ソースとターゲットの間でデータを同期します

BlueXP copy and sync

NetApp
April 08, 2024

目次

ソースとターゲットの間でデータを同期します

同期関係を作成する

同期関係を作成すると、BlueXPのコピーおよび同期サービスによってソースからターゲットにファイルがコピーされます。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。

一部の種類の同期関係を作成する前に、まずBlueXPで作業環境を作成する必要があります。

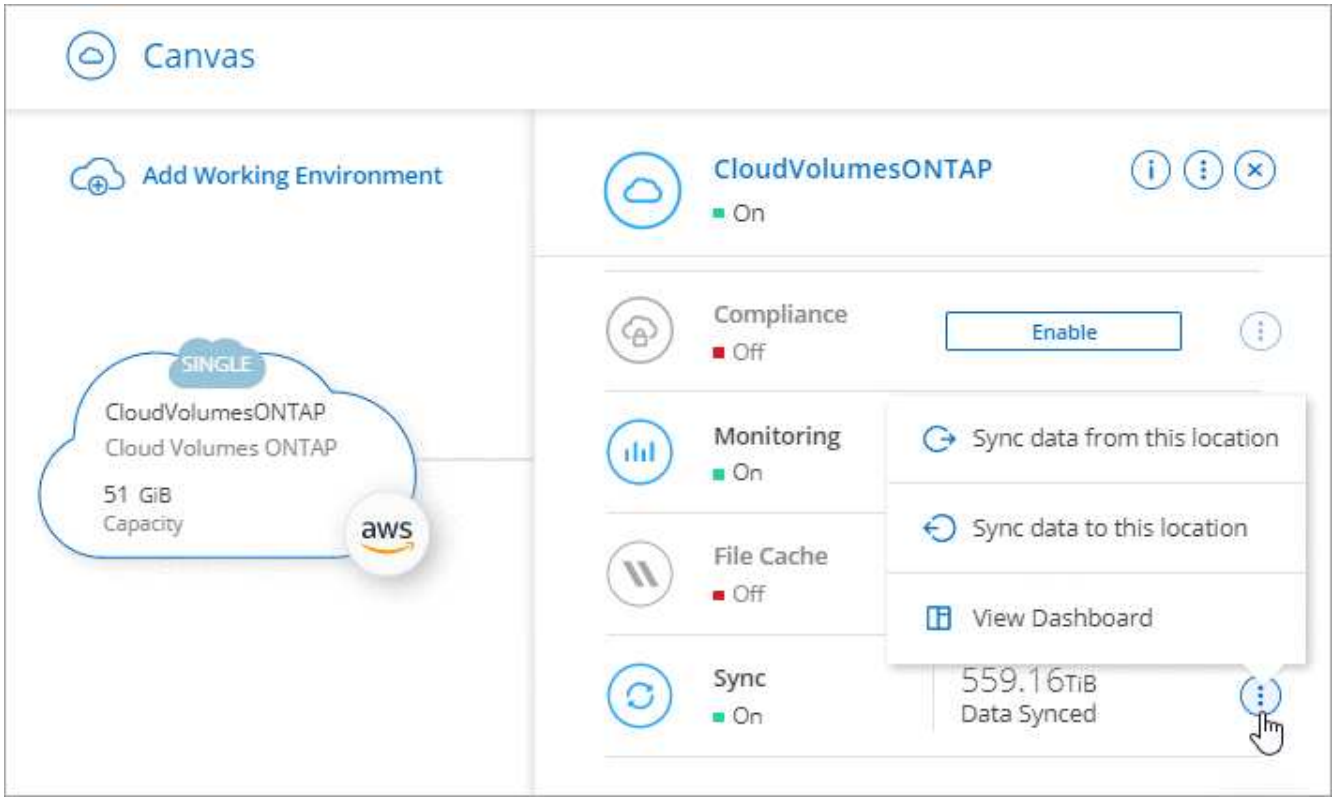
特定のタイプの作業環境の同期関係を作成します

次のいずれかの同期関係を作成する場合は、最初に作業環境を作成または検出する必要があります。

- ONTAP 対応の Amazon FSX
- Azure NetApp Files の特長
- Cloud Volumes ONTAP
- オンプレミスの ONTAP クラスタ

手順

1. 作業環境を作成または検出します。
    - "ONTAP 作業環境用の Amazon FSX を作成します"
    - "Azure NetApp Files をセットアップおよび検出しています"
    - "AWS での Cloud Volumes ONTAP の起動"
    - "Azure で Cloud Volumes ONTAP を起動します"
    - "Google Cloud で Cloud Volumes ONTAP を起動しています"
    - "既存の Cloud Volumes ONTAP システムの追加"
    - "ONTAP クラスタの検出"
2. [キャンバス]*を選択します。
3. 上記のいずれかのタイプに一致する作業環境を選択してください。
4. [同期] の横のアクションメニューを選択します。



5. この場所から * データを同期 * または * この場所へのデータの同期 * を選択し、プロンプトに従って同期関係を設定します。

他のタイプの同期関係を作成します

ONTAP 、 Azure NetApp Files 、 Cloud Volumes ONTAP 、オンプレミスの ONTAP クラスタで、 Amazon FSX 以外のサポートされているストレージタイプとの間でデータを同期するには、次の手順を実行します。以下の手順は、 NFS サーバから S3 バケットへの同期関係を設定する方法の例を示しています。

