ソースとターゲット間でデータを同期する

NetApp Copy and Sync

NetApp
December 16, 2025

目次

ソースとターゲット間でデータを同期する

NetApp Copy and Syncのオブジェクト ストレージ間でデータを同期するためのデータ ブローカーを準備します。

NetApp Copy and Syncでオブジェクト ストレージからオブジェクト ストレージへ (たとえば、Amazon S3 から Azure Blob) データを同期する予定の場合は、同期関係を作成する前にデータ ブローカー グループを準備する必要があります。

タスク概要

データ ブローカー グループを準備するには、スキャナーの構成を変更する必要があります。構成を変更しないと、この同期関係でパフォーマンスの問題が発生する可能性があります。

開始する前に

オブジェクト ストレージからオブジェクト ストレージにデータを同期するために使用するデータ ブローカー グループは、これらのタイプの同期関係のみを管理する必要があります。データ ブローカー グループが異なるタイプの同期関係 (たとえば、NFS から NFS、またはオブジェクト ストレージから SMB) を管理している場合、それらの同期関係のパフォーマンスに悪影響が及ぶ可能性があります。

手順

1. "コピーと同期にログイン" 。
2. [コピーと同期] から、[データ ブローカーの管理] を選択します。
3. 選択 
4. スキャナーの設定を更新します。
   a. *スキャナーの同時実行性*を*1*に変更します。
   b. *スキャナープロセスの制限*を*1*に変更します。
5. *構成の統合*を選択します。

結果

コピーと同期により、データ ブローカー グループの構成が更新されます。

次の手順

これで、構成したデータ ブローカー グループを使用して、オブジェクト ストレージ間の同期関係を作成できるようになりました。

NetApp Copy and Syncで同期関係を作成する

同期関係を作成すると、 NetApp Copy and Sync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、コピーと同期は変更されたデータを 24 時間ごとに同期します。

一部のタイプの同期関係を作成するには、まずNetApp Consoleでシステムを作成する必要があります。

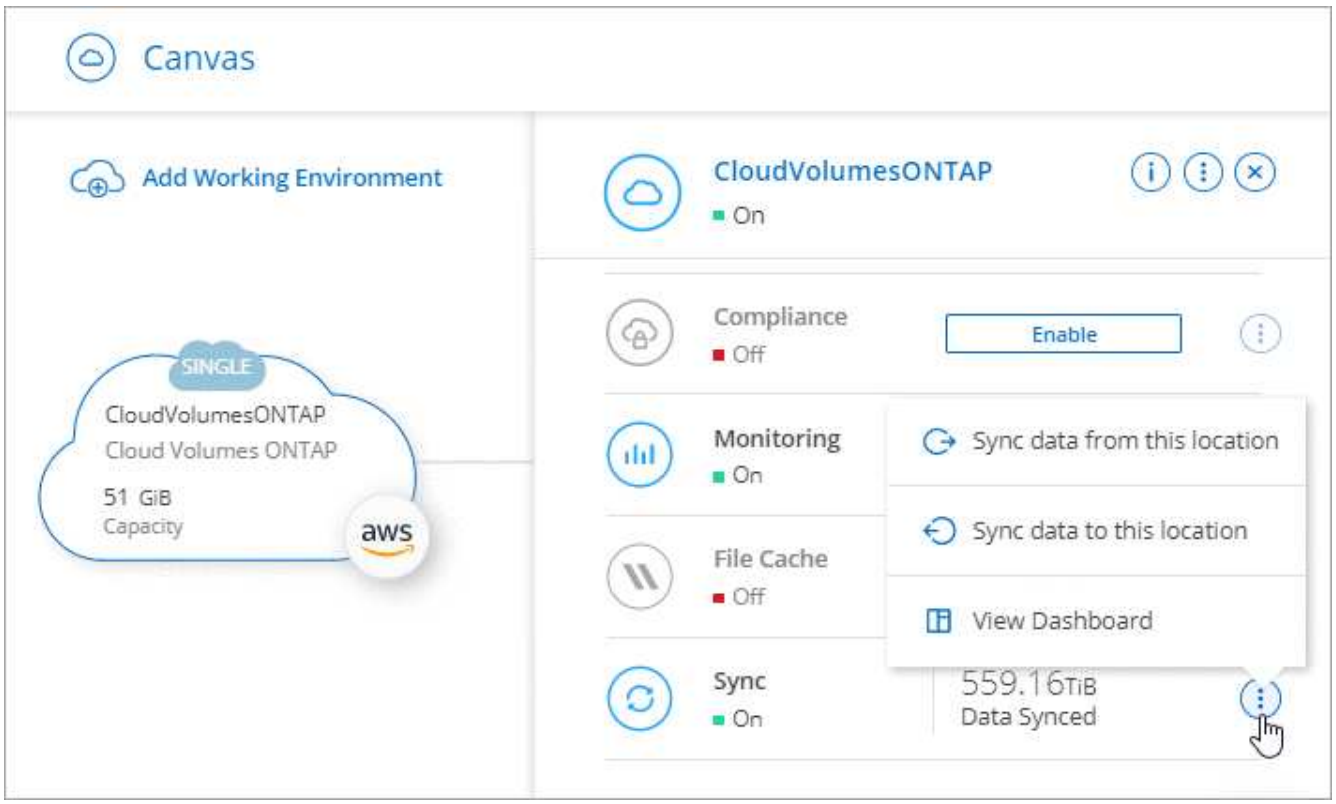
特定の種類のシステムの同期関係を作成する

次のいずれかの同期関係を作成する場合は、まずシステムを作成または検出する必要があります。

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- オンプレミスのONTAPクラスター

手順

1. "コピーと同期にログイン" 。
2. システムを作成または検出します。
   - "Amazon FSx for ONTAPシステムを作成する"
   - "Azure NetApp Files の設定と検出"
   - "AWS でCloud Volumes ONTAP を起動"
   - "Azure でCloud Volumes ONTAP を起動する"
   - "Google Cloud でCloud Volumes ONTAP を起動"
   - "既存のCloud Volumes ONTAPシステムの追加"
   - "ONTAPクラスターの検出"
3. *システムページ*を選択します。
4. 上記のいずれかのタイプに一致するシステムを選択してください。
5. [同期]の横にあるアクション メニューを選択します。



