



# Cloud Sync を使用します

## Cloud Sync

NetApp  
May 02, 2022

# 目次

Cloud Sync を使用します .....	1
ソースとターゲットの間でデータを同期します .....	1
無料トライアルの終了後に同期関係の料金を支払う .....	19
同期関係の管理 .....	21
データブローカーグループの管理 .....	26
レポートを作成および表示して、設定を調整します .....	34
データブローカーのアンインストール .....	37

# Cloud Sync を使用します

## 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、Cloud Sync サービスはソースからターゲットにファイルをコピーします。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。

一部のタイプの同期関係を作成する前に、Cloud Manager 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 クラスター

### 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 クラスターの検出"](#)
2. 「\* キャンバス \*」をクリックします。
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 クラスターで、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. Cloud Manager で、\* Sync \* をクリックします。
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]** をクリックします。



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。

Cloud Sync が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 \* をクリックし、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 \* をクリックして、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

指定した時間数または日数以内に同期が完了しなかった場合に、Cloud Sync がデータの同期をキャンセルするかどうかを定義します。

#### 通知

Cloud Managerの通知センターでCloud Sync 通知を受信す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

ファイルをスキップする前に Cloud Sync がファイルの同期を再試行する回数を定義します。

#### で比較してください

ファイルまたはディレクトリが変更され、再度同期する必要があるかどうかを判断するときに、Cloud Sync で特定の属性を比較するかどうかを選択します。

これらの属性をオフにしても、Cloud Sync はパス、ファイルサイズ、および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。

Cloud Sync では、次の属性の比較を有効または無効に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。ユーザがソース上のメタデータを変更すると、Cloud Sync は次の同期でこのオブジェクトをコピーしますが、ユーザがソース上のタグを変更した場合（データ自体は変更した場合を除く）、Cloud Sync は次の同期でその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。

タグのコピーは、S3 互換エンドポイント（S3、StorageGRID、または IBM Cloud Object Storage）を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せん。

