Sincronizzare i dati tra un'origine e una destinazione

NetApp Copy and Sync

NetApp
December 16, 2025

Sommario

Sincronizzare i dati tra un'origine e una destinazione

Preparare un broker di dati per sincronizzare i dati tra l'archiviazione degli oggetti in NetApp Copy and Sync

Se si prevede di sincronizzare i dati da un archivio di oggetti all'altro (ad esempio, da Amazon S3 ad Azure Blob) in NetApp Copy and Sync, è necessario preparare il gruppo di broker di dati prima di creare la relazione di sincronizzazione.

Informazioni su questo compito

Per preparare il gruppo di broker di dati, sarà necessario modificare la configurazione dello scanner. Se non modifichi la configurazione, potresti riscontrare problemi di prestazioni per questa relazione di sincronizzazione.

Prima di iniziare

Il gruppo di broker di dati utilizzato per sincronizzare i dati da un archivio di oggetti all'altro dovrebbe gestire solo questi tipi di relazioni di sincronizzazione. Se il gruppo di broker di dati gestisce un tipo diverso di relazione di sincronizzazione (ad esempio, da NFS a NFS o da archiviazione di oggetti a SMB), le prestazioni di tali relazioni di sincronizzazione potrebbero essere influenzate negativamente.

Passi

1. "Accedi a Copia e Sincronizza" .
2. Da Copia e sincronizzazione, seleziona **Gestisci broker di dati**.
3. Selezionare 
4. Aggiorna la configurazione dello scanner:
   a. Modificare **Scanner Concurrency** in **1**.
   b. Modificare **Limite processi scanner** in **1**.
5. Selezionare **Unifica configurazione**.

Risultato

Copia e sincronizzazione aggiorna la configurazione del gruppo di broker di dati.

Cosa succederà ora?

Ora puoi creare la relazione di sincronizzazione tra l'archiviazione degli oggetti utilizzando il gruppo di broker di dati appena configurato.

Crea relazioni di sincronizzazione in NetApp Copy and Sync

Quando si crea una relazione di sincronizzazione, NetApp Copy and Sync copia i file dall'origine alla destinazione. Dopo la copia iniziale, la funzione Copia e sincronizzazione sincronizza tutti i dati modificati ogni 24 ore.

Prima di poter creare alcuni tipi di relazioni di sincronizzazione, è necessario creare un sistema nella NetApp Console.

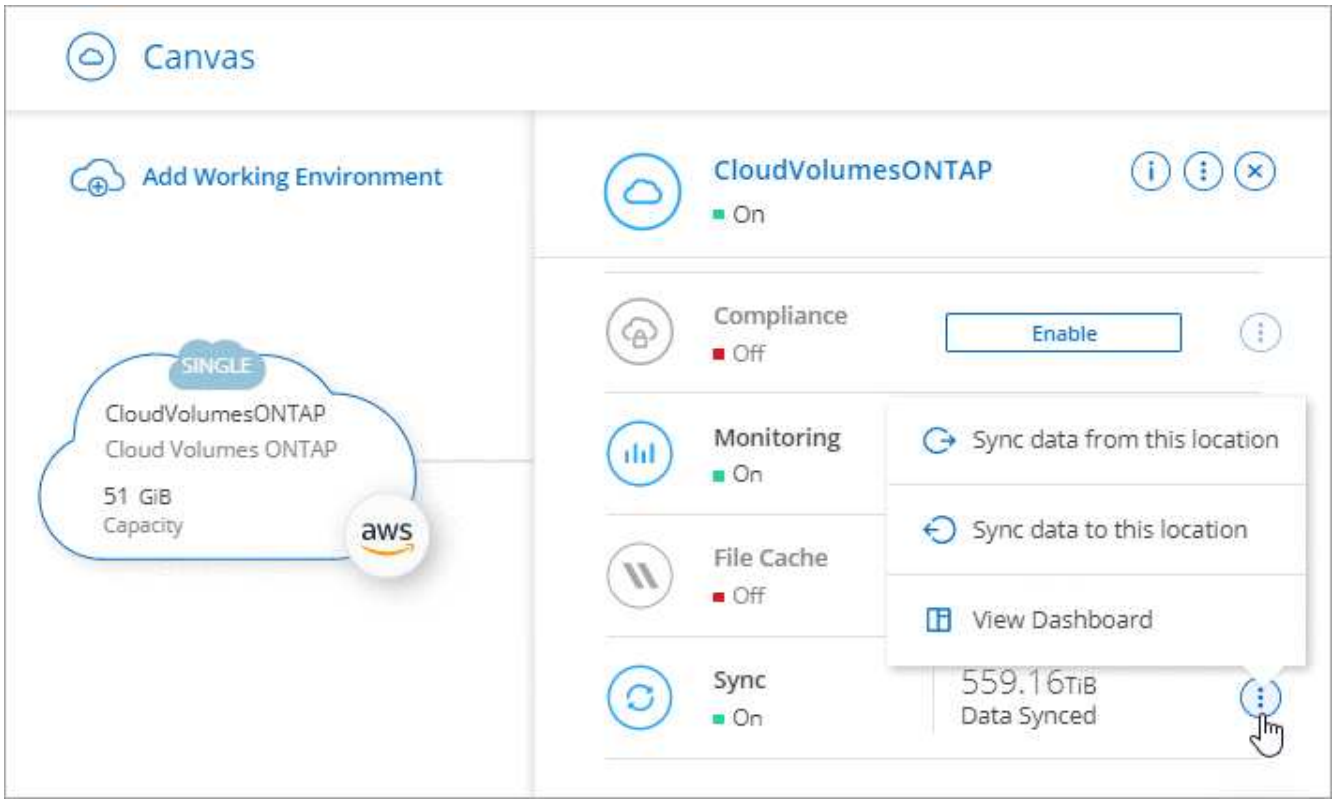
Creare relazioni di sincronizzazione per tipi specifici di sistemi

Se si desidera creare relazioni di sincronizzazione per uno qualsiasi dei seguenti elementi, è necessario prima creare o scoprire il sistema:

- Amazon FSx per ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Cluster ONTAP on-prem

Passi

1. "Accedi a Copia e Sincronizza" .
2. Creare o scoprire il sistema.
    - "Creare un sistema Amazon FSx per ONTAP"
    - "Configurazione e individuazione Azure NetApp Files"
    - "Avvio di Cloud Volumes ONTAP in AWS"
    - "Avvio di Cloud Volumes ONTAP in Azure"
    - "Avvio di Cloud Volumes ONTAP in Google Cloud"
    - "Aggiunta di sistemi Cloud Volumes ONTAP esistenti"
    - "Alla scoperta dei cluster ONTAP"
3. Selezionare **Pagina Sistemi**.
4. Seleziona un sistema che corrisponda a uno dei tipi elencati sopra.
5. Selezionare il menu azioni accanto a Sincronizza.



6. Selezionare **Sincronizza dati da questa posizione** o **Sincronizza dati con questa posizione** e seguire le istruzioni per impostare la relazione di sincronizzazione.

Creare altri tipi di relazioni di sincronizzazione

Utilizzare questi passaggi per sincronizzare i dati da o verso un tipo di archiviazione supportato diverso da Amazon FSx for ONTAP, Azure NetApp Files, Cloud Volumes ONTAP o cluster ONTAP locali. I passaggi seguenti forniscono un esempio che mostra come impostare una relazione di sincronizzazione da un server NFS a un bucket S3.