6. *この場所からデータを同期*または*この場所にデータを同期*を選択し、プロンプトに従って同期関係を設定します。

他の種類の同期関係を作成する

Amazon FSx for ONTAP、 Azure NetApp Files、 Cloud Volumes ONTAP、またはオンプレミスのONTAPクラスター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、次の手順に従います。以下の手順は、NFS サーバーから S3 バケットへの同期関係を設定する方法を示した例です。

1. NetApp Consoleで、[同期] 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。

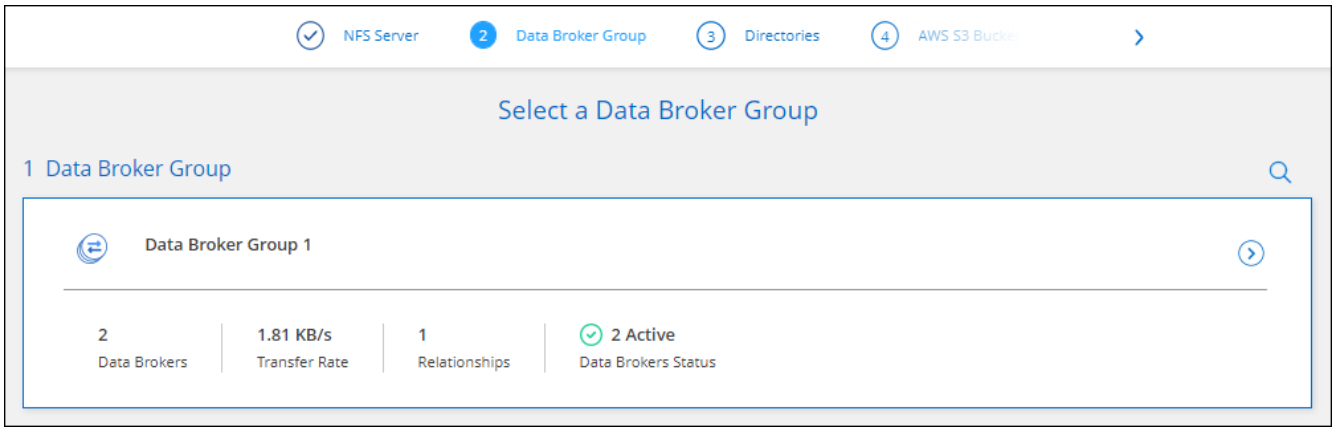
   次の手順は、NFS サーバーから S3 バケットへの同期関係を作成する方法の例を示しています。

3. **NFS** サーバー ページで、AWS に同期する NFS サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。
4. データ ブローカー グループ 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、既存の Linux ホストにデータ ブローカー ソフトウェアを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でデータブローカーを作成する"
- "Azureでデータブローカーを作成する"
- "Google Cloud でデータ ブローカーを作成する"
- "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。

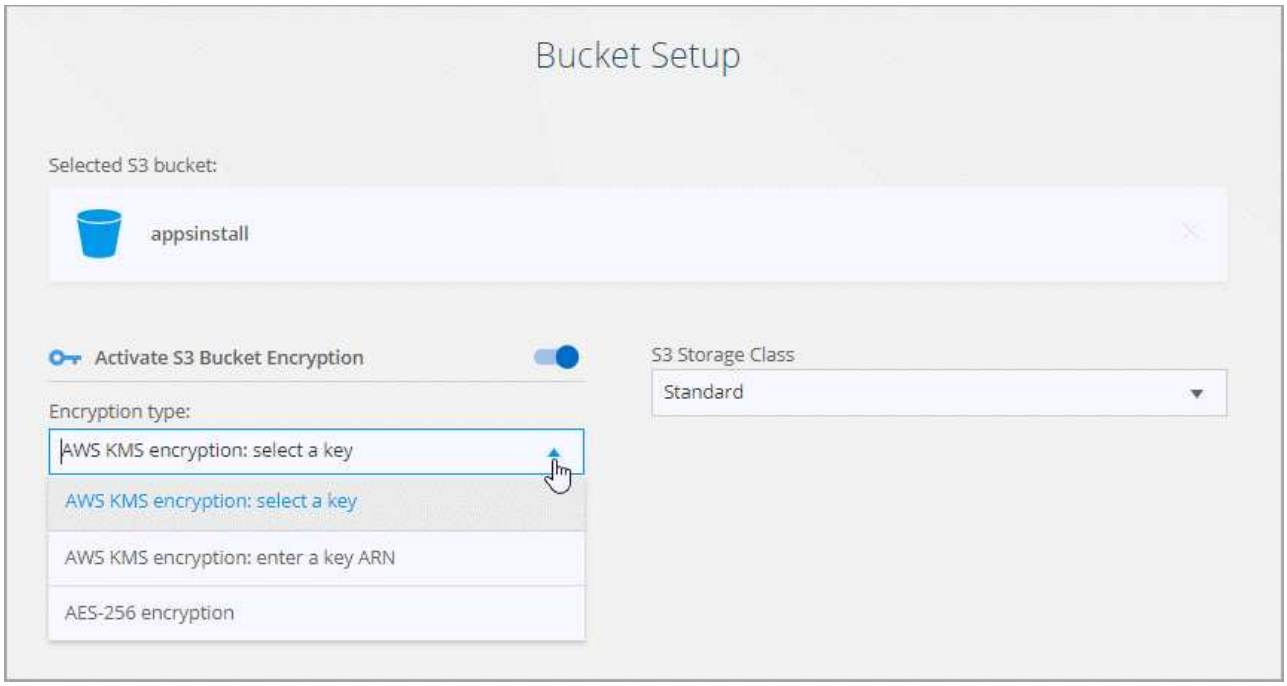


6. *ディレクトリ*ページで、最上位ディレクトリまたはサブディレクトリを選択します。

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 サーバー上の複数のディレクトリを同期する場合は、完了後に追加の同期関係を作成する必要があります。