- 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

Cloud Sync 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
    }
  }
}
```

## 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）を定義します。

## ファイル拡張子を除外します

ファイル拡張子を入力し、\* Enter \* キーを押して、同期から除外するファイル拡張子を指定します。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/cloud-manager-sync//media/video\\_file\\_extensions.mp4](https://docs.netapp.com/ja-jp/cloud-manager-sync//media/video_file_extensions.mp4) (video)

## 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、SMB サーバから ACL をコピーします。

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。

The screenshot shows the 'Relationship Tags' configuration page. At the top, there are navigation tabs: '<', 'AWS S3 Bucket', 'Settings', '6 Tags/Metadata', and '7 Review'. The main heading is 'Relationship Tags'. Below it, a message states: 'Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket. This enables you to search for the transferred files by using the tag values.' There are two radio buttons: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below these are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left is a button '+ Add Relationship Tag' and at the bottom right is the text 'Optional Field | [Up to 5]'.



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せん。

11. 同期関係の詳細を確認し、\* 関係の作成 \* をクリックします。

。結果 \*

クラウドの同期は、ソースとターゲットの間でデータの同期を開始します。

### Cloud Data Sense から同期関係を作成

Cloud Sync はクラウドデータセンスと統合されています。データセンス内から、Cloud Sync を使用してターゲットの場所と同期するソースファイルを選択できます。

Cloud Data Sense からデータ同期を開始すると、すべてのソース情報が 1 つの手順で表示されるため、重要な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。

"Cloud Data Sense から同期関係を開始する方法について説明します"。

## SMB 共有から ACL をコピーする

Cloud Sync は、ソース SMB 共有とターゲット SMB 共有の間、またはソース SMB 共有からオブジェクトストレージ（ONTAP S3 を除く）へ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。



Cloud Sync では、オブジェクトストレージから SMB 共有への ACL のコピーはサポートされていません。

### 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
- SMB 共有間で ACL を手動でコピーします

## Cloud Sync を設定して SMB サーバから ACL をコピーする

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 サーバから ACL をコピーします。

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. Cloud Sync で、\* 新しい同期を作成 \* をクリックします。
2. ソースに \* SMB サーバー \* をドラッグアンドドロップし、ターゲットとして SMB サーバーまたはオブジェクトストレージを選択して、\* 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。

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、またはソースの SMB 共有からオブジェクトストレージへの ACL を保持します。

### SMB 共有間での 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

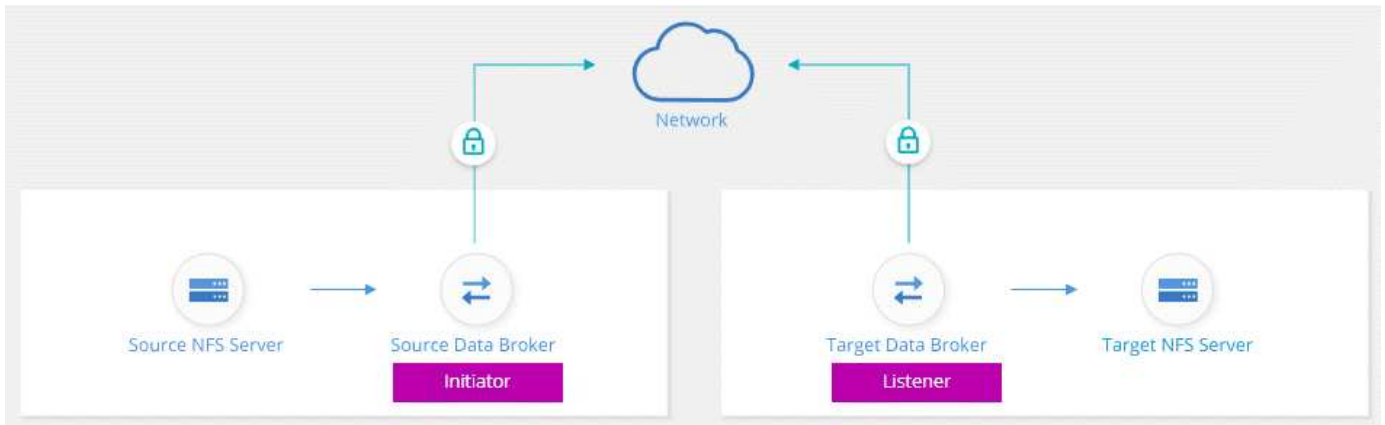
### 転送中のデータ暗号化を使用した NFS データの同期

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、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。
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・リスナーがどのデータ・ブローカ・リスナーを実行するか' 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 \* : 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。

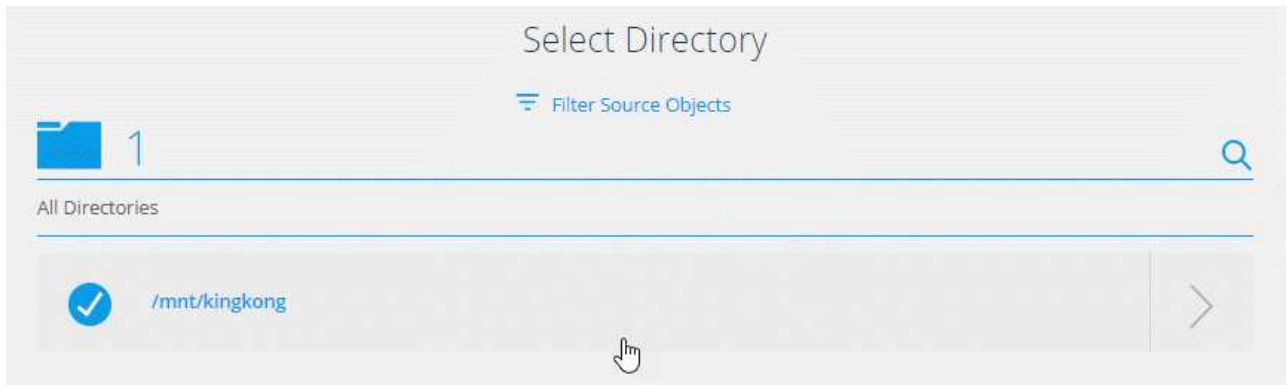
次の点に注意してください。

- 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、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。

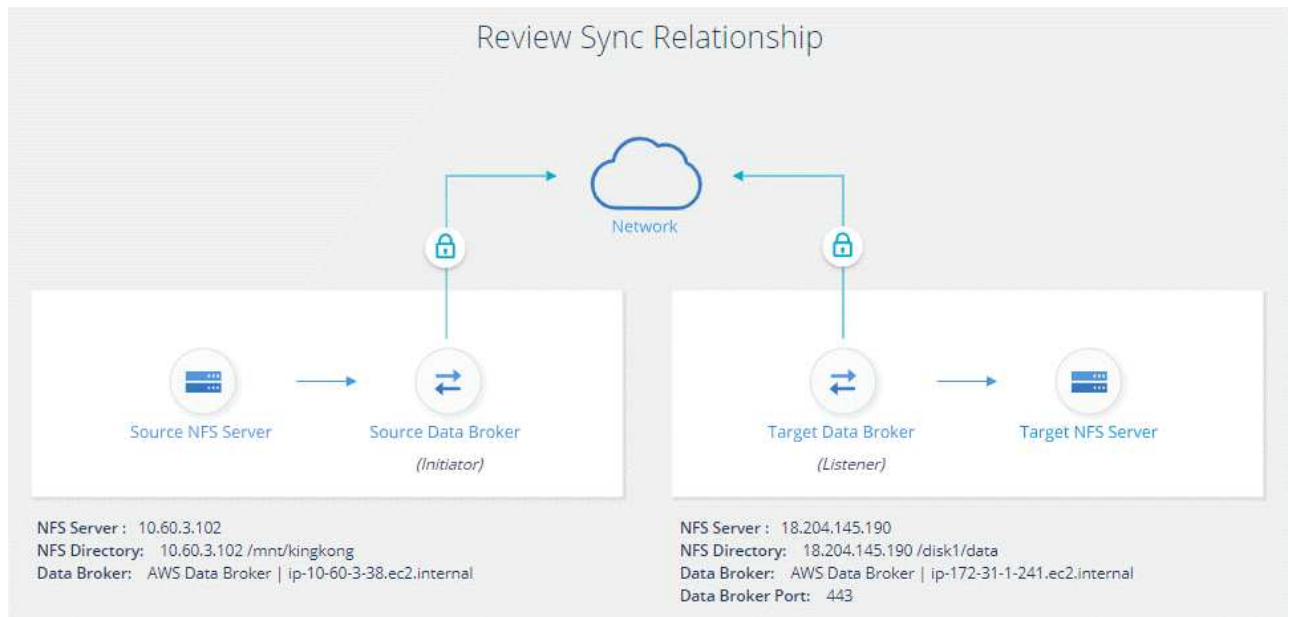
ターゲットデータブローカーがリスナーとして機能する場合は、新しいデータブローカーである必要があります。

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。

## 外部の橋本社ボ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 のクレデンシャルが必要な同期関係を作成する場合は、Cloud Sync のユーザー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、外部の橋本社ボ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、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。

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。ボルトのシークレットの URL は、`creds_` で終わる必要があります。

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。

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）

## Secretid&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。

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、"[このページのこのドキュメント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": "5e6e111d578dtuu1555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

## 無料トライアルの終了後に同期関係の料金を支払う

14 日間の無料トライアル終了後に、同期関係の料金を支払う方法は 2 通りあります。最初のオプションは、AWS または Azure から従量課金制または年払いのいずれかを購読することです。2 つ目の選択肢は、ネットアップから直接ライセンスを購入することです。

AWS Marketplace または Azure Marketplace からサブスクライブできます。両方から購読することはできません。

Marketplace サブスクリプションを使用して、ネットアップからライセンスを使用することもできます。たとえば、25 の同期関係がある場合は、ライセンスを使用して最初の 20 の同期関係に料金を支払い、残りの 5 つの同期関係を持つ AWS または Azure から従量課金制で支払うことができます。

"ライセンスの仕組みについては、こちらをご覧ください。"。

無料トライアルの終了後すぐに支払いをしない場合はどうすればよいですか？

追加の関係を作成することはできません。既存の関係は削除されませんが、ライセンスを登録または入力するまでは変更を加えることはできません。

## AWS からの登録

AWS を使用すると、従量課金制または年払いが可能です。

従量課金制の手順

1. [ 同期 ]、[ ライセンス ] の順にクリックします。
2. 「 \* AWS \* 」を選択します
3. [ **Subscribe** ] をクリックし、[ \* Continue \* ] をクリックします。
4. AWS Marketplace から登録し、Cloud Sync サービスに再度ログインして登録を完了します。

次のビデオは、プロセスを示しています。

▶ [https://docs.netapp.com/ja-jp/cloud-manager-sync//media/video\\_cloud\\_sync\\_registering.mp4](https://docs.netapp.com/ja-jp/cloud-manager-sync//media/video_cloud_sync_registering.mp4) (video)

年間の支払い手順

1. "AWS Marketplace ページに移動します。"。
2. [ \* 購読の続行 \* ] をクリックします。
