



# Cloud Sync のドキュメント

## Cloud Sync

NetApp  
June 21, 2022

# 目次

Cloud Sync のドキュメント	1
リリースノート	2
Cloud Sync の新機能	2
制限	13
はじめに	15
Cloud Sync の概要	15
Cloud Sync のクイックスタート	17
サポートされている同期関係	18
ソースとターゲットを準備します	26
Cloud Sync のネットワークの概要	32
データブローカーをインストール	36
Cloud Sync を使用します	52
ソースとターゲットの間でデータを同期します	52
無料トライアルの終了後に同期関係の料金を支払う	71
同期関係の管理	73
データブローカーグループの管理	78
レポートを作成および表示して、設定を調整します	86
データブローカーのアンインストール	89
クラウド同期 API	91
はじめに	91
API リファレンス	92
List API の使用	92
概念	95
ライセンスの概要	95
データのプライバシー	96
Cloud Sync テクニカル FAQ	96
知識とサポート	104
サポートに登録します	104
ヘルプを表示します	105
法的通知	107
著作権	107
商標	107
特許	107
プライバシーポリシー	107
オープンソース	107

# Cloud Sync のドキュメント

# リリースノート

## Cloud Sync の新機能

Cloud Sync の新機能をご確認ください。

**2022年6月6日**

### 継続的な同期

新しい設定を使用すると、ソースのS3バケットからターゲットに変更を継続的に同期できます。

初期データ同期が完了すると、Cloud Sync はソースS3バケットで変更をリスンし、ターゲットへの変更が発生した場合はその変更を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、S3バケットからS3、Google Cloud Storage、Azure BLOBストレージ、StorageGRID、またはIBMストレージに同期する場合にのみ使用できます。

データブローカーに関連付けられているIAMロールでは、この設定を使用するために次の権限が必要です。

```
"s3:GetBucketNotification",  
"s3:PutBucketNotification"
```

これらの権限は、新しく作成したすべてのデータブローカーに自動的に追加されます。

["Continuous Syncの詳細については、こちらをご覧ください"](#)。

### すべてのONTAP ボリュームを表示します

同期関係を作成するときに、ソースCloud Volumes ONTAP システム、オンプレミスONTAP クラスタ、またはCloud Sync ONTAP ファイルシステムのFSXにすべてのボリュームが表示されるようになりました。

以前は、Cloud Sync では、選択したプロトコルに一致するボリュームのみが表示されていました。すべてのボリュームが表示されますが、選択したプロトコルに一致しないボリュームや、共有やエクスポートがないボリュームはグレー表示され、選択できません。

### Azure Blobへのタグのコピー

Azure Blobがターゲットである同期関係を作成する際に、Cloud Sync でタグをAzure BLOBコンテナにコピーできるようになりました。

- [設定 (\* Settings ) ] ページでは、[ \* オブジェクトのコピー (\* Copy for Objects \*) ] 設定を使用して、ソースからAzure BLOBコンテナにタグをコピーできます。これは、メタデータのコピーに加えて機能します。
- \* Tags/Metadata\* ページで、Azure BLOBコンテナにコピーされるオブジェクトに設定するBLOBインデックスタグを指定できます。以前は、関係のメタデータしか指定できませんでした。

これらのオプションは、Azure Blobがターゲットで、ソースがAzure BlobエンドポイントまたはS3互換エンドポイント (S3、StorageGRID、IBM Cloud Object Storage) の場合にサポートされます。