7. **AWS S3** バケット 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。
   - AWS アカウントに関連付けられていない S3 バケットを選択するには、[リストに追加] を選択します。"S3バケットに特定の権限を適用する必要がある" 。
8. *バケット設定*ページでバケットを設定します。
   - S3 バケット暗号化を有効にするかどうかを選択し、AWS KMS キーを選択するか、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する" 。



9. *設定*ページで、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。

スケジュール

今後の同期の定期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。関係を 1 分ごとに同期するようにスケジュールできます。

同期タイムアウト

指定された分数、時間数、または日数内に同期が完了しなかった場合に、コピーと同期でデータ同期をキャンセルするかどうかを定義します。

通知

NetAppコンソールの通知センターでコピーと同期の通知を受信するかどうかを選択できます。成功したデータ同期、失敗したデータ同期、キャンセルされたデータ同期に関する通知を有効にすることができます。

再試行

コピーと同期がファイルをスキップする前に同期を再試行する回数を定義します。

連続同期

最初のデータ同期の後、コピーと同期はソースの S3 バケットまたは Google Cloud Storage バケットの変更をリッスンし、変更が発生するたびにターゲットに継続的に同期します。スケジュールされた間隔でソースを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とき、および S3 バケットまたは Google Cloud Storage から Azure Blob Storage、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、S3、 StorageGRIDに、または Azure Blob Storage から Azure Blob Storage、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、 StorageGRIDにデータを同期する場合にのみ使用できます。

この設定を有効にすると、他の機能に次の影響があります。

- 同期スケジュールは無効です。
- 次の設定は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、および変更日。
- S3 がソースの場合、サイズによるフィルターはコピー イベントで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)。
- 関係が作成された後は、関係を加速するか削除することしかできません。同期を中止したり、設定を変更したり、レポートを表示したりすることはできません。

  外部バケットとの継続的な同期関係を作成できます。これを行うには、次の手順に従ってください。

  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 すべて停止

    B. sudo pm2 すべて開始

  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を作成するために使用されるデータ ブローカーは、プロジェクト内のバケットとの別の継続的な同期関係を作成することはできません。

比較する

ファイルまたはディレクトリが変更されたかどうか、再度同期する必要があるかどうかを判断するときに、コピーと同期で特定の属性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、コピーと同期はパス、ファイル サイズ、ファイル名をチェックしてソースとターゲットを比較します。変更があった場合は、それらのファイルとディレクトリが同期されます。

次の属性を比較して、コピーと同期を有効にするか無効にするかを選択できます。

- **mtime**: ファイルの最終更新時刻。この属性はディレクトリには無効です。
- **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には、このオプションを有効にします。ユーザーがソースのメタデータを変更した場合、コピーと同期は次の同期でこのオブジェクトをコピーしますが、ユーザーがソースのタグを変更した場合 (データ自体ではなく)、コピーと同期は次の同期でオブジェクトをコピーしません。

関係を作成した後は、このオプションを編集することはできません。

タグのコピーは、Azure Blob または S3 互換エンドポイント (S3、 StorageGRID、または IBM Cloud Object Storage) をターゲットとして含む同期関係でサポートされます。

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 ブロブ
- Google Cloud Storage
- IBM Cloud Object Storage
- StorageGRID

最近変更されたファイル

スケジュールされた同期の前に最近変更されたファイルを除外することを選択します。

ソース上のファイルを削除

コピーと同期によってファイルがターゲットの場所にコピーされた後、ソースの場所からファイルを削除することを選択します。このオプションでは、ソース ファイルがコピー後に削除されるため、データが失われるリスクがあります。

このオプションを有効にする場合は、データ ブローカーの local.json ファイル内のパラメーター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後、再起動する必要があります。 `pm2 restart all` 。

ターゲット上のファイルを削除する

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を削除しません。

ファイルの種類

各同期に含めるファイルの種類（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 と NFS の関係でのみ使用できます。ユーザーは 1 つのスキャナー プロセスと 1 つのスキャナー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する

ファイル拡張子を入力して Enter キーを押すことで、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します。たとえば、*.log ファイルを除外するには、「*log*」または「*.log*」と入力します。複数の拡張子の場合、区切り文字は必要ありません。次のビデオでは短いデモを紹介します。

同期関係のファイル拡張子を除外する

> Regex または正規表現は、ワイルドカードや glob 表現とは異なります。この機能は正規表現でのみ動作します。

ディレクトリを除外する

同期から除外する正規表現またはディレクトリを最大 15 個指定するには、名前またはディレクトリのフル パスを入力して Enter キーを押します。デフォルトでは、.copy-offload、.snapshot、~snapshot ディレクトリは除外されます。

> Regex または正規表現は、ワイルドカードや glob 表現とは異なります。この機能は正規表現でのみ動作します。

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、特定のサイズ範囲内のファイルのみを同期するかを選択します。