3. 契約オプションを選択し、 \* 契約の作成 \* をクリックします。

## Azure からのサブスクリプション

Azure では、従量課金制または年間の支払いが可能です。

関連するサブスクリプションの投稿者または所有者権限を持つ Azure ユーザーアカウント。

手順

1. [ 同期 ]、[ ライセンス ] の順にクリックします。
2. 「 \* Azure \* 」を選択します。
3. [ **Subscribe** ] をクリックし、[ \* Continue \* ] をクリックします。
4. Azure ポータルで、 \* 作成 \* をクリックし、オプションを選択して \* サブスクライブ \* をクリックします。

「毎月 \* 」を選択すると、時間単位で支払います。または、「毎年」を選択すると、前払いした 1 年分の料金が支払われます。

5. 展開が完了したら、通知ポップアップで SaaS リソースの名前をクリックします。
6. 「アカウントの設定」をクリックして Cloud Sync に戻ります。

次のビデオは、プロセスを示しています。

▶ [https://docs.netapp.com/ja-jp/cloud-manager-sync//media/video\\_cloud\\_sync\\_registering\\_azure.mp4](https://docs.netapp.com/ja-jp/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4)

(video)

## ネットアップからライセンスを購入し、 **Cloud Sync** に追加する

同期関係の料金を事前に支払うには、1 つ以上のライセンスを購入して Cloud Sync サービスに追加する必要があります。

ライセンスのシリアル番号、およびライセンスが関連付けられているネットアップサポートサイトのアカウントのユーザ名とパスワードが必要です。

### 手順

1. mailto : [ng-cloudsync-contact@netapp.com](mailto:ng-cloudsync-contact@netapp.com) ? subject= Cloud %20Sync%20Service%20-%20BYOL %20License%20Purchase%20Request までにライセンスを購入してください。 [Contacting NetApp] 。
2. Cloud Manager で、 \* Sync > Licensing \* をクリックします。
3. [ ライセンスの追加 ] をクリックして、必要な情報を追加します。
  - a. シリアル番号を入力します。
  - b. 追加するライセンスに関連付けられているネットアップサポートサイトのアカウントを選択します。
    - Cloud Manager にアカウントがすでに追加されている場合は、ドロップダウンリストから選択します。
    - アカウントがまだ追加されていない場合は、 \*[Add NSS Credentials] をクリックし、ユーザー名とパスワードを入力し、 [\*Register] をクリックして、ドロップダウンリストから選択します。
  - c. [ 追加 (Add) ] をクリックします。

## ライセンスの更新

ネットアップから購入した Cloud Sync ライセンスを延長しても、新しい有効期限は Cloud Sync で自動的に更新されません。有効期限を更新するには、ライセンスを再度追加する必要があります。

### 手順

1. Cloud Manager で、 \* Sync > Licensing \* をクリックします。
2. [ ライセンスの追加 ] をクリックして、必要な情報を追加します。
  - a. シリアル番号を入力します。
  - b. 追加するライセンスに関連付けられているネットアップサポートサイトのアカウントを選択します。
  - c. [ 追加 (Add) ] をクリックします。

Cloud Sync は、既存のライセンスを新しい有効期限で更新します。


## 同期関係の管理

データの即時同期やスケジュールの変更などにより、いつでも同期関係を管理できます。

## データの即時同期を実行しています

スケジュールされた次回の同期を待つのではなく、ボタンを押すと、ソースとターゲットの間でデータをすぐに同期できます。

### 手順

1. ダッシュボード \* で同期関係に移動し、をクリックします 
2. [今すぐ同期] をクリックし、[\* 同期 \*] をクリックして確定します。

Cloud Sync は、関係のデータ同期プロセスを開始します。

## 同期パフォーマンスの高速化

同期関係を管理するグループにデータブローカーを追加することで、同期関係のパフォーマンスを向上できます。追加のデータブローカーには、\_NET\_DATA ブローカーを指定する必要があります。


データブローカーグループが他の同期関係を管理している場合、グループに追加した新しいデータブローカーを使用することで、同期関係のパフォーマンスも向上します。

たとえば、次の 3 つの関係があるとします。

- 関係 1 はデータブローカーグループ A によって管理されます
- 関係 2 はデータブローカーグループ B によって管理されます
- 関係 3 は、データブローカーグループ A によって管理されます

新しいデータブローカーをデータブローカーグループ A に追加するため、関係 1 のパフォーマンスを高速化したいと考えていますグループ A でも同期関係 3 が管理されるため、関係の同期パフォーマンスも自動的に高速化されます。

### 手順

1. 関係にある既存のデータブローカーの少なくとも 1 つがオンラインであることを確認します。
2. ダッシュボード \* で同期関係に移動し、をクリックします 
3. [\*Accelerate] をクリックします。
4. プロンプトに従って、新しいデータブローカーを作成します。

Cloud Sync が新しいデータブローカーをグループに追加次のデータ同期のパフォーマンスを高速化する必要があります。

## クレデンシャルを更新し

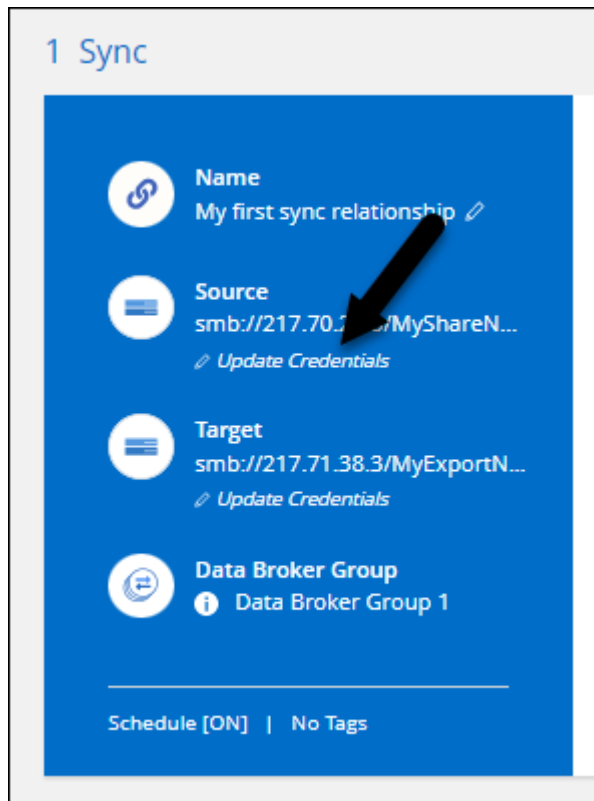
データブローカーを、既存の同期関係にあるソースまたはターゲットの最新のクレデンシャルで更新できます。クレデンシャルの更新は、セキュリティポリシーで定期的にクレデンシャルの更新が要求される場合に役立ちます。

クレデンシャルの更新は、Cloud Sync で Azure Blob サーバ、Box サーバ、IBM Cloud Object Storage、StorageGRID、ONTAP S3 ストレージ、SFTP サーバ、SMB サーバのクレデンシャルが必要なすべてのソースまたはターゲットでサポートされています。



## 手順

1. \* 同期ダッシュボード \* で、資格情報が必要な同期関係に移動し、\* 資格情報の更新 \* をクリックします。



ページの [ 資格情報の更新 ] オプションを示すスクリーンショット。"]

2. クレデンシャルを入力し、\* Update \* をクリックします。

SMB サーバに関する注意：新しいドメインの場合は、クレデンシャルを更新するときにドメインを指定する必要があります。ドメインが変更されていない場合は、再度入力する必要はありません。

同期関係の作成時にドメインを入力したが、クレデンシャルの更新時に新しいドメインを入力しなかった場合、Cloud Sync は指定した元のドメインを使用し続けます。

Cloud Sync でデータブローカーのクレデンシャルが更新されます。データブローカーがデータ同期用に更新されたクレデンシャルを使用して起動するまで、10 分程度かかる場合があります。

## 同期関係の設定を変更する

ソースファイルとフォルダの同期方法とターゲットの場所での保持方法を定義する設定を変更します。

1. ダッシュボード \* で同期関係に移動し、をクリックします ⓘ
2. [\* 設定 \*] をクリックします。
3. 設定を変更します。

General

Schedule	ON   Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼

Files and Directories

Compare By	The following attributes (and size): uid, gid, mode, mtime	▼
Recently Modified Files	Exclude files that are modified up to 30 Seconds before a scheduled sync	▼
Delete Files On Source	Never delete files from the source location	▼
Delete Files On Target	Never delete files from the target location	▼
File Types	Include All: Files, Directories, Symbolic Links	▼
Exclude File Extensions	None	▼
File Size	All	▼
Date Modified	All	▼
Date Created	All	▼
ACL - Access Control List	Inactive	▼

Reset to defaults

[ 削除ソース ] 各設定の簡単な説明を次に示します。

## 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

指定した時間数または日数以内に同期が完了しなかった場合に、Cloud Sync がデータの同期をキャンセルするかどうかを定義します。

## 通知

Cloud Managerの通知センターでCloud Sync 通知を受信す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

ファイルをスキップする前に Cloud Sync がファイルの同期を再試行する回数を定義します。

## で比較してください

ファイルまたはディレクトリが変更され、再度同期する必要があるかどうかを判断するときに、Cloud Sync で特定の属性を比較するかどうかを選択します。

これらの属性をオフにしても、Cloud Sync はパス、ファイルサイズ、および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。

Cloud Sync では、次の属性の比較を有効または無効に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

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。

## 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

Cloud Sync 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
    }
  }
}
```

