Proteggere i carichi di lavoro del volume ONTAP

NetApp Backup and Recovery

NetApp
November 26, 2025

Sommario

Proteggere i carichi di lavoro del volume ONTAP

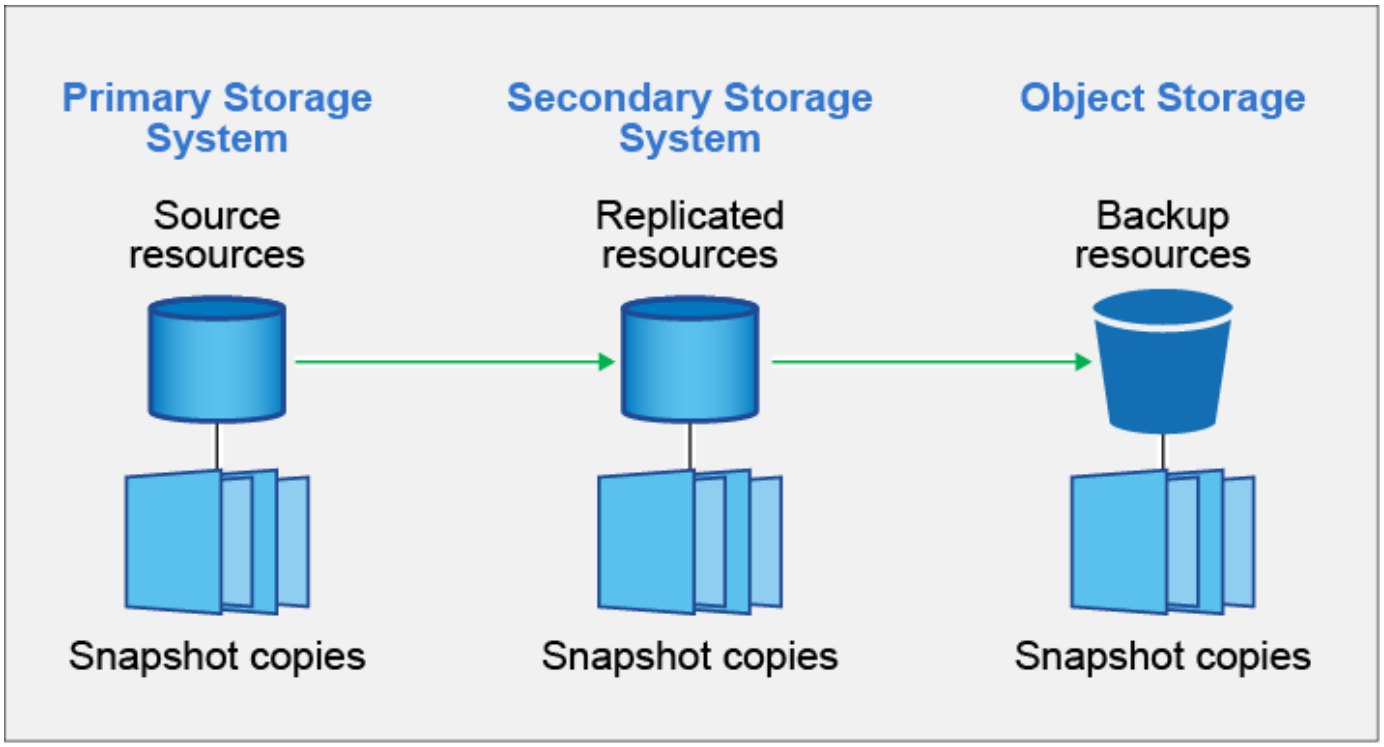
Proteggi i dati del tuo volume ONTAP utilizzando NetApp Backup and Recovery

NetApp Backup and Recovery offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del volume ONTAP . È possibile implementare una strategia 3-2-1 in cui si hanno 3 copie dei dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Dopo l'attivazione, il backup e il ripristino creano backup incrementali a livello di blocco, permanenti, che vengono archiviati su un altro cluster ONTAP e nell'archiviazione di oggetti nel cloud. Oltre al volume sorgente, avrai:

- Istantanea del volume sul sistema sorgente
- Volume replicato su un sistema di archiviazione diverso
- Backup del volume nell'archiviazione degli oggetti



NetApp Backup and Recovery sfrutta la tecnologia di replicazione dei dati SnapMirror di NetApp per garantire che tutti i backup siano completamente sincronizzati creando snapshot e trasferendoli nelle posizioni di backup.

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

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- L'utilizzo di diversi tipi di supporto aiuta a recuperare i dati se un tipo non funziona.
- È possibile ripristinare rapidamente dalla copia in loco e utilizzare le copie fuori sede se la copia in loco è compromessa.

Se necessario, è possibile ripristinare un intero *volume*, una *cartella* o uno o più *file* da una qualsiasi delle copie di backup sullo stesso sistema o su un sistema diverso.

Caratteristiche

Caratteristiche di replicazione:

- Replicare i dati tra i sistemi di archiviazione ONTAP per supportare il backup e il ripristino di emergenza.
- Garantisci l'affidabilità del tuo ambiente DR con elevata disponibilità.
- Crittografia ONTAP nativa in volo impostata tramite chiave pre-condivisa (PSK) tra i due sistemi.
- I dati copiati sono immutabili finché non vengono resi scrivibili e pronti per l'uso.
- La replicazione è auto-riparante in caso di errore di trasferimento.
- Rispetto a "NetApp Replication" , la replica in NetApp Backup and Recovery include le seguenti funzionalità:
  - Replicare più volumi FlexVol contemporaneamente su un sistema secondario.
  - Ripristina un volume replicato sul sistema di origine o su un sistema diverso tramite l'interfaccia utente.

Vedere"Limitazioni di replica per i volumi ONTAP" per un elenco delle funzionalità di replica non disponibili con NetApp Backup and Recovery per volumi ONTAP .

Funzionalità di backup su oggetto:

- Esegui il backup di copie indipendenti dei tuoi volumi di dati su un archivio di oggetti a basso costo.
- Applicare un singolo criterio di backup a tutti i volumi in un cluster oppure assegnare criteri di backup diversi ai volumi che hanno obiettivi di punto di ripristino univoci.
- Creare una policy di backup da applicare a tutti i volumi futuri creati nel cluster.
- Crea 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 possibili attacchi ransomware e rimuovi/sostituisci automaticamente i backup infetti.
- Per risparmiare sui costi, archivia i file di backup più vecchi.
- Eliminare la relazione di backup in modo da poter archiviare i volumi di origine non necessari, conservando al contempo i backup dei volumi.
- Esegui il backup da cloud a cloud e da sistemi on-premise a cloud pubblici o privati.
- I dati di backup sono protetti tramite crittografia AES a 256 bit a riposo e connessioni HTTPS TLS 1.2 in transito.
- Utilizza le tue chiavi gestite dal cliente per la crittografia dei dati anziché utilizzare le chiavi di crittografia predefinite del tuo provider cloud.
- Supporto per un massimo di 4.000 backup di un singolo volume.

Ripristina le funzionalità:

- Ripristina i dati da un punto specifico nel tempo da snapshot locali, volumi replicati o volumi sottoposti a backup nell'archiviazione di oggetti.
- Ripristina un volume, una cartella o singoli file nel sistema di origine o in un sistema diverso.
- Ripristinare i dati su un sistema utilizzando un abbonamento/account diverso o che si trova in una regione diversa.
- Esegue un *ripristino rapido* di un volume da un archivio cloud a un sistema Cloud Volumes ONTAP o a un sistema locale; perfetto per situazioni di disaster recovery in cui è necessario fornire l'accesso a un volume il prima possibile.
- Ripristina i dati a livello di blocco, posizionandoli direttamente nella posizione specificata, preservando al contempo gli ACL originali.
- Sfoglia e cerca nei cataloghi dei file per selezionare facilmente singole cartelle e file per il ripristino di singoli file.

Sistemi supportati per operazioni di backup e ripristino

NetApp Backup and Recovery supporta i sistemi ONTAP e i provider di cloud pubblici e privati.

Regioni supportate

NetApp Backup and Recovery è supportato con Cloud Volumes ONTAP in molte regioni di Amazon Web Services, Microsoft Azure e Google Cloud.

"Scopri di più utilizzando la mappa delle regioni globali"

Destinazioni di backup supportate

NetApp Backup and Recovery consente di eseguire il backup di volumi ONTAP dai seguenti sistemi di origine ai seguenti sistemi secondari e storage di oggetti nei provider di cloud pubblici e privati. Gli snapshot risiedono sul sistema di origine.

Sistema sorgente	Sistema secondario (Replicazione)	Archivio oggetti di destinazione (backup) ifdef::aws[]
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Amazon S3 endif::aws[] ifdef::azure[]
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Blob di Azure endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP in Google	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	Google Cloud Storage endif::gcp[]
Sistema ONTAP in sede	Cloud Volumes ONTAP Sistema ONTAP locale	ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Blob di Azure endif::azure[] ifdef::gcp[] Google Cloud Storage endif::gcp[] NetApp StorageGRID ONTAP S3

Destinazioni di ripristino supportate

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un sistema secondario (un volume replicato) o in un archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono nel sistema di origine e possono essere ripristinati solo sullo stesso sistema.

Posizione del file di backup		Sistema di destinazione
Archivio oggetti (backup)	**Sistema secondario (replicazione)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes ONTAP nel sistema ONTAP locale AWS endif::aws[] ifdef::azure[]
Blob azzurro	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure endif::azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP endif::gcp[]
NetApp StorageGRID	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede
ONTAP S3	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede

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

Volumi supportati

NetApp Backup and Recovery supporta i seguenti tipi di volumi:

- Volumi di lettura-scrittura FlexVol
- Volumi FlexGroup (richiede ONTAP 9.12.1 o versione successiva)
- Volumi SnapLock Enterprise (richiede ONTAP 9.11.1 o versione successiva)
- SnapLock Compliance per volumi on-premise (richiede ONTAP 9.14 o versione successiva)
- Volumi di destinazione della protezione dati (DP) SnapMirror

NetApp Backup and Recovery non supporta i backup dei volumi FlexCache .

Vedi le sezioni su"Limitazioni di backup e ripristino per i volumi ONTAP" per ulteriori requisiti e limitazioni.

Costo

L'utilizzo di NetApp Backup and Recovery con i sistemi ONTAP comporta due tipi di costi: costi delle risorse e costi dei servizi. Entrambi gli addebiti riguardano la parte di backup dell'oggetto del servizio.

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

Costi delle risorse

I costi delle risorse vengono pagati al provider cloud per la capacità di archiviazione degli oggetti e per la scrittura e la lettura dei file di backup sul cloud.

- Per il backup su storage di oggetti, paghi al tuo provider cloud i costi di storage di oggetti.

Poiché NetApp Backup and Recovery preserva l'efficienza di archiviazione del volume di origine, si pagano al provider cloud i costi di archiviazione degli oggetti per i dati *dopo* le efficienze ONTAP (per la quantità minore di dati dopo l'applicazione della deduplicazione e della compressione).

- Per ripristinare i dati tramite Search & Restore, alcune risorse vengono fornite dal tuo provider cloud e vi è un costo per TiB associato alla quantità di dati scansionati dalle tue richieste di ricerca. (Queste risorse non sono necessarie per Sfoglia e ripristina.)
  - In AWS, "Amazzone Atena" E "AWS Glue" le risorse vengono distribuite in un nuovo bucket S3.
  - In Azure, un "Area di lavoro di Azure Synapse" E "Archiviazione di Azure Data Lake" sono predisposti nel tuo account di archiviazione per archiviare e analizzare i tuoi dati.
- In Google, viene distribuito un nuovo bucket e il "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 che è stato spostato in un archivio di oggetti, il provider cloud applicherà una tariffa aggiuntiva per il recupero per GiB e una tariffa per richiesta.
- Se intendi analizzare un file di backup alla ricerca di ransomware durante il processo di ripristino dei dati del volume (se hai abilitato DataLock e Ransomware Resilience per i tuoi backup cloud), dovrai sostenere anche costi di uscita aggiuntivi dal tuo provider cloud.

Spese di servizio

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

Esistono tre modi per pagare il servizio Backup. La prima opzione è quella di abbonarsi al tuo provider cloud, che ti consente di pagare mensilmente. La seconda opzione è quella di stipulare un contratto annuale. La terza opzione è quella di acquistare le licenze direttamente da NetApp.

Licenza

NetApp Backup and Recovery è disponibile con i seguenti modelli di consumo:

- **BYOL**: licenza acquistata da NetApp che può essere utilizzata con qualsiasi provider cloud.
- **PAYGO**: un abbonamento orario dal marketplace del tuo provider cloud.
- **Annuale**: un contratto annuale dal marketplace del tuo provider cloud.

Una licenza di backup è richiesta solo per il backup e il ripristino da un archivio di oggetti. La creazione di snapshot e volumi replicati non richiede una licenza.

Porta la tua patente

BYOL è basato sulla durata (1, 2 o 3 anni) e sulla capacità, con incrementi di 1 TiB. Si paga 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 dovrai inserire nella NetApp Console per abilitare il servizio. Una volta raggiunto uno dei due limiti, sarà necessario rinnovare la licenza. La licenza Backup BYOL si applica a tutti i sistemi sorgente associati all'organizzazione o all'account NetApp Console .

"Scopri come gestire le tue licenze BYOL".

Abbonamento a consumo

NetApp Backup and Recovery offre licenze basate sul consumo con un modello di pagamento a consumo. Dopo aver sottoscritto l'abbonamento tramite il marketplace del tuo provider cloud, paghi per GiB per i dati sottoposti a backup, senza alcun pagamento anticipato. La fatturazione avviene tramite la bolletta mensile del tuo provider cloud.

"Scopri come impostare un abbonamento a consumo".

Tieni presente che è disponibile una prova gratuita di 30 giorni quando ti registri inizialmente con un abbonamento PAYGO.

Contratto annuale

Quando utilizzi AWS, sono disponibili due contratti annuali della durata di 1, 2 o 3 anni:

- Un piano "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.
- Un piano "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Sono inclusi backup illimitati per i Cloud Volumes ONTAP addebitati su questa licenza (la capacità di backup non viene conteggiata sulla licenza).

Quando si utilizza Azure, sono disponibili due contratti annuali della durata di 1, 2 o 3 anni:

- Un piano "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.
- Un piano "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Sono inclusi backup illimitati per i Cloud Volumes ONTAP addebitati su questa licenza (la capacità di backup non viene conteggiata sulla licenza).

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

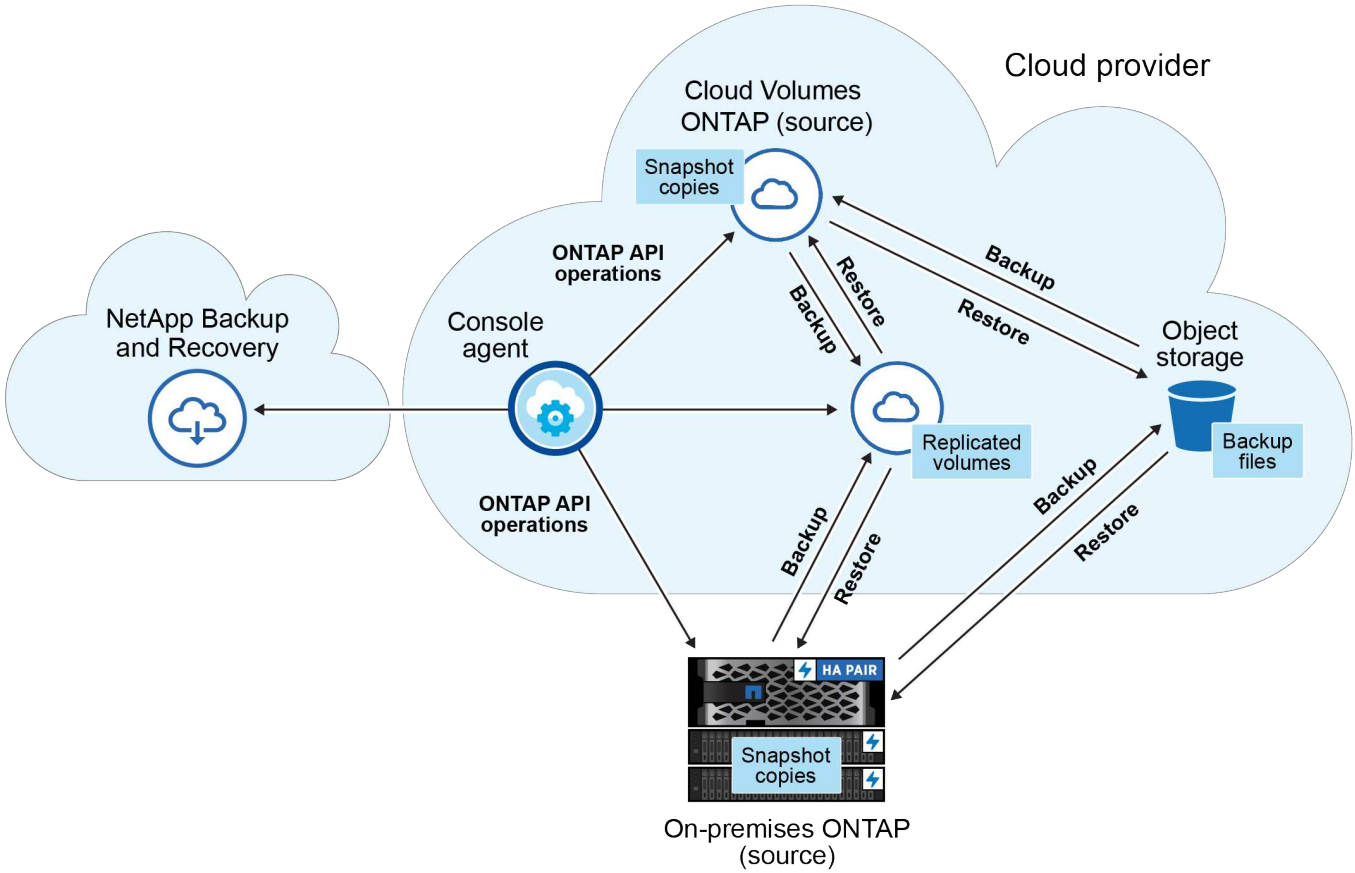
"Scopri come impostare contratti annuali".

Come funziona NetApp Backup and Recovery

Quando si abilita NetApp Backup and Recovery su un sistema Cloud Volumes ONTAP o ONTAP locale, il servizio esegue un backup completo dei dati. Dopo il backup iniziale, tutti i backup aggiuntivi sono incrementali, ovvero vengono sottoposti a backup solo i blocchi modificati e quelli nuovi. In questo modo il traffico di rete viene ridotto al minimo. Il backup su storage di oggetti è costruito sulla base di "Tecnologia NetApp SnapMirror Cloud" .

> Qualsiasi azione intrapresa direttamente dall'ambiente del tuo provider cloud per gestire o modificare i file di backup cloud potrebbe danneggiare i file e dare luogo a una configurazione non supportata.

L'immagine seguente mostra la relazione tra ciascun componente:



Questo diagramma mostra i volumi replicati su un sistema Cloud Volumes ONTAP , ma i volumi potrebbero essere replicati anche su un sistema ONTAP locale.

Dove risiedono i backup

I backup risiedono in posizioni diverse in base al tipo di backup:

- Gli *snapshot* risiedono sul volume di origine nel sistema di origine.
- I *volumi replicati* risiedono sul sistema di archiviazione secondario: un sistema Cloud Volumes ONTAP o ONTAP locale.
- Le *copie di backup* vengono archiviate in un archivio oggetti creato dalla Console nel tuo account cloud. Esiste un archivio oggetti per cluster/sistema e la Console assegna a tale archivio il seguente nome: "netapp-backup-clusteruuid". Assicurarsi di non eliminare questo archivio oggetti.

+ ** In AWS, la Console abilita la "Funzionalità di blocco dell'accesso pubblico di Amazon S3" sul bucket S3.

+ ** In Azure, la console utilizza un gruppo di risorse nuovo o esistente con un account di archiviazione per il contenitore BLOB. La console "blocca l'accesso pubblico ai dati del tuo blob" per impostazione predefinita.

+ ** In GCP, la Console utilizza un progetto nuovo o esistente con un account di archiviazione per il bucket Google Cloud Storage.

+ ** In StorageGRID, la console utilizza un account tenant esistente per il bucket S3.

+ ** In ONTAP S3, la console utilizza un account utente esistente per il bucket S3.

Se in futuro si desidera modificare l'archivio oggetti di destinazione per un cluster, sarà necessario"annullare la

registrazione NetApp Backup and Recovery per il sistema" e quindi abilitare NetApp Backup and Recovery utilizzando le informazioni del nuovo provider cloud.

Pianificazione di backup e impostazioni di conservazione personalizzabili

Quando si abilita NetApp Backup and Recovery per un sistema, tutti i volumi inizialmente selezionati vengono sottoposti a backup utilizzando i criteri selezionati. È possibile selezionare policy separate per snapshot, volumi replicati e file di backup. Se si desidera assegnare policy di backup diverse a determinati volumi con obiettivi di punto di ripristino (RPO) diversi, è possibile creare policy aggiuntive per quel cluster e assegnarle agli altri volumi dopo l'attivazione di NetApp Backup and Recovery .

È possibile scegliere una combinazione di backup orari, giornalieri, settimanali, mensili e annuali di tutti i volumi. Per il backup dell'oggetto è anche possibile selezionare una delle policy definite dal sistema che prevedono backup e conservazione per 3 mesi, 1 anno e 7 anni. Anche i criteri di protezione del backup creati sul cluster tramite ONTAP System Manager o ONTAP CLI verranno visualizzati come selezioni. Sono incluse le policy create 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 non vengono trovate etichette corrispondenti, non verrà creato alcun file di backup. Ad esempio, se si desidera creare volumi replicati e file di backup "settimanali", è necessario utilizzare un criterio Snapshot che crei snapshot "settimanali".

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

Il periodo di conservazione per i backup dei volumi di protezione dei dati è lo stesso definito nella relazione SnapMirror di origine. Se lo desideri, puoi modificarlo utilizzando l'API.

Impostazioni di protezione dei file di backup

Se il tuo cluster utilizza ONTAP 9.11.1 o versione successiva, puoi proteggere i tuoi backup nell'archiviazione degli oggetti da eliminazioni e attacchi ransomware. Ogni policy di backup prevede una sezione per *DataLock e Ransomware Resilience* 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.
- La *protezione ransomware* analizza i file di backup per cercare prove di un attacco ransomware quando viene creato un file di backup e quando i dati di un file di backup vengono ripristinati.

Le scansioni di protezione anti-ransomware pianificate sono abilitate per impostazione predefinita. L'impostazione predefinita per la frequenza di scansione è 7 giorni. La scansione avviene solo sull'ultimo snapshot. Per ridurre i costi, è possibile disattivare le scansioni pianificate. È possibile abilitare o disabilitare le scansioni ransomware pianificate sull'ultimo snapshot utilizzando l'opzione nella pagina Impostazioni avanzate. Se si attiva questa opzione, per impostazione predefinita le scansioni vengono eseguite settimanalmente. È possibile modificare la programmazione in giorni o settimane oppure disattivarla, risparmiando sui costi.

Il periodo di conservazione del backup è lo stesso del periodo di conservazione del backup programmato, più un buffer massimo di 31 giorni. Ad esempio, i backup *settimanali* con *5* copie conservate bloccheranno ogni file di backup per 5 settimane. I backup *mensili* con *6* copie conservate bloccheranno 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. Nelle versioni future verranno aggiunte altre destinazioni di provider di archiviazione.

Per maggiori dettagli fare riferimento a questa informativa:

- "Come funzionano la protezione da DataLock e Ransomware".
- "Come aggiornare le opzioni di protezione Ransomware nella pagina Impostazioni avanzate".

DataLock non può essere abilitato se si suddividono i backup in livelli di archiviazione.

Archiviazione per vecchi file di backup

Quando si utilizza un determinato tipo di archiviazione cloud, è possibile spostare i file di backup più vecchi in una classe di archiviazione/livello di accesso meno costoso dopo un certo numero di giorni. Puoi anche scegliere di inviare immediatamente i tuoi file di backup all'archivio, senza che vengano salvati nell'archiviazione cloud standard. Tieni presente che l'archiviazione non può essere utilizzata se hai abilitato DataLock.

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

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi in storage *S3 Glacier* o *S3 Glacier Deep Archive* nell'interfaccia utente NetApp Backup and Recovery 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 livello di accesso *Cool*.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi nell'archiviazione *Azure Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sull'archiviazione di Azure" .

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

  Se il cluster utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi in livelli di storage *Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sull'archiviazione di Google" .

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

  Se il cluster locale utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o versione successiva, è possibile archiviare i file di backup più vecchi nell'archiviazione cloud pubblica dopo un certo numero di giorni. Il supporto attuale riguarda i livelli di archiviazione AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. "Scopri di più sull'archiviazione dei file di backup da StorageGRID" .

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

Considerazioni sulla politica di tiering FabricPool

Ci sono alcune cose di cui devi essere a conoscenza quando il volume di cui stai eseguendo il backup risiede su un aggregato FabricPool e ha una politica di suddivisione in livelli assegnata diversa da `none` :

- Il primo backup di un volume FabricPool a livelli richiede la lettura di tutti i dati locali e a livelli (dall'archivio oggetti). Un'operazione di backup non "riscalda" i dati inattivi archiviati in livelli nell'archiviazione degli oggetti.

  Questa operazione potrebbe comportare un aumento una tantum dei costi di lettura dei dati dal tuo provider cloud.

  - I backup successivi sono incrementali e non hanno questo effetto.
  - Se il criterio di suddivisione in livelli viene assegnato al volume al momento della sua creazione iniziale, questo problema non verrà visualizzato.
- Considerare l'impatto dei backup prima di assegnare il `all` politica di suddivisione in livelli in base ai volumi. Poiché i dati vengono suddivisi immediatamente in livelli, NetApp Backup and Recovery leggerà i dati dal livello cloud anziché dal livello locale. Poiché le operazioni di backup simultanee condividono il collegamento di rete con l'archivio oggetti cloud, potrebbe verificarsi un calo delle prestazioni se le risorse di rete diventano sature. In questo caso, potrebbe essere opportuno configurare in modo proattivo più interfacce di rete (LIF) per ridurre questo tipo di saturazione della rete.

Pianifica il tuo percorso di protezione con NetApp Backup and Recovery

NetApp Backup and Recovery consente di creare fino a tre copie dei volumi di origine per proteggere i dati. Sono numerose le opzioni che puoi selezionare quando attivi Backup e Ripristino sui tuoi volumi, quindi dovresti rivedere le tue scelte per essere preparato.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Esamineremo le seguenti opzioni:

- Quali funzionalità di protezione utilizzerai: snapshot, volumi replicati e/o backup sul cloud
- Quale architettura di backup utilizzerai: un backup a cascata o a fan-out dei tuoi volumi
- Utilizzerai i criteri di backup predefiniti o dovrai creare criteri personalizzati?
- Desideri che il servizio crei i bucket cloud per te o desideri creare i contenitori di archiviazione degli oggetti prima di iniziare?
- Quale modalità di distribuzione dell'agente della console stai utilizzando (modalità standard, limitata o privata)

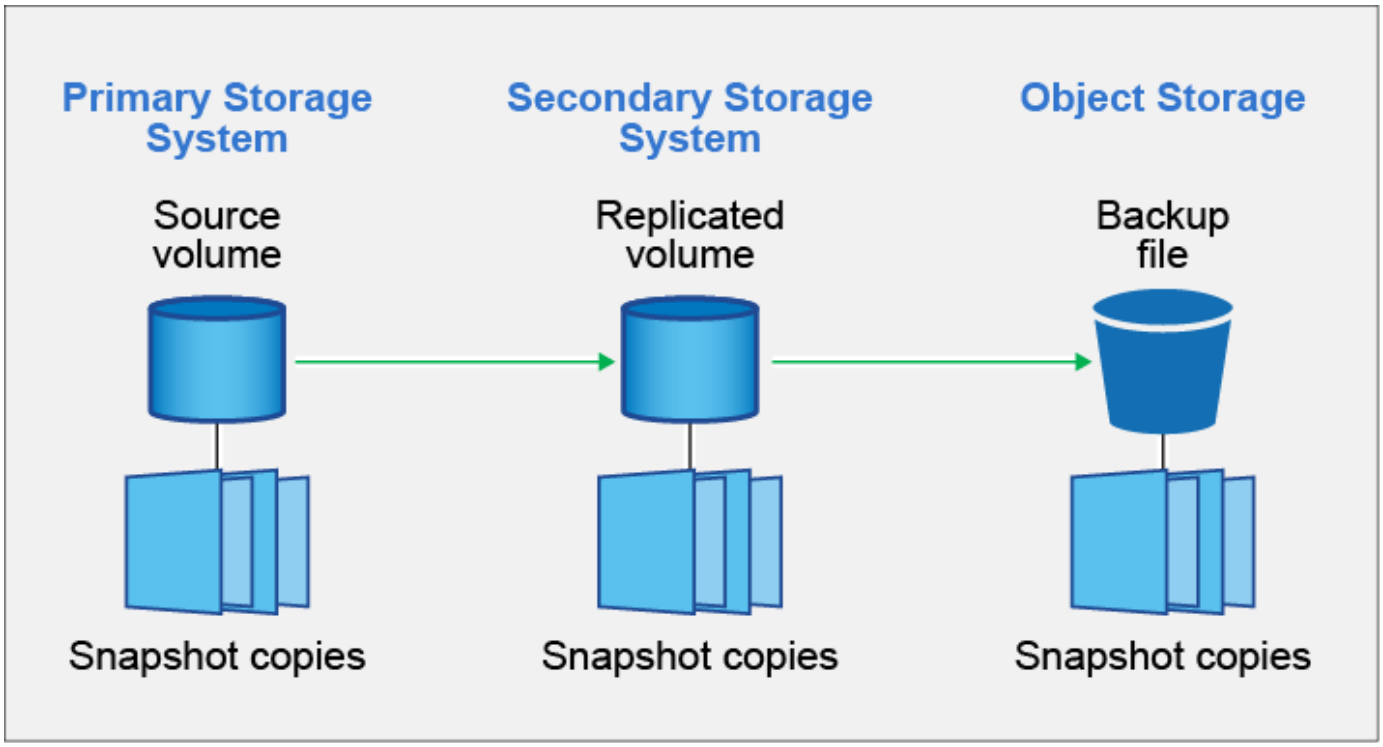
Quali funzionalità di protezione utilizzerai?

Prima di selezionare le funzionalità da utilizzare, ecco una breve spiegazione delle funzioni di ciascuna funzionalità e del tipo di protezione che offre.

Tipo di backup	Descrizione
Istantanea	Crea un'immagine di sola lettura e in un punto temporale specifico di un volume all'interno del volume di origine come snapshot. È possibile utilizzare lo snapshot per recuperare singoli file oppure per ripristinare l'intero contenuto di un volume.

Tipo di backup	Descrizione
Replicazione	Crea una copia secondaria dei dati su un altro sistema di archiviazione ONTAP e aggiorna continuamente i dati secondari. I tuoi dati saranno sempre aggiornati e disponibili ogni volta che ne avrai bisogno.
Backup su cloud	Crea backup dei tuoi dati sul cloud per proteggerli e archiviarli a lungo termine. Se necessario, è possibile ripristinare un volume, una cartella o singoli file dal backup sullo stesso sistema o su un sistema diverso.

Gli snapshot sono la base di tutti i metodi di backup e sono necessari per utilizzare il servizio di backup e ripristino. Uno snapshot è un'immagine di un volume, di sola lettura e memorizzata in un punto preciso nel tempo. L'immagine occupa uno spazio di archiviazione minimo e comporta un sovraccarico di prestazioni trascurabile, poiché registra solo le modifiche apportate ai file dall'ultima istantanea. Lo snapshot creato sul volume viene utilizzato 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 sia volumi replicati su un altro sistema di archiviazione ONTAP sia file di backup nel cloud. Oppure puoi semplicemente scegliere di creare volumi replicati o file di backup: la scelta è tua.

Riassumendo, ecco i flussi di protezione validi che puoi creare per i volumi nel tuo sistema ONTAP :

- Volume di origine → Snapshot → Volume replicato → File di backup
- Volume sorgente → Snapshot → File di backup
- Volume sorgente → Snapshot → Volume replicato

La creazione iniziale di un volume replicato o di un file di backup include una copia completa dei dati di origine: questo processo è denominato *trasferimento di base*. I trasferimenti successivi contengono solo copie differenziali dei dati di origine (lo snapshot).

Confronto tra i diversi metodi di backup

La tabella seguente mostra un confronto generalizzato dei tre metodi di backup. Sebbene lo spazio di archiviazione degli oggetti sia in genere meno costoso dell'archiviazione su disco in locale, se pensi di dover ripristinare frequentemente i dati dal cloud, le tariffe di uscita dei provider cloud possono ridurre parte dei tuoi risparmi. Dovrai stabilire con quale frequenza dovrai ripristinare i dati dai file di backup nel cloud.

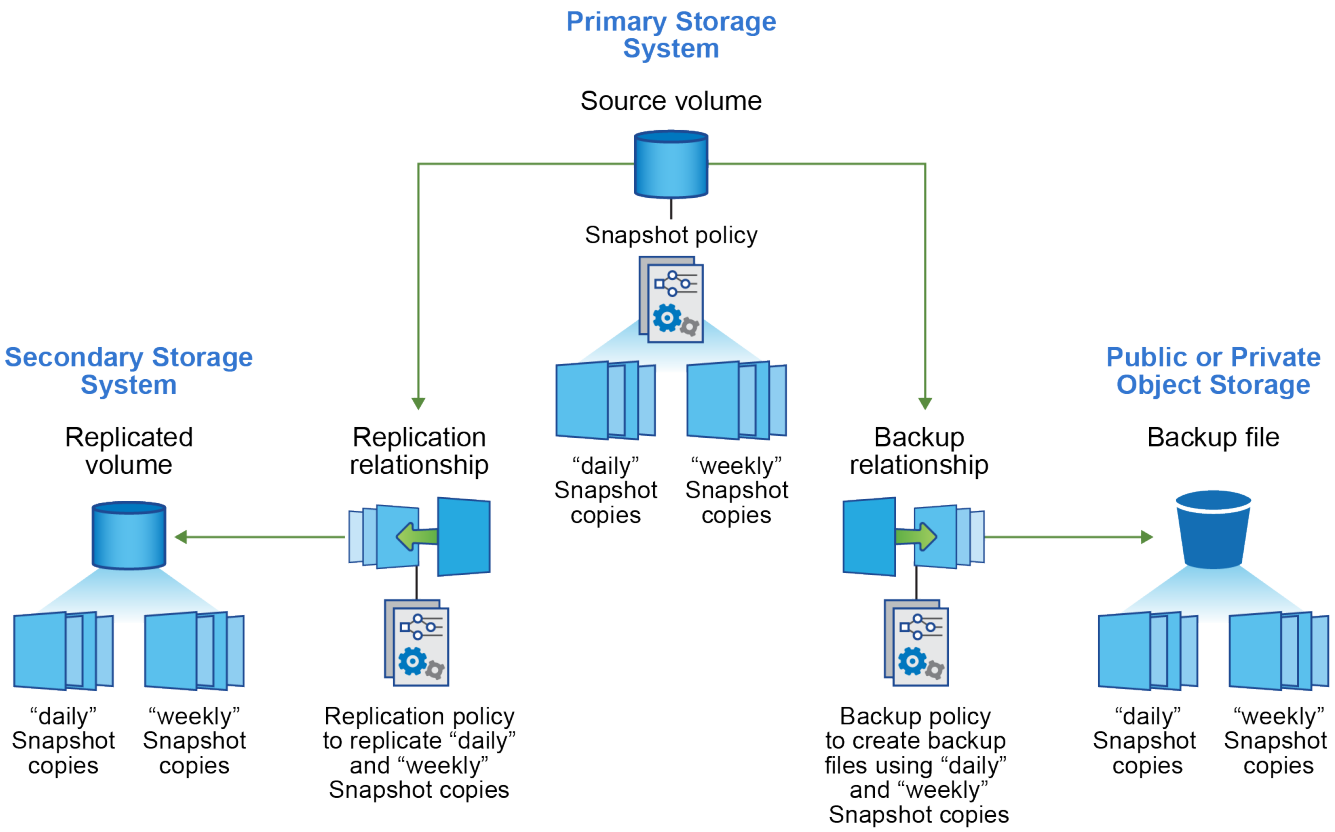
Oltre a questo criterio, l'archiviazione cloud offre opzioni di sicurezza aggiuntive se si utilizza la funzionalità DataLock e Ransomware Resilience, nonché ulteriori risparmi sui costi selezionando classi di archiviazione per i file di backup più vecchi. "Scopri di più sulla protezione DataLock e Ransomware e sulle impostazioni di archiviazione" .