更新日

最終更新日に関係なくすべてのファイル、特定の日付以降、特定の日付前、または時間範囲内で更新されたファイルを選択します。

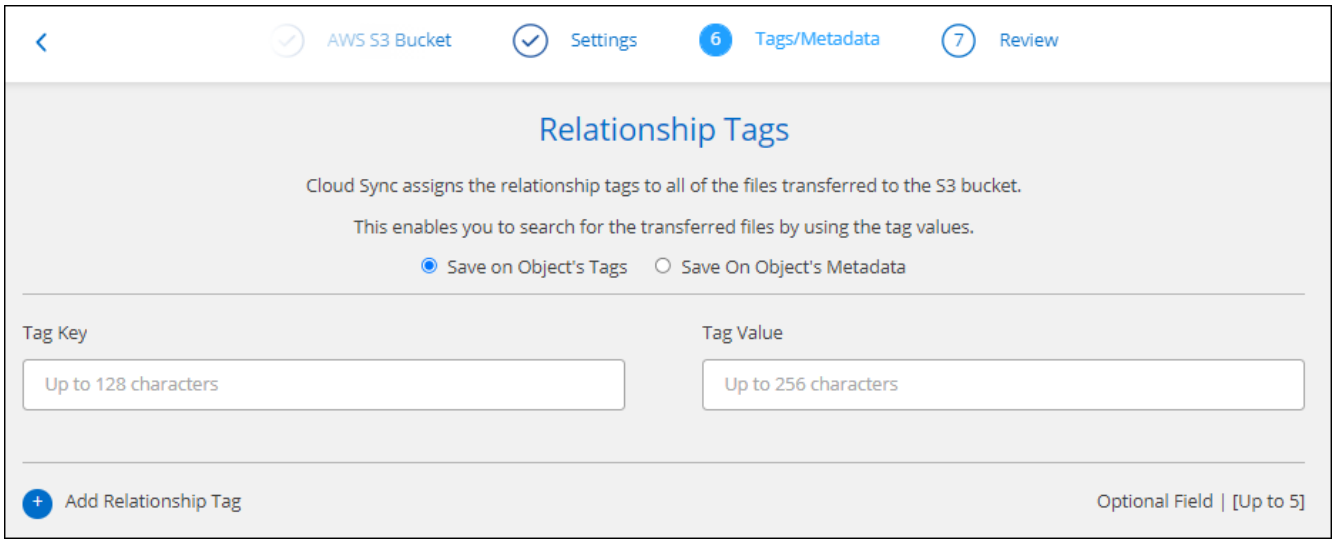
作成日

SMB サーバーがソースの場合、この設定により、特定の日付以降、特定の日付前、または特定の時間範囲内に作成されたファイルを同期できます。

ACL - アクセス制御リスト

関係を作成するとき、または関係を作成した後に設定を有効にして、SMB サーバーから ACL のみ、ファイルのみ、または ACL とファイルをコピーします。

10. *タグ/*メタデータ ページで、S3 バケットに転送される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。



同じ機能は、 StorageGRIDおよび IBM Cloud Object Storage にデータを同期するときにも利用できます。 Azure および Google Cloud Storage の場合、メタデータ オプションのみが利用可能です。

11. 同期関係の詳細を確認し、「関係の作成」を選択します。

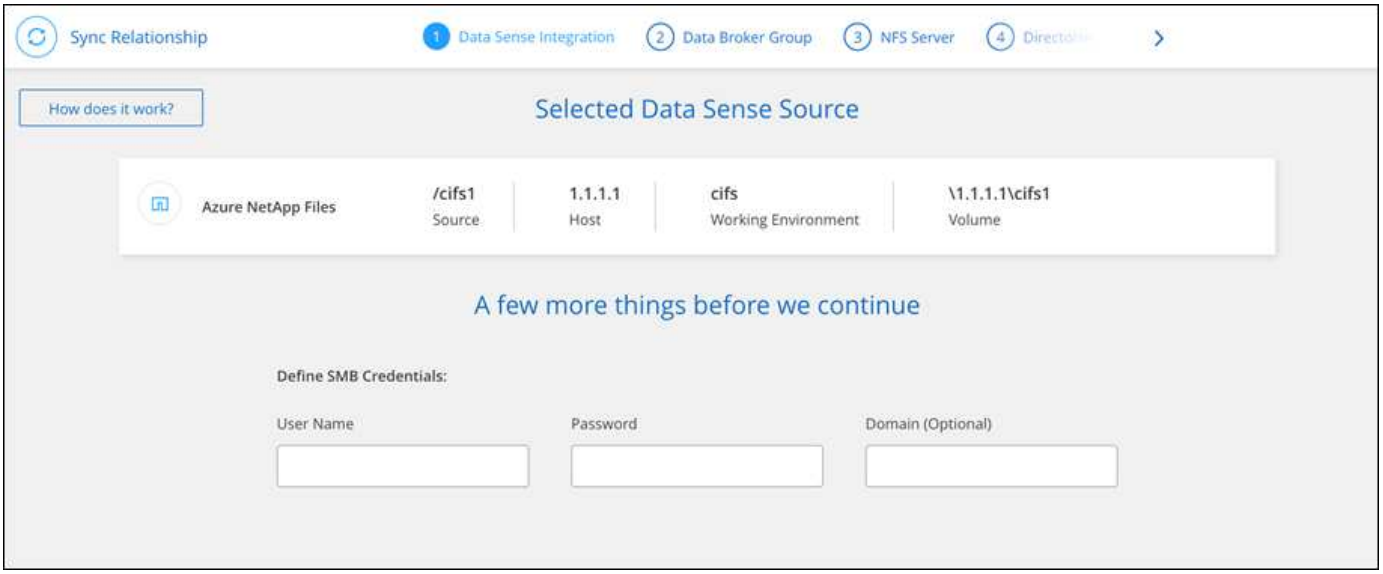
結果

コピーと同期は、ソースとターゲット間のデータの同期を開始します。同期にかかった時間、同期が停止したかどうか、コピー、スキャン、または削除されたファイルの数に関する同期統計が利用できます。その後、 "同期関係" 、 "データブローカーを管理する" 、 または "パフォーマンスと構成を最適化するためのレポートを作成する"。

NetApp Data Classificationから同期関係を作成する

コピーと同期はNetApp Data Classificationと統合されています。 NetApp Data Classification内から、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。

NetApp Data Classificationからデータ同期を開始すると、すべてのソース情報が 1 つの手順にまとめられ、いくつかの重要な詳細を入力するだけで済みます。次に、新しい同期関係のターゲットの場所を選択します。



"NetApp Data Classificationから同期関係を開始する方法を学びます" 。

NetApp Copy and Syncで SMB 共有から ACL をコピーする

NetApp Copy and Sync 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 SMB 共有間の ACL を手動で保持することもできます。

