チュートリアル

Cloud Manager

NetApp
July 12, 2021

目次

チュートリアル

SMB 共有間での ACL のコピー

Cloud Sync では、ソース SMB 共有とターゲット SMB 共有の間でアクセス制御リスト（ ACL ）をコピーできます。必要に応じて、 Robocopy を使用して手動で ACL を保存することができます。

選択肢

- ACL を自動的にコピーするように Cloud Sync を設定します
- ACL を手動でコピーします

SMB サーバ間で ACL をコピーするための Cloud Sync の設定

関係の作成時または関係の作成後に設定を有効にして、 SMB サーバ間の ACL をコピーします。

この機能は、 2020 年 2 月 23 日リリース以降に作成された新しい同期関係で使用できます。この機能をその日付より前に作成された既存の関係で使用する場合は、関係を再作成する必要があります。

必要なもの

- 2020 年 2 月 23 日リリース以降に作成された新しい同期関係または既存の同期関係。
- あらゆる種類のデータブローカーに対応

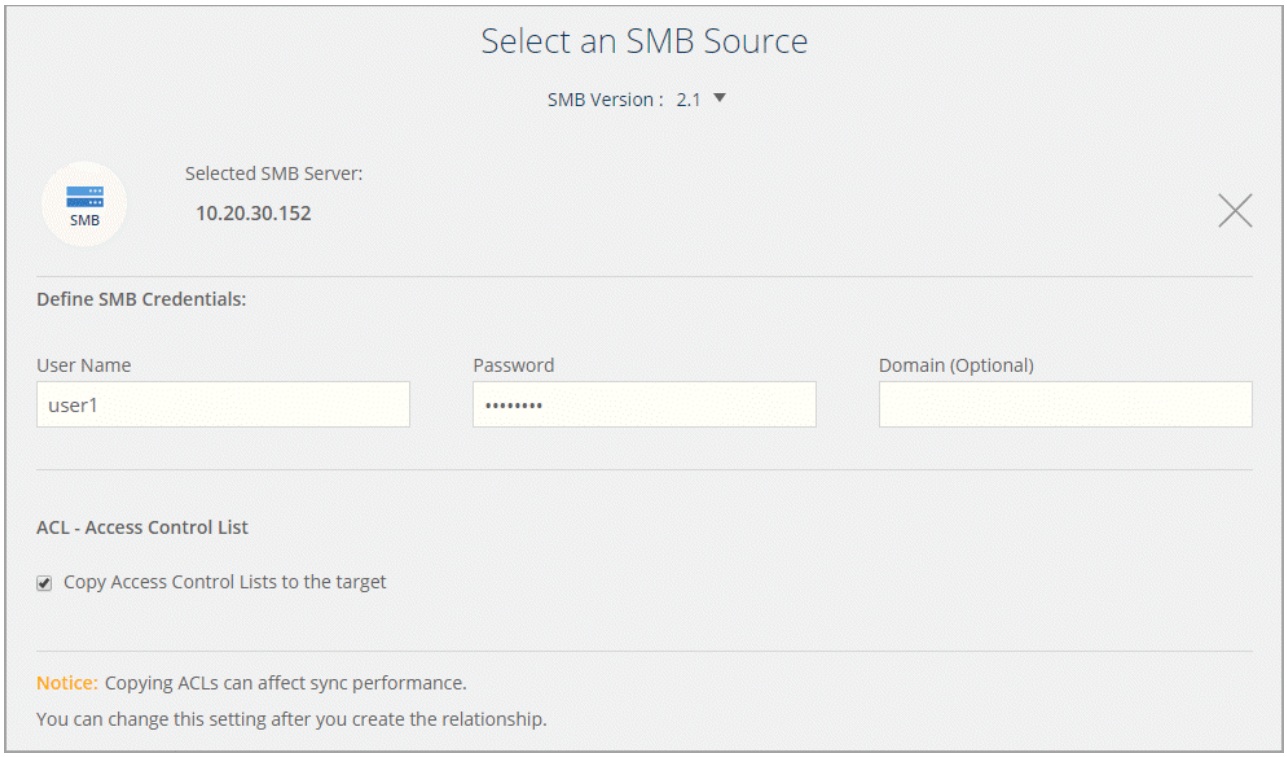
  この機能は、 _any_type のデータブローカー（ AWS 、 Azure 、 Google Cloud Platform 、オンプレミスのデータブローカー）と連携します。オンプレミスのデータブローカーを実行できます "サポートされているオペレーティングシステム"。