Tipo di backup	Velocità di backup	Costo di backup	Ripristinare la velocità	Costo di ripristino
Istantanea	Alto	Basso (spazio su disco)	Alto	Basso
Replicazione	Medio	Mezzo (spazio su disco)	Medio	Mezzo (rete)
Backup su cloud	Basso	Basso (spazio oggetto)	Basso	Alto (commissioni del fornitore)

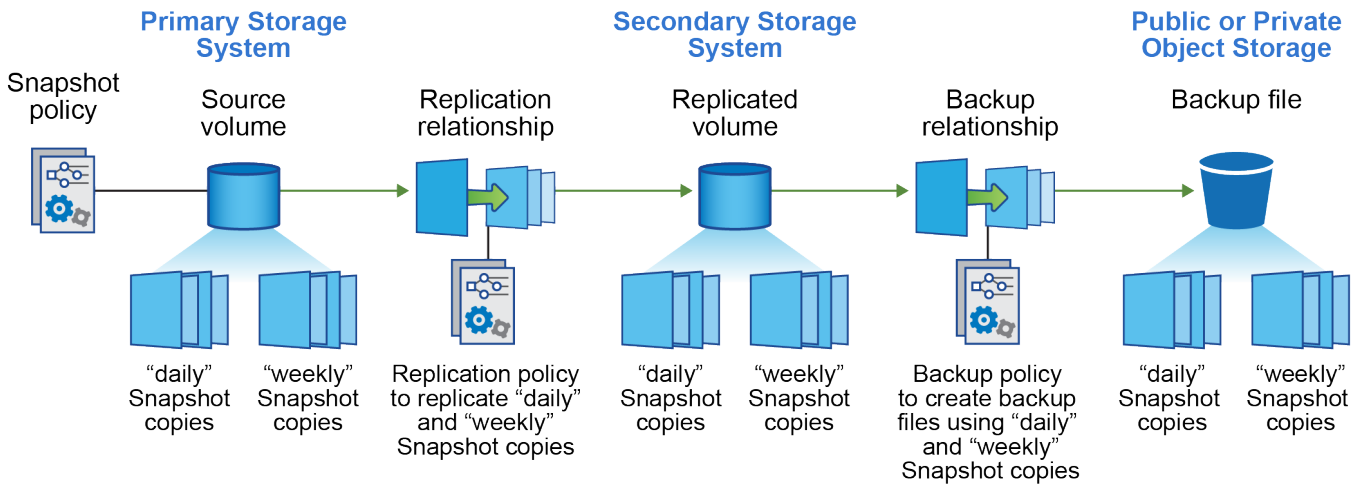
Quale architettura di backup utilizzerai?

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

Un'architettura **fan-out** trasferisce lo snapshot in modo indipendente sia al sistema di archiviazione di destinazione sia all'oggetto di backup nel cloud.



Un'architettura **a cascata** trasferisce prima lo snapshot al sistema di archiviazione di destinazione, dopodiché il sistema trasferisce la copia all'oggetto di backup nel cloud.



Confronto tra le diverse scelte architettoniche

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

Fan-out	Cascata
Piccolo impatto sulle prestazioni del sistema sorgente perché invia snapshot a 2 sistemi distinti	Minore impatto sulle prestazioni del sistema di archiviazione di origine perché invia lo snapshot una sola volta
Più facile da configurare perché tutte le policy, le reti e le configurazioni ONTAP vengono eseguite sul sistema sorgente	Richiede che alcune configurazioni di rete e ONTAP vengano eseguite anche dal sistema secondario.

Utilizzerai i criteri predefiniti per snapshot, repliche e backup?

Per creare i backup è possibile utilizzare i criteri predefiniti forniti da NetApp oppure creare criteri personalizzati. Quando si utilizza la procedura guidata di attivazione per abilitare il servizio di backup e ripristino per i volumi, è possibile selezionare tra i criteri predefiniti e qualsiasi altro criterio già esistente nel sistema (Cloud Volumes ONTAP o sistema ONTAP locale). Se si desidera utilizzare una policy diversa da quelle esistenti, è possibile crearla prima di iniziare o durante l'utilizzo della procedura guidata di attivazione.

- Il criterio di snapshot predefinito crea snapshot orari, giornalieri e settimanali, conservando 6 snapshot orari, 2 giornalieri e 2 settimanali.
- La policy di replica predefinita replica snapshot giornalieri e settimanali, conservando 7 snapshot giornalieri e 52 snapshot settimanali.
- La policy di backup predefinita replica snapshot giornalieri e settimanali, conservando 7 snapshot giornalieri e 52 settimanali.

Se si creano policy personalizzate per la replica o il backup, le etichette delle policy (ad esempio, "giornaliera" o "settimanale") devono corrispondere alle etichette presenti nelle policy snapshot, altrimenti i volumi replicati e i file di backup non verranno creati.

È possibile creare policy di archiviazione di snapshot, repliche e backup su oggetti nell'interfaccia utente NetApp Backup and Recovery . Vedi la sezione per"aggiunta di una nuova politica di backup" per i dettagli.

Oltre a utilizzare NetApp Backup and Recovery per creare policy personalizzate, è possibile utilizzare System Manager o l'interfaccia della riga di comando (CLI) ONTAP :

- "Creare un criterio di snapshot utilizzando System Manager o ONTAP CLI"
- "Creare una policy di replicazione utilizzando System Manager o ONTAP CLI"

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

Ecco alcuni esempi di comandi ONTAP CLI che potrebbero essere utili se si creano policy personalizzate. Si noti che è necessario utilizzare il vserver *admin* (VM di archiviazione) come `<vserver_name>` in questi comandi.

Descrizione della politica	Comando
Criterio di snapshot semplice	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
Backup semplice sul cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Backup su cloud con protezione DataLock e 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 classe di archiviazione	`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`
Semplice replica su un altro sistema di archiviazione	`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 il backup delle relazioni cloud è possibile utilizzare solo criteri di vault.

Dove risiedono le mie polizze?

Le policy di backup risiedono in posizioni diverse a seconda dell'architettura di backup che si intende utilizzare: Fan-out o Cascading. Le policy di replicazione e le policy di backup non sono progettate allo stesso modo perché le repliche accoppiano due sistemi di archiviazione ONTAP e il backup su oggetto utilizza un provider di archiviazione come destinazione.

- I criteri di snapshot risiedono sempre sul sistema di archiviazione primario.
- Le policy di replica risiedono sempre sul sistema di archiviazione secondario.
- I criteri di backup su oggetto vengono creati sul sistema in cui risiede il volume di origine: si tratta del cluster primario per le configurazioni fan-out e del cluster secondario per le configurazioni a cascata.

Queste differenze sono mostrate nella tabella.

Architettura	Politica di snapshot	Politica di replicazione	Politica di backup
Fan-out	Primario	Secondario	Primario
Cascata	Primario	Secondario	Secondario

Pertanto, se si prevede di creare policy personalizzate quando si utilizza l'architettura a cascata, sarà necessario creare le policy di replica e backup sugli 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 le policy di replica sul sistema secondario in cui verranno creati i volumi replicati e il backup sulle policy degli oggetti sul sistema primario.

Se si utilizzano i criteri predefiniti presenti su tutti i sistemi ONTAP , allora è tutto a posto.

Vuoi creare il tuo contenitore di archiviazione di oggetti

Quando si creano file di backup nell'archiviazione oggetti per un sistema, per impostazione predefinita il servizio di backup e ripristino crea il contenitore (bucket o account di archiviazione) per i file di backup nell'account di archiviazione oggetti configurato. Per impostazione predefinita, il bucket AWS o GCP è denominato "netapp-backup-<uuid>". L'account di archiviazione BLOB di Azure è denominato "netappbackup<uuid>".

È possibile creare autonomamente il contenitore nell'account del provider di oggetti se si desidera utilizzare un determinato prefisso o assegnare proprietà speciali. Se si desidera creare un contenitore personalizzato, è necessario crearlo prima di avviare la procedura guidata di attivazione. NetApp Backup and Recovery può utilizzare qualsiasi bucket e condividere i bucket. La procedura guidata di attivazione del backup rileverà automaticamente i contenitori forniti per l'account e le credenziali selezionati, in modo da poter selezionare quello che si desidera utilizzare.

Puoi creare il bucket dalla Console o dal tuo provider cloud.

- "Crea bucket Amazon S3 dalla console"
- "Creare account di archiviazione BLOB di Azure dalla console"
- "Crea bucket di Google Cloud Storage dalla Console"

Se si prevede di utilizzare un prefisso bucket diverso da "netapp-backup-xxxxxx", sarà necessario modificare le autorizzazioni S3 per il ruolo IAM dell'agente della console.

Impostazioni avanzate del bucket

Se intendi spostare i vecchi file di backup in un archivio o se intendi abilitare la protezione DataLock e Ransomware per bloccare i file di backup ed eseguirne la scansione alla ricerca di possibili ransomware, dovrai creare il contenitore con determinate impostazioni di configurazione:

- Al momento, l'archiviazione sui tuoi bucket è supportata nell'archiviazione AWS S3 quando utilizzi il software ONTAP 9.10.1 o versioni successive sui tuoi cluster. Per impostazione predefinita, i backup

vengono avviati nella classe di archiviazione S3 *Standard*. Assicurati di creare il bucket con le regole del ciclo di vita appropriate:

  - Spostare gli oggetti nell'intero ambito del bucket in S3 *Standard-IA* dopo 30 giorni.
  - Sposta 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 il software ONTAP 9.11.1 o versione successiva sui cluster e nello storage Azure quando si utilizza il software ONTAP 9.12.1 o versione successiva.
  - Per AWS, è necessario abilitare il blocco degli oggetti sul bucket utilizzando un periodo di conservazione di 30 giorni.
  - Per Azure, è necessario creare la classe di archiviazione con supporto di immutabilità a livello di versione.

Quale modalità di distribuzione dell'agente della console stai utilizzando?

Se stai già utilizzando la Console per gestire il tuo storage, significa che è già stato installato un agente Console. Se intendi utilizzare lo stesso agente Console con NetApp Backup and Recovery, sei a posto. Se è necessario utilizzare un agente Console diverso, sarà necessario installarlo prima di avviare l'implementazione del backup e del ripristino.

NetApp Console offre diverse modalità di distribuzione che consentono di utilizzare la console in base alle proprie esigenze aziendali e di sicurezza. La *modalità standard* sfrutta il livello SaaS della console per fornire funzionalità complete, mentre la *modalità limitata* e la *modalità privata* sono disponibili per le organizzazioni con restrizioni di connettività.

"Scopri di più sulle modalità di distribuzione NetApp Console".

Supporto per siti con connettività Internet completa

Quando NetApp Backup and Recovery viene utilizzato in un sito con connettività Internet completa (nota anche come *modalità standard* o *modalità SaaS*), è possibile creare volumi replicati su qualsiasi sistema ONTAP locale o Cloud Volumes ONTAP gestito dalla Console, nonché creare file di backup su storage di oggetti in uno qualsiasi dei provider cloud supportati. "Visualizza l'elenco completo delle destinazioni di backup supportate" .

Per un elenco delle posizioni valide degli agenti della console, fare riferimento a una delle seguenti procedure di backup per il provider cloud in cui si prevede di creare i file di backup. Esistono alcune restrizioni per cui l'agente Console deve essere installato manualmente su una macchina Linux o distribuito in uno specifico provider cloud.

- "Esegui il backup dei dati Cloud Volumes ONTAP su Amazon S3"
- "Eseguire il backup dei dati Cloud Volumes ONTAP su Azure Blob"
- "Esegui il backup dei dati Cloud Volumes ONTAP su Google Cloud"
- "Eseguire il backup dei dati ONTAP locali su Amazon S3"
- "Eseguire il backup dei dati ONTAP locali su Azure Blob"
- "Esegui il backup dei dati ONTAP locali su Google Cloud"
- "Eseguire il backup dei dati ONTAP locali su StorageGRID"
- "Eseguire il backup ONTAP in sede su ONTAP S3"

Supporto per siti con connettività Internet limitata

NetApp Backup and Recovery può essere utilizzato in un sito con connettività Internet limitata (nota anche come *modalità limitata*) per eseguire il backup dei dati del volume. In questo caso, sarà necessario distribuire l'agente Console nella regione cloud di destinazione.

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

Supporto per siti senza connettività Internet

NetApp Backup and Recovery può essere utilizzato in un sito senza connettività Internet (noto anche come *modalità privata* o *siti oscuri*) per eseguire il backup dei dati del volume. In questo caso, sarà necessario distribuire l'agente Console su un host Linux nello stesso sito.

> La modalità privata BlueXP (interfaccia BlueXP legacy) viene in genere utilizzata con ambienti locali privi di connessione Internet e con regioni cloud sicure, tra cui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. NetApp continua a supportare questi ambienti con l'interfaccia legacy BlueXP . Per la documentazione sulla modalità privata nell'interfaccia legacy BlueXP , fare riferimento a "Documentazione PDF per la modalità privata BlueXP" .

- È possibile eseguire il backup dei dati dai sistemi ONTAP locali sui sistemi NetApp StorageGRID locali. "Eseguire il backup dei dati ONTAP locali su StorageGRID" .
- È possibile eseguire il backup dei dati dai sistemi ONTAP locali in sede ai sistemi ONTAP locali in sede o ai sistemi Cloud Volumes ONTAP configurati per l'archiviazione di oggetti S3. "Eseguire il backup dei dati ONTAP locali su ONTAP S3" . ifdef::aws[]

Gestisci le policy di backup per i volumi ONTAP con NetApp Backup and Recovery

Con NetApp Backup and Recovery, puoi utilizzare le policy di backup predefinite fornite da NetApp per creare i tuoi backup oppure creare policy personalizzate. Le policy regolano la frequenza del backup, l'ora in cui viene eseguito e il numero di file di backup conservati.

> Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Quando si utilizza la procedura guidata di attivazione per abilitare il servizio di backup e ripristino per i volumi, è possibile selezionare tra i criteri predefiniti e qualsiasi altro criterio già esistente nel sistema (Cloud Volumes ONTAP o sistema ONTAP locale). Se si desidera utilizzare una policy diversa da quelle esistenti, è possibile crearla prima o durante l'utilizzo della procedura guidata di attivazione.

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

NetApp Backup and Recovery fornisce tre tipi di backup dei dati ONTAP : snapshot, repliche e backup su

storage di oggetti. Le loro policy risiedono in posizioni diverse in base all'architettura utilizzata e al tipo di backup:

Architettura	Posizione di archiviazione dei criteri di snapshot	Posizione di archiviazione della politica di replica	Backup nella posizione di archiviazione dei criteri degli oggetti
Fan-out	Primario	Secondario	Primario
Cascata	Primario	Secondario	Secondario

Crea criteri di backup utilizzando i seguenti strumenti in base al tuo ambiente, alle tue preferenze e al tipo di protezione:

- UI NetApp Console
- Interfaccia utente del gestore di sistema
- ONTAP CLI

Quando si utilizza System Manager, selezionare **Asincrono** come tipo di policy per le policy di replica e selezionare **Asincrono** e **Backup su cloud** per le policy di backup su oggetto.

Visualizza le policy per un sistema

1. Nell'interfaccia utente della console, seleziona **Volumi** > **Impostazioni di backup**.
2. Dalla pagina Impostazioni di backup, seleziona il sistema, seleziona **Azioni*** icona e seleziona ***Gestione criteri**.

   Viene visualizzata la pagina di gestione delle policy. Per impostazione predefinita, vengono visualizzati i criteri snapshot.

3. Per visualizzare altre policy presenti nel sistema, selezionare **Replication Policies** o **Backup Policies**. Se le policy esistenti possono essere utilizzate per i tuoi piani di backup, sei a posto. Se hai bisogno di una polizza con caratteristiche diverse, puoi creare nuove polizze da questa pagina.

Creare politiche

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

- Creare un criterio di snapshot prima di avviare lo snapshot
- Creare una politica di replicazione prima di avviare la replica
- Creare una policy di backup su storage di oggetti prima di avviare il backup

Creare un criterio di snapshot prima di avviare lo snapshot

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

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

Passi

1. Nell'interfaccia utente della console, seleziona **Volumi** > **Impostazioni di backup**.
2. Dalla pagina Impostazioni di backup, seleziona il sistema, seleziona **Azioni*** **icona e seleziona *Gestione criteri**.

   Viene visualizzata la pagina di gestione delle policy.
3. Nella pagina Criteri, seleziona **Crea criterio** > **Crea criterio Snapshot**.
4. Specificare il nome della policy.
5. Selezionare la pianificazione o le pianificazioni degli snapshot. Puoi avere un massimo di 5 etichette. Oppure crea un programma.
6. Se scegli di creare una pianificazione:
   a. Seleziona la frequenza: oraria, giornaliera, settimanale, mensile o annuale.
   b. Specificare le etichette degli snapshot che indicano la pianificazione e la conservazione.
   c. Inserisci quando e con quale frequenza verrà scattata l'istantanea.
   d. Conservazione: immettere il numero di snapshot da conservare.
7. Seleziona **Crea**.

Esempio di policy snapshot utilizzando l'architettura a cascata

Questo esempio crea un criterio snapshot con due cluster:

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

Creare una politica di replicazione prima di avviare la replica

La strategia 3-2-1 potrebbe includere la replica di un volume su un sistema di archiviazione diverso. La politica di replica risiede sul sistema di archiviazione **secondario**.

Passi

1. Nella pagina Criteri, seleziona **Crea criterio** > **Crea criterio di replicazione**.
2. Nella sezione Dettagli policy, specificare il nome della policy.
3. Specificare le etichette SnapMirror (massimo 5) che indicano la conservazione per ciascuna etichetta.
4. Specificare il programma di trasferimento.
5. Seleziona **Crea**.

Creare una policy di backup su storage di oggetti prima di avviare il backup

La strategia 3-2-1 potrebbe includere il backup di un volume su un archivio di oggetti.

Questa policy di archiviazione risiede in diverse posizioni del sistema di archiviazione a seconda dell'architettura di backup:

- Fan-out: sistema di archiviazione primario
- A cascata: sistema di stoccaggio secondario

Passi

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

   "Scopri di più sulle impostazioni di archiviazione".

6. (Facoltativo) Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Protezione DataLock e Ransomware**.

   Se il cluster utilizza ONTAP 9.11.1 o versione successiva, è possibile scegliere di proteggere i backup dall'eliminazione configurando *DataLock* e *Protezione ransomware*.

   "Scopri di più sulle impostazioni DataLock disponibili".

7. Seleziona **Crea**.

Modifica una policy

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

La modifica della policy di backup influisce su tutti i volumi che utilizzano tale policy.

Passi

1. Nella pagina di gestione delle policy, seleziona la policy, seleziona **Azioni*** **icona e seleziona *Modifica criterio**.

   Il processo è lo stesso per le policy di replica e backup.

2. Nella pagina Modifica policy, apporta le modifiche.
3. Seleziona **Salva**.

Elimina una policy

È possibile eliminare i criteri che non sono associati ad alcun volume.

Se una policy è associata a un volume e si desidera eliminarla, è necessario prima rimuoverla dal volume.

Passi

1. Nella pagina di gestione delle policy, seleziona la policy, seleziona **Azioni*** icona e seleziona *Elimina criterio Snapshot**.
2. Seleziona **Elimina**.

Trova maggiori informazioni

Per istruzioni sulla creazione di policy tramite System Manager o ONTAP CLI, vedere quanto segue:

"Creare un criterio Snapshot utilizzando System Manager" "Creare un criterio Snapshot utilizzando ONTAP CLI" "Creare una policy di replicazione utilizzando System Manager" "Creare una policy di replicazione utilizzando ONTAP CLI" "Creare un backup per la policy di archiviazione degli oggetti utilizzando System Manager" "Creare un backup per la policy di archiviazione degli oggetti utilizzando ONTAP CLI"

Opzioni della policy di backup su oggetto in NetApp Backup and Recovery

NetApp Backup and Recovery consente di creare policy di backup con una varietà di impostazioni per i sistemi ONTAP locali e Cloud Volumes ONTAP .

Queste impostazioni dei criteri sono rilevanti solo per l'archiviazione di backup su oggetti. Nessuna di queste impostazioni influisce sui criteri di snapshot o replica.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Opzioni di pianificazione del backup

NetApp Backup and Recovery consente di creare più policy di backup con pianificazioni univoche per ciascun sistema (cluster). È possibile assegnare criteri di backup diversi ai volumi che hanno obiettivi del punto di ripristino (RPO) diversi.

Ogni criterio di backup fornisce una sezione per *Etichette e conservazione* che è possibile applicare ai file di backup. Si noti che il criterio Snapshot applicato al volume deve essere uno dei criteri riconosciuti da NetApp Backup and Recovery , altrimenti i file di backup non verranno creati.

La pianificazione è composta da due parti: l'etichetta e il valore di conservazione:

- L'**etichetta** definisce la frequenza con cui un file di backup viene creato (o aggiornato) dal volume. È possibile scegliere tra i seguenti tipi di etichette:
  - Puoi scegliere uno o più intervalli di tempo **orari**, **giornalieri**, **settimanali**, **mensili** e **annuali**.
  - È possibile selezionare una delle policy definite dal sistema che forniscono backup e conservazione per 3 mesi, 1 anno o 7 anni.
  - Se sono stati creati criteri di protezione del backup personalizzati sul cluster utilizzando ONTAP System Manager o ONTAP CLI, è possibile selezionare uno di tali criteri.
- Il valore **retention** definisce quanti file di backup per ogni etichetta (intervallo di tempo) vengono conservati. Una volta raggiunto il numero massimo di backup in una categoria o intervallo, i backup più vecchi vengono rimossi, in modo da avere sempre a disposizione i backup più recenti. In questo modo si risparmia anche sui costi di archiviazione, perché i backup obsoleti non continuano a occupare spazio nel cloud.

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

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

I backup annuali vengono eliminati automaticamente dal sistema di origine dopo essere stati trasferiti nell'archiviazione degli oggetti. Questo comportamento predefinito può essere modificato nella pagina Impostazioni avanzate del sistema.

Opzioni di protezione DataLock e Ransomware

NetApp Backup and Recovery fornisce supporto per la protezione da DataLock e Ransomware per i backup dei volumi. Queste funzionalità consentono di bloccare i file di backup e di analizzarli per rilevare eventuali ransomware presenti sui file di backup. Si tratta di un'impostazione facoltativa che puoi definire nei tuoi criteri di backup quando desideri una protezione extra per i backup dei volumi di un cluster.

Entrambe queste funzionalità proteggono i tuoi file di backup, così avrai sempre a disposizione un file di backup valido da cui recuperare i dati in caso di tentativo di attacco ransomware ai tuoi backup. È utile anche per soddisfare determinati requisiti normativi in base ai quali i backup devono essere bloccati e conservati per un determinato periodo di tempo. Quando l'opzione DataLock and Ransomware Resilience è abilitata, il bucket cloud fornito come parte dell'attivazione di NetApp Backup and Recovery avrà il blocco degli oggetti e il controllo delle versioni degli oggetti abilitati.

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

- Se si prevede di utilizzare la protezione DataLock e Ransomware, è possibile abilitarla durante la creazione del primo criterio di backup e l'attivazione NetApp Backup and Recovery per quel cluster. Successivamente potrai abilitare o disabilitare la scansione ransomware utilizzando le impostazioni avanzate NetApp Backup and Recovery .
- Quando la Console esegue la scansione di un file di backup alla ricerca di ransomware durante il ripristino dei dati del volume, verranno addebitati costi di uscita aggiuntivi al provider cloud per accedere al contenuto del file di backup.

Che cos'è DataLock

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

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

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

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

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

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

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

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

Ecco alcuni esempi:

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

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

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

Abilita la protezione DataLock e Ransomware

È possibile abilitare la protezione DataLock e Ransomware quando si crea un criterio. Non è possibile abilitare, modificare o disabilitare questa opzione dopo aver creato il criterio.

1. Quando si crea un criterio, espandere la sezione **DataLock e Resilienza Ransomware**.
2. Scegli una delle seguenti opzioni:
   - **Nessuno**: la protezione DataLock e la resilienza al ransomware sono disabilitate.
   - **Sbloccato**: la protezione DataLock e la resilienza al ransomware sono abilitate. Gli utenti con autorizzazioni specifiche possono sovrascrivere o eliminare i file di backup protetti durante il periodo di

conservazione.

- **Bloccato**: la protezione DataLock e la resilienza al ransomware sono abilitate. Nessun utente può sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione. Ciò soddisfa pienamente la conformità normativa.

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

Che cos'è la protezione dal ransomware

La protezione ransomware analizza i file di backup per cercare prove di un attacco ransomware. Il rilevamento degli attacchi ransomware viene eseguito tramite un confronto di checksum. Se in un nuovo file di backup viene identificato un potenziale ransomware rispetto al file di backup precedente, il file di backup più recente viene sostituito dal file di backup più recente che non mostra alcun segno di attacco ransomware. (Il file identificato come vittima di un attacco ransomware viene eliminato 1 giorno dopo essere stato sostituito.)

Le scansioni vengono eseguite nelle seguenti situazioni:

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

Come funziona il processo di recupero?

Quando viene rilevato un attacco ransomware, il servizio utilizza l'API REST Integrity Checker dell'agente Active Data Console per avviare il processo di ripristino. La versione più vecchia degli oggetti dati è la fonte della verità e viene trasformata nella versione corrente come parte del processo di ripristino.

Vediamo come funziona:

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

Sistemi supportati e provider di archiviazione di oggetti

È possibile abilitare la protezione DataLock e Ransomware sui volumi ONTAP dai seguenti sistemi quando si utilizza l'archiviazione di oggetti nei seguenti provider di cloud pubblici e privati.

Sistema sorgente	Destinazione del file di backup ifdef::aws[]
Cloud Volumes ONTAP in AWS	Amazon S3 endif::aws[] ifdef::azure[]

Sistema sorgente	Destinazione del file di backup ifdef::aws[]
Cloud Volumes ONTAP in Azure	Blob di Azure endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP in Google Cloud	Google Cloud endif::gcp[]
Sistema ONTAP in sede	ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Blob di Azure endif::azure[] ifdef::gcp[] Google Cloud endif::gcp[] NetApp StorageGRID

Requisiti

- Per AWS:
  - I tuoi cluster devono eseguire ONTAP 9.11.1 o versione successiva
  - L'agente della console può essere distribuito nel cloud o in sede
  - Le seguenti autorizzazioni S3 devono far parte del ruolo IAM che fornisce le autorizzazioni all'agente della console. Si trovano nella sezione "backupS3Policy" per la risorsa "arn:aws:s3:::netapp-backup-*":

Autorizzazioni AWS S3

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:EliminaOggetto
- s3:EliminaTaggingOggetto
- s3:OttieniRitenzioneOggetto
- s3:EliminaObjectVersionTagging
- s3:PutObject
- s3:OttieniOggetto
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:OttieniTaggingBucket
- s3:EliminaVersioneOggetto
- s3:ListBucketVersions
- s3:ElencoBucket
- s3:PutBucketTagging
- s3:OttieniTaggingOggetto
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:OttieniPosizioneBucket
- s3:GetObjectVersion

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

- Per Azure:
  - I tuoi cluster devono eseguire ONTAP 9.12.1 o versione successiva
  - L'agente della console può essere distribuito nel cloud o in sede
- Per Google Cloud:
  - I cluster devono eseguire ONTAP 9.17.1 o versione successiva
  - L'agente della console può essere distribuito nel cloud o in sede
- Per StorageGRID:

- I tuoi cluster devono eseguire ONTAP 9.11.1 o versione successiva
- I sistemi StorageGRID devono eseguire la versione 11.6.0.3 o successiva
- L'agente Console deve essere distribuito presso la tua 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 le autorizzazioni all'agente della console:

Autorizzazioni StorageGRID S3

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:EliminaOggetto
- s3:EliminaTaggingOggetto
- s3:OttieniRitenzioneOggetto
- s3:EliminaObjectVersionTagging
- s3:PutObject
- s3:OttieniOggetto
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:OttieniTaggingBucket
- s3:EliminaVersioneOggetto
- s3:ListBucketVersions
- s3:ElencoBucket
- s3:PutBucketTagging
- s3:OttieniTaggingOggetto
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:OttieniPosizioneBucket
- s3:GetObjectVersion

Restrizioni

- La funzionalità di protezione DataLock e Ransomware non è disponibile se è stata configurata l'archiviazione nel criterio di backup.
- L'opzione DataLock selezionata durante l'attivazione NetApp Backup and Recovery 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 abilita 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 ai backup di nuovi volumi utilizzando un criterio di backup con protezione DataLock e Ransomware abilitata. Successivamente potrai abilitare o disabilitare queste funzionalità utilizzando l'opzione Impostazioni avanzate.
- I volumi FlexGroup possono utilizzare la protezione DataLock e Ransomware solo se si utilizza ONTAP 9.13.1 o versione successiva.

Suggerimenti su come ridurre i costi di DataLock

È possibile abilitare o disabilitare la funzionalità Ransomware Scan mantenendo attiva la funzionalità DataLock. Per evitare costi aggiuntivi, puoi disattivare le scansioni ransomware pianificate. Ciò consente di personalizzare le impostazioni di sicurezza ed evitare di sostenere costi con il provider cloud.

Anche se le scansioni ransomware pianificate sono disattivate, è comunque possibile eseguire scansioni su richiesta quando necessario.

Puoi scegliere diversi livelli di protezione:

- **DataLock *senza* scansioni ransomware**: fornisce protezione per i dati di backup nell'archiviazione di destinazione che può essere in modalità Governance o Compliance.
  - **Modalità di governance**: offre agli amministratori la flessibilità di sovrascrivere o eliminare i dati protetti.
  - **Modalità di conformità**: garantisce la completa indelebilità fino alla scadenza del periodo di conservazione. Ciò contribuisce a soddisfare i più rigorosi requisiti di sicurezza dei dati degli ambienti altamente regolamentati. I dati non possono essere sovrascritti o modificati durante il loro ciclo di vita, garantendo il massimo livello di protezione per le copie di backup.

    Microsoft Azure utilizza invece una modalità di blocco e sblocco.

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

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

Inoltre, è possibile ottenere preventivi per i costi associati a DataLock visitando il "Calcolatore del costo totale di proprietà (TCO) NetApp Backup and Recovery" .

Opzioni di archiviazione

Quando si utilizza AWS, Azure o Google Cloud Storage, è possibile spostare i file di backup più vecchi in una classe di archiviazione o in un livello di accesso meno costosi dopo un certo numero di giorni. Puoi anche scegliere di inviare immediatamente i tuoi file di backup all'archivio, senza che vengano salvati nell'archiviazione cloud standard. Basta inserire **0** come "Archivio dopo giorni" per inviare il file di backup direttamente all'archivio. Ciò può essere particolarmente utile per gli utenti che hanno raramente bisogno di

accedere ai dati dai backup su cloud o per gli utenti che stanno sostituendo una soluzione di backup su nastro.

I dati nei livelli di archiviazione non sono accessibili immediatamente quando necessario e comportano costi di recupero più elevati, pertanto è necessario valutare 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 all'archiviazione cloud, i blocchi di metadati vengono sempre scritti nell'archiviazione cloud standard.
- L'archiviazione non può essere utilizzata se è stato abilitato DataLock.
- Non è possibile modificare i criteri di archiviazione dopo aver selezionato **0** giorni (archiviazione immediata).

Ogni criterio di backup fornisce una sezione per i *Criteri di archiviazione* che è possibile applicare ai file di backup.

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

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

  - Se non selezioni alcun livello di archivio nella tua prima policy di backup quando attivi NetApp Backup and Recovery, *S3 Glacier* sarà la tua unica opzione di archiviazione per le policy future.
  - Se selezioni *S3 Glacier* nella tua prima policy di backup, puoi passare al livello *S3 Glacier Deep Archive* per le future policy di backup per quel cluster.
  - Se selezioni *S3 Glacier Deep Archive* nella tua prima policy di backup, quel livello sarà l'unico livello di archivio disponibile per le future policy di backup per quel cluster.
- In Azure, i backup sono associati al livello di accesso *Cool*.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile suddividere i backup più vecchi nell'archiviazione *Azure Archive*. "Scopri di più sull'archiviazione di Azure" .

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

  Se il cluster locale utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi nello storage *Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sull'archiviazione di Google" .

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

  Se il cluster locale utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o versione successiva, è possibile archiviare i file di backup più vecchi nell'archiviazione cloud pubblica.

+ ** Per AWS, è possibile suddividere i backup in livelli nello storage AWS *S3 Glacier* o *S3 Glacier Deep Archive*. "Scopri di più sullo storage di archiviazione AWS" .

+ ** Per Azure, è possibile suddividere i backup più vecchi nell'archiviazione *Azure Archive*. "Scopri di più sull'archiviazione di Azure" .

Gestisci le opzioni di archiviazione del backup su oggetto nelle impostazioni avanzate NetApp Backup and Recovery

È possibile modificare le impostazioni di archiviazione del backup su oggetto a livello di cluster definite durante l'attivazione di NetApp Backup and Recovery per ciascun sistema ONTAP utilizzando la pagina Impostazioni avanzate. È anche possibile modificare alcune impostazioni applicate come impostazioni di backup "predefinite". Ciò include la modifica della velocità di trasferimento dei backup nell'archiviazione degli oggetti, se gli snapshot storici vengono esportati come file di backup e se si abilitano o disabilitano le scansioni ransomware per un sistema.

Queste impostazioni sono disponibili solo per l'archiviazione di backup su oggetti. Nessuna di queste impostazioni influisce sulle impostazioni di snapshot o replica.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Nella pagina Impostazioni avanzate è possibile modificare le seguenti opzioni:

- Modifica della larghezza di banda di rete assegnata per caricare i backup nell'archivio oggetti utilizzando l'opzione Velocità di trasferimento massima ifdef::aws[]
- Modificare se gli snapshot storici vengono esportati come file di backup e inclusi nei file di backup di base iniziali per i volumi futuri
- Modificare se gli snapshot "annuali" vengono rimossi dal sistema sorgente
- Abilitazione o disabilitazione delle scansioni ransomware per un sistema, incluse le scansioni pianificate

Visualizza le impostazioni di backup a livello di cluster

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

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
3. Dalla pagina *Impostazioni di backup*, fare clic su••• per il sistema e selezionare **Impostazioni avanzate**.