## 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）を定義します。

ファイル拡張子を除外します

ファイル拡張子を入力し、\* Enter \* キーを押して、同期から除外するファイル拡張子を指定します。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/cloud-manager-sync//media/video\\_file\\_extensions.mp4](https://docs.netapp.com/ja-jp/cloud-manager-sync//media/video_file_extensions.mp4) (video)

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、SMB サーバから ACL をコピーします。


4. [ 設定の保存 \* ] をクリックします。

Cloud Sync は、新しい設定との同期関係を変更します。

## 関係の削除

ソースとターゲットの間でデータを同期する必要がなくなった場合は、同期関係を削除できます。このアクションでは、データブローカーグループ（または個々のデータブローカーインスタンス）は削除されず、ターゲットからデータが削除されることもありません。

手順

1. ダッシュボード \* で同期関係に移動し、をクリックします 
2. [ 削除 ] をクリックし、もう一度 [ 削除 ] をクリックして確定します。

Cloud Sync は同期関係を削除します。

## データブローカーグループの管理

データブローカーグループは、ソースの場所からターゲットの場所にデータを同期します。作成する同期関係ごとに、少なくとも 1 つのデータブローカーがグループに必要です。グループに新しいデータブローカーを追加し、グループに関する情報を表示するなどして、データブローカーグループを管理します。

## データブローカーグループの仕組み

データブローカーグループには、1 つ以上のデータブローカーを含めることができます。データブローカーをグループ化すると、同期関係のパフォーマンスを向上させることができます。

グループは複数の関係を管理できます

データブローカーグループは、一度に 1 つ以上の同期関係を管理できます。

たとえば、次の 3 つの関係があるとします。

- 関係 1 はデータブローカーグループ A によって管理されます
- 関係 2 はデータブローカーグループ B によって管理されます
- 関係 3 は、データブローカーグループ A によって管理されます

新しいデータブローカーをデータブローカーグループ A に追加するため、関係 1 のパフォーマンスを高速化したいと考えていますグループ A でも同期関係 3 が管理されるため、関係の同期パフォーマンスも自動的に高速化されます。

### グループ内のデータブローカーの数

多くの場合、1 つのデータブローカーで同期関係のパフォーマンス要件を満たすことができます。そうでない場合は、データブローカーをグループに追加することで、同期パフォーマンスを高速化できます。ただし、まず、同期のパフォーマンスに影響を与える可能性のある他の要因を確認する必要があります。"[複数のデータブローカーがいつ行われるかを確認する方法については、こちらをご覧ください](#) は必須です"。

## セキュリティに関する推奨事項

データブローカーマシンのセキュリティを確保するために、次のことを推奨します。

- SSH で X11 転送を許可しないでください
- SSH では、TCP 接続の転送を許可しないでください
- SSH ではトンネルを許可しないでください
- SSH では、クライアント環境変数を受け入れないでください

これらのセキュリティ推奨事項は、データブローカーマシンへの不正な接続を防止するのに役立ちます。

## 新しいデータブローカーをグループに追加

新しいデータブローカーを作成するには、いくつかの方法があります。

- 新しい同期関係を作成する場合

"[作成時に新しいデータブローカーを作成する方法について説明します 同期関係](#)"。

- [ データブローカーの管理 ] ページで、[ 新規追加 ] をクリックします データブローカー \*。新しいストレージにデータブローカーを作成します グループ
- 新しいを作成して、[ データブローカーの管理 ( Manage Data Brokers ) ] ページからアクセスします 既存のグループのデータブローカー

始める前に

- 暗号化された同期関係を管理するグループにデータブローカーを追加することはできません。
- 既存のグループにデータブローカーを作成する場合、データブローカーはオンプレミスのデータブローカーであるか、同じタイプのデータブローカーである必要があります。

たとえば、グループに AWS データブローカーが含まれている場合、そのグループに AWS データブローカーまたはオンプレミスのデータブローカーを作成できます。Azure データブローカーと Google Cloud データブローカーは、同じタイプのデータブローカーではないため、作成できません。

新しいグループにデータブローカーを作成する手順

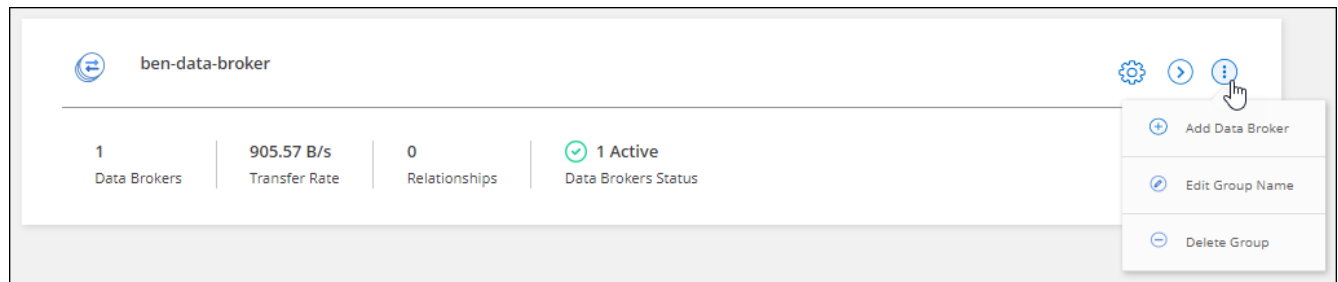
1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. [ 新しいデータブローカーの追加 ] をクリックします。
3. プロンプトに従ってデータブローカーを作成します。

ヘルプについては、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"](#)

既存のグループにデータブローカーを作成する手順

1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. アクションメニューをクリックし、\* データブローカーの追加 \* を選択します。