- NFS の場合は、 NFS バージョン 4 以降を使用する必要があります。

  ソースとターゲットのバージョンが同じである必要があります。たとえば、ソースでは 4.0 、ターゲットでは 4.0 がサポートされます。ただし、ソースでは 4.0 、ターゲットでは 4.1 はサポートされていません。これは、バージョンが異なるためです。

新しい関係の手順

1. Cloud Sync で、 * 新しい同期を作成 * をクリックします。
2. ソースとターゲットに * SMB サーバー * をドラッグアンドドロップし、 * 続行 * をクリックします。
3. [* SMB サーバー *] ページで、次の操作を行います。
   a. 新しい SMB サーバーを入力するか、既存のサーバーを選択して、 * 続行 * をクリックします。
   b. SMB サーバのクレデンシャルを入力します。
   c. [* アクセス制御リストをターゲットにコピーする] を選択し、 [続行 *] をクリックします。



4. 残りのプロンプトに従って、同期関係を作成します。

既存の関係に対する手順

1. 同期関係の上にカーソルを置いて、 [アクション] メニューをクリックします。
2. [* 設定 *] をクリックします。
3. [* アクセス制御リストをターゲットにコピーする *] を選択します。
4. [設定の保存 *] をクリックします。

データを同期する場合、 Cloud Sync はソースとターゲットの SMB 共有間の ACL を保持します。

ACL の手動コピー

Windows の Robocopy コマンドを使用すると、 SMB 共有間で ACL を手動で保存できます。

手順

1. 両方の SMB 共有へのフルアクセス権を持つ Windows ホストを特定します。
2. いずれかのエンドポイントで認証が必要な場合は、 * net use * コマンドを使用して Windows ホストからエンドポイントに接続します。

   Robocopy を使用する前に、この手順を実行する必要があります。

3. Cloud Sync で、ソースとターゲットの SMB 共有間の新しい関係を作成するか、既存の関係を同期します。
4. データの同期が完了したら、 Windows ホストから次のコマンドを実行して、 ACL と所有権を同期します。

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

UNC　形式を使用して、　source_or_target_　と　*target*　の両方を指定する必要があります。たとえば、\\<server>\<share>\<path> と入力します

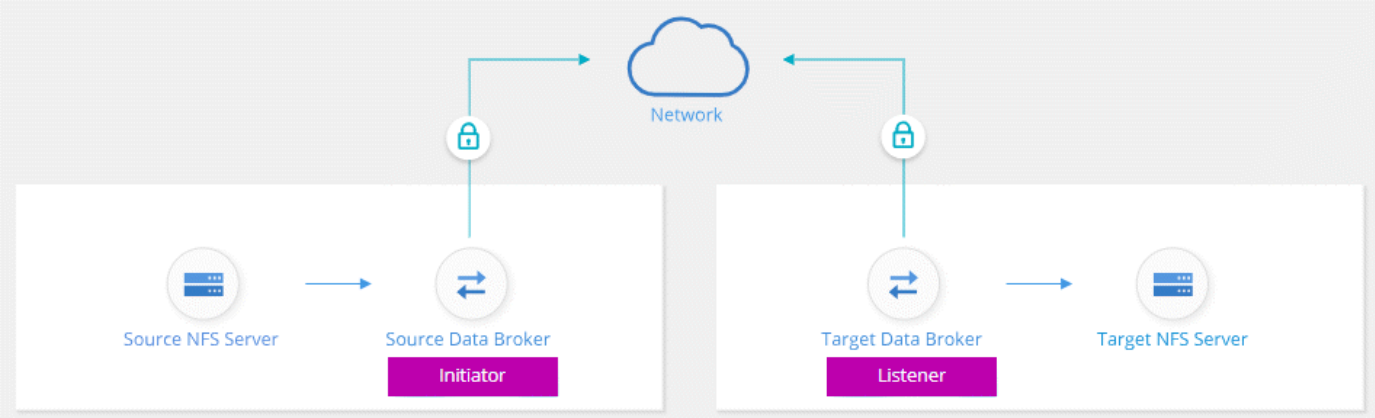
転送中のデータ暗号化を使用した NFS データの同期

厳格なセキュリティポリシーを適用している場合は、転送中データの暗号化を使用して NFS データを同期できます。この機能は、 NFS サーバから別の NFS サーバ、および Azure NetApp Files から Azure NetApp Files へサポートされます。