   La pagina *Impostazioni avanzate* mostra le impostazioni correnti per quel sistema.

4. Espandi l'opzione e apporta la modifica.

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

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

Modifica la larghezza di banda di rete disponibile per caricare i backup nell'archiviazione degli oggetti

Quando si attiva NetApp Backup and Recovery per un sistema, per impostazione predefinita ONTAP può

utilizzare una quantità illimitata di larghezza di banda per trasferire i dati di backup dai volumi del sistema all'archiviazione degli oggetti. Se noti che il traffico di backup influisce sui normali carichi di lavoro degli utenti, puoi limitare la quantità di larghezza di banda di rete utilizzata durante il trasferimento utilizzando l'opzione Velocità di trasferimento massima nella pagina Impostazioni avanzate.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su••• per il sistema e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Velocità di trasferimento massima**.
4. Scegli 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 vi è alcun limite.
6. Selezionare **Applica**.

Questa impostazione non influisce sulla larghezza di banda assegnata ad altre relazioni di replicazione che potrebbero essere configurate per i volumi nel sistema.

Modifica se gli snapshot storici vengono esportati come file di backup

Se sono presenti snapshot locali per volumi che corrispondono all'etichetta di pianificazione del backup utilizzata in questo sistema (ad esempio, giornaliera, settimanale, ecc.), è possibile esportare tali snapshot storici nell'archiviazione degli oggetti come file di backup. Ciò consente di inizializzare i backup nel cloud spostando gli snapshot più vecchi nella copia di backup di base.

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

Passi

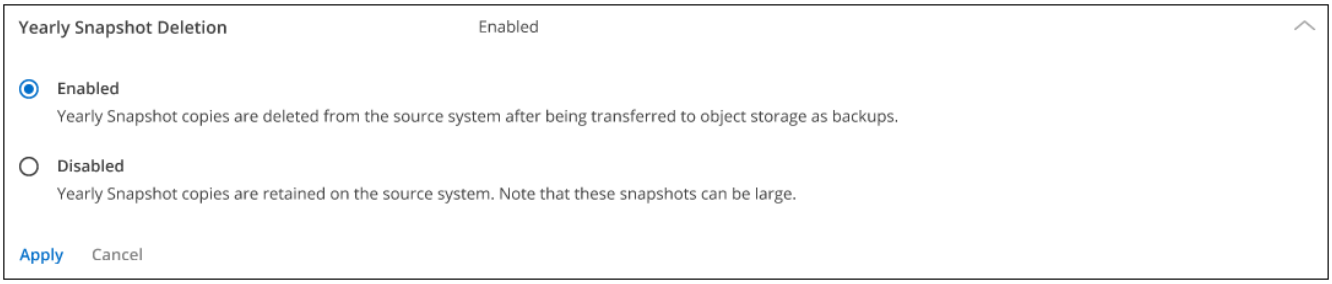
1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su••• per il sistema e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Esporta snapshot esistenti**.
4. Seleziona se desideri esportare gli snapshot esistenti.
5. Selezionare **Applica**.

Modifica se gli snapshot "annuali" vengono rimossi dal sistema sorgente

Quando si seleziona l'etichetta di backup "annuale" per un criterio di backup per uno qualsiasi dei volumi, lo snapshot creato è molto grande. Per impostazione predefinita, questi snapshot annuali vengono eliminati automaticamente dal sistema di origine dopo essere stati trasferiti nell'archiviazione degli oggetti. È possibile modificare questo comportamento predefinito dalla sezione Eliminazione snapshot annuale.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su••• per il sistema e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Eliminazione snapshot annuale**.



4. Selezionare **Disabilitato** per conservare gli snapshot annuali sul sistema di origine.
5. Selezionare **Applica**.

Abilita o disabilita le scansioni ransomware

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

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

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

L'attivazione delle scansioni ransomware comporterà costi aggiuntivi a seconda del provider cloud.

Le scansioni ransomware pianificate vengono eseguite solo sull'ultimo snapshot.

Se le scansioni ransomware pianificate sono disattivate, è comunque possibile eseguire scansioni su richiesta e la scansione durante un'operazione di ripristino verrà comunque eseguita.

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

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per il sistema e selezionare **Impostazioni avanzate**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Scansione ransomware**.
4. Abilita o disabilita la **Scansione ransomware**.
5. Seleziona **Scansione ransomware pianificata**.
6. Facoltativamente, è possibile modificare la scansione predefinita ogni settimana in giorni o settimane.
7. Imposta la frequenza in giorni o settimane con cui deve essere eseguita la scansione.
8. Selezionare **Applica**.

Esegui il backup dei dati Cloud Volumes ONTAP su Amazon S3 con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP su Amazon S3.

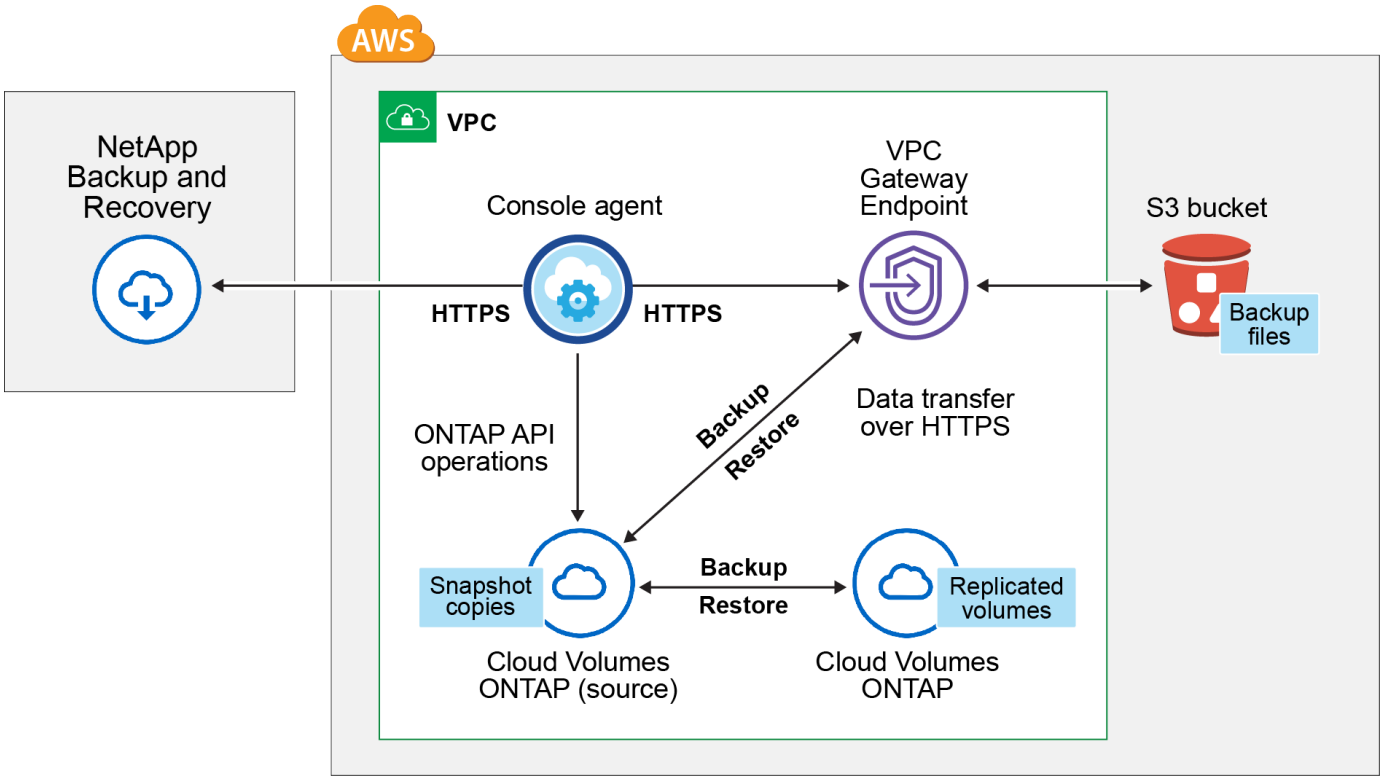
Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Verifica il supporto per la tua configurazione

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

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

Facoltativamente, 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 nella tua VPC. "Scopri di più sugli endpoint gateway" .

Versioni ONTAP supportate

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

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

Puoi scegliere le tue chiavi gestite dal cliente per la crittografia dei dati nella procedura guidata di attivazione anziché utilizzare le chiavi di crittografia Amazon S3 predefinite. In questo caso sarà necessario che le chiavi di crittografia gestite siano già impostate. "Scopri come usare le tue chiavi" .

Verificare i requisiti della licenza

Per le licenze NetApp Backup and Recovery PAYGO, è disponibile un abbonamento alla console in AWS Marketplace che consente le distribuzioni di Cloud Volumes ONTAP e NetApp Backup and Recovery. Devi "iscriviti a questo abbonamento NetApp Console" prima di abilitare NetApp Backup and Recovery. La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.

Per un contratto annuale che consente di eseguire il backup sia dei dati Cloud Volumes ONTAP che dei dati ONTAP locali, è necessario abbonarsi da "Pagina AWS Marketplace" poi "associa l'abbonamento alle tue credenziali AWS" .

Per un contratto annuale che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery, è necessario impostare il contratto annuale quando si crea un sistema Cloud Volumes ONTAP . Questa opzione non consente di eseguire il backup dei dati locali.

Per la licenza BYOL NetApp Backup and Recovery , 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 l'agente Console e il sistema Cloud Volumes ONTAP vengono distribuiti in un dark site.

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

Prepara il tuo agente Console

L'agente Console deve essere installato in una regione AWS con accesso a Internet completo o limitato (modalità "standard" o "limitata"). "Per i dettagli, vedere le modalità di distribuzione NetApp Console" .

- "Scopri di più sugli agenti della console"
- "Distribuisci un agente Console in AWS in modalità standard (accesso completo a Internet)"
- "Installa l'agente Console in modalità limitata (accesso in uscita limitato)"

Verificare o aggiungere autorizzazioni all'agente della console

Il ruolo IAM che fornisce alla Console le autorizzazioni deve includere le autorizzazioni S3 dall'ultima versione "Politica della console" . Se la policy non contiene tutte queste autorizzazioni, vedere "Documentazione AWS: modifica delle policy IAM" .

Ecco le autorizzazioni specifiche previste dalla 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 Cina, è necessario modificare il nome della risorsa AWS "arn" in tutte le sezioni *Resource* nelle policy IAM da "aws" a "aws-cn"; ad esempio `arn:aws-cn:s3:::netapp-backup-*` .

Autorizzazioni 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 le autorizzazioni a tale sistema deve includere un nuovo set di autorizzazioni S3 specifiche per NetApp Backup and Recovery dalla versione più recente "Criterio Cloud Volumes ONTAP" .

Se hai creato il sistema Cloud Volumes ONTAP utilizzando la versione 3.9.23 o successiva della console, queste autorizzazioni dovrebbero già far parte del ruolo IAM. Altrimenti sarà necessario aggiungere le autorizzazioni mancanti.

Regioni AWS supportate

NetApp Backup and Recovery è supportato in tutte le regioni AWS, comprese le regioni AWS GovCloud.

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

Per impostazione predefinita, i backup vengono creati utilizzando lo stesso account utilizzato per il sistema Cloud Volumes ONTAP . Se desideri utilizzare un account AWS diverso per i tuoi backup, devi:

- Verificare che le autorizzazioni "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" facciano parte del ruolo IAM che fornisce le autorizzazioni all'agente della console.
- Aggiungere le credenziali dell'account AWS di destinazione nella Console. "Scopri come fare" .
- Aggiungere le seguenti autorizzazioni nelle credenziali utente del 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 dei bucket per te. Se desideri utilizzare i tuoi bucket, puoi crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.
- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in subnet diverse, le subnet devono essere instradate insieme (questa è l'impostazione predefinita).

Abilita NetApp Backup and Recovery su Cloud Volumes ONTAP

Abilitare NetApp Backup and Recovery è semplice. I passaggi variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Abilita NetApp Backup and Recovery su un nuovo sistema

NetApp Backup and Recovery è abilitato per impostazione predefinita nella procedura guidata di sistema. Assicuratevi di mantenere l'opzione abilitata.

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

Passi

1. Dalla pagina **Sistemi** della console, seleziona **Aggiungi sistema**, scegli il provider cloud e seleziona **Aggiungi nuovo**. Selezionare **Crea Cloud Volumes ONTAP**.
2. Seleziona **Amazon Web Services** come provider cloud, quindi scegli un singolo nodo o un sistema HA.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina Servizi, lascia il servizio abilitato e seleziona **Continua**.
5. Completare le pagine della procedura guidata per distribuire il sistema.

Risultato

NetApp Backup and Recovery è abilitato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare NetApp Backup and Recovery e"attiva il backup su ogni volume che vuoi proteggere" .

Abilita NetApp Backup and Recovery su un sistema esistente

Abilita NetApp Backup and Recovery su un sistema esistente in qualsiasi momento direttamente dalla Console.

Passi

1. Dalla pagina **Sistemi** della console, seleziona il cluster e seleziona **Abilita** accanto a Backup e ripristino nel pannello di destra.

   Se la destinazione Amazon S3 per i backup esiste come cluster nella pagina **Sistemi**, è possibile trascinare il cluster sul sistema Amazon S3 per avviare la procedura guidata di configurazione.

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione AWS per i backup esiste come sistema nella pagina **Sistemi** della Console, è

possibile trascinare il cluster ONTAP nell'archivio oggetti AWS.

- Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **opzione icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

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

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario e da quello secondario all'archiviazione degli oggetti.
   - **Fan out**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario *e* dal primario all'archiviazione degli oggetti.

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

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.
5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Amazon Web Services**.

- **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

  Inserisci l'account AWS utilizzato per archiviare 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 nella Console e aggiungere le autorizzazioni "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" al ruolo IAM che fornisce le autorizzazioni alla Console.

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

  Crea un nuovo bucket oppure selezionane uno esistente.

- **Chiave di crittografia**: se hai creato un nuovo bucket, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia AWS predefinite oppure scegliere le chiavi gestite dal cliente dal tuo account AWS per gestire la crittografia dei tuoi dati. ("Scopri come utilizzare le tue chiavi di crittografia").

  Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave.

  Se hai scelto un bucket esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario inserirle ora.

- **Criterio di backup**: seleziona un criterio di archiviazione di backup su oggetto esistente o creane uno.

  Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
  - Seleziona **Crea**.

- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

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

Viene creato un bucket S3 nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse, e i file di backup vengono archiviati lì.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati Cloud Volumes ONTAP nell'archiviazione BLOB di Azure con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP allo storage BLOB di Azure.

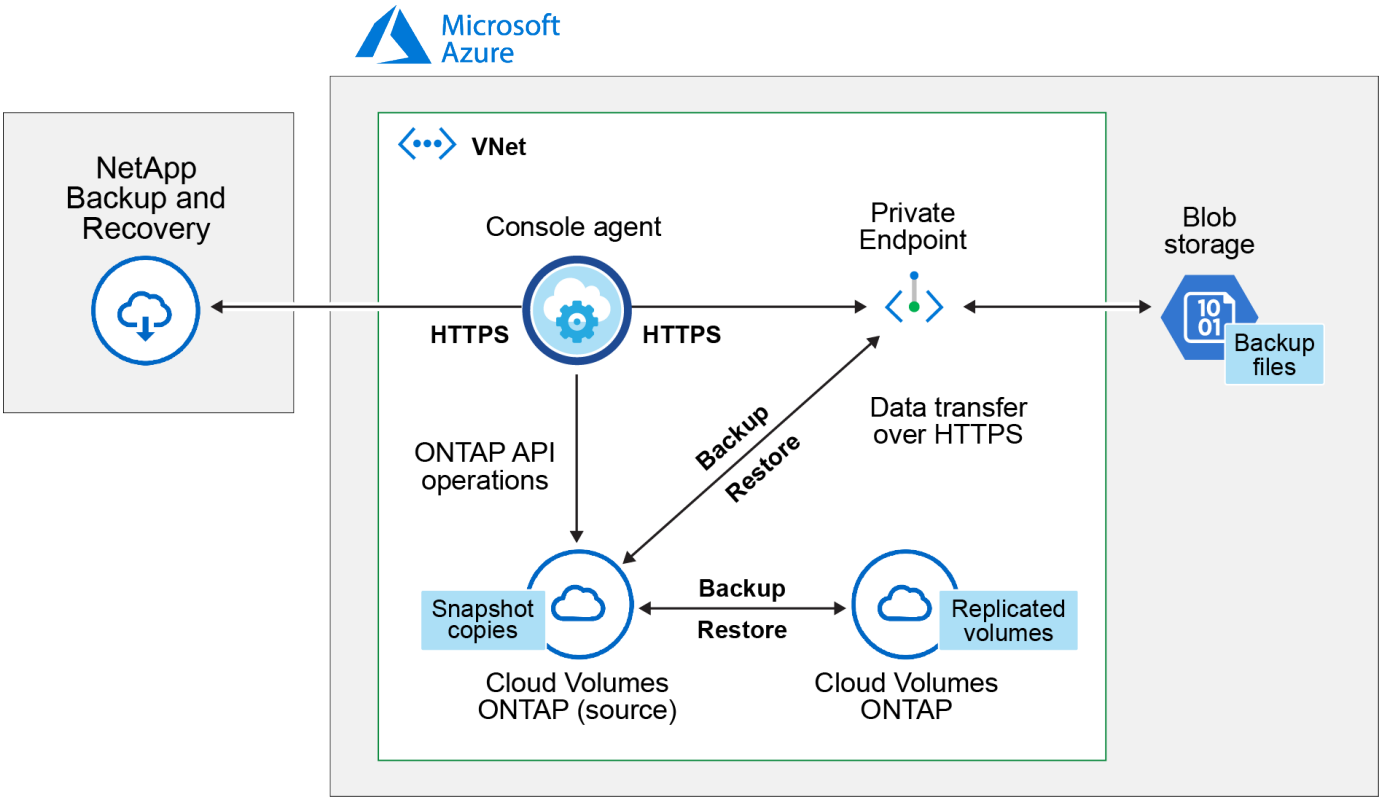
Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Verifica il supporto per la tua configurazione

Leggere i requisiti seguenti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei volumi nell'archiviazione BLOB di Azure.

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

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



Versioni ONTAP supportate

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

Regioni di Azure supportate

NetApp Backup and Recovery è supportato in tutte le regioni di Azure, comprese le regioni di Azure Government.

Per impostazione predefinita, NetApp Backup and Recovery fornisce al contenitore Blob la ridondanza locale (LRS) per ottimizzare i costi. È possibile modificare questa impostazione in Ridondanza di zona (ZRS) dopo aver attivato NetApp Backup and Recovery se si desidera assicurarsi che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modificando il modo in cui viene replicato il tuo account di archiviazione" .

Configurazione richiesta per la creazione di backup in una sottoscrizione Azure diversa

Per impostazione predefinita, i backup vengono creati utilizzando lo stesso abbonamento utilizzato per il sistema Cloud Volumes ONTAP .

Verificare i requisiti della licenza

Per le licenze NetApp Backup and Recovery PAYGO, è necessario un abbonamento tramite Azure Marketplace prima di abilitare NetApp Backup and Recovery. La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento. "Puoi iscriverti dalla pagina Dettagli e credenziali della procedura guidata di sistema" .

Per la licenza BYOL NetApp Backup and Recovery , 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 l'agente Console e il sistema Cloud Volumes ONTAP vengono

distribuiti in un sito oscuro ("modalità privata").

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di archiviazione in cui verranno salvati i backup.

Prepara il tuo agente Console

L'agente Console può essere installato in un'area di Azure con accesso a Internet completo o limitato (modalità "standard" o "limitata"). "Per i dettagli, vedere le modalità di distribuzione NetApp Console" .

- "Scopri di più sugli agenti della console"
- "Distribuisci un agente Console in Azure in modalità standard (accesso completo a Internet)"
- "Installa l'agente Console in modalità limitata (accesso in uscita limitato)"

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità di ricerca e ripristino NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere ad Azure Synapse Workspace e all'account Data Lake Storage. Consultare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Prima di iniziare

- È necessario registrare il provider di risorse di Azure Synapse Analytics (denominato "Microsoft.Synapse") con la sottoscrizione. "Scopri come registrare questo fornitore di risorse per il tuo abbonamento" . Per registrare il fornitore di risorse, devi essere il **Proprietario** o il **Collaboratore** dell'abbonamento.
- La porta 1433 deve essere aperta per la comunicazione tra l'agente della console e i servizi Azure Synapse SQL.

Passi

1. Identificare il ruolo assegnato alla macchina virtuale dell'agente Console:
   a. Nel portale di Azure, aprire il servizio Macchine virtuali.
   b. Selezionare la macchina virtuale dell'agente Console.
   c. In Impostazioni, seleziona **Identità**.
   d. Selezionare **Assegnazioni di ruolo di Azure**.
   e. Prendi nota del ruolo personalizzato assegnato alla macchina virtuale dell'agente Console.
2. Aggiorna il ruolo personalizzato:
   a. Nel portale di Azure, apri la tua sottoscrizione di Azure.
   b. Selezionare **Controllo accessi (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. Seleziona **Revisiona + aggiorna** e poi seleziona **Aggiorna**.

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

È possibile utilizzare le chiavi gestite dal cliente per la crittografia dei dati nella procedura guidata di attivazione anziché utilizzare le chiavi di crittografia predefinite gestite da Microsoft. In questo caso, sarà necessario disporre della sottoscrizione di Azure, del nome del Key Vault e della chiave. "Scopri come usare le tue chiavi" .

NetApp Backup and Recovery supporta i *criteri di accesso di Azure*, il modello di autorizzazione *Azure role-based access control* (Azure RBAC) e il *Managed Hardware Security Model* (HSM) (fare riferimento a "Che cos'è Azure Key Vault Managed HSM?").

Crea il tuo account di archiviazione BLOB di Azure

Per impostazione predefinita, il servizio crea account di archiviazione per te. Se si desidera utilizzare account di archiviazione personali, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali account di archiviazione nella procedura guidata.

"Scopri di più sulla creazione dei tuoi account di archiviazione".

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.
- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in subnet diverse, le subnet devono essere instradate insieme (questa è l'impostazione predefinita).

Abilita NetApp Backup and Recovery su Cloud Volumes ONTAP

Abilitare NetApp Backup and Recovery è semplice. I passaggi variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Abilita NetApp Backup and Recovery su un nuovo sistema

NetApp Backup and Recovery è abilitato per impostazione predefinita nella procedura guidata di sistema. Assicuratevi di mantenere l'opzione abilitata.

Vedere "Avvio di Cloud Volumes ONTAP in Azure" per requisiti e dettagli sulla creazione del sistema Cloud Volumes ONTAP .

Se si desidera scegliere il nome del gruppo di risorse, **disabilitare** NetApp Backup and Recovery durante la distribuzione Cloud Volumes ONTAP.

Passi

1. Dalla pagina **Sistemi** della console, seleziona **Aggiungi sistema**, scegli il provider cloud e seleziona **Aggiungi nuovo**. Selezionare **Crea Cloud Volumes ONTAP**.
2. Seleziona **Microsoft Azure** come provider cloud, quindi scegli un singolo nodo o un sistema HA.
3. Nella pagina Definisci credenziali di Azure, immetti il nome delle credenziali, l'ID client, il segreto client e l'ID directory, quindi seleziona **Continua**.
4. Compila la pagina Dettagli e credenziali e assicurati che sia attivo un abbonamento ad Azure Marketplace, quindi seleziona **Continua**.
5. Nella pagina Servizi, lascia il servizio abilitato e seleziona **Continua**.
6. Completare le pagine della procedura guidata per distribuire il sistema.

Risultato

NetApp Backup and Recovery è abilitato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare NetApp Backup and Recovery e"attiva il backup su ogni volume che vuoi proteggere" .

Abilita NetApp Backup and Recovery su un sistema esistente

Abilita NetApp Backup and Recovery in qualsiasi momento direttamente dal sistema.

Passi

1. Dalla pagina **Sistemi** della console, seleziona il sistema e seleziona **Abilita** accanto a Backup e ripristino nel pannello di destra.

   Se la destinazione di Azure Blob per i backup esiste come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster sul sistema Azure Blob per avviare la procedura guidata di configurazione.

2. Completare le pagine della procedura guidata per distribuire NetApp Backup and Recovery.
3. Quando si desidera avviare i backup, continuare conAttiva i backup sui tuoi volumi ONTAP .

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi ancheMostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione di Azure per i backup esiste come sistema nella pagina **Sistemi**, è possibile trascinare il cluster ONTAP nell'archivio oggetti BLOB di Azure.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

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

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 . (I volumi FlexGroup possono essere selezionati solo uno alla volta.) Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario e da quello secondario all'archiviazione degli oggetti.
   - **Fan out**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario *e* dal primario all'archiviazione degli oggetti.

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

   > Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     > Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

- Inserisci il nome della policy.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Microsoft Azure**.
   - **Impostazioni del provider**: inserisci i dettagli del provider.

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

     Crea un nuovo account di archiviazione oppure selezionane uno esistente.

     Immettere la sottoscrizione di Azure utilizzata per archiviare i backup. Potrebbe trattarsi di un abbonamento diverso da quello in cui risiede il sistema Cloud Volumes ONTAP .

     Crea il tuo gruppo di risorse che gestisce il contenitore BLOB oppure seleziona il tipo di gruppo di risorse e il gruppo.

     > Se vuoi proteggere i tuoi file di backup da modifiche o eliminazioni, assicurati che l'account di archiviazione sia stato creato con l'archiviazione immutabile abilitata utilizzando un periodo di conservazione di 30 giorni.

     > Se si desidera suddividere i file di backup più vecchi in Azure Archive Storage per un'ulteriore ottimizzazione dei costi, assicurarsi che l'account di archiviazione disponga della regola del ciclo di vita appropriata.

   - **Chiave di crittografia**: se hai creato un nuovo account di archiviazione di Azure, immetti le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Azure oppure scegliere le chiavi gestite dal cliente dal tuo account Azure per gestire la crittografia dei tuoi dati.

     Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave. "Impara a usare le tue chiavi" .

     > Se hai scelto un account di archiviazione Microsoft esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario immetterle ora.

   - **Networking**: scegli lo spazio IP e se utilizzerai un endpoint privato. Per impostazione predefinita, l'endpoint privato è disabilitato.
     i. Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
     ii. Facoltativamente, scegli se utilizzerai un endpoint privato di Azure precedentemente configurato. "Scopri di più sull'utilizzo di un endpoint privato di Azure" .
   - **Criterio di backup**: seleziona un criterio di archiviazione di backup su oggetto esistente.

     > Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

        - Inserisci il nome della policy.
        - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
        - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
        - Seleziona **Crea**.
    - **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.
6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti negli snapshot.

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

Viene creato un contenitore di archiviazione BLOB nel gruppo di risorse immesso e i file di backup vengono archiviati lì.

Per impostazione predefinita, NetApp Backup and Recovery fornisce al contenitore Blob la ridondanza locale (LRS) per ottimizzare i costi. È possibile modificare questa impostazione in Ridondanza di zona (ZRS) se si desidera assicurarsi che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modificando il modo in cui viene replicato il tuo account di archiviazione" .

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Cosa succederà ora?

- Puoi"gestire i file di backup e le policy di backup" . Ciò include l'avvio e l'interruzione dei backup, l'eliminazione dei backup, l'aggiunta e la modifica della pianificazione dei backup e altro ancora.
- Puoi"gestire le impostazioni di backup a livello di cluster" . Ciò include la modifica delle chiavi di archiviazione utilizzate ONTAP per accedere all'archiviazione cloud, la modifica della larghezza di banda di rete disponibile per caricare i backup nell'archiviazione degli oggetti, la modifica dell'impostazione di backup automatico per i volumi futuri e altro ancora.
- Puoi anche"ripristinare volumi, cartelle o singoli file da un file di backup" a un sistema Cloud Volumes ONTAP in AWS o a un sistema ONTAP locale.

Esegui il backup dei dati Cloud Volumes ONTAP su Google Cloud Storage con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP su Google Cloud Storage.

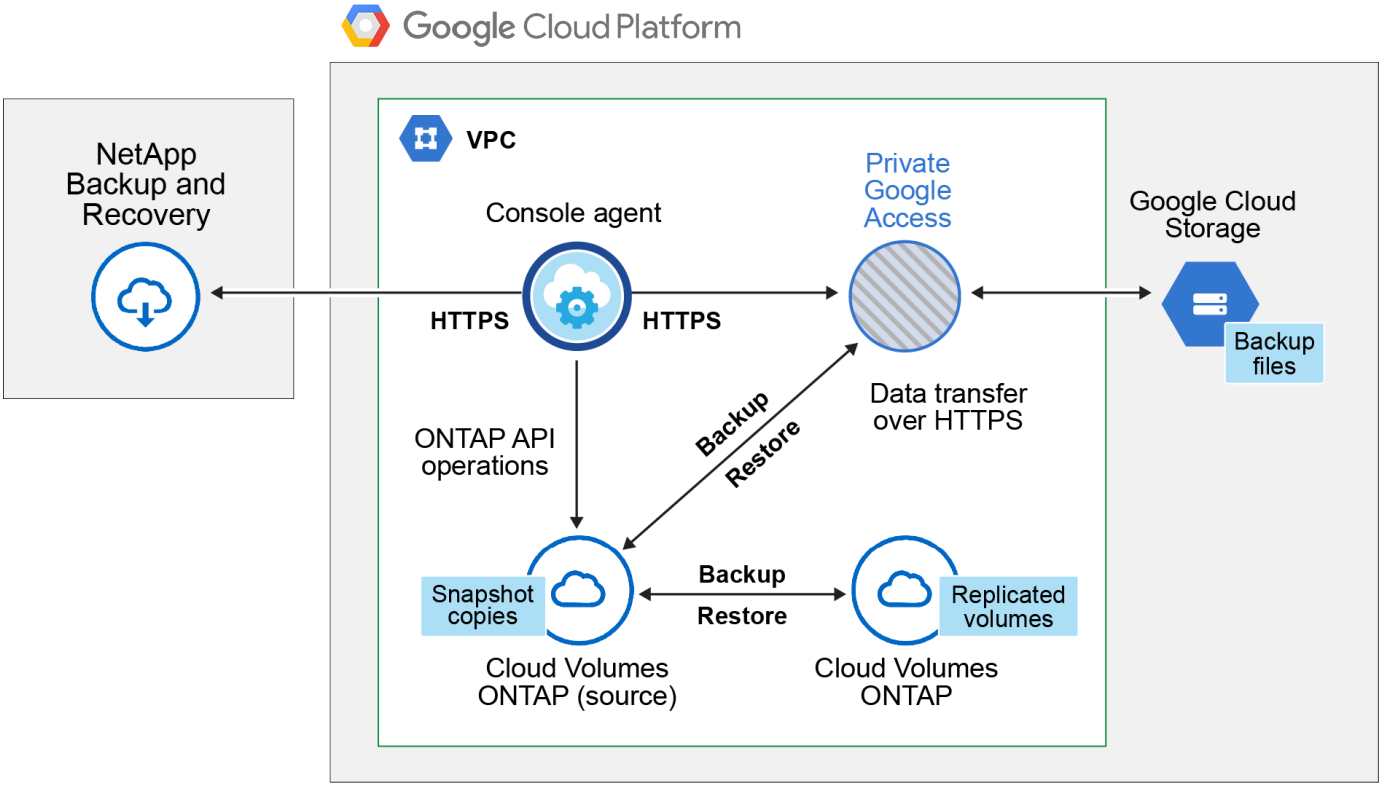
Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Verifica il supporto per la tua configurazione

Leggi i seguenti requisiti per assicurarti 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 predisporre tra di essi.

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



Versioni ONTAP supportate

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

Regioni GCP supportate

NetApp Backup and Recovery è supportato in tutte le regioni GCP.

Account di servizio GCP

Devi disporre di un account di servizio nel tuo progetto Google Cloud che abbia il ruolo personalizzato. "Scopri come creare un account di servizio" .

Il ruolo di amministratore di archiviazione non è più necessario per l'account di servizio che consente a NetApp Backup and Recovery di accedere ai bucket di Google Cloud Storage.

Verificare i requisiti della licenza

Per le licenze NetApp Backup and Recovery PAYGO, è disponibile un abbonamento alla console in Google Marketplace che consente le distribuzioni di Cloud Volumes ONTAP e NetApp Backup and Recovery. Devi "iscriviti a questo abbonamento alla Console" prima di abilitare NetApp Backup and Recovery. La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento. "Puoi iscriverti dalla pagina Dettagli e credenziali della procedura guidata di sistema" .

Per la licenza BYOL NetApp Backup and Recovery , 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 archiviazione in cui verranno salvati i backup.

Prepara il tuo agente Console

L'agente Console deve essere installato in una regione Google con accesso a Internet.

- "Scopri di più sugli agenti della console"
- "Distribuisci un agente Console in Google Cloud"

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità "Cerca e ripristina" NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere al servizio Google Cloud BigQuery. Consultare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, seleziona il progetto o l'organizzazione che contiene il ruolo che desideri modificare.
3. Seleziona un ruolo personalizzato.
4. Selezionare **Modifica ruolo** per aggiornare le autorizzazioni del ruolo.
5. Selezionare **Aggiungi autorizzazioni** 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)

Puoi utilizzare le tue chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi interregionali che quelle interprogetto, quindi è possibile scegliere un progetto per un bucket diverso dal progetto della chiave CMEK. Se intendi utilizzare le tue chiavi gestite dal cliente:

- Per poter aggiungere queste informazioni nella procedura guidata di attivazione, è necessario disporre del Key Ring e del Key Name. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .
- Sarà necessario verificare che le seguenti autorizzazioni richieste siano incluse nel ruolo dell'agente della console:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Dovrai verificare che l'API "Cloud Key Management Service (KMS)" di Google sia abilitata nel tuo progetto. Vedi il "Documentazione di Google Cloud: abilitazione delle API" per i dettagli.

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate da hardware) sia quelle generate da software.
- Sono supportate sia le chiavi Cloud KMS appena create che quelle importate.
- Sono supportate solo le chiavi regionali; le chiavi globali non sono supportate.
- Attualmente è supportata solo la funzione "Crittografia/decifratura simmetrica".
- All'agente di servizio associato all'account di archiviazione viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" da NetApp Backup and Recovery.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. Se desideri utilizzare i tuoi bucket, puoi crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in subnet diverse, le subnet devono essere instradate insieme (questa è l'impostazione predefinita).

Abilita NetApp Backup and Recovery su Cloud Volumes ONTAP

I passaggi per abilitare NetApp Backup and Recovery variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Abilita NetApp Backup and Recovery su un nuovo sistema

NetApp Backup and Recovery può essere abilitato una volta completata la procedura guidata di sistema per creare un nuovo sistema Cloud Volumes ONTAP .

È necessario che sia già configurato un account di servizio. Se non selezioni un account di servizio quando crei il sistema Cloud Volumes ONTAP , dovrai disattivare il sistema e aggiungere l'account di servizio a Cloud Volumes ONTAP dalla console GCP.

