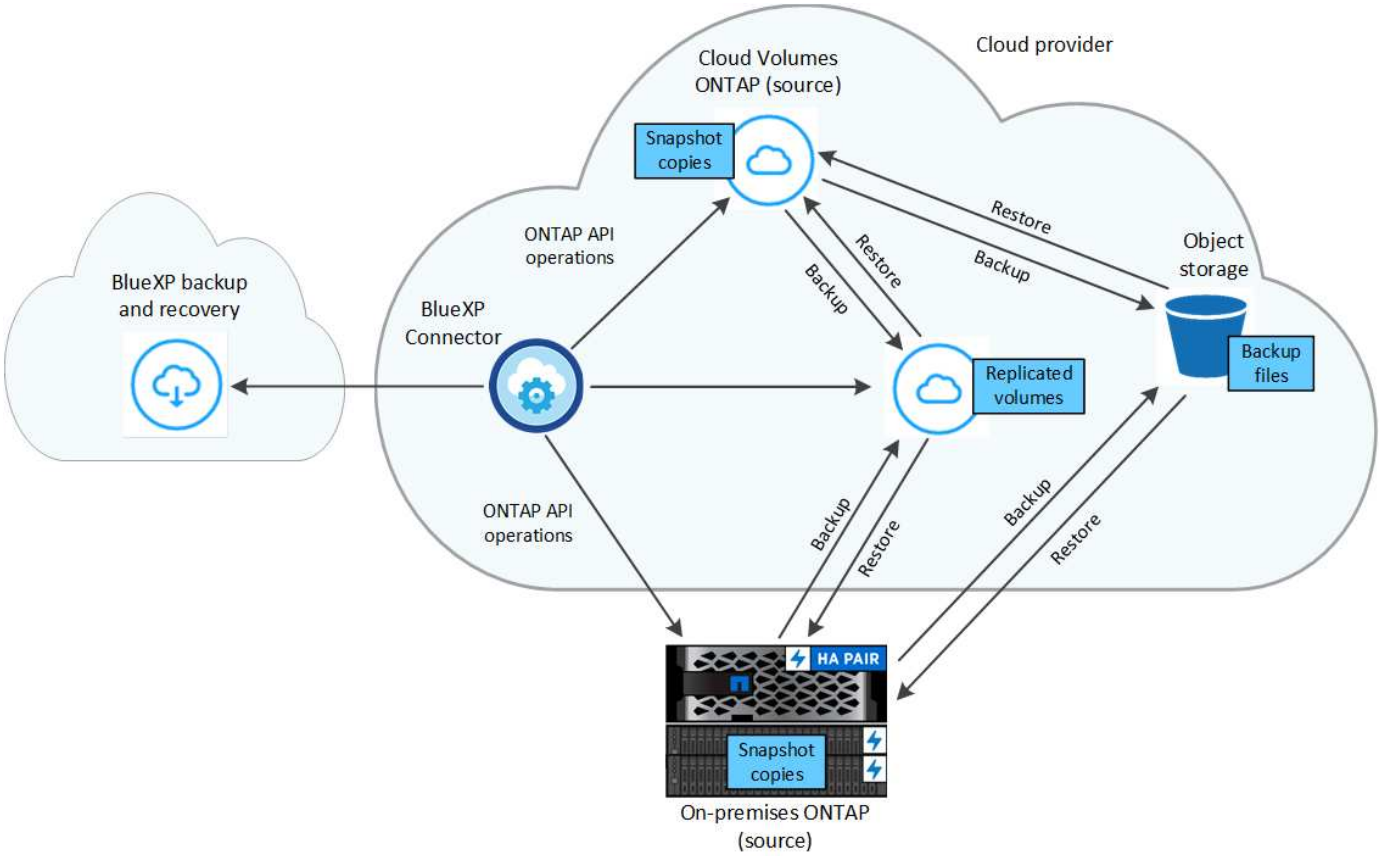
"Scopri come impostare i contratti annuali".

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)

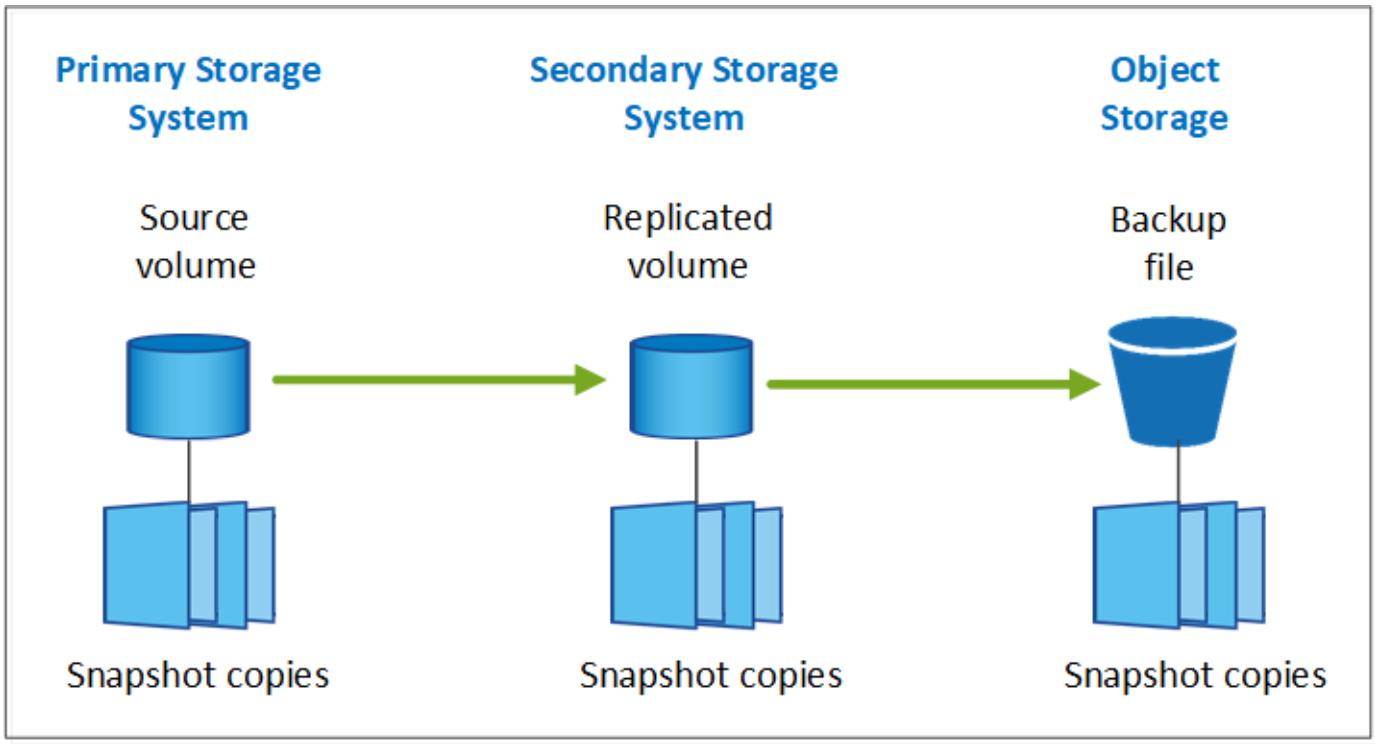
Quali funzioni di protezione utilizzerai

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.

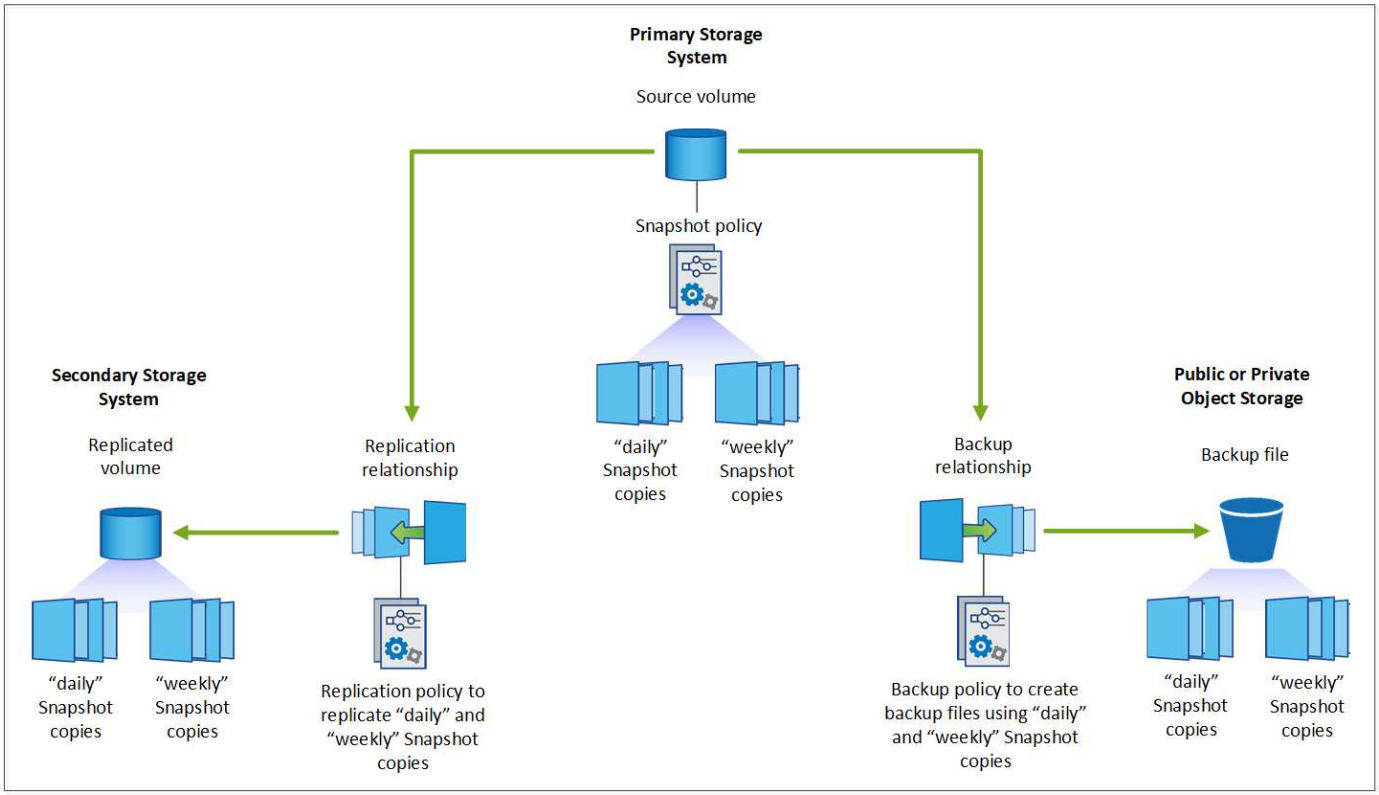
Oltre a questi criteri, lo storage cloud offre opzioni di sicurezza aggiuntive se si utilizza la funzionalità DataLock e ransomware Protection, oltre a risparmi aggiuntivi selezionando classi di storage di archiviazione per i file di backup meno recenti. "Scopri di più su DataLock e la protezione ransomware"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

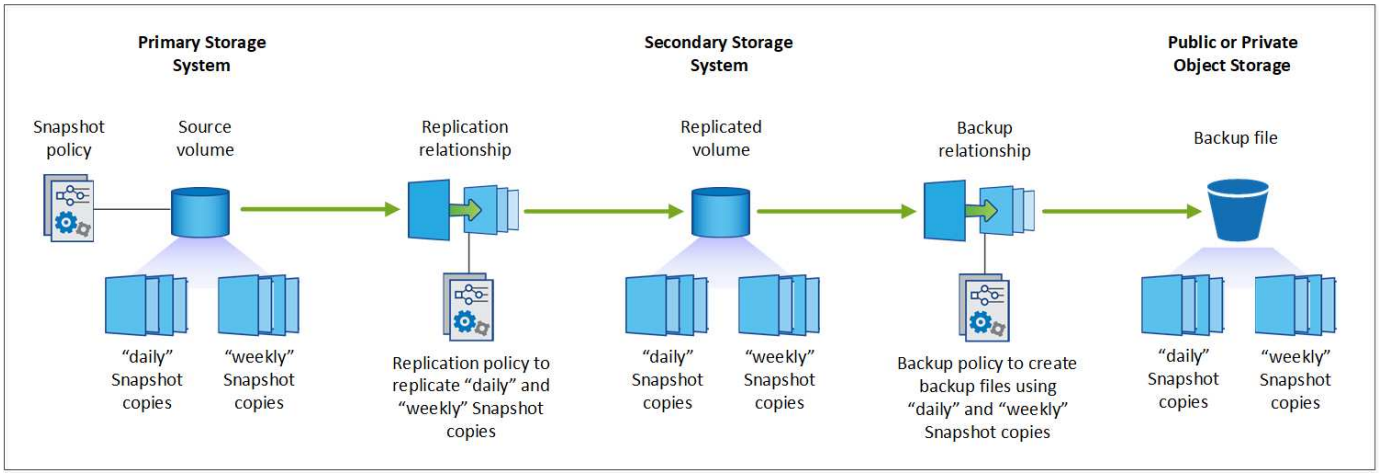
Quale architettura di backup utilizzerai

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:

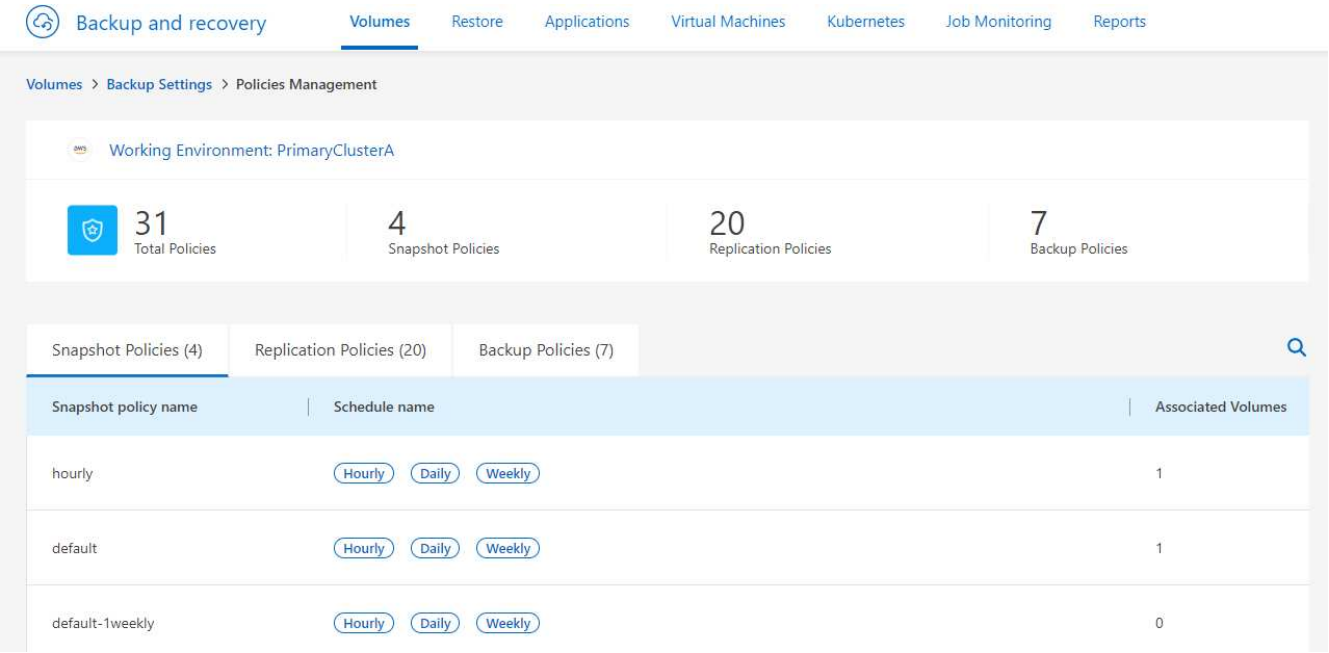
- Interfaccia utente di BlueXP
- Interfaccia utente di System Manager
- CLI ONTAP

> 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

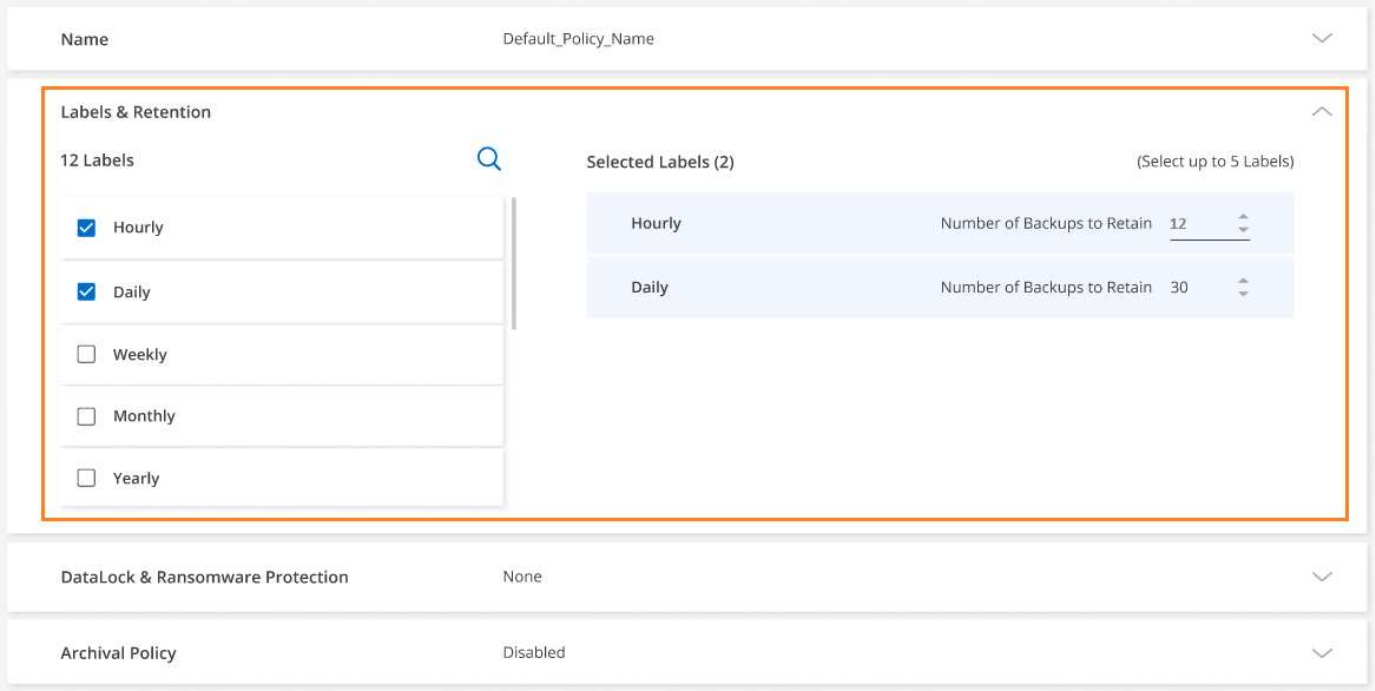
Il backup e recovery di BlueXP ti permette di creare policy di backup con una vasta gamma di impostazioni per i sistemi ONTAP e Cloud Volumes ONTAP on-premise.

> 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 3 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

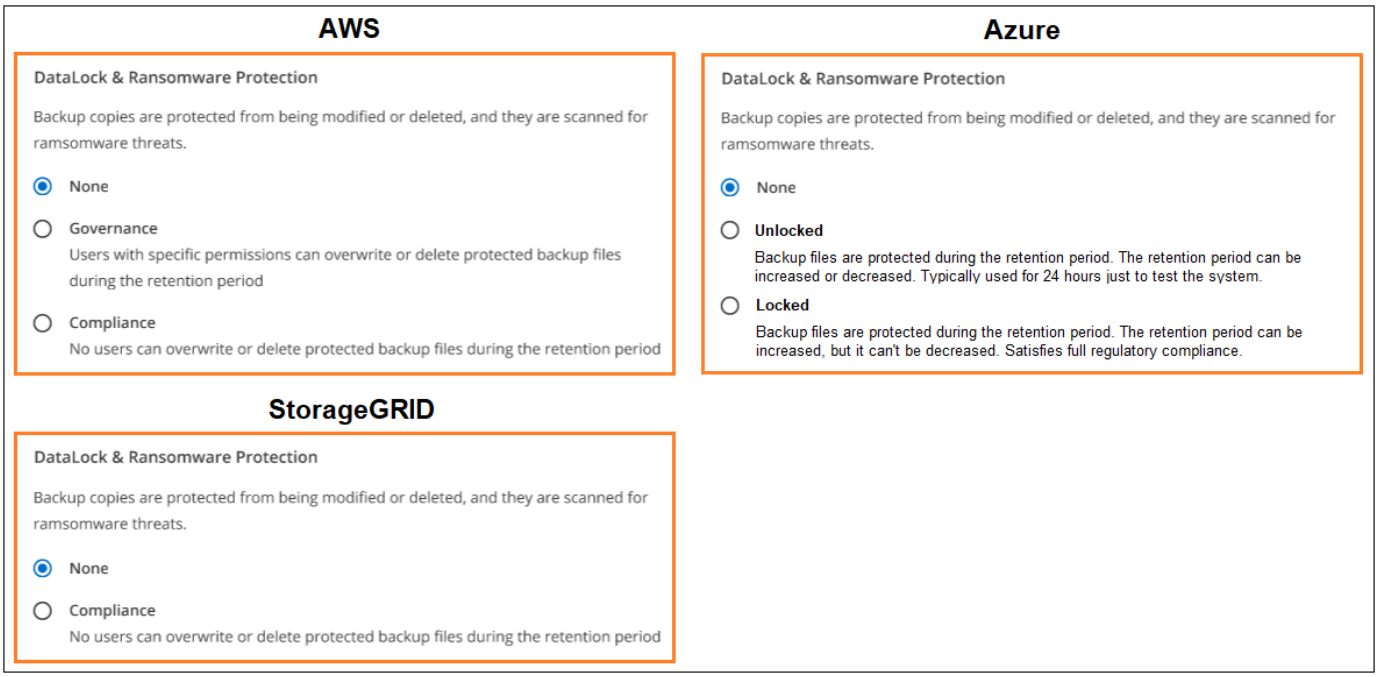
  È possibile scegliere di eseguire una scansione prima di ripristinare i dati da un file di backup oppure saltare questa scansione.

- 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.

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.

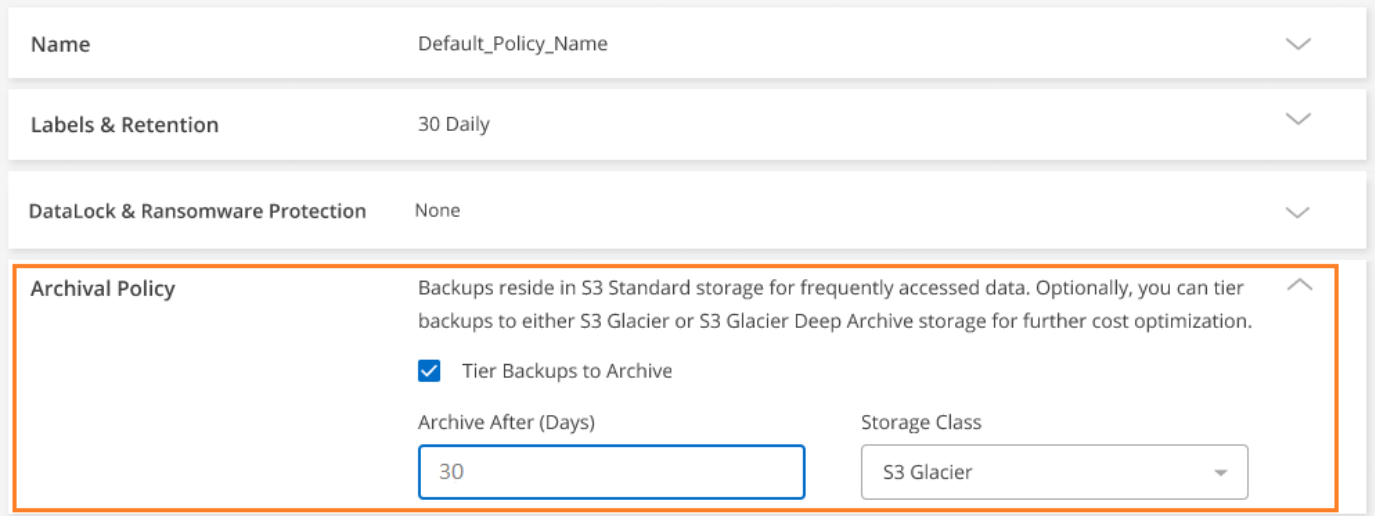
Opzioni di archiviazione

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

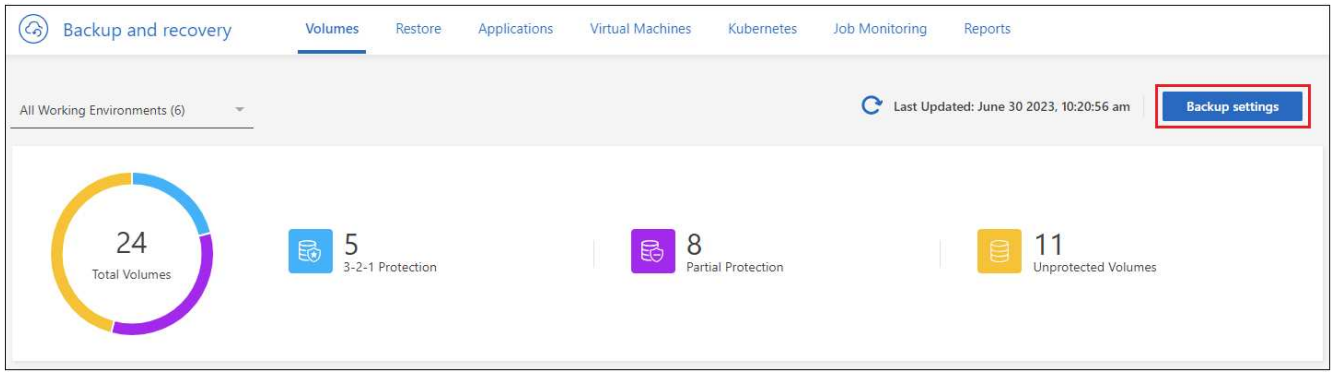
- Modifica dell'eventuale esportazione delle copie Snapshot storiche come file di backup e inclusione nei file di backup di base iniziali per volumi futuri
- Modifica della rimozione delle snapshot "annuali" dal sistema di origine
- Abilitazione o disabilitazione delle scansioni ransomware per un ambiente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

Visualizzare le impostazioni di backup a livello di cluster

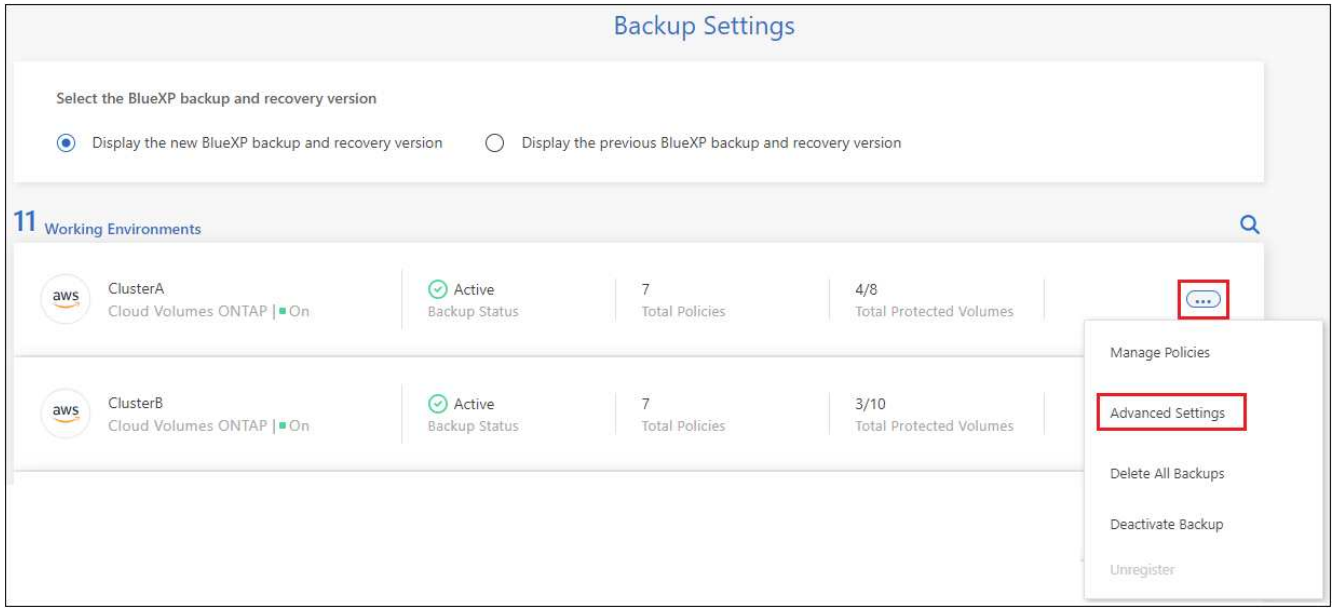
È possibile visualizzare le impostazioni di backup a livello di cluster per ciascun ambiente di lavoro.