1. Nella NetApp Console, seleziona **Sincronizza**.
2. Nella pagina **Definisci relazione di sincronizzazione**, seleziona un'origine e una destinazione.

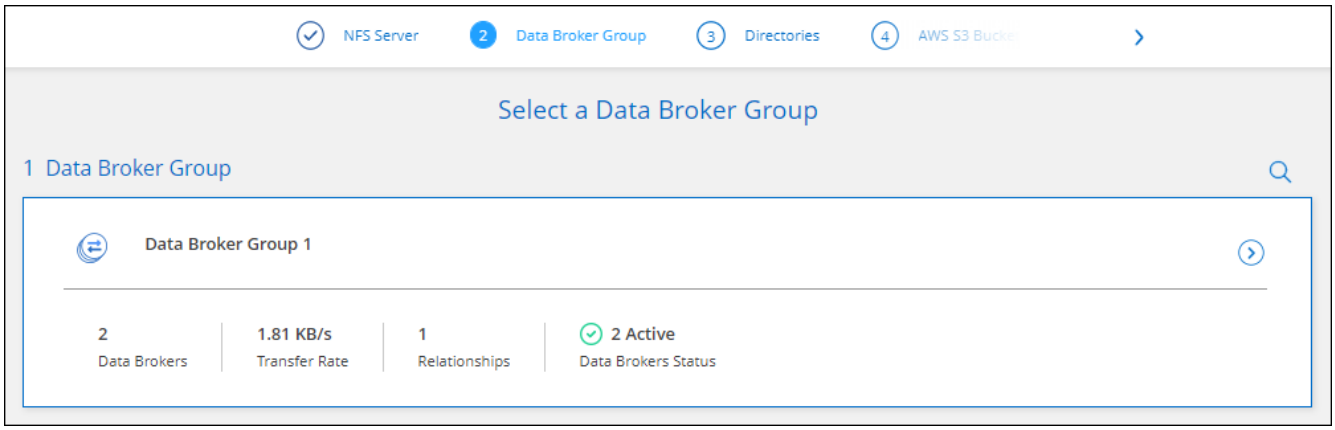
   I passaggi seguenti forniscono un esempio di come creare una relazione di sincronizzazione da un server NFS a un bucket S3.

3. Nella pagina **Server NFS**, immettere l'indirizzo IP o il nome di dominio completo del server NFS che si desidera sincronizzare con AWS.
4. Nella pagina **Data Broker Group**, seguire le istruzioni per creare una macchina virtuale del data broker in AWS, Azure o Google Cloud Platform oppure per installare il software del data broker su un host Linux esistente.

   Per maggiori dettagli consultare le seguenti pagine:

- "Creare un broker di dati in AWS"
- "Creare un broker di dati in Azure"
- "Creare un broker di dati in Google Cloud"
- "Installazione del data broker su un host Linux"

5. Dopo aver installato il broker di dati, seleziona **Continua**.

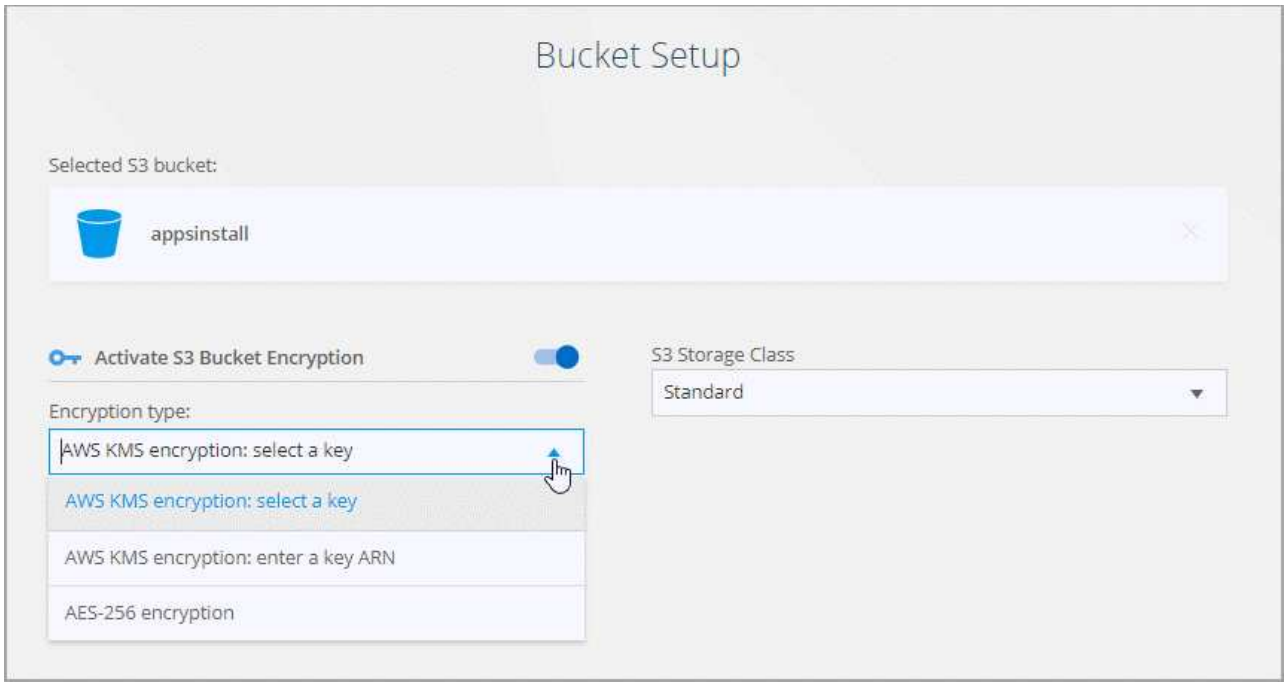


6. Nella pagina **Directory**, seleziona una directory o una sottodirectory di primo livello.

   Se Copia e sincronizzazione non riesce a recuperare le esportazioni, selezionare **Aggiungi esportazione manualmente** e immettere il nome di un'esportazione NFS.

   Se si desidera sincronizzare più di una directory sul server NFS, è necessario creare ulteriori relazioni di sincronizzazione al termine dell'operazione.

7. Nella pagina **AWS S3 Bucket**, seleziona un bucket:
   - Esegui il drill-down per selezionare una cartella esistente all'interno del bucket o per selezionare una nuova cartella creata all'interno del bucket.
   - Seleziona **Aggiungi all'elenco** per selezionare un bucket S3 non associato al tuo account AWS. "È necessario applicare autorizzazioni specifiche al bucket S3" .
8. Nella pagina **Configurazione bucket**, configura il bucket:
   - Scegli se abilitare la crittografia del bucket S3 e quindi seleziona una chiave AWS KMS, inserisci l'ARN di una chiave KMS o seleziona la crittografia AES-256.
   - Selezionare una classe di archiviazione S3. "Visualizza le classi di archiviazione supportate" .



9. Nella pagina **Impostazioni**, definisci come i file e le cartelle di origine vengono sincronizzati e mantenuti nella posizione di destinazione:

Programma

Scegli una pianificazione ricorrente per le sincronizzazioni future oppure disattiva la pianificazione della sincronizzazione. È possibile pianificare una relazione per sincronizzare i dati anche ogni minuto.

