Tutorial

Cloud Manager 3.8

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/it-it/occm38/task_sync_copying_acls.html on March 25, 2024. Always check docs.netapp.com for the latest.

Sommario

Tutorial

Copia degli ACL tra le condivisioni SMB

Cloud Sync può copiare gli elenchi di controllo degli accessi (ACL) tra una condivisione SMB di origine e una condivisione SMB di destinazione. Se necessario, è possibile conservare manualmente gli ACL utilizzando robocopy.

Scelte

- Impostare Cloud Sync per la copia automatica degli ACL
- Copiare manualmente gli ACL

Configurazione di Cloud Sync per copiare gli ACL tra server SMB

Copiare gli ACL tra server SMB attivando un'impostazione quando si crea una relazione o dopo la creazione di una relazione.

Questa funzionalità è disponibile per le nuove relazioni di sincronizzazione create dopo la release 23 febbraio 2020. Se si desidera utilizzare questa funzione con le relazioni esistenti create prima di tale data, sarà necessario ricreare la relazione.

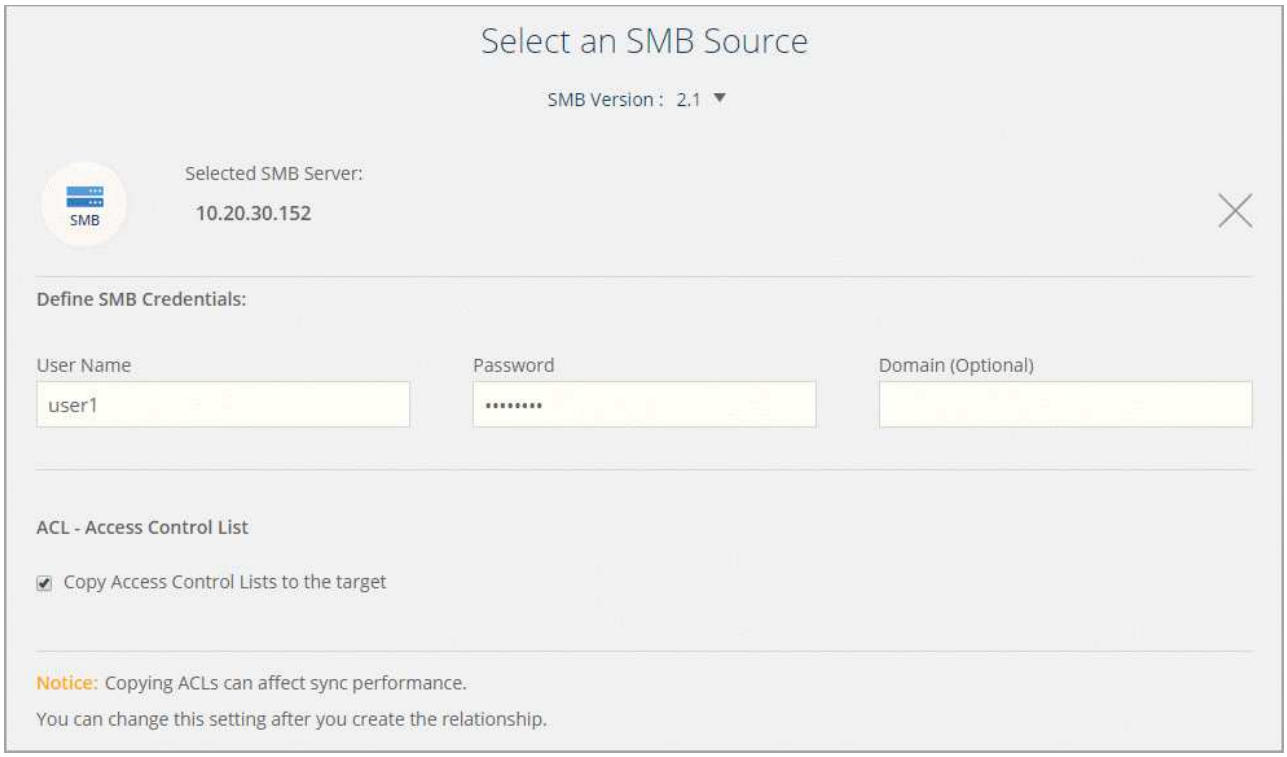
Di cosa hai bisogno

- Una nuova relazione di sincronizzazione o una relazione di sincronizzazione esistente creata dopo la release del 23 febbraio 2020.
- Qualsiasi tipo di broker di dati.

