Sincronizza i dati tra un'origine e una destinazione

BlueXP copy and sync

NetApp
April 08, 2024

Sommario

Sincronizza i dati tra un’origine e una destinazione

Creare relazioni di sincronizzazione

Quando si crea una relazione di sincronizzazione, il servizio di copia e sincronizzazione BlueXP copia i file dall’origine alla destinazione. Dopo la copia iniziale, il servizio sincronizza tutti i dati modificati ogni 24 ore.

Prima di creare alcuni tipi di relazioni di sincronizzazione, è necessario creare un ambiente di lavoro in BlueXP.

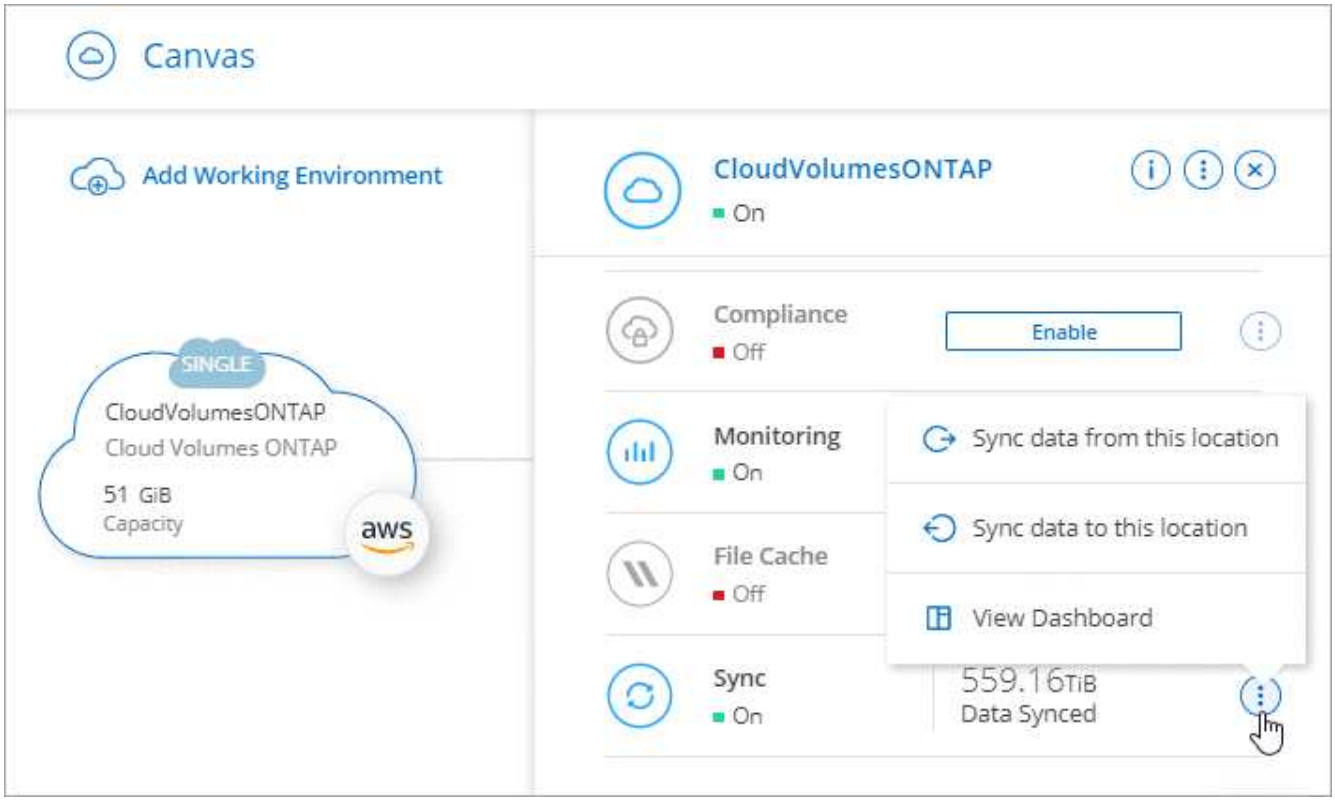
Creare relazioni di sincronizzazione per specifici tipi di ambienti di lavoro

Se si desidera creare relazioni di sincronizzazione per uno dei seguenti elementi, è necessario innanzitutto creare o individuare l’ambiente di lavoro:

- Amazon FSX per ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Cluster ONTAP on-premise

Fasi

1. Creare o scoprire l’ambiente di lavoro.
    - "Creare un ambiente di lavoro Amazon FSX per ONTAP"
    - "Configurazione e rilevamento di Azure NetApp Files"
    - "Avvio di Cloud Volumes ONTAP in AWS"
    - "Lancio di Cloud Volumes ONTAP in Azure"
    - "Lancio di Cloud Volumes ONTAP in Google Cloud"
    - "Aggiunta di sistemi Cloud Volumes ONTAP esistenti"
    - "Alla scoperta dei cluster ONTAP"
2. Selezionare **Canvas**.
3. Selezionare un ambiente di lavoro che corrisponda a uno dei tipi elencati sopra.
4. Selezionare il menu delle azioni accanto a Sincronizza.



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

Creare altri tipi di relazioni di sincronizzazione

Utilizzare questa procedura per sincronizzare i dati da o verso un tipo di storage supportato diverso da Amazon FSX per cluster ONTAP, Azure NetApp Files, Cloud Volumes ONTAP o ONTAP on-premise. I passaggi riportati di seguito forniscono un esempio che mostra come impostare una relazione di sincronizzazione da un server NFS a un bucket S3.