Fasi

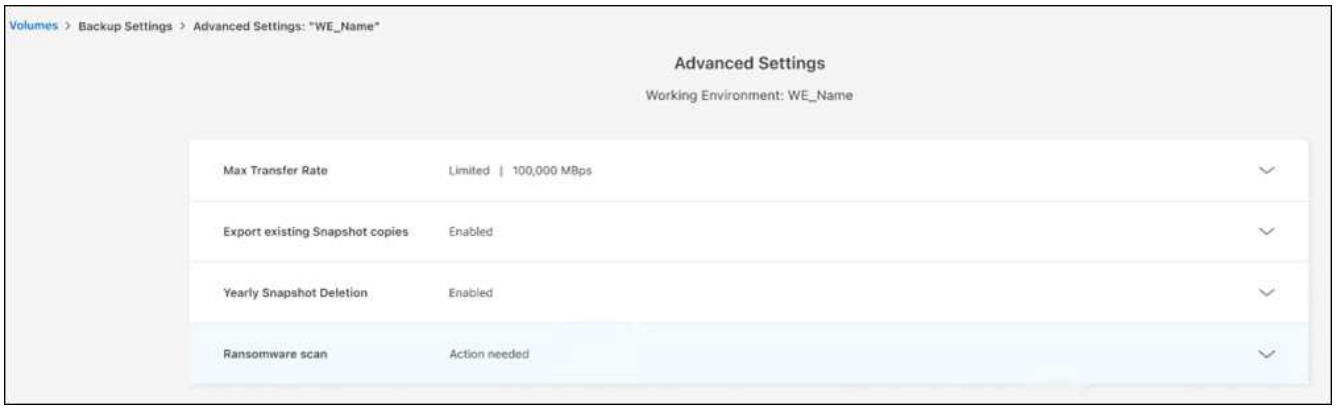
1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



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.

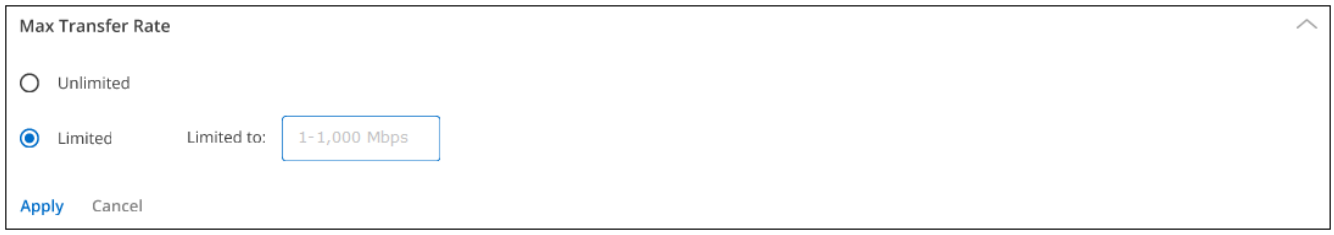
Tenere presente che alcune opzioni non sono disponibili in base alla versione di ONTAP nel cluster di origine e alla destinazione del provider cloud in cui risiedono i backup.

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.

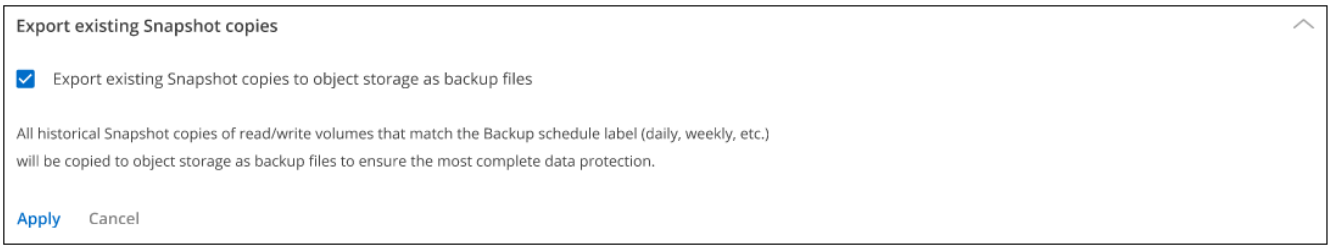
Consente di modificare se le copie Snapshot storiche vengono esportate come file di backup

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**.



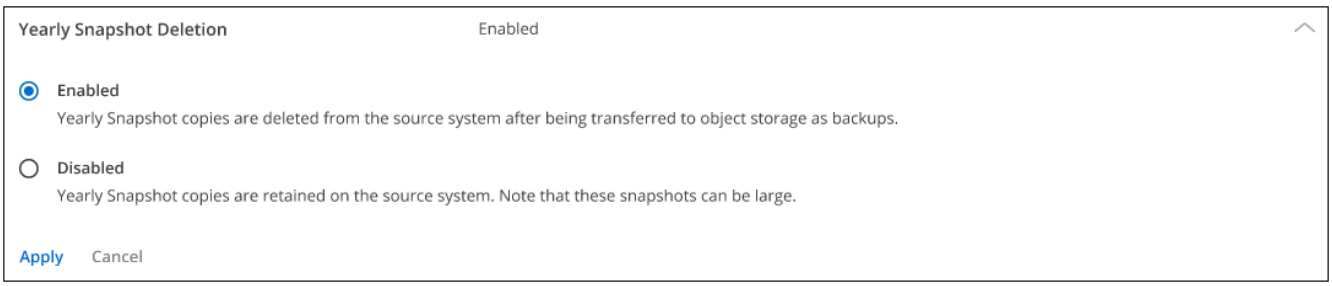
4. Selezionare se si desidera esportare le copie Snapshot esistenti.
5. Selezionare **Applica**.

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.

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

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**.

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".

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

Verificare i requisiti di licenza

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

Verificare i requisiti di licenza.

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.

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.

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.

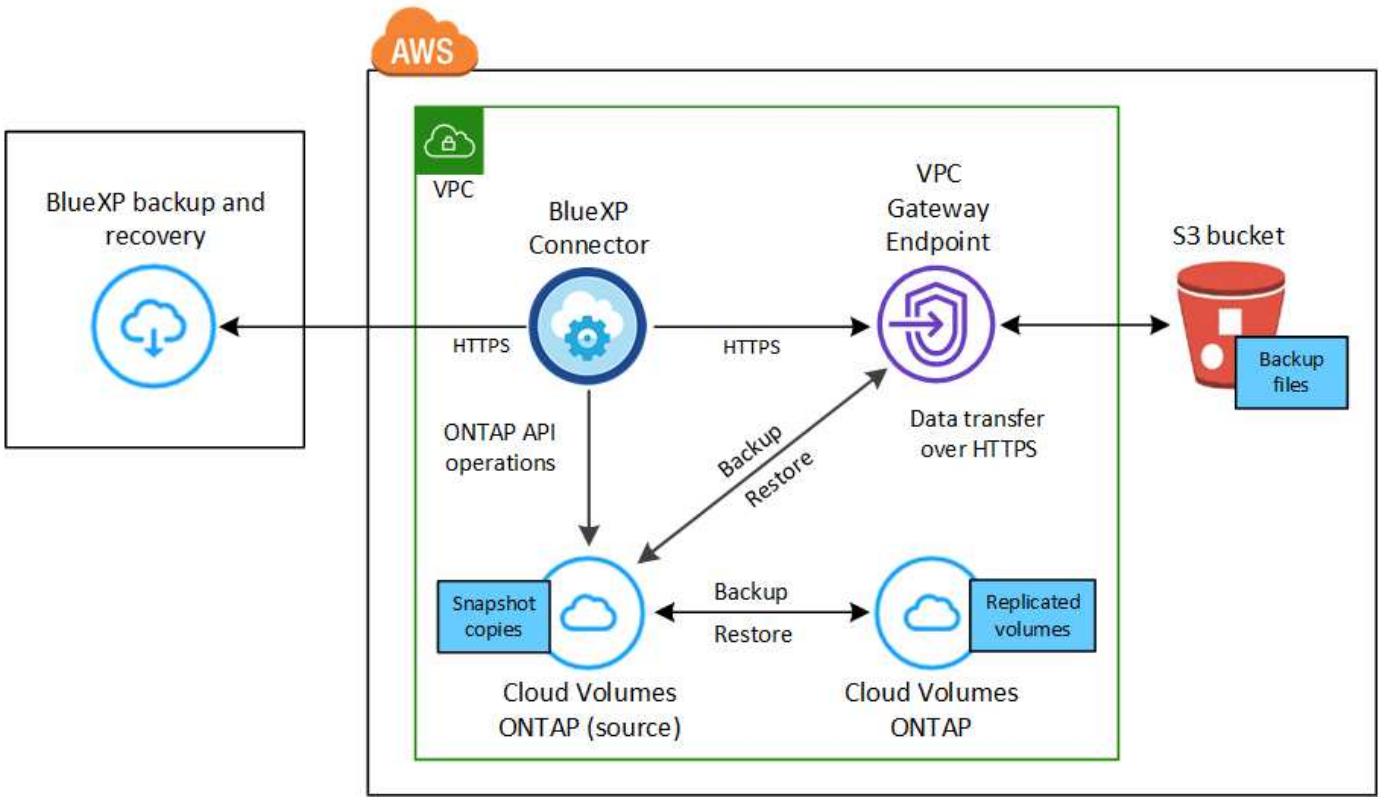
Attivare i backup sui volumi ONTAP.

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".

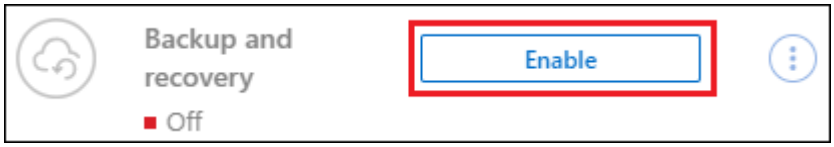
Attivare il backup e il ripristino BlueXP su un sistema esistente

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

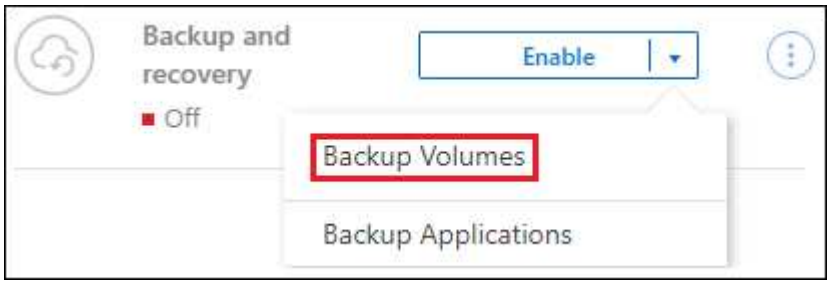
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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.

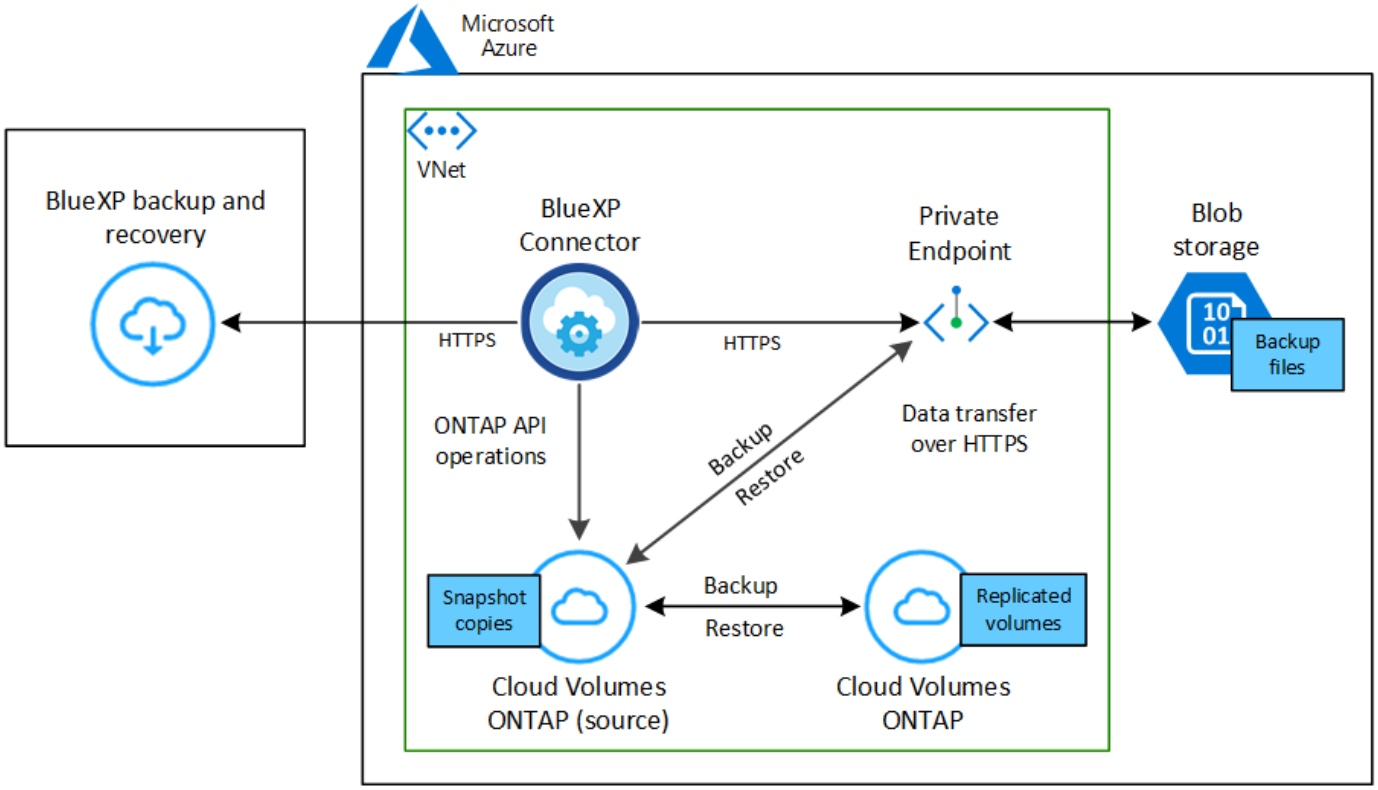
Attivare i backup sui volumi ONTAP.

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".

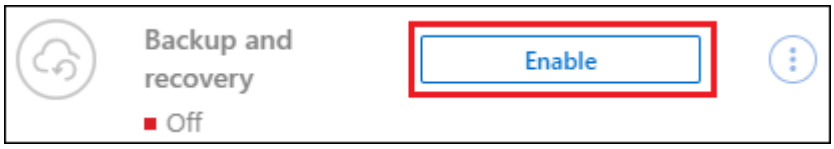
Attivare il backup e il ripristino BlueXP su un sistema esistente

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

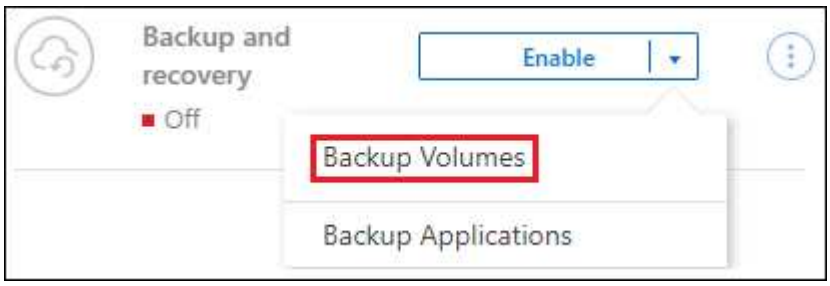
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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.

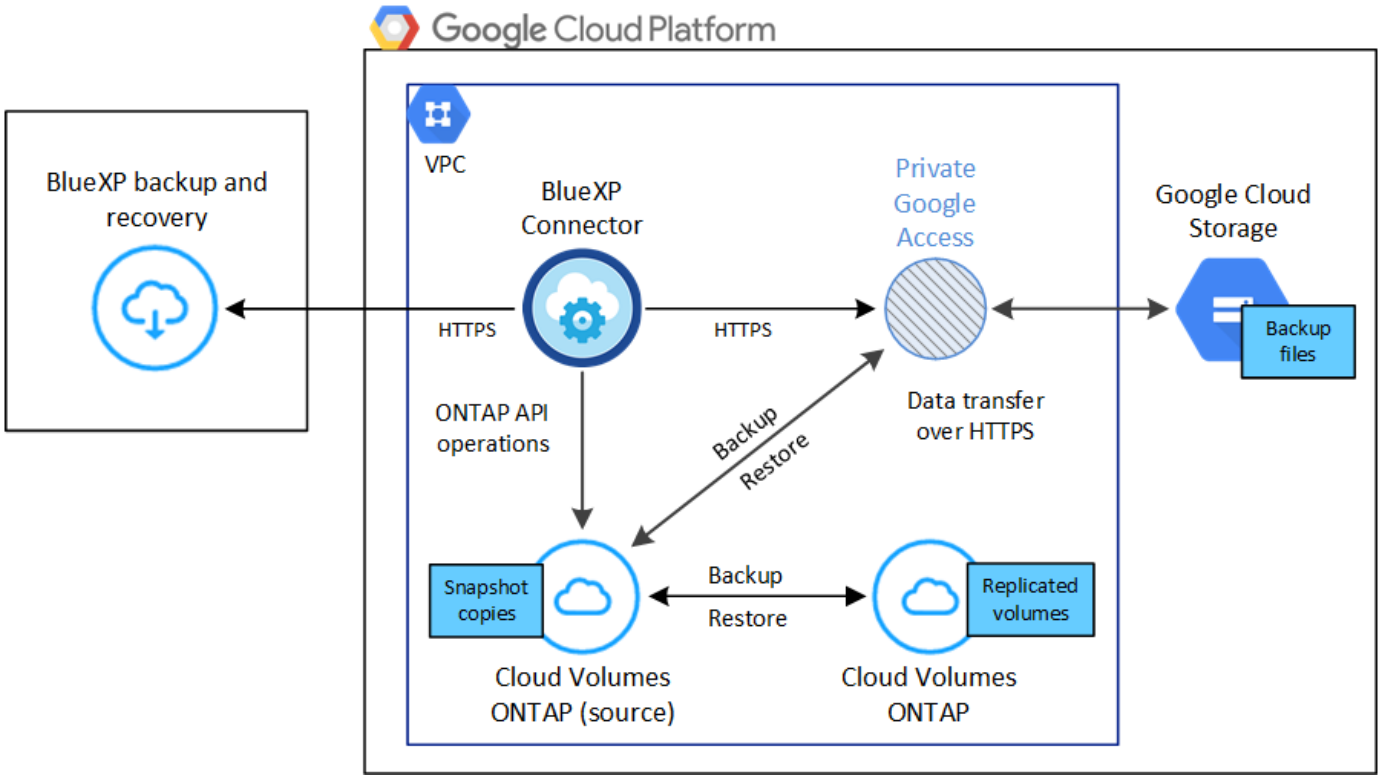
Attivare i backup sui volumi ONTAP.

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:

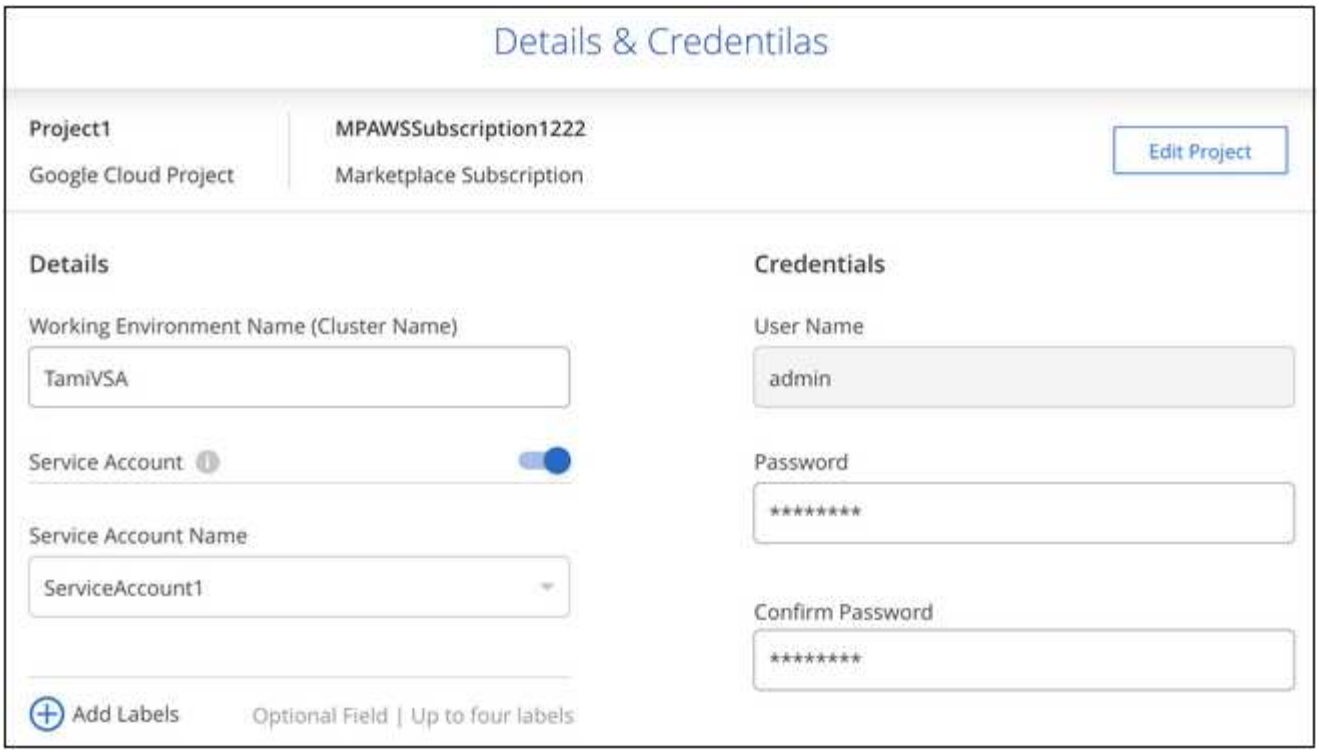
   a. Fare clic su **Edit Project** (Modifica progetto) e selezionare un nuovo progetto se quello che si desidera utilizzare è diverso dal progetto predefinito (dove si trova il connettore).

   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

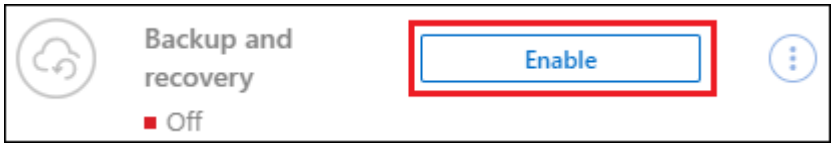
È possibile abilitare il backup e il ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro.