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

Passaggi per una nuova relazione

1. Da Cloud Sync, fare clic su **Crea nuova sincronizzazione**.
2. Trascinare **SMB Server** nell'origine e nella destinazione e fare clic su **Continue** (continua).
3. Nella pagina **SMB Server**:
   a. Immettere un nuovo server SMB o selezionare un server esistente e fare clic su **continua**.
   b. Immettere le credenziali per il server SMB.
   c. Selezionare **Copy Access Control Lists to the target** (Copia elenchi di controllo degli accessi nella destinazione) e fare clic su **Continue** (continua).



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

Passaggi per una relazione esistente

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Impostazioni**.
3. Selezionare **Copy Access Control Lists to the target** (Copia elenchi di controllo degli accessi nella destinazione).
4. Fare clic su **Save Settings** (Salva impostazioni).

Risultato

Durante la sincronizzazione dei dati, Cloud Sync preserva gli ACL tra le condivisioni SMB di origine e di destinazione.

Copia manuale degli ACL

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

Fasi

1. Identificare un host Windows con 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.

   Eseguire questa procedura prima di utilizzare robocopy.

3. Da Cloud Sync, creare una nuova relazione tra le condivisioni SMB di origine e di destinazione o sincronizzare 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]
```

È necessario specificare sia *source* che *target* utilizzando il formato UNC. Ad esempio: <server>/<share>/<path>