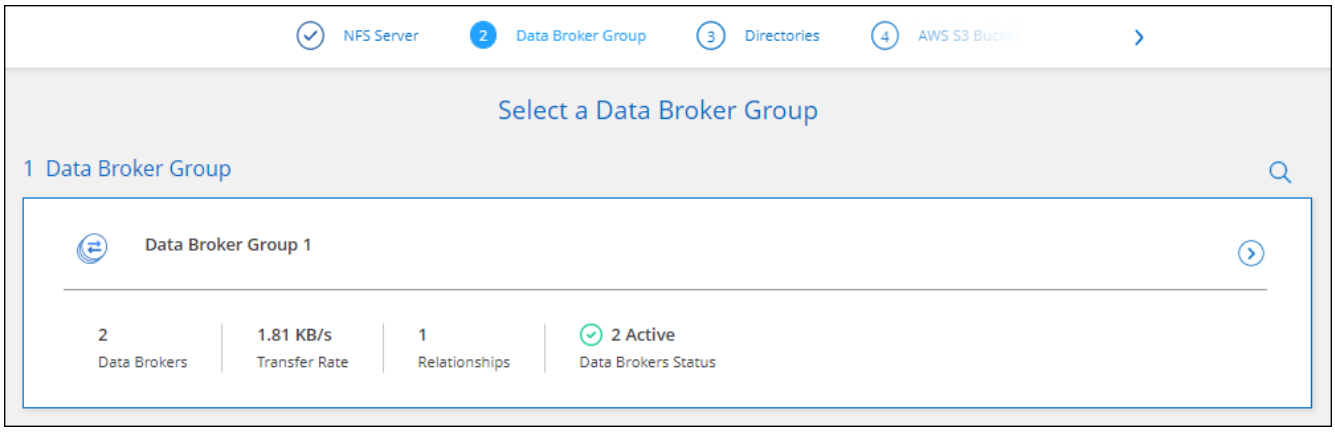
1. BlueXPで、* Sync *を選択します。
2. [同期関係の定義 *] ページで、ソースとターゲットを選択します。

   次の手順では、 NFS サーバから S3 バケットへの同期関係を作成する方法の例を示します。

3. NFS Server * ページで、 AWS と同期する NFS サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
4. [**Data Broker Group**] ページで、プロンプトに従って AWS 、 Azure 、または Google Cloud Platform にデータブローカー仮想マシンを作成するか、データブローカーソフトウェアを既存の Linux ホストにインストールします。

   詳細については、次のページを参照してください。

   - "AWS にデータブローカーを作成"
   - "Azure でデータブローカーを作成"
   - "Google Cloud でデータブローカーを作成"
   - "Linux ホストへのデータブローカーのインストール"
5. データブローカーをインストールしたら、*[続行]*を選択します。