Vedere "Avvio di Cloud Volumes ONTAP in GCP" per requisiti e dettagli sulla creazione del sistema Cloud Volumes ONTAP .

Passi

1. Dalla pagina **Sistemi** della console, seleziona **Aggiungi sistema**, scegli il provider cloud e seleziona **Aggiungi nuovo**. Selezionare **Crea Cloud Volumes ONTAP**.
2. **Scegli una posizione**: seleziona **Google Cloud Platform**.
3. **Scegli tipo**: seleziona * Cloud Volumes ONTAP* (nodo singolo o alta disponibilità).
4. **Dettagli e credenziali**: Inserisci le seguenti informazioni:
   a. Fare clic su **Modifica progetto** e selezionare un nuovo progetto se quello che si desidera utilizzare è diverso dal progetto predefinito (in cui risiede l'agente della console).
   b. Specificare il nome del cluster.
   c. Abilitare l'opzione **Account di servizio** e selezionare l'Account di servizio che ha il ruolo di Amministratore di archiviazione predefinito. Ciò è necessario per abilitare i backup e la suddivisione in livelli.
   d. Specificare le credenziali.

      Assicurati di avere un abbonamento a GCP Marketplace.
5. **Servizi**: Lasciare abilitato NetApp Backup and Recovery e fare clic su **Continua**.
6. Completare le pagine della procedura guidata per distribuire il sistema come descritto in "Avvio di Cloud Volumes ONTAP in GCP" .

Risultato

NetApp Backup and Recovery è abilitato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare NetApp Backup and Recovery e"attiva il backup su ogni volume che vuoi proteggere" .

Abilita NetApp Backup and Recovery su un sistema esistente

È possibile abilitare NetApp Backup and Recovery in qualsiasi momento direttamente dal sistema.

Passi

1. Dalla pagina **Sistemi** della console, seleziona il sistema e seleziona **Abilita** accanto a Backup e ripristino nel pannello di destra.

   Se la destinazione di Google Cloud Storage per i backup esiste come sistema nella pagina **Sistemi** della console, puoi trascinare il cluster sul sistema Google Cloud Storage per avviare la procedura guidata di configurazione.

Prepara Google Cloud Storage come destinazione di backup

Per preparare Google Cloud Storage come destinazione di backup, sono necessari i seguenti passaggi:

- Imposta le autorizzazioni.
- (Facoltativo) Crea i tuoi bucket. (Se lo desideri, il servizio creerà dei bucket per te.)
- (Facoltativo) Impostare le chiavi gestite dal cliente per la crittografia dei dati

Imposta i permessi

È necessario fornire le chiavi di accesso all'archiviazione per un account di servizio che dispone di autorizzazioni specifiche utilizzando un ruolo personalizzato. Un account di servizio consente a NetApp Backup and Recovery di autenticare e accedere ai bucket di Cloud Storage utilizzati per archiviare i backup. Le chiavi sono necessarie affinché Google Cloud Storage sappia chi sta effettuando la richiesta.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. "Crea 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, "vai alla pagina Account di servizio" .
4. Seleziona il tuo progetto Cloud.
5. Seleziona **Crea account di servizio** e fornisci le informazioni richieste:
   a. **Dettagli dell'account di servizio**: inserisci un nome e una descrizione.
   b. **Concedi a questo account di servizio l'accesso al progetto**: seleziona il ruolo personalizzato appena creato.
   c. Selezionare **Fatto**.

6. Vai a "Impostazioni di archiviazione GCP" e creare chiavi di accesso per l'account di servizio:
   a. Seleziona un progetto e seleziona **Interoperabilità**. Se non lo hai già fatto, seleziona **Abilita accesso interoperabilità**.
   b. In **Chiavi di accesso per gli account di servizio**, seleziona **Crea una chiave per un account di servizio**, seleziona l'account di servizio appena creato e fai clic su **Crea chiave**.

      Sarà necessario immettere le chiavi in NetApp Backup and Recovery in un secondo momento, quando si configura il servizio di backup.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Impostare le chiavi di crittografia gestite dal cliente (CMEK) per la crittografia dei dati

Puoi utilizzare le tue chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi interregionali che quelle interprogetto, quindi è possibile scegliere un progetto per un bucket diverso dal progetto della chiave CMEK.

Se intendi utilizzare le tue chiavi gestite dal cliente:

- Per poter aggiungere queste informazioni nella procedura guidata di attivazione, è necessario disporre del Key Ring e del Key Name. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .
- Sarà necessario verificare che le seguenti autorizzazioni richieste siano incluse nel ruolo dell'agente della console:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Dovrai verificare che l'API "Cloud Key Management Service (KMS)" di Google sia abilitata nel tuo progetto. Vedi il "Documentazione di Google Cloud: abilitazione delle API" per i dettagli.

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate da hardware) sia quelle generate da software.
- Sono supportate sia le chiavi Cloud KMS appena create che quelle importate.
- Sono supportate solo le chiavi regionali, le chiavi globali non sono supportate.
- Attualmente è supportata solo la funzione "Crittografia/decifratura simmetrica".

- All’agente di servizio associato all’account di archiviazione viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" da NetApp Backup and Recovery.

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l’attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione GCP per i backup esiste come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell’archivio oggetti GCP.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

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

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l’opzione **Aggiungi un agente Console**. Fare riferimento a Prepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario e da quello secondario all'archiviazione degli oggetti.
   - **Fan out**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno.

   Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Per i criteri di backup su oggetto, configurare Datalock e Ransomware Resilience. Per i dettagli su Datalock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
   - Seleziona **Crea**.

4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Google Cloud**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

     Crea un nuovo bucket oppure selezionane uno esistente.

   - **Chiave di crittografia**: se hai creato un nuovo bucket Google, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Google Cloud oppure scegliere le chiavi gestite dal cliente dal tuo account Google per gestire la crittografia dei tuoi dati.

     Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave.

     Se hai scelto un bucket Google Cloud esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario inserirle ora.

   - **Criterio di backup**: seleziona un criterio di archiviazione di backup su oggetto esistente o creane uno.

     Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

- Inserisci il nome della policy.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

◦ **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

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

Viene creato un bucket di Google Cloud Storage nell'account di servizio indicato dalla chiave di accesso e dalla chiave segreta di Google immesse, dove vengono archiviati i file di backup.

Per impostazione predefinita, i backup sono associati alla classe di archiviazione *Standard*. È possibile utilizzare le classi di archiviazione più economiche *Nearline*, *Coldline* o *Archive*. Tuttavia, la classe di archiviazione viene configurata tramite Google e non tramite l'interfaccia utente NetApp Backup and Recovery . Vedi l'argomento di Google "Modifica della classe di archiviazione predefinita di un bucket" per i dettagli.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Cosa succederà ora?

- Puoi"gestire i file di backup e le policy di backup" . Ciò include l'avvio e l'interruzione dei backup, l'eliminazione dei backup, l'aggiunta e la modifica della pianificazione dei backup e altro ancora.
- Puoi"gestire le impostazioni di backup a livello di cluster" . Ciò include la modifica delle chiavi di archiviazione utilizzate ONTAP per accedere all'archiviazione cloud, la modifica della larghezza di banda di rete disponibile per caricare i backup nell'archiviazione degli oggetti, la modifica dell'impostazione di backup automatico per i volumi futuri e altro ancora.
- Puoi anche"ripristinare volumi, cartelle o singoli file da un file di backup" a un sistema Cloud Volumes ONTAP in AWS o a un sistema ONTAP locale.

Esegui il backup dei dati ONTAP locali su Amazon S3 con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali a un sistema di storage secondario e allo storage cloud Amazon S3.

I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

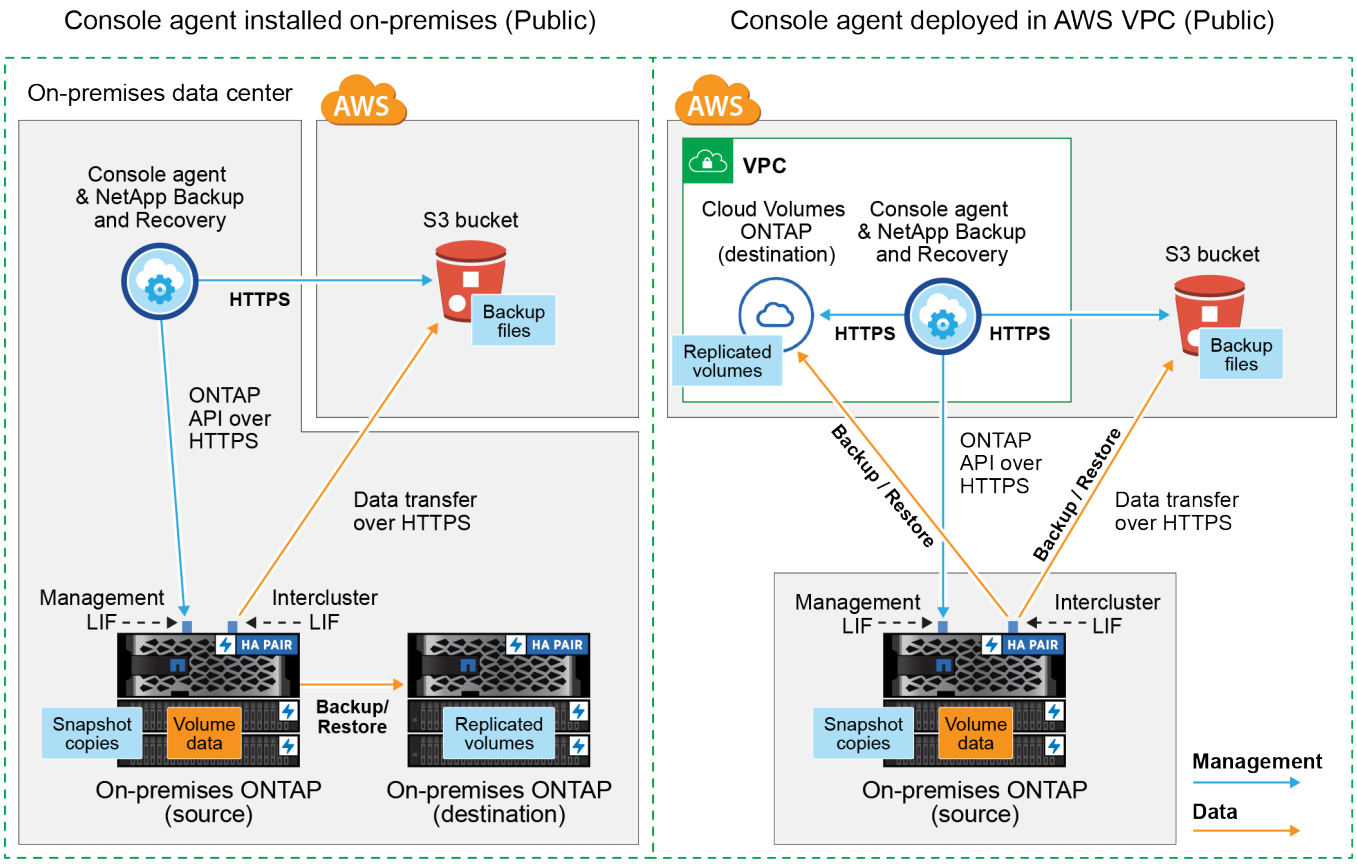
Identificare il metodo di connessione

Scegli quale dei due metodi di connessione utilizzerai durante la configurazione dei backup dai sistemi ONTAP locali ad AWS S3.

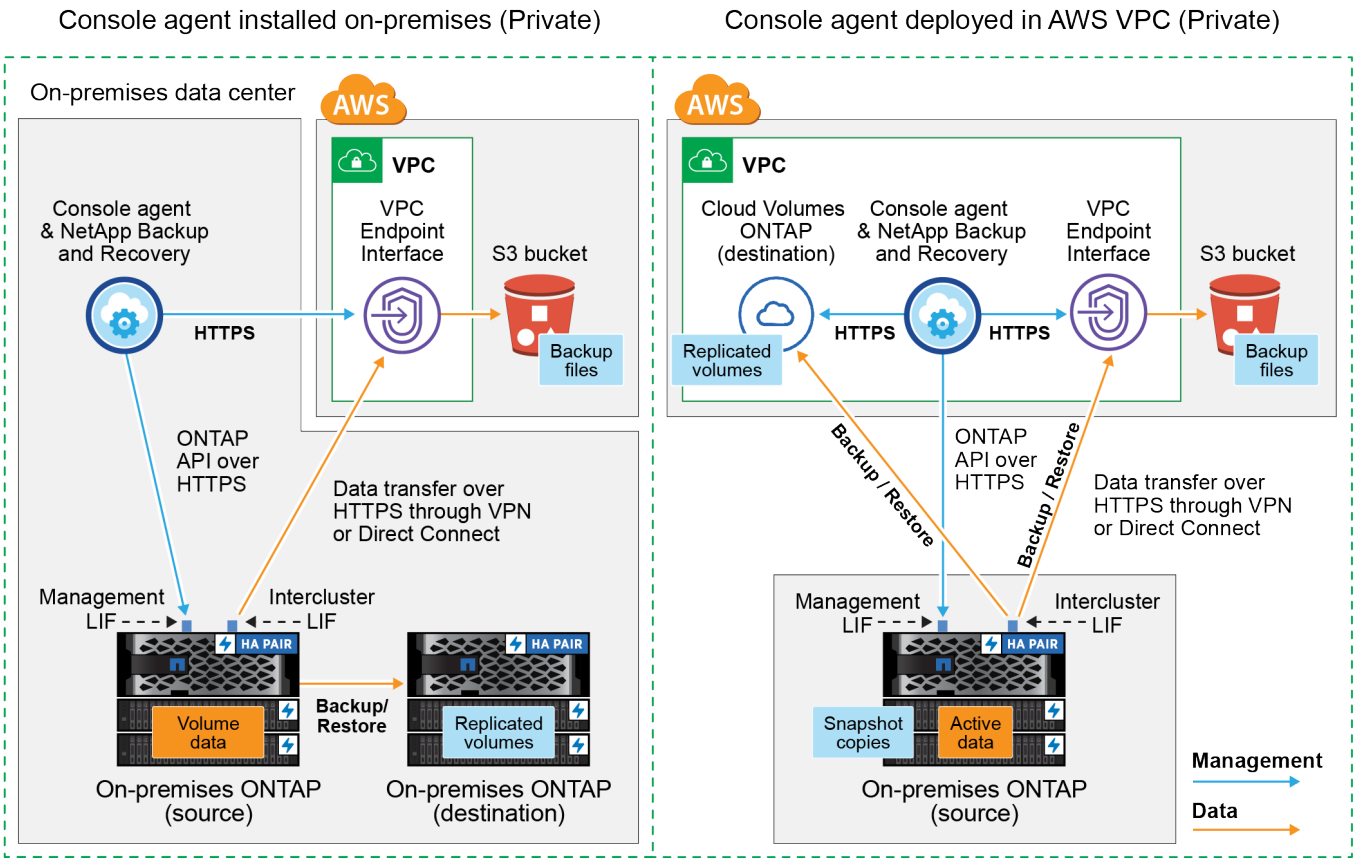
- **Connessione pubblica** - Connetti direttamente il sistema ONTAP ad AWS S3 utilizzando un endpoint S3 pubblico.
- **Connessione privata**: utilizza una VPN o AWS Direct Connect e instrada il traffico tramite un'interfaccia endpoint VPC che utilizza un indirizzo IP privato.

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

Il diagramma seguente mostra il metodo di **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. Puoi utilizzare un agente Console installato in sede oppure un agente Console distribuito nella VPC AWS.



Il diagramma seguente mostra il metodo di **connessione privata** e le connessioni che è necessario preparare tra i componenti. Puoi utilizzare un agente Console installato in sede oppure un agente Console distribuito nella VPC AWS.



Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità NetApp Console . Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Se hai già un agente Console distribuito nella tua AWS VPC o in sede, sei a posto.

In caso contrario, sarà necessario creare un agente Console in una di queste posizioni per eseguire il backup dei dati ONTAP nello storage AWS S3. Non è possibile utilizzare un agente Console distribuito in un altro provider cloud.

- "Scopri di più sugli agenti della console"
- "Installa un agente Console in AWS"
- "Installa un agente Console nei tuoi locali"
- "Installa un agente Console in una regione AWS GovCloud"

  NetApp Backup and Recovery è supportato nelle regioni GovCloud quando l'agente Console è distribuito nel cloud, non quando è installato nella tua sede. Inoltre, è necessario distribuire l'agente della console da AWS Marketplace. Non è possibile distribuire l'agente Console in una regione governativa dal sito Web NetApp Console SaaS.

Preparare i requisiti di rete dell'agente della console

Assicurarsi che siano soddisfatti i seguenti requisiti di rete:

- Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:
  - Una connessione HTTPS sulla porta 443 a NetApp Backup and Recovery e al tuo archivio di oggetti S3("vedere l'elenco degli endpoint")
  - Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
  - Per le distribuzioni AWS e AWS GovCloud sono necessarie regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per l'agente della console in AWS" per i dettagli.
- Se disponi di una connessione Direct Connect o VPN dal tuo cluster ONTAP alla VPC e desideri che la comunicazione tra l'agente della console e S3 rimanga nella tua rete interna AWS (una connessione **privata**), dovrai abilitare un'interfaccia VPC Endpoint per S3. Configura il tuo sistema per una connessione privata utilizzando un'interfaccia endpoint VPC .

Verificare i requisiti della licenza

Sarà necessario verificare i requisiti di licenza sia per AWS che per la NetApp Console:

- Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai abbonarti a un'offerta NetApp Console Marketplace con pagamento in base al consumo (PAYGO) di AWS oppure acquistare e attivare una licenza NetApp Backup and Recovery BYOL da NetApp. Queste licenze sono riservate al tuo account e possono essere utilizzate su più sistemi.
  - Per la licenza NetApp Backup and Recovery PAYGO, è necessario un abbonamento a "Offerta NetApp Console da AWS Marketplace" . La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.
  - Per la licenza BYOL NetApp Backup and Recovery , avrai bisogno del numero di serie di NetApp che ti consentirà di utilizzare il servizio per la durata e la capacità della licenza.
- È necessario disporre di un abbonamento AWS per lo spazio di archiviazione degli oggetti in cui verranno archiviati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali ad Amazon S3 in tutte le regioni, comprese le regioni AWS GovCloud. Quando si configura il servizio, è possibile specificare la regione in cui verranno archiviati i backup.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .
- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di 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 ingresso dall'agente della console al LIF di gestione del cluster.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Questi LIF intercluster devono essere in grado di accedere all'archivio oggetti.

  Il cluster avvia una connessione HTTPS in uscita tramite la porta 443 dai LIF intercluster allo storage Amazon S3 per le operazioni di backup e ripristino. ONTAP legge e scrive dati da e verso l'archiviazione di oggetti: l'archiviazione di oggetti non si avvia mai, si limita a rispondere.
- I LIF intercluster devono essere associati allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui sono associati questi LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

  Se si utilizza uno spazio IP diverso da "Default", potrebbe essere necessario creare un percorso statico per accedere all'archiviazione degli oggetti.

Tutti i LIF intercluster all'interno dell'IPspace devono avere accesso all'archivio oggetti. Se non è possibile configurarlo per l'IPspace corrente, sarà necessario creare un IPspace dedicato in cui tutti i LIF intercluster abbiano accesso all'archivio oggetti.

- I server DNS devono essere stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se necessario, aggiornare le regole del firewall per consentire le connessioni NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).
- Se si utilizza un endpoint di interfaccia VPC privata in AWS per la connessione S3, affinché venga utilizzato HTTPS/443 sarà necessario caricare il certificato dell'endpoint S3 nel cluster ONTAP . Configura il tuo sistema per una connessione privata utilizzando un'interfaccia endpoint VPC.
- Assicurati che il tuo cluster ONTAP disponga delle autorizzazioni per accedere al bucket S3.

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.

Prepara Amazon S3 come destinazione di backup

Per preparare Amazon S3 come destinazione di backup, sono necessari i seguenti passaggi:

- Impostare le autorizzazioni S3.
- (Facoltativo) Crea i tuoi bucket S3. (Se lo desideri, il servizio creerà dei bucket per te.)
- (Facoltativo) Configurare le chiavi AWS gestite dal cliente per la crittografia dei dati.
- (Facoltativo) Configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC.

Imposta le autorizzazioni S3

Sarà necessario configurare due set di autorizzazioni:

- Autorizzazioni per l'agente della console per creare e gestire il bucket S3.
- Autorizzazioni per il cluster ONTAP locale in modo che possa leggere e scrivere dati nel bucket S3.

Passi

1. Assicurarsi che l'agente della console disponga delle autorizzazioni richieste. Per i dettagli, vedere "Autorizzazioni dei criteri NetApp Console" .

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

2. Quando attivi il servizio, la procedura guidata di backup ti chiederà di immettere una chiave di accesso e una chiave segreta. Queste credenziali vengono trasmesse al cluster ONTAP in modo che ONTAP possa eseguire il backup e il ripristino dei dati nel bucket S3. Per farlo, dovrai creare un utente IAM con le seguenti autorizzazioni.