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

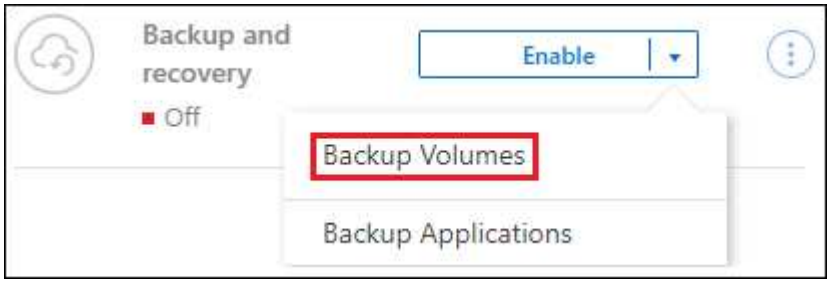
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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

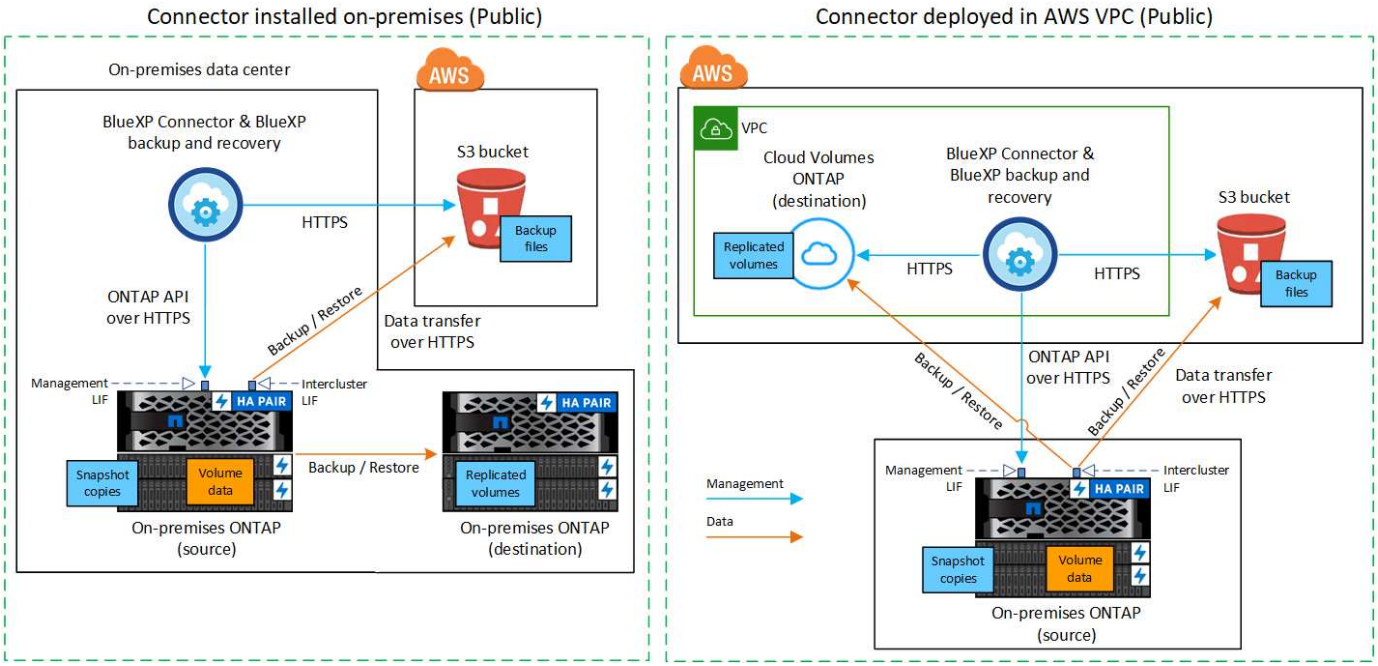
Scegliere quale dei due metodi di connessione utilizzare per la configurazione dei backup da sistemi ONTAP on-premise ad AWS S3.

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

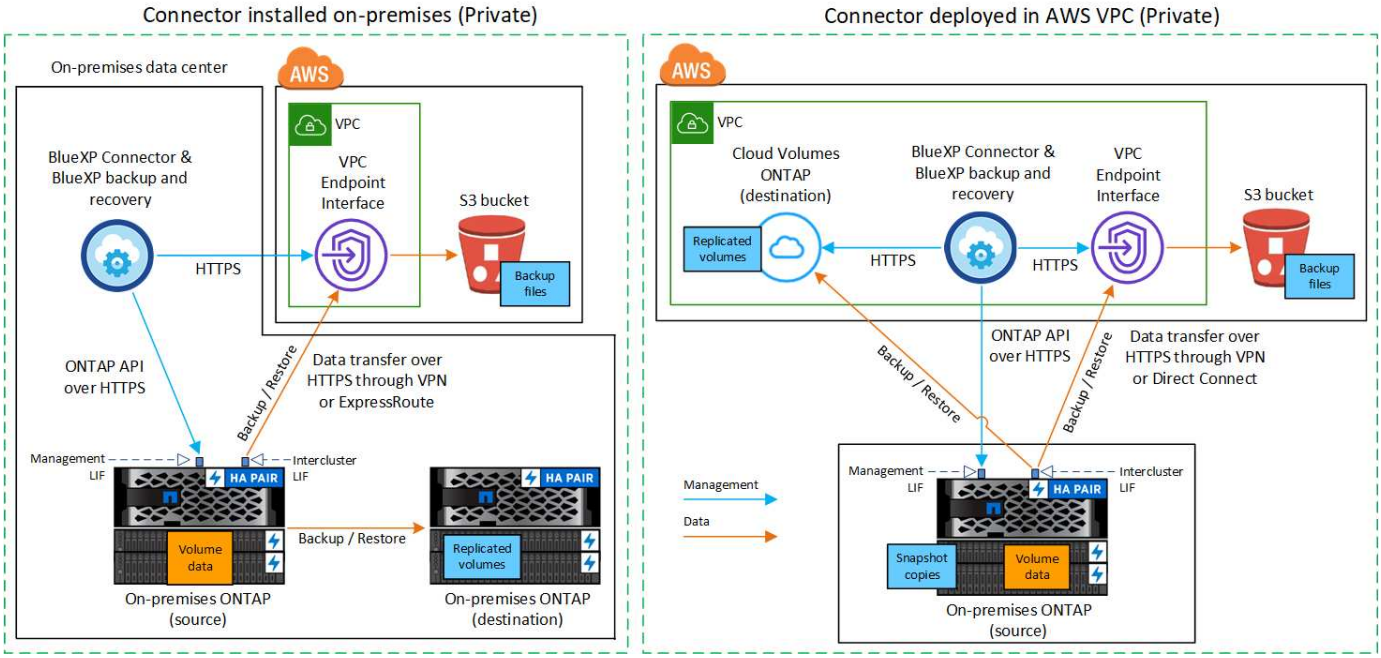
- **Connessione privata** - utilizza una connessione VPN o AWS Direct e instrada il traffico attraverso un'interfaccia endpoint VPC che utilizza un indirizzo IP privato.

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

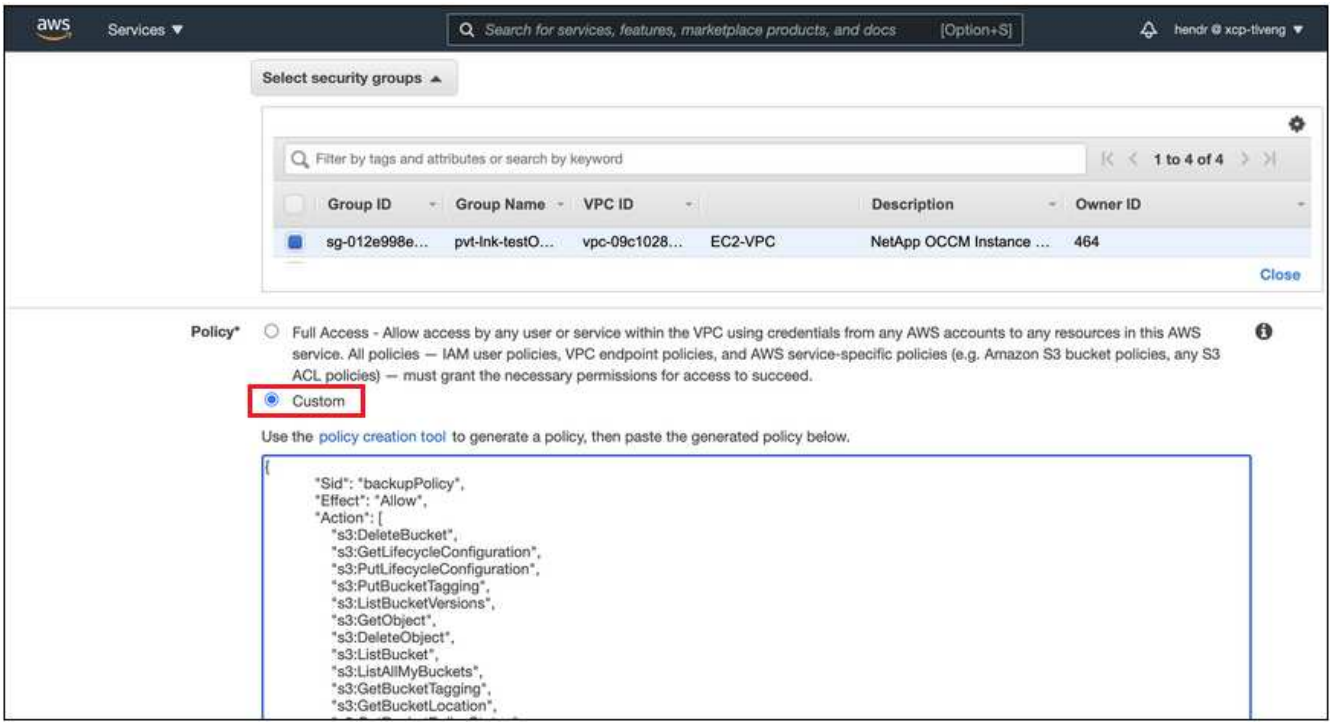
Se si desidera utilizzare una connessione Internet pubblica standard, tutte le autorizzazioni vengono impostate dal connettore e non è necessario eseguire altre operazioni. Questo tipo di connessione viene mostrato nella "primo diagramma".

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

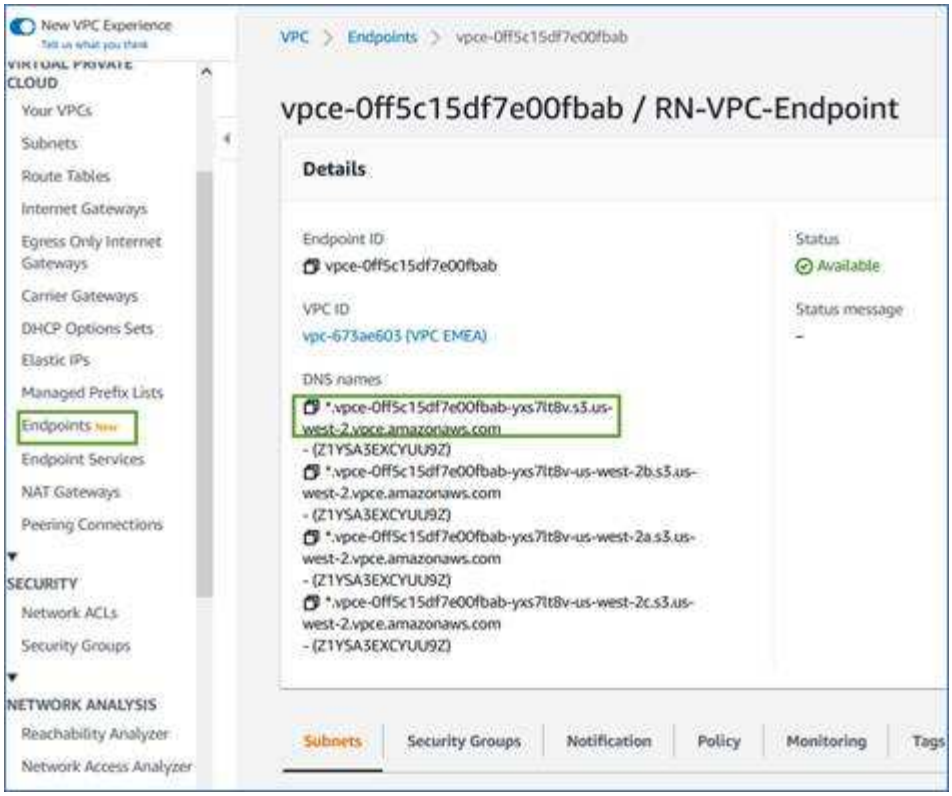
1. Creare una configurazione dell'endpoint dell'interfaccia utilizzando la console Amazon VPC o la riga di comando. "Consulta i dettagli sull'utilizzo di AWS PrivateLink per Amazon S3".
2. Modificare la configurazione del gruppo di protezione associata a BlueXP Connector. È necessario modificare la policy 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.

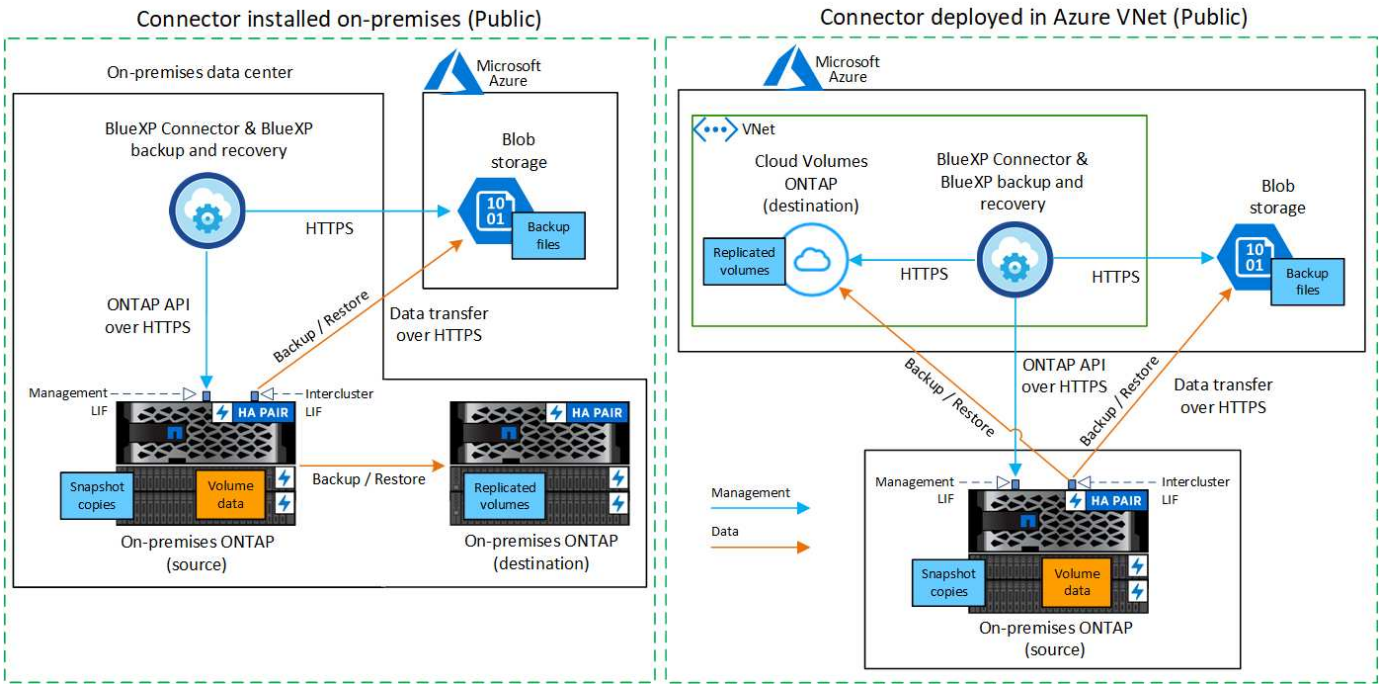
Identificare il metodo di connessione

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

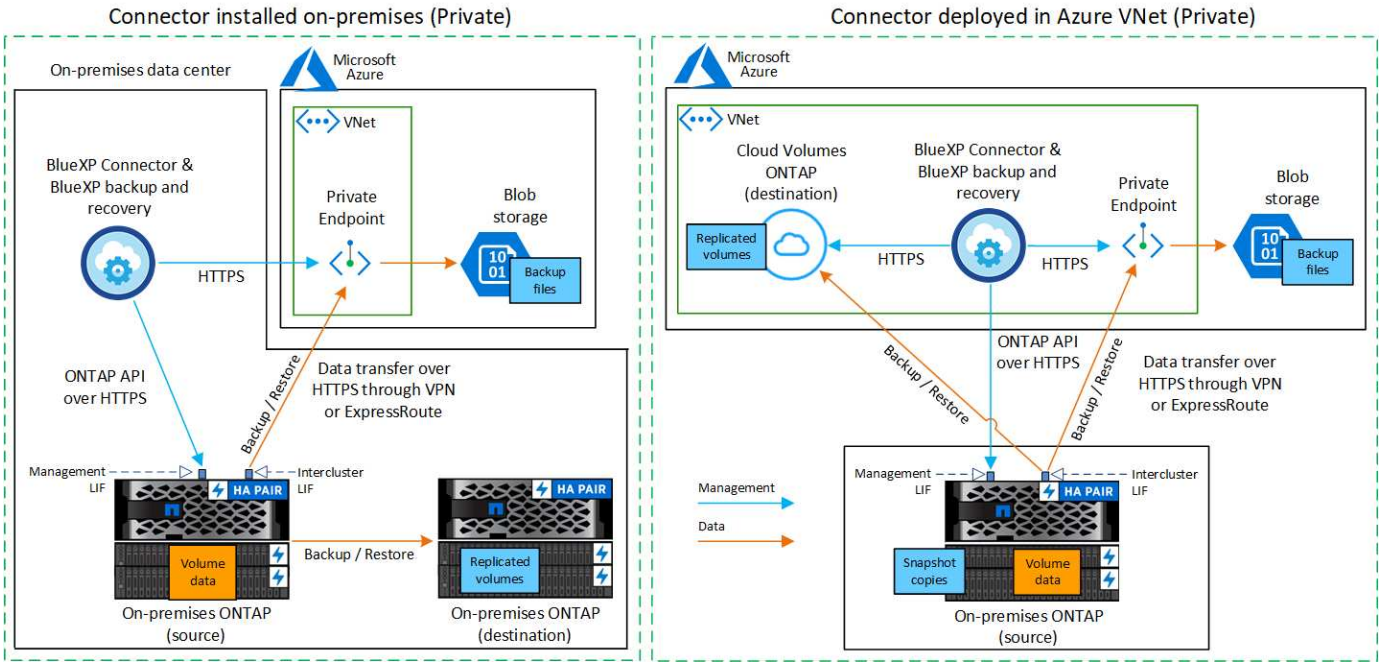
- **Connessione pubblica** - connette direttamente il sistema ONTAP allo storage Azure Blob utilizzando un endpoint Azure pubblico.
- **Connessione privata** - utilizza una VPN o ExpressRoute e instrada il traffico attraverso un VNET Private Endpoint che utilizza un indirizzo IP privato.

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:

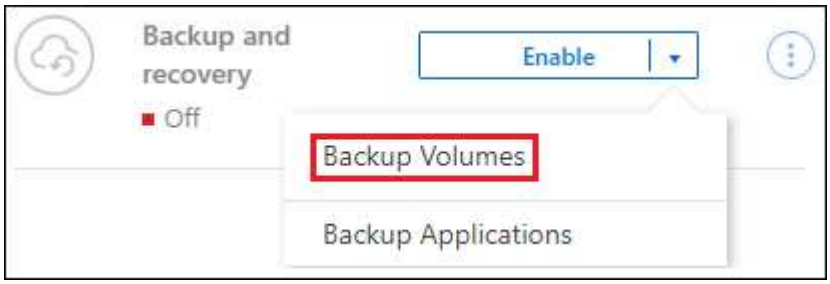
- Selezionare i volumi di cui si desidera eseguire il backup
- Definire la strategia di backup
- Rivedere le selezioni

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.

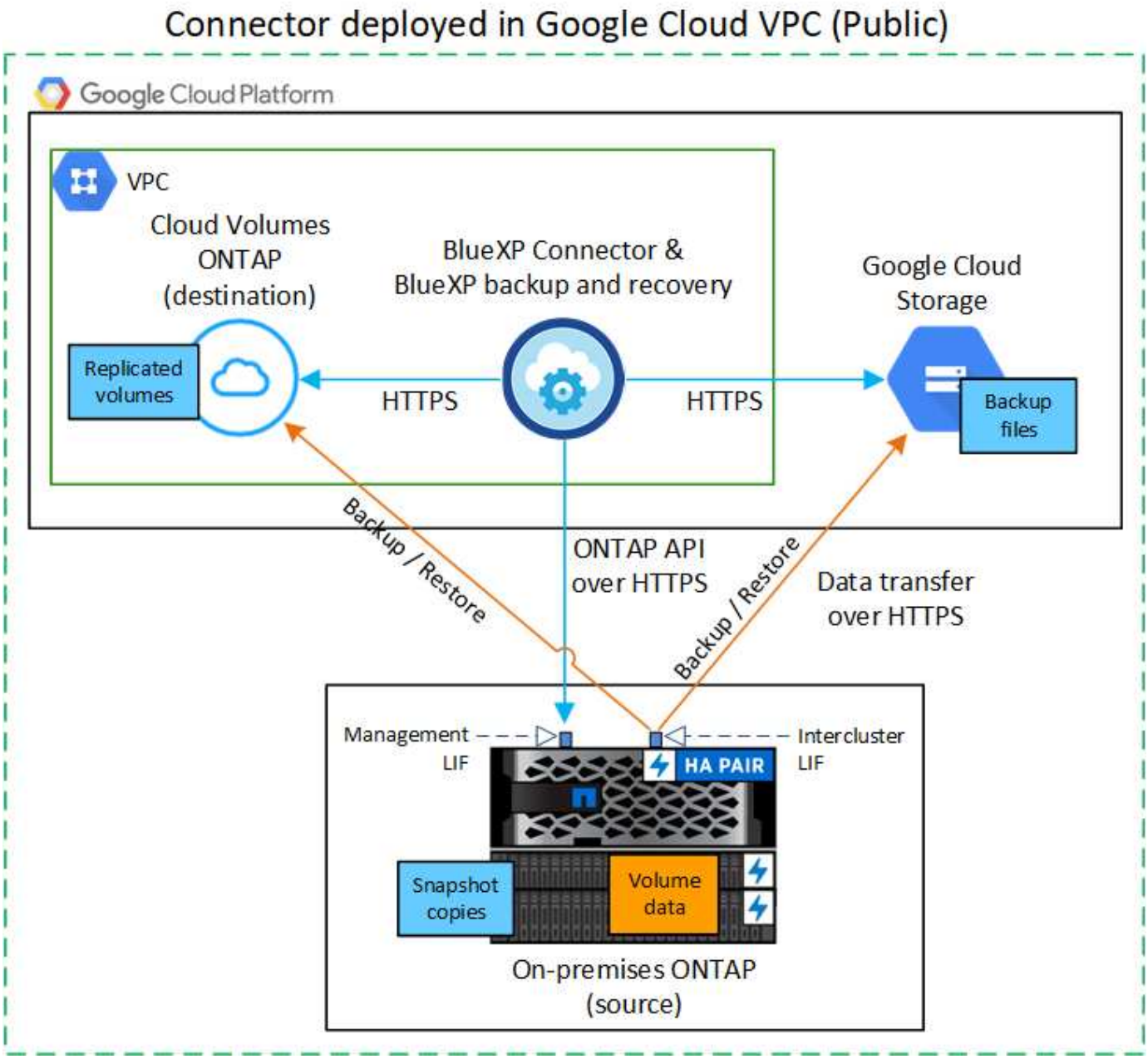
Identificare il metodo di connessione

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

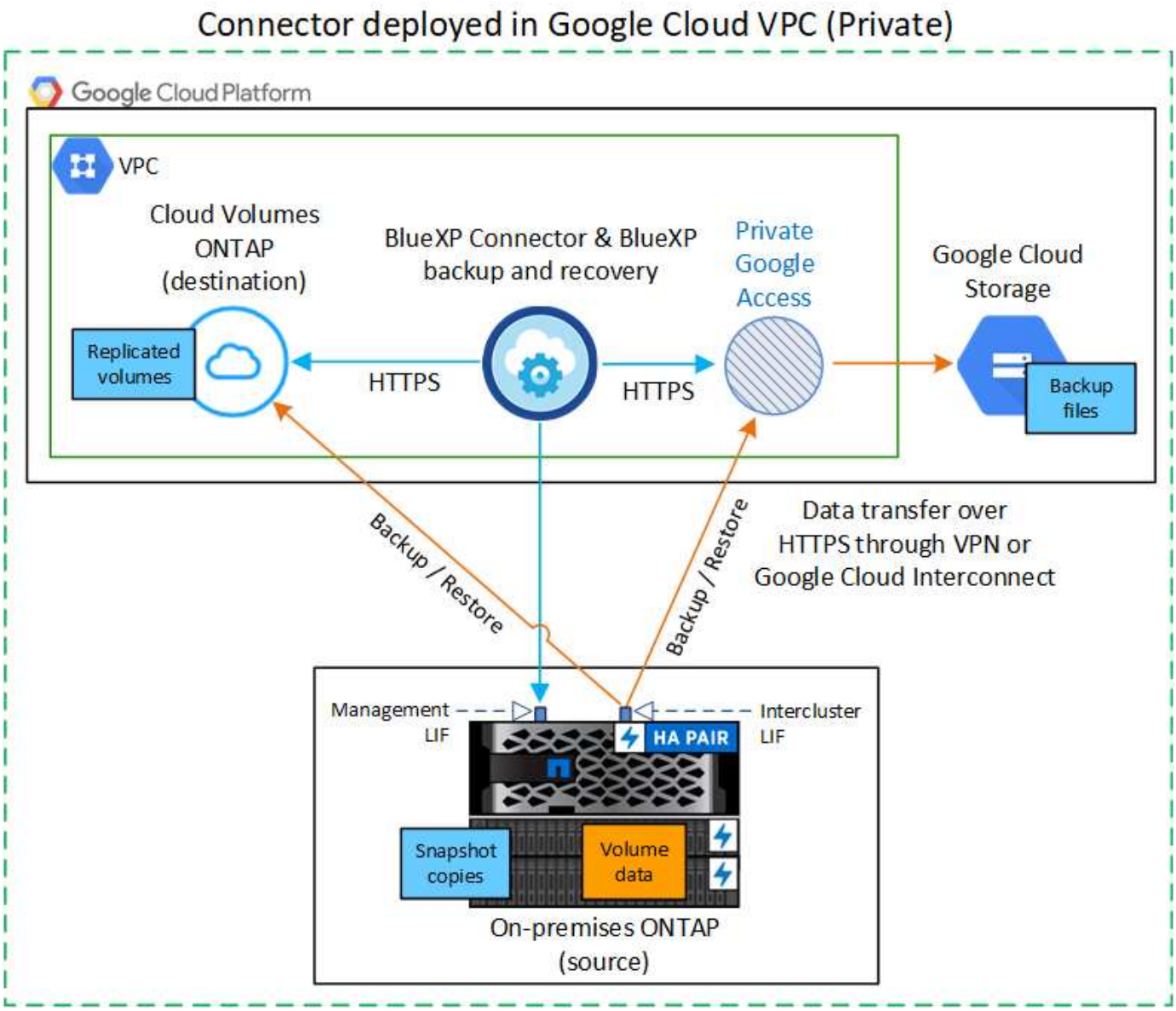
- **Connessione pubblica** - consente di connettere direttamente il sistema ONTAP allo storage cloud di Google utilizzando un endpoint pubblico di Google.
- **Connessione privata** - utilizza una VPN o Google Cloud Interconnect e instrada il traffico attraverso un'interfaccia privata di Google Access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

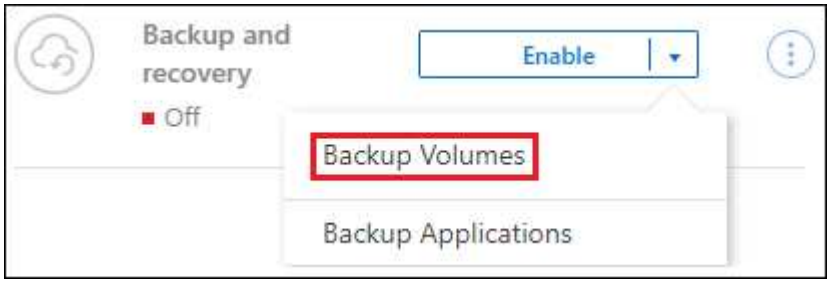
Puoi anche farlo Mostra i comandi API durante la fase di revisione, è possibile copiare il codice per automatizzare l'attivazione del backup per gli ambienti di lavoro futuri.