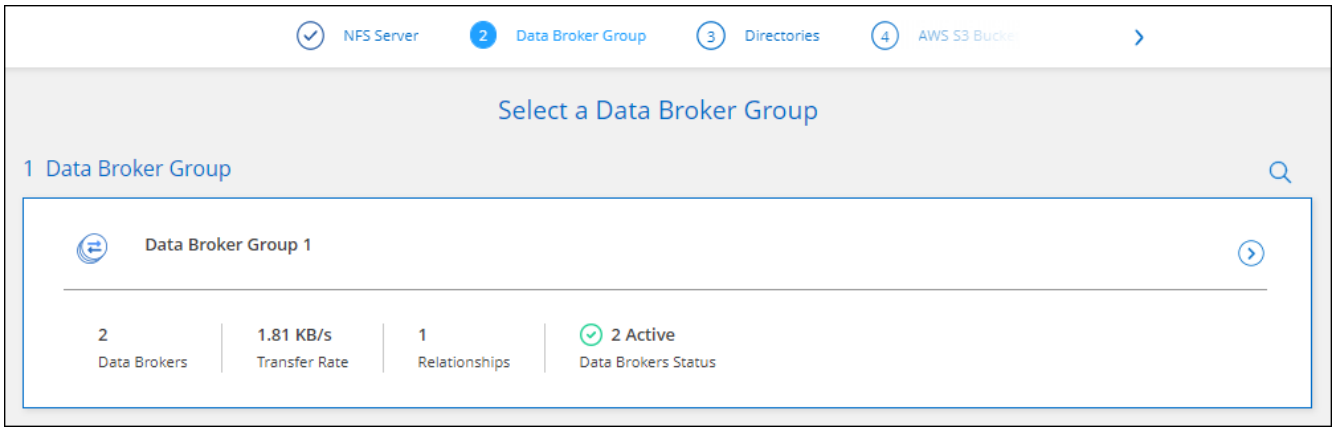
1. In BlueXP, selezionare **Sync**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione.

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

3. Nella pagina **NFS Server**, inserire 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 per broker di dati in AWS, Azure o Google Cloud Platform, oppure per installare il software per broker di dati su un host Linux esistente.

   Per ulteriori informazioni, consultare le seguenti pagine:

   - "Creare un data broker in AWS"
   - "Crea un data broker in Azure"
   - "Crea un data broker in Google Cloud"
   - "Installazione del data broker su un host Linux"
5. Dopo aver installato il data broker, selezionare **continua**.

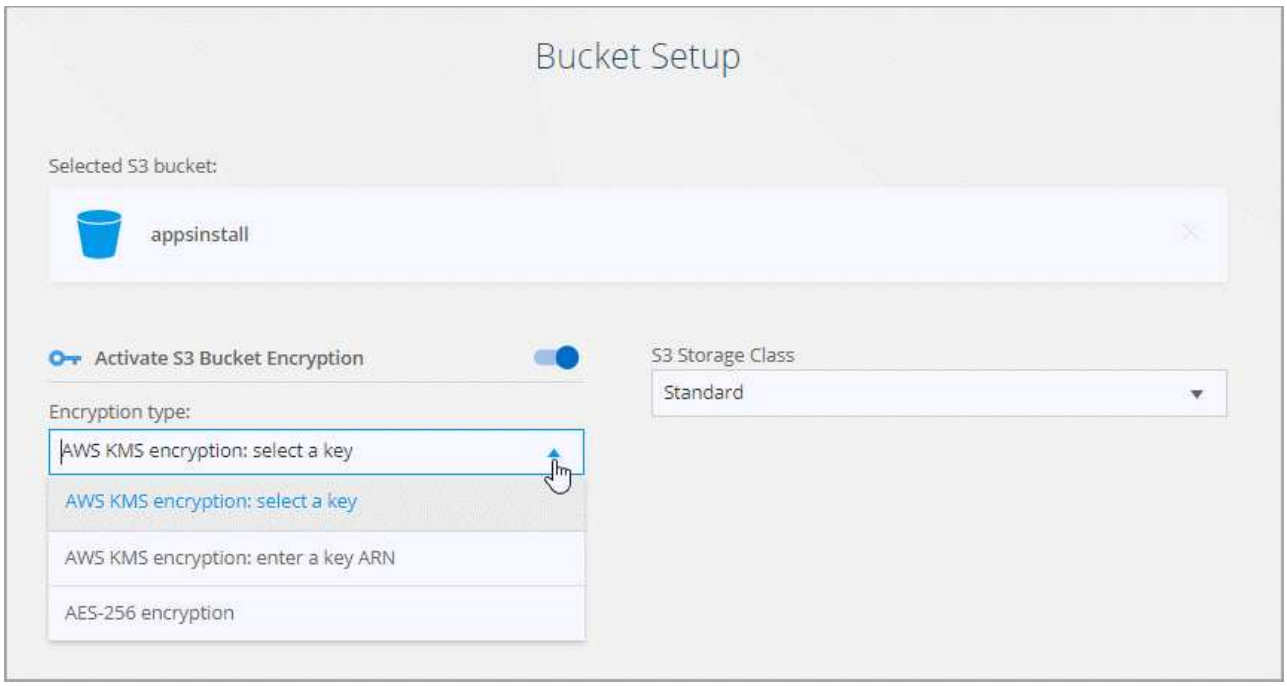


6. nella pagina **Directory**, selezionare una directory o una sottodirectory di livello superiore.

   Se BlueXP copy and Sync non riesce a recuperare le esportazioni, selezionare **Add Export Manually** (Aggiungi esportazione manualmente) e inserire 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 **bucket AWS S3**, selezionare un bucket:
   - Eseguire il drill-down per selezionare una cartella esistente all'interno del bucket o per selezionare una nuova cartella creata all'interno del bucket.
   - Selezionare **Aggiungi all'elenco** per selezionare un bucket S3 non associato all'account AWS. "Al bucket S3 devono essere applicate autorizzazioni specifiche".
8. Nella pagina **Bucket Setup**, impostare il bucket:
   - Scegliere se attivare la crittografia del bucket S3, quindi selezionare una chiave AWS KMS, immettere l'ARN di una chiave KMS o selezionare la crittografia AES-256.
   - Selezionare una classe di storage S3. "Visualizzare le classi di storage supportate".