3. プロンプトに従って、グループにデータブローカーを作成します。

ヘルプについては、次のページを参照してください。

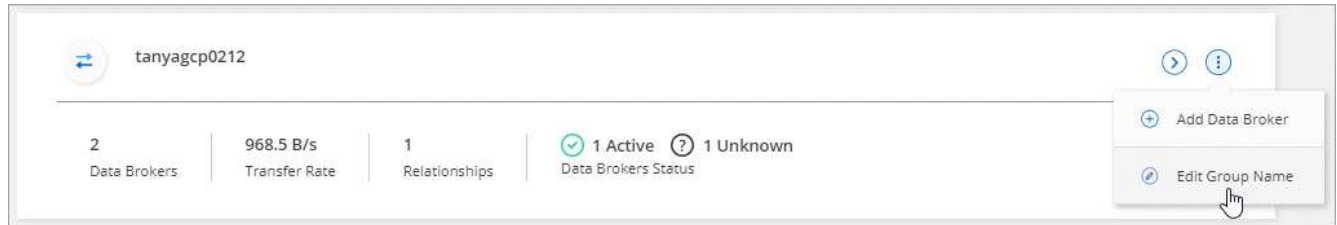
- ["AWS にデータブローカーを作成"](#)
- ["Azure でデータブローカーを作成"](#)
- ["Google Cloud でデータブローカーを作成"](#)
- ["Linux ホストへのデータブローカーのインストール"](#)

## グループの名前を編集します

データブローカーグループの名前は、いつでも変更できます。

手順

1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. アクションメニューをクリックし、\* グループ名の編集 \* を選択します。



3. 新しい名前を入力し、\* 保存 \* をクリックします。

Cloud Sync によってデータブローカーグループの名前が更新されます。

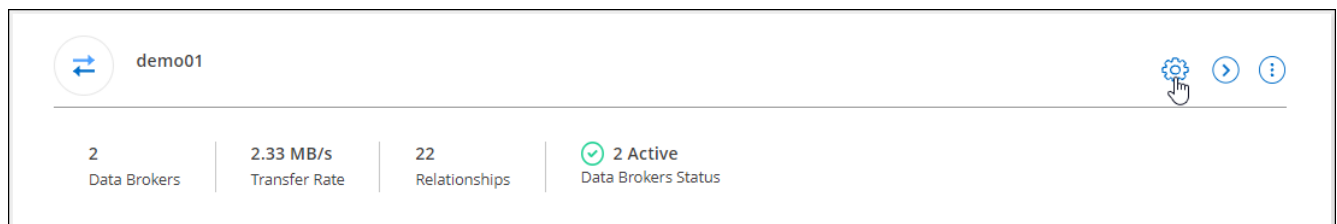
## ユニファイド構成をセットアップする

同期プロセス中に同期関係でエラーが発生した場合は、データブローカーグループの同時実行を統合すると、同期エラーの数を減らすことができます。グループの設定を変更すると、転送速度が遅くなるため、パフォーマンスに影響する可能性があります。

自分で設定を変更することはお勧めしません。設定を変更するタイミングと変更方法については、ネットアップに相談してください。

手順

1. [ \* データブローカーの管理 \* ] をクリックします。
2. データブローカーグループの [ 設定 ] アイコンをクリックします。



3. 必要に応じて設定を変更し、\* Unify Configuration\* をクリックします。

次の点に注意してください。

- 変更する設定を選択できます。4 つすべてを一度に変更する必要はありません。
- 新しい構成がデータブローカーに送信されると、データブローカーは自動的に再起動し、新しい構成を使用します。
- 変更が反映されて Cloud Sync インターフェイスに表示されるまで、1 分程度かかる場合があります。

- データブローカーが実行されていないと、Cloud Sync がデータブローカーと通信できないため、設定が変更されません。データブローカーが再起動すると設定が変更されます。
- ユニファイド構成を設定すると、新しいデータブローカーでは自動的に新しい構成が使用されます。

## データブローカーをグループ間で移動


ターゲットのデータブローカーグループのパフォーマンスを高速化する必要がある場合は、データブローカーをあるグループから別のグループに移動します。

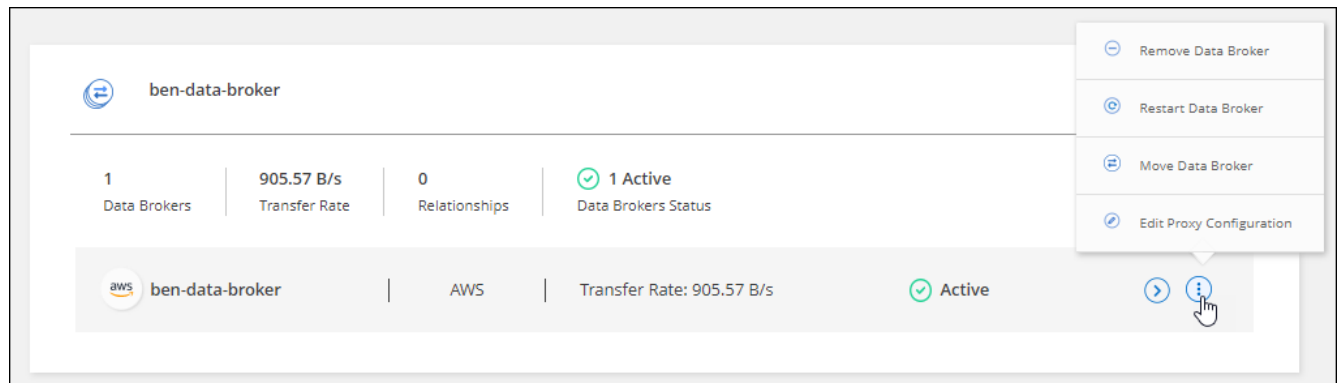
たとえば、データブローカーで同期関係が管理されなくなった場合、同期関係を管理している別のグループに簡単に移動できます。

### 制限

- データブローカーグループが同期関係を管理していて、グループにデータブローカーが 1 つしかない場合、そのデータブローカーを別のグループに移動することはできません。
- 暗号化された同期関係を管理するグループとの間でデータブローカーを移動することはできません。
- 現在導入中のデータブローカーは移動できません。

### 手順

1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. をクリックします  をクリックして、グループ内のデータブローカーのリストを展開します。
3. データブローカーのアクションメニューをクリックし、\* データブローカーの移動 \* を選択します。



4. 新しいデータブローカーグループを作成するか、既存のデータブローカーグループを選択してください。
5. [ 移動 ( Move ) ] をクリックします。


Cloud Sync は、データブローカーを新規または既存のデータブローカーグループに移動します。前のグループに他のデータブローカーが存在しない場合、Cloud Sync はそのデータブローカーを削除します。

## プロキシ設定を更新します

データブローカーのプロキシ設定を更新するには、新しいプロキシ設定に関する詳細を追加するか、既存のプロキシ設定を編集します。

### 手順



1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. をクリックします  をクリックして、グループ内のデータブローカーのリストを展開します。
3. データブローカーのアクションメニューをクリックし、 \* プロキシ構成の編集 \* を選択します。
4. プロキシに関する詳細を指定します。ホスト名、ポート番号、ユーザ名、パスワードです。
5. [ 更新 ( Update ) ] をクリックします。

