転送中のデータ暗号化を使用した NFS データの同期

Cloud Manager

Ben Cammett
April 24, 2021

目次

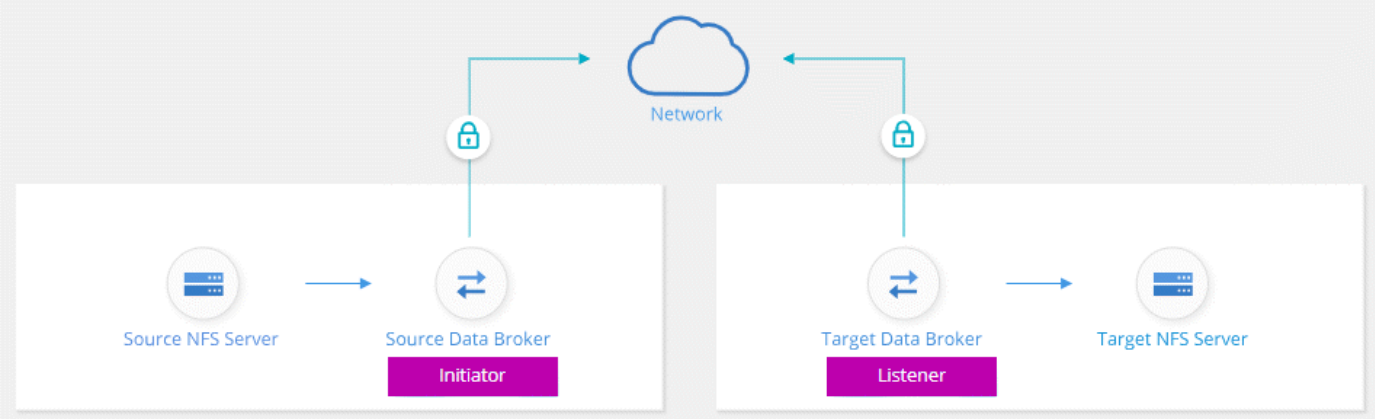
転送中のデータ暗号化を使用した NFS データの同期

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"