   Fare riferimento al "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 dei bucket per te. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Se si creano bucket personalizzati, è consigliabile utilizzare il nome "netapp-backup". Se è necessario utilizzare un nome personalizzato, modificare il `ontapcloud-instance-policy-netapp-backup` IAMRole per i CVO esistenti e aggiungere il seguente blocco JSON alle autorizzazioni S3 `Statement` vettore. Devi includere `"Resource": "arn:aws:s3:::*"` e assegnare tutte le autorizzazioni necessarie che devono essere associate al bucket.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "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:::*"
  }
]
```

Imposta le chiavi AWS gestite dal cliente per la crittografia dei dati

Se desideri utilizzare le chiavi di crittografia Amazon S3 predefinite per crittografare i dati trasmessi tra il cluster locale e il bucket S3, sei a posto perché l'installazione predefinita utilizza quel tipo di crittografia.

Se invece si desidera utilizzare le chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi predefinite, sarà necessario che le chiavi di crittografia gestite siano già configurate prima di avviare la procedura guidata NetApp Backup and Recovery .

"Scopri come utilizzare le tue chiavi di crittografia Amazon con Cloud Volumes ONTAP".

"Scopri come utilizzare le tue chiavi di crittografia Amazon con NetApp Backup and Recovery".

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

Se si desidera utilizzare una connessione Internet pubblica standard, tutte le autorizzazioni vengono impostate dall'agente Console e non è necessario fare altro.

Se desideri una connessione Internet più sicura dal tuo data center locale alla VPC, puoi selezionare una connessione AWS PrivateLink nella procedura guidata di attivazione del backup. È obbligatorio se si prevede di utilizzare una VPN o AWS Direct Connect per connettere il sistema locale tramite un'interfaccia VPC Endpoint che utilizza un indirizzo IP privato.

Passi

1. Crea una configurazione dell'endpoint dell'interfaccia utilizzando la console Amazon VPC o la riga di comando. "Fare riferimento ai dettagli sull'utilizzo di AWS PrivateLink per Amazon S3" .
2. Modificare la configurazione del gruppo di sicurezza associato all'agente Console. Devi modificare la policy in "Personalizzata" (da "Accesso completo") e deviaggiungere le autorizzazioni S3 dalla policy di backup come mostrato in precedenza.

   Se si utilizza la porta 80 (HTTP) per la comunicazione con l'endpoint privato, il problema è risolto. Ora puoi abilitare NetApp Backup and Recovery 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 mostrato nei 4 passaggi successivi.

3. Ottieni il nome DNS dell'endpoint dalla console AWS.
4. Ottieni il certificato dall'endpoint VPC S3. Lo fai tramite "accesso alla VM che ospita l'agente della console" ed eseguendo il seguente comando. Quando si immette il nome DNS dell'endpoint, aggiungere "bucket" all'inizio, sostituendo "*":

   ```
   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 inclusi):

```
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. Accedi alla CLI del cluster ONTAP e applica il certificato copiato utilizzando il seguente comando (sostituisci il nome della tua VM di archiviazione):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione Amazon S3 per i backup esiste come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nello storage di oggetti Amazon S3.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina

Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dall'archivio primario a quello secondario, all'archivio degli oggetti, e da quello secondario all'archivio degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

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

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .
4. Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
   - Seleziona **Crea**.
5. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.
6. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Amazon Web Services**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione AWS in cui verranno archiviati 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**: scegli un bucket S3 esistente o creane uno nuovo. Fare riferimento a "Aggiungi bucket S3" .
- **Chiave di crittografia**: se hai creato un nuovo bucket S3, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Amazon S3 oppure scegliere le chiavi gestite dal cliente dal tuo account AWS per gestire la crittografia dei tuoi dati.

  Se hai scelto un bucket esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario inserirle ora.

- **Networking**: scegli lo spazio IP e se utilizzerai un endpoint privato. Per impostazione predefinita, l'endpoint privato è disabilitato.
  i. Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  ii. Facoltativamente, scegli se utilizzare un AWS PrivateLink precedentemente configurato. "Visualizza i dettagli sull'utilizzo di AWS PrivateLink per Amazon S3" .
- **Criterio di backup**: seleziona un criterio di backup esistente o creane uno nuovo.

  Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Seleziona **Crea**.
- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

7. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati primari contenuti negli snapshot.

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

Il bucket S3 viene creato nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse e i file di backup vengono archiviati lì. Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali nell'archiviazione BLOB di Azure con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali a un sistema di archiviazione secondario e all'archiviazione BLOB di Azure.

I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

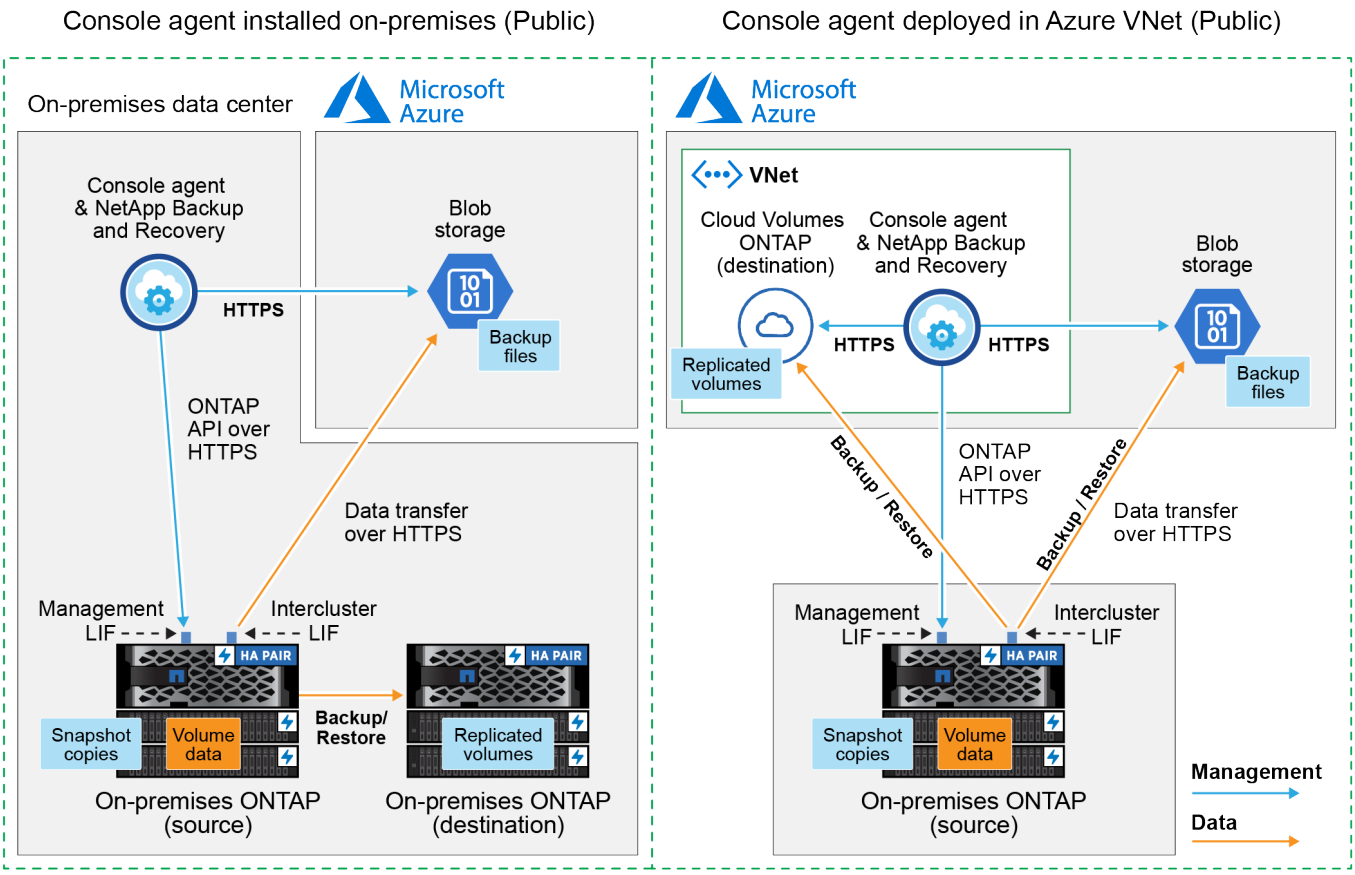
Identificare il metodo di connessione

Scegli quale dei due metodi di connessione utilizzerai durante la configurazione dei backup dai sistemi ONTAP locali ad Azure Blob.

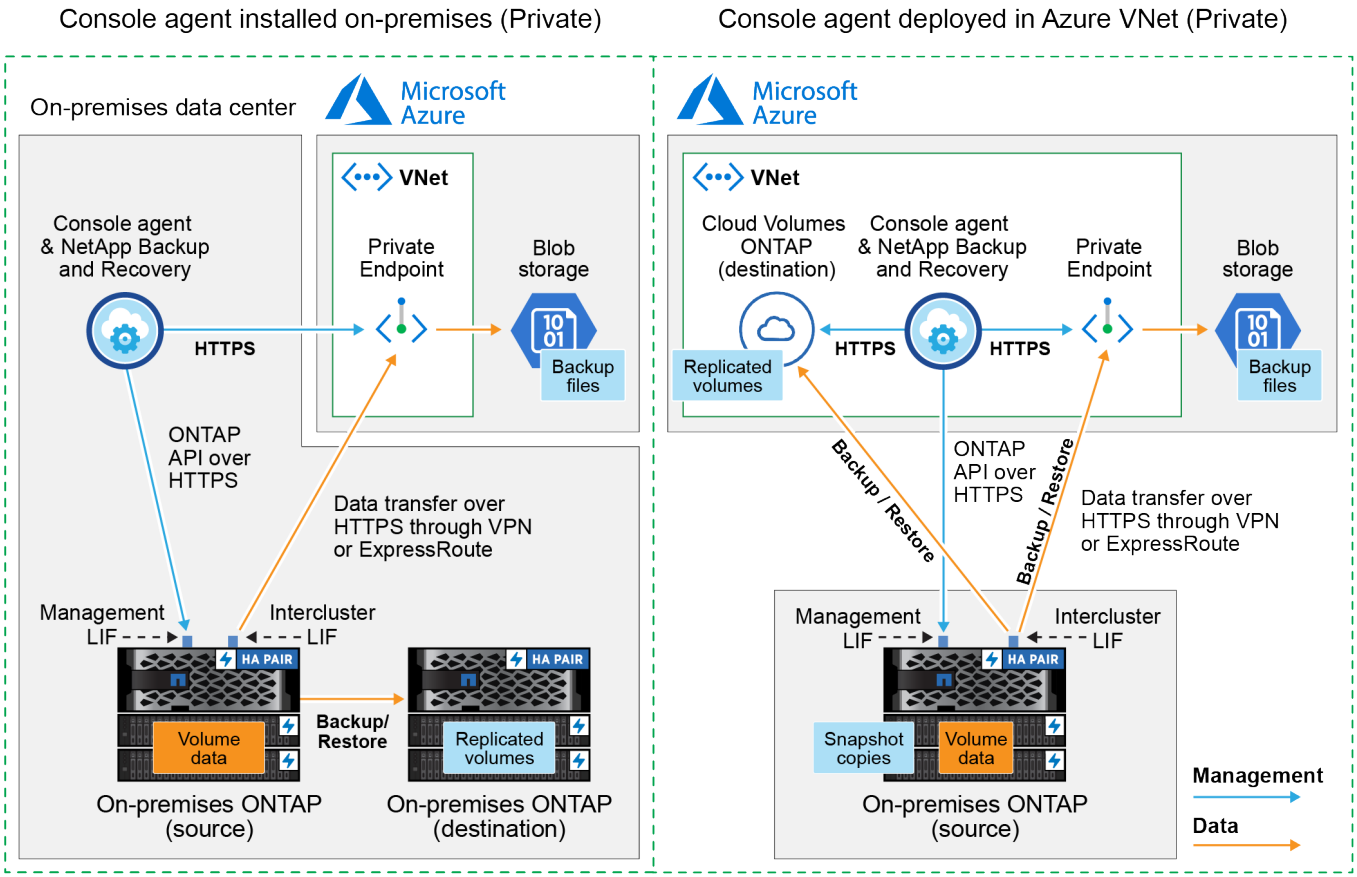
- **Connessione pubblica**: connette direttamente il sistema ONTAP all'archiviazione BLOB di Azure tramite un endpoint pubblico di Azure.
- **Connessione privata**: utilizza una VPN o ExpressRoute e instrada il traffico attraverso un endpoint privato VNet che utilizza un indirizzo IP privato.

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

Il diagramma seguente mostra il metodo di **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un agente Console installato in locale oppure un agente Console distribuito nella rete virtuale di Azure.



Il diagramma seguente mostra il metodo di **connessione privata** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un agente Console installato in locale oppure un agente Console distribuito nella rete virtuale di Azure.



Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità NetApp Console . Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Se hai già un agente Console distribuito nella tua rete virtuale di Azure o in locale, sei a posto.

In caso contrario, sarà necessario creare un agente Console in una di queste posizioni per eseguire il backup dei dati ONTAP nell'archiviazione BLOB di Azure. Non è possibile utilizzare un agente Console distribuito in un altro provider cloud.

- "Scopri di più sugli agenti della console"
- "Installa un agente console in Azure"
- "Installa un agente Console nei tuoi locali"
- "Installare un agente Console in un'area di Azure Government"

  NetApp Backup and Recovery è supportato nelle regioni Azure Government quando l'agente Console è distribuito nel cloud, non quando è installato in sede. Inoltre, è necessario distribuire l'agente Console da Azure Marketplace. Non è possibile distribuire l'agente Console in una regione governativa dal sito Web Console SaaS.

Preparare la rete per l'agente della console

Assicurarsi che l'agente della console disponga delle connessioni di rete richieste.

Passi

1. Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:
   - Una connessione HTTPS sulla porta 443 a NetApp Backup and Recovery e al tuo archivio di oggetti BLOB("vedere l'elenco degli endpoint")
   - Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
   - Per il corretto funzionamento della funzionalità NetApp Backup and Recovery Search & Restore, la porta 1433 deve essere aperta per la comunicazione tra l'agente della console e i servizi Azure Synapse SQL.
   - Per le distribuzioni di Azure e Azure Government sono necessarie regole aggiuntive per i gruppi di sicurezza in ingresso. Vedere "Regole per l'agente Console in Azure" per i dettagli.
2. Abilitare un endpoint privato VNet per l'archiviazione di Azure. Questa operazione è necessaria se si dispone di una connessione ExpressRoute o VPN dal cluster ONTAP alla VNet e si desidera che la comunicazione tra l'agente della console e l'archiviazione BLOB rimanga nella rete privata virtuale (una connessione **privata**).

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità di ricerca e ripristino NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere ad Azure Synapse Workspace e all'account Data Lake Storage. Consultare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Prima di iniziare

È necessario registrare il provider di risorse di Azure Synapse Analytics (denominato "Microsoft.Synapse") con la sottoscrizione. "Scopri come registrare questo fornitore di risorse per il tuo abbonamento" . Per registrare il fornitore di risorse, devi essere il **Proprietario** o il **Collaboratore** dell'abbonamento.

Passi

1. Identificare il ruolo assegnato alla macchina virtuale dell'agente Console:
   a. Nel portale di Azure, aprire il servizio Macchine virtuali.
   b. Selezionare la macchina virtuale dell'agente Console.
   c. In **Impostazioni**, seleziona **Identità**.
   d. Selezionare **Assegnazioni di ruolo di Azure**.
   e. Prendi nota del ruolo personalizzato assegnato alla macchina virtuale dell'agente Console.
2. Aggiorna il ruolo personalizzato:
   a. Nel portale di Azure, apri la tua sottoscrizione di Azure.
   b. Selezionare **Controllo accessi (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. Seleziona **Revisiona + aggiorna** e poi seleziona **Aggiorna**.

Verificare i requisiti della licenza

Sarà necessario verificare i requisiti di licenza sia per Azure che per la console:

- Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai abbonarti a un'offerta di Console Marketplace con pagamento in base al consumo (PAYGO) di Azure oppure acquistare e attivare una licenza BYOL di NetApp Backup and Recovery da NetApp. Queste licenze sono riservate al tuo account e possono essere utilizzate su più sistemi.
  - Per la licenza NetApp Backup and Recovery PAYGO, è necessario un abbonamento a "Offerta NetApp Console da Azure Marketplace" . La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.
  - Per la licenza BYOL NetApp Backup and Recovery , avrai bisogno del numero di serie di NetApp che ti consentirà 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 archiviazione degli oggetti in cui verranno salvati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali ad Azure Blob in tutte le aree geografiche, comprese le aree di Azure Government. Quando si configura il servizio, si specifica la regione in cui verranno archiviati i backup.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .

- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di 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 intercluster all'archiviazione BLOB di Azure per le operazioni di backup e ripristino.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster. L'agente della console può risiedere in una rete virtuale di Azure.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF dei nodi e degli intercluster sono in grado di accedere all'archivio oggetti.
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se si utilizza uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere all'archiviazione degli oggetti.
- Se necessario, aggiornare le regole del firewall per consentire le connessioni del servizio NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza 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 anziché utilizzare le chiavi di crittografia predefinite gestite da Microsoft. In questo caso sarà necessario disporre della sottoscrizione di Azure, del nome del Key Vault e della chiave. "Impara a usare le tue chiavi" .

   Si noti che Backup e ripristino supportano *criteri di accesso di Azure* come modello di autorizzazione. Il modello di autorizzazione *Azure role-based access control* (Azure RBAC) non è attualmente supportato.

2. Se desideri una connessione più sicura tramite Internet pubblica dal tuo data center locale alla rete virtuale, è disponibile un'opzione per configurare un endpoint privato di Azure nella procedura guidata di attivazione. In questo caso sarà necessario conoscere la VNet e la Subnet per questa connessione. "Fare riferimento ai dettagli sull'utilizzo di un endpoint privato" .

Crea il tuo account di archiviazione BLOB di Azure

Per impostazione predefinita, il servizio crea account di archiviazione per te. Se si desidera utilizzare account di archiviazione personali, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali account di archiviazione nella procedura guidata.

"Scopri di più sulla creazione dei tuoi account di archiviazione".

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto al servizio Backup e ripristino nel pannello di destra.

Se la destinazione di Azure per i backup è presente nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell'archivio oggetti BLOB di Azure.

- Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

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

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio Snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal primario al secondario e dal secondario all'archiviazione degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

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

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.
5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:

- **Provider**: seleziona **Microsoft Azure**.
- **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

  Crea un nuovo account di archiviazione oppure selezionane uno esistente.

  Crea il tuo gruppo di risorse che gestisce il contenitore BLOB oppure seleziona il tipo di gruppo di risorse e il gruppo.

  > Se vuoi proteggere i tuoi file di backup da modifiche o eliminazioni, assicurati che l'account di archiviazione sia stato creato con l'archiviazione immutabile abilitata utilizzando un periodo di conservazione di 30 giorni.

  > Se si desidera suddividere i file di backup più vecchi in Azure Archive Storage per un'ulteriore ottimizzazione dei costi, assicurarsi che l'account di archiviazione disponga della regola del ciclo di vita appropriata.

- **Chiave di crittografia**: se hai creato un nuovo account di archiviazione di Azure, immetti le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Azure oppure scegliere le chiavi gestite dal cliente dal tuo account Azure per gestire la crittografia dei tuoi dati.

  Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave.

  > Se hai scelto un account di archiviazione Microsoft esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario immetterle ora.

- **Networking**: scegli lo spazio IP e se utilizzerai un endpoint privato. Per impostazione predefinita, l'endpoint privato è disabilitato.
  i. Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  ii. Facoltativamente, scegli se utilizzerai un endpoint privato di Azure precedentemente configurato. "Scopri di più sull'utilizzo di un endpoint privato di Azure" .
- **Criterio di backup**: seleziona un criterio di backup esistente per l'archiviazione degli oggetti oppure creane uno nuovo.

  > Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
  - Seleziona **Crea**.
- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot

locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

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

Viene creato un account di archiviazione BLOB nel gruppo di risorse immesso e i file di backup vengono archiviati lì. Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su Google Cloud Storage con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP primari locali a un sistema di storage secondario e a Google Cloud Storage.

I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

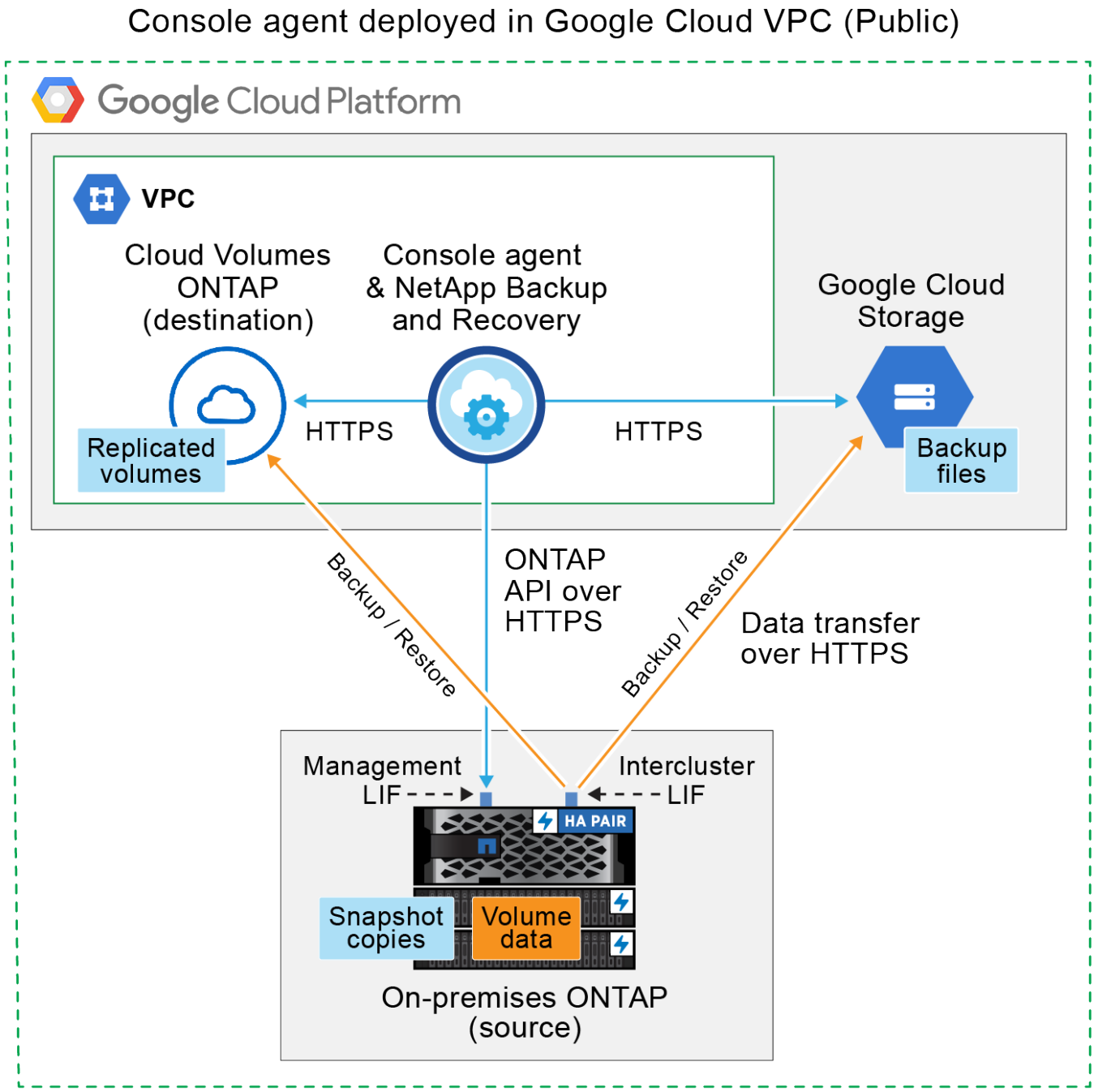
Identificare il metodo di connessione

Scegli quale dei due metodi di connessione utilizzerai quando configuri i backup dai sistemi ONTAP locali a Google Cloud Storage.

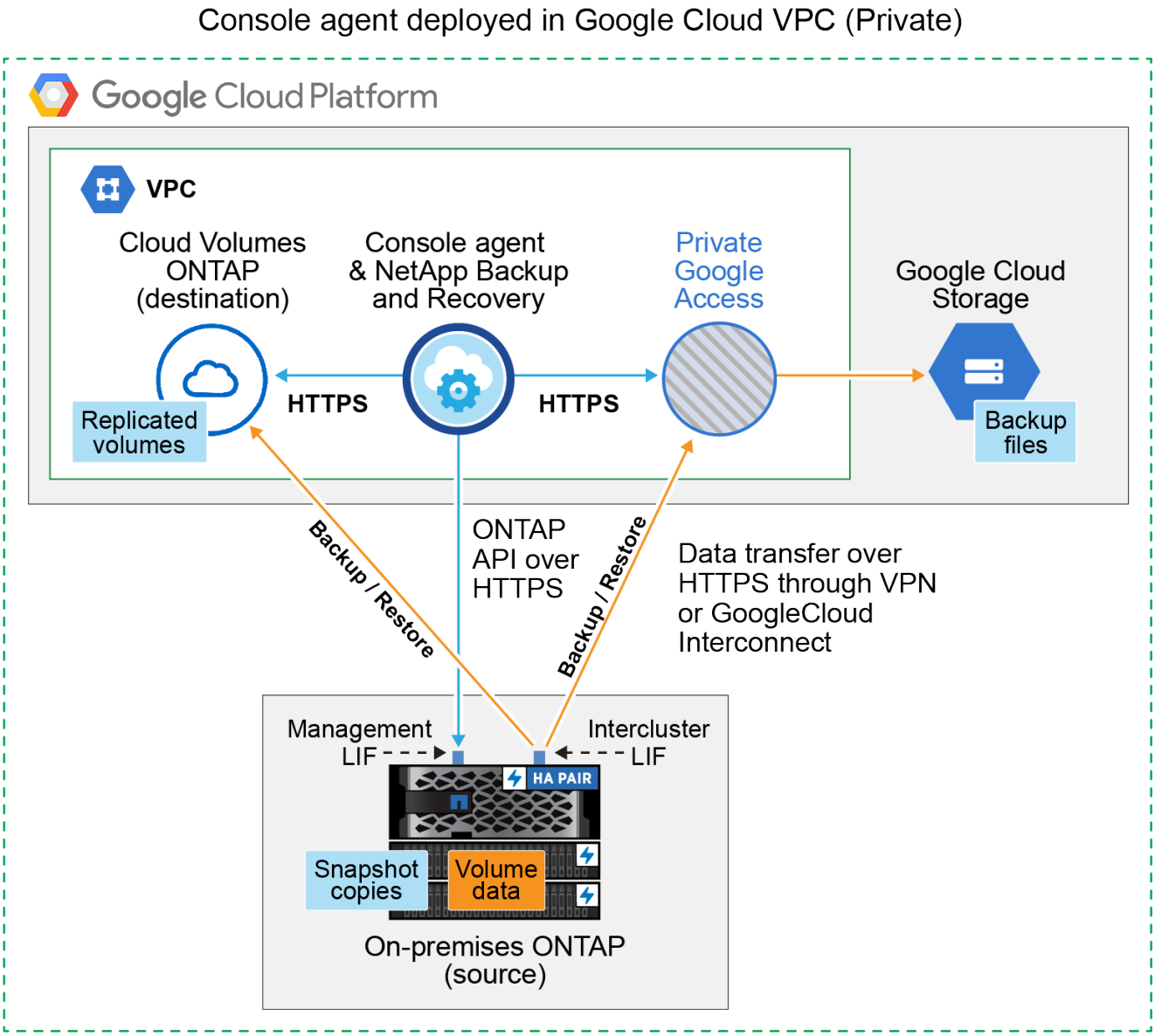
- **Connessione pubblica** - Collega direttamente il sistema ONTAP a Google Cloud Storage tramite un endpoint pubblico di Google.
- **Connessione privata**: utilizza una VPN o Google Cloud Interconnect e instrada il traffico tramite un'interfaccia Google Access privata che utilizza un indirizzo IP privato.

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

Il diagramma seguente mostra il metodo di **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. L'agente della console deve essere distribuito nella VPC di Google Cloud Platform.



Il diagramma seguente mostra il metodo di **connessione privata** e le connessioni che è necessario preparare tra i componenti. L'agente della console deve essere distribuito nella VPC di Google Cloud Platform.



Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità Console. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Se hai già un agente Console distribuito nella tua VPC di Google Cloud Platform, sei a posto.

In caso contrario, sarà necessario creare un agente Console in quella posizione per eseguire il backup dei dati ONTAP su Google Cloud Storage. Non è possibile utilizzare un agente Console distribuito in un altro provider cloud o in locale.

- "Scopri di più sugli agenti della console"
- "Installa un agente Console in GCP"

Preparare la rete per l'agente della console

Assicurarsi che l'agente della console disponga delle connessioni di rete richieste.

Passi

1. Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:
   - Una connessione HTTPS sulla porta 443 a NetApp Backup and Recovery e al tuo spazio di archiviazione Google Cloud("vedere l'elenco degli endpoint")
   - Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
2. Abilitare Private Google Access (o Private Service Connect) sulla subnet in cui si prevede di distribuire l'agente Console. "Accesso privato a Google" O "Connessione al servizio privato" sono necessari se si dispone di una connessione diretta dal cluster ONTAP alla VPC e si desidera che la comunicazione tra l'agente della console e Google Cloud Storage rimanga nella rete privata virtuale (una connessione **privata**).

   Segui le istruzioni di Google per impostare queste opzioni di accesso privato. Assicurati che i tuoi server DNS siano stati configurati per puntare `www.googleapis.com` E `storage.googleapis.com` agli indirizzi IP interni (privati) corretti.

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità "Cerca e ripristina" NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere al servizio Google Cloud BigQuery. Esaminare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, seleziona il progetto o l'organizzazione che contiene il ruolo che desideri modificare.
3. Seleziona un ruolo personalizzato.
4. Selezionare **Modifica ruolo** per aggiornare le autorizzazioni del ruolo.
5. Selezionare **Aggiungi autorizzazioni** 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 della licenza

- Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai abbonarti a un'offerta Console Marketplace pay-as-you-go (PAYGO) di Google oppure acquistare e attivare una licenza BYOL NetApp Backup and Recovery da NetApp. Queste licenze sono riservate al tuo account e possono essere utilizzate su più sistemi.
  - Per la licenza NetApp Backup and Recovery PAYGO, è necessario un abbonamento a "Offerta NetApp Console da Google Marketplace" . La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.
  - Per la licenza BYOL NetApp Backup and Recovery , avrai bisogno del numero di serie di NetApp che ti consentirà 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 archiviazione degli oggetti in cui verranno salvati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali su Google Cloud Storage in tutte le regioni. Quando si configura il servizio, è possibile specificare la regione in cui verranno archiviati i backup.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .

- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di 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 intercluster a Google Cloud Storage per le operazioni di backup e ripristino.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster. L'agente della console può risiedere in una VPC di Google Cloud Platform.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF intercluster dei nodi sono in grado di accedere all'archivio oggetti.
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .

  Se utilizzi Private Google Access o Private Service Connect, assicurati che i tuoi server DNS siano stati configurati per puntare `storage.googleapis.com` all'indirizzo IP interno (privato) corretto.

- Tieni presente che se utilizzi uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare una route statica per accedere all'archiviazione degli oggetti.
- Se necessario, aggiornare le regole del firewall per consentire le connessioni NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel

provider cloud. In genere si tratta di una connessione VPN.

- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.

Prepara Google Cloud Storage come destinazione di backup

Per preparare Google Cloud Storage come destinazione di backup, sono necessari i seguenti passaggi:

- Imposta le autorizzazioni.
- (Facoltativo) Crea i tuoi bucket. (Se lo desideri, il servizio creerà dei bucket per te.)
- (Facoltativo) Impostare le chiavi gestite dal cliente per la crittografia dei dati

Imposta i permessi

È necessario fornire le chiavi di accesso all'archiviazione per un account di servizio che dispone di autorizzazioni specifiche utilizzando un ruolo personalizzato. Un account di servizio consente a NetApp Backup and Recovery di autenticare e accedere ai bucket di Cloud Storage utilizzati per archiviare i backup. Le chiavi sono necessarie affinché Google Cloud Storage sappia chi sta effettuando la richiesta.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. "Crea 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, "vai alla pagina Account di servizio" .
4. Seleziona il tuo progetto Cloud.
5. Seleziona **Crea account di servizio** e fornisci le informazioni richieste:

a. **Dettagli dell'account di servizio**: inserisci un nome e una descrizione.

b. **Concedi a questo account di servizio l'accesso al progetto**: seleziona il ruolo personalizzato appena creato.

c. Selezionare **Fatto**.

6. Vai a "Impostazioni di archiviazione GCP" e creare chiavi di accesso per l'account di servizio:

a. Seleziona un progetto e seleziona **Interoperabilità**. Se non lo hai già fatto, seleziona **Abilita accesso interoperabilità**.

b. In **Chiavi di accesso per gli account di servizio**, seleziona **Crea una chiave per un account di servizio**, seleziona l'account di servizio appena creato e fai clic su **Crea chiave**.

Sarà necessario immettere le chiavi in NetApp Backup and Recovery in un secondo momento, quando si configura il servizio di backup.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Impostare le chiavi di crittografia gestite dal cliente (CMEK) per la crittografia dei dati

Puoi utilizzare le tue chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi interregionali che quelle interprogetto, quindi è possibile scegliere un progetto per un bucket diverso dal progetto della chiave CMEK.

Se intendi utilizzare le tue chiavi gestite dal cliente:

- Per poter aggiungere queste informazioni nella procedura guidata di attivazione, è necessario disporre del Key Ring e del Key Name. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .
- Sarà necessario verificare che le seguenti autorizzazioni richieste siano incluse nel ruolo dell'agente della console:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Dovrai verificare che l'API "Cloud Key Management Service (KMS)" di Google sia abilitata nel tuo progetto. Vedi il "Documentazione di Google Cloud: abilitazione delle API" per i dettagli.

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate da hardware) sia quelle generate da software.
- Sono supportate sia le chiavi Cloud KMS appena create che quelle importate.
- Sono supportate solo le chiavi regionali, le chiavi globali non sono supportate.
- Attualmente è supportata solo la funzione "Crittografia/decifratura simmetrica".
- All'agente di servizio associato all'account di archiviazione viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" da NetApp Backup and Recovery.

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione di Google Cloud Storage per i backup è presente nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell'archivio oggetti di Google Cloud.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

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

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento a Prepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una

combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal primario al secondario e dal secondario all'archiviazione degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.

4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Google Cloud**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

     Crea un nuovo bucket oppure selezionane uno già creato.

     Se desideri suddividere i file di backup più vecchi nell'archiviazione di Google Cloud Archive per un'ulteriore ottimizzazione dei costi, assicurati che il bucket disponga della regola del ciclo di vita appropriata.

     Inserisci la chiave di accesso e la chiave segreta di Google Cloud.

   - **Chiave di crittografia**: se hai creato un nuovo account di archiviazione Google Cloud, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Google Cloud oppure scegliere le chiavi gestite dal cliente dal tuo account Google Cloud per gestire la crittografia dei tuoi dati.

     Se hai scelto un account di archiviazione Google Cloud esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario inserirle ora.

     Se scegli di utilizzare le tue chiavi gestite dal cliente, inserisci il portachiavi e il nome della chiave. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .

- **Networking**: Seleziona lo spazio IP.

  Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.

- **Criterio di backup**: seleziona un criterio di backup esistente per l'archiviazione degli oggetti oppure creane uno nuovo.

  Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Seleziona **Crea**.

- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli 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 immesse, dove vengono archiviati i file di backup. Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura

guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su ONTAP S3 con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali principali. È possibile inviare i backup a un sistema di archiviazione ONTAP secondario (un volume replicato) o a un bucket su un sistema ONTAP configurato come server S3 (un file di backup) o a entrambi.

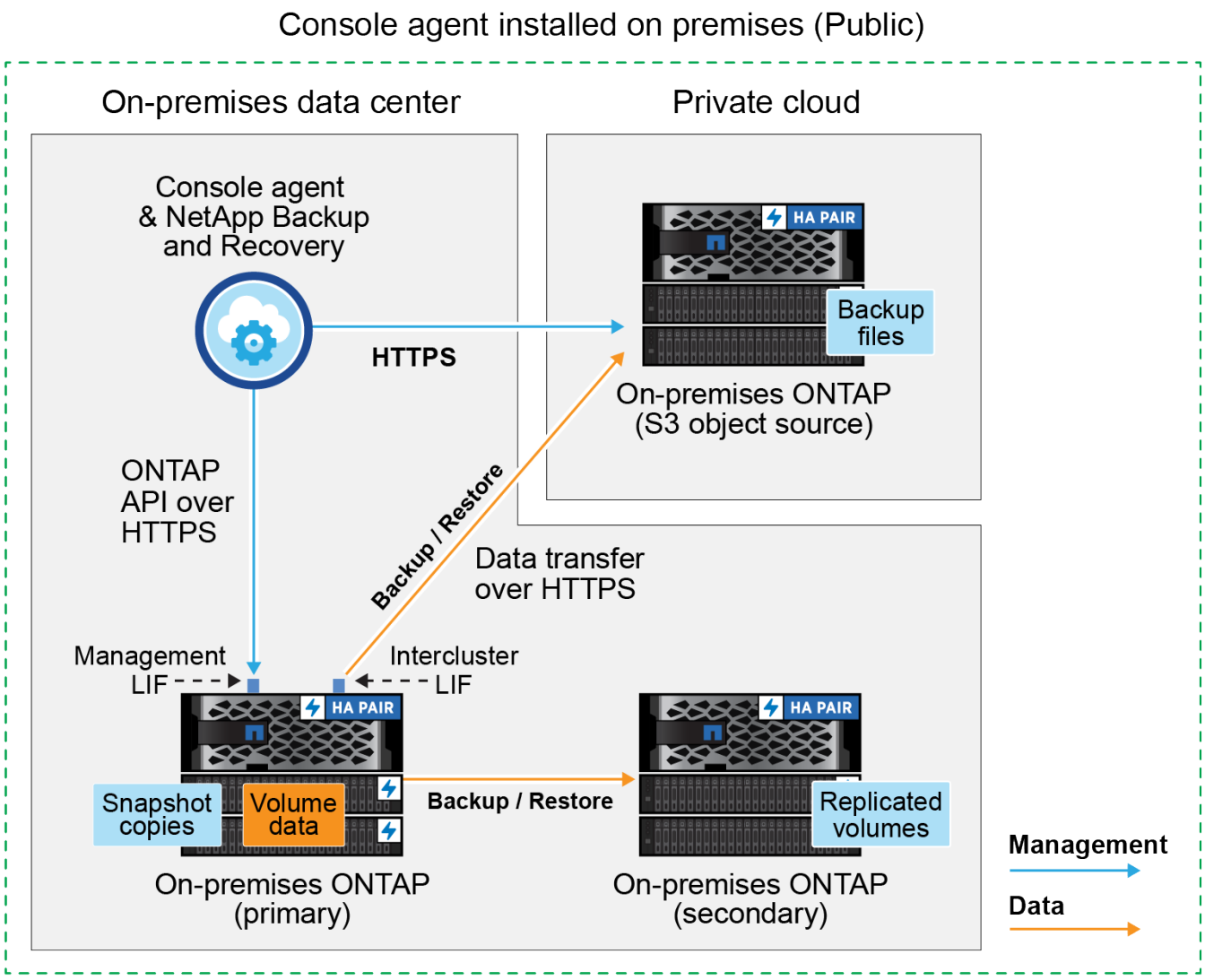
Il sistema ONTAP principale in sede può essere un sistema FAS, AFF o ONTAP Select . Il sistema ONTAP secondario può essere un ONTAP locale o un sistema Cloud Volumes ONTAP . L'archiviazione degli oggetti può essere su un sistema ONTAP locale o su un sistema Cloud Volumes ONTAP su cui è stato abilitato un server di archiviazione degli oggetti Simple Storage Service (S3).

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Identificare il metodo di connessione

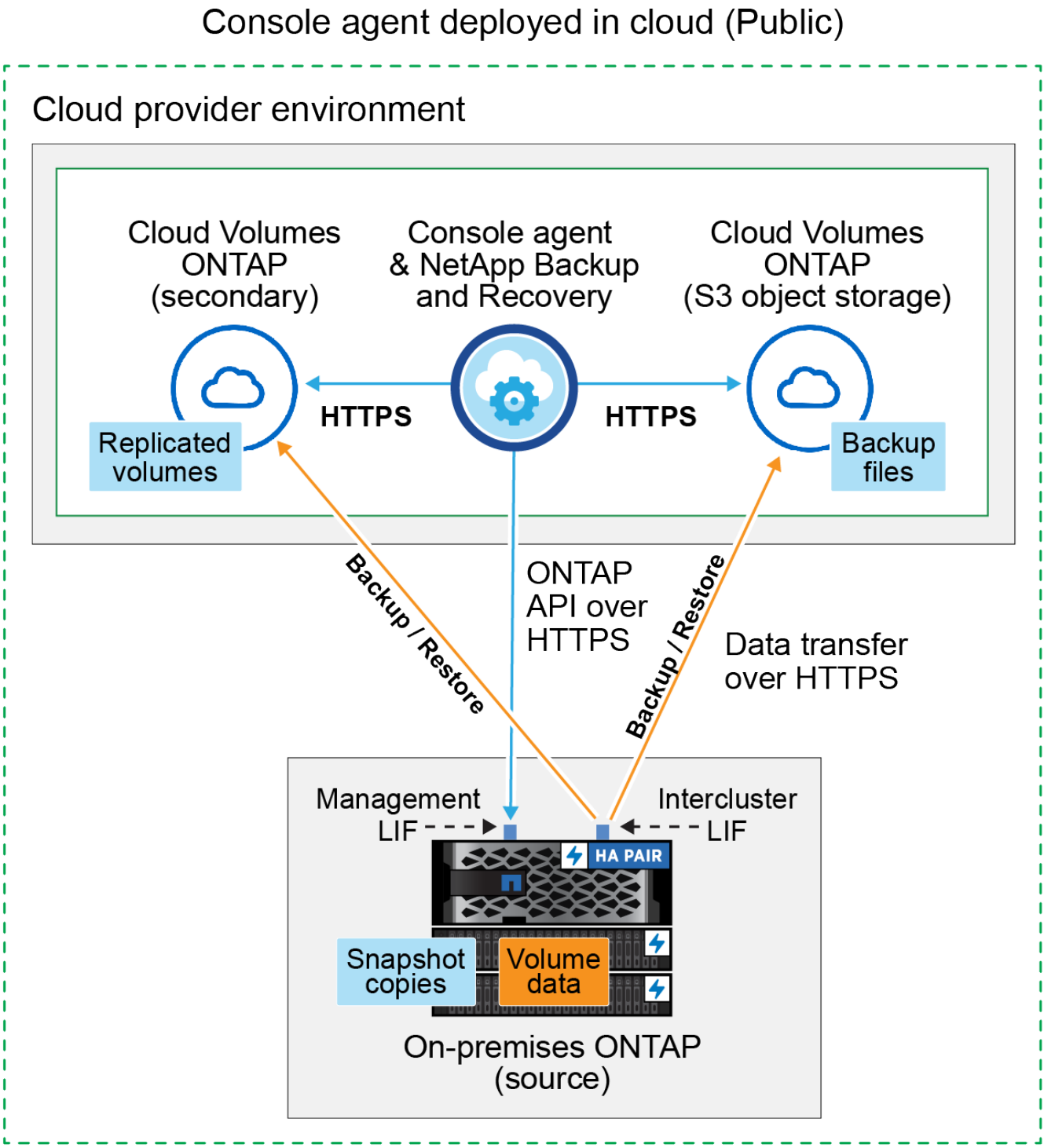
Esistono numerose configurazioni in cui è possibile creare backup su un bucket S3 su un sistema ONTAP . Di seguito sono illustrati due scenari.

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario in locale su un sistema ONTAP in locale configurato per S3 e le connessioni che è necessario preparare tra di essi. Mostra anche una connessione a un sistema ONTAP secondario nella stessa posizione locale per replicare i volumi.



Quando l'agente Console e il sistema ONTAP primario in sede vengono installati in una posizione in sede senza accesso a Internet (una distribuzione in modalità "privata"), il sistema ONTAP S3 deve trovarsi nello stesso data center in sede.

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario on-premise su un sistema Cloud Volumes ONTAP configurato per S3 e le connessioni che è necessario preparare tra di essi. Mostra anche una connessione a un sistema Cloud Volumes ONTAP secondario nello stesso ambiente del provider cloud per replicare i volumi.



In questo scenario, l'agente Console dovrebbe essere distribuito nello stesso ambiente del provider cloud in cui sono distribuiti i sistemi Cloud Volumes ONTAP .

Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità Console. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Quando si esegue il backup dei dati su ONTAP S3, è necessario che un agente Console sia disponibile in sede o nel cloud. Sarà necessario installare un nuovo agente Console oppure assicurarsi che l'agente Console attualmente selezionato risieda in una di queste posizioni. L'agente Console locale può essere installato in un sito con o senza accesso a Internet.

- "Scopri di più sugli agenti della console"
- "Installa l'agente Console nel tuo ambiente cloud"
- "Installazione dell'agente Console su un host Linux con accesso a Internet"
- "Installazione dell'agente Console su un host Linux senza accesso a Internet"
- "Passaggio tra gli agenti della console"

Preparare i requisiti di rete dell'agente della console

Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:

- Una connessione HTTPS sulla porta 443 al server ONTAP S3
- Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP di origine
- Una connessione Internet in uscita sulla porta 443 verso NetApp Backup and Recovery (non necessaria quando l'agente Console è installato in un sito "oscuro")

Considerazioni sulla modalità privata (sito oscuro)

La funzionalità NetApp Backup and Recovery è integrata nell'agente Console. Se installato in modalità privata, sarà necessario aggiornare periodicamente il software dell'agente della console per accedere alle nuove funzionalità. Controlla il"NetApp Backup and Recovery: novità" per vedere le nuove funzionalità di ogni versione NetApp Backup and Recovery . Quando vuoi utilizzare le nuove funzionalità, segui i passaggi per "aggiornare il software dell'agente della console" .

Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS standard, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel cloud. Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket ONTAP S3 in cui vengono archiviati i backup.

Verificare i requisiti della licenza

Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai acquistare e attivare una licenza NetApp Backup and Recovery BYOL da NetApp. La licenza è per il backup e il ripristino su storage di oggetti: non è necessaria alcuna licenza per creare snapshot o volumi replicati. Questa licenza è per l'account e può essere utilizzata su più sistemi.

Avrai bisogno del numero di serie di NetApp che ti consentirà 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 durante il backup dei file su ONTAP S3.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .

- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario assicurarsi che i seguenti requisiti siano soddisfatti sul sistema che si connette all'archiviazione di oggetti.

- Quando si utilizza un'architettura di backup fan-out, le impostazioni devono essere configurate sul sistema di archiviazione *primario*.
- Quando si utilizza un'architettura di backup a cascata, le impostazioni devono essere configurate sul sistema di archiviazione *secondario*.

  "Scopri di più sui tipi di architettura di backup".

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster ONTAP avvia una connessione HTTPS tramite una porta specificata dall'utente dal LIF intercluster al server ONTAP S3 per le operazioni di backup e ripristino. La porta è configurabile durante la configurazione del backup.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia

mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF intercluster dei nodi sono in grado di accedere all'archivio oggetti (non necessario quando l'agente Console è installato in un sito "dark").
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se si utilizza uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere all'archiviazione degli oggetti.
- Se necessario, aggiornare le regole del firewall per consentire le connessioni del servizio NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta specificata (in genere la porta 443) e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.

Prepara ONTAP S3 come destinazione di backup

È necessario abilitare un server di archiviazione oggetti Simple Storage Service (S3) nel cluster ONTAP che si prevede di utilizzare per i backup di archiviazione oggetti. Vedi il "Documentazione ONTAP S3" per i dettagli.

Nota: è possibile aggiungere questo cluster alla pagina **Sistemi** della console, ma non viene identificato come server di archiviazione oggetti S3 e non è possibile trascinare un sistema sorgente su questo sistema S3 per avviare l'attivazione del backup.

Questo sistema ONTAP deve soddisfare i seguenti requisiti.

Versioni ONTAP supportate

Per i sistemi ONTAP locali 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 al proprio storage ONTAP S3. "Per i dettagli, consultare la documentazione ONTAP S3" .

Quando si configura 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 a NetApp Backup and Recovery di autenticarsi e accedere ai bucket ONTAP S3 utilizzati per archiviare i backup. Le chiavi sono necessarie affinché 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",
"s3:GetBucketLocation"
```

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia e le policy di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:
    - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.
    - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona l'opzione **Azioni (…)** e seleziona **Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup nell'archiviazione oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, repliche e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina

Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criteri di snapshot, criteri di replica, criteri di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

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

- Opzioni di protezione: se si desidera implementare una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura: se si desidera utilizzare un'architettura di backup a fan-out o a cascata
- Criterio di snapshot locale
- Destinazione e politica di replicazione
- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:

- **Snapshot locali**: crea snapshot locali.
- **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
- **Backup**: esegue il backup dei volumi in un bucket su un sistema ONTAP configurato per S3.