Timeout di sincronizzazione

Definisci se Copia e sincronizzazione deve annullare una sincronizzazione dei dati se la sincronizzazione non è stata completata entro il numero specificato di minuti, ore o giorni.

Notifiche

Consente di scegliere se ricevere notifiche di copia e sincronizzazione nel Centro notifiche della console NetApp . È possibile abilitare le notifiche per le sincronizzazioni dei dati riuscite, non riuscite e annullate.

Nuovi tentativi

Definisci il numero di volte in cui Copia e sincronizzazione devono riprovare a sincronizzare un file prima di saltarlo.

Sincronizzazione continua

Dopo la sincronizzazione iniziale dei dati, Copy and Sync ascolta le modifiche sul bucket S3 di origine o sul bucket Google Cloud Storage e sincronizza continuamente tutte le modifiche con la destinazione non appena si verificano. Non è necessario ripetere la scansione della sorgente a intervalli programmati.

Questa impostazione è disponibile solo quando si crea una relazione di sincronizzazione e quando si sincronizzano i dati da un bucket S3 o Google Cloud Storage ad Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3 e StorageGRID **oppure** da Azure Blob Storage ad Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS e StorageGRID.

Se si attiva questa impostazione, verranno influenzate anche altre funzionalità come segue:

- La pianificazione della sincronizzazione è disabilitata.
- Le seguenti impostazioni vengono ripristinate ai valori predefiniti: Timeout sincronizzazione, File modificati di recente e Data di modifica.
- Se S3 è l'origine, il filtro per dimensione sarà attivo solo sugli eventi di copia (non sugli eventi di eliminazione).
- Dopo aver creato la relazione, puoi solo accelerarla o eliminarla. Non è possibile interrompere le sincronizzazioni, modificare le impostazioni o visualizzare i report.

  È possibile creare una relazione di sincronizzazione continua con un bucket esterno. Per farlo, segui questi passaggi:

  i. Vai alla console Google Cloud per il progetto del bucket esterno.

  ii. Vai su **Cloud Storage > Impostazioni > Account del servizio di archiviazione cloud**.

  iii. Aggiorna il file local.json:

```
{
"protocols": {
    "gcp": {
        "storage-account-email": <storage account email>
}
}
}
```

  iv. Riavviare il broker di dati:

    A. sudo pm2 stop all

    B. sudo pm2 avvia tutto

  v. Creare una relazione di sincronizzazione continua con il bucket esterno pertinente.

> Un broker di dati utilizzato per creare una relazione di sincronizzazione continua con un bucket esterno non sarà in grado di creare un'altra relazione di sincronizzazione continua con un bucket nel suo progetto.

Confronta per

Scegliere se Copia e Sincronizzazione debbano confrontare determinati attributi per determinare se un file o una directory sono stati modificati e devono essere sincronizzati di nuovo.

Anche se deselezioni questi attributi, Copia e sincronizzazione confronta comunque l'origine con la destinazione controllando i percorsi, le dimensioni dei file e i nomi dei file. Se ci sono modifiche, sincronizza i file e le directory.

È possibile scegliere di abilitare o disabilitare Copia e sincronizzazione per confrontare i seguenti attributi:

- **mtime**: Ora dell'ultima modifica di un file. Questo attributo non è valido per le directory.
- **uid**, **gid** e **mode**: flag di autorizzazione per Linux.

Copia per oggetti

Abilita questa opzione per copiare i metadati e i tag dell'archiviazione degli oggetti. Se un utente modifica i metadati sulla sorgente, Copia e sincronizzazione copia questo oggetto nella sincronizzazione successiva, ma se un utente modifica i tag sulla sorgente (e non i dati stessi), Copia e sincronizzazione non copia l'oggetto nella sincronizzazione successiva.

Non è possibile modificare questa opzione dopo aver creato la relazione.

La copia dei tag è supportata con relazioni di sincronizzazione che includono Azure Blob o un endpoint compatibile con S3 (S3, StorageGRID o IBM Cloud Object Storage) come destinazione.

La copia dei metadati è supportata con relazioni "cloud-to-cloud" tra uno qualsiasi dei seguenti endpoint:

- AWS S3
- Blob azzurro
- Google Cloud Storage
- IBM Cloud Object Storage
- StorageGRID

File modificati di recente

Scegli di escludere i file che sono stati modificati di recente prima della sincronizzazione pianificata.

Elimina i file sulla sorgente

Scegliere di eliminare i file dalla posizione di origine dopo che Copia e sincronizzazione ha copiato i file nella posizione di destinazione. Questa opzione comporta il rischio di perdita di dati, poiché i file sorgente vengono eliminati dopo essere stati copiati.

Se si abilita questa opzione, è necessario modificare anche un parametro nel file local.json sul data broker. Aprire il file e aggiornarlo come segue:

```
{
"workers":{
"transferrer":{
"delete-on-source": true
}
}
}
```

Dopo aver aggiornato il file local.json, dovresti riavviare: `pm2 restart all`.

Elimina i file sul bersaglio

Scegli di eliminare i file dalla posizione di destinazione, se sono stati eliminati dalla posizione di origine. L'impostazione predefinita è di non eliminare mai i file dalla posizione di destinazione.

Tipi di file

Definisci i tipi di file da includere in ogni sincronizzazione: file, directory, collegamenti simbolici e collegamenti fisici.

I collegamenti fisici sono disponibili solo per relazioni NFS-NFS non protette. Gli utenti saranno limitati a un solo processo di scansione e a una sola scansione contemporanea e le scansioni dovranno essere eseguite da una directory radice.

Escludi estensioni di file

Specificare l'espressione regolare o le estensioni dei file da escludere dalla sincronizzazione digitando l'estensione del file e premendo **Invio**. Ad esempio, digitare *log* o *.log* per escludere i file *.log. Per più estensioni non è necessario un separatore. Il seguente video fornisce una breve dimostrazione:

Escludere le estensioni dei file per una relazione di sincronizzazione

Le espressioni regolari (o regex) sono diverse dai caratteri jolly o dalle espressioni glob. Questa funzionalità funziona **solo** con le espressioni regolari.

Escludi directory

Specificare un massimo di 15 espressioni regolari o directory da escludere dalla sincronizzazione digitandone il nome o il percorso completo della directory e premendo **Invio**. Le directory .copy-offload, .snapshot, ~snapshot sono escluse per impostazione predefinita.

Le espressioni regolari (o regex) sono diverse dai caratteri jolly o dalle espressioni glob. Questa funzionalità funziona **solo** con le espressioni regolari.

Dimensione del file

Scegli di sincronizzare tutti i file, indipendentemente dalle loro dimensioni, oppure solo i file che rientrano in un intervallo di dimensioni specifico.

Data di modifica

Seleziona tutti i file indipendentemente dalla data dell'ultima modifica, i file modificati dopo una data specifica, prima di una data specifica o in un intervallo di tempo.