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

Pianificazione

Scegliere una pianificazione ricorrente per le sincronizzazioni future o disattivare la pianificazione della sincronizzazione. È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

Timeout di sincronizzazione

Definire se la copia e la sincronizzazione di BlueXP devono annullare una sincronizzazione dei dati se la sincronizzazione non è stata completata nel numero specificato di minuti, ore o giorni.

Notifiche

Consente di scegliere se ricevere notifiche di copia e sincronizzazione BlueXP nel Centro notifiche di BlueXP. È possibile attivare le notifiche per la sincronizzazione dei dati riuscita, per la sincronizzazione dei dati non riuscita e per la sincronizzazione dei dati annullata.

Tentativi

Definire il numero di tentativi di copia e sincronizzazione di BlueXP per sincronizzare un file prima di ignorarlo.

Sincronizzazione continua

Dopo la sincronizzazione iniziale dei dati, BlueXP Copy and Sync ascolta le modifiche apportate al bucket S3 di origine o al bucket Google Cloud Storage e sincronizza continuamente le modifiche apportate al target nel momento in cui si verificano. Non è necessario eseguire una nuova scansione dell'origine a intervalli pianificati.

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

Se si attiva questa impostazione, questa influisce sulle altre funzioni nel modo seguente:

- La pianificazione della sincronizzazione è disattivata.
- Vengono ripristinati i valori predefiniti delle seguenti impostazioni: Timeout di sincronizzazione, file modificati di recente e Data di modifica.
- Se S3 è l'origine, il filtro per dimensione sarà attivo solo per gli eventi di copia (non per gli eventi di eliminazione).
- Una volta creata la relazione, è possibile solo accelerare o eliminare la relazione. 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. A tale scopo, attenersi alla seguente procedura:

  i. Vai alla console di Google Cloud per il progetto del bucket esterno.
  ii. Accedere a **archiviazione cloud > Impostazioni > account del servizio archiviazione cloud**.
  iii. Aggiornare il file local.json:

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

iv. Riavviare il data broker:

   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 un rapporto di sincronizzazione continua con un bucket esterno non sarà in grado di creare un'altra relazione di sincronizzazione continua con un bucket nel progetto.

Confronta per

Scegliere se la copia e la sincronizzazione di BlueXP devono confrontare determinati attributi quando si determina se un file o una directory è stata modificata e deve essere nuovamente sincronizzata.

Anche se si deselezionano questi attributi, BlueXP copy and Sync confronta ancora l'origine con la destinazione controllando i percorsi, le dimensioni dei file e i nomi dei file. In caso di modifiche, i file e le directory vengono sincronizzati.

È possibile scegliere di attivare o disattivare la copia e la sincronizzazione BlueXP confrontando i seguenti attributi:

- **Mtime**: L'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 gli oggetti

Attivare questa opzione per copiare tag e metadati dello storage a oggetti. Se un utente modifica i metadati sull'origine, BlueXP copia e sincronizza questo oggetto nella sincronizzazione successiva, ma se un utente modifica i tag sull'origine (e non i dati stessi), BlueXP copia e sincronizza 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 dei seguenti endpoint:

- AWS S3
- Azure Blob
- Storage Google Cloud

- Storage a oggetti IBM Cloud
- StorageGRID

File modificati di recente

Scegliere di escludere i file modificati di recente prima della sincronizzazione pianificata.

Elimina file in origine

Scegliere di eliminare i file dalla posizione di origine dopo che BlueXP copia e Sync copia i file nella posizione di destinazione. Questa opzione include il rischio di perdita dei dati perché i file di origine vengono cancellati dopo la copia.

Se si attiva 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, è necessario riavviare: `pm2 restart all`.

Eliminare i file di destinazione

Scegliere di eliminare i file dalla posizione di destinazione, se sono stati eliminati dall'origine. Per impostazione predefinita, i file non vengono mai eliminati dalla posizione di destinazione.

Tipi di file

Definire i tipi di file da includere in ogni sincronizzazione: File, directory, collegamenti simbolici e collegamenti hardware.

> I collegamenti hardware sono disponibili solo per le relazioni NFS-NFS non protette. Gli utenti saranno limitati a un processo scanner e a una concorrenza scanner e le scansioni devono essere eseguite da una directory principale.

Escludi estensioni file

Specificare il regex o le estensioni del file da escludere dalla sincronizzazione digitando l'estensione del file e premendo **Invio**. Ad esempio, digitare *log* o *.log* per escludere i file *.log. Non è necessario un separatore per più interni. Il seguente video fornisce una breve demo:

► https://docs.netapp.com/it-it/bluexp-copy-sync//media/video_file_extensions.mp4 *(video)*

> Le espressioni regex, o regolari, differiscono dai caratteri jolly o dalle espressioni glob. Questa caratteristica **only** funziona con regex.

Escludi directory

Specificare un massimo di 15 regex o directory da escludere dalla sincronizzazione digitando il nome o il percorso completo della directory e premendo **Invio**. Le directory .copy-offload, .snapshot, ~snapshot

sono escluse per impostazione predefinita.

> Le espressioni regex, o regolari, differiscono dai caratteri jolly o dalle espressioni glob. Questa caratteristica **only** funziona con regex.

Dimensione del file

Scegliere di sincronizzare tutti i file indipendentemente dalle dimensioni o solo i file che si trovano in un intervallo di dimensioni specifico.