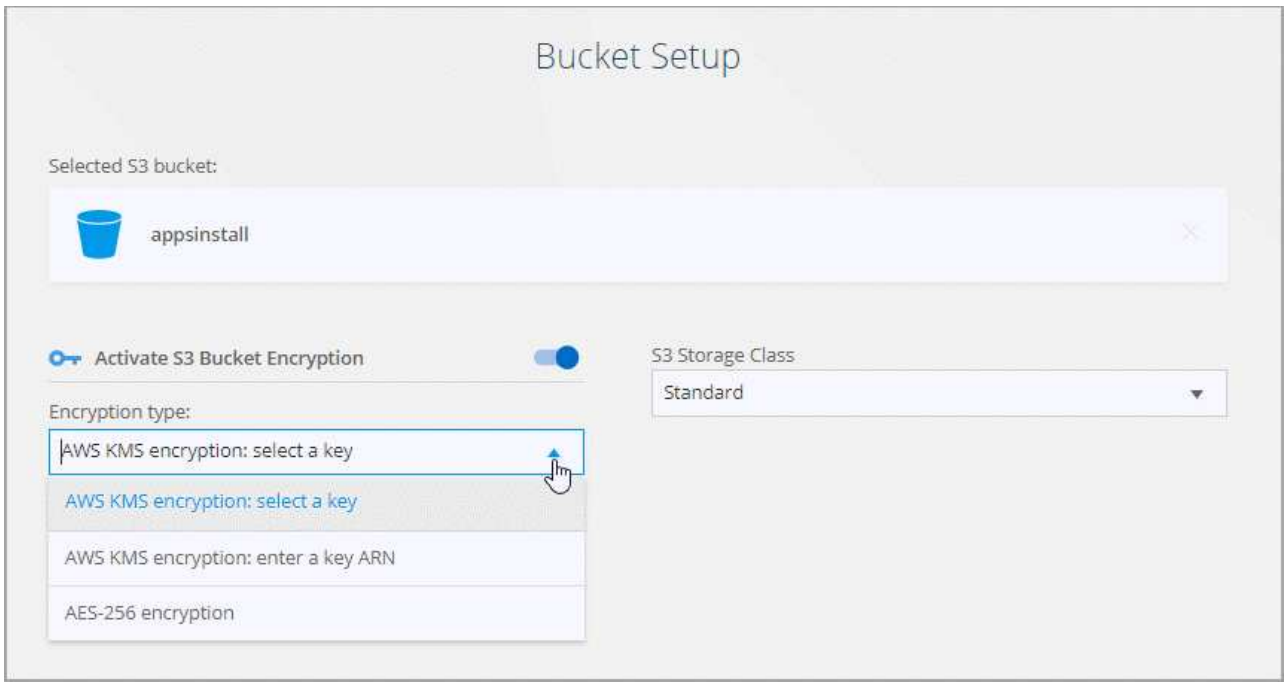


6. [**Directories**] ページで、最上位のディレクトリまたはサブディレクトリを選択します。

BlueXPのコピーと同期でエクスポートを取得できない場合は、*[エクスポートを手動で追加]*を選択し、NFSエクスポートの名前を入力します。

> NFS サーバ上の複数のディレクトリを同期する場合は、同期関係を作成してから同期関係を作成する必要があります。

7. 「 * AWS S3 Bucket * 」ページで、バケットを選択します。
   - ドリルダウンして、バケット内の既存のフォルダを選択するか、バケット内に作成した新しいフォルダを選択します。
   - [リストに追加]*を選択して、AWSアカウントに関連付けられていないS3バケットを選択します。 "S3バケットには特定の権限を適用する必要があります。"。
8. [* Bucket Setup*] ページで、バケットを設定します。
   - S3 バケットの暗号化を有効にするかどうかを選択し、 AWS KMS キーの ARN を入力するか、 AES-256 暗号化を選択します。
   - S3 ストレージクラスを選択します。 "サポートされているストレージクラスを表示します。"。



9. * ページで、ソースファイルとフォルダーを同期してターゲットの場所に保持する方法を定義します。

スケジュール

以降の同期に対して繰り返し実行するスケジュールを選択するか、同期スケジュールをオフにします。データを 1 分ごとに同期するように関係をスケジュールできます。

同期タイムアウト

指定した時間、時間、または日数内に同期が完了していない場合に、BlueXPのコピーと同期をキャンセルするかどうかを定義します。

通知

BlueXPのコピーと同期の通知をBlueXPの通知センターで受け取るかどうかを選択できます。データの同期が成功した場合、データの同期が失敗した場合、データの同期がキャンセルされた場合の通知を有効にできます。

再試行

BlueXPのコピーと同期がファイルの同期をスキップするまでに再試行する回数を定義します。

継続的同期

初回のデータ同期後、BlueXPのコピーと同期はソースのS3バケットまたはGoogle Cloud Storageバケットに対する変更をリスンし、ターゲットへの変更が発生したときに継続的に同期します。ソースを定期的に再スキャンする必要はありません。

この設定は、同期関係を作成する場合、およびS3バケットまたはGoogle Cloud StorageからAzure BLOBストレージ、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、S3のデータを同期する場合にのみ使用できます。 Azure Blob StorageからAzure Blob Storage、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、StorageGRID へのStorageGRID または。

この設定を有効にすると、他の機能に次のように影響します。

- 同期スケジュールが無効になっています。
- 次の設定がデフォルト値に戻ります。同期タイムアウト、最近変更されたファイル、更新日。
- S3がソースの場合、サイズでのフィルタはコピーイベントに対してのみアクティブになります（削除イベントではアクティブになりません）。
- 関係を作成したあとは、関係を高速化または削除する必要があります。同期の中止、設定の変更、レポートの表示はできません。

  外部バケットとの間で継続的な同期関係を作成することができます。これを行うには、次の手順を実行します。

  i. 外部バケットのプロジェクトのGoogle Cloudコンソールに移動します。
  ii. [クラウドストレージ]>[設定]>[クラウドストレージサービスアカウント]*に移動します。
  iii. local.jsonファイルを更新します。

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

iv. データブローカーを再起動します。

   A. sudo PM2 STOP ALL

   B. sudo PM2 start all

v. 関連する外部バケットとの継続的な同期関係を作成します。

> ⓘ 外部バケットとの継続的な同期関係の作成に使用したデータブローカーでは、プロジェクト内のバケットとの間に別の継続的同期関係を作成することはできません。

で比較してください

ファイルやディレクトリが変更されたかどうか、再同期が必要かどうかを判断する際に、BlueXPのコピーと同期を比較するかどうかを選択します。

これらの属性のチェックを外しても、BlueXPのコピーと同期ではパス、ファイルサイズ、ファイル名がチェックされてソースとターゲットが比較されます。変更がある場合は、それらのファイルとディレクトリが同期されます。

BlueXPのコピーと同期を有効または無効にして、次の属性を比較することができます。

- **mtime**: ファイルの最終変更時刻。この属性はディレクトリに対しては無効です。
- **uid** 、 **gid** * 、および * **mode** ： Linux の権限フラグ。

オブジェクトのコピー

オブジェクトストレージのメタデータとタグをコピーする場合は、このオプションを有効にします。ユーザがソースのメタデータを変更した場合、BlueXPのコピーと同期は次回の同期でこのオブジェクトをコピーしますが、ユーザが（データ自体ではなく）ソースのタグを変更した場合、BlueXPのコピーと同期は次回の同期でオブジェクトをコピーしません。

関係の作成後にこのオプションを編集することはできません。

ターゲットにAzure BlobまたはS3互換エンドポイント（S3、StorageGRID 、IBM Cloud Object Storage）を含む同期関係では、タグのコピーがサポートされます。

メタデータのコピーは、次のいずれかのエンドポイント間の「クラウド間」関係でサポートされます。

- AWS S3
- Azure Blob の略

- Google クラウドストレージ
- IBM クラウドオブジェクトストレージ
- StorageGRID

最近変更されたファイル

スケジュールされた同期よりも前に最近変更されたファイルを除外するように選択します。

ソース上のファイルを削除します

BlueXPのコピーと同期でターゲットの場所にファイルがコピーされたあとに、ソースの場所からファイルを削除するように選択します。このオプションには、コピー後にソースファイルが削除されるため、データ損失のリスクも含まれます。