2022年5月1日

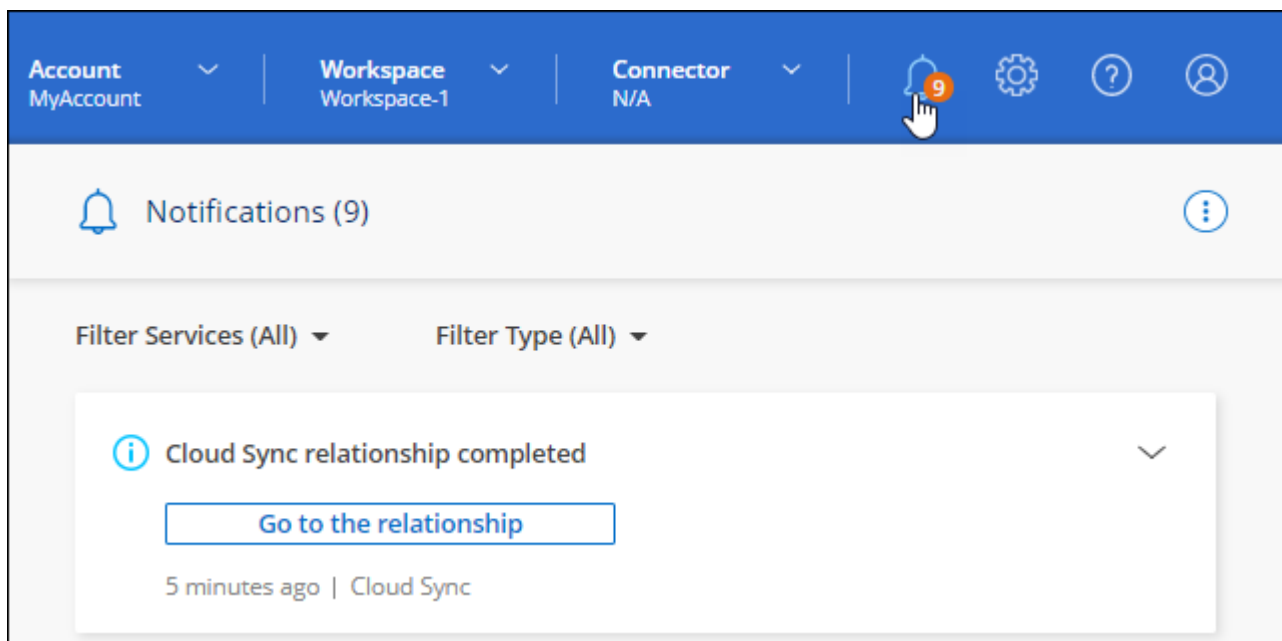
## 同期タイムアウト

新しい\* Sync Timeout \*設定を同期関係に使用できるようになりました。この設定を使用すると、指定した時間数または日数内に同期が完了していない場合にCloud Sync でデータの同期をキャンセルするかどうかを定義できます。

["同期関係の設定の変更の詳細については、こちらをご覧ください"](#)。

## 通知

新しい\* Notifications \*設定を同期関係に使用できるようになりました。この設定を使用すると、Cloud Sync 通知をCloud Managerの通知センターで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。



["同期関係の設定の変更の詳細については、こちらをご覧ください"](#)。

2022 年 4 月 3 日

## データブローカーグループの機能拡張

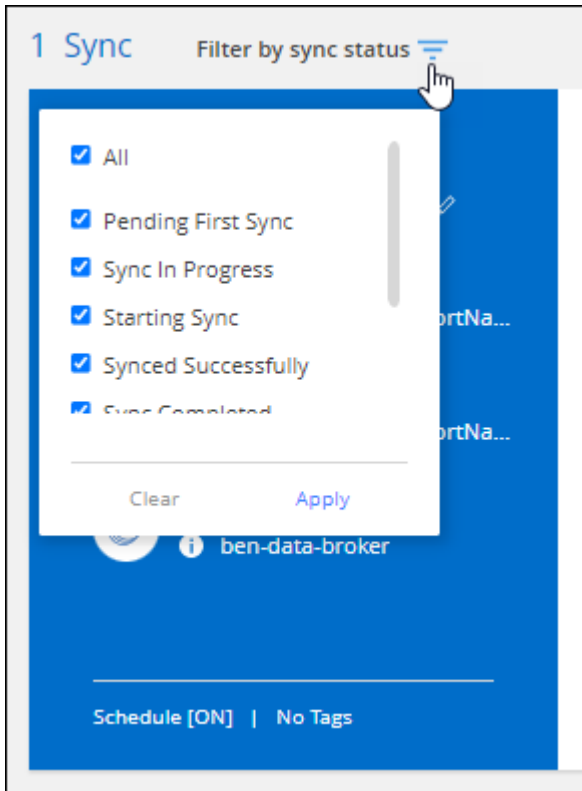
データブローカーグループには、次のような機能拡張が行われました。

- データブローカーを新規または既存のグループに移動できるようになりました。
- データブローカーのプロキシ設定を更新できるようになりました。
- 最後に、データブローカーグループを削除することもできます。