Data di modifica

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

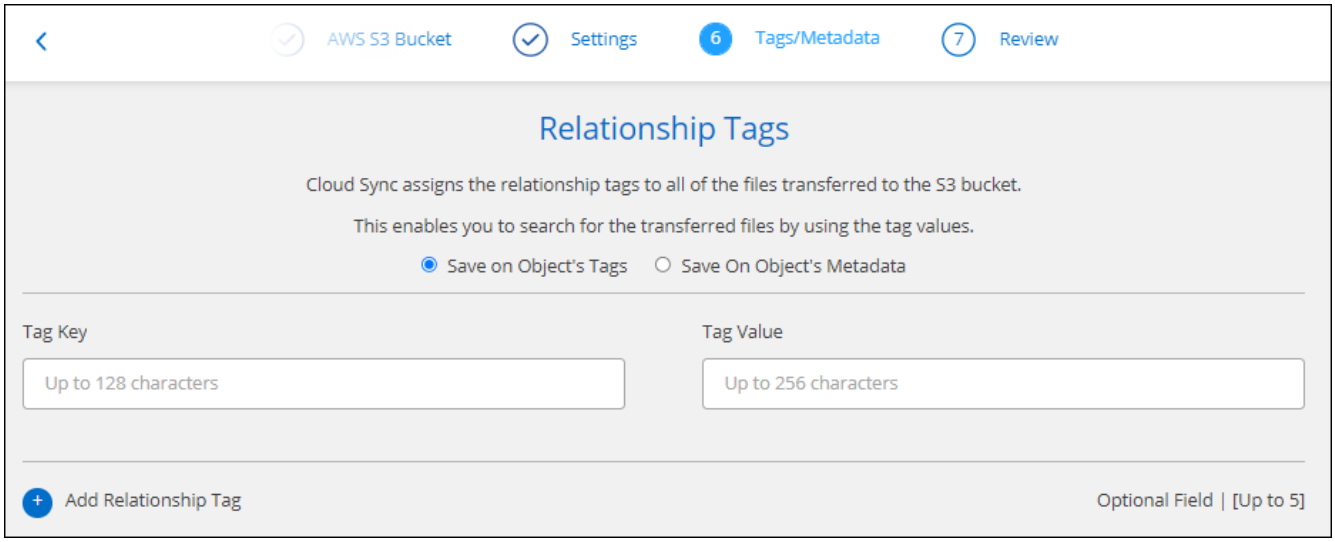
Data di creazione

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

ACL - Access Control List (elenco di controllo degli accessi)

Copia solo ACL, solo file o ACL e file da un server SMB attivando un'impostazione quando si crea una relazione o dopo la creazione di una relazione.

10. Nella pagina **Tags/Metadata**, scegliere se salvare una coppia valore-chiave come tag su tutti i file trasferiti al bucket S3 o assegnare una coppia valore-chiave di metadati su tutti i file.



> Questa 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**.

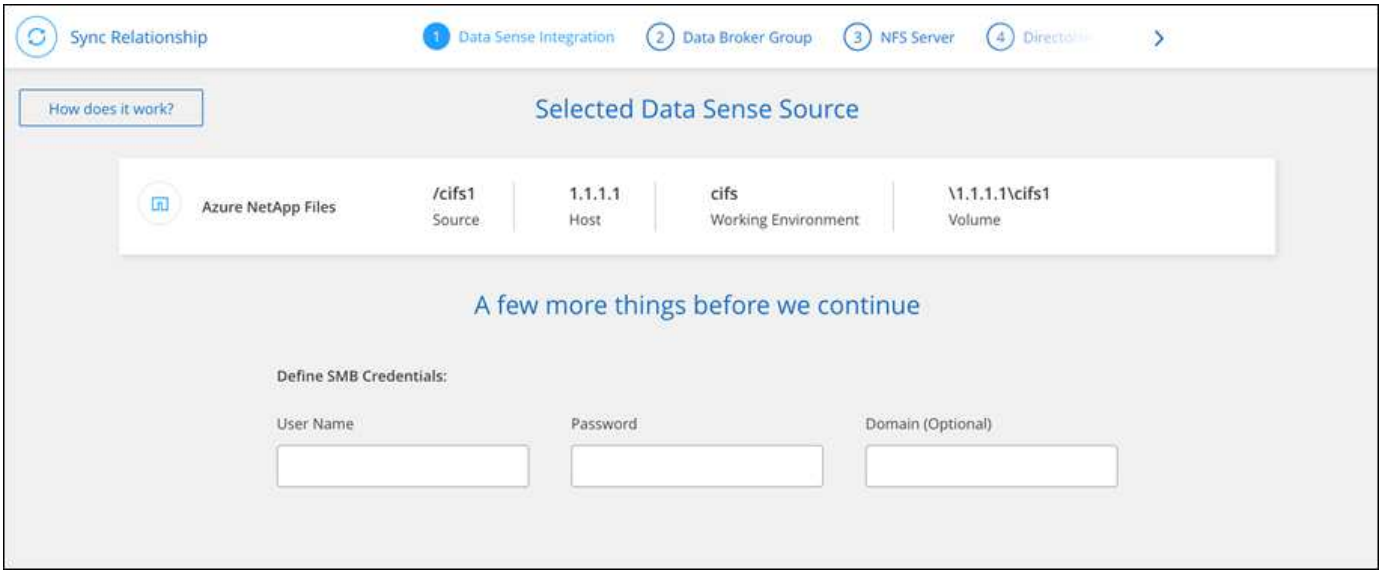
Risultato

BlueXP copy and Sync avvia la sincronizzazione dei dati tra l'origine e la destinazione.