2. **Architettura**: se hai scelto sia la replica che il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: i dati di backup fluiscono dal sistema primario a quello secondario e poi da quest'ultimo all'archivio oggetti.
   - **Fan out**: i dati di backup fluiscono dal sistema primario a quello secondario *e* dal sistema primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Se si desidera creare una policy personalizzata prima di attivare lo Snapshot, è possibile utilizzare System Manager o ONTAP CLI `snapmirror policy create` comando. Fare riferimento a .

   Per creare una policy personalizzata utilizzando Backup e Ripristino, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.

4. **Replica**: se hai selezionato **Replica**, imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato di destinazione (o gli aggregati per i volumi FlexGroup) e un prefisso o un suffisso che verrà aggiunto al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: Seleziona * ONTAP S3*.
   - **Impostazioni del provider**: immettere i dettagli del nome di dominio completo (FQDN) del server S3, la porta, la chiave di accesso e la chiave segreta degli utenti.

     La chiave di accesso e la chiave segreta servono all'utente creato per concedere al cluster ONTAP l'accesso al bucket S3.

   - **Networking**: seleziona lo spazio IP nel cluster ONTAP di origine in cui risiedono i volumi di cui vuoi eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita (non richiesto quando l'agente Console è installato in un sito "dark").

Selezionando lo spazio IP corretto si garantisce che NetApp Backup and Recovery possa impostare una connessione da ONTAP al tuo storage di oggetti ONTAP S3.

- **Criterio di backup**: seleziona un criterio di backup esistente o creane uno nuovo.

  È possibile creare una policy con System Manager o ONTAP CLI. Per creare una policy personalizzata utilizzando ONTAP CLI `snapmirror policy create` comando, fare riferimento a .

  Per creare una policy personalizzata utilizzando Backup e Ripristino, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
  - Seleziona **Crea**.

- **Esporta snapshot esistenti nell'archivio oggetti come file di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup. Se i criteri non corrispondono, i backup non verranno creati.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti negli snapshot.

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

Viene creato un bucket S3 nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse, e i file di backup vengono archiviati lì.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su StorageGRID con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP primari locali a un sistema di storage secondario e allo storage di oggetti nei tuoi sistemi NetApp StorageGRID .

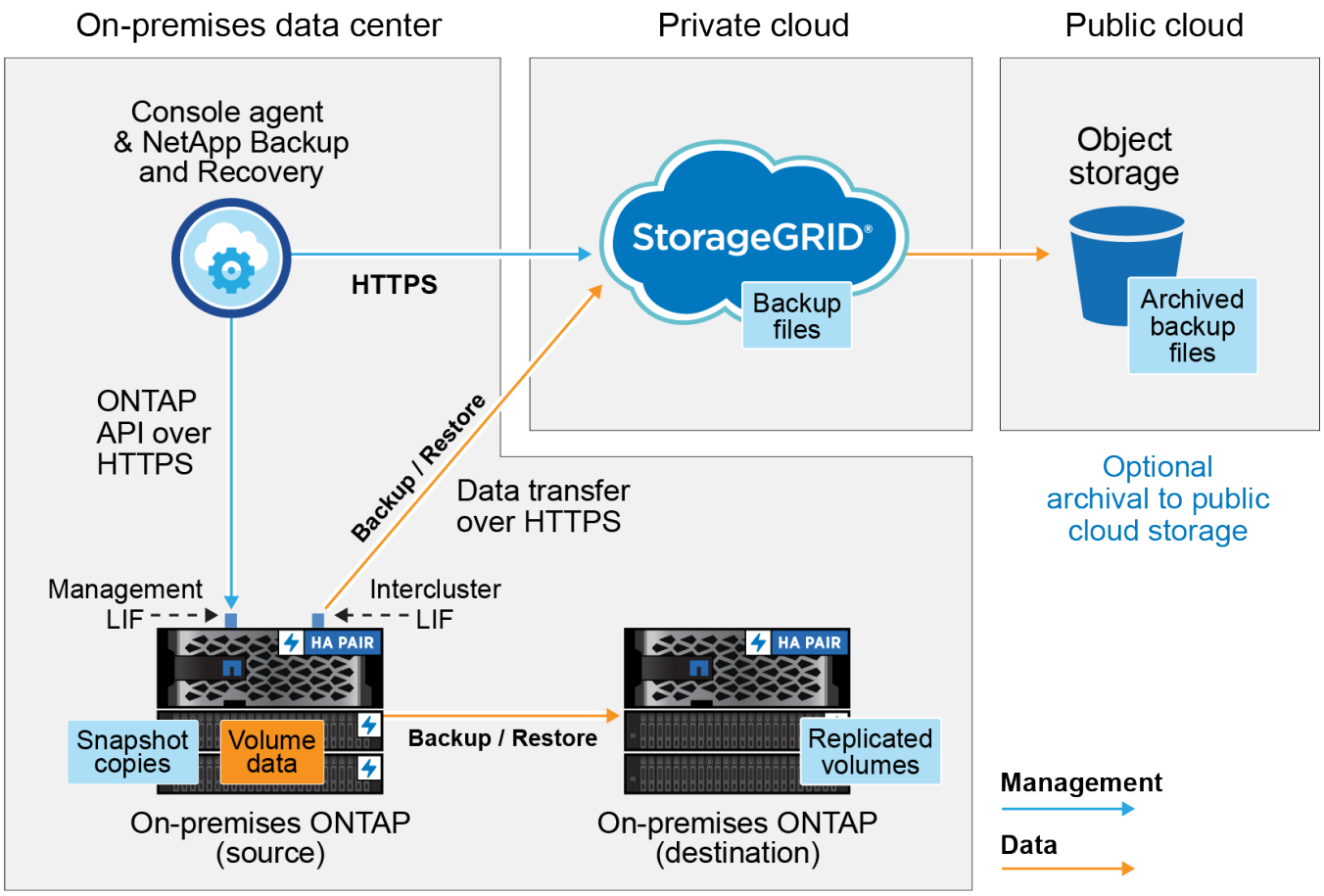
I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Identificare il metodo di connessione

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP locale su StorageGRID e le connessioni che è necessario preparare tra di essi.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario nella stessa posizione locale per replicare i volumi.



Quando l'agente Console e il sistema ONTAP locale vengono installati in una posizione locale senza accesso a Internet (un "dark site"), il sistema StorageGRID deve trovarsi nello stesso data center locale. L'archiviazione dei vecchi file di backup sul cloud pubblico non è supportata nelle configurazioni dark site.

Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità Console. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Quando si esegue il backup dei dati su StorageGRID, è necessario che un agente Console sia disponibile presso la propria sede. Sarà necessario installare un nuovo agente Console oppure assicurarsi che l'agente Console attualmente selezionato risieda in locale. L'agente Console può essere installato in un sito con o senza accesso a Internet.

- "Scopri di più sugli agenti della console"
- "Installazione dell'agente Console su un host Linux con accesso a Internet"
- "Installazione dell'agente Console su un host Linux senza accesso a Internet"
- "Passaggio tra gli agenti della console"

Preparare i requisiti di rete dell'agente della console

Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:

- Una connessione HTTPS sulla porta 443 al nodo gateway StorageGRID
- Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
- Una connessione Internet in uscita sulla porta 443 verso NetApp Backup and Recovery (non necessaria quando l'agente Console è installato in un sito "oscuro")

Considerazioni sulla modalità privata (sito oscuro)

- La funzionalità NetApp Backup and Recovery è integrata nell'agente Console. Se installato in modalità privata, sarà necessario aggiornare periodicamente il software dell'agente della console per accedere alle nuove funzionalità. Controlla il"NetApp Backup and Recovery: novità" per vedere le nuove funzionalità di ogni versione NetApp Backup and Recovery . Quando vuoi utilizzare le nuove funzionalità, segui i passaggi per "aggiornare il software dell'agente della console" .

  La nuova versione di NetApp Backup and Recovery , che include la possibilità di pianificare e creare snapshot e volumi replicati, oltre a creare backup nell'archiviazione di oggetti, richiede l'utilizzo della versione 3.9.31 o successiva dell'agente Console. Ti consigliamo quindi di scaricare questa versione più recente per gestire tutti i tuoi backup.

- Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel cloud. Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket StorageGRID in cui vengono archiviati i backup.

Verificare i requisiti della licenza

Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai acquistare e attivare una licenza NetApp Backup and Recovery BYOL da NetApp. Questa licenza è per l'account e può essere utilizzata su più sistemi.

Avrai bisogno del numero di serie di NetApp che ti consentirà 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 durante il backup dei file su StorageGRID.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password

dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .
- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di oggetti.

- Quando si utilizza un'architettura di backup fan-out, è necessario configurare le seguenti impostazioni sul sistema di archiviazione *primario*.
- Quando si utilizza un'architettura di backup a cascata, è necessario configurare le seguenti impostazioni sul sistema di archiviazione *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster ONTAP avvia una connessione HTTPS tramite una porta specificata dall'utente dal LIF 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 dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia mai, risponde e basta.
- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster. L'agente della Console deve risiedere presso la tua sede.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.
- I LIF intercluster dei nodi sono in grado di accedere all'archivio oggetti (non necessario quando l'agente Console è installato in un sito "dark").
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se si utilizza uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare un percorso

statico per accedere all'archiviazione degli oggetti.

- Se necessario, aggiornare le regole del firewall per consentire le connessioni del servizio NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta specificata (in genere la porta 443) e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione 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 sicurezza predefinito.

Prepara StorageGRID come destinazione di backup

StorageGRID deve soddisfare i seguenti requisiti. Vedi il "Documentazione StorageGRID" per maggiori informazioni.

Per i dettagli sui requisiti di DataLock e Ransomware Resilience per StorageGRID, fare riferimento a"Opzioni di policy di backup su oggetto" .

Versioni StorageGRID supportate

StorageGRID 10.3 e versioni successive sono supportati.

Per utilizzare DataLock & Ransomware Resilience per i backup, i sistemi StorageGRID devono eseguire la versione 11.6.0.3 o successiva.

Per suddividere i backup più vecchi in archivi cloud, i sistemi StorageGRID devono eseguire la versione 11.3 o successiva. Inoltre, i sistemi StorageGRID devono essere rilevati nella pagina **Sistemi** della console.

Per l'archiviazione degli utenti è necessario l'accesso IP del nodo amministratore.

L'accesso IP al gateway è sempre necessario.

Credenziali S3

Per controllare l'accesso al tuo storage StorageGRID , devi aver creato un account tenant S3. "Per i dettagli, consultare la documentazione di StorageGRID" .

Quando si configura 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 a NetApp Backup and Recovery di autenticare e accedere ai bucket StorageGRID utilizzati per archiviare i backup. Le chiavi sono

necessarie affinché 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"
```

Versionamento degli oggetti

Non è necessario abilitare manualmente il controllo delle versioni degli oggetti StorageGRID sul bucket di archiviazione degli oggetti.

Preparati ad archiviare i vecchi file di backup su un archivio cloud pubblico

L'archiviazione dei file di backup più vecchi consente di risparmiare denaro, utilizzando una classe di archiviazione meno costosa per i backup di cui potresti non aver bisogno. StorageGRID è una soluzione on-premise (cloud privato) che non fornisce archiviazione, ma consente di spostare i file di backup più vecchi nell'archiviazione su cloud pubblico. Quando utilizzati in questo modo, i dati archiviati su cloud storage o ripristinati da cloud storage vengono trasferiti tra StorageGRID e cloud storage: la Console non è coinvolta 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 la versione 11.4 o successiva.
- Il tuo StorageGRID deve essere "scoperto e disponibile nella Console" .

Requisiti Amazon S3

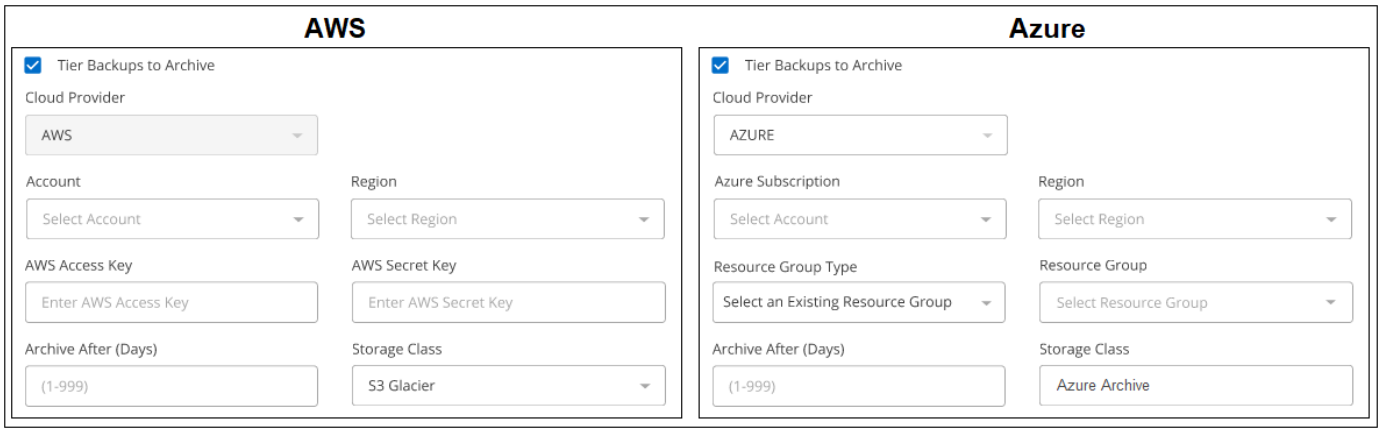
- Sarà necessario registrarsi per un account Amazon S3 per lo spazio di archiviazione in cui verranno archiviati i backup.
- È possibile scegliere di suddividere i backup in livelli su AWS S3 Glacier o S3 Glacier Deep Archive. "Scopri di più sui livelli di archiviazione AWS" .
- StorageGRID dovrebbe avere accesso completo al bucket(`s3:*`); tuttavia, se ciò non è possibile, la policy del 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

- Sarà necessario sottoscrivere un abbonamento Azure per lo spazio di archiviazione in cui verranno archiviati i backup.
- La procedura guidata di attivazione consente di utilizzare un gruppo di risorse esistente per gestire il contenitore BLOB in cui verranno archiviati i backup oppure è possibile creare un nuovo gruppo di risorse.

Quando definisci le impostazioni di archiviazione per la policy di backup del tuo cluster, dovrai immettere le credenziali del tuo provider cloud e selezionare la classe di archiviazione che desideri utilizzare. NetApp Backup and Recovery crea il bucket cloud quando si attiva il backup per il cluster. Di seguito sono riportate le informazioni necessarie per l'archiviazione AWS e Azure.



Le impostazioni dei criteri di archiviazione selezionate genereranno un criterio di gestione del ciclo di vita delle informazioni (ILM) in StorageGRID e aggiungeranno le impostazioni come "regole".

- Se è già presente una policy ILM attiva, verranno aggiunte nuove regole alla policy ILM per spostare i dati al livello di archivio.
- Se esiste una policy ILM nello stato "proposto", non sarà possibile creare e attivare una nuova policy ILM. "Scopri di più sulle policy e le regole StorageGRID ILM" .

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione dei backup è presente come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell'archivio oggetti.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona l'opzione **Azioni (…)** e seleziona **Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup nell'archiviazione oggetti).

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

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (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 SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

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

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.

   - Facoltativamente, filtra 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 (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.

2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

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

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: se hai scelto sia la replica che il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal primario al secondario e poi dal secondario all'archiviazione degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

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

   > Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     > Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

- Inserisci il nome della policy.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: Seleziona * StorageGRID*.
   - **Impostazioni del 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.

   - **Networking**: selezionare lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita (non richiesto quando l'agente Console è installato in un sito "dark").

     Selezionando lo spazio IP corretto si garantisce che NetApp Backup and Recovery possa impostare una connessione da ONTAP al tuo storage di oggetti StorageGRID .

   - **Criterio di backup**: seleziona un criterio di backup su archiviazione oggetti esistente o creane uno.

     Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .

       Se il tuo cluster utilizza ONTAP 9.11.1 o versione successiva, puoi scegliere di proteggere i tuoi backup da eliminazioni e attacchi ransomware configurando *DataLock e Ransomware Resilience*. *DataLock* protegge i file di backup da modifiche o eliminazioni, mentre *Ransomware Resilience* esegue la scansione dei file di backup per cercare prove di un attacco ransomware nei file di backup.

     - Seleziona **Crea**.

     Se il cluster utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o versione successiva, è possibile scegliere di suddividere i backup più vecchi in livelli di archivio cloud pubblico dopo un certo numero di giorni. Il supporto attuale riguarda i livelli di archiviazione AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. Scopri come configurare i tuoi sistemi per questa funzionalità .

   - **Backup a livelli su cloud pubblico**: seleziona il provider cloud su cui desideri eseguire il backup a livelli e inserisci i dettagli del provider.

     Seleziona o crea un nuovo cluster StorageGRID . Per i dettagli sulla creazione di un cluster StorageGRID in modo che la Console possa rilevarlo, fare riferimento a "Documentazione

StorageGRID" .

- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti negli snapshot.

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

Viene creato un bucket S3 nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse, e i file di backup vengono archiviati lì.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

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

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Migrare i volumi utilizzando SnapMirror su Cloud Resync in NetApp Backup and Recovery

La funzionalità SnapMirror to Cloud Resync di NetApp Backup and Recovery semplifica la protezione e la continuità dei dati durante le migrazioni dei volumi negli ambienti

NetApp . Quando un volume viene migrato tramite SnapMirror Logical Replication (LRSE) da una distribuzione NetApp locale a un'altra o a una soluzione basata su cloud come Cloud Volumes ONTAP, SnapMirror to Cloud Resync garantisce che i backup cloud esistenti rimangano intatti e operativi.

Questa funzionalità elimina la necessità di un processo di riconfigurazione della baseline e consente di continuare i backup dopo la migrazione. Questa funzionalità è utile negli scenari di migrazione del carico di lavoro, supportando sia FlexVols che FlexGroups ed è disponibile a partire dalla versione 9.16.1 ONTAP .

Questa funzionalità è disponibile a partire dalla versione 4.0.3 NetApp Backup and Recovery, rilasciata a maggio 2025.

SnapMirror to Cloud Resync mantiene la continuità del backup tra gli ambienti, semplificando la gestione dei dati in configurazioni ibride e multi-cloud.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster ONTAP di destinazione deve eseguire ONTAP versione 9.16.1 o successiva.
- Il vecchio cluster ONTAP di origine deve essere protetto tramite NetApp Backup and Recovery.
- La funzionalità SnapMirror to Cloud Resync è disponibile a partire dalla versione 4.0.3 NetApp Backup and Recovery, rilasciata a maggio 2025.
- Assicurarsi che l'ultimo backup nell'archivio oggetti sia lo snapshot comune tra la vecchia origine, la nuova origine e l'archivio oggetti. Non utilizzare uno snapshot comune più vecchio dell'ultimo snapshot sottoposto a backup nell'archivio oggetti.
- Sia i criteri snapshot che SnapMirror utilizzati sul vecchio cluster ONTAP devono essere creati sul nuovo cluster ONTAP prima di avviare l'operazione di risincronizzazione. Se si utilizza un criterio nel processo di risincronizzazione, è necessario anche creare tale criterio. L'operazione di risincronizzazione non crea policy.
- Assicurarsi che il criterio SnapMirror applicato alla relazione SnapMirror del volume di migrazione includa la stessa etichetta utilizzata dalla relazione cloud. Per evitare problemi, utilizzare la policy che gestisce un mirror esatto del volume e di tutti gli snapshot.

Al momento, SnapMirror su Cloud Resync dopo le migrazioni tramite i metodi SVM-Migrate, SVM-DR o Head Swap non è supportato.

Come funziona NetApp Backup and Recovery SnapMirror to Cloud Resync

Se si completa un aggiornamento tecnico o si migrano volumi da un cluster ONTAP a un altro, è importante che i backup continuino a funzionare senza interruzioni. NetApp Backup and Recovery SnapMirror to Cloud Resync aiuta in questo, garantendo che i backup cloud rimangano coerenti anche dopo una migrazione del volume.

Ecco un esempio:

Immagina di avere un volume locale denominato Vol1a. Questo volume contiene tre istantanee: S1, S2 e S3. Questi snapshot sono punti di ripristino. Il backup di Vol1 sul cloud avviene tramite SnapMirror to Cloud (SM-

C), ma solo S1 e S2 sono presenti nell'archivio oggetti.

Ora vuoi migrare Vol1 su un altro cluster ONTAP . Per fare ciò, si crea una relazione SnapMirror Logical Replication (LRSE) su un nuovo volume cloud denominato Vol1b. In questo modo vengono trasferiti tutti e tre gli snapshot (S1, S2 e S3) da Vol1a a Vol1b.

Una volta completata la migrazione, la configurazione sarà la seguente:

- La relazione SM-C originale (Vol1a → Archivio oggetti) viene eliminata.
- Viene eliminata anche la relazione LRSE (Vol1a → Vol1b).
- Vol1b è ora il tuo volume attivo.

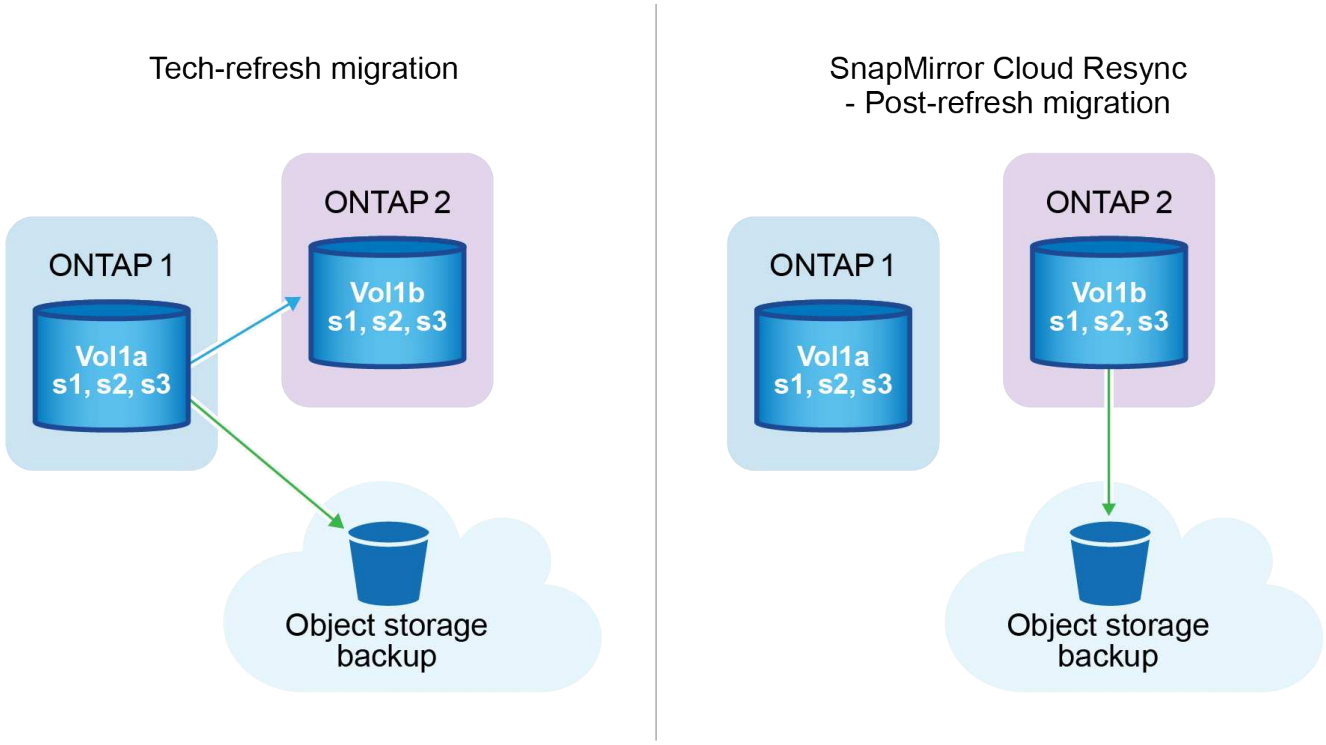
A questo punto, si desidera continuare a eseguire il backup di Vol1b sullo stesso endpoint cloud. Ma invece di avviare un backup completo da zero (che richiederebbe tempo e risorse), puoi usare SnapMirror per Cloud Resync.

Ecco come funziona la risincronizzazione:

- Il sistema verifica la presenza di uno snapshot comune tra Vol1a e Object Store. In questo caso, entrambi hanno S2.
- Grazie a questa istantanea condivisa, il sistema deve trasferire solo le modifiche incrementali tra S2 e S3.

Ciò significa che solo i nuovi dati aggiunti dopo S2 vengono inviati all'archivio oggetti, non l'intero volume.

Questo processo impedisce backup duplicati, consente di risparmiare larghezza di banda e mantiene i backup in esecuzione dopo la migrazione.



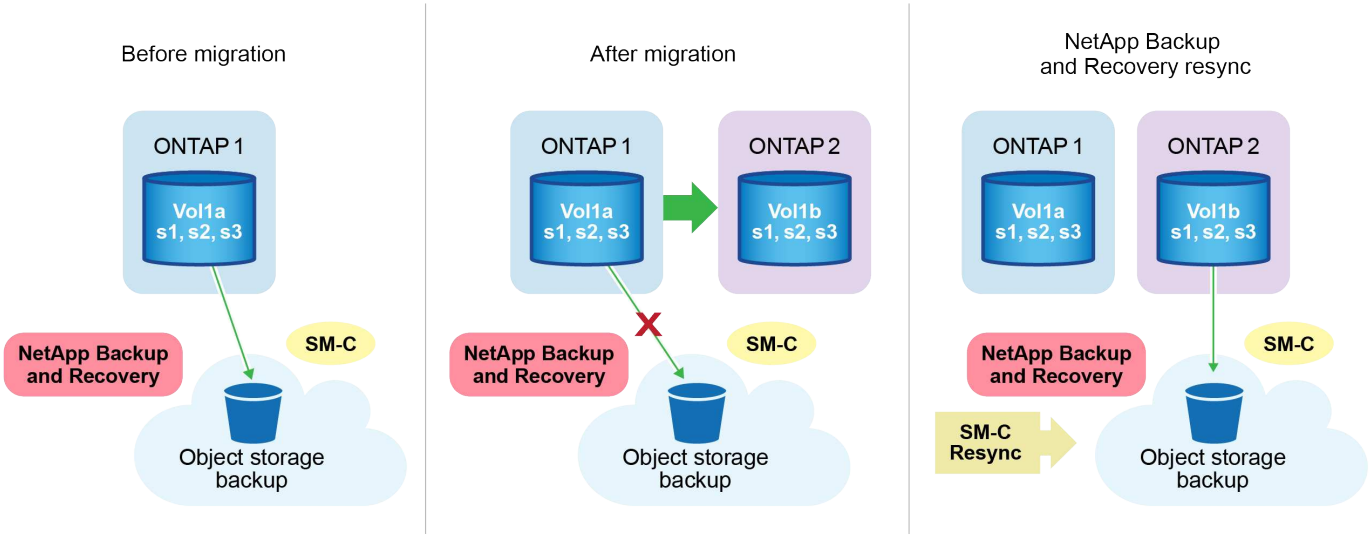
Note sulla procedura

- Le migrazioni e gli aggiornamenti tecnologici non vengono eseguiti tramite NetApp Backup and Recovery. Dovrebbero essere eseguiti da un team di servizi professionali o da un amministratore di storage qualificato.
- Un team di migrazione NetApp crea la relazione SnapMirror tra i cluster ONTAP di origine e di destinazione per agevolare lo spostamento dei volumi.
- Assicurarsi che la migrazione durante un aggiornamento tecnologico sia basata sulla migrazione basata su SnapMirror.

Come migrare i volumi utilizzando SnapMirror su Cloud Resync

La migrazione dei volumi tramite SnapMirror su Cloud Resync prevede i seguenti passaggi principali, ciascuno descritto più dettagliatamente di seguito:

- **Seguire una checklist pre-migrazione**: prima di iniziare la migrazione, un team NetApp Tech Refresh verifica che siano soddisfatti i seguenti prerequisiti per evitare la perdita di dati e garantire un processo di migrazione senza intoppi.
- **Seguire una checklist post-migrazione**: dopo la migrazione, un team NetApp Tech Refresh verifica che vengano completati i seguenti passaggi per stabilire la protezione e preparare la risincronizzazione.
- **Eseguire un'operazione di risincronizzazione SnapMirror a Cloud**: dopo la migrazione, un team NetApp Tech Refresh esegue un'operazione di risincronizzazione SnapMirror a Cloud per riprendere i backup su cloud dai volumi appena migrati.



Seguire una checklist pre-migrazione

Prima della migrazione, il team NetApp Tech Refresh verifica questi prerequisiti per evitare la perdita di dati e garantire un processo senza intoppi.

1. Assicurarsi che tutti i volumi da migrare siano protetti tramite NetApp Backup and Recovery.
2. Registra gli UUID delle istanze del volume. Annotare gli UUID delle istanze di tutti i volumi prima di avviare la migrazione. Questi identificatori sono fondamentali per le successive operazioni di mappatura e risincronizzazione.
3. Eseguire uno snapshot finale di ciascun volume per preservare lo stato più recente, prima di eliminare

qualsiasi relazione SnapMirror .

4. Criteri SnapMirror del documento. Registrare la policy SnapMirror attualmente associata alla relazione di ciascun volume. Questo sarà necessario in seguito durante il processo di risincronizzazione da SnapMirror a Cloud.
5. Eliminare le relazioni di SnapMirror Cloud con l'archivio oggetti.
6. Creare una relazione SnapMirror standard con il nuovo cluster ONTAP per migrare il volume al nuovo cluster ONTAP di destinazione.

Seguire una checklist post-migrazione

Dopo la migrazione, un team NetApp Tech Refresh verifica che vengano completati i seguenti passaggi per stabilire la protezione e preparare la risincronizzazione.

1. Registra i nuovi UUID delle istanze di volume di tutti i volumi migrati nel cluster ONTAP di destinazione.
2. Verificare che tutti i criteri SnapMirror richiesti disponibili nel vecchio cluster ONTAP siano configurati correttamente nel nuovo cluster ONTAP .
3. Aggiungere il nuovo cluster ONTAP come sistema nella pagina **Sistemi** della Console.

> Deve essere utilizzato l'UUID dell'istanza del volume, non l'ID del volume. L'UUID dell'istanza del volume è un identificatore univoco che rimane coerente durante le migrazioni, mentre l'ID del volume può cambiare dopo la migrazione.

Eseguire una risincronizzazione SnapMirror su Cloud

Dopo la migrazione, un team NetApp Tech Refresh esegue un'operazione SnapMirror to Cloud Resync per riprendere i backup cloud dai volumi appena migrati.

1. Aggiungere il nuovo cluster ONTAP come sistema nella pagina **Sistemi** della Console.
2. Consultare la pagina NetApp Backup and Recovery Volumes per assicurarsi che i dettagli del vecchio sistema di origine siano disponibili.
3. Dalla pagina NetApp Backup and Recovery Volumes, seleziona **Impostazioni di backup**.
   - Nella pagina Impostazioni di backup, seleziona **Visualizza tutto**.
   - Dal menu Azioni … a destra della *nuova* origine, seleziona **Risincronizza backup**.
4. Nella pagina del sistema di risincronizzazione, procedere come segue:
   a. **Nuovo sistema sorgente**: immettere il nuovo cluster ONTAP in cui sono stati migrati i volumi.
   b. **Archivio oggetti di destinazione esistente**: selezionare l'archivio oggetti di destinazione che contiene i backup del vecchio sistema di origine.
5. Selezionare **Scarica modello CSV** per scaricare il foglio Excel dei dettagli di risincronizzazione. Utilizzare questo foglio per immettere i dettagli dei volumi da migrare. Nel file CSV, inserisci i seguenti dettagli:
   - Il vecchio UUID dell'istanza del volume dal cluster di origine
   - Il nuovo UUID dell'istanza del volume dal cluster di destinazione
   - Criterio SnapMirror da applicare alla nuova relazione.
6. Selezionare **Carica** in **Carica dettagli mapping volume** per caricare il foglio CSV completato nell'interfaccia utente NetApp Backup and Recovery .

Deve essere utilizzato l'UUID dell'istanza del volume, non l'ID del volume. L'UUID dell'istanza del volume è un identificatore univoco che rimane coerente durante le migrazioni, mentre l'ID del volume può cambiare dopo la migrazione.

7. Immettere le informazioni di configurazione del provider e della rete necessarie per l'operazione di risincronizzazione.
8. Selezionare **Invia** per avviare il processo di convalida.

   NetApp Backup and Recovery verifica che ogni volume selezionato per la risincronizzazione sia lo snapshot più recente e disponga di almeno uno snapshot comune. Ciò garantisce che i volumi siano pronti per l'operazione SnapMirror to Cloud Resync.

9. Esaminare i risultati della convalida, inclusi i nuovi nomi dei volumi di origine e lo stato di risincronizzazione per ciascun volume.
10. Verificare l'idoneità del volume. Il sistema verifica se i volumi sono idonei per la risincronizzazione. Se un volume non è idoneo, significa che non si tratta dell'ultimo snapshot oppure non è stato trovato alcun snapshot comune.

    Per garantire che i volumi rimangano idonei per l'operazione SnapMirror su Cloud Resync, eseguire uno snapshot finale di ciascun volume prima di eliminare qualsiasi relazione SnapMirror durante la fase di pre-migrazione. In questo modo si preserva lo stato più recente dei dati.

11. Selezionare **Risincronizzazione** per avviare l'operazione di risincronizzazione. Il sistema utilizza lo snapshot più recente e comune per trasferire solo le modifiche incrementali, garantendo la continuità del backup.
12. Monitorare il processo di risincronizzazione nella pagina Job Monitor.

Ripristinare i dati di configurazione di NetApp Backup and Recovery in un sito oscuro

Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, noto come *modalità privata*, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host dell'agente Console, è possibile distribuire un nuovo agente Console e ripristinare i dati critici NetApp Backup and Recovery .

Questa procedura si applica solo ai dati di volume ONTAP .

Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS con l'agente Console distribuito presso il provider cloud o sul proprio host connesso a Internet, il sistema esegue il backup e protegge tutti i dati di configurazione importanti nel cloud. Se riscontri un problema con l'agente Console, crea un nuovo agente Console e aggiungi i tuoi sistemi. I dettagli del backup vengono ripristinati automaticamente.

Esistono due tipi di dati sottoposti a backup:

- Database NetApp Backup and Recovery : contiene un elenco di tutti i volumi, file di backup, policy di backup e informazioni di configurazione.

- File di catalogo indicizzati: contengono indici dettagliati utilizzati per la funzionalità di ricerca e ripristino, che rendono le ricerche molto rapide ed efficienti quando si cercano dati di volume che si desidera ripristinare.

Questi dati vengono sottoposti a backup una volta al giorno a mezzanotte e vengono conservate al massimo 7 copie di ciascun file. Se l'agente Console gestisce più sistemi ONTAP locali, i file NetApp Backup and Recovery vengono archiviati nel bucket del sistema attivato per primo.

Nessun dato di volume viene mai incluso nel database NetApp Backup and Recovery o nei file del catalogo indicizzato.

Ripristina i dati NetApp Backup and Recovery su un nuovo agente Console

Se l'agente della console locale smette di funzionare, sarà necessario installare un nuovo agente della console e quindi ripristinare i dati di NetApp Backup and Recovery sul nuovo agente della console.

Per ripristinare il funzionamento del sistema NetApp Backup and Recovery, è necessario eseguire le seguenti operazioni:

- Installa un nuovo agente Console
- Ripristinare il database NetApp Backup and Recovery
- Ripristina i file del catalogo indicizzato
- Riscopri tutti i tuoi sistemi ONTAP on-premise e i sistemi StorageGRID nell'interfaccia utente NetApp Console

Dopo aver verificato il funzionamento del sistema, crea nuovi file di backup.

Cosa ti servirà

Sarà necessario accedere ai backup più recenti del database e dell'indice dal bucket StorageGRID o ONTAP S3 in cui sono archiviati i file di backup:

- File del database MySQL NetApp Backup and Recovery

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/` , e si chiama `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- File zip di backup del catalogo indicizzato

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/catalog_backup/` , e si chiama `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installa un nuovo agente Console su un nuovo host Linux locale

Quando si installa un nuovo agente Console, scaricare la stessa versione software dell'agente originale. Le modifiche apportate al database NetApp Backup and Recovery potrebbero impedire il funzionamento delle versioni software più recenti con i vecchi backup del database. Puoi "aggiornare il software dell'agente della console alla versione più recente dopo aver ripristinato il database di backup" .

1. "Installa l'agente Console su un nuovo host Linux locale"
2. Accedi alla Console utilizzando le credenziali utente amministratore appena create.

Ripristinare il database NetApp Backup and Recovery

1. Copiare il backup MySQL dalla posizione di backup al nuovo host dell'agente della console. Di seguito utilizzeremo il nome file di esempio "CBS_DB_Backup_23_05_2023.sql".
2. Copiare il backup nel contenitore Docker MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accedere alla shell del contenitore MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Nella shell del contenitore, distribuire "env".
5. Ti servirà la password del database MySQL, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il database MySQL NetApp Backup and Recovery utilizzando il seguente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verificare che il database MySQL NetApp Backup and Recovery sia stato ripristinato correttamente utilizzando i seguenti comandi SQL:

```
mysql -u root -p cloud_backup
```

8. Inserisci la password.