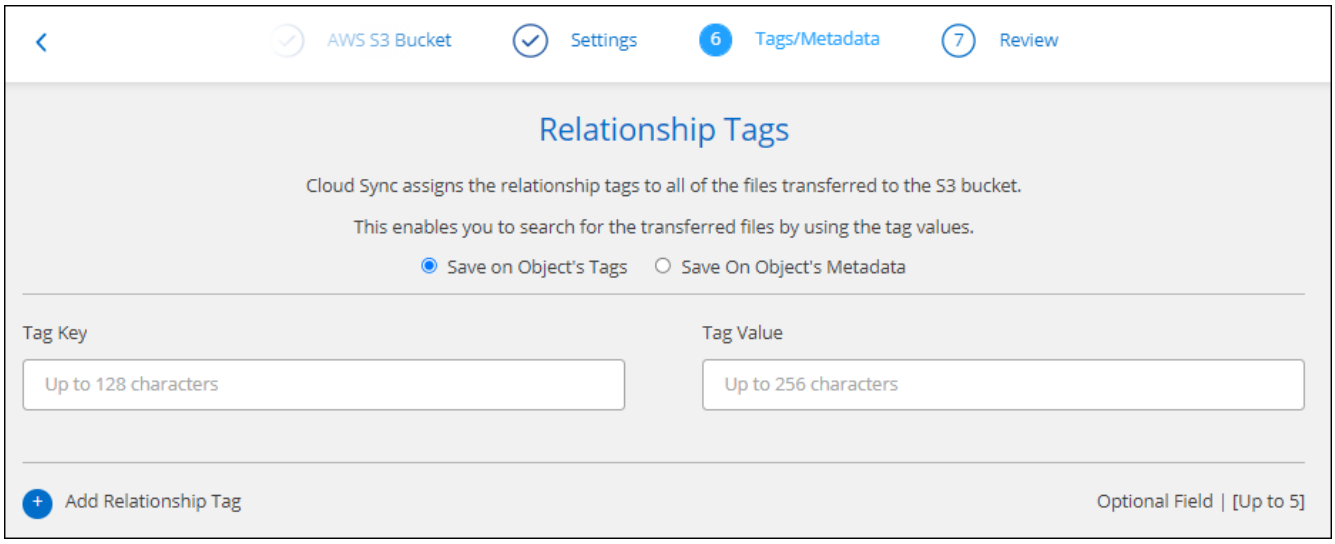
Data di creazione

Quando l'origine è un server SMB, questa impostazione consente di sincronizzare i file creati dopo una data specifica, prima di una data specifica o in un intervallo di tempo specifico.

ACL - Elenco di controllo degli accessi

Copia solo ACL, solo file o ACL e file da un server SMB abilitando un'impostazione quando crei una relazione o dopo averla creata.

10. Nella pagina **Tag/Metadati**, scegli se salvare una coppia chiave-valore come tag su tutti i file trasferiti al bucket S3 oppure assegnare una coppia chiave-valore di metadati a tutti i file.



La stessa funzionalità è disponibile quando si sincronizzano i dati con StorageGRID e IBM Cloud Object Storage. Per Azure e Google Cloud Storage è disponibile solo l'opzione metadati.

11. Esaminare i dettagli della relazione di sincronizzazione, quindi selezionare **Crea relazione**.

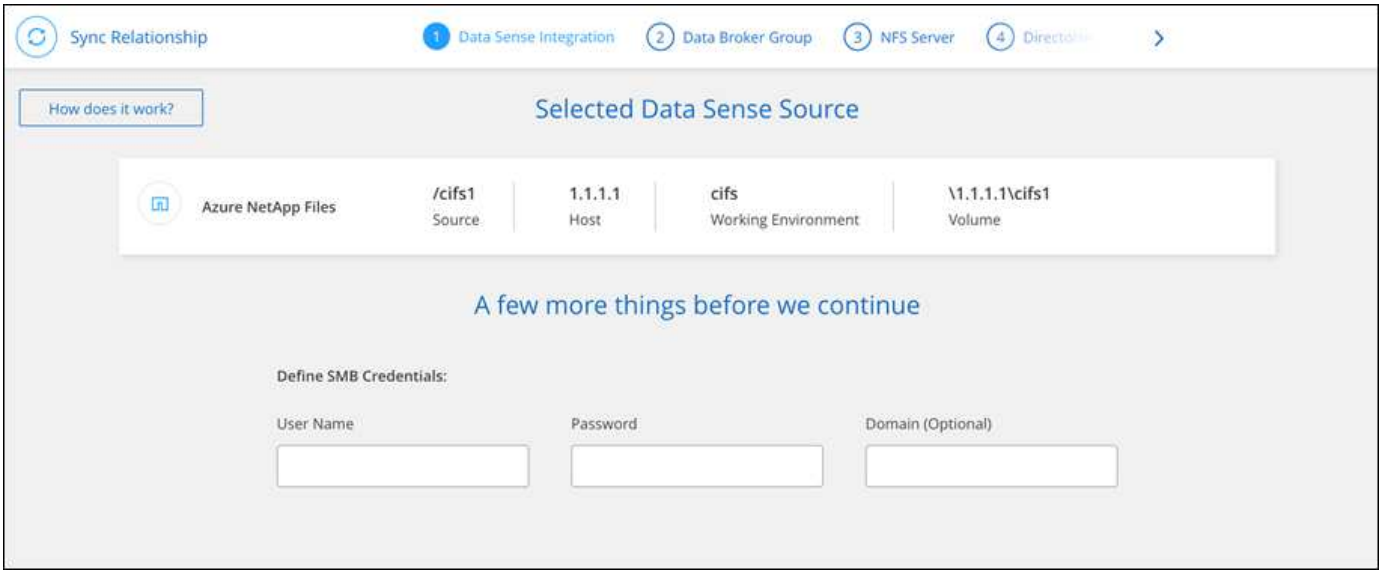
Risultato

Copia e sincronizzazione avvia la sincronizzazione dei dati tra l'origine e la destinazione. Sono disponibili statistiche sulla sincronizzazione che indicano la durata della stessa, se si è interrotta e quanti file sono stati copiati, analizzati o eliminati. Puoi quindi gestire il tuo "relazioni di sincronizzazione" , "gestisci i tuoi broker di dati" , O "creare report per ottimizzare le prestazioni e la configurazione" .

Crea relazioni di sincronizzazione da NetApp Data Classification

Copia e sincronizzazione sono integrati con NetApp Data Classification. Da NetApp Data Classification, puoi selezionare i file di origine che desideri sincronizzare con una posizione di destinazione utilizzando Copia e sincronizzazione.

Dopo aver avviato una sincronizzazione dei dati da NetApp Data Classification, tutte le informazioni sulla fonte sono contenute in un unico passaggio e richiedono solo l'immissione di alcuni dettagli chiave. Quindi scegli la posizione di destinazione per la nuova relazione di sincronizzazione.



"Scopri come avviare una relazione di sincronizzazione da NetApp Data Classification" .

Copia ACL dalle condivisioni SMB in NetApp Copy and Sync

NetApp Copy and Sync può copiare gli elenchi di controllo degli accessi (ACL) tra condivisioni SMB e tra una condivisione SMB e un archivio di oggetti (ad eccezione di ONTAP S3). Se necessario, è anche possibile preservare manualmente gli ACL tra le condivisioni SMB utilizzando robocopy.

Scelte

- Imposta Copia e Sincronizza per copiare automaticamente gli ACL
- Copiare manualmente gli ACL tra le condivisioni SMB

Imposta Copia e Sincronizza per copiare gli ACL

Copia gli ACL tra le condivisioni SMB e tra le condivisioni SMB e l'archiviazione degli oggetti abilitando un'impostazione quando crei una relazione o dopo averla creata.