Creare relazioni di sincronizzazione dalla classificazione BlueXP

BlueXP copy and Sync è integrato con la classificazione BlueXP. Dall'interno della classificazione BlueXP, è possibile selezionare i file di origine che si desidera sincronizzare in una posizione di destinazione utilizzando la copia e la sincronizzazione BlueXP.

Dopo aver avviato una sincronizzazione dei dati dalla classificazione BlueXP, tutte le informazioni di origine sono contenute in un singolo passaggio e richiedono solo l'immissione di alcuni dettagli chiave. Quindi, scegliere la posizione di destinazione per la nuova relazione di sincronizzazione.



"Scopri come avviare una relazione di sincronizzazione dalla classificazione BlueXP".

Copia degli ACL dalle condivisioni SMB

BlueXP copy and Sync può copiare gli elenchi di controllo degli accessi (ACL) tra le condivisioni SMB e tra una condivisione SMB e lo storage a oggetti (ad eccezione di ONTAP S3). Se necessario, puoi anche mantenere manualmente gli ACL tra le condivisioni SMB utilizzando robocopy.

Scelte

- Impostare la copia e la sincronizzazione di BlueXP per copiare automaticamente gli ACL
- Copiare manualmente gli ACL tra le condivisioni SMB

Impostare la copia BlueXP e la sincronizzazione per copiare gli ACL

Copiare gli ACL tra le condivisioni SMB e tra le condivisioni SMB e lo storage a oggetti attivando un'impostazione quando si crea una relazione o dopo la creazione di una relazione.

Prima di iniziare

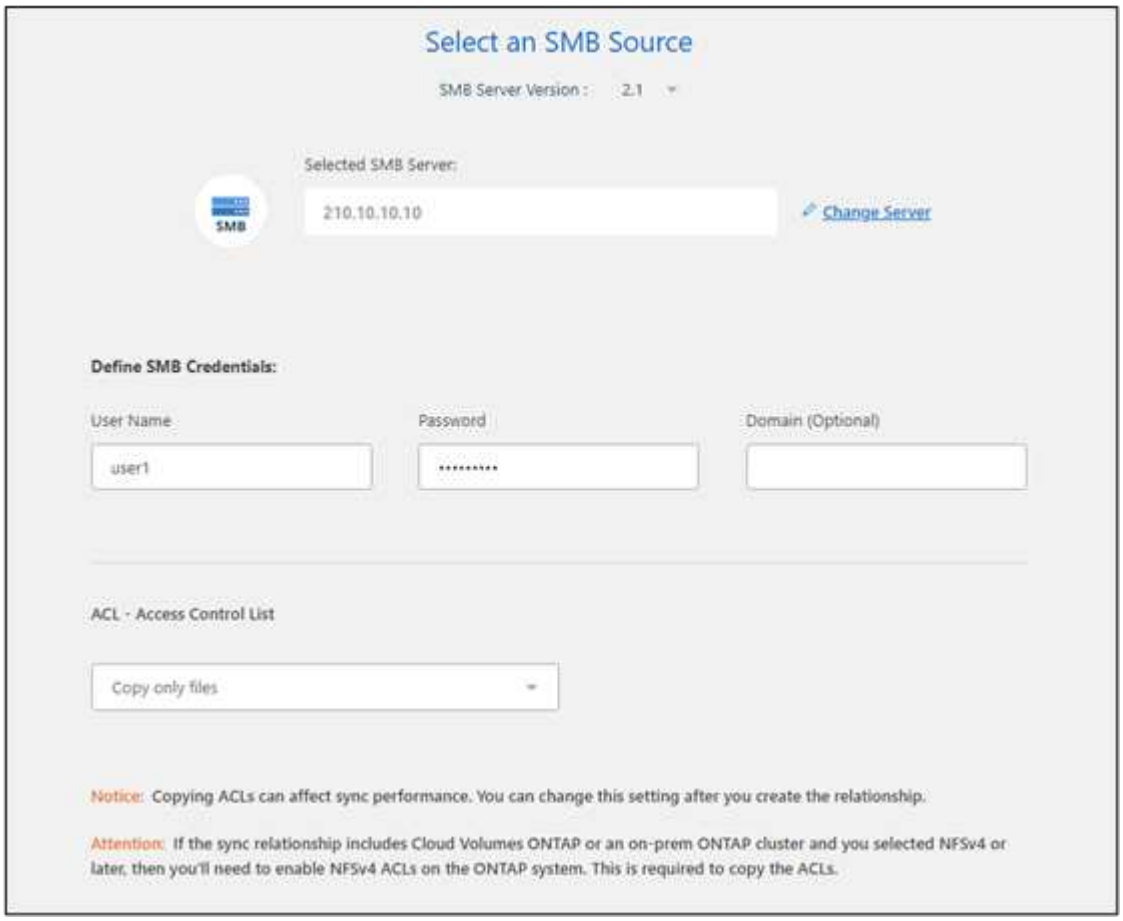
Questa funzionalità funziona con *qualsiasi* tipo di data broker: AWS, Azure, Google Cloud Platform o data broker on-premise. Il data broker on-premise può essere eseguito "qualsiasi sistema operativo supportato".

Passaggi per una nuova relazione

1. Da BlueXP copy and Sync (Copia e sincronizzazione BlueXP), selezionare **Create New Sync** (Crea nuova

sincronizzazione).