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.

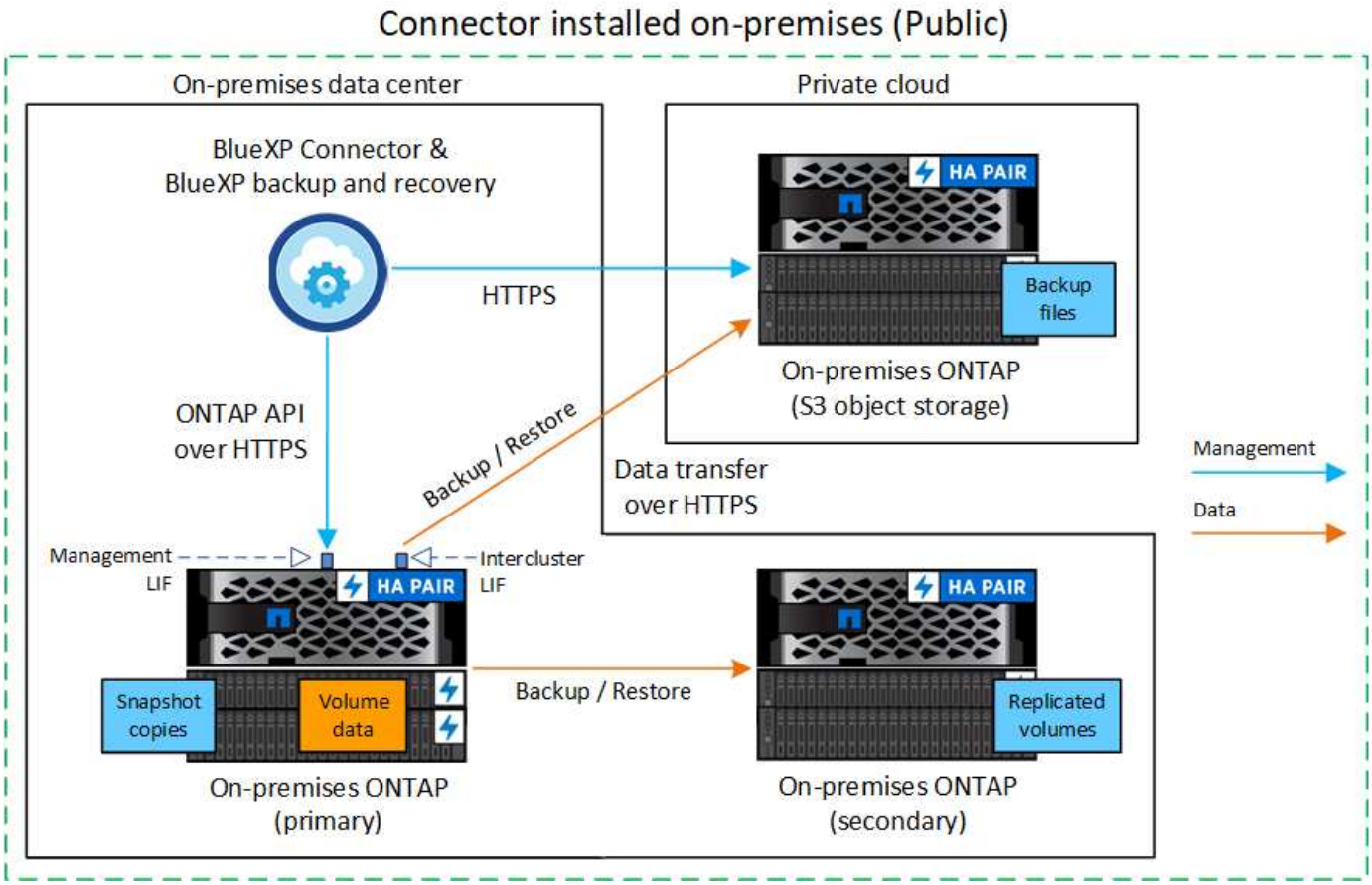
Attivare i backup sui ONTAP Volumes.

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.

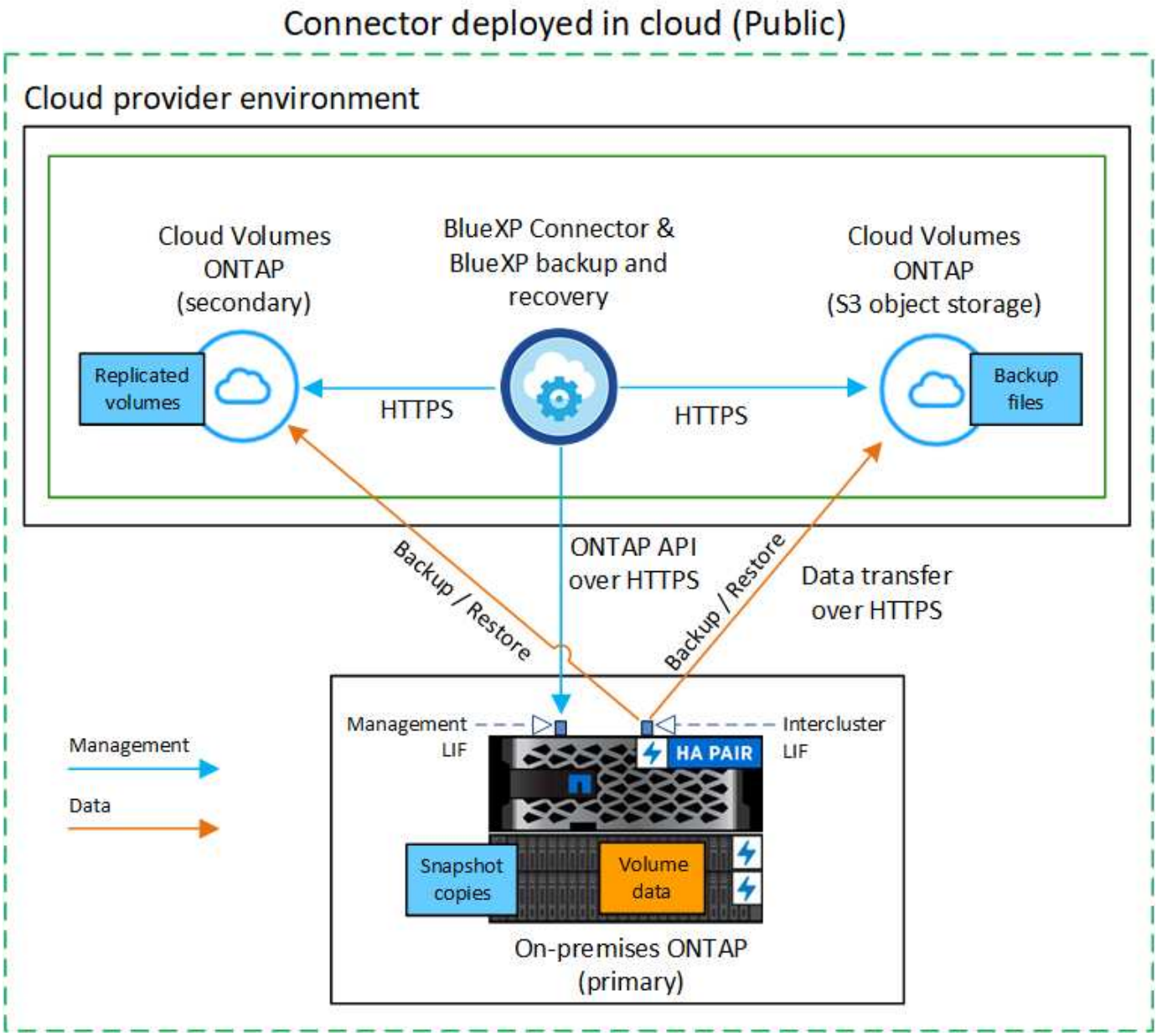
L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario on-premise su un sistema ONTAP on-premise configurato per S3 e le connessioni da preparare tra di essi. Mostra inoltre

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

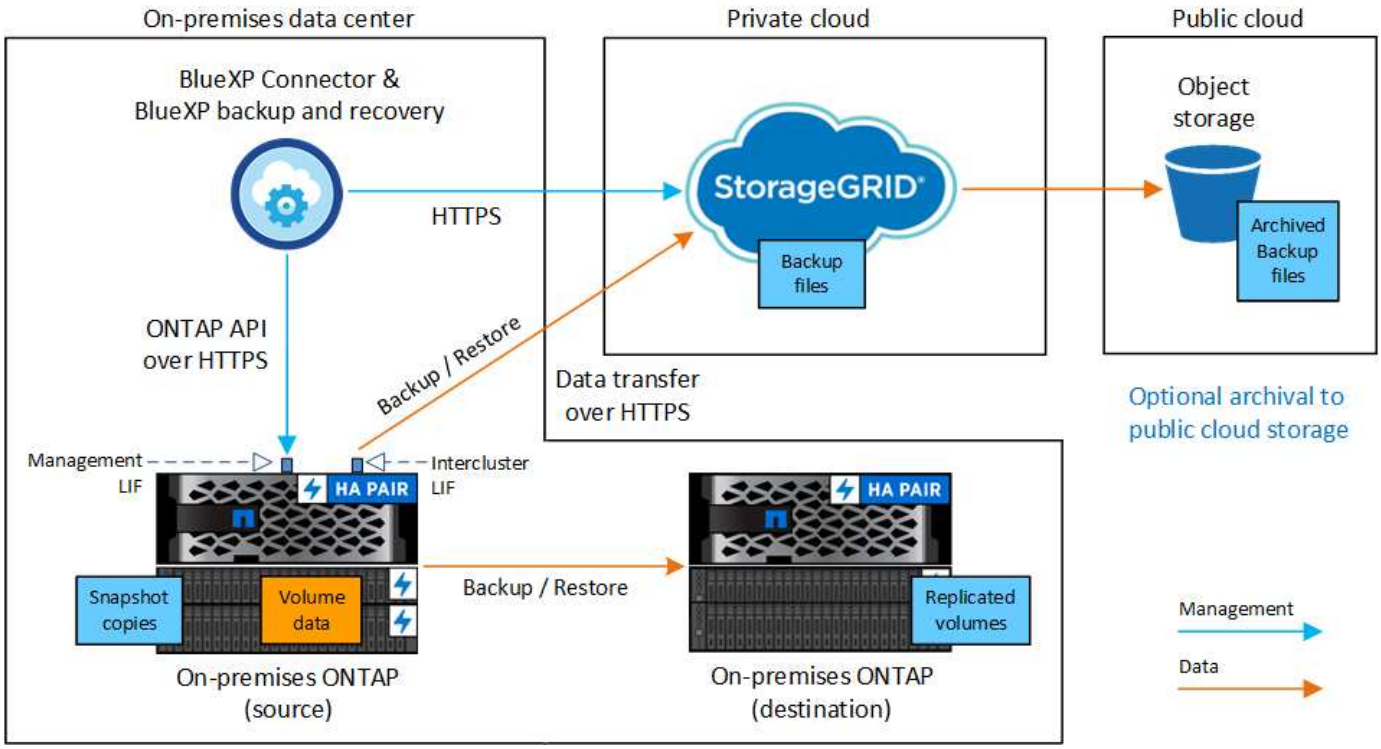
Selezionare l'ambiente di lavoro e fare clic su **Enable > Backup Volumes** (Abilita > volumi di backup) accanto al servizio di backup e ripristino nel pannello di destra. Quindi, seguire la procedura di installazione guidata per selezionare i criteri di replica e backup da utilizzare e i volumi di cui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

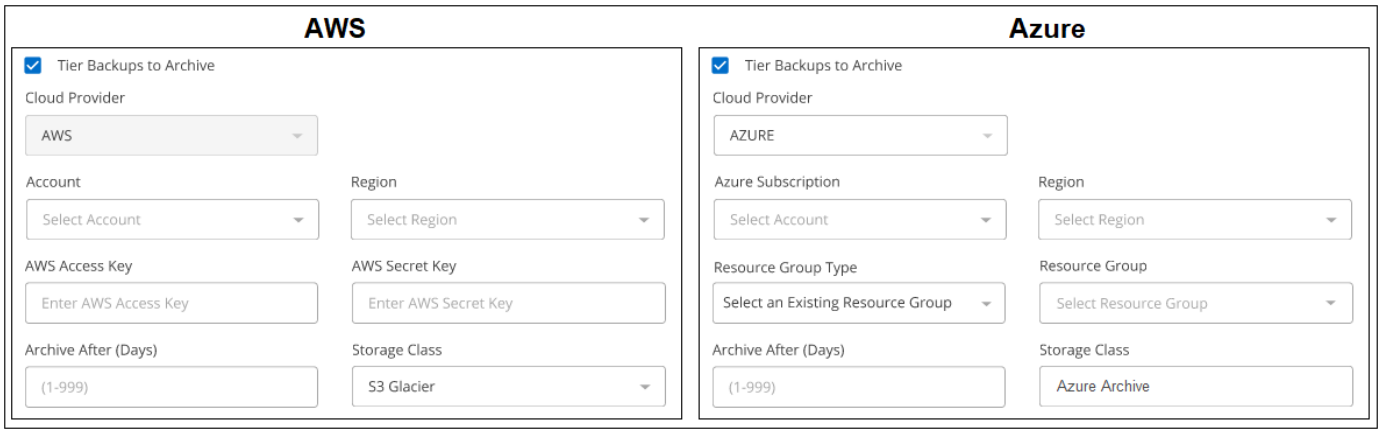
- Dovrai creare un account Amazon S3 per lo spazio di storage in cui verranno archiviati i backup.
- È possibile scegliere di eseguire il Tier dei backup nello storage AWS S3 Glacier o S3 Glacier Deep Archive. "Scopri di più sui Tier di archiviazione AWS".
- StorageGRID deve avere accesso completo al 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.

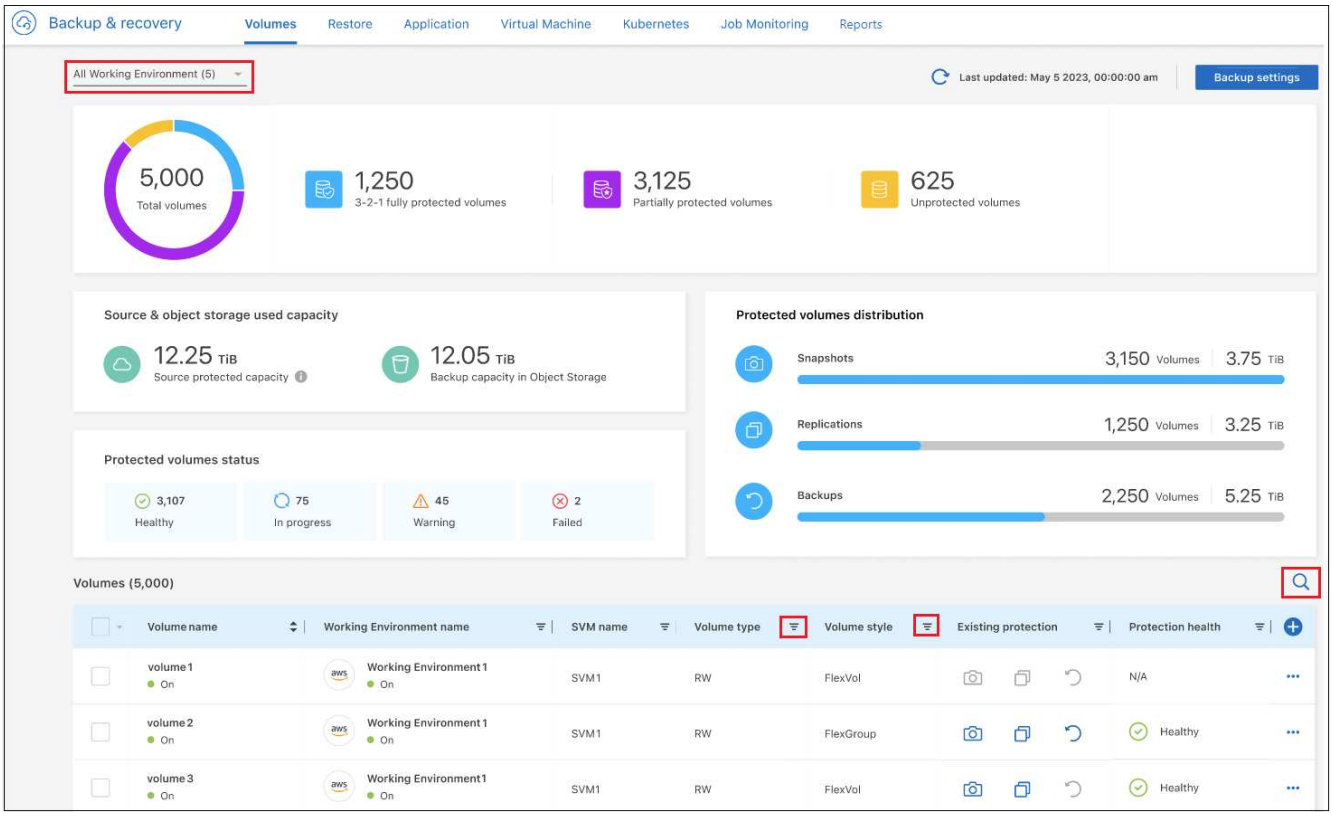
> Non gestire o modificare i file di backup direttamente sui sistemi storage o dall'ambiente del cloud provider. Questo potrebbe danneggiare i file e causare una configurazione non supportata.

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".

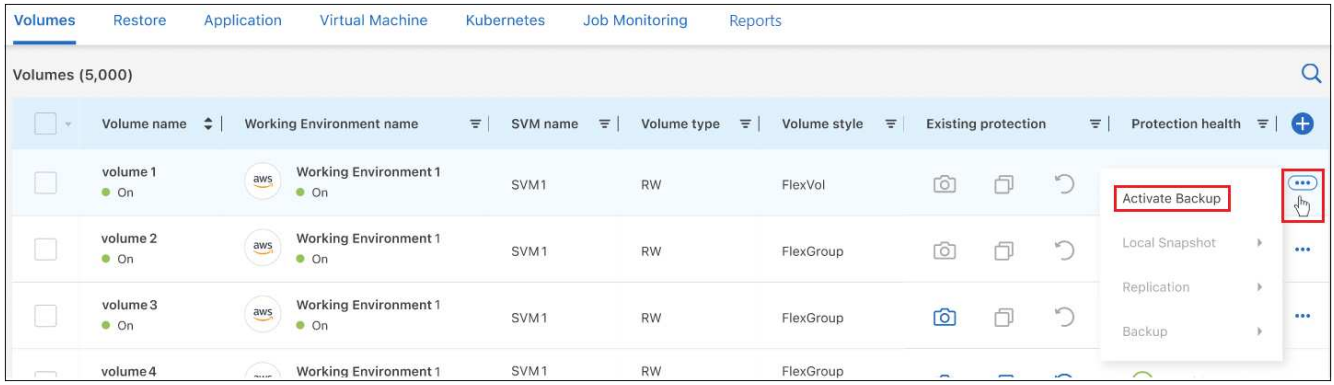
   Ogni icona è blu quando il tipo di backup è attivato e grigia quando il tipo di backup è inattivo. È possibile spostare il cursore su ciascuna icona per visualizzare la policy di backup utilizzata e altre informazioni pertinenti per ciascun tipo di backup.

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

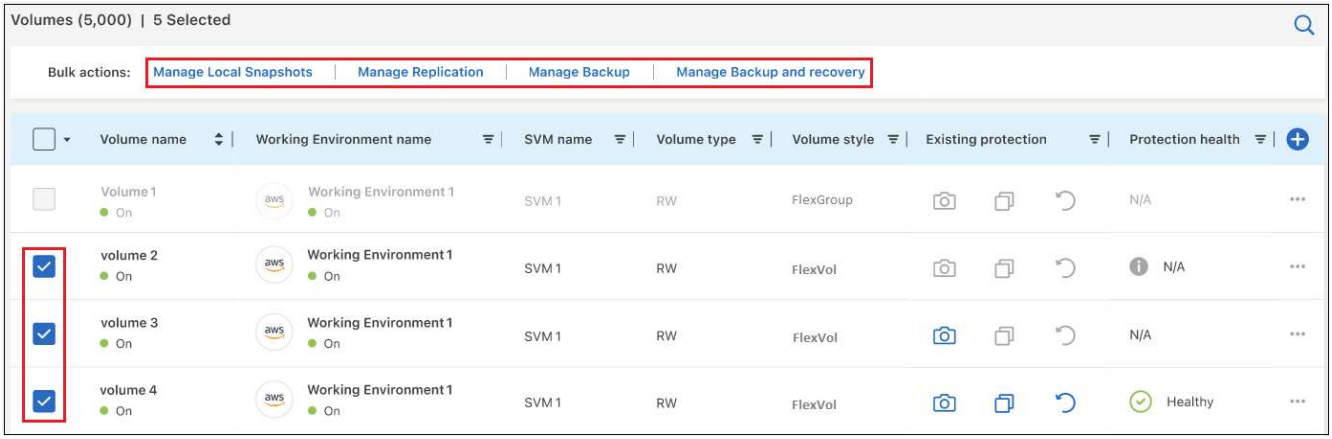
Se si desidera utilizzare le stesse impostazioni di backup su più volumi, è possibile attivare o modificare le impostazioni di backup su più volumi contemporaneamente. È possibile selezionare volumi che non dispongono di impostazioni di backup, solo di impostazioni Snapshot, solo di backup su impostazioni 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.