["データブローカーグループの管理方法について説明します"](#)。

## ダッシュボードフィルタ

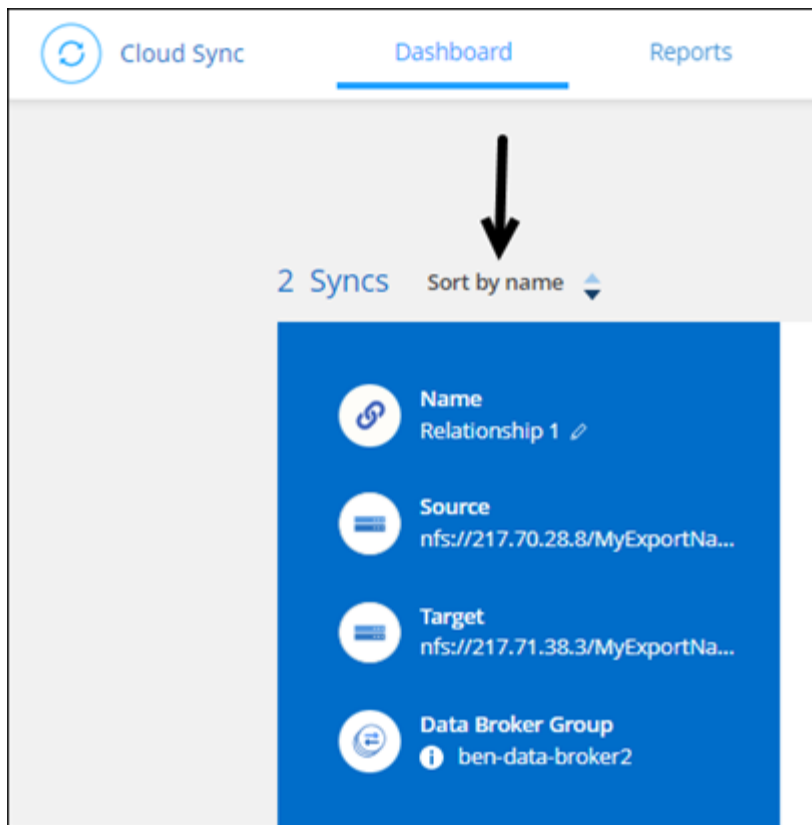
Sync Dashboard の内容をフィルタリングして、特定のステータスに一致する同期関係を簡単に見つけることができるようになりました。たとえば、ステータスが「失敗」の同期関係をフィルタリングできます



**2022 年 3 月 3 日**

ダッシュボードでソートします

ダッシュボードを同期関係名でソートできるようになりました。



オプションを示すスクリーンショット。"]

## データセンスの統合の強化

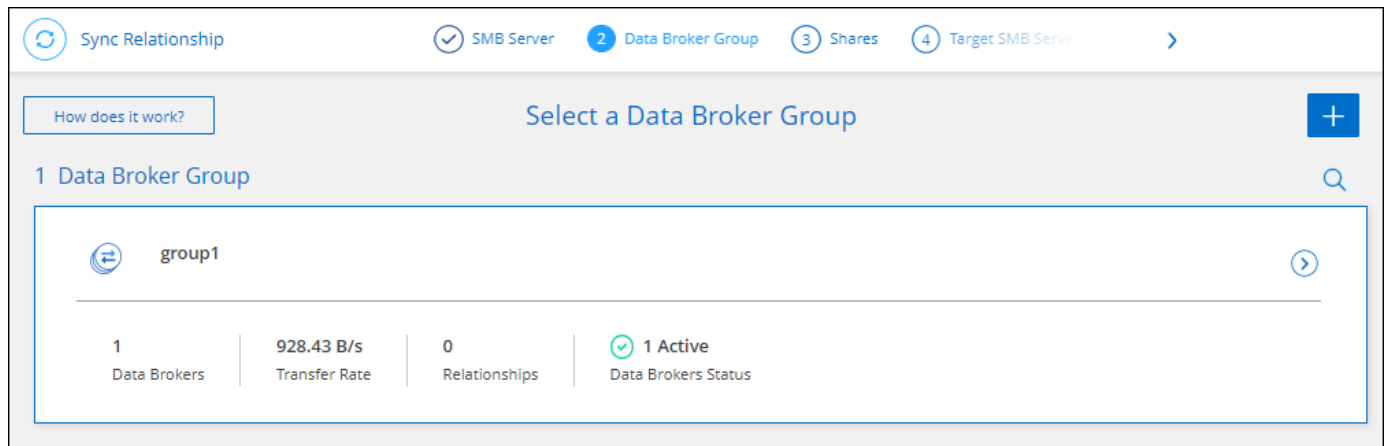
以前のリリースでは、Cloud Sync とクラウドデータセンスの統合を導入しました。この更新プログラムでは、同期関係を簡単に作成できるように統合を強化しました。Cloud Data Sense からデータ同期を開始すると、すべてのソース情報が 1 つの手順で表示されるため、重要な情報をいくつか入力するだけで済みます。