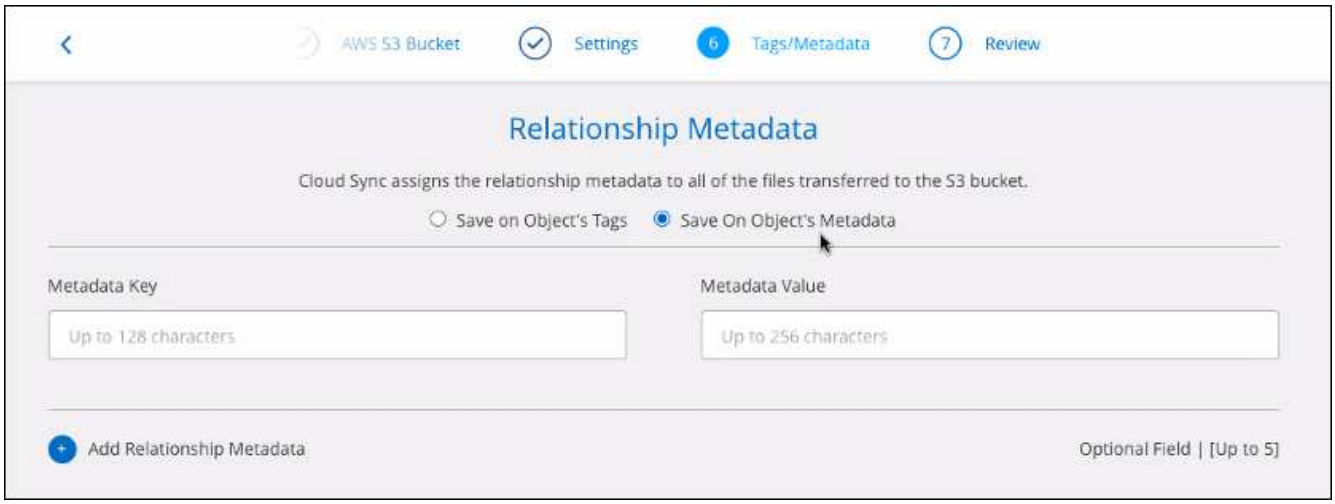
2. Trascinare un server SMB o uno storage a oggetti come origine e un server SMB o storage a oggetti come destinazione, quindi selezionare **continua**.
3. Nella pagina **SMB Server**:
   a. Immettere un nuovo server SMB o selezionare un server esistente e selezionare **continua**.
   b. Immettere le credenziali per il server SMB.
   c. Scegliere **Copy only Files** (Copia solo file), **Copy Only ACL** (Copia solo ACL) o **Copy Files and ACL** (Copia file e ACL) e selezionare **Continue** (continua).



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

   Quando si copiano gli ACL da SMB allo storage a 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 della fase in cui è possibile effettuare questa scelta.



Passaggi per una relazione esistente

1. Passare il mouse sulla relazione di sincronizzazione e selezionare il menu delle azioni.
2. Selezionare **Impostazioni**.
3. Scegliere **Copy only Files** (Copia solo file), **Copy Only ACL** (Copia solo ACL) o **Copy Files and ACL** (Copia file e ACL) e selezionare **Continue** (continua).
4. Selezionare **Save Settings** (Salva impostazioni).

Risultato

Durante la sincronizzazione dei dati, BlueXP Copy and Sync preserva gli ACL tra origine e destinazione.

Copia manualmente gli ACL tra le condivisioni SMB

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 BlueXP copy and 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>

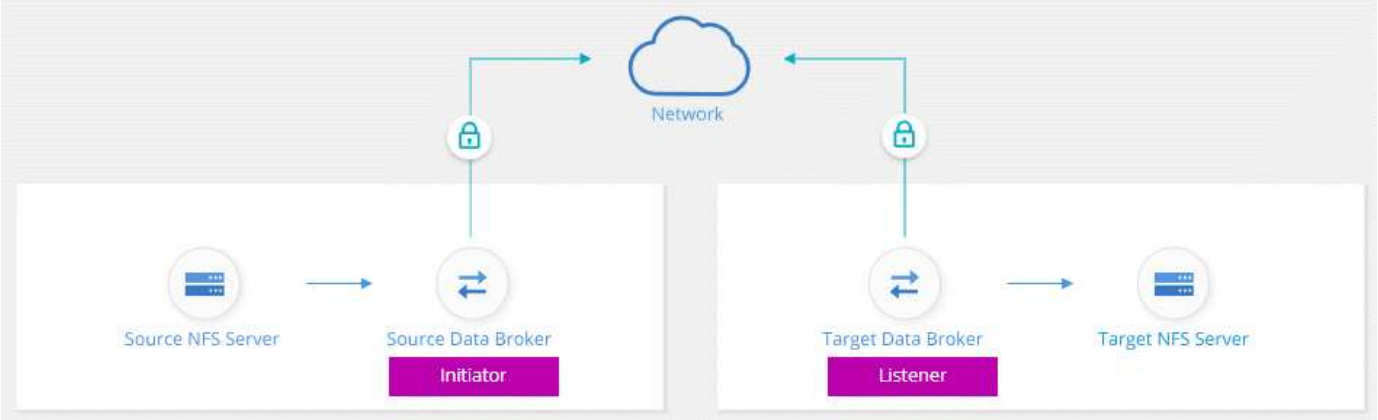
Sincronizzazione dei dati NFS con crittografia data-in-flight

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.

Limitazione del server proxy

Se si crea una relazione di sincronizzazione crittografata, i dati crittografati vengono inviati tramite HTTPS e non possono essere instradati attraverso un server proxy.

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 si desidera utilizzare un gruppo di broker di dati esistente, il gruppo deve disporre di un solo broker di dati. I broker di dati multipli in un gruppo non sono supportati con relazioni di sincronizzazione crittografate.

  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 Google Cloud"
  - "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. Selezionare **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.
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.