Cloud Sync は、インターネットアクセスにプロキシ設定を使用するようにデータブローカーを更新します。

## データブローカーの構成を表示します

データブローカーの詳細を確認することで、ホスト名、IP アドレス、使用可能な CPU や RAM など特定することができます。



Cloud Sync では、データブローカーに関する以下の詳細が提供されています。

- 基本情報：インスタンス ID、ホスト名など
- ネットワーク：リージョン、ネットワーク、サブネット、プライベート IP など
- ソフトウェア：Linux ディストリビューション、データブローカーのバージョンなど
- ハードウェア：CPU と RAM
- 設定：データブローカーの 2 種類の主なプロセスの詳細（スキャナと転送元）



スキャナはソースとターゲットをスキャンし、コピーする対象を決定します。転送元は実際のコピーを行います。ネットアップの担当者は、これらの構成の詳細を使用して、パフォーマンスを最適化するための推奨アクションを提示することが

### 手順

1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. をクリックします  をクリックして、グループ内のデータブローカーのリストを展開します。
3. をクリックします  をクリックしてください。

Category	Item	Value
Information	Broker ID	5fc766b3d3e3664b9e116...
	Instance ID	288871247573080556
	Host Name	tanyagcp0212-mnx-data...
	Project Id	cloudsync-dev-214020
Network	Region	us-east1-b
	Subnet	255.255.240.0
Software	Linux Distribution & Version	linux
	Data Broker Version	1.3.0.18650-73f960d-integ
Hardware	Available CPUs	4
	Available RAM	62.22 MB
Configuration	Scanner Concurrency	50
	Transferrer CPUs	4

## データブローカーの問題に対処

Cloud Sync では、問題のトラブルシューティングに役立つ各データブローカーのステータスが表示されます。

### 手順

1. ステータスが「Unknown」または「Failed」のデータブローカーを特定します。

Broker Name	Environment	Transfer Rate	Status
tanyagcp0212	GCP	968.5 B/s	Active
tanya1	ONPREM	N/A	Unknown

2. の上にカーソルを置きます アイコンをクリックして失敗の理由を確認してください。
3. 問題を修正します。

たとえば、オフラインのデータブローカーを再起動するだけで、初期導入に失敗した場合はデータブローカーの削除が必要になることがあります。


## データブローカーをグループから削除

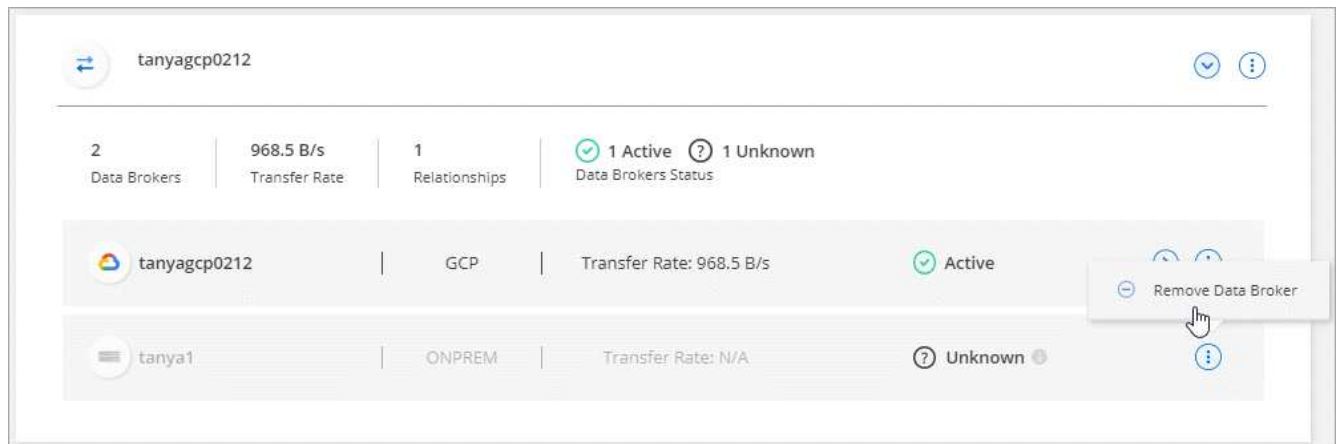
データブローカーが不要になった場合や初期導入に失敗した場合は、グループから削除することができます。この操作では、データブローカーが Cloud Sync のレコードから削除されます。データブローカーとその他のクラウドリソースについては、手動で削除する必要があります。

### 知っておくべきこと

- ・グループから最後のデータブローカーを削除すると、Cloud Sync によってグループが削除されます。
- ・グループを使用している関係がある場合、そのグループから最後のデータブローカーを削除することはできません。

### 手順

1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. をクリックします  をクリックして、グループ内のデータブローカーのリストを展開します。
3. データブローカーのアクションメニューをクリックし、\* データブローカーの削除 \* を選択します。



4. [ データブローカーの削除 ] をクリックします。

Cloud Sync がデータブローカーをグループから削除

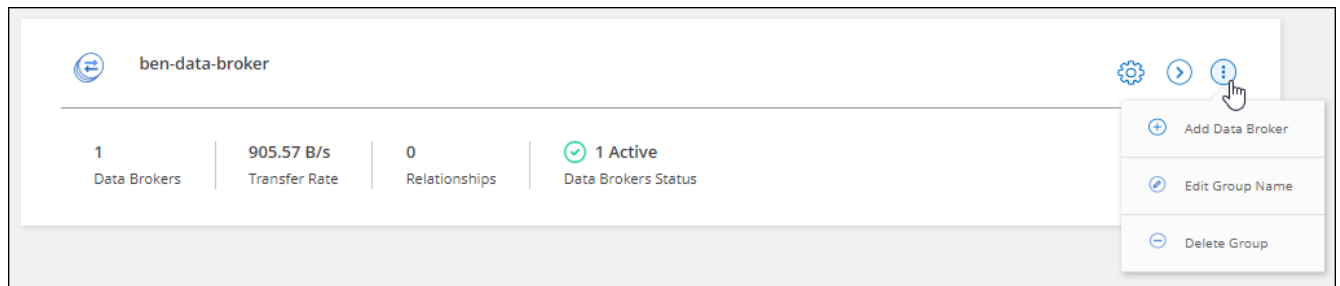
## データブローカーグループを削除

同期関係がデータブローカーグループで管理されなくなった場合は、グループを削除することで、すべてのデータブローカーを Cloud Sync から削除できます。

Cloud Sync によって削除されるデータブローカーは、Cloud Sync のレコードからのみ削除されます。クラウドプロバイダからデータブローカーインスタンスを手動で削除し、追加のクラウドリソースを削除する必要があります。

### 手順

1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. アクションメニューをクリックし、\* グループの削除 \* を選択します。



3. 確認するには、グループの名前を入力し、\* グループの削除 \* をクリックします。

Cloud Sync によってデータブローカーが削除され、グループが削除されます。

## レポートを作成および表示して、設定を調整します

レポートを作成して表示すると、ネットアップの担当者が支援する情報を入手して、データブローカーの設定を調整し、パフォーマンスを向上させることができます。

各レポートには、同期関係にあるパスに関する詳細情報が表示されます。たとえば、ファイルシステムのレポートには、ディレクトリとファイルの数、ファイルサイズの分布、ディレクトリの深さと幅などが表示されます。