たとえば、異なるネットワークにある 2 つの NFS サーバ間でデータを同期できます。また、サブネットやリージョン間で Azure NetApp Files 上のデータをセキュアに転送しなければならない場合もあります。

データインフライト暗号化の仕組み

データ転送中の暗号化では、 2 つのデータブローカー間でネットワークを介して送信される NFS データが暗号化されます。次の図は、 2 つの NFS サーバと 2 つのデータブローカーの関係を示しています。



1 つのデータブローカーは、 *initiator* として機能します。データを同期するときは、接続要求をもう 1 つのデータブローカー（つまり *listener_* ）に送信します。そのデータブローカーは、ポート 443 で要求をリスンします。必要に応じて別のポートを使用できますが、そのポートが別のサービスで使用されていないことを確認してください。

たとえば、オンプレミスの NFS サーバからクラウドベースの NFS サーバにデータを同期する場合、接続要求を受信するデータブローカーと送信するデータブローカーを選択できます。

転送中の暗号化の仕組みは次のとおりです。

1. 同期関係を作成すると、イニシエータは他のデータブローカーとの暗号化された接続を開始します。
2. ソースデータブローカーは、 TLS 1.3 を使用してソースのデータを暗号化します。
3. 次に、ネットワーク経由でデータをターゲットデータブローカーに送信します。
4. ターゲットのデータブローカーは、ターゲットに送信する前にデータを復号化します。

5. 最初のコピーの後、変更されたデータは 24 時間ごとに同期されます。同期するデータがある場合は、イニシエータが他のデータブローカーとの暗号化された接続を開いてプロセスが開始されます。

   データをより頻繁に同期する場合は、 "スケジュールは関係の作成後に変更することができます"。

サポートされている **NFS** のバージョン

- NFS サーバでは、データ転送時の暗号化が NFS バージョン 3 、 4.0 、 4.1 、 4.2 でサポートされています。
- Azure NetApp Files では、 NFS バージョン 3 および 4.1 でデータ転送時の暗号化がサポートされます。

プロキシサーバの制限事項

暗号化された同期関係を作成すると、暗号化されたデータは HTTPS 経由で送信され、プロキシサーバ経由でルーティングすることはできません。

作業を開始するために必要なもの

次のものを用意してください。

- に対応した 2 台の NFS サーバ "移行元と移行先の要件" または、 2 つのサブネットまたはリージョンの Azure NetApp Files 。
- サーバの IP アドレスまたは完全修飾ドメイン名。
- 2 つのデータブローカーのネットワークロケーション。

  既存のデータブローカーを選択できますが、イニシエータとして機能する必要があります。リスナーデータブローカーは、 _NET_DATA ブローカである必要があります。

  データブローカーをまだ導入していない場合は、データブローカーの要件を確認します。厳格なセキュリティポリシーがあるため、ポート 443 およびからの発信トラフィックを含むネットワーク要件を確認してください "インターネットエンドポイント" データブローカーの連絡先。

  - "AWS のインストールを確認します"
  - "Azure のインストールを確認します"
  - "GCP のインストールを確認します"
  - "Linux ホストのインストールを確認します"