**2022 年 2 月 6 日**

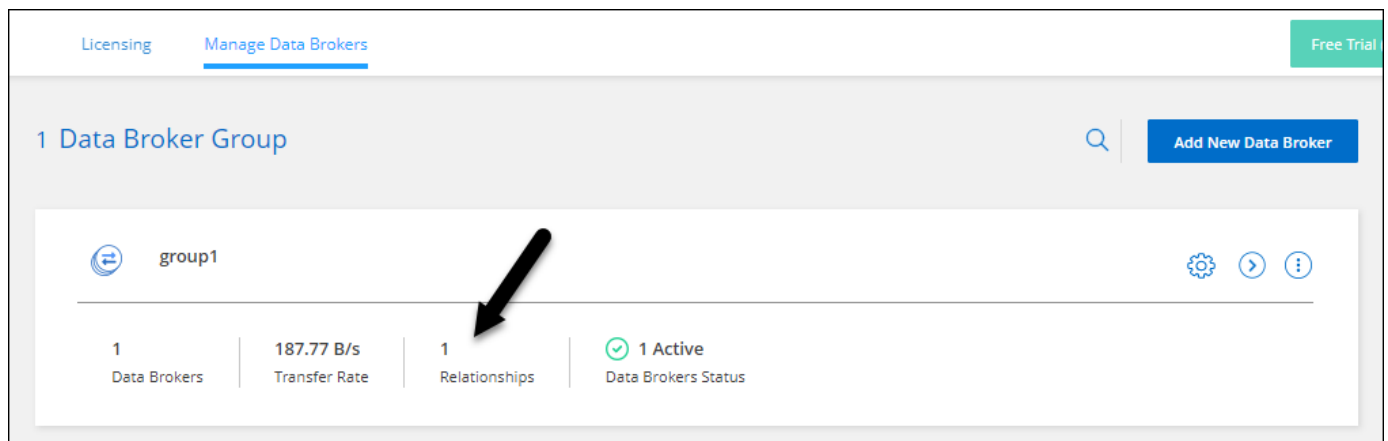
## データブローカーグループの機能拡張

データブローカーの操作方法は、dataBroker\_groups\_を 強調するように変更されました。

たとえば、新しい同期関係を作成する場合は、特定のデータブローカーではなく、データブローカーの \_GROP\_To がその関係で使用するよう選択します。



[データブローカーの管理 \*] タブには、データブローカーグループが管理している同期関係の数も表示されます。



**PDF** レポートをダウンロードできます

レポートの PDF をダウンロードできるようになりました。

"レポートの詳細については、[こちらをご覧ください](#)。"

**2022 年 1 月 2 日**

新しい **Box** 同期関係

2 つの新しい同期関係がサポートされています。

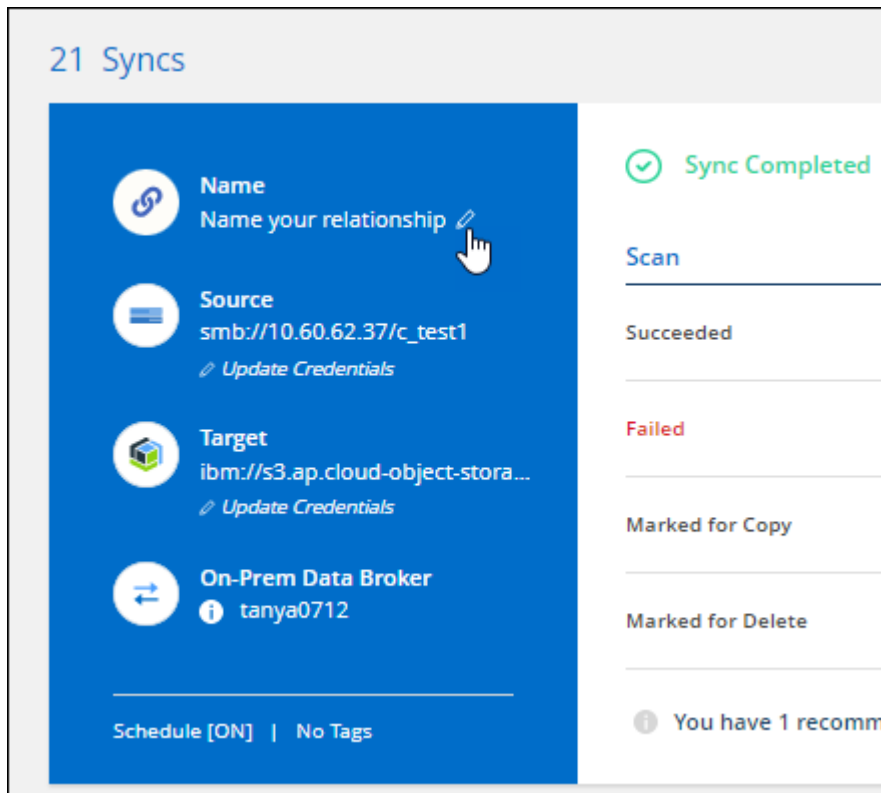
- Box to Azure NetApp Files の略
- Box から Amazon FSX for ONTAP に移動します

"サポートされている同期関係のリストを表示します"。



## 関係名

同期関係ごとにわかりやすい名前を指定できるようになり、各関係の目的を簡単に特定できるようになりました。この名前は、関係の作成時および作成後にいつでも追加できます。



## S3 プライベートリンク

Amazon S3 との間でデータを同期する際に、S3 プライベートリンクを使用するかどうかを選択できます。データブローカーは、ソースからターゲットにデータをコピーする際、プライベートリンクを経由します。

データブローカーに関連付けられている IAM ロールでは、この機能を使用するために次の権限が必要です。

```
"ec2:DescribeVpcEndpoints"
```

この権限は、作成した新しいデータブローカーに自動的に追加されます。

## Glacier のインスタント検索

Amazon S3 が同期関係のターゲットである場合に、\_Glacier Instant Retrieve\_storage クラスを選択できるようになりました。