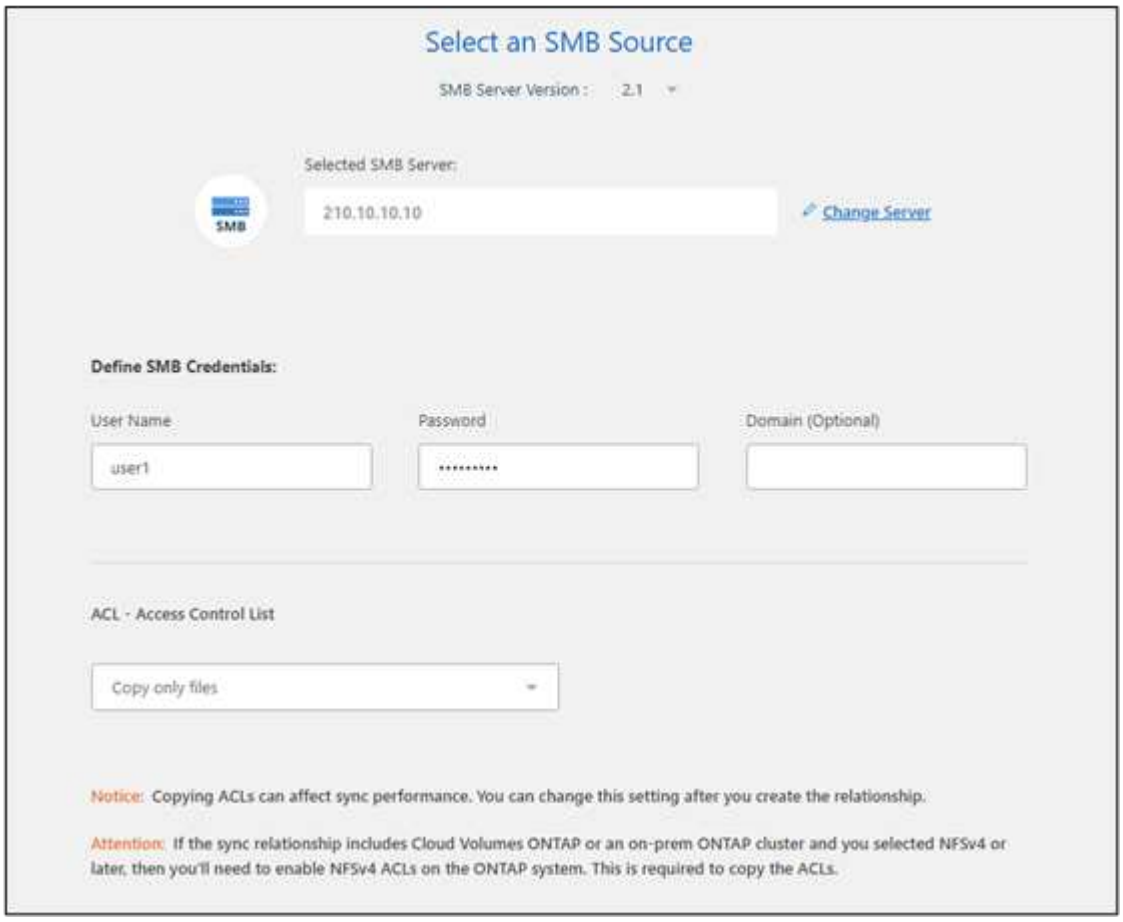
Prima di iniziare

Questa funzionalità funziona con *qualsiasi* tipo di broker di dati: AWS, Azure, Google Cloud Platform o broker di dati on-prem. Il broker di dati on-prem può essere eseguito"qualsiasi sistema operativo supportato" .

Passi per una nuova relazione

1. "Accedi a Copia e Sincronizza" .
2. Da Copia e sincronizza, seleziona **Crea nuova sincronizzazione**.
3. Trascina e rilascia un server SMB o un archivio oggetti come origine e un server SMB o un archivio oggetti come destinazione, quindi seleziona **Continua**.
4. Nella pagina **Server SMB**:
   a. Inserisci un nuovo server SMB oppure seleziona un server esistente e seleziona **Continua**.
   b. Immettere le credenziali per il server SMB.

c. Scegliere **Copia solo file**, **Copia solo ACL** o **Copia file e ACL** e selezionare **Continua**.



5. Seguire le istruzioni rimanenti per creare la relazione di sincronizzazione.

   Quando si copiano gli ACL da SMB all'archiviazione degli oggetti, è possibile scegliere di copiare gli ACL nei tag dell'oggetto o nei metadati dell'oggetto, a seconda della destinazione. Per Azure e Google Cloud Storage è disponibile solo l'opzione metadati.

   La seguente schermata mostra un esempio del passaggio in cui è possibile effettuare questa scelta.

Passaggi per una relazione esistente

1. Passa il mouse sulla relazione di sincronizzazione e seleziona il menu delle azioni.
2. Selezionare **Impostazioni**.
3. Scegliere **Copia solo file**, **Copia solo ACL** o **Copia file e ACL** e selezionare **Continua**.
4. Selezionare **Salva impostazioni**.

> Copia e sincronizzazione conserva gli ACL SMB (autorizzazioni), ma non copia la proprietà di file o cartelle. La proprietà non è inclusa nell'operazione di trasferimento ACL SMB.

Risultato

Durante la sincronizzazione dei dati, Copia e sincronizzazione conserva gli ACL tra l'origine e la destinazione.

Copia manualmente gli ACL tra le condivisioni SMB

È possibile preservare manualmente gli ACL tra le condivisioni SMB utilizzando il comando robocopy di Windows.

> Se è necessario preservare la proprietà (proprietario e gruppo) oltre agli ACL, è possibile utilizzare `robocopy` comando. Utilizzando il `/copyall` flag copia ACL, proprietà e informazioni di controllo.

Passi

1. Identificare un host Windows che abbia accesso completo a entrambe le condivisioni SMB.
2. Se uno degli endpoint richiede l'autenticazione, utilizzare il comando **net use** per connettersi agli endpoint dall'host Windows.

   È necessario eseguire questo passaggio prima di utilizzare Robocopy.
3. Da Copia e sincronizzazione, crea una nuova relazione tra le condivisioni SMB di origine e di destinazione oppure sincronizza una relazione esistente.
4. Una volta completata la sincronizzazione dei dati, eseguire il seguente comando dall'host Windows per sincronizzare gli ACL e la proprietà:

   ```
   robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
   /UNILOG:"[logfilepath]
   ```

   Sia *source* che *target* devono essere specificati utilizzando il formato UNC. Ad esempio: \\<server>\<condivisione>\<percorso>