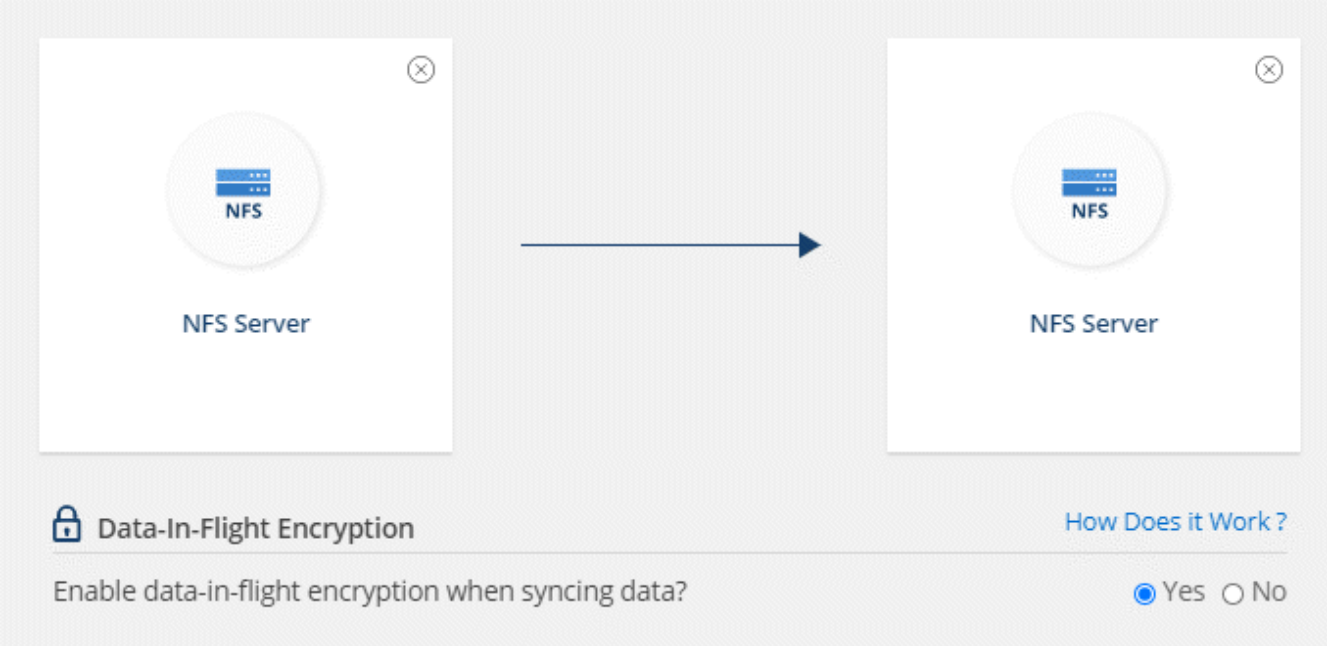
転送中のデータ暗号化を使用した **NFS** データの同期

2 つの NFS サーバ間または Azure NetApp Files 間で新しい同期関係を作成し、転送中の暗号化オプションを有効にして、画面の指示に従います。

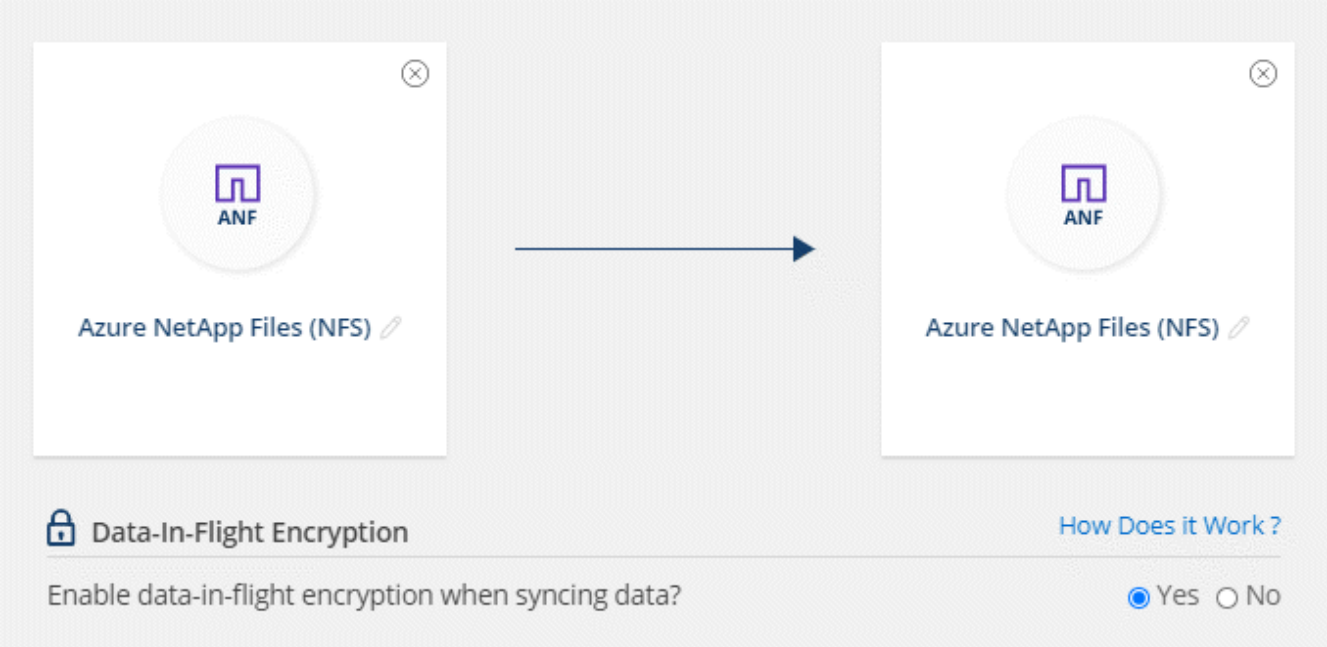
手順

1. [新しい同期の作成 *] をクリックします。
2. NFS サーバ * をソースとターゲットの場所にドラッグアンドドロップするか、 * Azure NetApp Files * をソースとターゲットの場所にドラッグアンドドロップして、 * はい * を選択して転送中のデータ暗号化を有効にします。