このオプションを有効にする場合は、データブローカーで local.json ファイルのパラメータも変更する必要があります。ファイルを開き、次のように更新します。

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

local.jsonファイルを更新したら、再起動します。 `pm2 restart all`。

ターゲット上のファイルを削除します

ソースからファイルが削除された場合は、ターゲットの場所からファイルを削除することを選択します。デフォルトでは、ターゲットの場所からファイルが削除されることはありません。

ファイルの種類

各同期に含めるファイルタイプ（ファイル、ディレクトリ、シンボリックリンク、ハードリンク）を定義します。

> ハードリンクは、セキュリティ保護されていないNFSからNFSへの関係でのみ使用できます。ユーザーは1つのスキャナプロセスと1つのスキャナ同時実行に制限され、スキャンはルートディレクトリから実行する必要があります。

ファイル拡張子を除外します

同期から除外する正規表現またはファイル拡張子を指定するには、ファイル拡張子を入力して*Enter*キーを押します。たとえば、「 *LOG_OR*.log_ 」と入力すると、 *.log ファイルが除外されます。複数の拡張子に区切り文字は必要ありません。次のビデオでは、簡単なデモを紹介しています。

▶ https://docs.netapp.com/ja-jp/bluexp-copy-sync//media/video_file_extensions.mp4 *(video)*

> 正規表現（正規表現）は、ワイルドカードやglob式とは異なります。この機能*only*は正規表現で動作します。

ディレクトリを除外します

同期から除外する正規表現またはディレクトリの名前またはフルパスを入力して*Enter*キーを押し、最大15個の正規表現またはディレクトリを指定します。デフォルトでは、.copy-Offload、.snapshot、~snapshotディレクトリが除外されます。

> 正規表現（正規表現）は、ワイルドカードやglob式とは異なります。この機能*only*は正規表現で動作します。

ファイルサイズ

サイズに関係なくすべてのファイルを同期するか、特定のサイズ範囲のファイルのみを同期するかを選択します。

変更日

最後に変更した日付、特定の日付以降に変更されたファイル、特定の日付より前、または期間に関係なく、すべてのファイルを選択します。

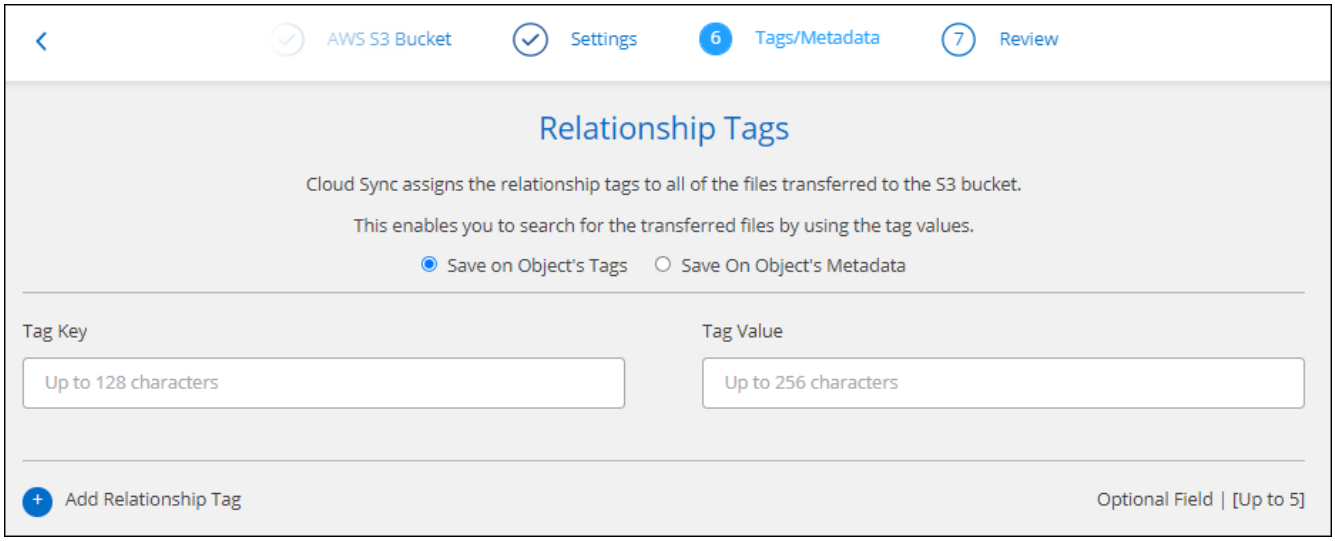
作成日

SMB サーバがソースの場合、この設定を使用すると、指定した日付の前、特定の日付の前、または特定の期間の間に作成されたファイルを同期できます。

[ACL] - アクセスコントロールリスト

関係の作成時または関係の作成後に設定を有効にして、ACLのみ、ファイルのみ、またはACLとファイルをSMBサーバからコピーします。

10. * Tags/Metadata* ページで、 S3 バケットに転送されたすべてのファイルにキーと値のペアをタグとして保存するか、すべてのファイルにメタデータのキーと値のペアを割り当てるかを選択します。



> この機能は、 StorageGRID と IBM Cloud Object Storage にデータを同期する場合にも使用できます。Azure と Google Cloud Storage では、メタデータオプションのみを使用できます。