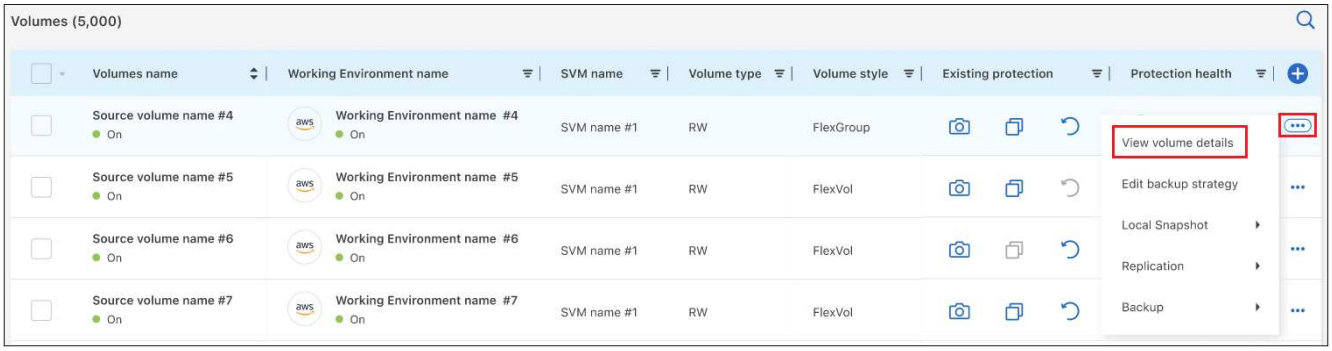
Visualizzare l'elenco dei backup per ciascun volume

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

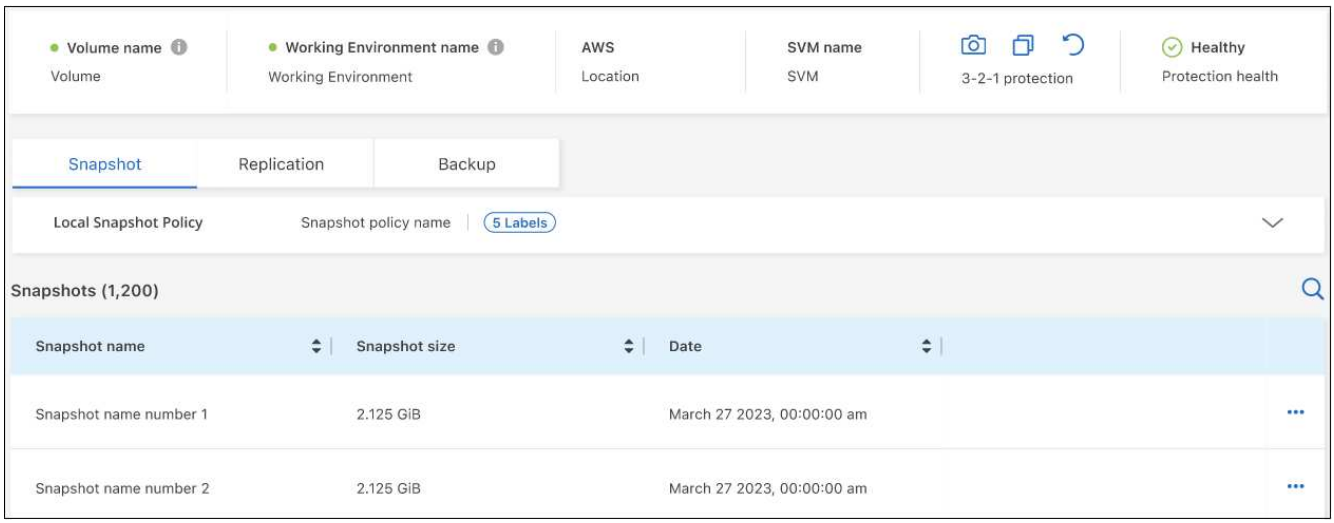
esempio l'ultimo backup eseguito, la policy di backup corrente, le dimensioni del file di backup e altro ancora.

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

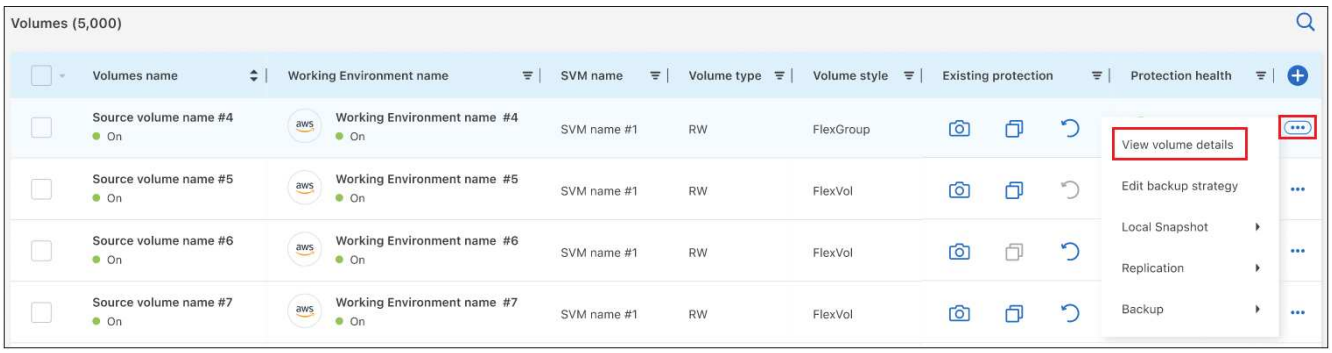
Il software di protezione ransomware di NetApp esegue la scansione dei file di backup per cercare la prova di un attacco ransomware quando viene creato un file di backup su oggetto e quando vengono ripristinati i dati di un file di backup. È inoltre possibile eseguire una scansione di protezione ransomware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

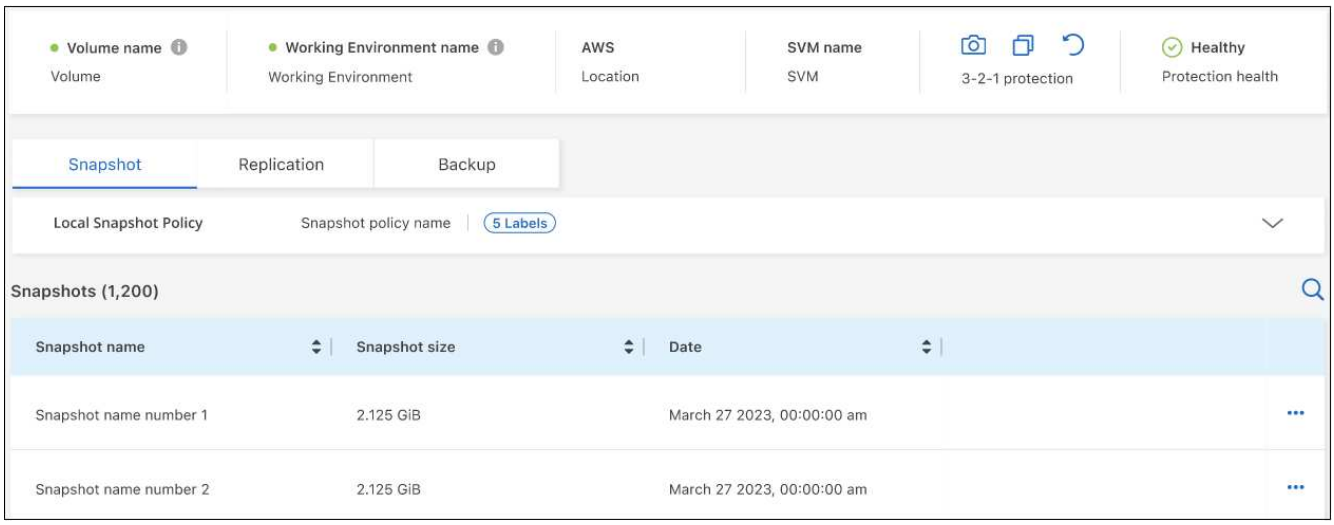
Questa funzione è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.11.1 o superiore e se sono stati attivati *DataLock e protezione ransomware* nel criterio di backup su oggetto.

Fasi

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

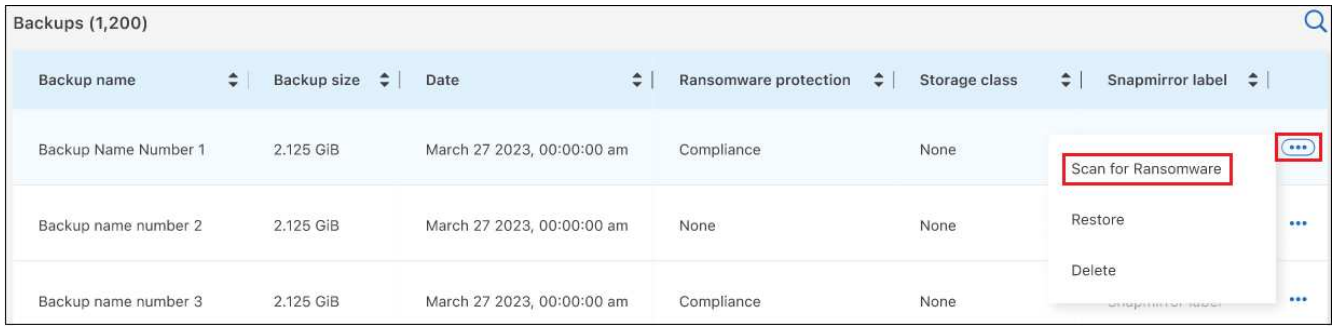


Vengono visualizzati i dettagli del volume.



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**.



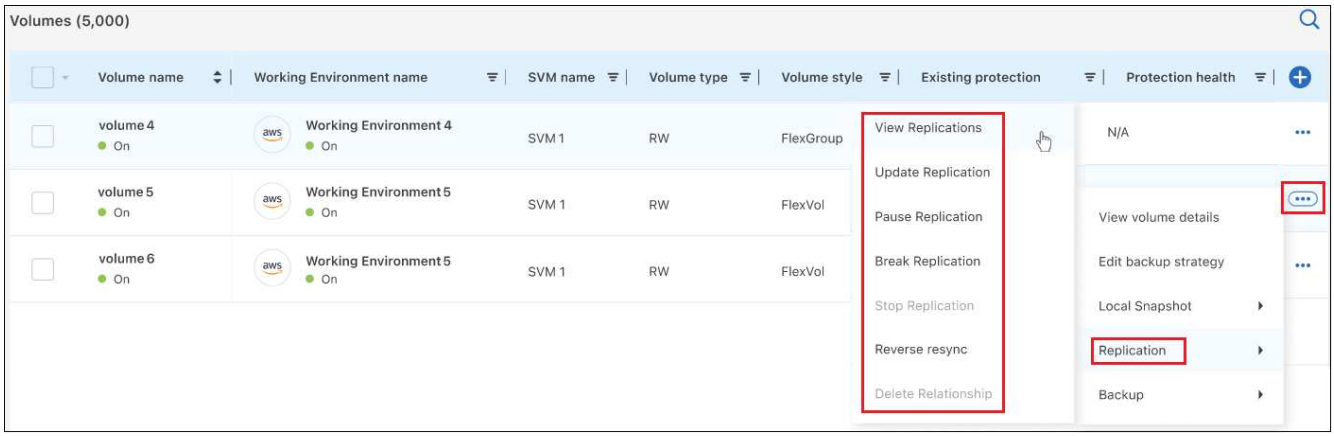
La colonna ransomware Protection (protezione ransomware) indica che la scansione è in corso.

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.

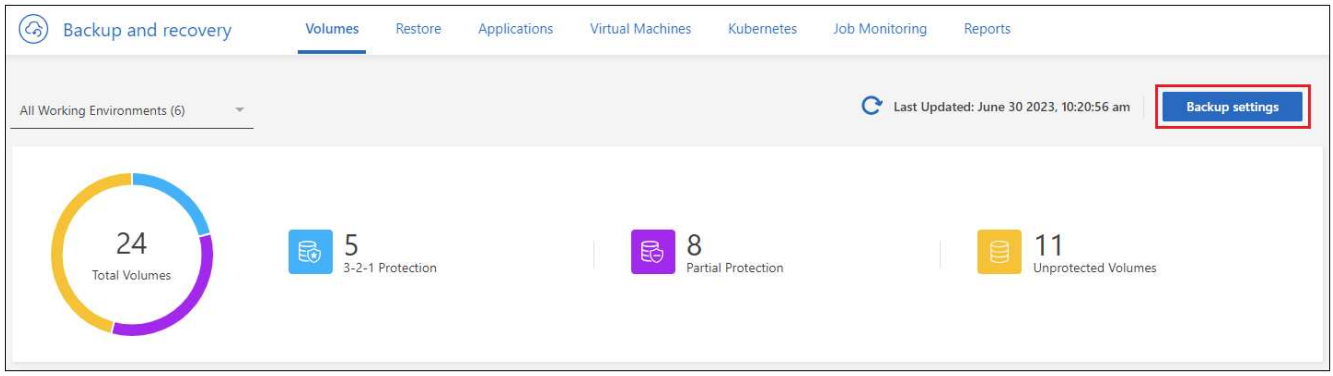
Modifica di una policy di backup nel cloud esistente

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.

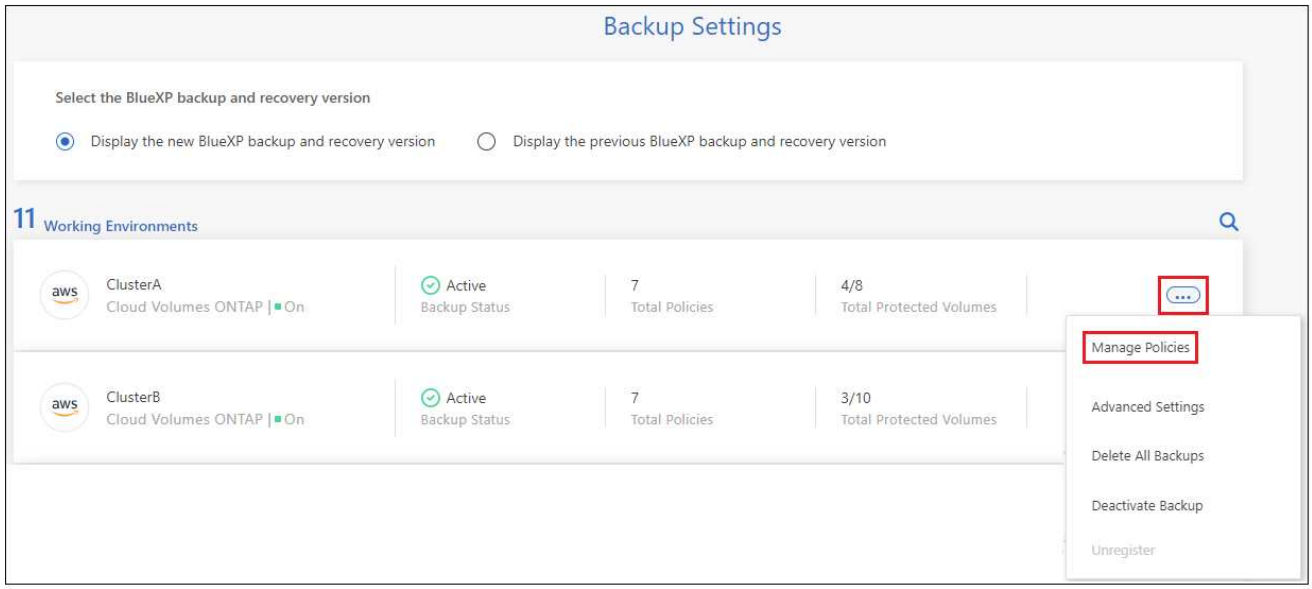
- Se sono stati attivati *DataLock e ransomware Protection* nel criterio iniziale quando si attiva il backup e il ripristino di BlueXP per questo cluster, tutti i criteri modificati devono essere configurati con la stessa impostazione DataLock (Governance o Compliance). Inoltre, se non sono stati attivati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

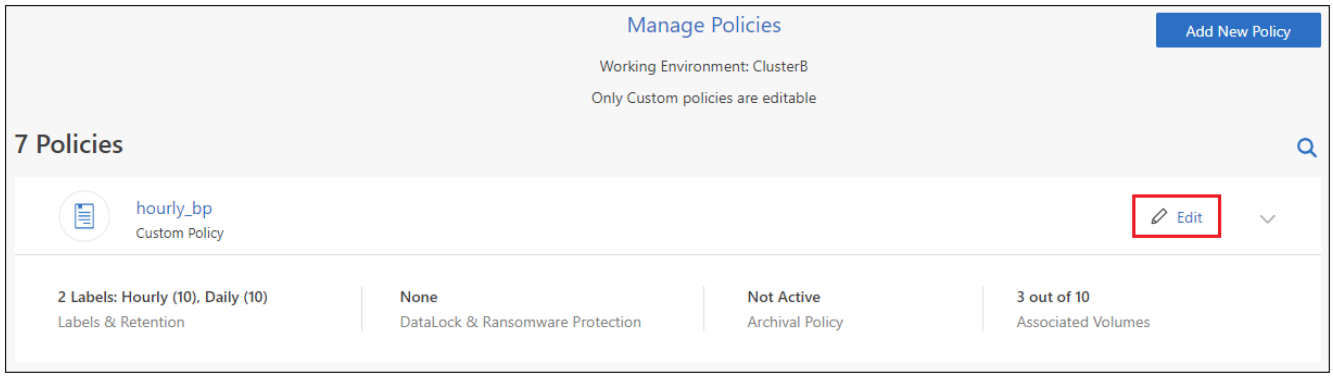
1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



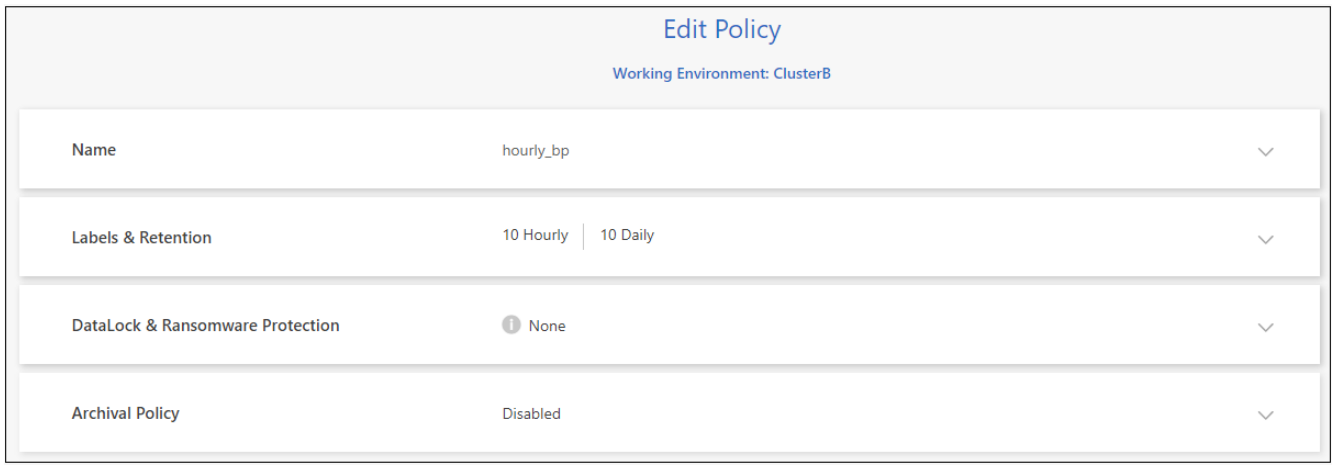
2. Nella pagina *Backup Settings*, fare clic su ••• Per l'ambiente di lavoro in cui si desidera modificare le impostazioni dei criteri e selezionare **Gestisci criteri**.



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**.

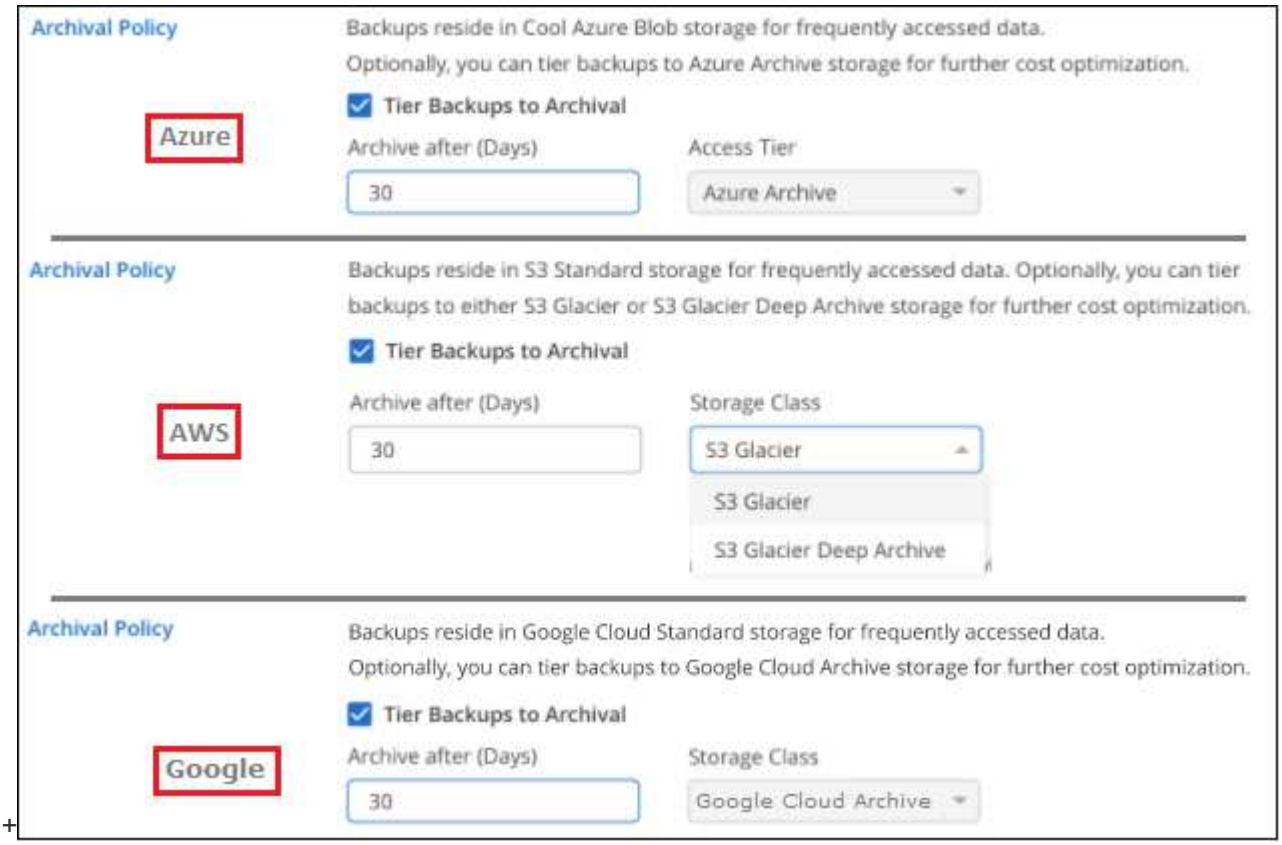


Se nel cluster è in esecuzione ONTAP 9.10.1 o versione successiva, è possibile attivare o disattivare il tiering dei backup nello storage di archiviazione dopo un certo numero di giorni.

"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

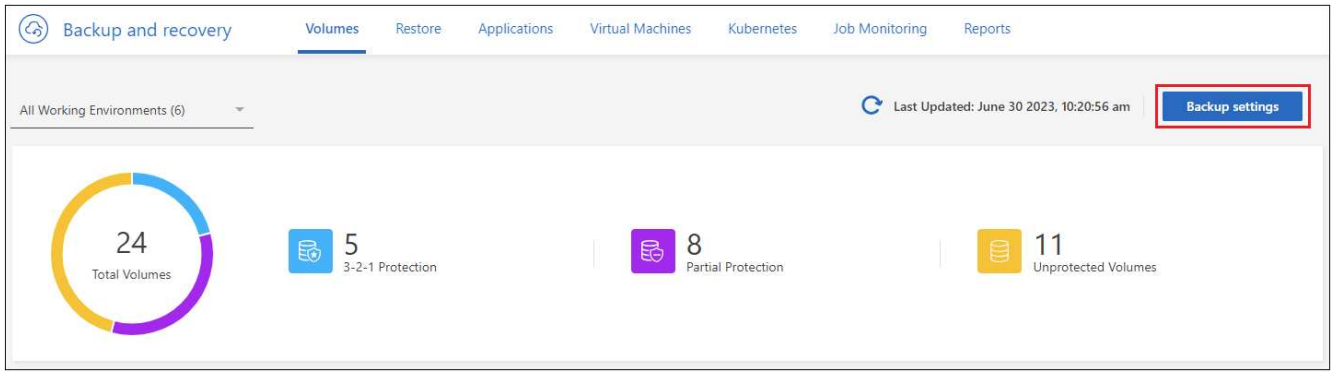
Quando si attiva il backup e il ripristino BlueXP per un ambiente di lavoro, tutti i volumi selezionati inizialmente vengono sottoposti a backup utilizzando il criterio di backup predefinito definito. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi RPO (Recovery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

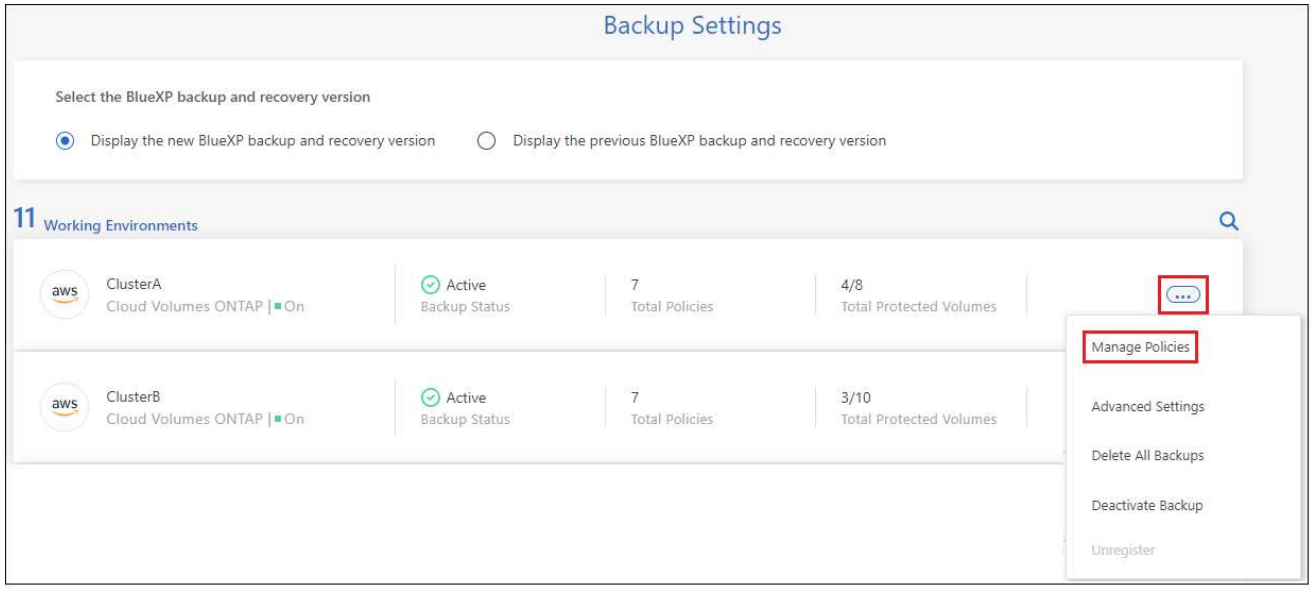
- Se sono stati attivati *DataLock e ransomware Protection* nella policy iniziale quando si attiva il backup e il ripristino di BlueXP per questo cluster, qualsiasi policy aggiuntiva creata deve essere configurata con la stessa impostazione DataLock (Governance o Compliance). Inoltre, se non sono stati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

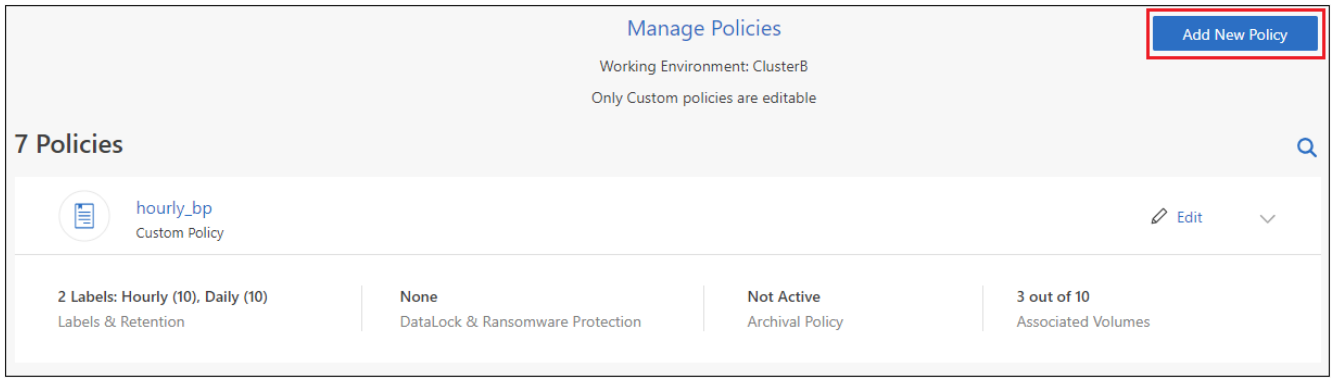
1. Dalla scheda **Volumes** (volumi), selezionare **Backup Settings** (Impostazioni di backup).