## オブジェクトストレージから SMB 共有への ACL

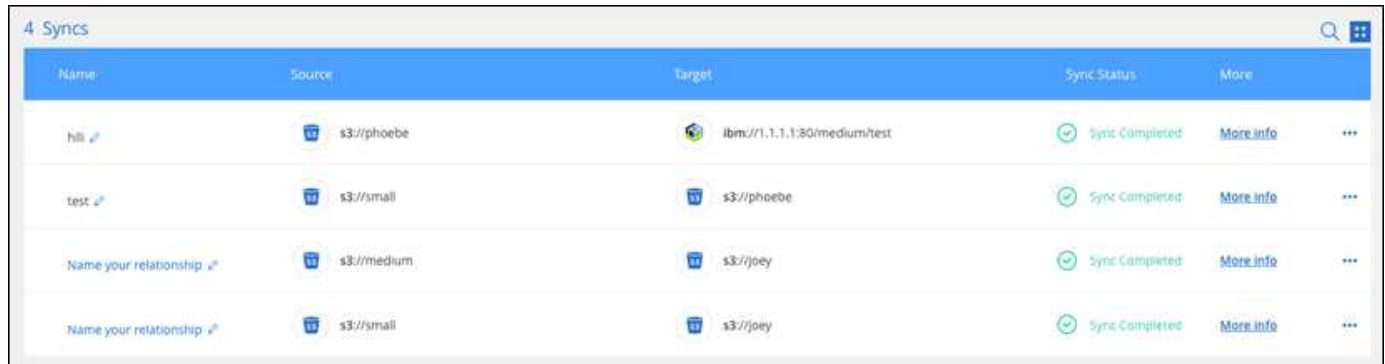
Cloud Sync で、オブジェクトストレージから SMB 共有への ACL のコピーがサポートされるようになりました。これまでは、SMB 共有からオブジェクトストレージへの ACL のコピーのみがサポートされていました。

## S3 への SFTP を使用します

SFTP から Amazon S3 への同期関係の作成がユーザーインターフェイスでサポートされるようになりました。この同期関係は、以前は API でのみサポートされていました。

## テーブルビューの拡張機能

ダッシュボードのテーブルビューを再設計して使いやすくしました。詳細情報 \* をクリックすると、ダッシュボードが Cloud Sync でフィルタされ、その関係に関する詳細情報が表示されます。



Name	Source	Target	Sync Status	More
hll	s3://phoebe	ibm://1.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

## Jarkarta 地域のサポート

Cloud Sync は、AWS アジア太平洋（ジャカルタ）リージョンでのデータブローカーの導入をサポートするようになりました。

**2021 年 11 月 28 日**

## SMB からオブジェクトストレージへの ACL

ソースの SMB 共有からオブジェクトストレージ（ONTAP S3 を除く）への同期関係を設定する際に、Cloud Sync でアクセス制御リスト（ACL）をコピーできるようになりました。

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。

["SMB 共有から ACL をコピーする方法について説明します"](#)。

## ライセンスを更新します

拡張した Cloud Sync ライセンスを更新できるようになりました。

ネットアップから購入した Cloud Sync ライセンスを延長した場合は、ライセンスを再度追加して有効期限を更新できます。

["ライセンスを更新する方法について説明します"](#)。

## Box の資格情報を更新します

既存の同期関係の Box クレデンシャルを更新できるようになりました。

["クレデンシャルを更新する方法について説明します"](#)。

## 2021 年 10 月 31 日

### ボックスサポート

Cloud Sync ユーザーインターフェイスで Box サポートがプレビューとして利用できるようになりました。

Box は、複数のタイプの同期関係のソースまたはターゲットにすることができます。 ["サポートされている同期関係のリストを表示します"](#)。

### 作成日の設定

SMB サーバがソースの場合、 `_Date Created` という名前の新しい同期関係設定によって、特定の日付以前、特定の日付以前、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。

["Cloud Sync 設定の詳細については、こちらをご覧ください"](#)。

## 2021 年 10 月 4 日

### 追加のボックスサポート

Cloud Sync で追加の同期関係がサポートされるようになりました ["ボックス"](#) Cloud Sync API を使用する場合：

- Amazon S3 の機能です
- IBM Cloud Object Storage to Box の略
- StorageGRID To Box の略
- Box を NFS サーバに接続します
- Box を SMB サーバーに追加します