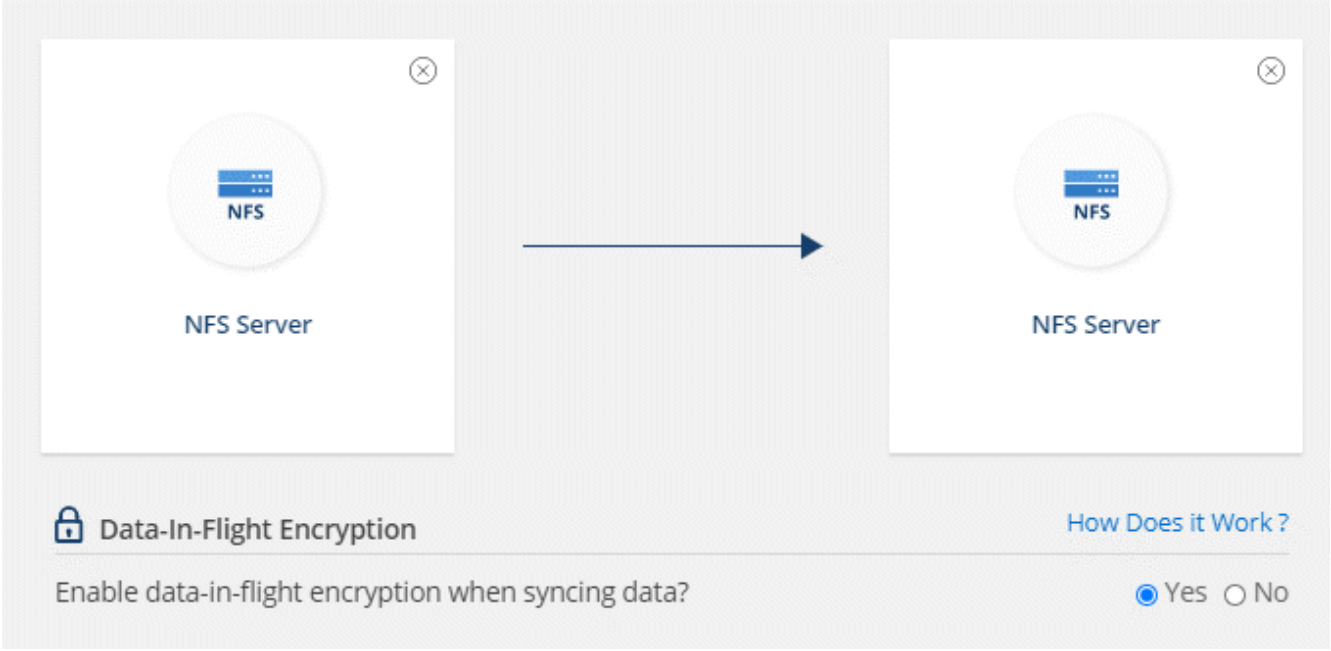
転送中のデータ暗号化を使用した **NFS** データの同期

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。

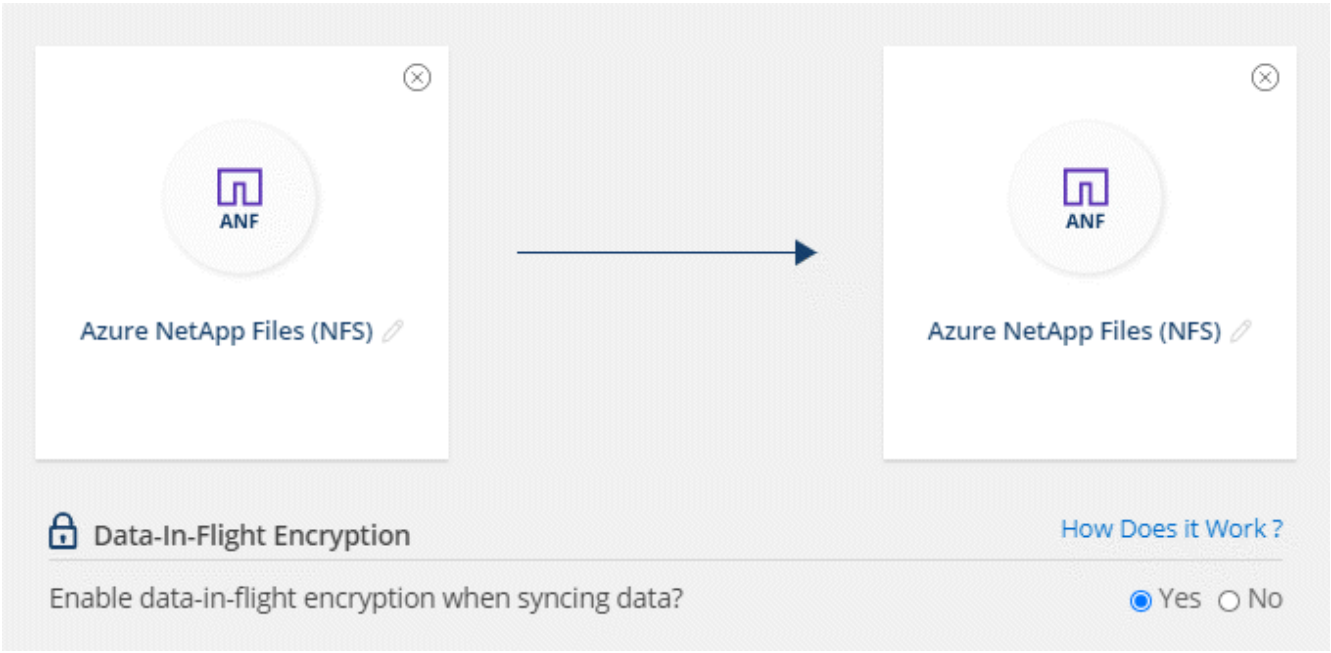
手順

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。