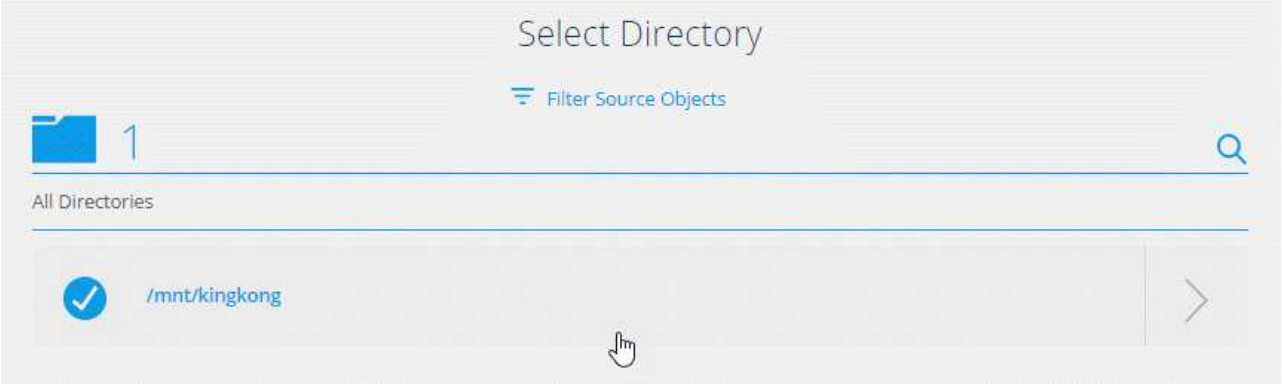
c. **Data Broker**: Seguire le istruzioni per aggiungere un nuovo data broker di origine o selezionare un data broker esistente.

   Tenere presente quanto segue:

   - Se si desidera utilizzare un gruppo di broker di dati esistente, il gruppo deve disporre di un solo broker di dati. I broker di dati multipli in un gruppo non sono supportati con relazioni di sincronizzazione crittografate.
   - Se il broker di dati di origine agisce come listener, deve essere un nuovo broker di dati.
   - Se hai bisogno di un nuovo data broker, BlueXP Copy and Sync ti 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.

   Selezionare **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.

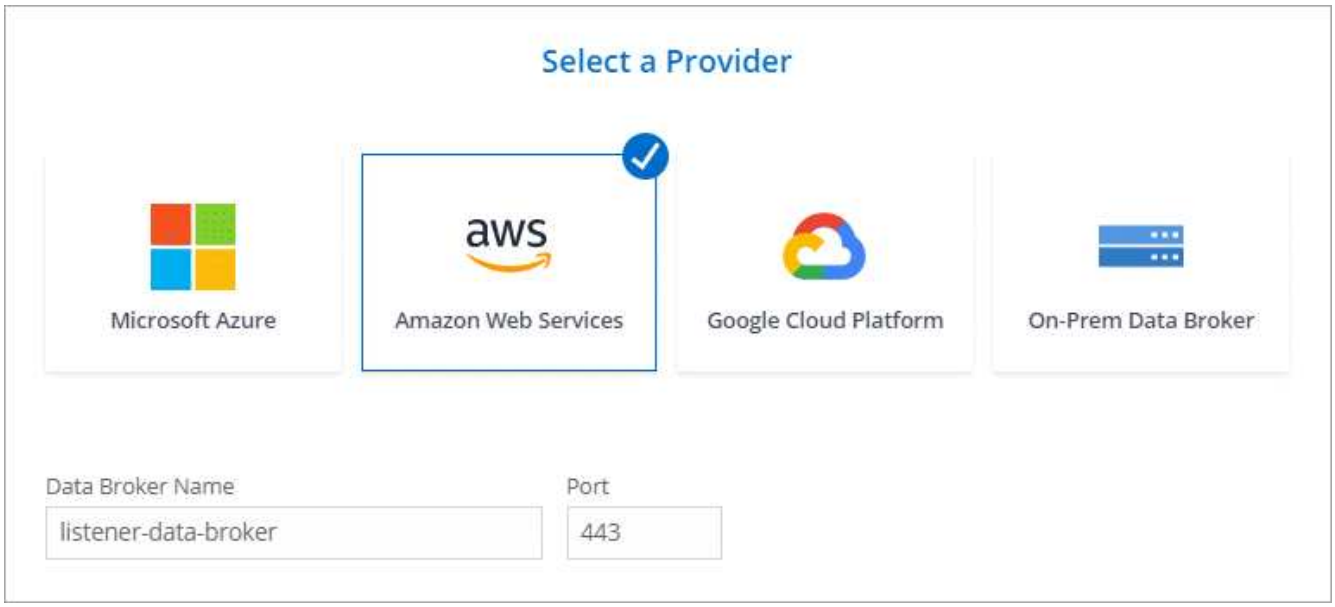


e. **Server NFS di destinazione/Azure NetApp Files di destinazione**: Scegliere la versione di NFS, quindi inserire una nuova destinazione NFS o selezionare un server esistente.

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.