["API を使用して同期関係を設定する方法について説明します"](#)。

### SFTP パスに関するレポート

次の操作を実行できます。 ["レポートを作成します"](#) SFTP パスの場合

## 2021 年 9 月 2 日

### ONTAP の FSX のサポート

Amazon FSX for ONTAP ファイルシステムとの間でデータを同期できるようになりました。

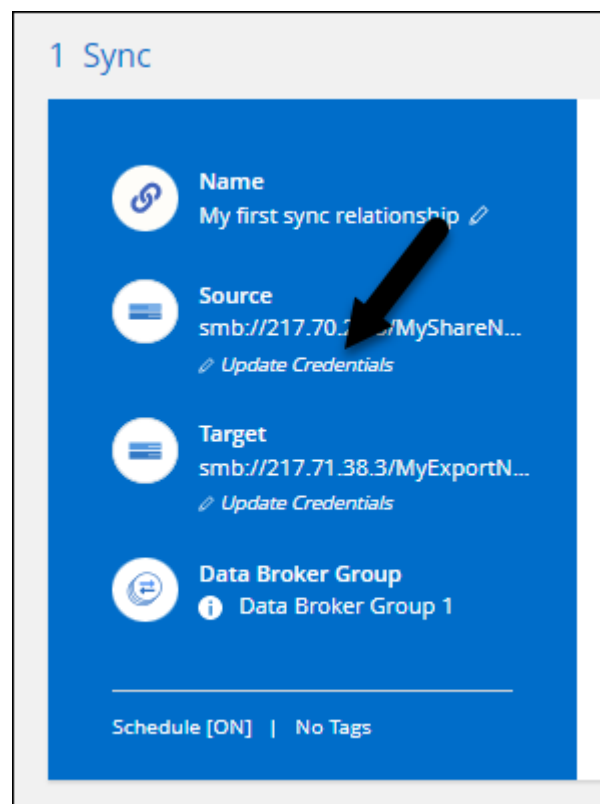
- ["Amazon FSX for ONTAP の詳細をご覧ください"](#)
- ["サポートされている同期関係を表示する"](#)
- ["Amazon FSX for ONTAP の同期関係を作成する方法について説明します"](#)

2021 年 8 月 1 日

## クレデンシャルを更新

Cloud Sync で、既存の同期関係のソースまたはターゲットの最新のクレデンシャルを使用してデータブローカーを更新できるようになりました。

この拡張機能は、セキュリティポリシーで定期的にクレデンシャルを更新するように要求される場合に役立ちます。 "[クレデンシャルを更新する方法について説明します](#)"。



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。"]

## オブジェクトストレージターゲットのタグ

同期関係を作成するときに、同期関係内のオブジェクトストレージターゲットにタグを追加できるようになりました。

タグの追加は、Amazon S3 、 Azure Blob 、 Google Cloud Storage 、 IBM Cloud Object Storage 、 および StorageGRID でサポートされています。

<

✓ AWS S3 Bucket

✓ Settings

6 Tags/Metadata

7 Review

## Relationship Tags

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.

☒ Save on Object's Tags ☐ Save On Object's Metadata

Tag Key

Up to 128 characters

Tag Value

Up to 256 characters

+ Add Relationship Tag

Optional Field | [Up to 5]

## Box のサポート

Cloud Sync は現在サポートされています **"ボックス"** Cloud Sync API を使用する際に、Amazon S3、StorageGRID、IBM Cloud Object Storage との同期関係のソースとして使用。

["API を使用して同期関係を設定する方法について説明します"](#)。

## Google Cloud のデータブローカー用パブリック IP

Google Cloud にデータブローカーを導入する際に、仮想マシンインスタンスに対してパブリック IP アドレスを有効にするか無効にするかを選択できるようになりました。

["Google Cloud にデータブローカーを導入する方法をご確認ください"](#)。

## Azure NetApp Files 用のデュアルプロトコル・ボリューム

Azure NetApp Files のソースボリュームまたはターゲットボリュームを選択した場合、同期関係用に選択したプロトコルに関係なく、Cloud Sync にデュアルプロトコルボリュームが表示されるようになりました。

## 2021 年 7 月 7 日

## ONTAP S3 ストレージと Google Cloud Storage

Cloud Sync のユーザーインターフェイスで、ONTAP S3 ストレージと Google Cloud Storage バケットの間の同期関係がサポートされるようになりました。

["サポートされている同期関係のリストを表示します"](#)。

## オブジェクトメタデータタグ

同期関係を作成して設定を有効にすると、Cloud Sync でオブジェクトベースのストレージ間でオブジェクトのメタデータとタグをコピーできるようになりました。

["\[ オブジェクトのコピー 設定の詳細については、を参照してください\]"](#)。

## 橋本事業者のためのサポート

Google Cloud サービスアカウントで認証することで、外部の橋本 Vault からクレデンシャルにアクセスするようにデータブローカーを設定できるようになりました。

["データブローカーでの橋 Corp Vault の使用の詳細を確認"](#)。

### S3 バケットのタグまたはメタデータを定義する

Amazon S3 バケットとの同期関係を設定する際に、ターゲットの S3 バケット内のオブジェクトに保存するタグまたはメタデータを同期関係ウィザードで定義できるようになりました。

タグ付けオプションは、以前は同期関係の設定に含まれていました。

## 2021 年 6 月 7 日

### Google Cloud のストレージクラス

同期関係のターゲットが Google Cloud Storage バケットの場合、使用するストレージクラスを選択できるようになりました。Cloud Sync では、次のストレージクラスがサポートされます。