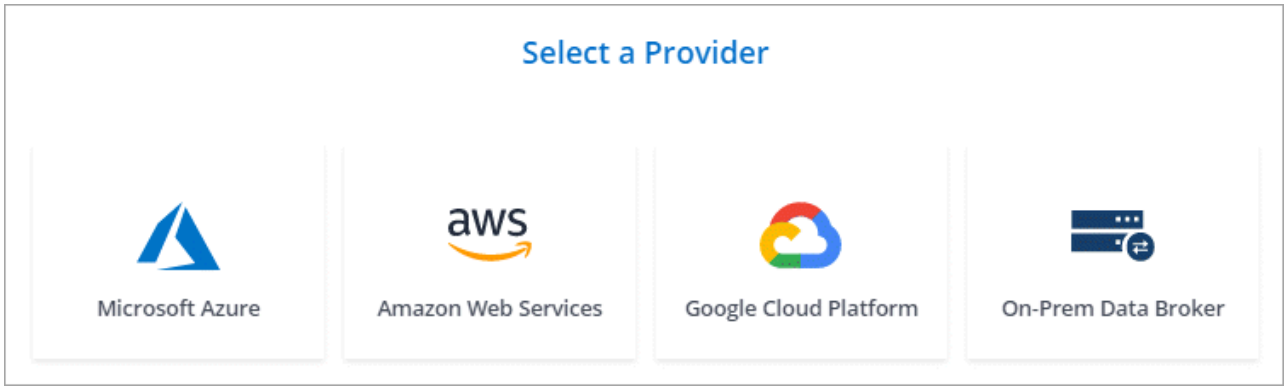
   b. * データブローカー機能の定義 *: ポート上での接続要求に対して ' どのデータ・ブローカ・リスン _ がどのデータ・ブローカ・リスン _ を実行するか ' およびどのデータ・ブローカが接続を開始するかを定義しますネットワーキング要件に基づいて選択してください。