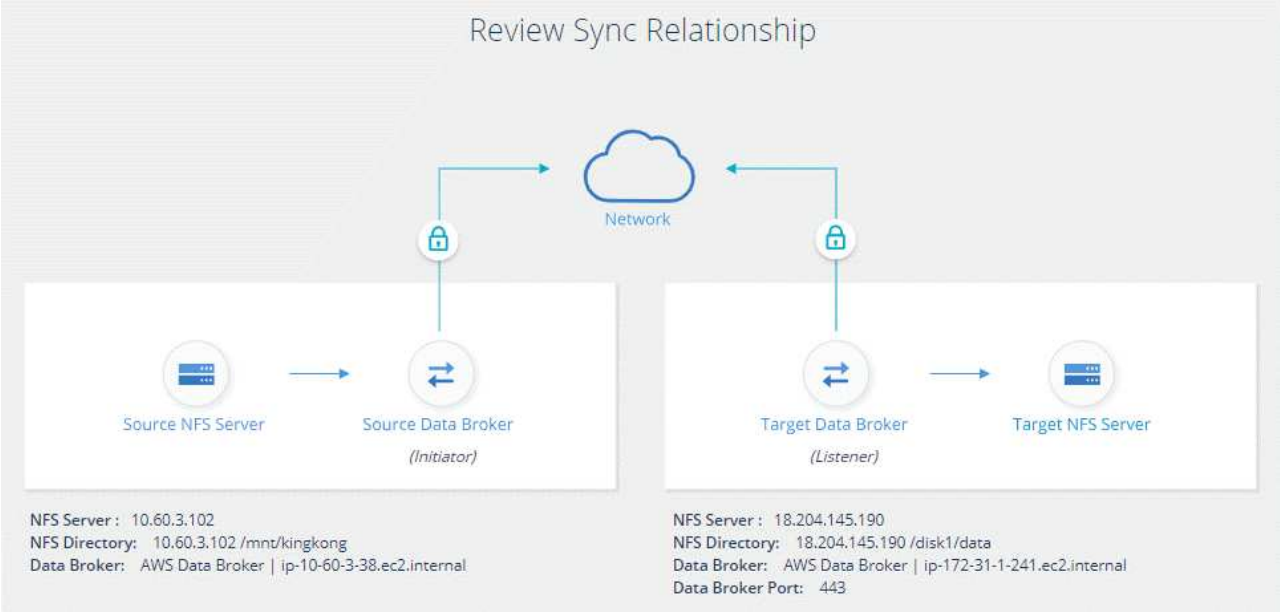
   Ecco un esempio del prompt quando il broker di dati di destinazione funziona come listener. Notare l'opzione per specificare la porta.



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 selezionare **Crea relazione**.



Risultato

BlueXP copy and Sync inizia a creare la nuova relazione di sincronizzazione. Al termine dell'operazione, selezionare **View in Dashboard** (Visualizza nella dashboard) per visualizzare i dettagli sulla nuova relazione.

Impostazione di un gruppo di broker di dati per l'utilizzo di un vault HashiCorp esterno

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 di copia e sincronizzazione BlueXP. Un'alternativa è impostare il gruppo di broker di dati per accedere alle credenziali (o *secrets*) direttamente da un vault HashiCorp esterno.

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

1. **Preparare il vault**

Preparare il vault per fornire le credenziali al gruppo di broker di 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 ogni broker di dati nel gruppo.

3. **Creare una relazione di sincronizzazione utilizzando l'API**

Una volta configurato tutto, è possibile inviare una chiamata API per creare una relazione di sincronizzazione che utilizzi il vault per ottenere i segreti.

Preparazione del vault

È necessario fornire una copia BlueXP e sincronizzarla con l'URL con i segreti nel vault. Preparare il vault impostando questi URL. È necessario impostare gli URL in base alle credenziali per ciascuna origine e destinazione nelle relazioni di sincronizzazione che si intende creare.

L'URL deve essere impostato come segue:

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

Percorso

Il percorso del prefisso per il segreto. Questo può essere un valore qualsiasi per te.

ID richiesta

ID richiesta da generare. Quando si crea la relazione di sincronizzazione, è necessario fornire l'ID in una delle intestazioni della richiesta API POST.

Protocollo endpoint

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

Credi

L'URL deve terminare con *Creds*.

Esempi

Gli esempi seguenti mostrano gli URL per i segreti.

Esempio di URL completo e percorso per le credenziali di origine

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

Come si può 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 di URL completo e 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.

Preparazione del 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 ogni broker di dati nel gruppo.

Fasi

1. SSH a un broker di dati del gruppo.
2. Modificare il file local.json che risiede in /opt/netapp/databroker/config.
3. Impostare enable su **true** e i campi dei parametri di configurazione in *external-integrations.hashicorp* come segue:

   attivato
   - Valori validi: Vero/falso
   - Tipo: Booleano
   - Valore predefinito: False
   - Vero: Il data broker ottiene segreti dal tuo vault HashiCorp esterno
   - Falso: Il data broker memorizza le credenziali nel proprio vault locale

   url
   - Digitare: String
   - Valore: L'URL del vault esterno

   percorso
   - Digitare: String
   - Valore: Inserire il percorso del segreto con le credenziali

   Rifiuta-non autorizzato
   - Determina se si desidera che il data broker rifiuti un vault esterno non autorizzato
   - Tipo: Booleano
   - Predefinito: Falso

   authod
   - Il metodo di autenticazione che il data broker deve utilizzare per accedere alle credenziali dal vault esterno
   - Digitare: String

- Valori validi: "aws-iam" / "role-app" / "gcp-iam"

nome-ruolo

- Digitare: String
- Nome del tuo ruolo (nel caso in cui utilizzi aws-iam o gcp-iam)

Secretid e rootid

- Digitare: String (se si utilizza app-role)

Namespace

- Digitare: String
- Spazio dei nomi (intestazione X-Vault-namespace, se necessario)

4. Ripetere questa procedura per tutti gli altri broker di dati del gruppo.

Esempio di autenticazione con ruolo aws

```
{
        "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"
      }
    }
  }
}
```

Impostazione delle autorizzazioni quando si utilizza l'autenticazione gcp-iam

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

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

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

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

Una volta configurato tutto, è possibile inviare una chiamata API per creare una relazione di sincronizzazione che utilizzi il vault per ottenere i segreti.

Pubblicare la relazione utilizzando la copia BlueXP e l'API REST di sincronizzazione.

```
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 BlueXP, "fare riferimento a questa pagina nella documentazione".
- Per costruire un corpo per la tua relazione post, "Fare riferimento alla chiamata all'API Relarcitazioni 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"
        }
    }
}
```