11. 同期関係の詳細を確認し、*[関係の作成]*を選択します。

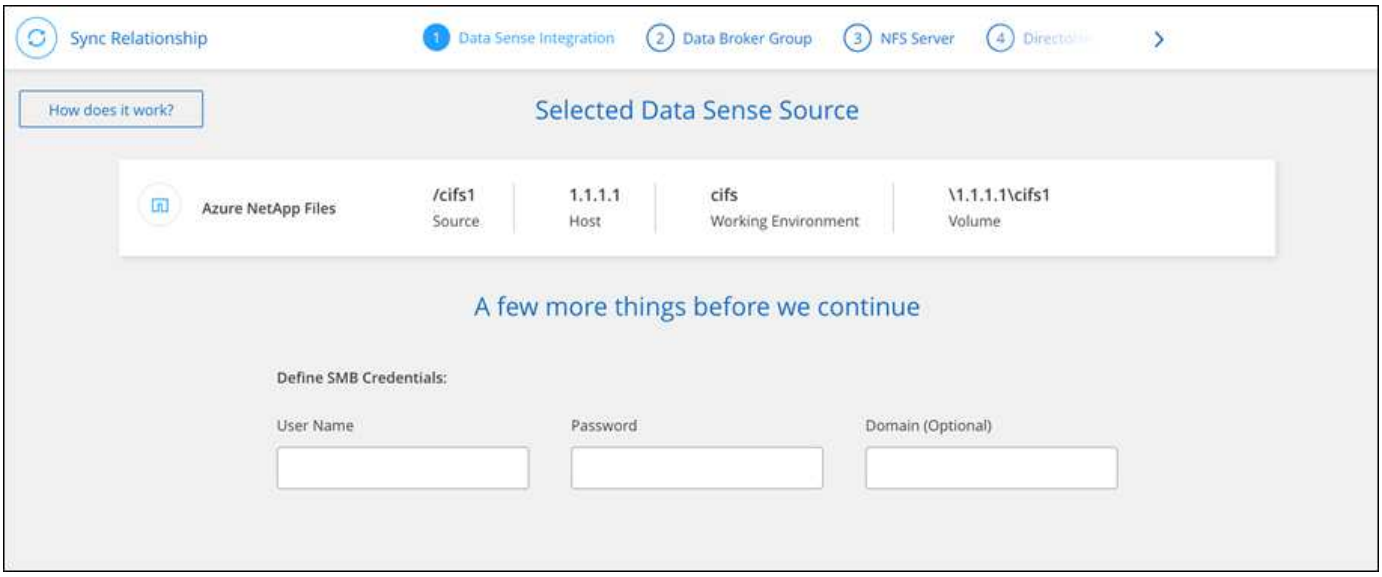
    - 結果 *

BlueXPのコピーと同期で、ソースとターゲット間のデータの同期が開始されます。

BlueXPの分類から同期関係を作成

BlueXPのコピーと同期はBlueXPの分類機能に統合されています。BlueXPの分類から、BlueXPのコピーと同期を使用して、ターゲットの場所に同期するソースファイルを選択できます。

BlueXPの分類からデータの同期を開始すると、すべてのソース情報が1つの手順で格納され、重要な詳細情報をいくつか入力するだけで済みます。その後、新しい同期関係の作成先を選択します。



"BlueXPの分類から同期関係を開始する方法"。

SMB 共有から ACL をコピーする

BlueXPのコピーと同期では、SMB共有間、およびSMB共有とオブジェクトストレージ（ONTAP S3を除く）間でAccess Control List（ACL；アクセス制御リスト）をコピーできます。必要に応じて、 Robocopy を使用して SMB 共有間の ACL を手動で保持することもできます。

選択肢

- ACLを自動的にコピーするようにBlueXPのコピーと同期を設定
- SMB 共有間で ACL を手動でコピーします

BlueXPのコピーと同期を設定してACLをコピー

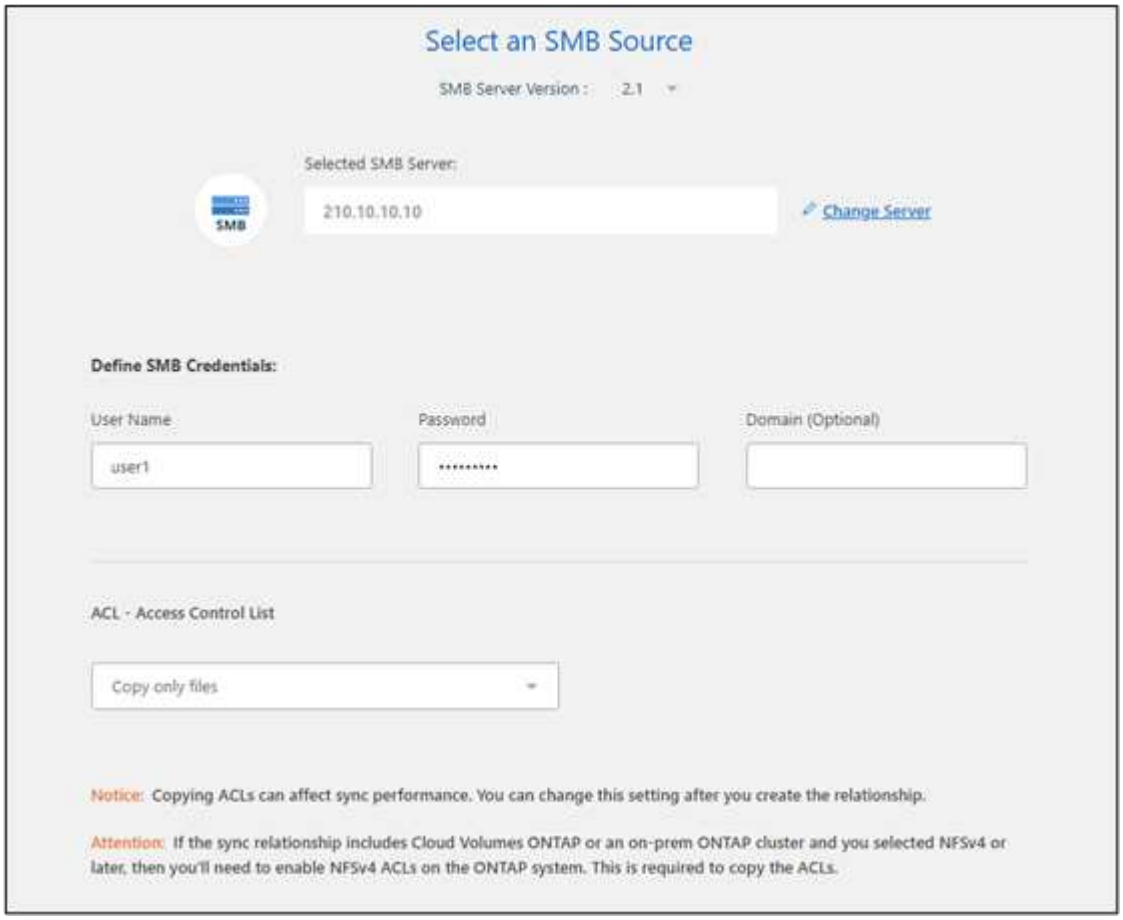
SMB共有間およびSMB共有とオブジェクトストレージ間でACLをコピーするには、関係の作成時または作成後に設定を有効にします。