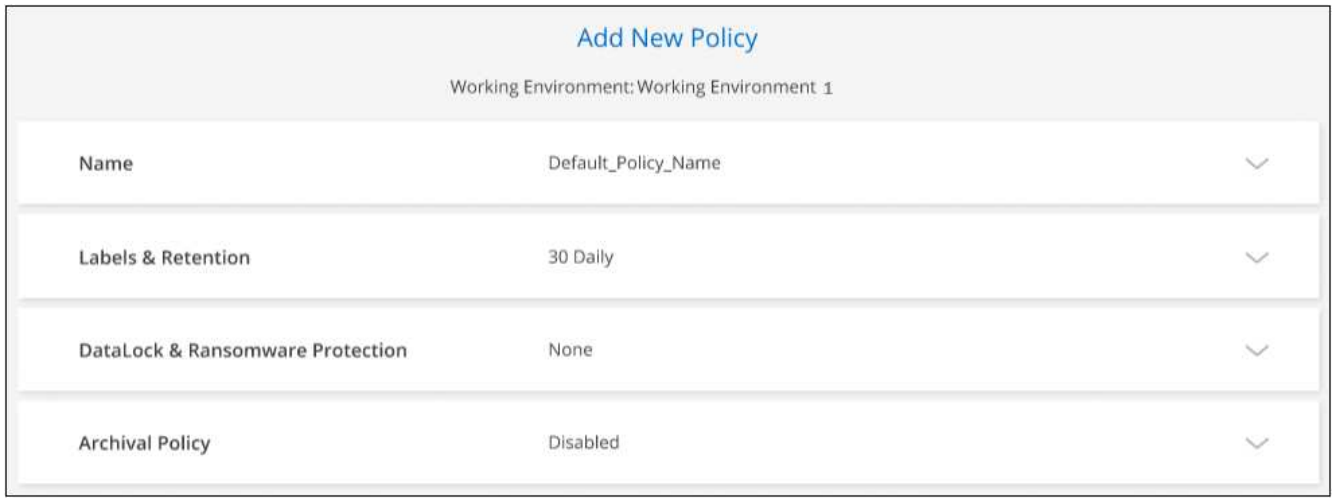
2. Nella pagina *Backup Settings*, fare clic su ••• Per l'ambiente di lavoro in cui si desidera aggiungere il nuovo criterio e selezionare **Gestisci criteri**.



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**.

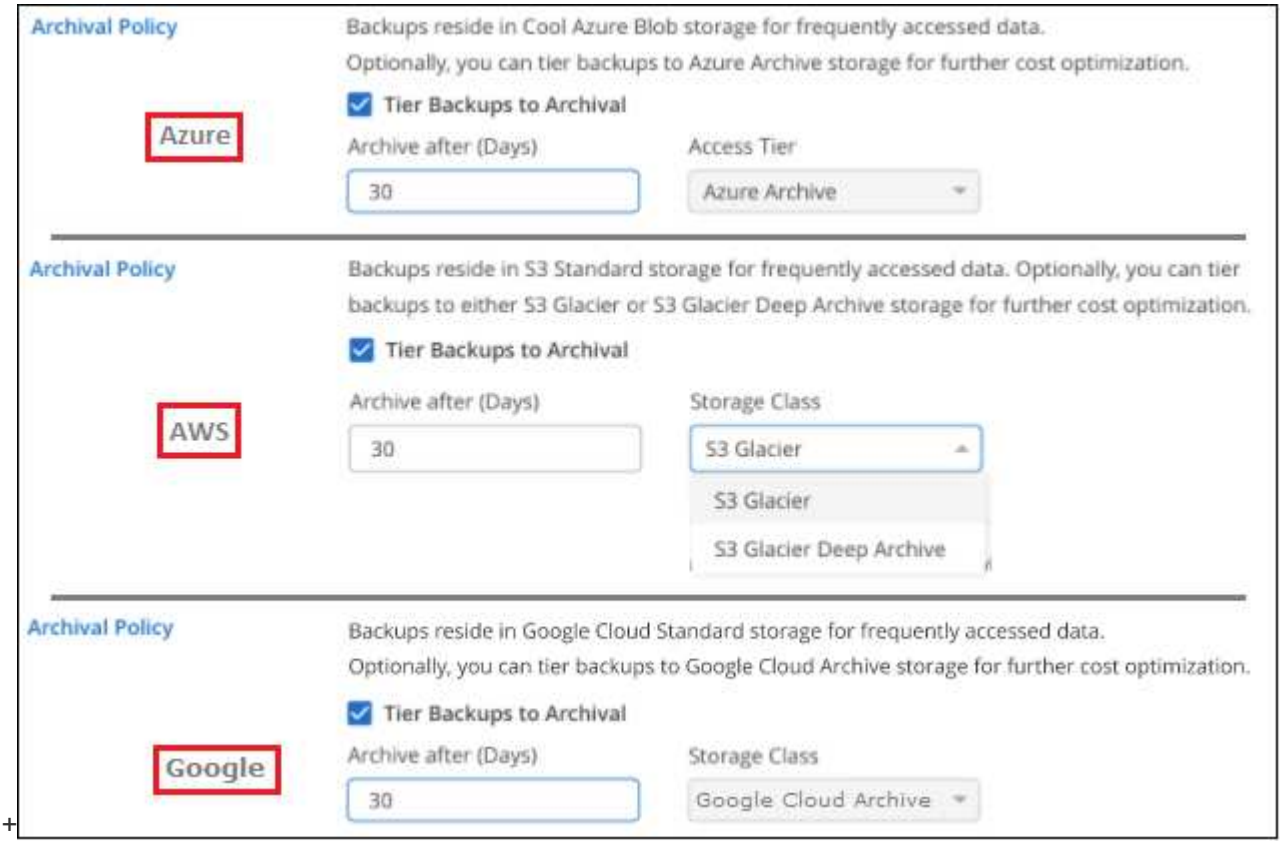


Se nel cluster è in esecuzione ONTAP 9.10.1 o versione successiva, è possibile attivare o disattivare il tiering dei backup nello storage di archiviazione dopo un certo numero di giorni.

"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

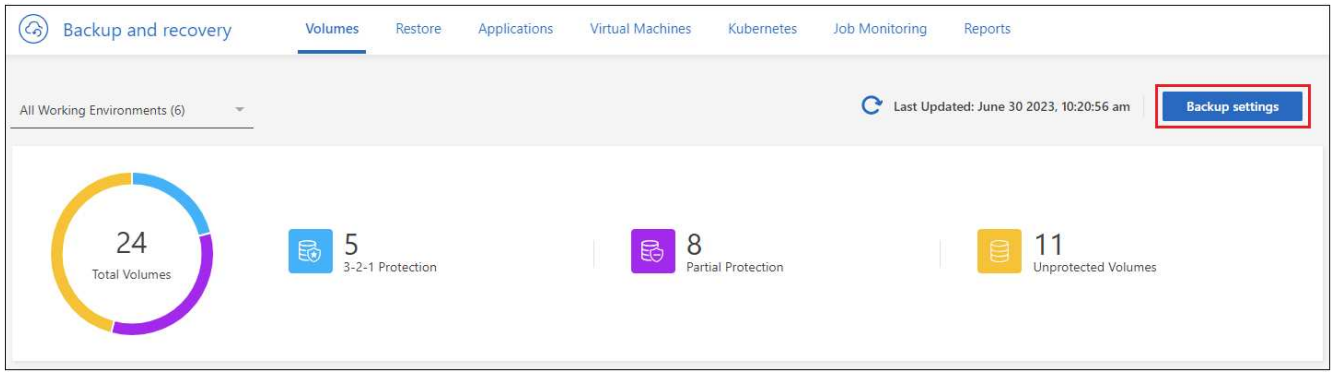
L'eliminazione di tutti i backup sullo storage a oggetti per un ambiente di lavoro non disattiva i backup futuri dei volumi in questo ambiente di lavoro. Se si desidera interrompere la creazione di backup di tutti i volumi in un ambiente di lavoro, è possibile disattivare i backup come descritto qui.

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

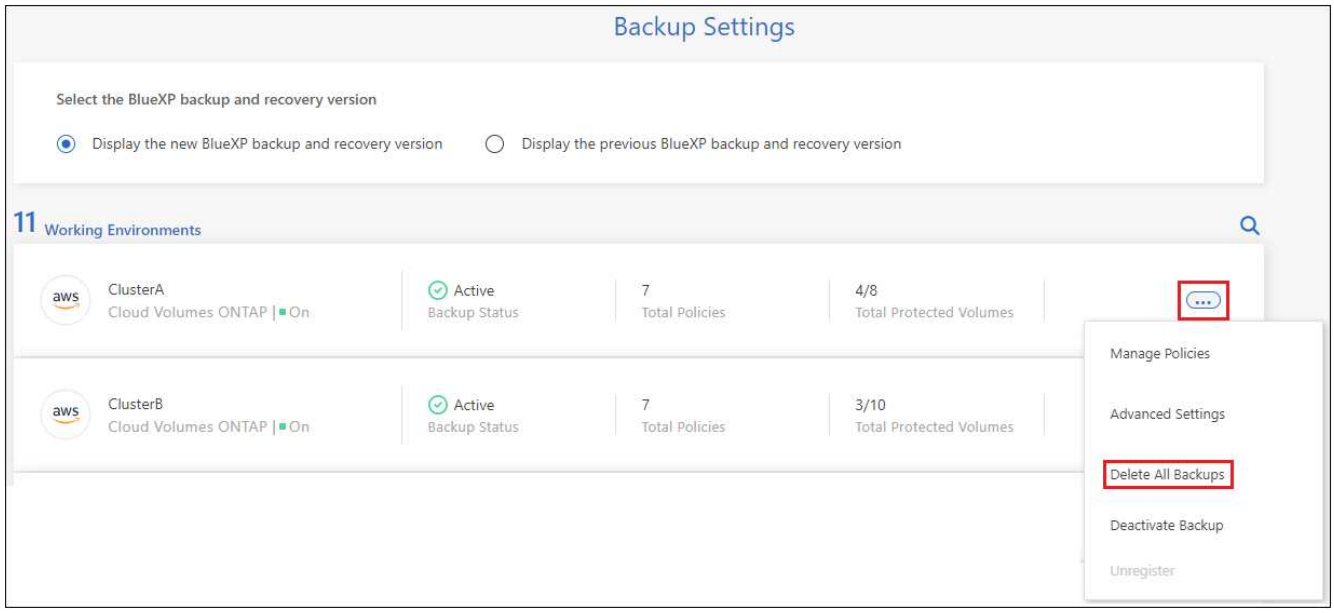
non vengono eliminati.

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).

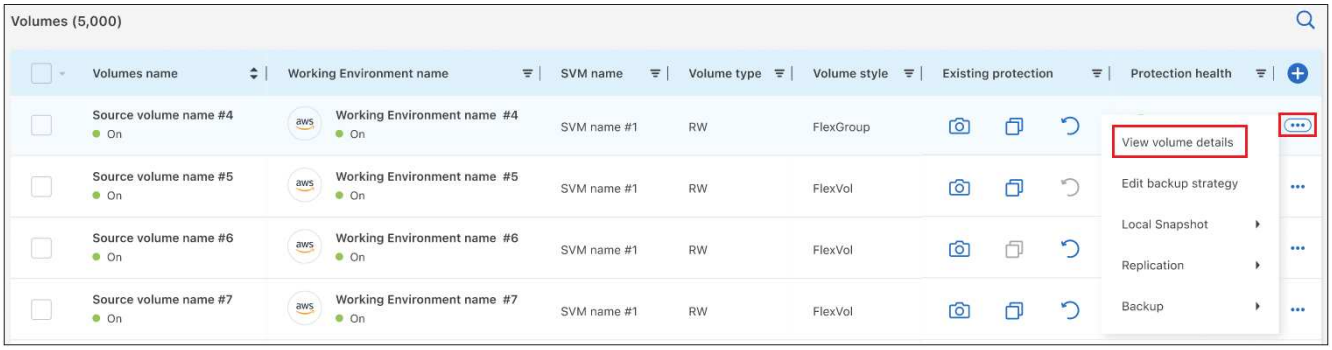
Eliminare un singolo file di backup per un volume

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.

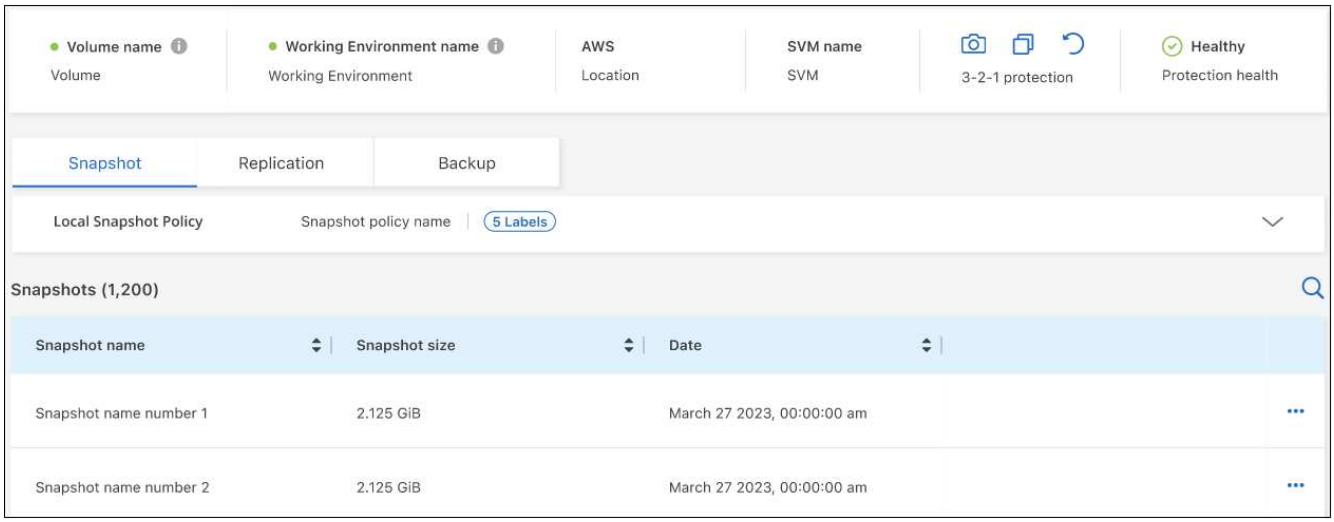
Non è possibile eliminare i volumi replicati (volumi di protezione dei dati).

Fasi

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

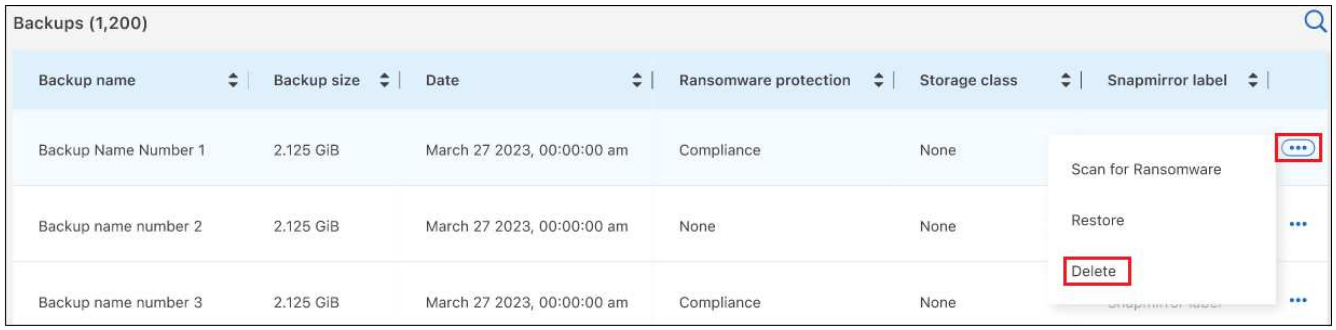


Vengono visualizzati i dettagli del volume ed è possibile selezionare **Snapshot**, **Replication** o **Backup** per visualizzare l'elenco di tutti i file di backup del volume. Per impostazione predefinita, vengono visualizzate le copie Snapshot disponibili.



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.

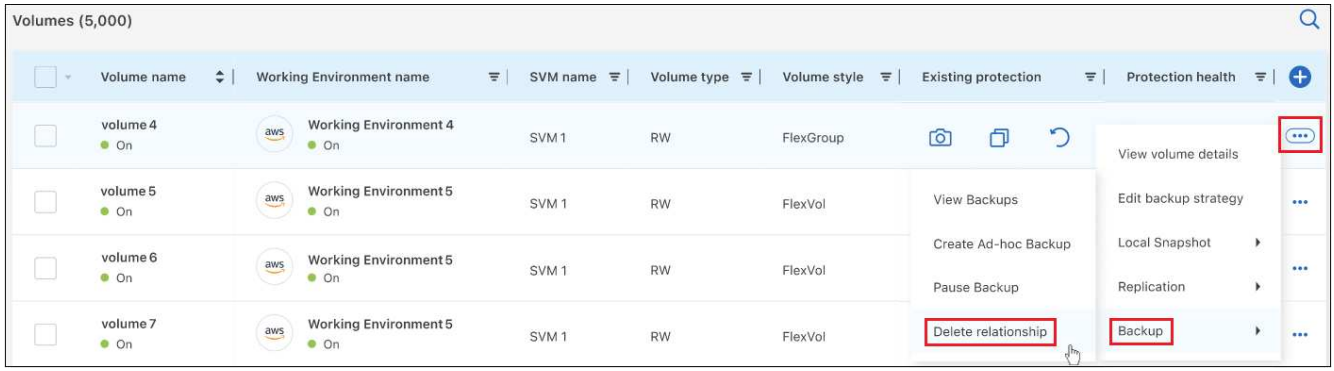
Questa funzione è disponibile solo se nel sistema è in esecuzione ONTAP 9.12.1 o versione successiva.

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**.



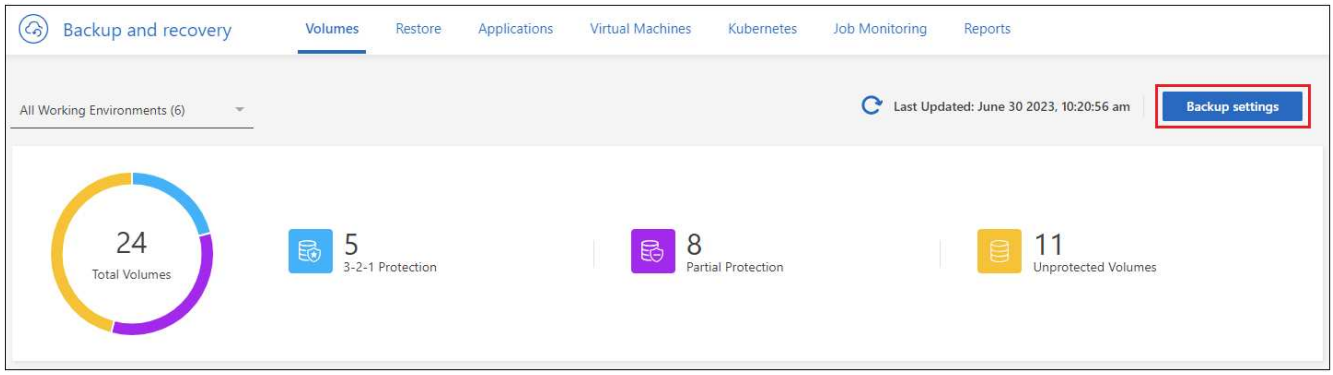
Disattivare il backup e ripristino BlueXP per un ambiente di lavoro

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.

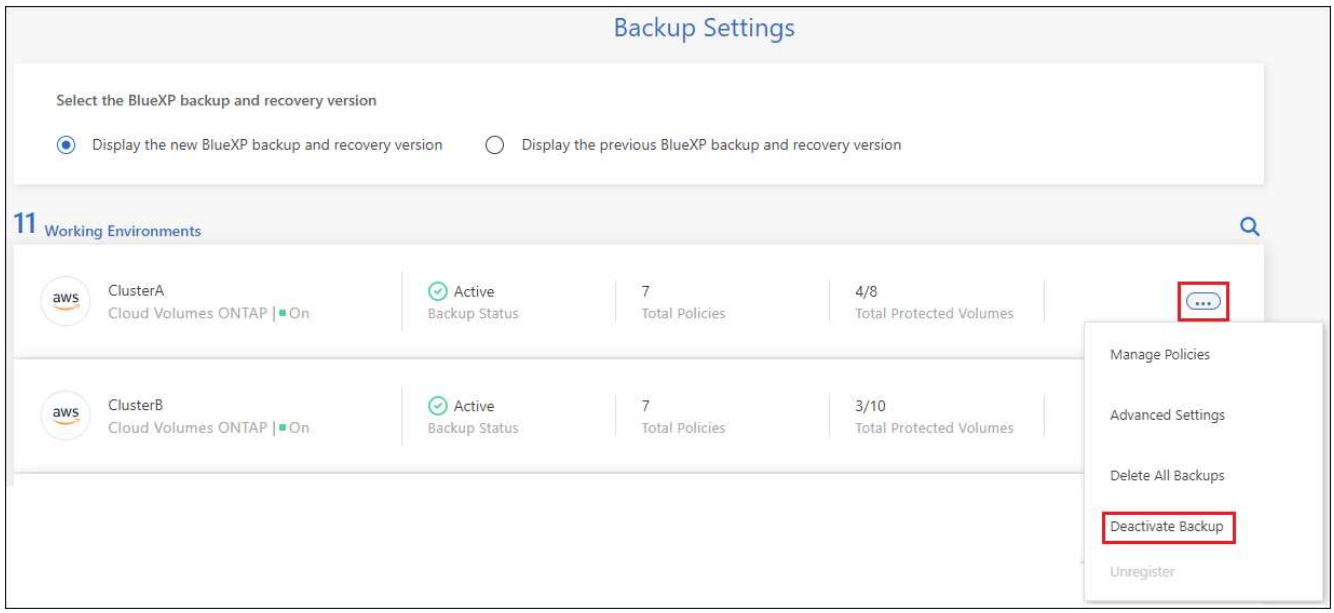
Tieni presente che il tuo cloud provider continuerà a addebitare i costi dello storage a oggetti per la capacità utilizzata dai backup, a meno che tu non lo utilizzi eliminare i backup.

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.