次の図は、 2 つの NFS サーバ間でデータを同期する際に選択する内容を示しています。



次の図は、 Azure NetApp Files 間でデータを同期する際に選択する内容を示しています。



3. プロンプトに従って関係を作成します。

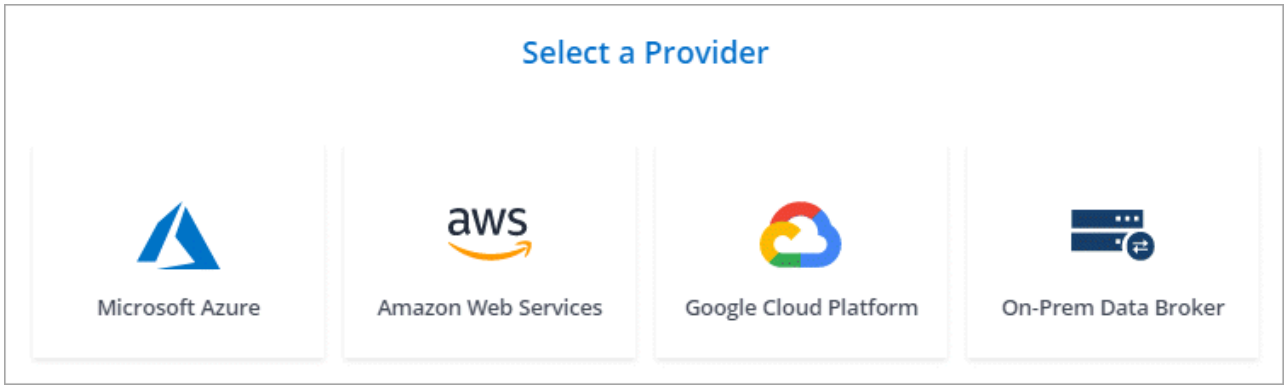
   a. * NFS サーバ * / * Azure NetApp Files * ： NFS のバージョンを選択し、新しい NFS ソースを指定するか、既存のサーバを選択します。

   b. * データブローカー機能の定義 *: ポート上での接続要求に対して ' どのデータ・ブローカ・リスン _ がどのデータ・ブローカ・リスン _ を実行するか ' およびどのデータ・ブローカが接続を開始するかを定義しますネットワーキング要件に基づいて選択してください。