```
mysql> show tables;
mysql> select * from volume;
```

9. Assicurarsi che i volumi visualizzati siano gli stessi presenti nell'ambiente originale.

Ripristina i file del catalogo indicizzato

1. Copiare il file zip di backup del catalogo indicizzato (utilizzeremo il nome file di esempio "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") dalla posizione di backup al nuovo host

dell'agente della console nella cartella "/opt/application/netapp/cbs".

2. Decomprimere il file "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" utilizzando il seguente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Eseguire il comando **ls** per assicurarsi che sia stata creata la cartella "catalogdb1" con le sottocartelle "changes" e "snapshots".

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti i sistemi ONTAP on-prem"che erano disponibili nel tuo ambiente precedente. Ciò include il sistema ONTAP utilizzato come server S3.
2. "Scopri i tuoi sistemi StorageGRID".

Impostare i dettagli dell'ambiente StorageGRID

Aggiungere i dettagli del sistema StorageGRID associato ai sistemi ONTAP così come sono stati configurati nella configurazione originale dell'agente della console utilizzando "API NetApp Console" .

Le seguenti informazioni si applicano alle installazioni in modalità privata a partire da NetApp Console 3.9.xx. Per le versioni precedenti, utilizzare la seguente procedura: "DarkSite Cloud Backup: backup e ripristino di MySQL e catalogo indicizzato" .

Sarà necessario eseguire questi passaggi per ogni sistema che esegue il backup dei dati su StorageGRID.

1. Estrarre il token di autorizzazione utilizzando la seguente API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   Mentre l'indirizzo IP, il nome utente e le password sono valori personalizzati, il nome dell'account non lo è. Il nome dell'account è sempre "account-DARKSITE1". Inoltre, il nome utente deve essere formattato come indirizzo email.

   Questa API restituirà una risposta simile alla seguente. È possibile recuperare il token di autorizzazione come mostrato di seguito.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Estrarre l'ID di sistema e l'X-Agent-Id utilizzando l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Questa API restituirà una risposta simile alla seguente. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-agent-id*.


```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```


3. Aggiornare il database NetApp Backup and Recovery con i dettagli del sistema StorageGRID associato ai sistemi. Assicurarsi di immettere il nome di dominio completo di StorageGRID, nonché la chiave di accesso e la chiave di archiviazione come mostrato di seguito:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verificare le impostazioni NetApp Backup and Recovery

1. Selezionare ciascun sistema ONTAP e fare clic su **Visualizza backup** accanto al servizio Backup e ripristino nel pannello di destra.

   Dovresti vedere tutti i backup creati per i tuoi volumi.

2. Nella Dashboard di ripristino, nella sezione Cerca e ripristina, fai clic su **Impostazioni di indicizzazione**.

   Assicurarsi che i sistemi in cui era abilitata in precedenza la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Cerca e ripristina, esegui alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato sia stato completato correttamente.

Gestisci i backup per i tuoi sistemi ONTAP con NetApp Backup and Recovery

Con NetApp Backup and Recovery puoi gestire i backup per i tuoi sistemi Cloud Volumes ONTAP e ONTAP on-premise modificando la pianificazione dei backup, abilitando/disabilitando i backup dei volumi, sospendendo i backup, eliminando i backup, forzando l'eliminazione dei backup e molto altro. Ciò include tutti i tipi di backup, tra cui snapshot, volumi replicati e file di backup nell'archiviazione di oggetti. È anche possibile annullare la registrazione NetApp Backup and Recovery.

Non gestire o modificare i file di backup direttamente sui tuoi sistemi di archiviazione o dall'ambiente del tuo provider cloud. Ciò potrebbe danneggiare i file e dar luogo a una configurazione non supportata.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Visualizza lo stato di backup dei volumi nei tuoi sistemi

È possibile visualizzare un elenco di tutti i volumi attualmente sottoposti a backup nella dashboard di backup dei volumi. Ciò include tutti i tipi di backup, tra cui snapshot, volumi replicati e file di backup nell'archiviazione di oggetti. È anche possibile visualizzare i volumi nei sistemi di cui non è attualmente in corso il backup.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare il menu **Volumi** per visualizzare l'elenco dei volumi sottoposti a backup per i sistemi Cloud Volumes ONTAP e ONTAP locali.
3. Se stai cercando volumi specifici in determinati sistemi, puoi restringere l'elenco in base al sistema e al volume. È anche possibile utilizzare il filtro di ricerca oppure ordinare le colonne in base allo stile del volume (FlexVol o FlexGroup), al tipo di volume e altro ancora.

   Per visualizzare colonne aggiuntive (aggregati, stile di sicurezza (Windows o UNIX), criterio di snapshot, criterio di replica e criterio di backup), selezionare il segno più.

4. Controllare lo stato delle opzioni di protezione nella colonna "Protezione esistente". Le 3 icone stanno per "Snapshot locali", "Volumi replicati" e "Backup nell'archiviazione di oggetti".

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

Attiva il backup su volumi aggiuntivi in un sistema

Se hai attivato il backup solo su alcuni volumi di un sistema quando hai abilitato per la prima volta NetApp Backup and Recovery, puoi attivare i backup su volumi aggiuntivi in un secondo momento.

Passi

1. Dalla scheda **Volumi**, identifica il volume su cui desideri attivare i backup, seleziona il menu Azioni ••• alla fine della riga e seleziona **Attiva backup**.
2. Nella pagina *Definisci strategia di backup*, seleziona l'architettura di backup, quindi definisci i criteri e altri dettagli per snapshot locali, volumi replicati e file di backup. Consulta i dettagli per le opzioni di backup dai volumi iniziali attivati in questo sistema. Quindi seleziona **Avanti**.
3. Rivedere le impostazioni di backup per questo volume, quindi selezionare **Attiva backup**.

Modificare le impostazioni di backup assegnate ai volumi esistenti

È possibile modificare i criteri di backup assegnarti ai volumi esistenti a cui sono stati assegnati criteri. È possibile modificare i criteri per gli snapshot locali, i volumi replicati e i file di backup. Ogni nuovo snapshot, replica o criterio di backup che si desidera applicare ai volumi deve già esistere.

Modifica le impostazioni di backup su un singolo volume

Passi

1. Dalla scheda **Volumi**, identifica il volume su cui vuoi apportare modifiche ai criteri, seleziona il menu Azioni ••• alla fine della riga e seleziona **Modifica strategia di backup**.
2. Nella pagina *Modifica strategia di backup*, apportare modifiche ai criteri di backup esistenti per snapshot locali, volumi replicati e file di backup e selezionare **Avanti**.

   Se hai abilitato *DataLock e Ransomware Resilience* per i backup cloud nella policy di backup iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, vedrai solo le altre policy configurate con DataLock. Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, vedrai solo altri criteri di backup cloud che non hanno DataLock configurato.

3. Rivedere le impostazioni di backup per questo volume, quindi selezionare **Attiva backup**.

Modifica le impostazioni di backup su più volumi

Se si desidera utilizzare le stesse impostazioni di backup su più volumi, è possibile attivare o modificare le impostazioni di backup su più volumi contemporaneamente. È possibile selezionare volumi privi di impostazioni di backup, con solo impostazioni di snapshot, con solo impostazioni di backup su cloud e così via, e apportare modifiche in blocco su tutti questi volumi con diverse impostazioni di backup.

Quando si lavora con più volumi, tutti i volumi devono avere le seguenti caratteristiche comuni:

- stesso sistema
- stesso stile (volume FlexVol o FlexGroup)
- stesso tipo (volume di lettura-scrittura o di protezione dati)

Se sono abilitati più di cinque volumi per il backup, NetApp Backup and Recovery inizializza solo cinque volumi alla volta. Una volta completati, crea il batch successivo di cinque sotto-processi per avviare il set successivo e continua finché tutti i volumi non vengono inizializzati.

Passi

1. Dalla scheda **Volumi**, filtrare in base al sistema su 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…	Seleziona questo pulsante…
Gestisci le impostazioni di backup degli snapshot	**Gestisci snapshot locali**
Gestisci le impostazioni di backup della replica	**Gestisci replicazione**
Gestisci le impostazioni di backup sul cloud	**Gestisci backup**
Gestisci più tipi di impostazioni di backup. Questa opzione consente anche di modificare l'architettura di backup.	**Gestisci backup e ripristino**

4. Nella pagina di backup visualizzata, apportare modifiche ai criteri di backup esistenti per snapshot locali, volumi replicati o file di backup e selezionare **Salva**.

Se hai abilitato *DataLock e Ransomware Resilience* per i backup cloud nella policy di backup iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, vedrai solo le altre policy configurate con DataLock. Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, vedrai solo altri criteri di backup cloud che non hanno DataLock configurato.

Crea un backup manuale del volume in qualsiasi momento

È possibile creare un backup su richiesta in qualsiasi momento per acquisire lo stato corrente del volume. Questa opzione può essere utile se sono state apportate modifiche molto importanti a un volume e non si desidera attendere il successivo backup pianificato per proteggere i dati. È possibile utilizzare questa funzionalità anche per creare un backup di un volume di cui non è attualmente in corso il backup e di cui si desidera acquisire lo stato attuale.

È possibile creare uno snapshot ad hoc o un backup dell'oggetto di un volume. Non è possibile creare un volume replicato ad hoc.

Il nome del backup include la marca temporale, in modo da poter distinguere il backup su richiesta da altri backup pianificati.

Se hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery 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 sulla protezione da DataLock e Ransomware" .

Quando si crea un backup ad hoc, viene creato uno snapshot sul volume di origine. Poiché questo snapshot non fa parte di una normale pianificazione degli snapshot, non verrà disattivato. Una volta completato il backup, potrebbe essere necessario eliminare manualmente questo snapshot dal volume di origine. Ciò consentirà di liberare i blocchi correlati a questo snapshot. Il nome dello Snapshot inizierà con `cbs-snapshot-adhoc-` . "Scopri come eliminare uno Snapshot utilizzando ONTAP CLI" .

Il backup del volume su richiesta non è supportato sui volumi di protezione dati.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume e seleziona **Backup** > **Crea backup ad hoc**.

Nella colonna Stato backup per quel volume viene visualizzato "In corso" finché il backup non viene creato.

Visualizza l'elenco dei backup per ciascun volume

È possibile visualizzare l'elenco di tutti i file di backup esistenti per ciascun volume. Questa pagina mostra i dettagli sul volume di origine, sulla posizione di destinazione e sui dettagli del backup, come l'ultimo backup eseguito, la politica di backup corrente, le dimensioni del file di backup e altro ancora.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume sorgente e seleziona **Visualizza dettagli volume**.

   Vengono visualizzati i dettagli del volume e l'elenco degli snapshot.

2. Selezionare **Snapshot**, **Replica** o **Backup** per visualizzare l'elenco di tutti i file di backup per ciascun tipo di backup.

Eseguire una scansione ransomware su un backup del volume nell'archiviazione degli oggetti

NetApp Backup and Recovery analizza i file di backup per cercare prove di un attacco ransomware quando viene creato un backup su file oggetto e quando vengono ripristinati i dati da un file di backup. È inoltre possibile eseguire una scansione su richiesta in qualsiasi momento per verificare l'usabilità di uno specifico file di backup nell'archiviazione degli oggetti. Ciò può essere utile se si è verificato un problema di ransomware su un volume specifico e si desidera verificare che i backup per quel volume non siano interessati.

Questa funzionalità è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.11.1 o versione successiva e se è stato abilitato *DataLock e Ransomware Resilience* nel criterio di backup su oggetto.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume sorgente e seleziona **Visualizza dettagli volume**.

   Vengono visualizzati i dettagli del volume.

2. Selezionare **Backup** per visualizzare l'elenco dei file di backup nell'archivio oggetti.
3. Selezionare••• per il file di backup del volume che vuoi analizzare per individuare ransomware e clicca su **Analizza ransomware**.

   La colonna Resilienza 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.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume sorgente e selezionare l'opzione **Replica**. Puoi vedere tutte le opzioni disponibili.
2. Selezionare l'azione di replicazione che si desidera eseguire.

   La tabella seguente 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.
Aggiorna replica	Avvia un trasferimento incrementale per aggiornare il volume di destinazione da sincronizzare con il volume di origine.
Sospendi replicazione	Sospendi il trasferimento incrementale degli snapshot per aggiornare il volume di destinazione. È possibile riprendere in seguito se si desidera riavviare gli aggiornamenti incrementali.

Azione	Descrizione
Interrompere la replicazione	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 in genere utilizzata quando il volume di origine non può gestire i dati a causa di eventi quali danneggiamento dei dati, eliminazione accidentale o stato offline.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["Scopri come configurare un volume di destinazione per l'accesso ai dati e riattivare un volume di origine nella documentazione ONTAP"^]
Interrompere la replicazione	Disabilita i backup di questo volume sul sistema di destinazione e disabilita anche la possibilità di ripristinare un volume. Tutti i backup esistenti non verranno eliminati. Ciò non elimina 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 viene sovrascritto dal contenuto del volume di destinazione. Questa funzione è utile quando si desidera riattivare un volume sorgente che è andato offline. Tutti i dati scritti sul volume di origine originale tra l'ultima replica dei dati e il momento in cui il volume di origine è stato disabilitato 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, ovvero non lo rende di lettura/scrittura. Questa azione elimina anche la relazione peer del cluster e la relazione peer della VM di archiviazione (SVM), se non sono presenti altre relazioni di protezione dei dati tra i sistemi.

Risultato

Dopo aver selezionato un'azione, la Console aggiorna la relazione.

Modifica una policy di backup su cloud esistente

È possibile modificare gli attributi di un criterio di backup attualmente applicato ai volumi di un sistema. La modifica della policy di backup influisce su tutti i volumi esistenti che utilizzano la policy.

- Se hai abilitato *DataLock e Ransomware Resilience* nella policy iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, tutte le policy modificate devono essere configurate con la stessa impostazione DataLock (Governance o Compliance). Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, non puoi abilitare 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 NetApp Backup and Recovery, quel livello sarà l'unico livello di archiviazione disponibile quando si modificano le policy di backup. Se non hai selezionato alcun livello di archivio nella tua prima policy di backup, *S3 Glacier* sarà la tua unica opzione di archiviazione quando modifichi una policy.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona ••• per il sistema in cui si desidera modificare le impostazioni dei criteri e selezionare **Gestisci criteri**.
3. Dalla pagina *Gestisci criteri*, seleziona **Modifica** per il criterio di backup che desideri modificare in quel sistema.

4. Dalla pagina *Modifica policy*, seleziona la freccia rivolta verso il basso per espandere la sezione *Etichette e conservazione* per modificare la pianificazione e/o la conservazione del backup, quindi seleziona **Salva**.

   Se il cluster esegue ONTAP 9.10.1 o versione successiva, è anche possibile abilitare o disabilitare la suddivisione in livelli dei backup nell'archiviazione dopo un certo numero di giorni.

"Scopri di più sull'utilizzo dell'archiviazione AWS".

"Scopri di più sull'utilizzo dell'archiviazione di Azure".

"Scopri di più sull'utilizzo dell'archiviazione di Google". (Richiede ONTAP 9.12.1.)

+ Tieni presente che tutti i file di backup che sono stati suddivisi in livelli di archiviazione vengono lasciati in quel livello se interrompi la suddivisione dei backup in archivi: non vengono automaticamente spostati di nuovo nel livello standard. Solo i nuovi backup dei volumi risiederanno nel livello standard.

Aggiungi una nuova policy di backup su cloud

Quando si abilita NetApp Backup and Recovery per un sistema, tutti i volumi inizialmente selezionati vengono sottoposti a backup utilizzando la policy di backup predefinita definita. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi del punto di ripristino (RPO) diversi, è possibile creare criteri aggiuntivi per quel cluster e assegnarli ad altri volumi.

Se si desidera applicare una nuova policy di backup a determinati volumi di un sistema, è necessario prima aggiungere la policy di backup al sistema. Allora puoiapplicare la policy ai volumi in quel sistema .

- Se hai abilitato *DataLock e Ransomware Resilience* nella policy iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, tutte le policy aggiuntive che crei devono essere configurate con la stessa impostazione DataLock (Governance o Compliance). Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, non puoi 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 NetApp Backup and Recovery, quel livello sarà l'unico livello di archiviazione disponibile per le future policy di backup per quel cluster. Se non hai selezionato alcun livello di archivio nella tua prima policy di backup, *S3 Glacier* sarà la tua unica opzione di archiviazione per le policy future.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona••• per il sistema in cui si desidera aggiungere la nuova policy e selezionare **Gestisci policy**.
3. Dalla pagina *Gestisci criteri*, seleziona **Aggiungi nuovo criterio**.
4. Dalla pagina *Aggiungi nuova policy*, seleziona la freccia rivolta verso il basso per espandere la sezione *Etichette e conservazione* per definire la pianificazione e la conservazione del backup, quindi seleziona **Salva**.

   Se il cluster esegue ONTAP 9.10.1 o versione successiva, è anche possibile abilitare o disabilitare la suddivisione in livelli dei backup nell'archiviazione dopo un certo numero di giorni.

"Scopri di più sull'utilizzo dell'archiviazione AWS".

"Scopri di più sull'utilizzo dell'archiviazione di Azure".

"Scopri di più sull'utilizzo dell'archiviazione di Google". (Richiede ONTAP 9.12.1.)

Elimina i backup

NetApp Backup and Recovery consente di eliminare un singolo file di backup, eliminare tutti i backup per un volume o eliminare tutti i backup di tutti i volumi in un sistema. Potresti voler eliminare tutti i backup se non ne hai più bisogno o se hai eliminato il volume di origine e vuoi rimuovere tutti i backup.

Non è possibile eliminare i file di backup bloccati tramite DataLock e la protezione Ransomware. L'opzione "Elimina" non sarà disponibile nell'interfaccia utente se hai selezionato uno o più file di backup bloccati.

> Se si prevede di eliminare un sistema o un cluster che dispone di backup, è necessario eliminare i backup **prima** di eliminare il sistema. NetApp Backup and Recovery non elimina automaticamente i backup quando si elimina un sistema e attualmente non è presente alcun supporto nell'interfaccia utente per eliminare i backup dopo l'eliminazione del sistema. Continuerai a pagare i costi di archiviazione degli oggetti per tutti i backup rimanenti.

Elimina tutti i file di backup per un sistema

L'eliminazione di tutti i backup nell'archivio oggetti di un sistema non disabilita i backup futuri dei volumi in questo sistema. Se si desidera interrompere la creazione di backup di tutti i volumi in un sistema, è possibile disattivare i backupcome descritto qui .

Si noti che questa azione non influisce sugli snapshot o sui volumi replicati: questi tipi di file di backup non vengono eliminati.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Selezionare••• per il sistema in cui si desidera eliminare tutti i backup e selezionare **Elimina tutti i backup**.
3. Nella finestra di dialogo di conferma, immettere il nome del sistema.
4. Selezionare **Impostazioni avanzate**.
5. **Forza eliminazione backup**: indica se desideri o meno forzare l'eliminazione di tutti i backup.

   In alcuni casi estremi, potresti voler impedire a NetApp Backup and Recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di sistema).

   > Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. NetApp Backup and Recovery non avrà più accesso a questi backup, anche se non vengono eliminati dall'archiviazione degli oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

6. Seleziona **Elimina**.

Elimina tutti i file di backup per un volume

L'eliminazione di tutti i backup di un volume disabilita anche i backup futuri per quel volume.

Passi

1. Dalla scheda **Volumi**, fare clic su••• per il volume di origine e selezionare **Dettagli e elenco di backup**.

   Viene visualizzato l'elenco di tutti i file di backup.

2. Selezionare **Azioni** > **Elimina tutti i backup**.
3. Immettere il nome del volume.
4. Selezionare **Impostazioni avanzate**.
5. **Forza eliminazione backup**: indica se desideri o meno forzare l'eliminazione di tutti i backup.

   In alcuni casi estremi, potresti voler impedire a NetApp Backup and Recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di sistema).

   Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. NetApp Backup and Recovery non avrà più accesso a questi backup, anche se non vengono eliminati dall'archiviazione degli oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

6. Seleziona **Elimina**.

Elimina un singolo file di backup per un volume

È possibile eliminare un singolo file di backup se non ne hai più bisogno. Ciò include l'eliminazione di un singolo backup di uno snapshot del volume o di un backup nell'archiviazione degli oggetti.

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

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume sorgente e seleziona **Visualizza dettagli volume**.

   Vengono visualizzati i dettagli del volume ed è possibile selezionare **Snapshot**, **Replica** o **Backup** per visualizzare l'elenco di tutti i file di backup per il volume. Per impostazione predefinita, vengono visualizzati gli snapshot disponibili.

2. Selezionare **Snapshot** o **Backup** per visualizzare il tipo di file di backup che si desidera eliminare.
3. Selezionare••• per il file di backup del volume che vuoi eliminare e seleziona **Elimina**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina**.

Elimina 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, ma conservare tutti i file di backup esistenti. Ciò ti dà la possibilità di ripristinare il volume dal file di backup in futuro, se necessario, liberando spazio dal tuo sistema di archiviazione di origine.

Non è necessario eliminare necessariamente il volume sorgente. 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 si continua a utilizzare la copia di backup di base originale: non viene

creata né esportata nel cloud una nuova copia di backup di base. Si noti che se si riattiva una relazione di backup, al volume viene assegnato il criterio di backup predefinito.

Questa funzionalità è disponibile solo se il sistema esegue ONTAP 9.12.1 o versione successiva.

Non è possibile eliminare il volume di origine dall'interfaccia utente NetApp Backup and Recovery . Tuttavia, è possibile aprire la pagina Dettagli volume nella pagina **Sistemi** della console e "elimina il volume da lì" .

> Non è possibile eliminare singoli file di backup del volume una volta eliminata la relazione. Tuttavia, è possibile eliminare tutti i backup del volume.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume di origine e selezionare **Backup** > **Elimina relazione**.

Disattivare NetApp Backup and Recovery per un sistema

La disattivazione di NetApp Backup and Recovery per un sistema disabilita i backup di ciascun volume sul sistema e disabilita anche la possibilità di ripristinare un volume. Tutti i backup esistenti non verranno eliminati. Ciò non annulla la registrazione del servizio di backup da questo sistema: in pratica consente di sospendere tutte le attività di backup e ripristino per un periodo di tempo.

Tieni presente che il tuo provider cloud continuerà a addebitarti i costi di archiviazione degli oggetti per la capacità utilizzata dai tuoi backup, a meno che tu noneliminare i backup .

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona••• per il sistema in cui si desidera disattivare i backup e selezionare **Disattiva backup**.
3. Nella finestra di dialogo di conferma, seleziona **Disattiva**.

> Quando il backup è disabilitato, per quel sistema viene visualizzato il pulsante **Attiva backup**. È possibile selezionare questo pulsante quando si desidera riattivare la funzionalità di backup per quel sistema.

Annullare la registrazione NetApp Backup and Recovery per un sistema

È possibile annullare la registrazione di NetApp Backup and Recovery per un sistema se non si desidera più utilizzare la funzionalità di backup e non si desidera più ricevere addebiti per i backup in quel sistema. In genere questa funzionalità viene utilizzata quando si pianifica di eliminare un sistema e si desidera annullare il servizio di backup.

È possibile utilizzare questa funzionalità anche se si desidera modificare l'archivio oggetti di destinazione in cui vengono archiviati i backup del cluster. Dopo aver annullato la registrazione NetApp Backup and Recovery per il sistema, è possibile abilitare NetApp Backup and Recovery per quel cluster utilizzando le informazioni del nuovo provider cloud.

Prima di poter annullare la registrazione NetApp Backup and Recovery, è necessario eseguire i seguenti passaggi, nell'ordine indicato:

- Disattivare NetApp Backup and Recovery per il sistema
- Elimina tutti i backup per quel sistema

L'opzione di annullamento della registrazione non è disponibile finché queste due azioni non sono state completate.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona ••• per il sistema in cui si desidera annullare la registrazione del servizio di backup e selezionare **Annulla registrazione**.
3. Nella finestra di dialogo di conferma, seleziona **Annulla registrazione**.

Ripristina dai backup ONTAP

Ripristina i dati ONTAP dai file di backup con NetApp Backup and Recovery

I backup dei dati del volume ONTAP vengono archiviati come snapshot, su volumi replicati o nell'archiviazione di oggetti. È possibile ripristinare i dati da una qualsiasi di queste posizioni in un momento specifico. Con NetApp Backup and Recovery puoi ripristinare un intero volume, una cartella o singoli file, a seconda delle tue esigenze.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

- È possibile ripristinare un **volume** (come nuovo volume) sul sistema originale, su un sistema diverso che utilizza lo stesso account cloud o su un sistema ONTAP locale.
- È possibile ripristinare una **cartella** su un volume nel sistema originale, su un volume in un sistema diverso che utilizza lo stesso account cloud o su un volume in un sistema ONTAP locale.
- È possibile ripristinare **file** su un volume nel sistema originale, su un volume in un sistema diverso che utilizza lo stesso account cloud o su un volume in un sistema ONTAP locale.

Per ripristinare i dati su un sistema di produzione è necessaria una licenza NetApp Backup and Recovery valida.

Riassumendo, ecco i flussi validi che è possibile utilizzare per ripristinare i dati del volume in un sistema ONTAP :

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

Se l'operazione di ripristino non viene completata, attendere che Job Monitor visualizzi "Fallito" prima di riprovare l'operazione di ripristino.

Per le limitazioni relative al ripristino dei dati ONTAP , vedere"Limitazioni di backup e ripristino per i volumi ONTAP" .

La dashboard di ripristino

Utilizzare la dashboard di ripristino per eseguire operazioni di ripristino di volumi, cartelle e file. Per accedere alla Dashboard di ripristino, selezionare **Backup e ripristino** dal menu Console, quindi selezionare la scheda

Ripristina. Puoi anche selezionare > **Visualizza la dashboard di ripristino** dal servizio Backup e ripristino dal pannello Servizi.

NetApp Backup and Recovery deve essere già attivato per almeno un sistema e devono esistere i file di backup iniziali.

La dashboard di ripristino offre due modi diversi per ripristinare i dati dai file di backup: **Sfoglia e ripristina** e **Cerca e ripristina**.

Confronto tra Sfoglia e Ripristina e Cerca e Ripristina

In termini generali, *Sfoglia e ripristina* è in genere più indicato quando è necessario ripristinare un volume, una cartella o un file specifico dell'ultima settimana o dell'ultimo mese, e si conoscono il nome e la posizione del file, nonché la data dell'ultima volta in cui era in buone condizioni. *Cerca e ripristina* è in genere la soluzione migliore quando è necessario ripristinare un volume, una cartella o un file, ma non si ricorda il nome esatto, il volume in cui si trova o la data dell'ultima volta in cui è stato in buone condizioni.

Questa tabella fornisce un confronto delle caratteristiche dei due metodi.

Sfoglia e ripristina	Cerca e ripristina
Sfoglia una struttura in stile cartella per trovare il volume, la cartella o il file all'interno di un singolo file di backup.	Cerca un volume, una cartella o un file in **tutti i file di backup** per nome parziale o completo del volume, nome parziale o completo della cartella/file, intervallo di dimensioni e filtri di ricerca aggiuntivi.
Non gestisce il recupero del file se il file è stato eliminato o rinominato e l'utente non conosce il nome originale del file	Gestisce le directory appena create/eliminate/rinominate e i file appena creati/eliminati/rinominati
È supportato il ripristino rapido.	Il ripristino rapido non è supportato.

Questa tabella fornisce un elenco di operazioni di ripristino valide in base alla posizione in cui risiedono i file di backup.

Tipo di backup	Sfoglia e ripristina			Cerca e ripristina		
	Ripristina volume	Ripristina file	Ripristina cartella	Ripristina volume	Ripristina file	Ripristina cartella
Istantanea	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, configurare l'ambiente in modo che soddisfi i requisiti delle risorse. Per i dettagli, vedere le sezioni seguenti.

Consultare i requisiti e i passaggi di ripristino per il tipo di operazione di ripristino che si desidera utilizzare:

- "Ripristina i volumi utilizzando Sfoglia e Ripristina"

- "Ripristina cartelle e file utilizzando Sfoglia e Ripristina"
- "Ripristina volumi, cartelle e file utilizzando Cerca e ripristina"

Ripristina dai backup ONTAP utilizzando Cerca e ripristina

È possibile utilizzare Cerca e ripristina per recuperare volumi, cartelle o file dai file di backup ONTAP . Search & Restore consente di effettuare ricerche in tutti i backup (inclusi snapshot locali, volumi replicati e storage di oggetti) senza dover specificare i nomi esatti di sistema, volume o file.

Il ripristino da snapshot locali o volumi replicati è in genere più rapido e meno costoso rispetto al ripristino da storage di oggetti.

Quando si ripristina un volume completo, NetApp Backup and Recovery crea un nuovo volume utilizzando i dati di backup. È possibile ripristinare il sistema originale, un altro sistema all'interno dello stesso account cloud o un sistema ONTAP locale. Le cartelle e i file possono essere ripristinati nella loro posizione originale, in un volume diverso nello stesso sistema, in un altro sistema nello stesso account cloud o in un sistema locale.

Le capacità di ripristino dipendono dalla versione ONTAP :

- **Cartelle:** utilizzando ONTAP 9.13.0 o versioni successive, è possibile ripristinare cartelle con tutti i file e le sottocartelle; con le versioni precedenti, era possibile ripristinare solo i file nella cartella.
- **Archiviazione:** il ripristino dall'archiviazione (disponibile con ONTAP 9.10.1 o versioni successive) è più lento e potrebbe comportare costi aggiuntivi.
- **Requisiti del cluster di destinazione:**
  - Ripristino del volume: ONTAP 9.10.1 o versione successiva
  - Ripristino file: ONTAP 9.11.1 o versione successiva
  - Google Archive and StorageGRID: ONTAP 9.12.1 o versione successiva
  - Ripristino cartella: ONTAP 9.13.1 o versione successiva

"Scopri di più sul ripristino dall'archiviazione AWS".

"Scopri di più sul ripristino dall'archiviazione di Azure".

"Scopri di più sul ripristino dall'archivio di Google".

- Se il file di backup nell'archiviazione oggetti è stato configurato con protezione DataLock e Ransomware, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare l'intero volume dal file di backup e quindi accedere alla cartella e ai file necessari.
- Se il file di backup nell'archiviazione degli oggetti risiede nell'archiviazione di archivio, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. 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 dati dall'archiviazione di Azure nei sistemi StorageGRID .
- Il ripristino delle cartelle non è attualmente supportato dai volumi nell'archiviazione di oggetti ONTAP S3.

Prima di iniziare, dovresti avere un'idea del nome o della posizione del volume o del file che vuoi ripristinare.

Sistemi supportati da Search & Restore e provider di archiviazione di oggetti

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un sistema secondario (un volume replicato) o in un archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono sul sistema di origine e possono essere ripristinati solo su quello stesso sistema.

Nota: è possibile ripristinare volumi e file da qualsiasi tipo di file di backup, ma al momento è possibile ripristinare una cartella solo dai file di backup nell'archivio oggetti.

Posizione del file di backup		**Sistema di destinazione**
Archivio oggetti (backup)	**Sistema secondario (replicazione)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes ONTAP nel sistema ONTAP locale AWS endif::aws[] ifdef::azure[]
Blob azzurro	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure endif::azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP endif::gcp[]
NetApp StorageGRID	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede
ONTAP S3	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede

Per Search & Restore, l'agente Console può essere installato nei seguenti percorsi:

- Per Amazon S3, l'agente della console può essere distribuito in AWS o nei tuoi locali
- Per Azure Blob, l'agente Console può essere distribuito in Azure o nei tuoi locali
- Per Google Cloud Storage, l'agente della console deve essere distribuito nella VPC di Google Cloud Platform

- Per StorageGRID, l'agente della console deve essere distribuito nei tuoi locali, con o senza accesso a Internet
- Per ONTAP S3, l'agente della console può essere distribuito presso la tua sede (con o senza accesso a Internet) o in un ambiente di provider cloud

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

Prerequisiti per la ricerca e il ripristino

Prima di abilitare Ricerca e ripristino, assicurati che il tuo ambiente soddisfi questi requisiti:

- Requisiti del cluster:
  - La versione ONTAP deve essere 9.8 o successiva.
  - La VM di archiviazione (SVM) su cui risiede il volume deve avere un LIF dati configurato.
  - NFS deve essere abilitato sul volume (sono supportati sia i volumi NFS che SMB/CIFS).
  - Il server SnapDiff RPC deve essere attivato sull'SVM. La Console esegue questa operazione automaticamente quando si abilita l'indicizzazione sul sistema. (SnapDiff è la tecnologia che identifica rapidamente le differenze di file e directory tra gli snapshot.)
- NetApp consiglia di montare un volume separato sull'agente Console per aumentare la resilienza di Search & Restore. Per le istruzioni, fare riferimento amontare il volume per reindicizzare il catalogo .

Prerequisiti per Legacy Search & Restore (utilizzando Indexed Catalog v1)

Di seguito sono riportati i requisiti per Search & Restore quando si utilizza l'indicizzazione legacy:

- Requisiti AWS:
  - È necessario aggiungere autorizzazioni specifiche per Amazon Athena, AWS Glue e AWS S3 al ruolo utente che fornisce le autorizzazioni alla Console. "Assicurati che tutte le autorizzazioni siano configurate correttamente" .