- 標準
- ニアライン
- コールドライン（Coldline）
- Archive サービスの略

## 2021 年 5 月 2 日

### レポート内のエラー

レポートで見つかったエラーを表示し、最後のレポートまたはすべてのレポートを削除できるようになりました。

["レポートを作成して表示する方法の詳細については、を参照してください 設定"](#)。

### 属性を比較します

同期関係ごとに新しい \* Compare by \* 設定を使用できるようになりました。

この詳細設定では、ファイルまたはディレクトリが変更されたために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できます。

["同期関係の設定の変更の詳細については、こちらをご覧ください"](#)。

## 2021 年 4 月 11 日

### スタンドアロンの Cloud Sync サービスは廃止されました

スタンドアロンの Cloud Sync サービスは廃止されました。Cloud Sync には Cloud Manager から直接アクセスできるようになりました。同じ機能がすべて利用可能です。

Cloud Manager にログインしたら、上部の Sync タブに切り替えて、以前と同様に関係を表示できます。

さまざまなプロジェクトで **Google Cloud** バケットを使用できます

同期関係を設定する際、データブローカーのサービスアカウントに必要な権限を指定している場合は、異なるプロジェクトの Google Cloud バケットから選択できます。

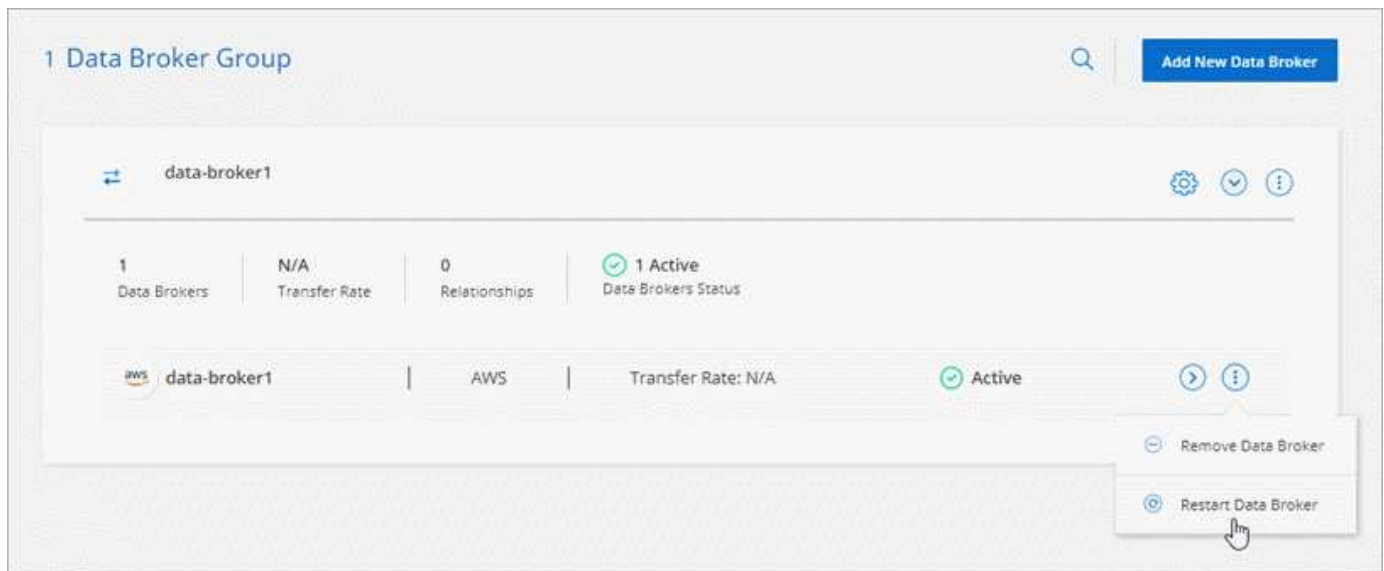
["サービスアカウントの設定方法について説明します"](#)。

## Google Cloud Storage と S3 の間のメタデータ

Cloud Sync は、Google Cloud Storage と S3 プロバイダ（AWS S3、StorageGRID、IBM Cloud Object Storage）間でメタデータをコピーするようになりました。

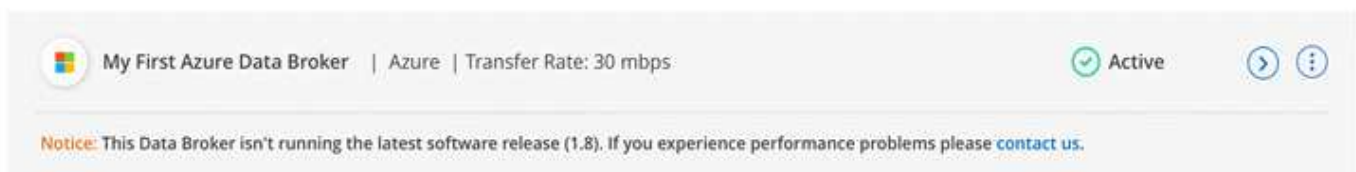
データブローカーを再起動

Cloud Sync からデータブローカーを再起動できるようになりました。



最新リリースを実行していない場合に表示されるメッセージです

Cloud Sync は、データブローカーで最新のソフトウェアリリースが実行されていないことを確認できるようになりました。このメッセージは、最新の機能を実際に利用するために役立ちます。