   c. * データブローカー * ：新しいソースデータブローカーを追加するか、既存のデータブローカーを選択するよう求められます。

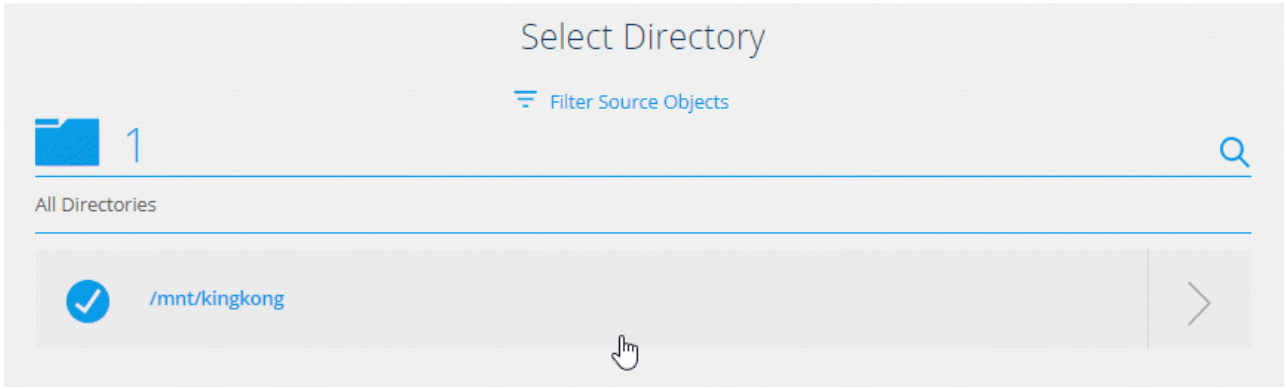
ソースデータブローカーがリスナーとして機能する場合は、新しいデータブローカーである必要があります。

新しいデータブローカーが必要な場合は、インストール手順が表示されます。クラウドにデータブローカーを導入したり、独自の Linux ホスト用のインストールスクリプトをダウンロードしたりできます。



d. * ディレクトリ *: すべてのディレクトリを選択するか、ドリルダウンしてサブディレクトリを選択して、同期するディレクトリを選択します。

「 * ソースオブジェクトのフィルター * 」をクリックして、ソースファイルとフォルダーの同期方法とターゲットの場所での維持方法を定義する設定を変更します。



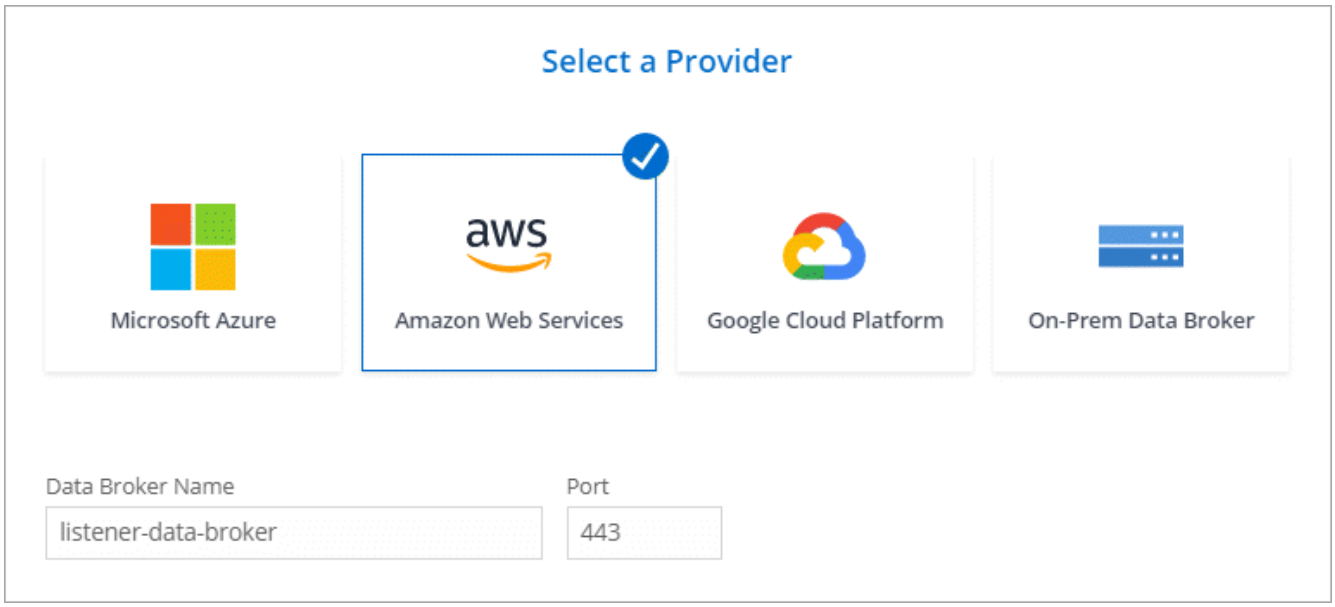
オプションを選択するオプションを示すスクリーンショット。 "]