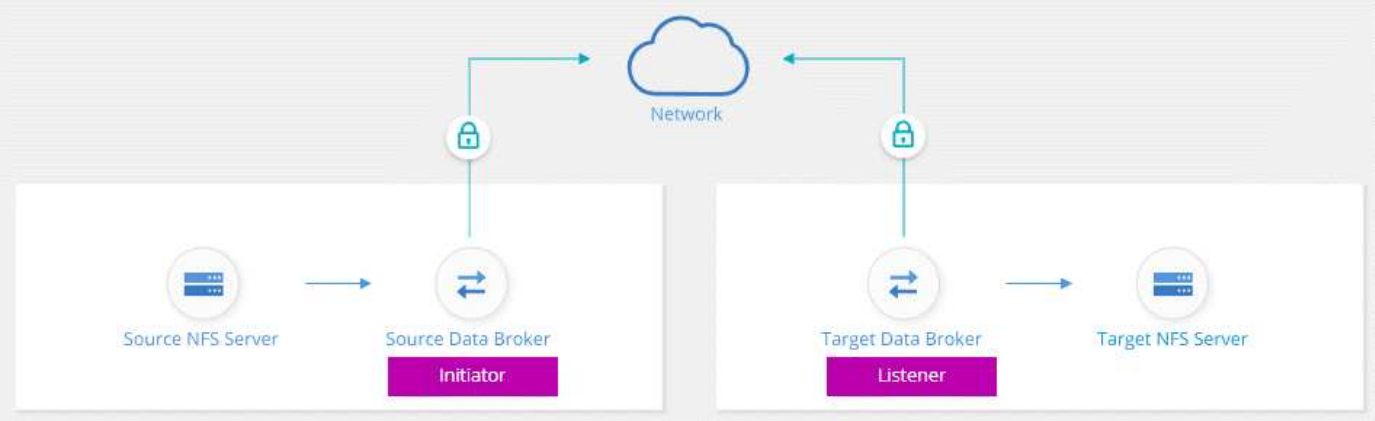
Sincronizzazione dei dati NFS con crittografia data-in-flight

Se la tua azienda ha policy di sicurezza rigorose, puoi sincronizzare i dati NFS utilizzando la crittografia data-in-flight. Questa funzionalità è supportata da un server NFS a un altro server NFS e da Azure NetApp Files a Azure NetApp Files.

Ad esempio, è possibile sincronizzare i dati tra due server NFS che si trovano in reti diverse. In alternativa, potrebbe essere necessario trasferire in modo sicuro i dati su Azure NetApp Files tra sottoreti o regioni.

Come funziona la crittografia dei dati in volo

La crittografia Data-in-flight crittografa i dati NFS quando vengono inviati in rete tra due broker di dati. La seguente immagine mostra una relazione tra due server NFS e due broker di dati:



Un data broker funziona come *initiator*. Quando è il momento di sincronizzare i dati, invia una richiesta di connessione all’altro data broker, che è il *listener*. Il data broker ascolta le richieste sulla porta 443. Se necessario, è possibile utilizzare un’altra porta, ma assicurarsi che la porta non sia utilizzata da un altro servizio.

Ad esempio, se si sincronizzano i dati da un server NFS on-premise a un server NFS basato sul cloud, è possibile scegliere quale broker di dati ascoltare le richieste di connessione e quale inviarle.

Ecco come funziona la crittografia in-flight:

1. Dopo aver creato la relazione di sincronizzazione, l’iniziatore avvia una connessione crittografata con l’altro data broker.