オプション

- コピーと同期を設定して ACL を自動的にコピーする
- SMB共有間でACLを手動でコピーする

ACLをコピーするにはコピーと同期を設定する

関係を作成するとき、または関係を作成した後に設定を有効にして、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 をコピーします。

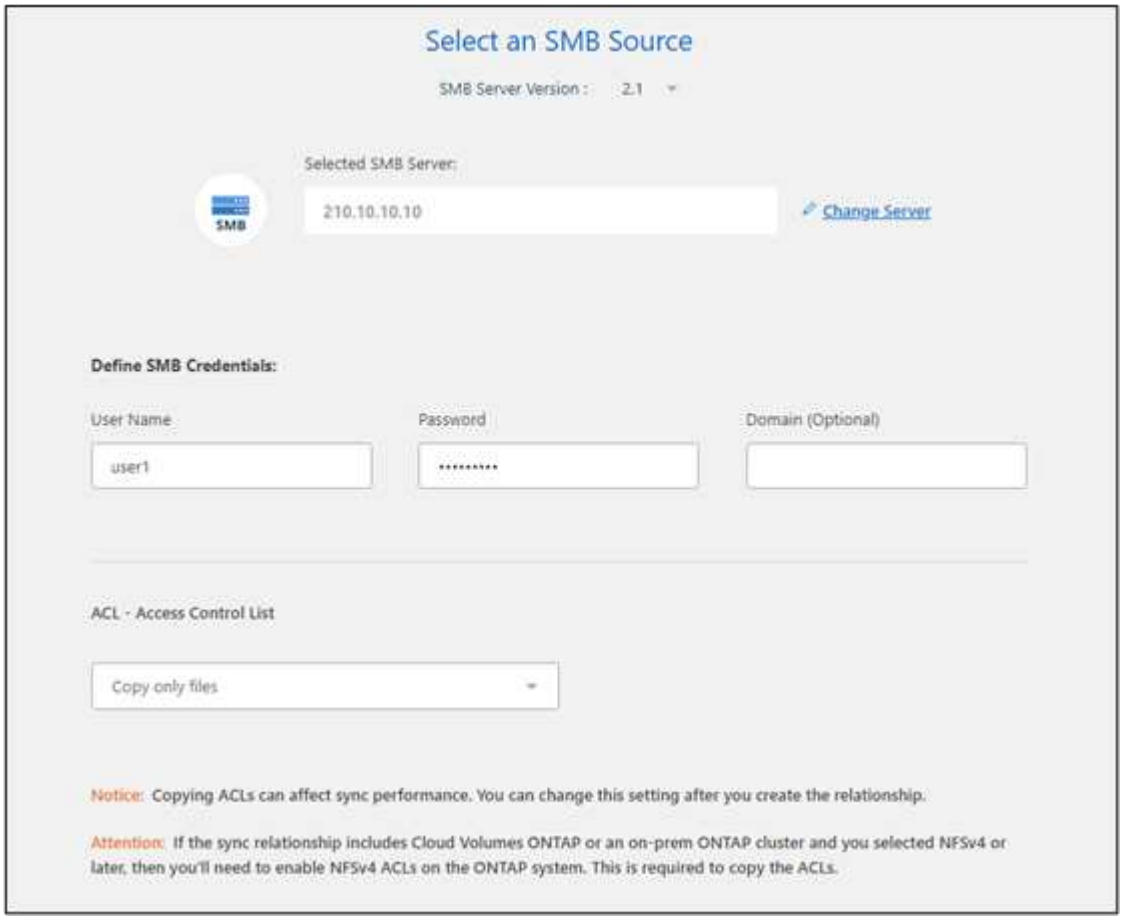
開始する前に

この機能は、AWS、Azure、Google Cloud Platform、オンプレミスのデータブローカーなど、あらゆるタイプのデータブローカーで動作します。オンプレミスのデータブローカーは、"サポートされているオペレーティングシステム" 。

新しい関係を築くためのステップ

1. "コピーと同期にログイン" 。
2. 「コピーと同期」から、「新しい同期の作成」を選択します。
3. SMB サーバーまたはオブジェクト ストレージをソースとして、SMB サーバー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。
4. **SMB** サーバー ページで:
   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] を選択します。
   b. SMB サーバーの資格情報を入力します。

c. ファイルのみコピー、**ACL** のみコピー、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。



5. 残りの指示に従って同期関係を作成します。

SMB からオブジェクト ストレージに ACL をコピーする場合、ターゲットに応じて、ACL をオブジェクトのタグにコピーするか、オブジェクトのメタデータにコピーするかを選択できます。 Azure および Google Cloud Storage の場合、メタデータ オプションのみが利用可能です。

次のスクリーンショットは、この選択を行うことができる手順の例を示しています。

既存の関係のための手順

1. 同期関係にマウスを移動し、アクション メニューを選択します。
2. *設定*を選択します。
3. ファイルのみコピー、**ACL** のみコピー、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. *設定を保存*を選択します。

> コピーと同期では SMB ACL (アクセス許可) は保持されますが、ファイルまたはフォルダーの所有権はコピーされません。所有権は SMB ACL 転送操作には含まれません。

結果

データを同期する際、コピーと同期はソースとターゲット間の ACL を保持します。

SMB共有間でACLを手動でコピーする

Windows robocopy コマンドを使用して、SMB 共有間の ACL を手動で保持できます。

> ACLに加えて所有権（所有者とグループ）を保持する必要がある場合は、 `robocopy`指示。使用して `/copyall`フラグは ACL、所有権、監査情報をコピーします。