e. * ターゲット NFS サーバー */ * ターゲット Azure NetApp Files * ： NFS バージョンを選択し、新しい NFS ターゲットを入力するか、既存のサーバーを選択します。

f. * ターゲットデータブローカー * ：新しいソースデータブローカーを追加するか、既存のデータブローカーを選択するよう求められます。

ターゲットデータブローカーがリスナーとして機能する場合は、新しいデータブローカーである必要があります。

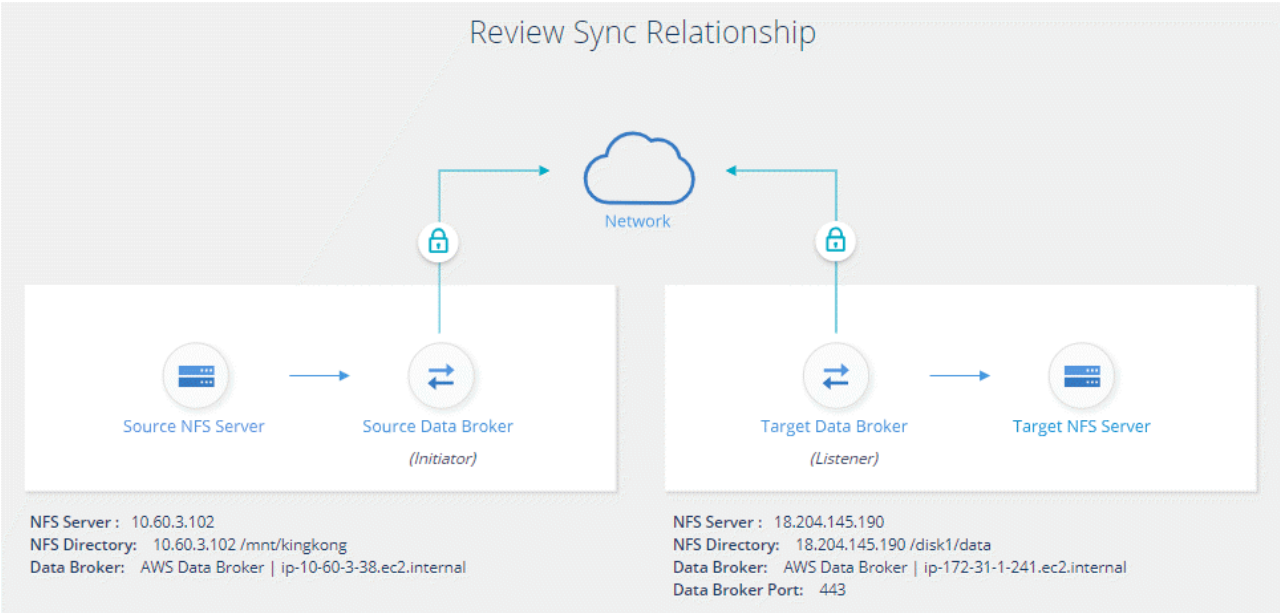
ターゲットのデータブローカーがリスナーとして機能する場合のプロンプトの例を次に示します。ポートを指定するオプションに注目してください。



a. * ターゲットディレクトリ * ：トップレベルのディレクトリを選択するか、ドリルダウンして既存のサブディレクトリを選択するか、エクスポート内に新しいフォルダを作成します。

b. * 設定 * ：ソースファイルとフォルダをターゲットの場所で同期および維持する方法を定義します。

c. * 確認 * ：同期関係の詳細を確認し、 * 関係の作成 * をクリックします。



Cloud Sync が新しい同期関係の作成を開始します。完了したら、 [ダッシュボードで表示] をクリックして、新しい関係の詳細を表示します。

外部の橋本 **Corp** を使用するようにデータブローカーを設定する バックアップ

Amazon S3 、 Azure 、または Google Cloud のクレデンシャルが必要な同期関係を作成する場合は、 Cloud Sync のユーザインターフェイスまたは API を使用してそれらのクレデンシャルを指定する必要があります。別の方法として、データブローカーをセットアップして、外部の橋本社ボールトから直接クレデンシャル（ま

たは *secrets*） にアクセスする方法もあります。

この機能は、 Cloud Sync API を使用し、 Amazon S3 、 Azure 、または Google Cloud のクレデンシャルを必要とする同期関係をサポートします。