   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

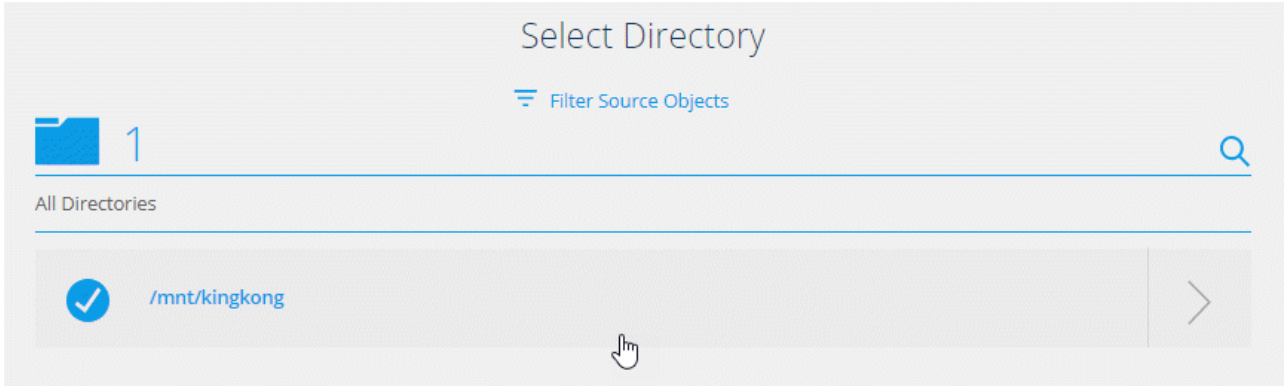
ります。

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。



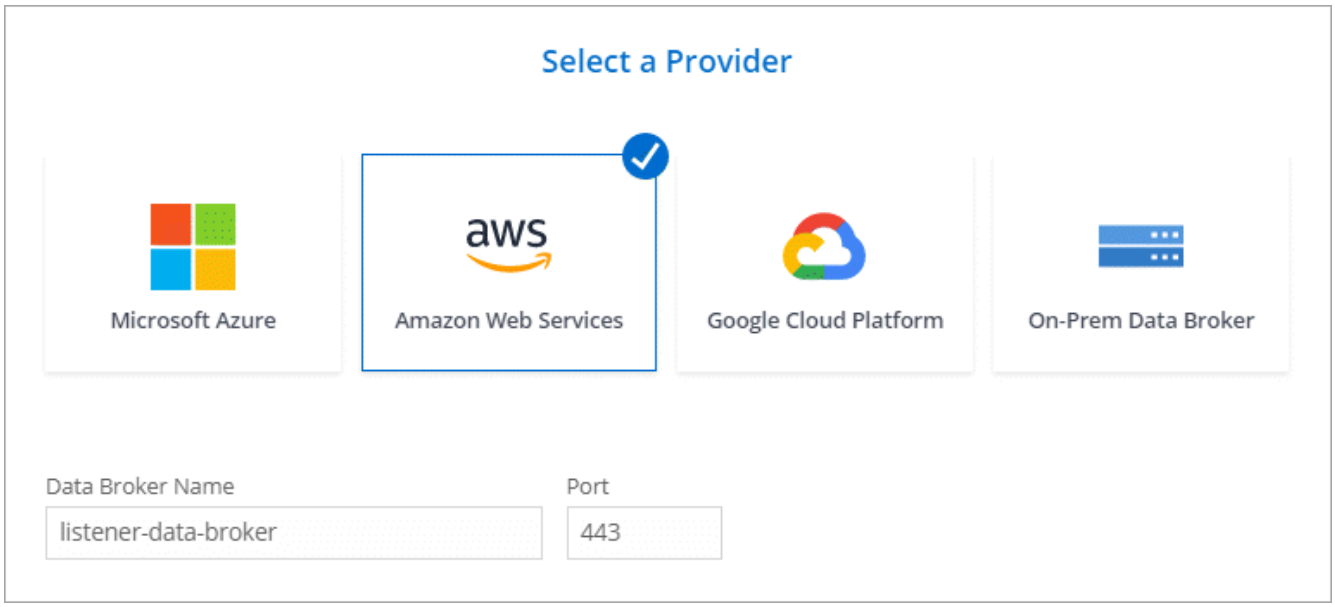
オプションを選択するオプションを示すスクリーンショット。 "]

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。

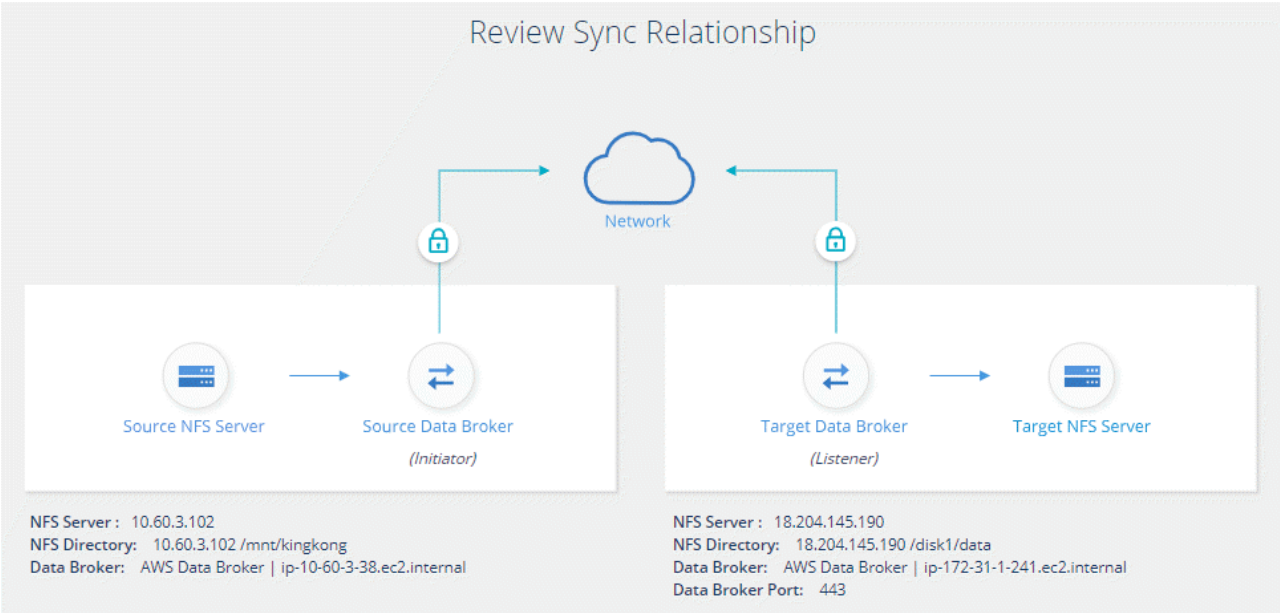
ターゲットのデータブローカーがリスナーとして機能する場合のプロンプトの例を次に示します。ポートを指定するオプションに注目してください。



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。