手順

1. 両方の SMB 共有に完全にアクセスできる 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. 「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]
   ```

   source と *target* は両方とも UNC 形式を使用して指定する必要があります。例: \\<サーバー>\<共有>\<パス>

NetApp Copy and Syncの Data In Flight 暗号化を使用して NFS データを同期する

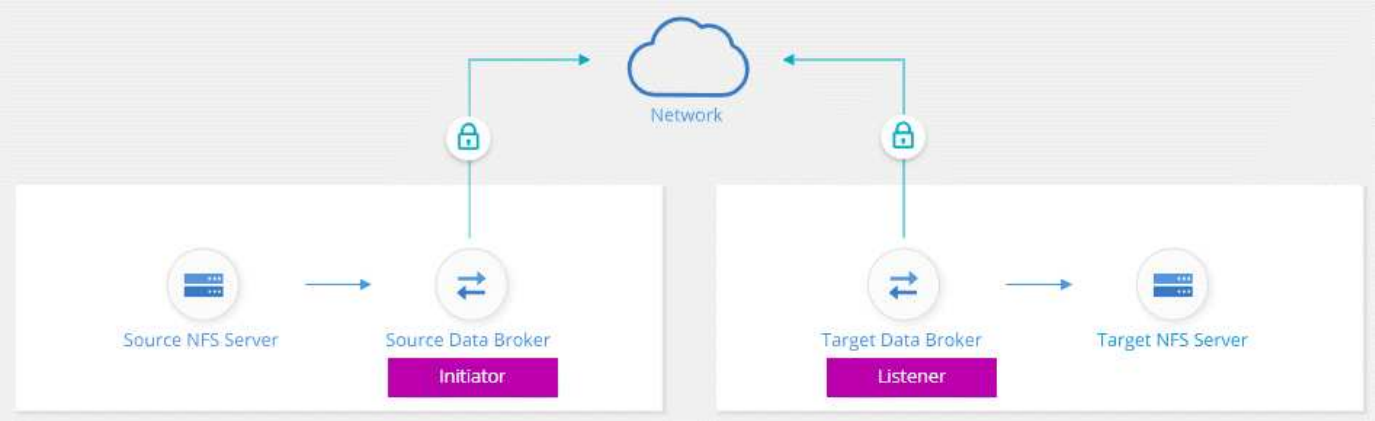
企業に厳格なセキュリティ ポリシーがある場合は、 NetApp Copy and Syncの転送中データ暗号化を使用して NFS データを同期できます。この機能は、NFS サーバーから別の NFS サーバー、およびAzure NetApp FilesからAzure NetApp Files間でサポートされ

ます。

たとえば、異なるネットワークにある 2 つの NFS サーバー間でデータを同期したい場合があります。あるいは、サブネットまたはリージョン間でAzure NetApp Files上のデータを安全に転送する必要がある場合もあります。

転送中のデータ暗号化の仕組み

データインフライト暗号化は、2 つのデータ ブローカー間でネットワーク経由で送信される NFS データを暗号化します。次の図は、2 つの NFS サーバーと 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 ブローカーが イニシエーター として機能します。データを同期する時間になると、他のデータ ブローカー (リスナー) に接続要求を送信します。そのデータ ブローカーはポート 443 で要求をリッスンします。必要に応じて別のポートを使用することもできますが、そのポートが別のサービスによって使用されていないことを必ず確認してください。

たとえば、オンプレミスの NFS サーバーからクラウドベースの NFS サーバーにデータを同期する場合、接続要求をリッスンするデータ ブローカーと接続要求を送信するデータ ブローカーを選択できます。

飛行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、イニシエーターは他のデータ 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 を使用してソースからのデータを暗号化します。
3. 次に、データをネットワーク経由でターゲットのデータ ブローカーに送信します。
4. ターゲット データ ブローカーは、データをターゲットに送信する前に復号化します。
5. 最初のコピーの後、コピーと同期は変更されたデータを 24 時間ごとに同期します。同期するデータがある場合、イニシエーターが他のデータ ブローカーとの暗号化された接続を開くことでプロセスが開始されます。

   より頻繁にデータを同期したい場合は、"関係を作成した後でもスケジュールを変更できます" 。

サポートされるNFSバージョン

- NFS サーバーの場合、データインフライト暗号化は NFS バージョン 3、4.0、4.1、および 4.2 でサポートされます。
- Azure NetApp Filesの場合、データインフライト暗号化は NFS バージョン 3 および 4.1 でサポートされま

す。

プロキシサーバーの制限

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 サーバー経由でルーティングできなくなります。

始めるために必要なもの

以下のものを必ず用意してください。

- 2つのNFSサーバーが"ソースとターゲットの要件"または、2 つのサブネットまたはリージョンにAzure NetApp Files。
- サーバーの 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の場所。

  既存のデータ ブローカーを選択できますが、イニシエーター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、新しいデータ ブローカー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、グループに含まれるデータ ブローカーが 1 つだけである必要があります。暗号化された同期関係では、グループ内の複数のデータ ブローカーはサポートされません。

  データ ブローカーをまだデプロイしていない場合は、データ ブローカーの要件を確認してください。厳格なセキュリティポリシーがあるため、ポート443からの送信トラフィックと、"インターネットエンドポイント"データブローカーが連絡する。

  - "AWSのインストールを確認する"
  - "Azureのインストールを確認する"
  - "Google Cloud のインストールを確認する"
  - "Linuxホストのインストールを確認する"

データインフライト暗号化を使用して **NFS** データを同期する