ボルトを準備します

URL　を設定して、データブローカーにクレデンシャルを提供するようにヴォールトを準備します。ボールトのシークレットの URL は、 *creds_* で終わる必要があります。

データブローカーを準備

データブローカーのローカル構成ファイルを変更し、外部ボルトからクレデンシャルを取得するようにデータブローカーを準備します。

API を使用して同期関係を作成してください

すべての設定が完了したら、　API　呼び出しを送信して、ヴォールトを使用してシークレットを取得する同期関係を作成できます。

ヴォールトを準備しています

ボールトのシークレットに Cloud Sync の URL を指定する必要があります。URL を設定してボールトを準備します。作成する同期関係の各ソースとターゲットのクレデンシャルへの URL を設定する必要があります。

URL は次のように設定する必要があります。

「 /<path>/<RequestID>/<endpoint-protocol> creds 」を指定します

パス
: シークレットへのプレフィックスパス。この値は、お客様に固有の任意の値にすることができます。

リクエスト **ID**
: 生成する必要があるリクエスト ID 。同期関係を作成するときは、 API POST 要求のいずれかのヘッダーに ID を指定する必要があります。

エンドポイントプロトコル
: 定義されている次のいずれかのプロトコル "v2 以降の関係に関するドキュメント"： S3 、 Azure 、 GCP （それぞれ大文字で入力する必要があります）。

Creds （作成）
: URL の末尾は *creds*. にする必要があります。

例

次の例は、シークレットへの URL を示しています。

ソースクレデンシャルの完全な **URL** とパスの例
: この例のように、プレフィックスパスは */my-path/all-secrets/* で、要求 ID は _hb312vdasr2_で 、ソースエンドポイントは S3 です。

ターゲットクレデンシャルの完全な **URL** とパスの例

プレフィックスパスは */my-path/all-secrets/* 、要求 ID は *n32hcbnejk2*、 ターゲットエンドポイントは Azure です。

データブローカーの準備

データブローカーのローカル構成ファイルを変更し、外部ボルトからクレデンシャルを取得するようにデータブローカーを準備します。

手順

1. SSH をデータブローカーに接続
2. /opt/netapp/databroker/config にある local.json ファイルを編集します。
3. enable を * true * に設定し、 _external-m積分 .hashicorp_as の下に config パラメータフィールドを設定します。

有効

- 有効な値は、 true または false です
- type ：ブール値
- デフォルト値： false
- true ：データブローカーは、社内の外部の橋本社から機密情報を入手します
- false ：データブローカーのクレデンシャルがローカルボールトに格納されます

URL

- 文字列を入力します
- 値：外部ボルトの URL

パス

- 文字列を入力します
- 値：クレデンシャルを使用してシークレットへのプレフィックスパスを指定します

拒否 **-** 承認されていません

- データブローカーで権限のないことを拒否するかどうかを指定します 外部ボールト
- type ：ブール値
- デフォルト： false

auth-method を指定します

- データブローカーが外部ボルトのクレデンシャルにアクセスする際に使用する認証方式
- 文字列を入力します
- 有効な値は「 AWS- IAM 」 / 「 role-app 」 / 「 GCP-IAM 」です。

ロール名

- 文字列を入力します
- ロール名（ AWS- IAM または GCP-IAM を使用している場合）

Secretd&rootid

- タイプ： string （ app-role を使用する場合）

ネームスペース

- 文字列を入力します
- ネームスペース（必要に応じて X-Vault - 名前空間ヘッダー）

AWS ロール認証の例

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

GCP - IAM 認証の例

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

GCP - IAM 認証を使用する場合に権限を設定します

_GCP-AM_authentication メソッドを使用している場合、データブローカーには次の GCP 権限が必要です。

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

"データブローカーの GCP 権限要件の詳細については、こちらをご覧ください"。

ヴォールトのシークレットを使用して、新しい同期関係を作成します

すべての設定が完了したら、 API 呼び出しを送信して、ヴォールトを使用してシークレットを取得する同期関係を作成できます。

Cloud Sync REST API を使用して関係をポストします。

```
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
```

- ユーザトークンと Cloud Central アカウント ID を取得するには、 "のドキュメントのこのページを参照してください"。
- 投稿関係の本文を作成するには、 "relationships-v2 API 呼び出しを参照してください"。

例

POST 要求の例：

```
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"
        }
    }
}
```