### レポートの作成

レポートを作成するたびに、Cloud Sync はパスをスキャンし、レポートに詳細をコンパイルします。

#### 手順

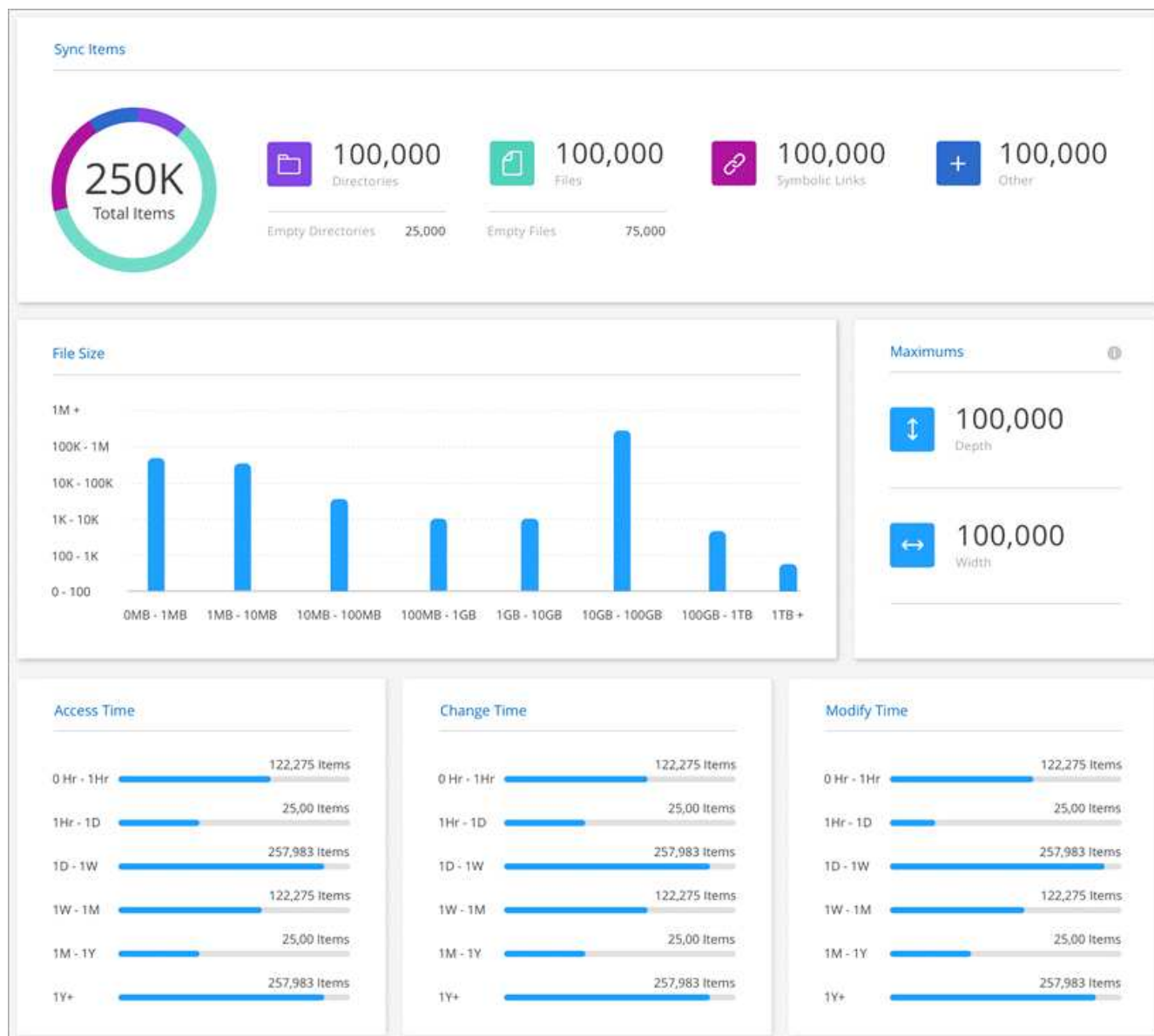
1. [\* 同期 > レポート \*] をクリックします。

同期関係のそれぞれのパス（ソースまたはターゲット）が表形式で表示されます。

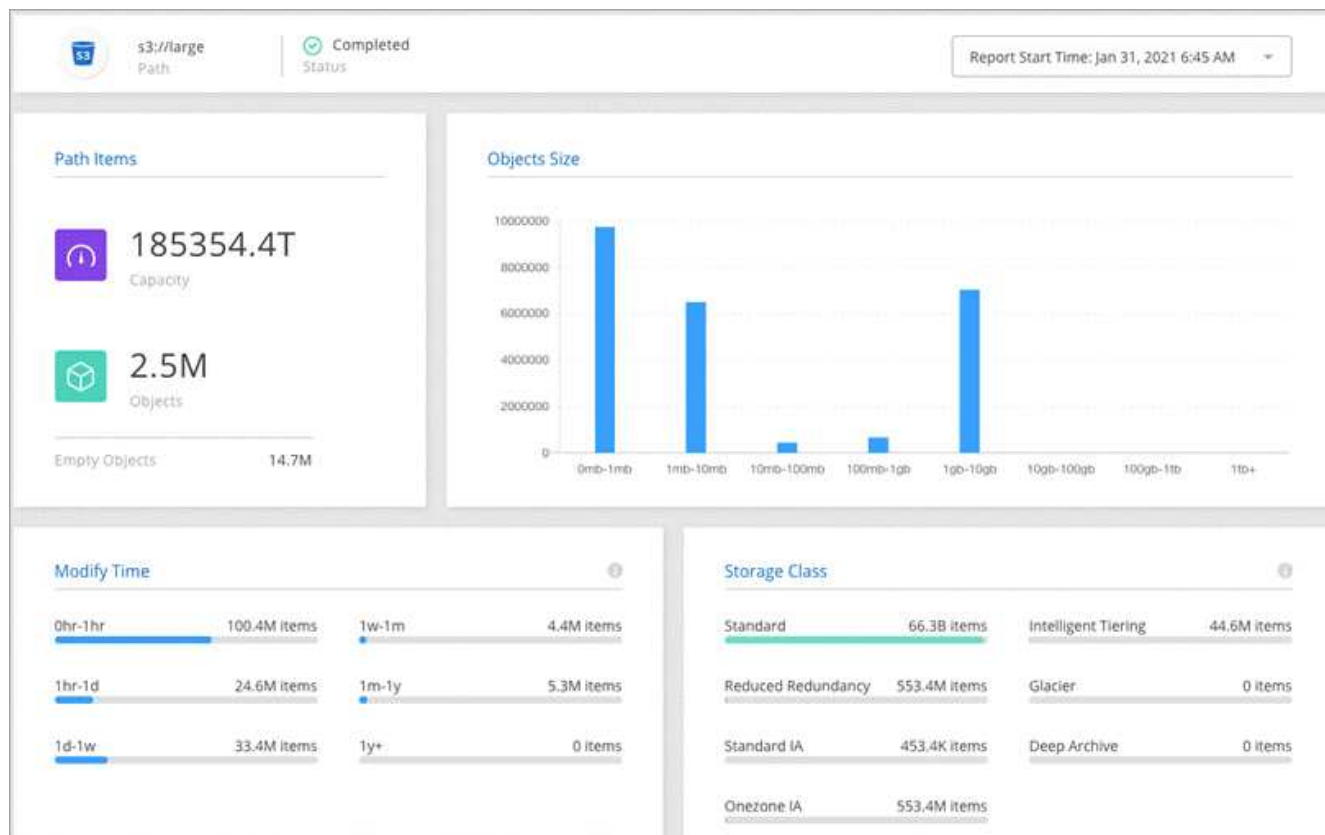
2. [\* レポートアクション \* (\* Reports Actions \*)] 列で、特定のパスに移動して [\* 作成 \* (\* Create \*)] をクリックするか、アクションメニューをクリックして [\* 新規作成 \* (\* Create New \*)] を選択します。