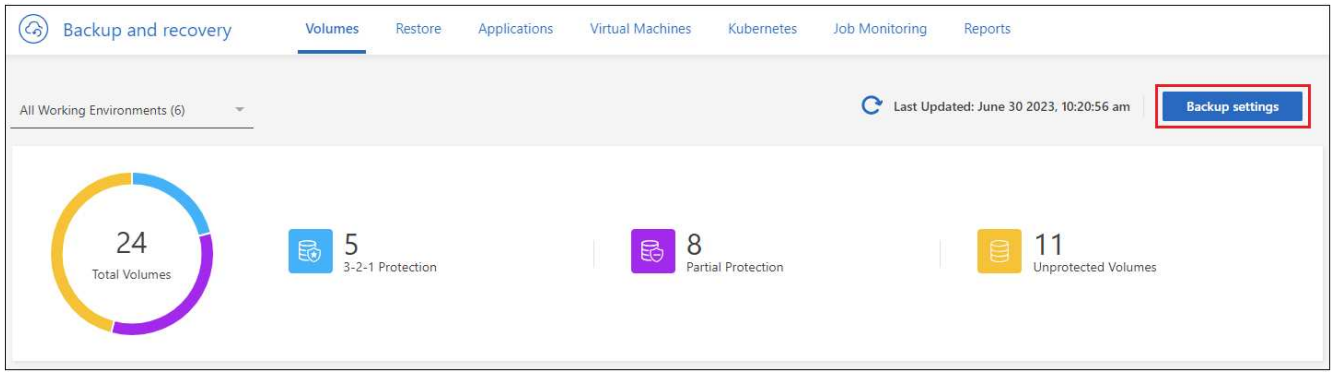
Prima di annullare la registrazione di backup e ripristino BlueXP, è necessario eseguire le seguenti operazioni, nell'ordine indicato:

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

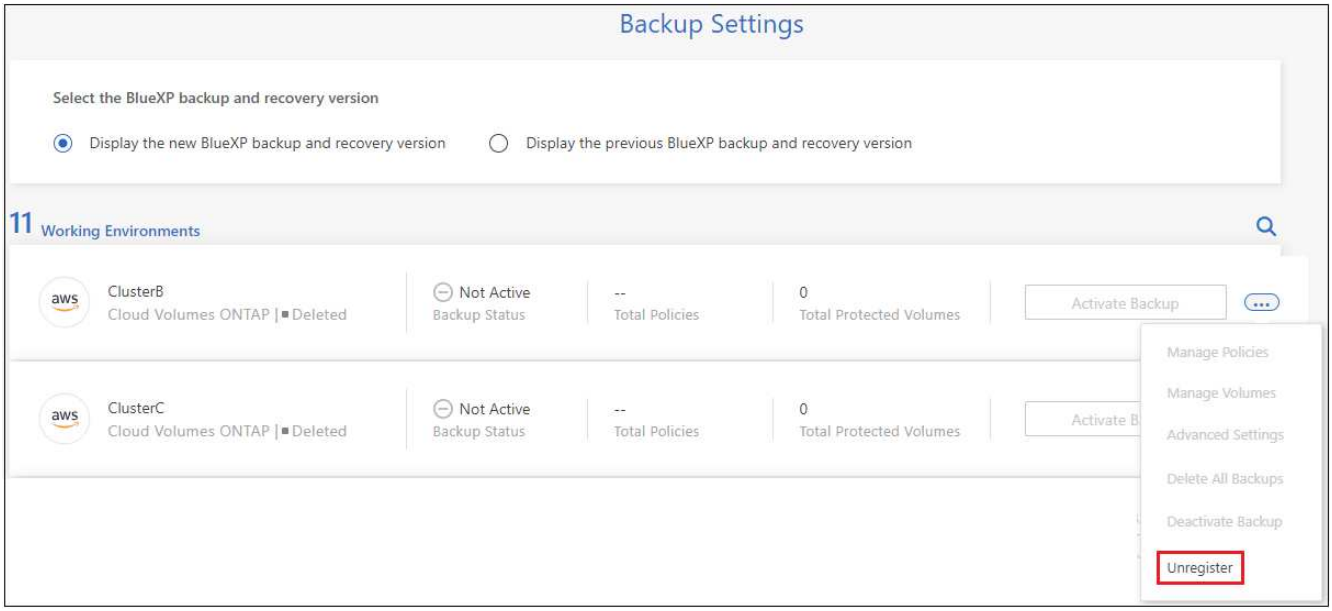
L'opzione di annullamento della registrazione non è disponibile fino al completamento di queste due azioni.

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:

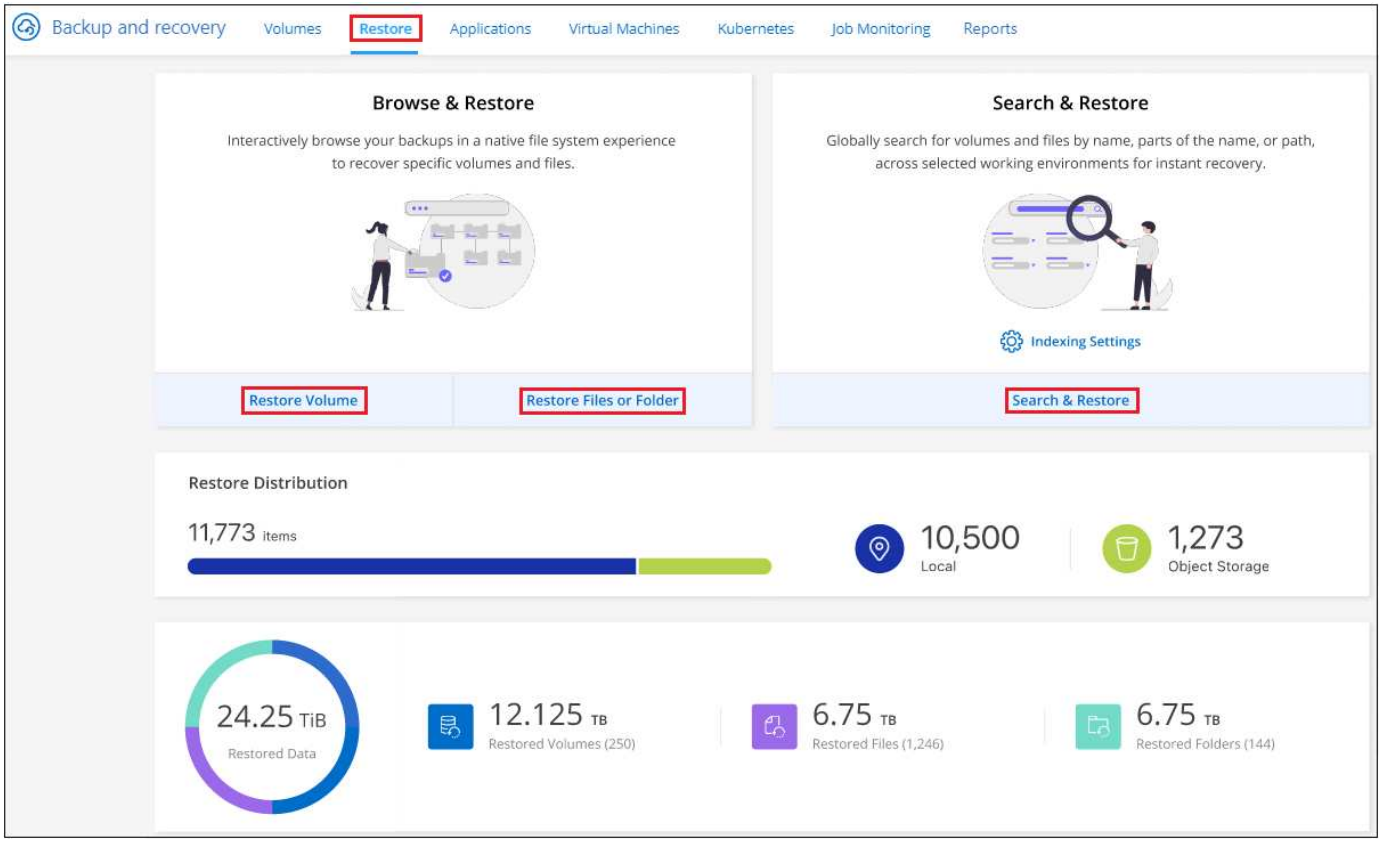
- File di backup → volume ripristinato
- Volume replicato → volume ripristinato
- Copia Snapshot → Volume ripristinato

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.

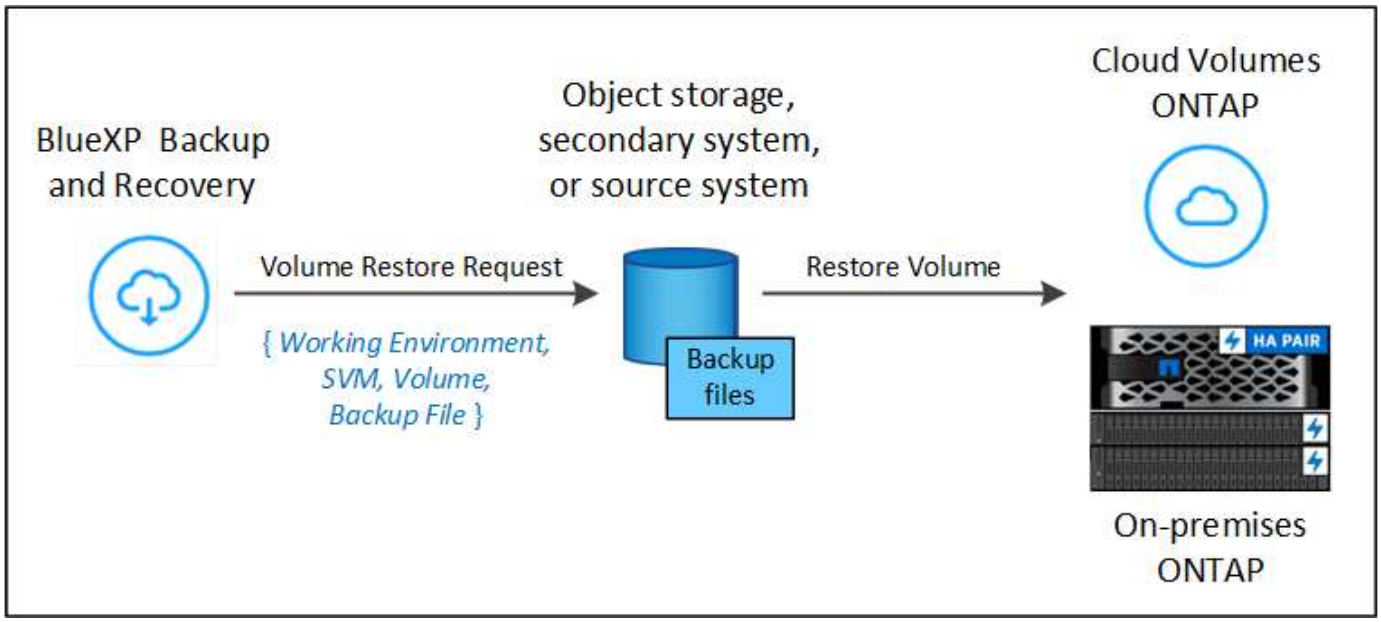
Ripristinare i volumi utilizzando Sfoglia & Ripristina

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.

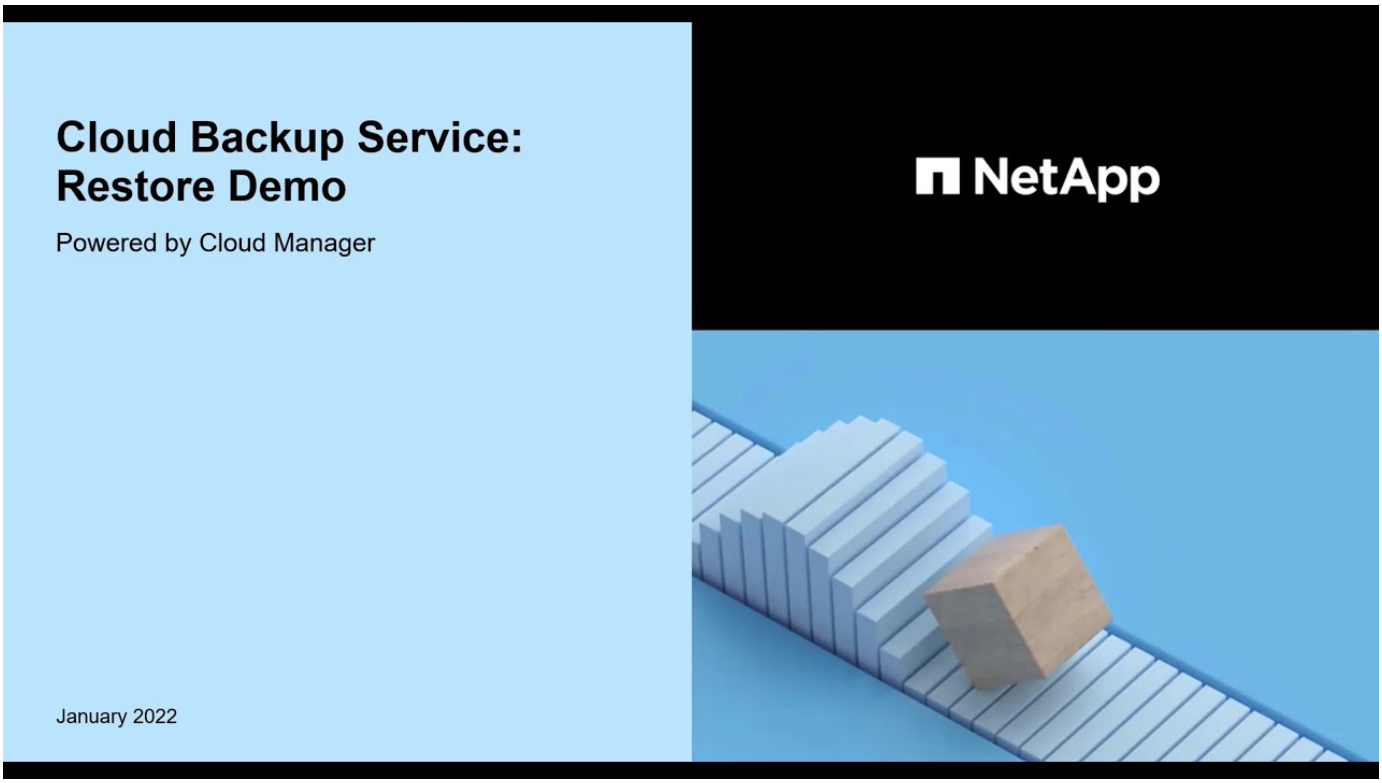
Quando si esegue il ripristino da un volume replicato, è possibile ripristinare il volume nell'ambiente di lavoro originale o in un sistema Cloud Volumes ONTAP o ONTAP on-premise.



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:

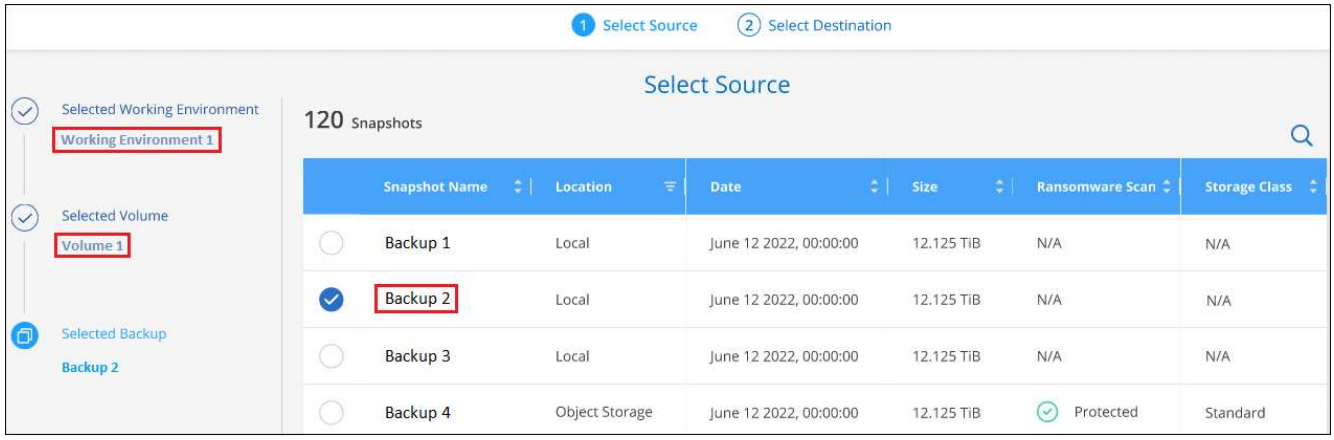


Fasi

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.

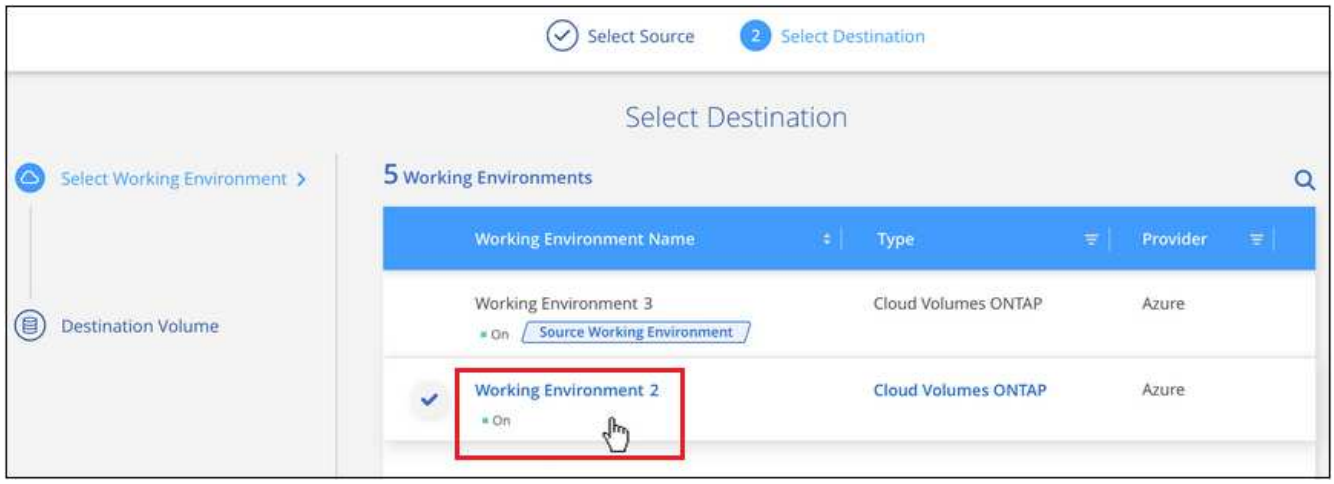
   La colonna **percorso** indica se il file di backup (Snapshot) è **locale** (una copia Snapshot sul sistema di origine), **secondario** (un volume replicato su un sistema ONTAP secondario) o **archiviazione oggetto** (un file di backup nello storage a oggetti). Scegliere il file che si desidera ripristinare.



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).

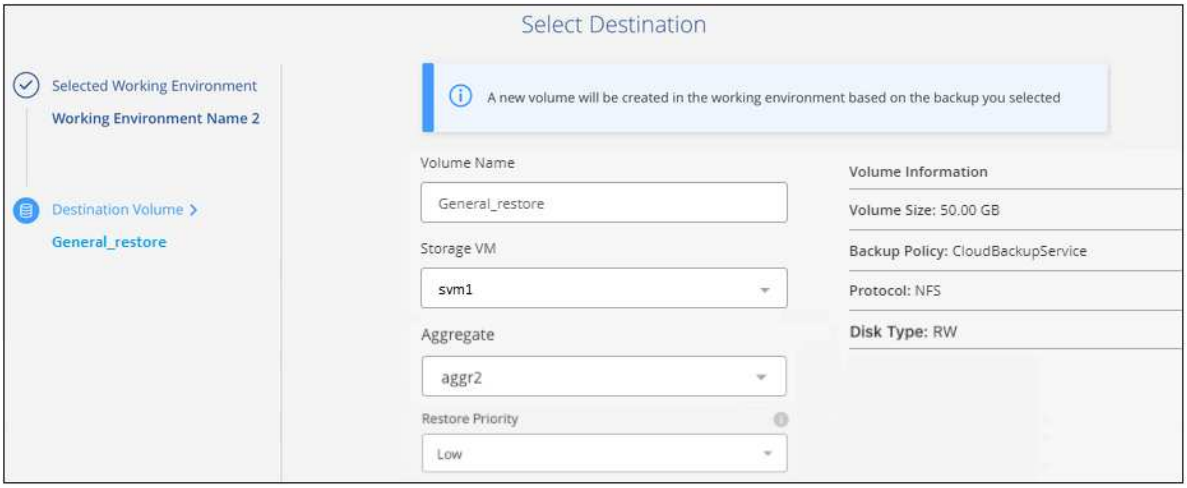
6. Nella pagina *Select Destination*, selezionare **Working Environment** (ambiente di lavoro) in cui si desidera ripristinare il volume.



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*.

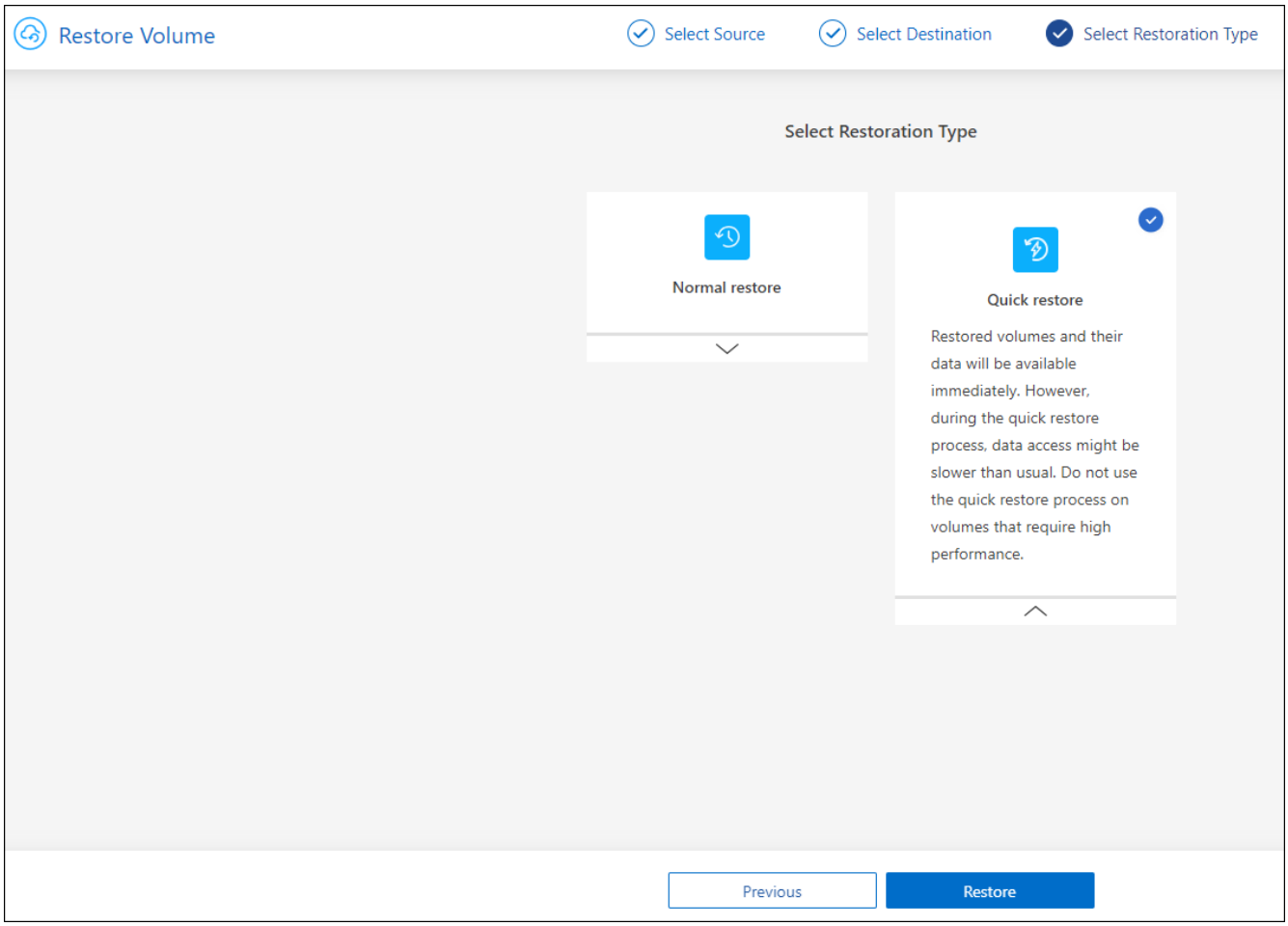
Se si sta ripristinando il volume da un file di backup che risiede in un Tier di storage di archiviazione (disponibile a partire da ONTAP 9.10.1), è possibile selezionare la priorità di ripristino.

"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.

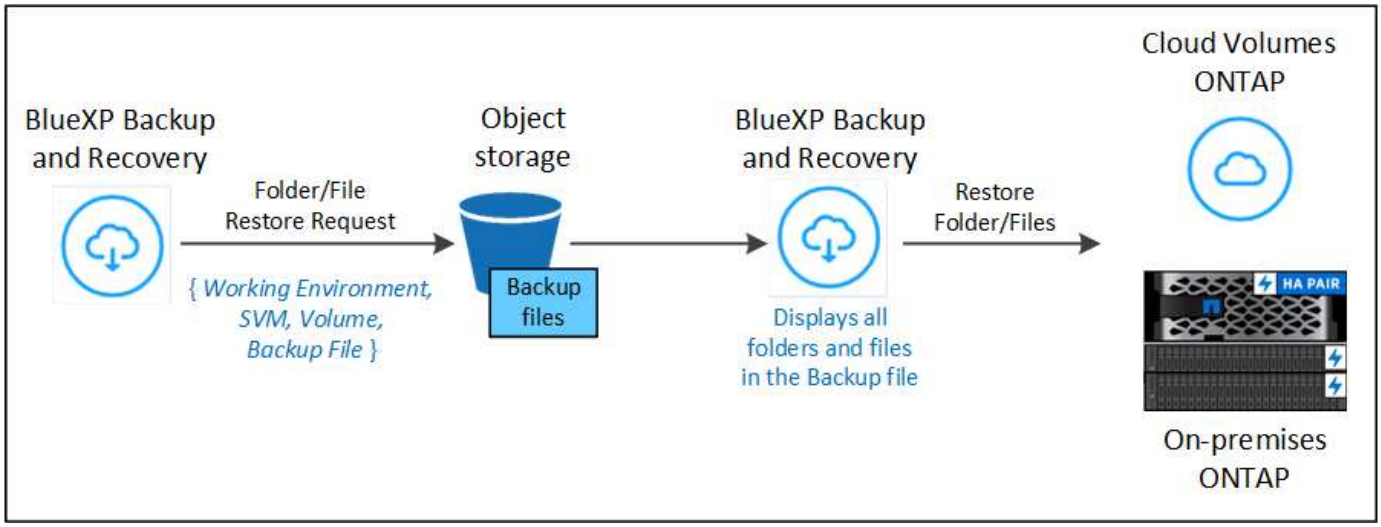
Prerequisiti

- 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.