2 つの NFS サーバー間またはAzure NetApp Files間で新しい同期関係を作成し、インフライト暗号化オプションを有効にして、プロンプトに従います。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. **NFS** サーバー 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、はい を選択して、転送中のデータ暗号化を有効にします。
4. 指示に従って関係を作成します。

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

b. データ ブローカーの機能の定義: ポートで接続要求を リッスン するデータ ブローカーと、接続を 開始 するデータ ブローカーを定義します。ネットワーク要件に基づいて選択してください。

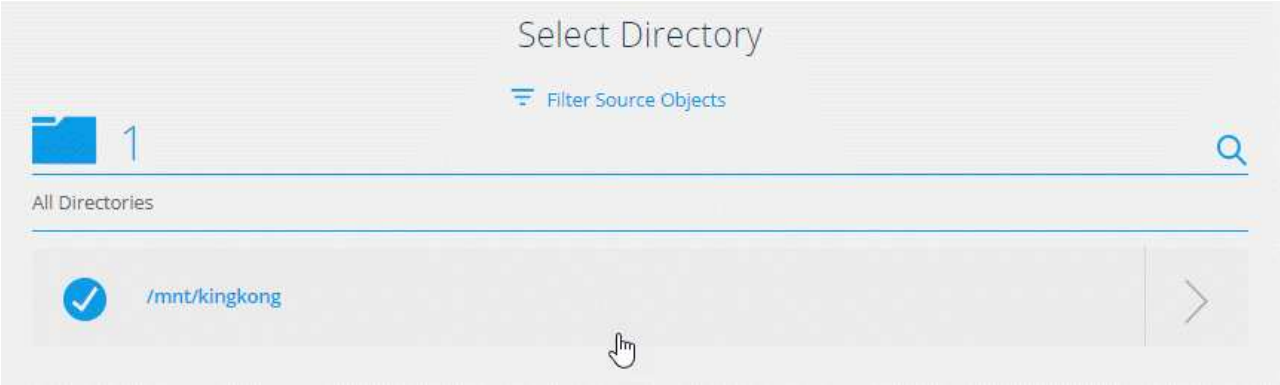
c. データ ブローカー: プロンプトに従って新しいソース データ ブローカーを追加するか、既存のデータ ブローカーを選択します。

   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、グループに含まれるデータ ブローカーが 1 つだけである必要があります。暗号化された同期関係では、グループ内の複数のデータ ブローカー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、それは新しいデータ 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、Copy and Sync によってインストール手順が表示されます。データ ブローカーをクラウドにデプロイすることも、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することもできます。

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 ファイルとフォルダー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するには、[ソース オブジェクトのフィルター] を選択します。

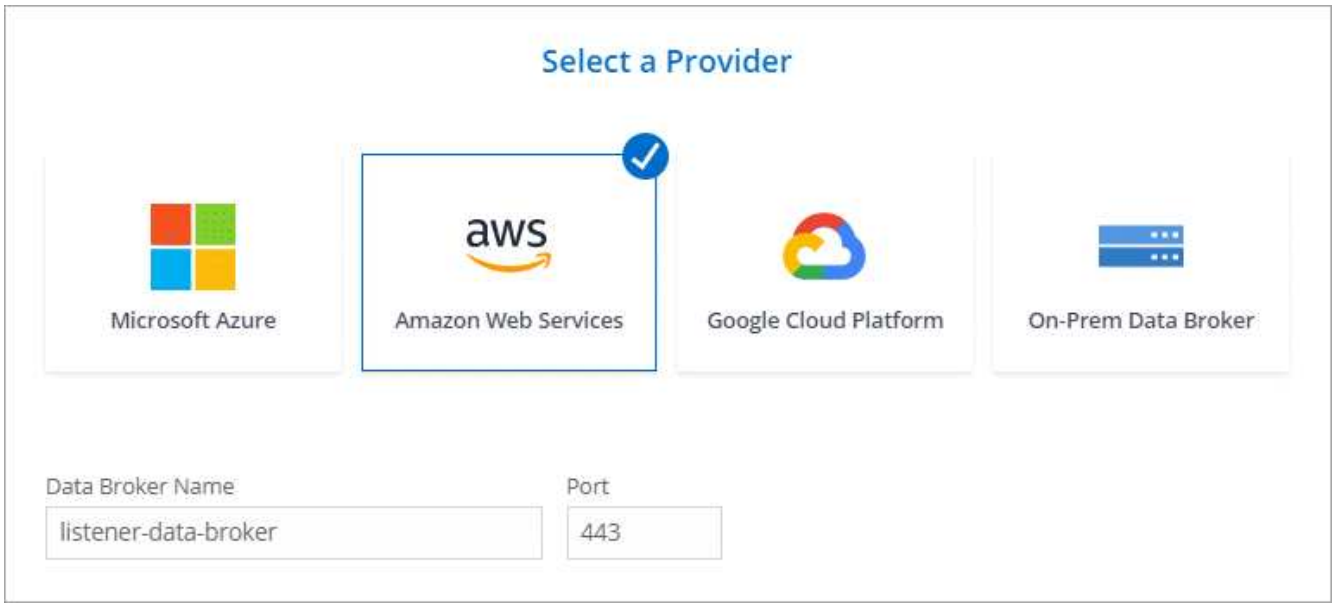


e. ターゲット **NFS** サーバー/ターゲット**Azure NetApp Files**: NFS バージョンを選択し、新しい NFS ターゲットを入力するか、既存のサーバーを選択します。

f. ターゲット データ ブローカー: プロンプトに従って新しいソース データ ブローカーを追加するか、既存のデータ ブローカーを選択します。

   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、新しいデータ ブローカーである必要があります。

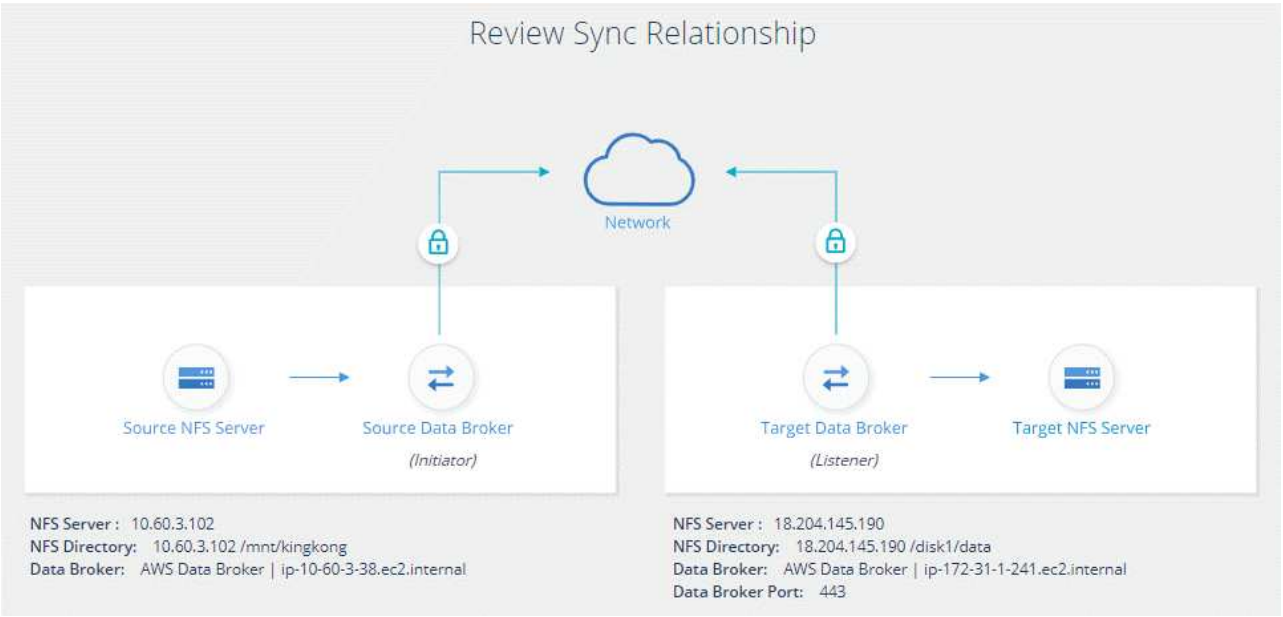
   ターゲット データ ブローカーがリスナーとして機能する場合のプロンプトの例を次に示します。ポートを指定するオプションに注意してください。



a. ターゲット ディレクトリ: 最上位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ーを作成します。

b. 設定: ソース ファイルとフォルダー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

コピーと同期により、新しい同期関係の作成が開始されます。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。

NetApp Copy and Syncで外部 HashiCorp Vault を使用するためのデータ ブローカー グループを設定する

Amazon S3、Azure、または Google Cloud の認証情報を必要とする同期関係を作成する

場合は、 NetApp Copy and Syncユーザー インターフェイスまたは API を通じてそれらの認証情報を指定する必要があります。別の方法としては、データ ブローカー グループを設定して、外部の HashiCorp Vault から資格情報 (または シークレット) に直接アクセスすることもできます。

この機能は、Amazon S3、Azure、または Google Cloud の資格情報を必要とする同期関係を持つコピーおよび同期 API を通じてサポートされます。


金庫の準備

URL を設定して、データ ブローカー グループに資格情報を提供するためのボールトを準備します。ボールト内のシークレットの URL は、*Creds* で終わる必要があります。


データブローカーグループの準備

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、データ ブローカー グループが外部ボールトから資格情報を取得できるように準備します。


APIを使用して同期関係を作成する

すべての設定が完了したら、API 呼び出しを送信して、ボ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。

金庫の準備

コピーと同期に、ボールト内のシークレットの URL を提供する必要があります。これらの URL を設定して、Vault を準備します。作成する予定の同期関係の各ソースとターゲットの資格情報への 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
```