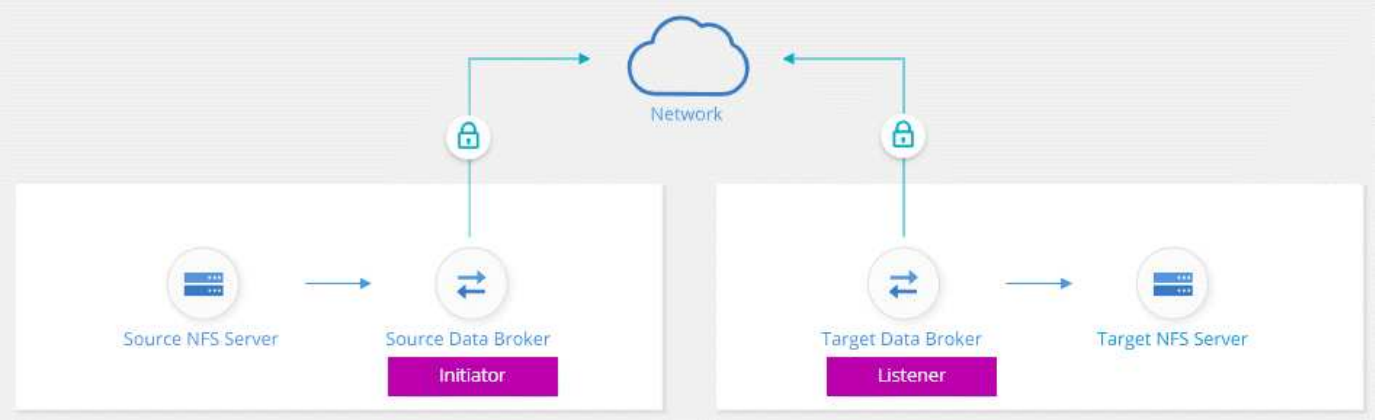
Sincronizza i dati NFS utilizzando la crittografia dei dati in transito in NetApp Copy and Sync

Se la tua azienda ha rigide politiche di sicurezza, puoi sincronizzare i dati NFS utilizzando la crittografia dei dati in transito in NetApp Copy and Sync. Questa funzionalità è supportata da un server NFS a un altro server NFS e da Azure NetApp Files ad Azure NetApp Files.

Ad esempio, potresti voler sincronizzare i dati tra due server NFS che si trovano in reti diverse. Oppure potrebbe essere necessario trasferire in modo sicuro i dati su Azure NetApp Files tra subnet o regioni.

Come funziona la crittografia dei dati in transito

La crittografia dei dati in transito crittografa i dati NFS quando vengono inviati in rete tra due broker di dati. L'immagine seguente mostra una relazione tra due server NFS e due broker di dati:



Un broker di dati svolge la funzione di *iniziatore*. Quando è il momento di sincronizzare i dati, invia una richiesta di connessione all'altro broker di dati, ovvero il listener. Il broker di dati ascolta le richieste sulla porta 443. Se necessario, puoi utilizzare una porta diversa, ma assicurati di verificare che la porta non sia utilizzata da un altro servizio.

Ad esempio, se si sincronizzano i dati da un server NFS locale a un server NFS basato su cloud, è possibile scegliere quale broker di dati ascolta le richieste di connessione e quale le invia.

Ecco come funziona la crittografia in volo:

1. Dopo aver creato la relazione di sincronizzazione, l'iniziatore avvia una connessione crittografata con l'altro broker di dati.
2. Il broker di dati di origine crittografa i dati dalla sorgente utilizzando TLS 1.3.
3. Invia quindi i dati tramite la rete al broker di dati di destinazione.
4. Il broker di dati di destinazione decrittografa i dati prima di inviarli alla destinazione.
5. Dopo la copia iniziale, Copia e sincronizzazione sincronizza tutti i dati modificati ogni 24 ore. Se ci sono dati da sincronizzare, il processo inizia con l'iniziatore che apre una connessione crittografata con l'altro broker di dati.

   Se preferisci sincronizzare i dati più frequentemente,"puoi modificare la pianificazione dopo aver creato la relazione" .

Versioni NFS supportate

- Per i server NFS, la crittografia dei dati in transito è supportata con le versioni NFS 3, 4.0, 4.1 e 4.2.
- Per Azure NetApp Files, la crittografia dei dati in transito è supportata con le versioni NFS 3 e 4.1.

Limitazione del server proxy

Se si crea una relazione di sincronizzazione crittografata, i dati crittografati vengono inviati tramite HTTPS e

non sono instradabili tramite un server proxy.

Cosa ti servirà per iniziare

Assicuratevi di avere quanto segue:

- Due server NFS che si incontrano"requisiti di origine e destinazione" o Azure NetApp Files in due subnet o regioni.
- Gli indirizzi IP o i nomi di dominio completi dei server.
- Posizioni di rete per due broker di dati.

  È possibile selezionare un broker di dati esistente, ma deve fungere da iniziatore. Il broker di dati listener deve essere un *nuovo* broker di dati.

  Se si desidera utilizzare un gruppo di broker di dati esistente, il gruppo deve avere un solo broker di dati. Non sono supportati più broker di dati in un gruppo con relazioni di sincronizzazione crittografate.

  Se non hai ancora implementato un broker di dati, rivedi i requisiti del broker di dati. Poiché si dispone di rigide politiche di sicurezza, assicurarsi di rivedere i requisiti di rete, che includono il traffico in uscita dalla porta 443 e"endpoint Internet" che il broker di dati contatta.

  - "Revisione dell'installazione di AWS"
  - "Esaminare l'installazione di Azure"
  - "Esaminare l'installazione di Google Cloud"
  - "Esaminare l'installazione dell'host Linux"

Sincronizza i dati NFS utilizzando la crittografia dei dati in transito

Creare una nuova relazione di sincronizzazione tra due server NFS o tra Azure NetApp Files, abilitare l'opzione di crittografia in corso e seguire le istruzioni.

Passi

1. "Accedi a Copia e Sincronizza" .
2. Seleziona **Crea nuova sincronizzazione**.
3. Trascinare e rilasciare **NFS Server** nei percorsi di origine e di destinazione oppure * Azure NetApp Files* nei percorsi di origine e di destinazione e selezionare **Sì** per abilitare la crittografia dei dati in transito.
4. Segui le istruzioni per creare la relazione:

   a. **Server NFS**/* Azure NetApp Files*: scegliere la versione NFS e quindi specificare una nuova origine NFS oppure selezionare un server esistente.

   b. **Definisci funzionalità del broker di dati**: definisci quale broker di dati *ascolta* le richieste di connessione su una porta e quale *avvia* la connessione. Fai la tua scelta in base alle tue esigenze di rete.

   c. **Data Broker**: seguire le istruzioni per aggiungere un nuovo data broker di origine o selezionarne uno esistente.

      Notare quanto segue:

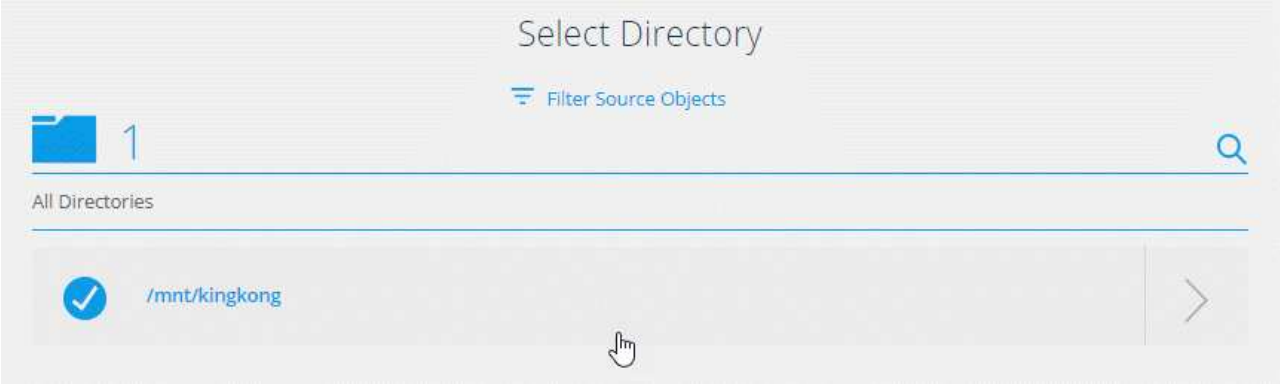
      - Se si desidera utilizzare un gruppo di broker di dati esistente, il gruppo deve avere un solo broker di dati. Non sono supportati più broker di dati in un gruppo con relazioni di sincronizzazione

crittografate.