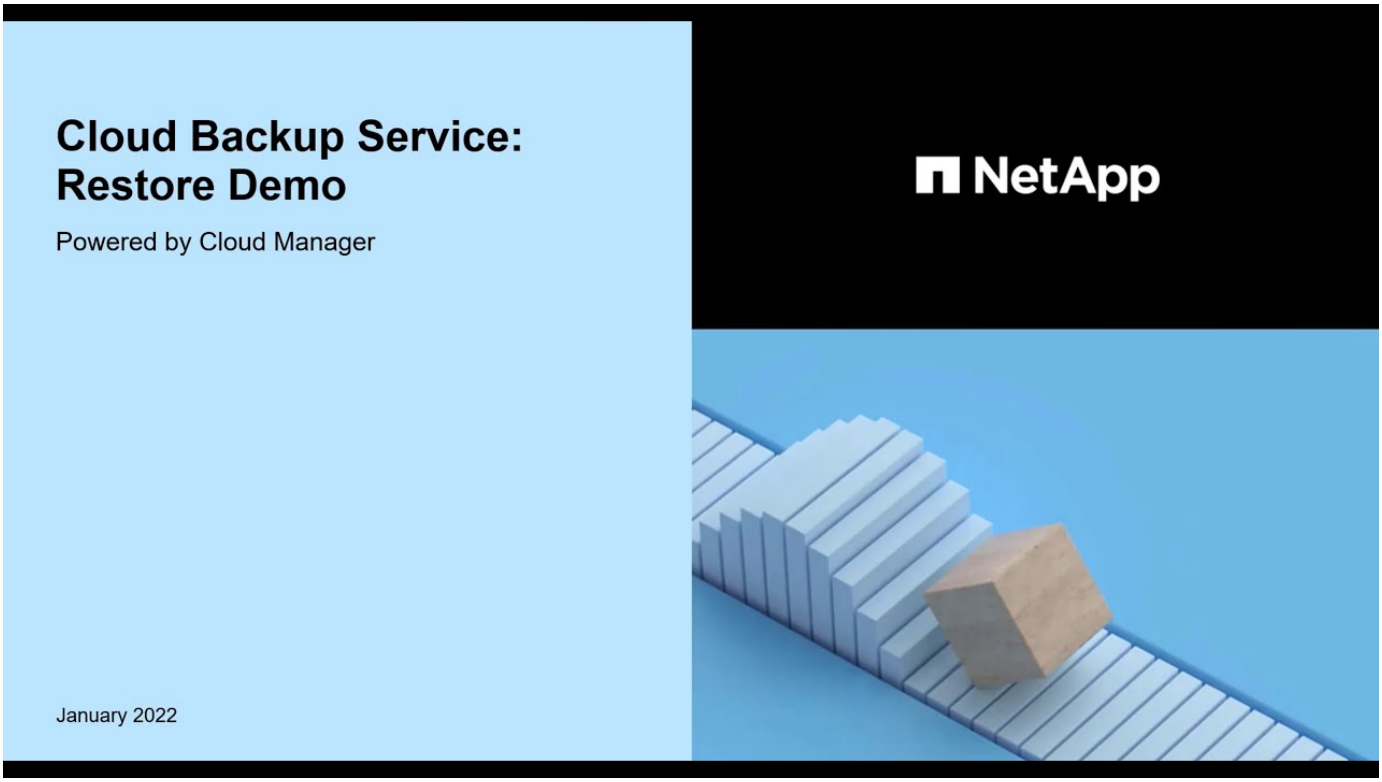


Come si può vedere, è necessario conoscere il nome dell'ambiente di lavoro, il nome del volume, la data del file di backup e il nome della cartella/file per eseguire il ripristino di una cartella o di un file.

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.

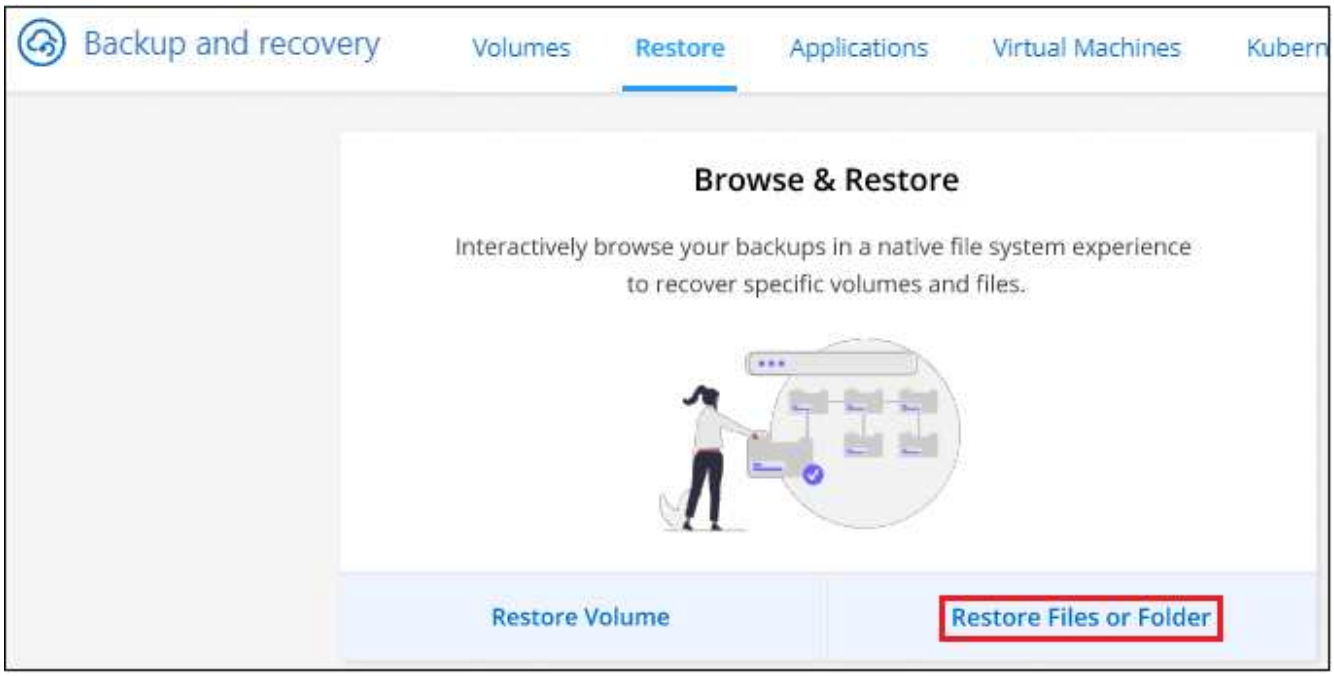
Il video seguente mostra una rapida procedura dettagliata per il ripristino di un singolo file:



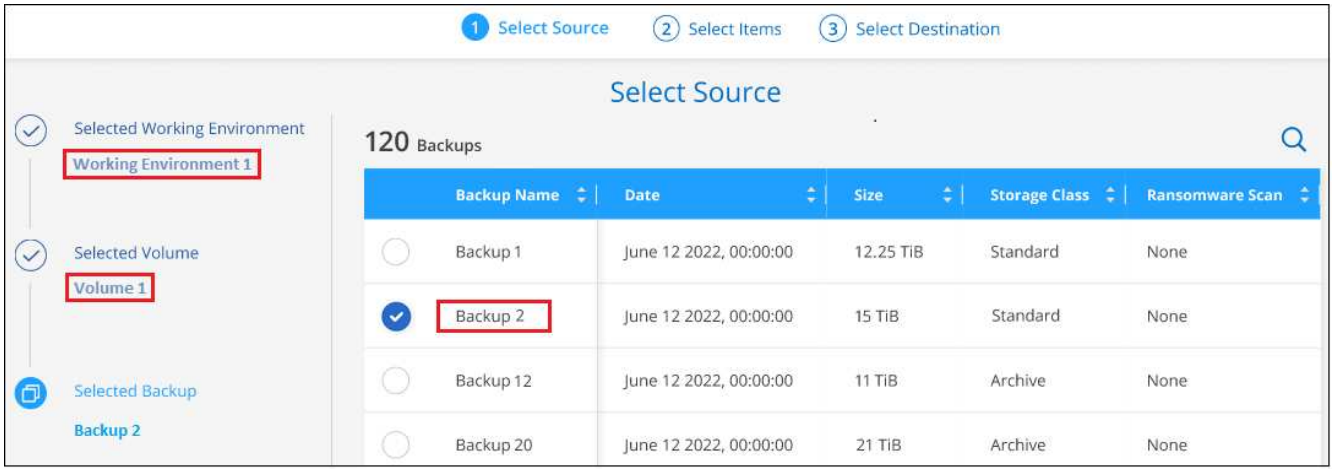
Fasi

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.

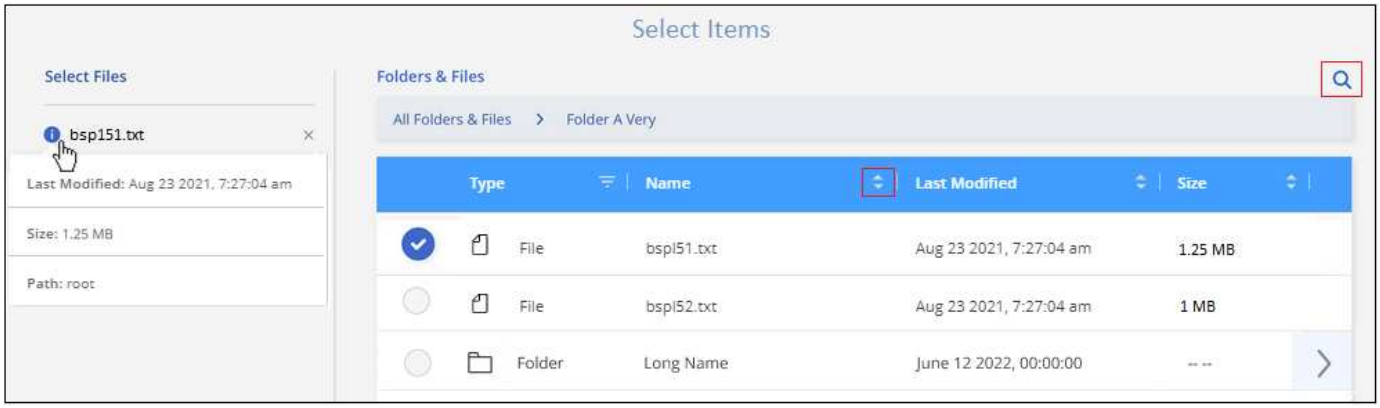
"Scopri di più sul ripristino dallo storage di archiviazione AWS".

"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).

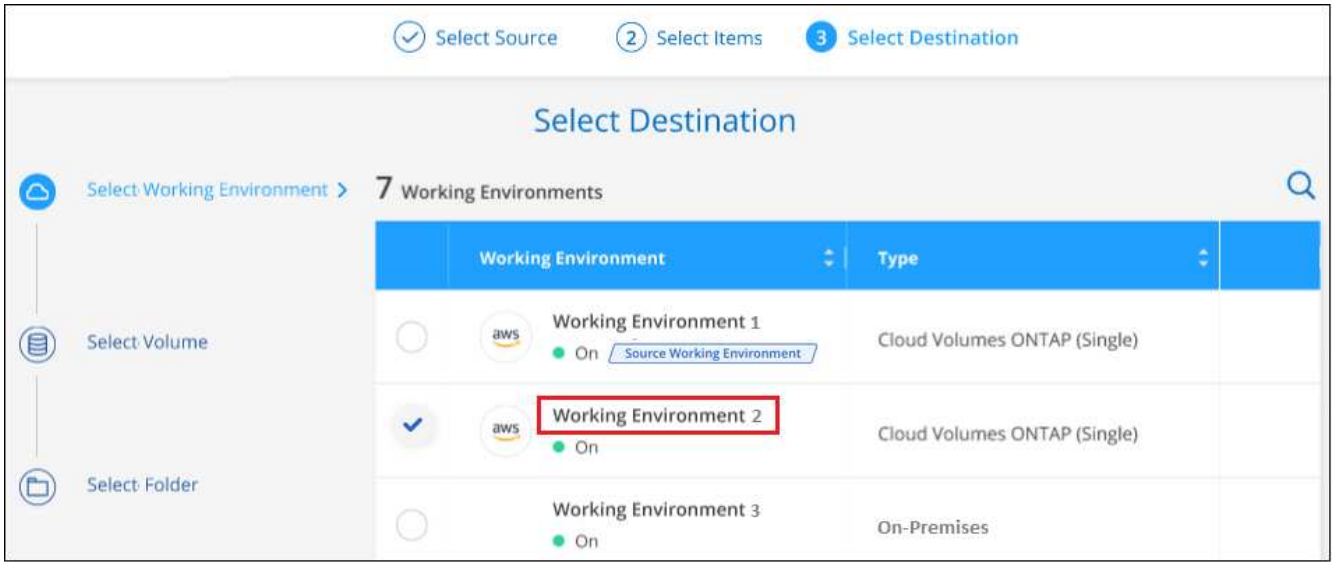
+



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.

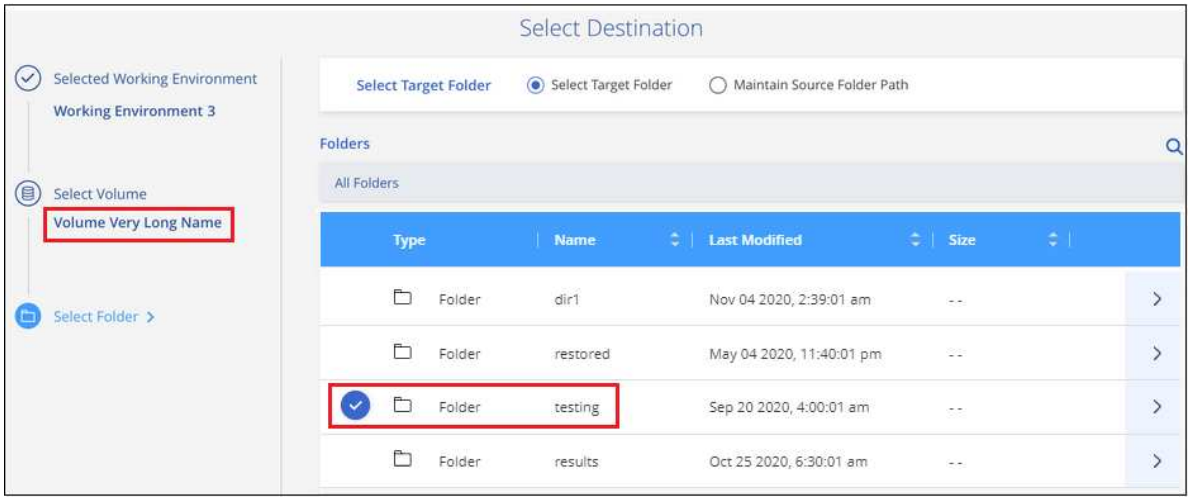
2. Nella pagina *Select Destination* (Seleziona destinazione), selezionare **Working Environment** (ambiente di lavoro) in cui si desidera ripristinare gli elementi.



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.

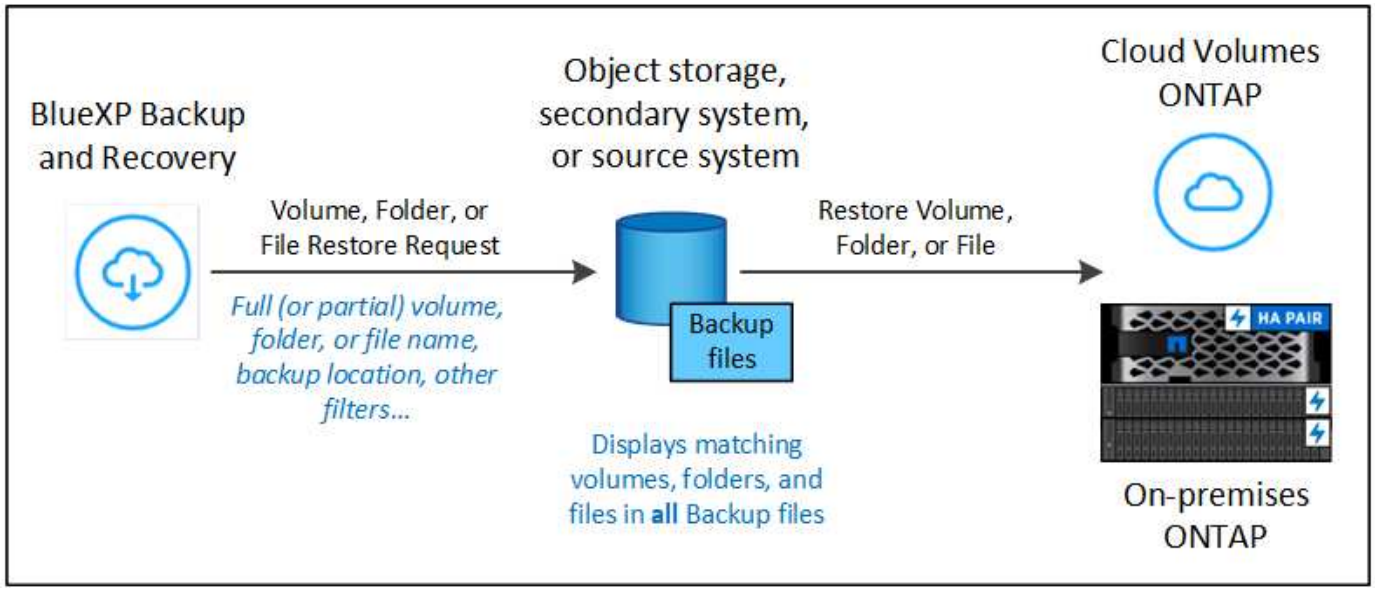
Processo di ricerca e ripristino

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:

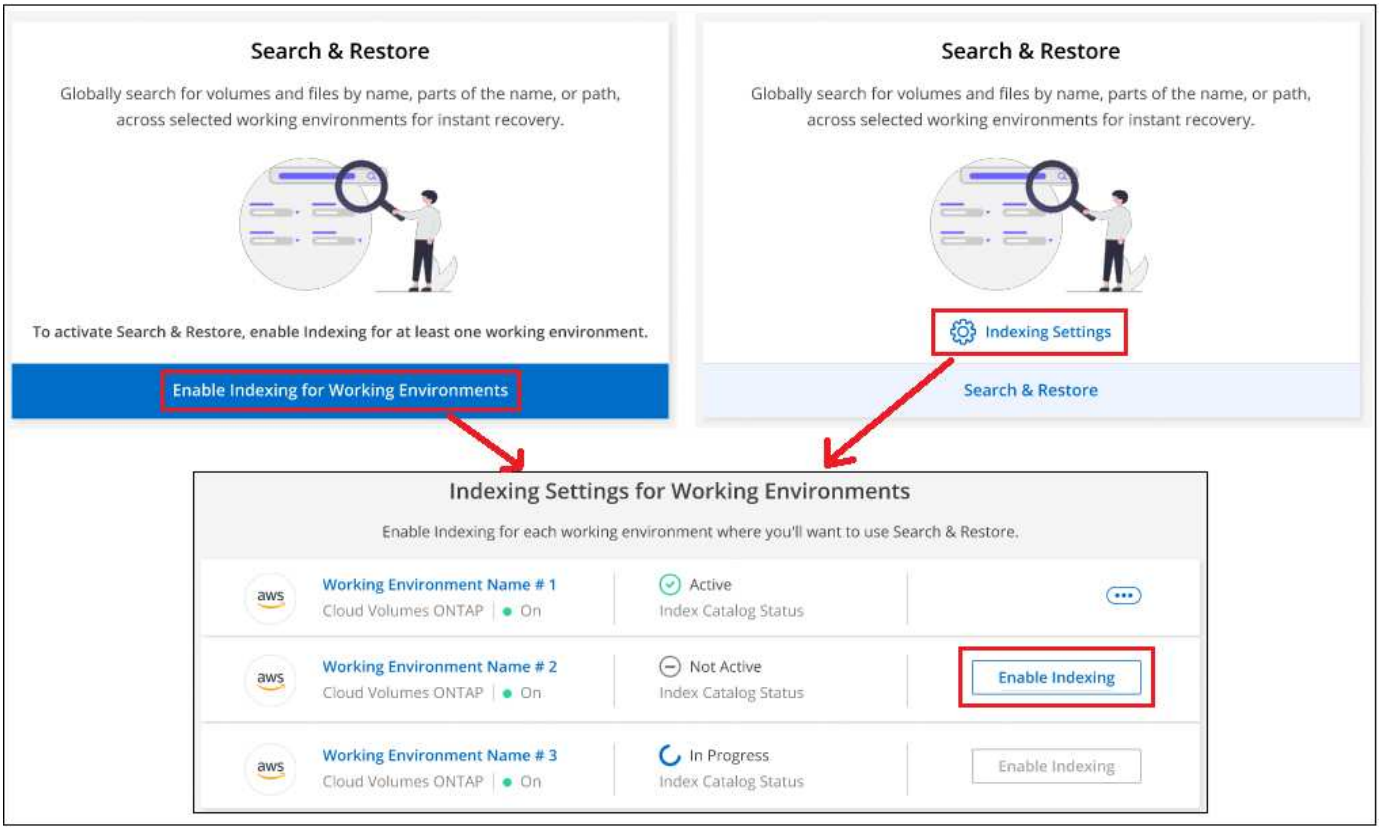
- Per i backup memorizzati in AWS, fornisce un nuovo bucket S3 e il "Servizio di query interattiva Amazon Athena" e. "Servizio di integrazione dei dati senza server AWS Glue".
- Per i backup memorizzati in Azure, il sistema fornisce un'area di lavoro di Azure Synapse e un file system di Data Lake come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

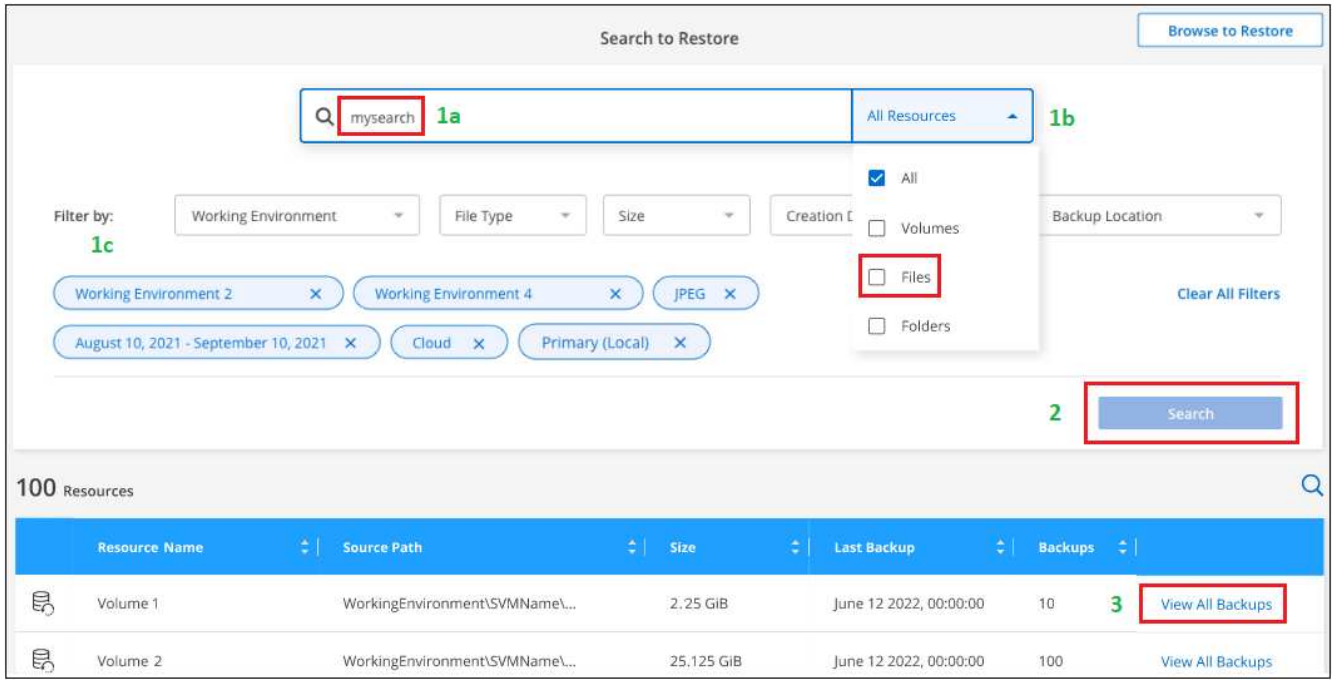
Ripristinare volumi, cartelle e file utilizzando Search & Restore

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.

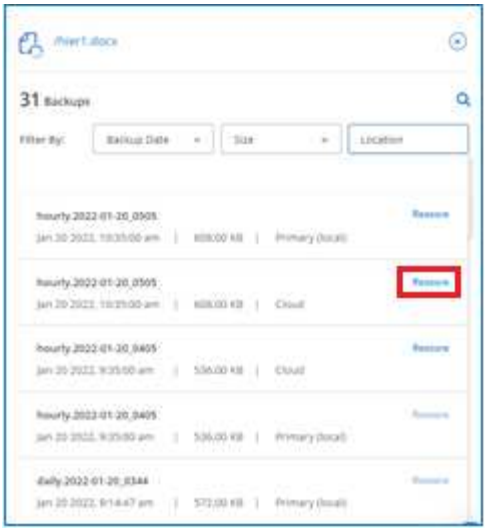
Fasi

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.