パス

シークレットへのプレフィックス パス。これは、あなたに固有の任意の値にすることができます。

Request 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に、API POST リクエストのヘッダーの 1 つに 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

定義される以下のプロトコルのいずれか "ポストリレーションシップv2ドキュメント": S3、AZURE、または GCP (それぞれ大文字にする必要があります)。

資格情報

URL は *Creds* で終わる必要があります。

例

次の例は、シークレットの URL を示しています。

ソース資格情報の完全な **URL** とパスの例
http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds

例からわかるように、プレフィックス パスは */my-path/all-secrets/*、リクエスト ID は *hb312vdasr2*、ソース エンドポイントは S3 です。

ターゲット資格情報の完全な **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の準備

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、データ ブローカー グループが外部ボールトから資格情報を取得できるように準備します。

手順

1. グループ内のデータ ブローカーに SSH で接続します。
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-integrations.hashicorp* の下の構成パラメータ フィールドを次のように設定します。

   有効
   - 有効な値: true/false
   - タイプ: ブール値
   - デフォルト値: false
   - 真実: データブローカーは独自の外部HashiCorp Vaultから秘密情報を取得します
   - False: データブローカーは資格情報をローカルの保管庫に保存します

   URL
   - タイプ: 文字列
   - 値: 外部の金庫へのURL

   path（パス）
   - タイプ: 文字列
   - 値: シークレットへのパスの先頭に資格情報を入力します

   拒否-不正
   - データブローカーが不正な外部ボールトを拒否するかどうかを決定します
   - タイプ: ブール値

- デフォルト: false

認証方法
- データブローカーが外部のボールトから資格情報にアクセスするために使用する認証方法
- タイプ: 文字列
- 有効な値: "aws-iam" / "role-app" / "gcp-iam"

ロール名
- タイプ: 文字列
- ロール名（aws-iam または gcp-iam を使用する場合）

シークレットイドとルートイド
- タイプ: 文字列 (app-role を使用する場合)

ネームスペース
- タイプ: 文字列
- 名前空間（必要な場合は X-Vault-Namespace ヘッダー）

4. グループ内の他のデータ ブローカーに対しても、これらの手順を繰り返します。

aws-role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 認証を使用する際の権限の設定

gcp-iam 認証方法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" 。

ボールトからのシークレットを使用して新しい同期関係を作成する

すべての設定が完了したら、API 呼び出しを送信して、ボ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。

コピーおよび同期 REST API を使用して関係を投稿します。

```
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
```

- ユーザートークンとNetApp ConsoleアカウントIDを取得するには、"ドキュメントのこのページを参照してください"。
- 結婚後の体を作るには、 "relationship-v2 API呼び出しを参照してください"。

例

POSTリクエストの例:

```
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"
        }
    }
}
```

著作権に関する情報

商標に関する情報