- Se il broker di dati di origine funge da listener, allora deve essere un nuovo broker di dati.
- Se hai bisogno di un nuovo broker di dati, Copy and Sync ti fornirà le istruzioni per l'installazione. È possibile distribuire il data broker nel cloud oppure scaricare uno script di installazione per il proprio host Linux.

d. **Directory**: scegli le directory che vuoi sincronizzare selezionando tutte le directory oppure effettuando un drill-down e selezionando una sottodirectory.

   Selezionare **Filtra oggetti sorgente** per modificare le impostazioni che definiscono il modo in cui i file e le cartelle di origine vengono sincronizzati e gestiti nella posizione di destinazione.

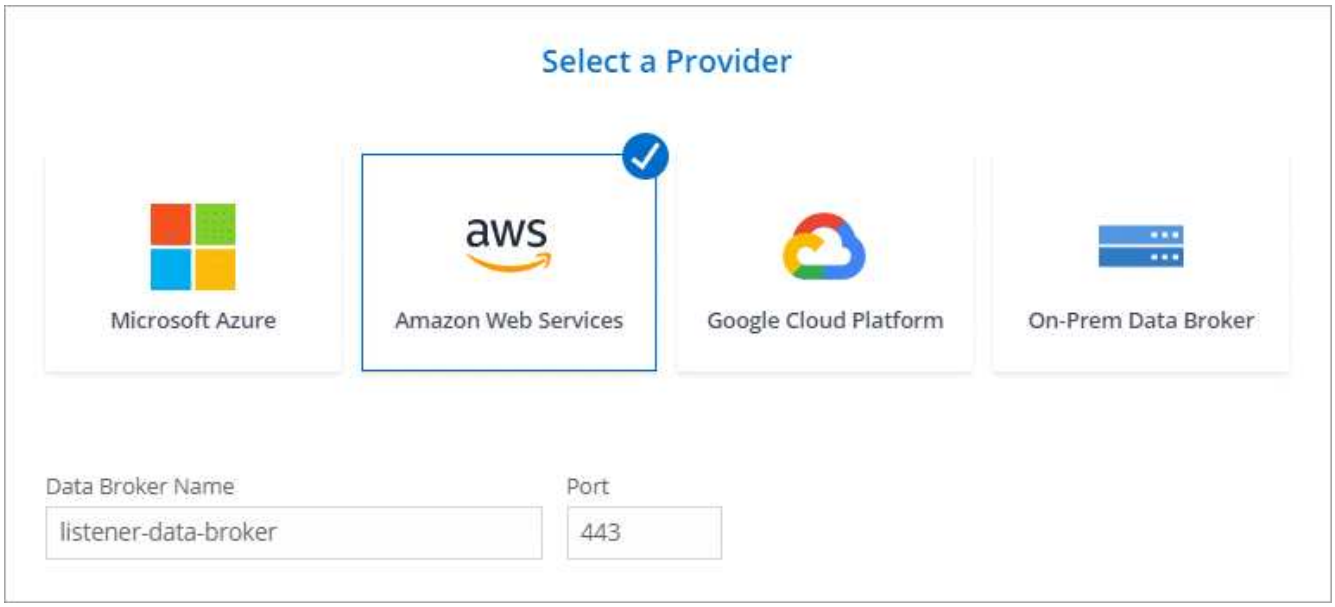


e. **Server NFS di destinazione**/* Azure NetApp Files di destinazione*: scegliere la versione NFS, quindi immettere una nuova destinazione NFS o selezionare un server esistente.

f. **Data Broker di destinazione**: seguire le istruzioni per aggiungere un nuovo data broker di origine o selezionarne uno esistente.

   Se il broker di dati di destinazione funge da listener, allora deve essere un nuovo broker di dati.

   Ecco un esempio del prompt quando il broker di dati di destinazione funge da listener. Notare l'opzione per specificare la porta.

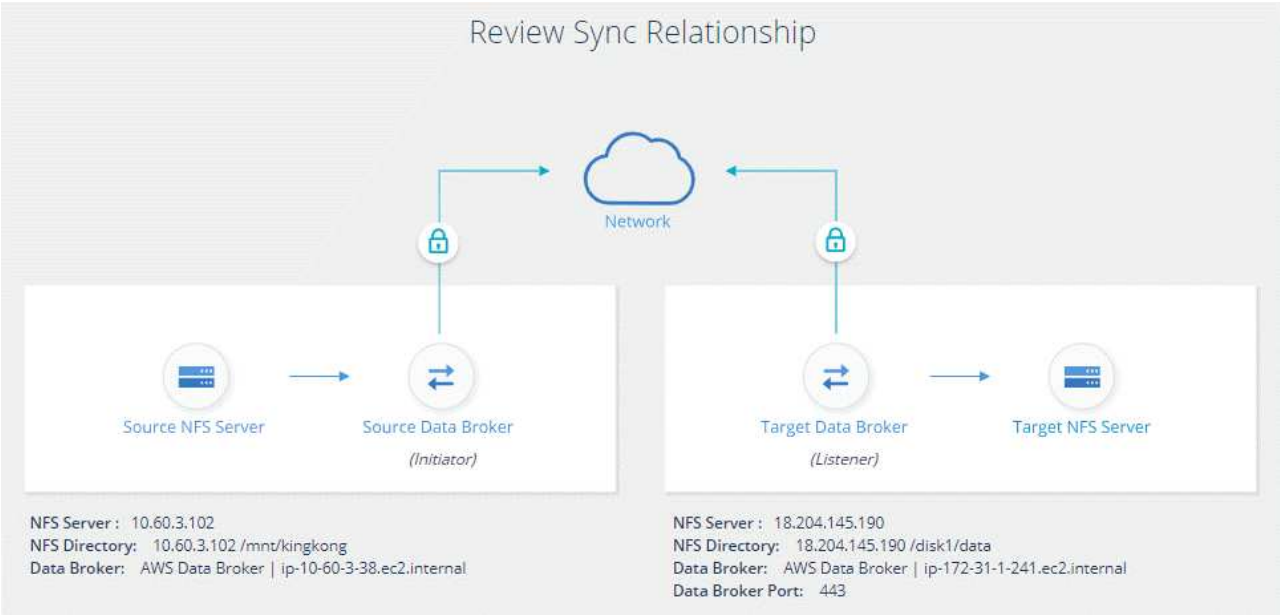


a. **Directory di destinazione**: seleziona una directory di primo livello oppure esegui il drill-down per

selezionare una sottodirectory esistente o per creare una nuova cartella all'interno di un'esportazione.

b. **Impostazioni**: definisce come i file e le cartelle di origine vengono sincronizzati e mantenuti nella posizione di destinazione.

c. **Revisione**: rivedere i dettagli della relazione di sincronizzazione e quindi selezionare **Crea relazione**.