3. レポートの準備ができたら、アクションメニューをクリックし、\* 表示 \* を選択します。

ファイルシステムパスのサンプルレポートを次に示します。



次に、オブジェクトストレージに関するレポートの例を示します。

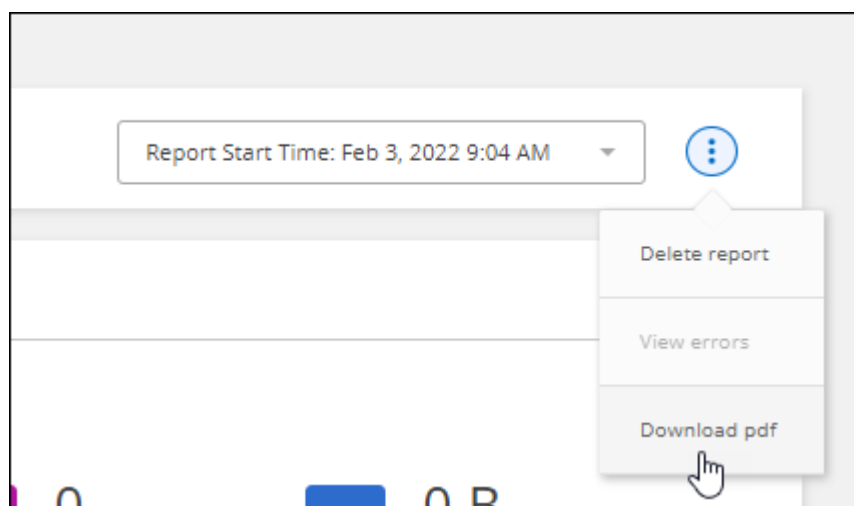


## レポートのダウンロード

レポートを PDF 形式でダウンロードして、オフラインで表示したり共有したりできます。

### 手順

1. [\* 同期 > レポート \*] をクリックします。
2. [\* レポートアクション \* (\* Reports Actions \*)] 列で、アクションメニューをクリックし、[\* 表示 \* (\* View \*)] を選択します。
3. レポートの右上にあるアクションメニューをクリックし、\* PDF のダウンロード \* を選択します。



## レポートエラーの表示

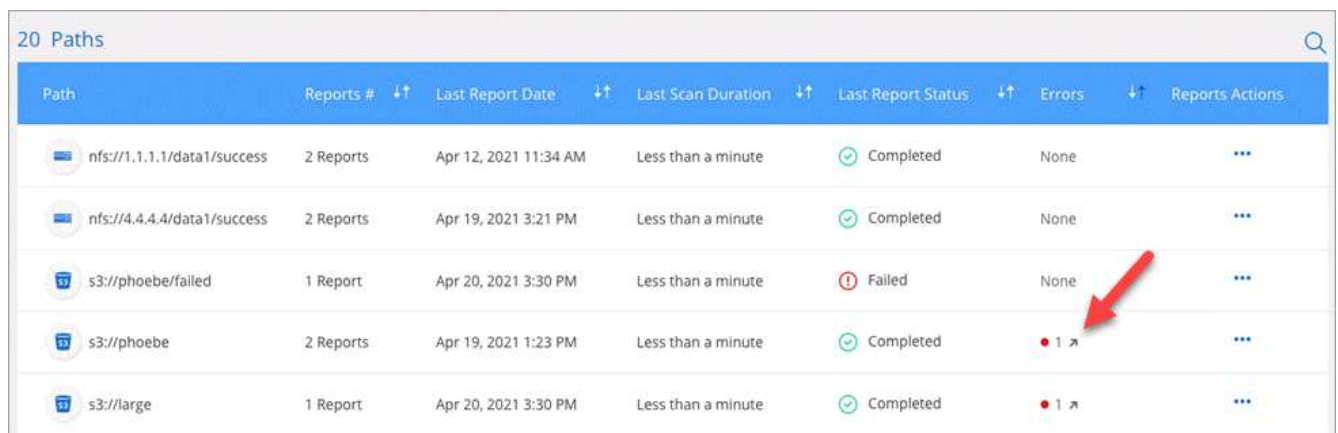
Paths テーブルは、最新のレポートにエラーがあるかどうかを示します。エラーは、Cloud Sync がパスのスキャン時に直面した問題を示します。

たとえば、レポートに権限拒否エラーが含まれている場合があります。このようなエラーは、Cloud Sync が一連のファイルおよびディレクトリ全体をスキャンする機能に影響を及ぼす可能性があります。

エラーのリストを確認したら、問題に対処してからレポートを再実行できます。

### 手順

1. [ \* 同期 > レポート \* ] をクリックします。
2. [ エラー \* ] 列で、レポートにエラーがあるかどうかを確認します。
3. エラーがある場合は、エラーの数の横にある矢印をクリックします。



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

テーブルのスクリーンショット。[Errors] 列にはクリック可能な小さな矢印が表示されています。"]

4. エラーの情報を使用して、問題を修正します。

問題を解決すると、次回レポートを実行したときにエラーが表示されなくなります。

## レポートの削除

修正したエラーが含まれているレポートや、削除した同期関係に関連するレポートを削除することができます。

### 手順

1. [ \* 同期 > レポート \* ] をクリックします。
2. [ \* レポートアクション \* ( \* Reports Actions \* ) ] 列で、パスのアクションメニューをクリックし、[ \* 最後のレポートを削除 ( \* Delete last report ) ] または [ \* すべてのレポートを削除 ( \* Delete all reports ) ] を選択します。
3. レポートを削除することを確認します。

## データブローカーのアンインストール

必要に応じて、アンインストールスクリプトを実行して、データブローカー、およびデ

ータブローカーのインストール時に作成されたパッケージとディレクトリを削除します。

#### 手順

1. データブローカーホストにログインします。
2. データ・ブローカー・ディレクトリ（ /opt/NetApp/databroker' ）に変更します
3. 次のコマンドを実行します。

```
chmod +x アンインストーラ - databroker.sh` ./uninstaller - databroker.sh`
```

4. 「 y 」 を押してアンインストールを確定します。



## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.