2. Il broker dei dati di origine crittografa i dati dall’origine utilizzando TLS 1.3.
3. Quindi, invia i dati in rete al data broker di destinazione.
4. Il broker di dati di destinazione decrta i dati prima di inviarli alla destinazione.
5. Dopo la copia iniziale, il servizio sincronizza tutti i dati modificati ogni 24 ore. Se sono presenti dati da

sincronizzare, il processo inizia con l'iniziatore che apre una connessione crittografata con l'altro data broker.

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

Versioni NFS supportate

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

Cosa ti serve per iniziare

Assicurarsi di disporre di quanto segue:

- Due server NFS che si incontrano "requisiti di origine e destinazione" O Azure NetApp Files in due sottoreti 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 data broker esistente, ma deve funzionare come iniziatore. Il data broker listener deve essere un *new* data broker.

  Se non hai ancora implementato un data broker, esamina i requisiti del data broker. Poiché si dispone di policy di sicurezza rigorose, assicurarsi di esaminare i requisiti di rete, che includono il traffico in uscita dalla porta 443 e da "endpoint internet" che il data broker contatta.

  - "Esaminare l'installazione di AWS"
  - "Esaminare l'installazione di Azure"
  - "Esaminare l'installazione di GCP"
  - "Esaminare l'installazione dell'host Linux"

Sincronizzazione dei dati NFS con crittografia data-in-flight

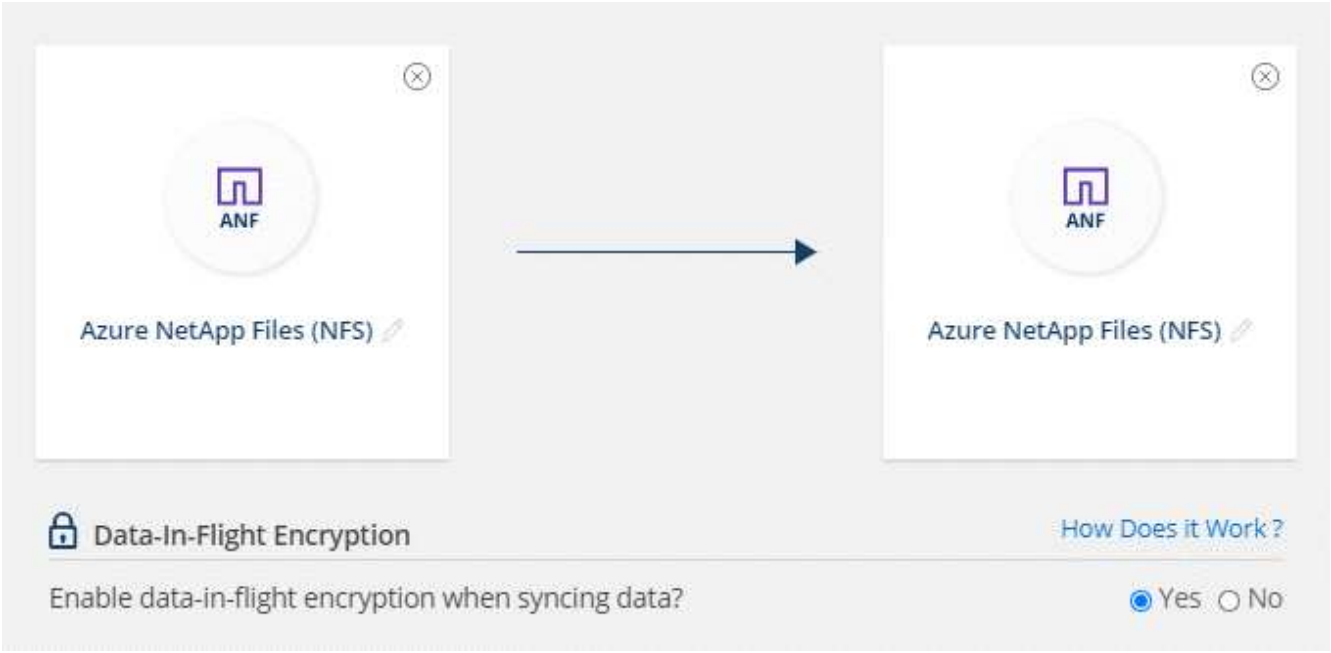
Creare una nuova relazione di sincronizzazione tra due server NFS o tra Azure NetApp Files, attivare l'opzione di crittografia in-flight e seguire le istruzioni.

Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Trascinare **server NFS** nelle posizioni di origine e destinazione o **Azure NetApp Files** nelle posizioni di origine e destinazione e selezionare **Sì** per attivare la crittografia dei dati in volo.

   La seguente immagine mostra ciò che si desidera selezionare per sincronizzare i dati tra due server NFS:

La seguente immagine mostra ciò che si desidera selezionare per sincronizzare i dati tra Azure NetApp Files:



3. Seguire le istruzioni per creare la relazione:

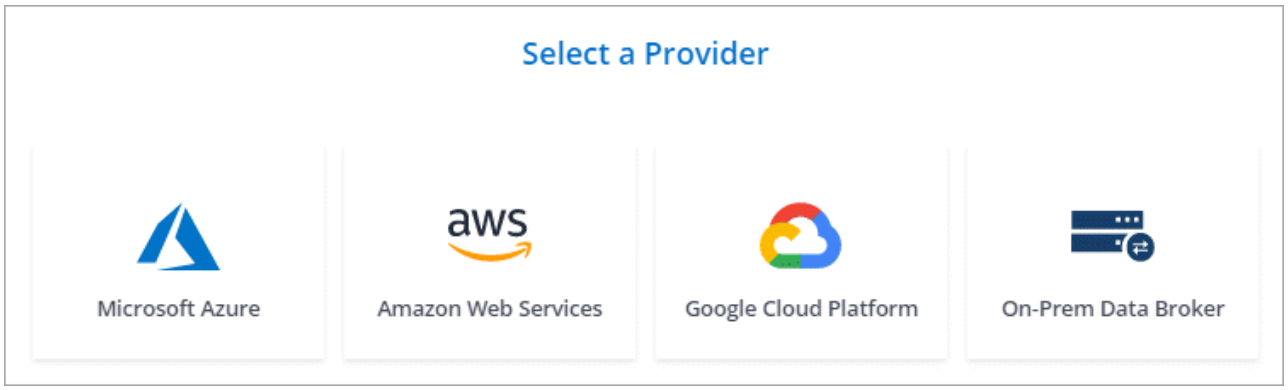
   a. **Server NFS/Azure NetApp Files**: Scegliere la versione di NFS e specificare una nuova origine NFS oppure selezionare un server esistente.

   b. **Definisci funzionalità Data Broker**: Definire quale broker di dati *ascolta* per le richieste di connessione su una porta e quale *avvia* la connessione. Scegli la tua scelta in base ai tuoi requisiti di rete.

   c. **Data Broker**: Seguire le istruzioni per aggiungere un nuovo data broker di origine o selezionare un data broker esistente.

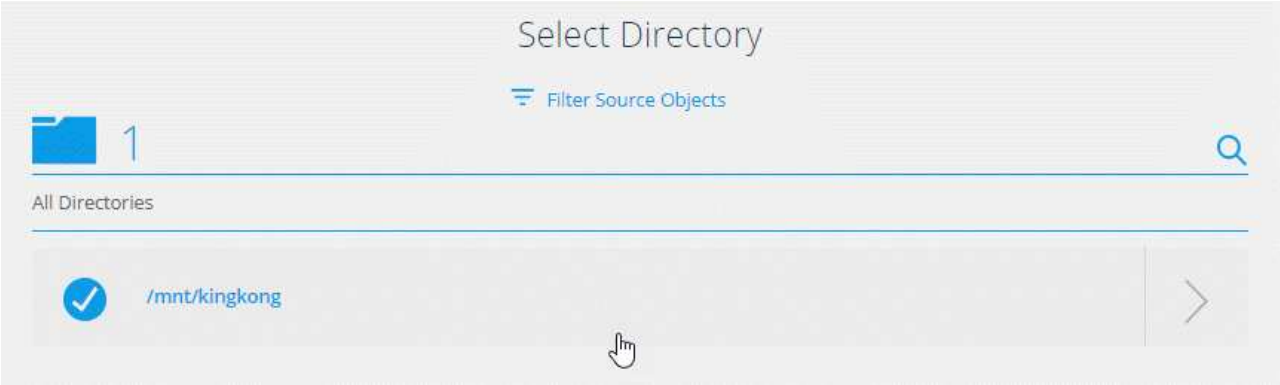
      Se il broker di dati di origine agisce come listener, deve essere un nuovo broker di dati.

Se è necessario un nuovo data broker, Cloud Sync richiede le istruzioni per l'installazione. Puoi implementare il data broker nel cloud o scaricare uno script di installazione per il tuo host Linux.



d. **Directory**: Scegliere le directory che si desidera sincronizzare selezionando tutte le directory oppure eseguendo il drill-down e selezionando una sottodirectory.