Risultato

Copia e sincronizzazione avvia la creazione della nuova relazione di sincronizzazione. Al termine, seleziona **Visualizza nella dashboard** per visualizzare i dettagli sulla nuova relazione.

Impostare un gruppo di broker di dati per utilizzare un HashiCorp Vault esterno in NetApp Copy and Sync

Quando si crea una relazione di sincronizzazione che richiede credenziali Amazon S3, Azure o Google Cloud, è necessario specificare tali credenziali tramite l'interfaccia utente o l'API NetApp Copy and Sync . Un'alternativa è quella di configurare il gruppo del broker di dati per accedere alle credenziali (o *segreti*) direttamente da un HashiCorp Vault esterno.

Questa funzionalità è supportata tramite l'API Copia e sincronizzazione con relazioni di sincronizzazione che richiedono credenziali Amazon S3, Azure o Google Cloud.

1 Preparare la cassaforte

Preparare il vault per fornire le credenziali al gruppo del broker dati impostando gli URL. Gli URL dei segreti nel vault devono terminare con *Creds*.

2 Preparare il gruppo di broker di dati

Preparare il gruppo di broker di dati a recuperare le credenziali dal vault esterno modificando il file di configurazione locale per ciascun broker di dati nel gruppo.

3 Crea una relazione di sincronizzazione utilizzando l'API

Ora che tutto è impostato, puoi inviare una chiamata API per creare una relazione di sincronizzazione che utilizzi il tuo vault per ottenere i segreti.

Preparare la cassaforte

Dovrai fornire a Copia e Sincronizza l'URL dei segreti nel tuo vault. Preparare il vault impostando tali URL. È necessario impostare gli URL per le credenziali per ogni origine e destinazione nelle relazioni di sincronizzazione che si intende creare.

L'URL deve essere impostato come segue:

```
/<path>/<requestid>/<endpoint-protocol>Creds
```

Sentiero

Il percorso prefisso per raggiungere il segreto. Può trattarsi di qualsiasi valore che sia unico per te.

ID richiesta

Un ID richiesta che devi generare. Quando crei la relazione di sincronizzazione, dovrai fornire l'ID in una delle intestazioni della richiesta API POST.

Protocollo endpoint

Uno dei seguenti protocolli, come definito "nella documentazione post relazione v2" : S3, AZURE o GCP (ognuno deve essere in maiuscolo).

Crediti

L'URL deve terminare con *Creds*.

Esempi

Gli esempi seguenti mostrano gli URL dei segreti.

Esempio per l'URL completo e il percorso per le credenziali di origine

\ http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds

Come puoi vedere nell'esempio, il percorso del prefisso è */my-path/all-secrets/*, l'ID della richiesta è *hb312vdasr2* e l'endpoint di origine è S3.

Esempio per l'URL completo e il percorso per le credenziali di destinazione

\ http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds

Il percorso del prefisso è */my-path/all-secrets/*, l'ID della richiesta è *n32hcbnejk2* e l'endpoint di destinazione è Azure.

Preparare il gruppo di broker di dati

Preparare il gruppo di broker di dati a recuperare le credenziali dal vault esterno modificando il file di configurazione locale per ciascun broker di dati nel gruppo.

Passi

1. Eseguire l'SSH su un broker di dati del gruppo.

2. Modificare il file local.json che si trova in /opt/netapp/databroker/config.
3. Impostare enable su **true** e impostare i campi dei parametri di configurazione in *external-integrations.hashicorp* come segue:

   abilitato
   - Valori validi: vero/falso
   - Tipo: Booleano
   - Valore predefinito: falso
   - Vero: il broker di dati ottiene i segreti dal tuo HashiCorp Vault esterno
   - Falso: il broker di dati memorizza le credenziali nel suo vault locale

   URL
   - Tipo: stringa
   - Valore: l'URL del tuo vault esterno

   sentiero
   - Tipo: stringa
   - Valore: aggiungi il prefisso al percorso del segreto con le tue credenziali

   Rifiuta-non autorizzato
   - Determina se si desidera che il broker di dati rifiuti il vault esterno non autorizzato
   - Tipo: Booleano
   - Predefinito: falso

   metodo di autenticazione
   - Il metodo di autenticazione che il broker di dati deve utilizzare per accedere alle credenziali dal vault esterno
   - Tipo: stringa
   - Valori validi: "aws-iam" / "role-app" / "gcp-iam"

   nome-ruolo
   - Tipo: stringa
   - Il nome del tuo ruolo (nel caso in cui utilizzi aws-iam o gcp-iam)

   Secretid e rootid
   - Tipo: stringa (nel caso in cui si utilizzi app-role)

   Spazio dei nomi
   - Tipo: stringa
   - Il tuo spazio dei nomi (intestazione X-Vault-Namespace se necessario)

4. Ripetere questi passaggi per tutti gli altri broker di dati nel gruppo.

Esempio di autenticazione aws-role

```
{
          “external-integrations”: {
                  “hashicorp”: {
                          “enabled”: true,
                          “url”: “https://example.vault.com:8200”,
                          “path”: ““my-path/all-secrets”,
                          “reject-unauthorized”: false,
                          “auth-method”: “aws-role”,
                          “aws-role”: {
                                “role-name”: “my-role”
                          }
                  }
        }
}
```

Esempio di autenticazione gcp-iam

```
{
"external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": http://ip-10-20-30-55.ec2.internal:8200,
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
"gcp-iam": {
          "role-name": "my-iam-role"
      }
    }
  }
}
```

Impostare le autorizzazioni quando si utilizza l’autenticazione gcp-iam

Se si utilizza il metodo di autenticazione *gcp-iam*, il broker di dati deve disporre della seguente autorizzazione GCP:

```
- iam.serviceAccounts.signJwt
```

"Scopri di più sui requisiti di autorizzazione GCP per il broker di dati" .

Creazione di una nuova relazione di sincronizzazione utilizzando i segreti del vault

Ora che tutto è impostato, puoi inviare una chiamata API per creare una relazione di sincronizzazione che utilizzi il tuo vault per ottenere i segreti.

Pubblica la relazione utilizzando l'API REST Copia e Sincronizza.

```
Headers:
Authorization: Bearer <user-token>
Content-Type: application/json
x-account-id: <accountid>
x-netapp-external-request-id-src: request ID as part of path for source
credentials
x-netapp-external-request-id-trg: request ID as part of path for target
credentials
Body: post relationship v2 body
```

- Per ottenere un token utente e l'ID dell'account NetApp Console ,"fare riferimento a questa pagina nella documentazione" .
- Per costruire un corpo per la tua relazione post, "fare riferimento alla chiamata API relationships-v2" .

Esempio

Esempio per la richiesta POST:

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik…"
Body:
{
"dataBrokerId": "5e6e111d578dtyuu1555sa60",
"source": {
        "protocol": "s3",
        "s3": {
                "provider": "sgws",
                "host": "1.1.1.1",
                "port": "443",
                "bucket": "my-source"
     },
"target": {
        "protocol": "s3",
        "s3": {
                "bucket": "my-target-bucket"
        }
    }
}
```