作業を開始する前に

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"。

新しい関係の手順

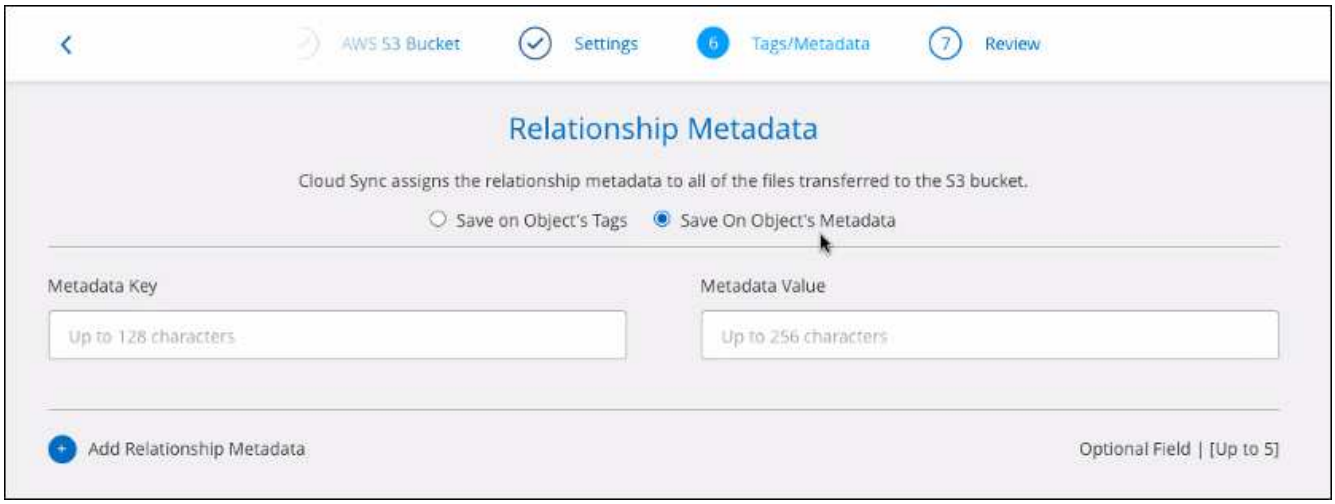
1. BlueXPのコピーと同期で、*[Create New Sync]*を選択します。
2. SMBサーバまたはオブジェクトストレージをソースとして、SMBサーバまたはオブジェクトストレージをターゲットとしてドラッグアンドドロップし、*[続行]*を選択します。
3. [* SMB サーバー *] ページで、次の操作を行います。
   a. 新しいSMBサーバを入力するか、既存のサーバを選択して*[続行]*を選択します。
   b. SMB サーバのクレデンシャルを入力します。
   c. ファイルのみをコピー、* ACLのみをコピー*、または*ファイルとACLをコピー*のいずれかを選択し、*続行*を選択します。



4. 残りのプロンプトに従って、同期関係を作成します。

   ACL を SMB からオブジェクトストレージにコピーする際、ターゲットに応じて、オブジェクトのタグまたはオブジェクトのメタデータに ACL をコピーするかを選択できます。Azure と Google Cloud Storage では、メタデータオプションのみを使用できます。

   次のスクリーンショットは、このオプションを選択できる手順の例を示しています。



既存の関係に対する手順

1. 同期関係にカーソルを合わせ、操作メニューを選択します。
2. [設定]*を選択します。
3. ファイルのみをコピー、* ACLのみをコピー*、または*ファイルとACLをコピー*のいずれかを選択し、*続行*を選択します。
4. [設定の保存]*を選択します。

結果

BlueXPのコピーと同期では、データの同期時にソースとターゲットの間のACLが保持されます。

SMB共有間でACLを手動でコピーします

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. BlueXPのコピーと同期から、ソースとターゲットのSMB共有間に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