   Fare clic su **Filter Source Objects** (Filtra oggetti origine) per modificare le impostazioni che definiscono la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.

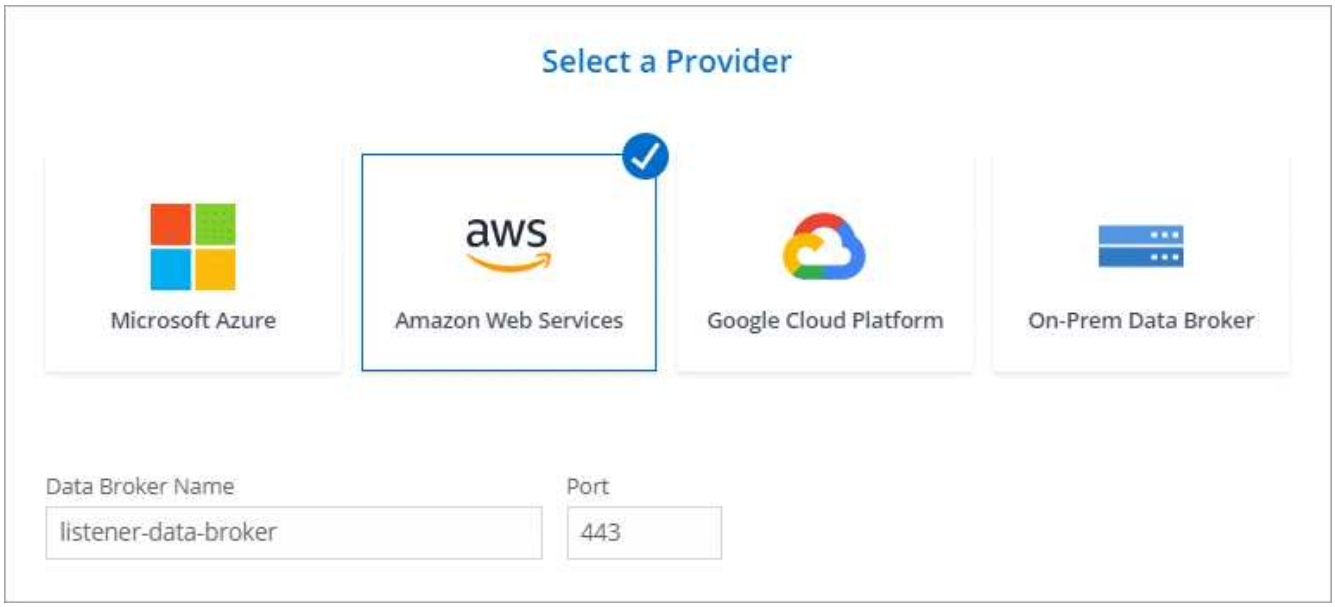


e. **Server NFS di destinazione/Azure NetApp Files di destinazione**: Scegliere la versione di NFS, quindi inserire una nuova destinazione NFS o selezionare un server esistente.

f. **Target Data Broker**: Seguire le istruzioni per aggiungere un nuovo broker di dati di origine o selezionare un broker di dati esistente.

   Se il data broker di destinazione agisce come listener, deve essere un nuovo data broker.

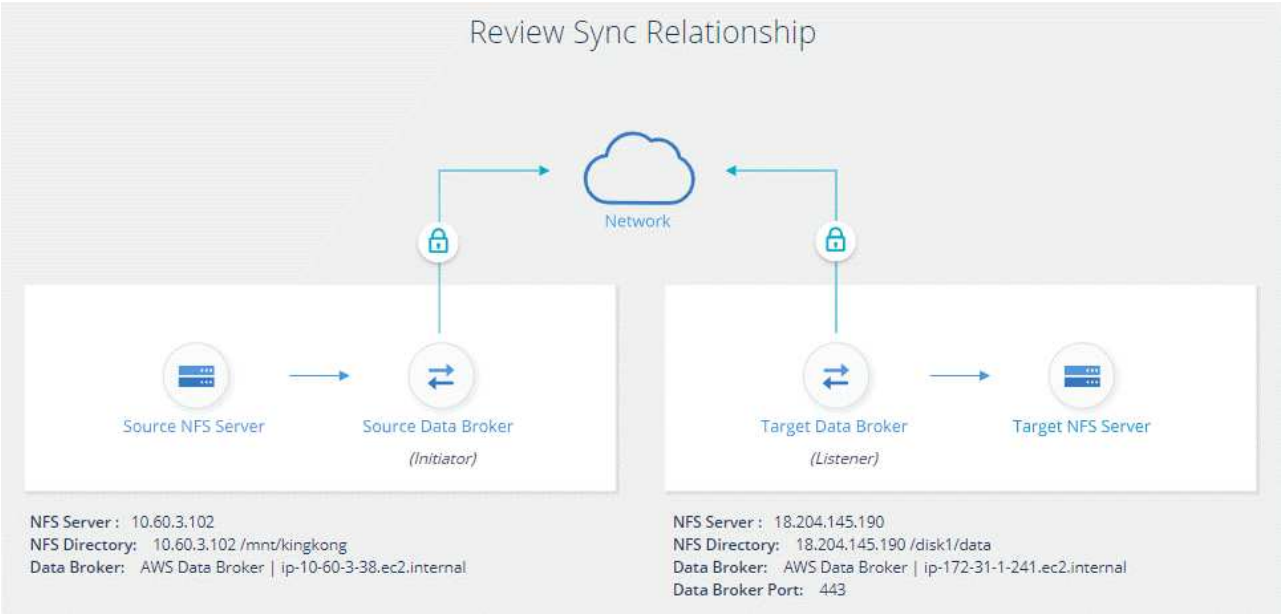
   Ecco un esempio del prompt quando il broker di dati di destinazione funziona come listener. Notare l'opzione per specificare la porta.



a. **Directory di destinazione**: Selezionare una directory di primo livello oppure eseguire il drill-down per selezionare una sottodirectory esistente o per creare una nuova cartella all'interno di un'esportazione.

b. **Impostazioni**: Consente di definire la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.

c. **Revisione**: Esaminare i dettagli della relazione di sincronizzazione, quindi fare clic su **Crea relazione**.



Risultato

Cloud Sync inizia a creare la nuova relazione di sincronizzazione. Al termine, fare clic su **View in Dashboard** (Visualizza in Dashboard) per visualizzare i dettagli sulla nuova relazione.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.