    Tieni presente che se stavi già utilizzando NetApp Backup and Recovery con un agente Console configurato in passato, ora dovrai aggiungere le autorizzazioni Athena e Glue al ruolo utente Console. Sono necessari per la ricerca e il ripristino.

- Requisiti di Azure:
  - È necessario registrare il provider di risorse di Azure Synapse Analytics (denominato "Microsoft.Synapse") con la sottoscrizione. "Scopri come registrare questo fornitore di risorse per il tuo abbonamento" . Per registrare il fornitore di risorse, devi essere il **Proprietario** o il **Collaboratore** dell'abbonamento.
  - È necessario aggiungere autorizzazioni specifiche per Azure Synapse Workspace e per l'account Data Lake Storage al ruolo utente che fornisce le autorizzazioni alla console. "Assicurati che tutte le autorizzazioni siano configurate correttamente" .

    Tieni presente che se utilizzavi già NetApp Backup and Recovery con un agente Console configurato in passato, ora dovrai aggiungere le autorizzazioni Azure Synapse Workspace e Data Lake Storage Account al ruolo utente Console. Sono necessari per la ricerca e il ripristino.

  - L'agente Console deve essere configurato **senza** un server proxy per la comunicazione HTTP con Internet. Se hai configurato un server proxy HTTP per il tuo agente Console, non puoi utilizzare la funzionalità Cerca e ripristina.
- Requisiti di Google Cloud:
  - È necessario aggiungere autorizzazioni specifiche di Google BigQuery al ruolo utente che fornisce le autorizzazioni alla NetApp Console . "Assicurati che tutte le autorizzazioni siano configurate correttamente" .

    Se utilizzavi già NetApp Backup and Recovery con un agente Console configurato in passato, ora dovrai aggiungere le autorizzazioni BigQuery al ruolo utente Console. Sono necessari per la ricerca e il ripristino.

- Requisiti StorageGRID e ONTAP S3:

  A seconda della configurazione, la funzione Ricerca e ripristino può essere implementata in due modi:

  - Se nel tuo account non sono presenti credenziali del provider cloud, le informazioni del catalogo indicizzato vengono archiviate nell'agente della console.

    Per informazioni sul Catalogo indicizzato v2, vedere la sezione seguente su come abilitare il Catalogo indicizzato.

  - Se si utilizza un agente Console in un sito privato (oscuro), le informazioni del catalogo indicizzato vengono archiviate nell'agente Console (richiede l'agente Console versione 3.9.25 o successiva).
  - Se hai "Credenziali AWS" O "Credenziali di Azure" nell'account, il catalogo indicizzato viene archiviato presso il provider cloud, proprio come con un agente Console distribuito nel cloud. (Se si possiedono entrambe le credenziali, AWS è selezionato per impostazione predefinita.)

    Anche se si utilizza un agente Console locale, è necessario soddisfare i requisiti del provider

cloud sia per le autorizzazioni dell'agente Console sia per le risorse del provider cloud. Per utilizzare questa implementazione, consultare i requisiti AWS e Azure sopra indicati.

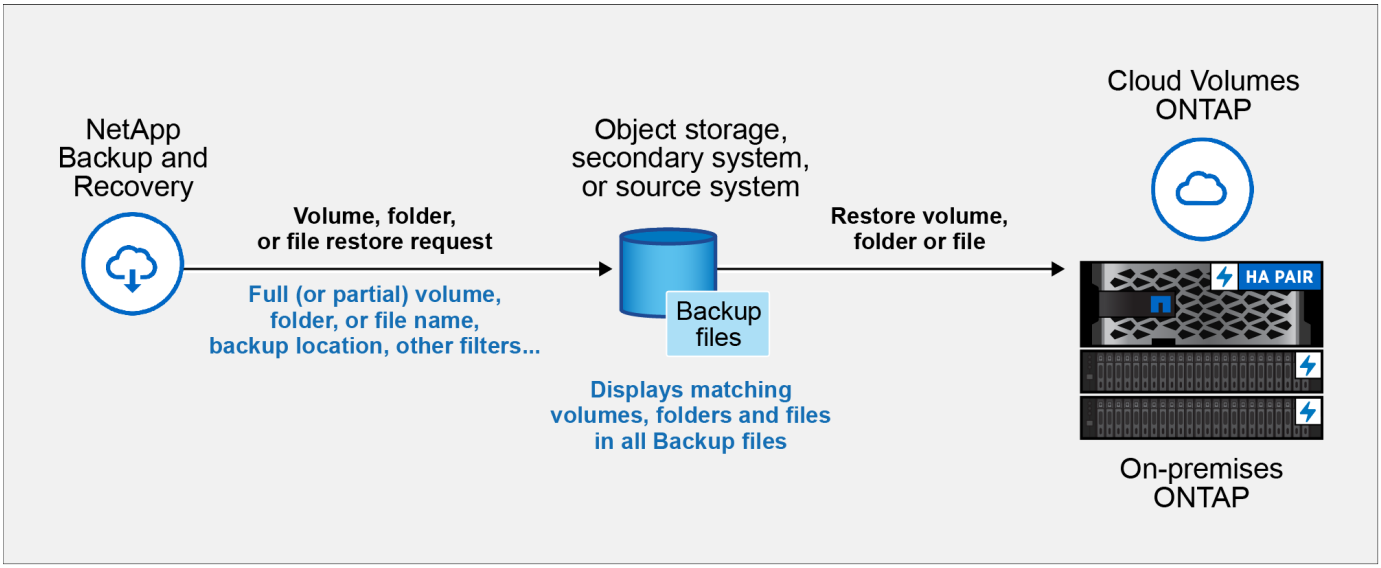
Processo di ricerca e ripristino

Il processo è il seguente:

1. Prima di poter utilizzare Ricerca e ripristino, è necessario abilitare "Indicizzazione" su ciascun sistema sorgente da cui si desidera ripristinare i dati del volume. Ciò consente al catalogo indicizzato di tenere traccia dei file di backup per ogni volume.
2. Quando si desidera ripristinare un volume o dei file da un backup del volume, in *Cerca e ripristina*, selezionare **Cerca e ripristina**.
3. Immettere i criteri di ricerca per un volume, una cartella o un file in base al nome parziale o completo del volume, al nome parziale o completo del file, alla posizione del backup, all'intervallo di dimensioni, all'intervallo di date di creazione, ad altri filtri di ricerca e selezionare **Cerca**.

   La pagina Risultati della ricerca mostra tutte le posizioni in cui è presente un file o un volume che corrisponde ai criteri di ricerca.

4. Selezionare **Visualizza tutti i backup** per la posizione che si desidera utilizzare per ripristinare il volume o il file, quindi selezionare **Ripristina** sul file di backup effettivo che si desidera utilizzare.
5. Selezionare la posizione in cui si desidera ripristinare il volume, la cartella o i file e selezionare **Ripristina**.
6. Il volume, la cartella o il/i file vengono ripristinati.



Basta conoscere un nome parziale e NetApp Backup and Recovery cercherà in tutti i file di backup che corrispondono alla tua ricerca.

Abilita il catalogo indicizzato per ogni sistema

Prima di poter utilizzare Ricerca e ripristino, è necessario abilitare "Indicizzazione" su ciascun sistema di origine da cui si prevede di ripristinare volumi o file. Ciò consente al catalogo indicizzato di tenere traccia di ogni volume e di ogni file di backup, rendendo le ricerche molto rapide ed efficienti.

Il catalogo indicizzato è un database che memorizza i metadati relativi a tutti i volumi e ai file di backup

presenti nel sistema. Viene utilizzato dalla funzionalità Cerca e ripristina per trovare rapidamente i file di backup che contengono i dati che si desidera ripristinare.

Caratteristiche del catalogo indicizzato

NetApp Backup and Recovery non fornisce un bucket separato quando si utilizza il catalogo indicizzato. Invece, per i backup archiviati in AWS, Azure, Google Cloud Platform, StorageGRID o ONTAP S3, il servizio predispone lo spazio sull'agente della console o sull'ambiente del provider cloud.

Il catalogo indicizzato supporta quanto segue:

- Efficienza di ricerca globale in meno di 3 minuti
- Fino a 5 miliardi di file
- Fino a 5000 volumi per cluster
- Fino a 100.000 snapshot per volume
- Il tempo massimo per l'indicizzazione di base è inferiore a 7 giorni. Il tempo effettivo varierà a seconda dell'ambiente.

Passaggi per abilitare l'indicizzazione per un sistema:

Se l'indicizzazione è già stata abilitata per il sistema, passare alla sezione successiva per ripristinare i dati.

Per prima cosa dovrai montare un volume separato per contenere i file di catalogo. In questo modo si evita la perdita di dati se le dimensioni dei file che contengono gli snapshot diventano troppo grandi. Questa operazione non è richiesta su tutti i cluster: è possibile montare un volume qualsiasi da uno qualsiasi dei cluster presenti nel proprio ambiente. In caso contrario, l'indicizzazione potrebbe non funzionare correttamente.

Per il volume montato, utilizzare le seguenti indicazioni di dimensionamento:

- Utilizzare un volume NetApp NFS
- Archiviazione AFF consigliata con throughput del disco di 300 MB/s. Una minore produttività avrà un impatto sulla ricerca e su altre operazioni.
- Abilita gli snapshot NetApp per proteggere i metadati del catalogo oltre ai file zip di backup del catalogo
- 50 GB per 1 miliardo di file
- 20 GB per i dati del catalogo con spazio aggiuntivo per la creazione di file zip e file temporanei

Passaggio per montare il volume per reindicizzare il catalogo

1. Montare il volume su `/opt/application/netapp/cbs` immettendo il seguente comando, dove:
    - `volume name` è il volume sul cluster in cui verranno archiviati i file di catalogo
    - `/opt/application/netapp/cbs` è il percorso in cui viene montato

    ```
    mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
    ```

    Esempio:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Passaggi per abilitare l'indice

1. Eseguire una delle seguenti operazioni:
   - Se non è stato indicizzato alcun sistema, nella Dashboard di ripristino in *Cerca e ripristina*, seleziona **Abilita indicizzazione per i sistemi**.
   - Se almeno un sistema è già stato indicizzato, nella Dashboard di ripristino in *Cerca e ripristina*, seleziona **Impostazioni di indicizzazione**.
2. Selezionare **Abilita indicizzazione** per il sistema.

Risultato

Dopo che tutti i servizi sono stati forniti e il catalogo indicizzato è stato attivato, il sistema viene visualizzato come "Attivo".

A seconda delle dimensioni dei volumi nel sistema 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 sempre aggiornato.

Ripristina volumi, cartelle e file utilizzando Cerca e ripristina

Dopo averindicizzazione abilitata per il tuo sistema , puoi ripristinare volumi, cartelle e file utilizzando Cerca e ripristina. Ciò consente di utilizzare un'ampia gamma di filtri per trovare il file o il volume esatto che si desidera ripristinare da tutti i file di backup.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** e verrà visualizzata la Dashboard di ripristino.
3. Dalla sezione *Cerca e ripristina*, seleziona **Cerca e ripristina**.
4. Dalla sezione *Cerca e ripristina*, seleziona **Cerca e ripristina**.
5. Dalla pagina Cerca e ripristina:
   a. Nella *barra di ricerca*, immettere un nome completo o parziale del volume, un nome della cartella o un nome del file.
   b. Selezionare il tipo di risorsa: **Volumi**, **File**, **Cartelle** o **Tutti**.
   c. Nell'area *Filtra per*, seleziona i criteri di filtro. Ad esempio, è possibile selezionare il sistema in cui risiedono i dati e il tipo di file, ad esempio un file .JPEG. In alternativa, è possibile selezionare il tipo di posizione di backup se si desidera cercare risultati solo all'interno degli snapshot disponibili o dei file di backup nell'archiviazione degli oggetti.
6. Seleziona **Cerca** e nell'area Risultati della ricerca verranno visualizzate tutte le risorse che contengono un file, una cartella o un volume corrispondente alla tua ricerca.
7. Individua la risorsa che contiene i dati che desideri ripristinare e seleziona **Visualizza tutti i backup** per visualizzare tutti i file di backup che contengono il volume, la cartella o il file corrispondente.
8. Individua il file di backup che desideri utilizzare per ripristinare i dati e seleziona **Ripristina**.

   Si noti che i risultati identificano gli snapshot dei volumi locali e i volumi replicati remoti che contengono il file nella ricerca. È possibile scegliere di ripristinare dal file di backup cloud, dallo snapshot o dal volume replicato.

9. Selezionare la posizione di destinazione in cui si desidera ripristinare il volume, la cartella o i file e selezionare **Ripristina**.

- Per i volumi, è possibile selezionare il sistema di destinazione originale oppure un sistema alternativo. Quando si ripristina un volume FlexGroup , è necessario scegliere più aggregati.
- Per le cartelle, è possibile ripristinare la posizione originale oppure selezionare una posizione alternativa, tra cui sistema, volume e cartella.
- Per i file, è possibile ripristinarli nella posizione originale oppure selezionare una posizione alternativa, tra cui il sistema, il volume e la cartella. Quando si seleziona la posizione originale, è possibile scegliere di sovrascrivere i file di origine o di crearne di nuovi.

  Se selezioni un sistema ONTAP locale e non hai ancora configurato la connessione del cluster all'archiviazione degli oggetti, ti verrà richiesto di immettere informazioni aggiuntive:

  - Durante il ripristino da Amazon S3, seleziona lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, immetti la chiave di accesso e la chiave segreta per l'utente creato per concedere al cluster ONTAP l'accesso al bucket S3 e, facoltativamente, scegli un endpoint VPC privato per il trasferimento sicuro dei dati. "Vedi i dettagli su questi requisiti" .
    - Durante il ripristino da Azure Blob, selezionare lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione e, facoltativamente, scegliere un endpoint privato per il trasferimento sicuro dei dati selezionando la rete virtuale e la subnet. "Vedi i dettagli su questi requisiti" .
    - Quando si esegue il ripristino da Google Cloud Storage, selezionare lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, nonché la chiave di accesso e la chiave segreta per accedere all'archiviazione degli oggetti. "Vedi i dettagli su questi requisiti" .
    - Durante 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 all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione. "Vedi i dettagli su questi requisiti" .
    - Durante 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'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione. "Vedi i dettagli su questi requisiti" .

Risultati

Il volume, la cartella o i file vengono ripristinati e si torna alla Dashboard di ripristino, dove è possibile esaminare l'avanzamento dell'operazione di ripristino. È anche possibile selezionare la scheda **Monitoraggio processi** per visualizzare l'avanzamento del ripristino. Vedere"Pagina di monitoraggio dei lavori" .

Ripristina i dati ONTAP utilizzando Sfoglia e ripristina

Con NetApp Backup and Recovery, ripristina i dati ONTAP utilizzando Browse & Restore. Prima di effettuare il ripristino, annotare il nome del volume di origine, il sistema di origine e l'SVM, nonché la data del file di backup. È possibile ripristinare i dati ONTAP da uno snapshot, da un volume replicato o da backup archiviati nell'archiviazione di oggetti.

Le capacità di ripristino dipendono dalla versione ONTAP :

- **Cartelle:** utilizzando ONTAP 9.13.0 o versioni successive, è possibile ripristinare cartelle con tutti i file e le sottocartelle; con le versioni precedenti, era possibile ripristinare solo i file nella cartella.
- **Archiviazione:** il ripristino dall'archiviazione (disponibile con ONTAP 9.10.1 o versioni successive) è più lento e potrebbe comportare costi aggiuntivi.

- **Requisiti del cluster di destinazione:**
  - Ripristino del volume: ONTAP 9.10.1 o versione successiva
  - Ripristino file: ONTAP 9.11.1 o versione successiva
  - Google Archive and StorageGRID: ONTAP 9.12.1 o versione successiva
  - Ripristino cartella: ONTAP 9.13.1 o versione successiva

"Scopri di più sul ripristino dall'archiviazione AWS".

"Scopri di più sul ripristino dall'archiviazione di Azure".

"Scopri di più sul ripristino dall'archivio di Google".

La priorità Alta non è supportata durante il ripristino dei dati dall'archiviazione di Azure ai sistemi StorageGRID .

Esplora e ripristina i sistemi supportati e i provider di archiviazione di oggetti

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un sistema secondario (un volume replicato) o in un archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono sul sistema di origine e possono essere ripristinati solo su quello stesso sistema.

Nota: è possibile ripristinare un volume da qualsiasi tipo di file di backup, ma al momento è possibile ripristinare una cartella o singoli file solo da un file di backup nell'archivio oggetti.

Da Object Store (Backup)	Da Primario (Snapshot)	Dal sistema secondario (replicazione)	Al sistema di destinazione ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes ONTAP nel sistema ONTAP locale AWS endif::aws[] ifdef::azure[]	Blob azzurro
Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure endif::azure[] ifdef::gcp[]	Google Cloud Storage	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP
Cloud Volumes ONTAP nel sistema Google On-premises ONTAP endif::gcp[]	NetApp StorageGRID	Sistema ONTAP in sede	Sistema ONTAP on-premise Cloud Volumes ONTAP
Al sistema ONTAP locale	ONTAP S3	Sistema ONTAP in sede	Sistema ONTAP on-premise Cloud Volumes ONTAP

Per Sfoglia e Ripristina, l'agente Console può essere installato nei seguenti percorsi:

- Per Amazon S3, l'agente della console può essere distribuito in AWS o nei tuoi locali
- Per Azure Blob, l'agente Console può essere distribuito in Azure o nei tuoi locali
- Per Google Cloud Storage, l'agente della console deve essere distribuito nella VPC di Google Cloud Platform

- Per StorageGRID, l'agente della console deve essere distribuito nei tuoi locali, con o senza accesso a Internet
- Per ONTAP S3, l'agente della console può essere distribuito presso la tua sede (con o senza accesso a Internet) o in un ambiente di provider cloud

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

Se la versione ONTAP sul sistema è precedente alla 9.13.1, non sarà possibile ripristinare cartelle o file se il file di backup è stato configurato con DataLock e Ransomware. In questo caso, puoi ripristinare l'intero volume dal file di backup e quindi accedere ai file di cui hai bisogno.

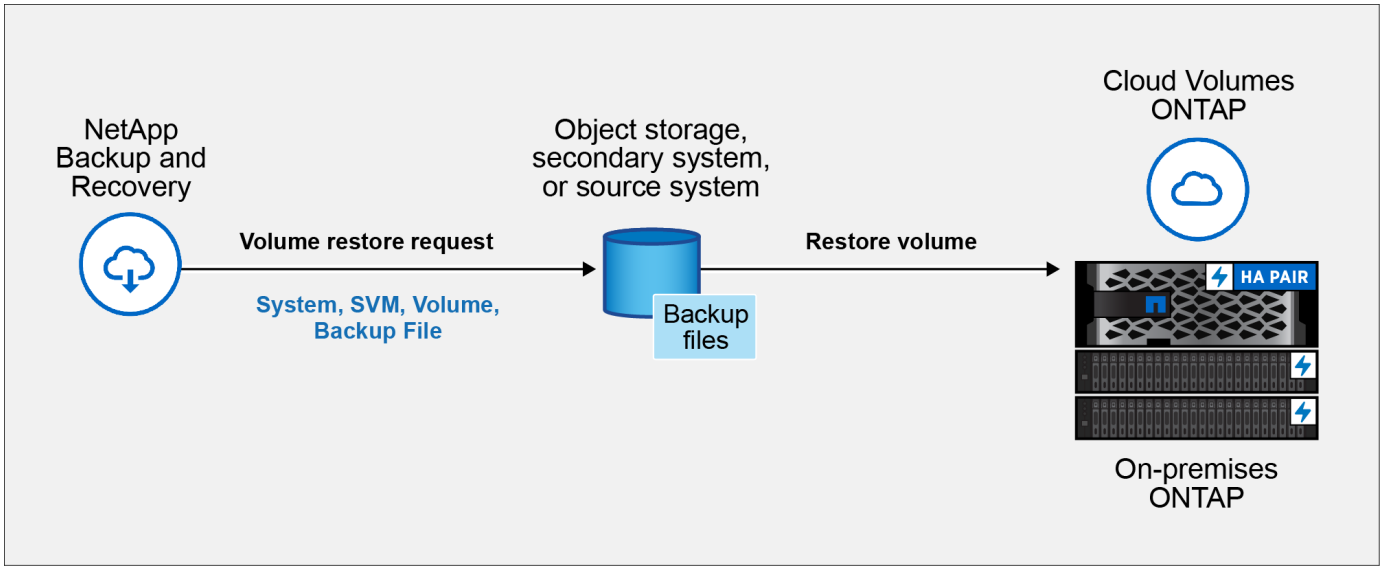
Ripristina i volumi utilizzando Sfoglia e ripristina

Quando si ripristina un volume da un file di backup, NetApp Backup and Recovery crea un *nuovo* volume utilizzando i dati del backup. Quando si utilizza un backup da un archivio di oggetti, è possibile ripristinare i dati su un volume nel sistema originale, su un sistema diverso situato nello stesso account cloud del sistema di origine o su un sistema ONTAP locale.

Quando si ripristina un backup cloud su un sistema Cloud Volumes ONTAP che utilizza ONTAP 9.13.0 o versione successiva oppure su un sistema ONTAP locale che esegue ONTAP 9.14.1, sarà possibile eseguire un'operazione di *ripristino rapido*. Il ripristino rapido è ideale per le situazioni di disaster recovery in cui è necessario fornire l'accesso a un volume il prima possibile. Un ripristino rapido ripristina i metadati dal file di backup a un volume anziché ripristinare l'intero file di backup. Il ripristino rapido non è consigliato per applicazioni sensibili alle prestazioni o alla latenza e non è supportato con i backup in storage archiviati.

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 versione successiva. Ed è supportato per i volumi SnapLock solo se il sistema di origine eseguiva ONTAP 9.11.0 o versione successiva.

Quando si esegue il ripristino da un volume replicato, è possibile ripristinare il volume sul sistema originale oppure su un sistema Cloud Volumes ONTAP o ONTAP locale.



Per ripristinare un volume sono necessari il nome del sistema di origine, la macchina virtuale di archiviazione, il nome del volume e la data del file di backup.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** e verrà visualizzata la Dashboard di ripristino.
3. Dalla sezione *Sfoglia e ripristina*, seleziona **Ripristina volume**.
4. Nella pagina *Seleziona origine*, vai al file di backup per il volume che desideri ripristinare. Selezionare il **sistema**, il **volume** e il file **backup** con la data/ora da cui si desidera effettuare il ripristino.

   La colonna **Posizione** mostra se il file di backup (Snapshot) è **Locale** (uno snapshot sul sistema di origine), **Secondario** (un volume replicato su un sistema ONTAP secondario) o **Archiviazione oggetti** (un file di backup nell'archiviazione oggetti). Seleziona il file che vuoi ripristinare.

5. Selezionare **Avanti**.

   Tieni presente che se selezioni un file di backup nell'archiviazione oggetti e Ransomware Resilience è attivo per quel backup (se hai abilitato DataLock e Ransomware Resilience nel criterio di backup), ti verrà chiesto di eseguire un'ulteriore scansione ransomware sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione del file di backup per individuare eventuali ransomware. (Per accedere al contenuto del file di backup, verranno addebitati costi di uscita aggiuntivi dal tuo provider cloud.)

6. Nella pagina *Seleziona destinazione*, seleziona il **sistema** in cui desideri ripristinare il volume.
7. Quando si ripristina un file di backup da un archivio oggetti, se si seleziona un sistema ONTAP locale e non è ancora stata configurata la connessione del cluster all'archivio oggetti, vengono richieste informazioni aggiuntive:
   - Durante il ripristino da Amazon S3, seleziona lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, immetti la chiave di accesso e la chiave segreta per l'utente creato per concedere al cluster ONTAP l'accesso al bucket S3 e, facoltativamente, scegli un endpoint VPC privato per il trasferimento sicuro dei dati.

     - Durante il ripristino da Azure Blob, selezionare lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, selezionare la sottoscrizione di Azure per accedere all'archiviazione degli oggetti e, facoltativamente, scegliere un endpoint privato per il trasferimento sicuro dei dati selezionando la rete virtuale e la subnet.
     - Durante il ripristino da Google Cloud Storage, seleziona il progetto Google Cloud, la chiave di accesso e la chiave segreta per accedere all'archiviazione degli oggetti, alla regione in cui sono archiviati i backup e allo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione.
     - Durante 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 all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione.
     - Durante 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'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione.

       a. Immettere il nome che si desidera utilizzare per il volume ripristinato e selezionare la VM di archiviazione e l'aggregato in cui risiederà il volume. Quando si ripristina un volume FlexGroup , è necessario selezionare più aggregati. Per impostazione predefinita, come nome del volume viene utilizzato **<source_volume_name>_restore**.

          Quando si ripristina un backup da un archivio di oggetti a un sistema Cloud Volumes ONTAP che utilizza ONTAP 9.13.0 o versione successiva oppure a un sistema ONTAP locale che

esegue ONTAP 9.14.1, sarà possibile eseguire un'operazione di *ripristino rapido*.

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

"Scopri di più sul ripristino dall'archiviazione AWS".

"Scopri di più sul ripristino dall'archiviazione di Azure".

"Scopri di più sul ripristino dall'archivio di Google". I file di backup nel livello di archiviazione di Google Archive vengono ripristinati quasi immediatamente e non richiedono alcuna priorità di ripristino.

1. Selezionare **Avanti** per scegliere se si desidera eseguire un ripristino normale o un ripristino rapido:
   - **Ripristino normale**: utilizzare il ripristino normale sui volumi che richiedono prestazioni elevate. I volumi non saranno disponibili finché il processo di ripristino non sarà completato.
   - **Ripristino rapido**: i volumi e i dati ripristinati saranno disponibili immediatamente. Non utilizzare questa opzione su volumi che richiedono prestazioni elevate perché durante il processo di ripristino rapido l'accesso ai dati potrebbe essere più lento del solito.
2. Selezionando **Ripristina** si torna alla Dashboard di ripristino, dove è possibile esaminare l'avanzamento dell'operazione di ripristino.

Risultato

NetApp Backup and Recovery crea un nuovo volume in base al backup selezionato.

Si noti che il ripristino di un volume da un file di backup residente in un archivio può richiedere molti minuti o ore, a seconda del livello di archivio e della priorità di ripristino. È possibile selezionare la scheda **Monitoraggio processi** per visualizzare l'avanzamento del ripristino.

Ripristina cartelle e file utilizzando Sfoglia e ripristina

Se è necessario ripristinare solo alcuni file da un backup del volume ONTAP , è possibile scegliere di ripristinare una cartella o singoli file anziché ripristinare l'intero volume. È possibile ripristinare cartelle e file su un volume esistente nel sistema originale oppure su un sistema diverso che utilizza lo stesso account cloud. È anche possibile ripristinare cartelle e file su un volume su un sistema ONTAP locale.

Al momento è possibile ripristinare una cartella o singoli file solo da un file di backup nell'archivio oggetti. Il ripristino di file e cartelle non è attualmente supportato da uno snapshot locale o da un file di backup che risiede in un sistema secondario (un volume replicato).

Se si selezionano più file, questi vengono ripristinati nello stesso volume di destinazione. Per ripristinare i file su volumi diversi, eseguire il processo più volte.

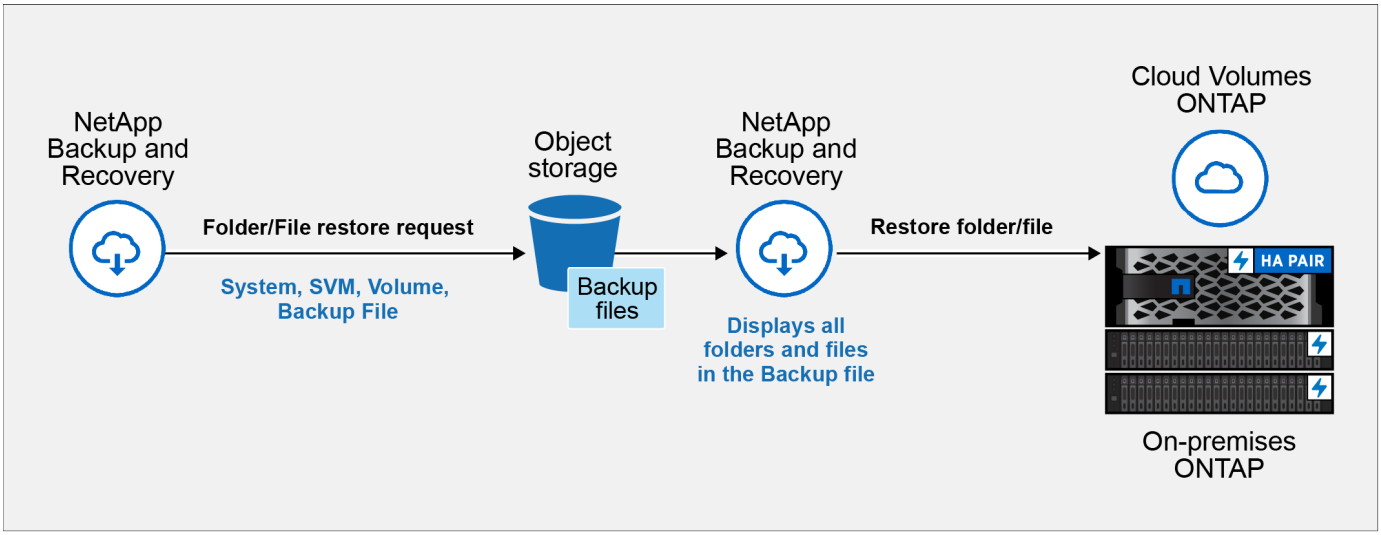
Se si utilizza ONTAP 9.13.0 o versione successiva, è possibile ripristinare una cartella insieme a tutti i file e le sottocartelle in essa contenuti. Quando si utilizza una versione di ONTAP precedente alla 9.13.0, vengono ripristinati solo i file di quella cartella, ma non le sottocartelle o i file nelle sottocartelle.

- Se il file di backup è stato configurato con la protezione DataLock e Ransomware, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare l'intero volume dal file di backup e quindi accedere alla cartella e ai file necessari.
- Se il file di backup risiede in un archivio, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare la cartella da un file di backup più recente che non è stato archiviato oppure è possibile ripristinare l'intero volume dal backup archiviato e quindi accedere alla cartella e ai file necessari.
- Con ONTAP 9.15.1 è possibile ripristinare le cartelle FlexGroup utilizzando l'opzione "Sfoglia e ripristina". Questa funzionalità è in modalità Anteprima tecnologica.

  È possibile testarlo utilizzando un flag speciale descritto in "Blog sulla versione NetApp Backup and Recovery di luglio 2024" .

Ripristina cartelle e file

Per ripristinare cartelle o file su un volume da un backup del volume ONTAP , seguire questi passaggi. Dovresti conoscere il nome del volume e la data del file di backup che vuoi utilizzare per ripristinare la cartella o il/i file. Questa funzionalità utilizza la navigazione in tempo reale per consentirti di visualizzare l'elenco delle directory e dei file all'interno di ciascun file di backup.



Prima di iniziare

- Per eseguire operazioni di ripristino dei file, la versione ONTAP deve essere 9.6 o successiva.
- Per eseguire operazioni di ripristino delle *cartelle*, la versione ONTAP deve essere 9.11.1 o successiva. La versione 9.13.1 ONTAP è richiesta se i dati si trovano in un archivio o se il file di backup utilizza la protezione DataLock e Ransomware.
- Per ripristinare le directory FlexGroup utilizzando l'opzione Sfoglia e ripristina, la versione ONTAP deve essere 9.15.1 p2 o successiva.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** e verrà visualizzata la Dashboard di ripristino.
3. Dalla sezione *Sfoglia e ripristina*, seleziona **Ripristina file o cartella**.

4. Nella pagina *Seleziona origine*, vai al file di backup per il volume che contiene la cartella o i file che desideri ripristinare. Selezionare il **sistema**, il **volume** e il **backup** che presenta la data/ora da cui si desidera ripristinare i file.
5. Selezionare **Avanti** e verrà visualizzato 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 archiviazione, è possibile selezionare la Priorità di ripristino.

   "Scopri di più sul ripristino dall'archiviazione AWS". "Scopri di più sul ripristino dall'archiviazione di Azure" . "Scopri di più sul ripristino dall'archivio di Google" . I file di backup nel livello di archiviazione di Google Archive vengono ripristinati quasi immediatamente e non richiedono alcuna priorità di ripristino.

   Se Ransomware Resilience è attivo per il file di backup (se hai abilitato DataLock e Ransomware Resilience nel criterio di backup), ti verrà chiesto di eseguire un'ulteriore scansione ransomware sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione del file di backup per individuare eventuali ransomware. (Per accedere al contenuto del file di backup, verranno addebitati costi di uscita aggiuntivi dal tuo provider cloud.)

6. Nella pagina *Seleziona elementi*, seleziona la cartella o i file che desideri ripristinare e seleziona **Continua**. Per aiutarti a trovare l'articolo:
   - Se vedi il nome della cartella o del file, puoi selezionarlo.
   - È possibile selezionare l'icona di ricerca e immettere il nome della cartella o del file per passare direttamente all'elemento.
   - È possibile spostarsi nei livelli inferiori delle cartelle utilizzando la freccia giù alla fine della riga per trovare file specifici.

     Man mano che selezioni i file, questi vengono aggiunti al lato sinistro della pagina, così puoi vedere i file che hai già scelto. Se necessario, è possibile rimuovere un file da questo elenco selezionando la **x** accanto al nome del file.
7. Nella pagina *Seleziona destinazione*, seleziona il **sistema** in cui desideri ripristinare gli elementi.

   Se selezioni un cluster locale e non hai ancora configurato la connessione del cluster all'archiviazione di oggetti, ti verranno richieste informazioni aggiuntive:

   - Quando si esegue il ripristino da Amazon S3, immettere lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione, nonché la chiave di accesso AWS e la chiave segreta necessarie per accedere allo storage degli oggetti. È anche possibile selezionare una configurazione di collegamento privato per la connessione al cluster.
     - Quando si esegue il ripristino da Azure Blob, immettere lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione. È anche possibile selezionare una configurazione endpoint privata per la connessione al cluster.
     - Quando si esegue il ripristino da Google Cloud Storage, immettere lo spazio IP nel cluster ONTAP in cui risiedono i volumi di destinazione, nonché la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti.
     - Durante 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 all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione.

       a. Quindi seleziona il **Volume** e la **Cartella** in cui desideri ripristinare la cartella o il/i file.

Sono disponibili alcune opzioni per la posizione durante il ripristino di cartelle e file.

- Dopo aver scelto **Seleziona cartella di destinazione**, come mostrato sopra:

◦ Puoi selezionare qualsiasi cartella.

◦ È possibile passare il mouse su una cartella e fare clic alla fine della riga per visualizzare in dettaglio le sottocartelle, quindi selezionare una cartella.

- Se hai selezionato lo stesso sistema di destinazione e lo stesso volume in cui si trovava la cartella/il file di origine, puoi selezionare **Mantieni percorso cartella di origine** per ripristinare la cartella o i file nella stessa cartella in cui si trovavano nella struttura di origine. Tutte le cartelle e sottocartelle devono già esistere; non vengono create cartelle. Quando si ripristinano i file nella loro posizione originale, è possibile scegliere di sovrascrivere i file di origine o di crearne di nuovi.

a. Selezionare **Ripristina** per tornare alla Dashboard di ripristino e rivedere l'avanzamento dell'operazione di ripristino.