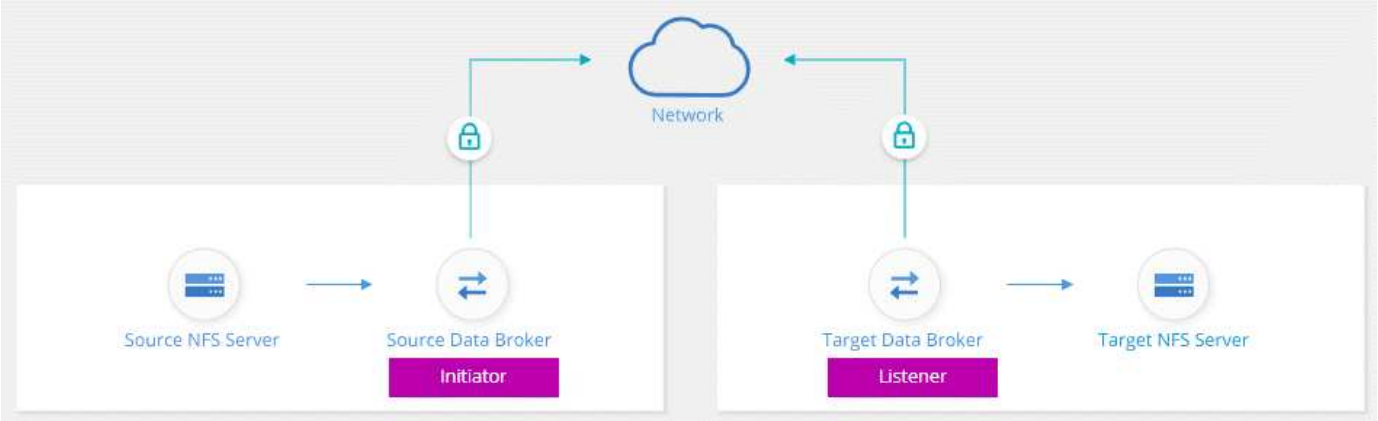
転送中のデータ暗号化を使用した NFS データの同期

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。

開始するには、何が必要ですか

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。

  既存のデータブローカーグループを使用する場合は、データブローカーが 1 つだけである必要があります。グループ内の複数のデータブローカーは、暗号化された同期関係ではサポートされません。

  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"
  - "Google Cloud のインストール状況を確認します"
  - "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]*を選択します。
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。
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。

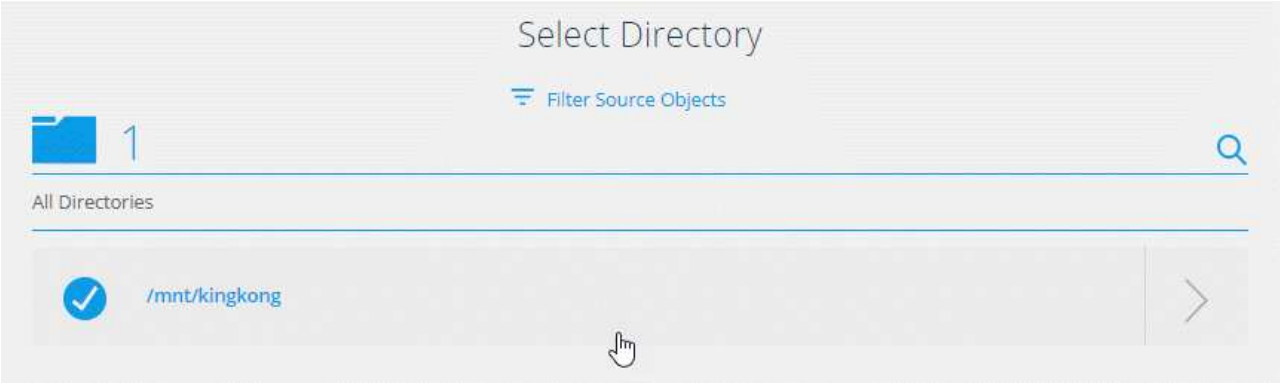
c. * データブローカー * ：新しいソースデータブローカーを追加するか、既存のデータブローカーを選択するよう求められます。

   次の点に注意してください。

   - 既存のデータブローカーグループを使用する場合は、データブローカーが 1 つだけである必要があります。グループ内の複数のデータブローカーは、暗号化された同期関係ではサポートされません。
   - 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、BlueXPのコピーと同期によって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]*を選択して、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。



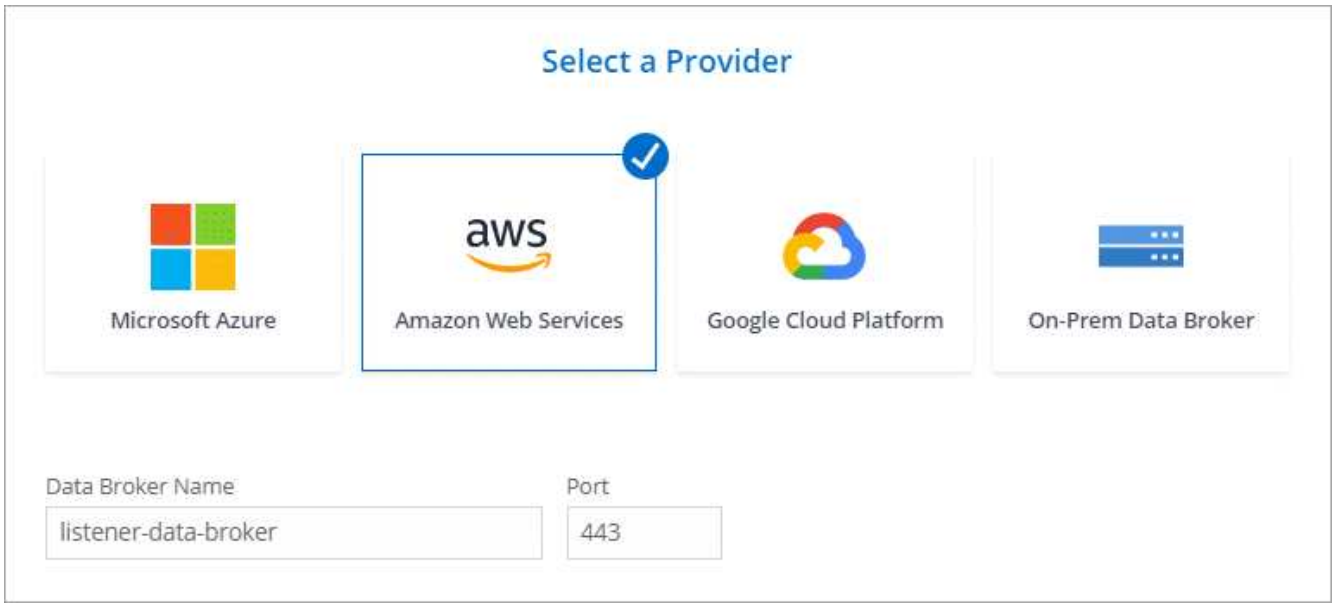
   オプションを選択するオプションを示すスクリーンショット。 "]

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。

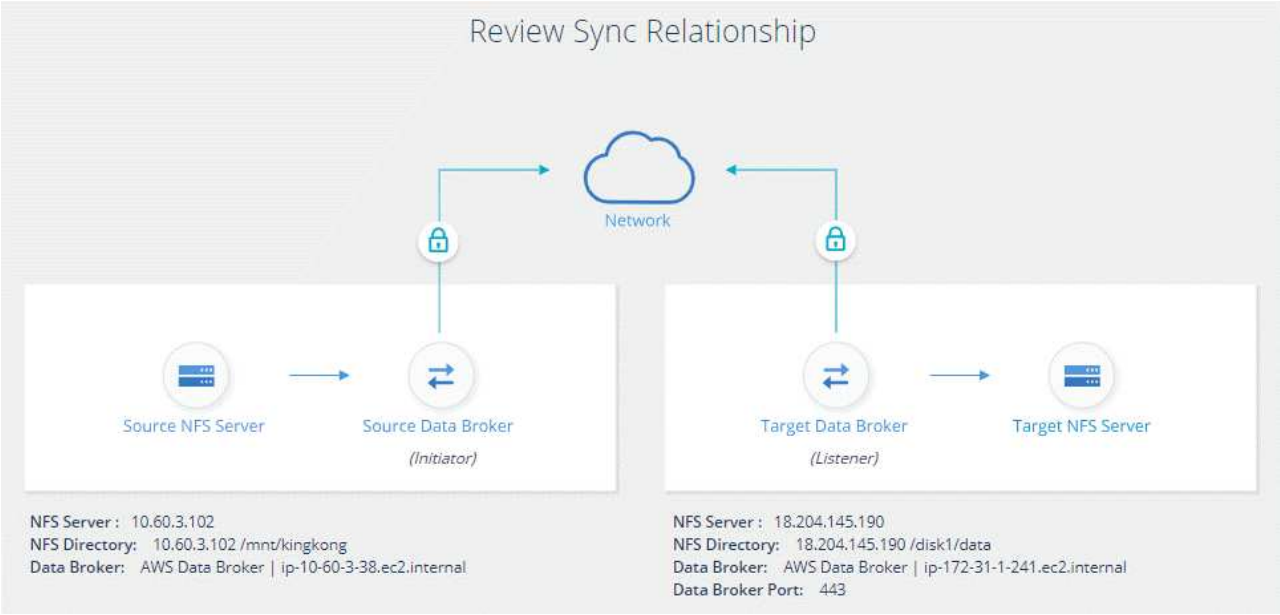
   ターゲットのデータブローカーがリスナーとして機能する場合のプロンプトの例を次に示します。ポートを指定するオプションに注目してください。



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]*を選択します。



結果

BlueXPのコピーと同期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]*を選択して、新しい関係の詳細を表示します。

外部の橋本社ボールトを使用するようにデータブローカーグループを設定する

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作

成する場合は、BlueXPのコピーと同期のユーザインターフェイスまたはAPIで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、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*） にアクセスするようにデータブローカーグループを設定する方法もあります。

この機能は、Amazon S3、Azure、Google Cloudのクレデンシャルを必要とする同期関係を備えたBlueXPのコピーおよび同期APIでサポートされます。

1. ボルトを準備します

URL を設定して、データブローカーグループ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。

2. データブローカーグループを準備

グループ内の各データブローカーのローカル構成ファイルを変更して、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グループを準備します。

3. **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

BlueXPのコピーを提供し、ボルト内のシークレットのURLと同期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

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

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

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

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。

データブローカーグループを準備しています

グループ内の各データブローカーのローカル構成ファイルを変更して、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グループを準備します。

手順

1. グループ内のデータブローカーへの SSH 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）

4. グループ内の他のすべてのデータブローカーについて、上記の手順を繰り返します。

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。

BlueXPのコピーを使用して関係をPOSTし、REST APIを同期

```
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
```

- ユーザートークンとBlueXP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"
        }
    }
}
```