## 制限

既知の制限事項は、このリリースの製品でサポートされていないプラットフォーム、デバイス、機能、または製品と正しく相互運用できない機能を特定します。これらの制限

事項を慎重に確認してください

次の地域ではCloud Sync はサポートされていません。

- AWSの行政機関向けのサービスです
- Azure Governmentリージョン
- 中国



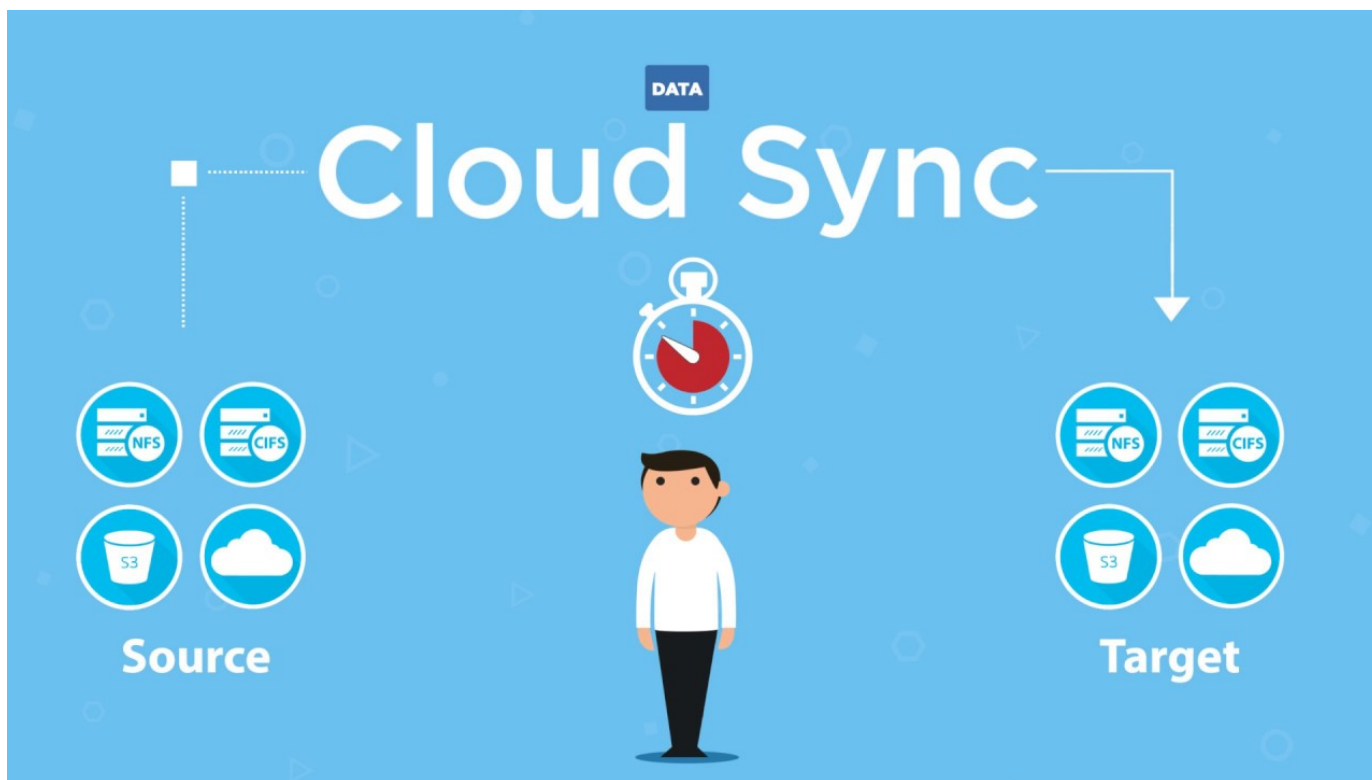
# はじめに

## Cloud Sync の概要

ネットアップのクラウド同期サービスは、データをクラウド内や社内の任意のターゲットに移行するための、シンプルでセキュアな自動化された方法を提供します。ファイルベースの NAS データセット（NFS または SMB）、Amazon Simple Storage Service（S3）のオブジェクト形式、NetApp StorageGRID® アプライアンス、その他のクラウドプロバイダのオブジェクトストアのいずれであっても、Cloud Sync は変換と移動を行うことができます。

### の機能

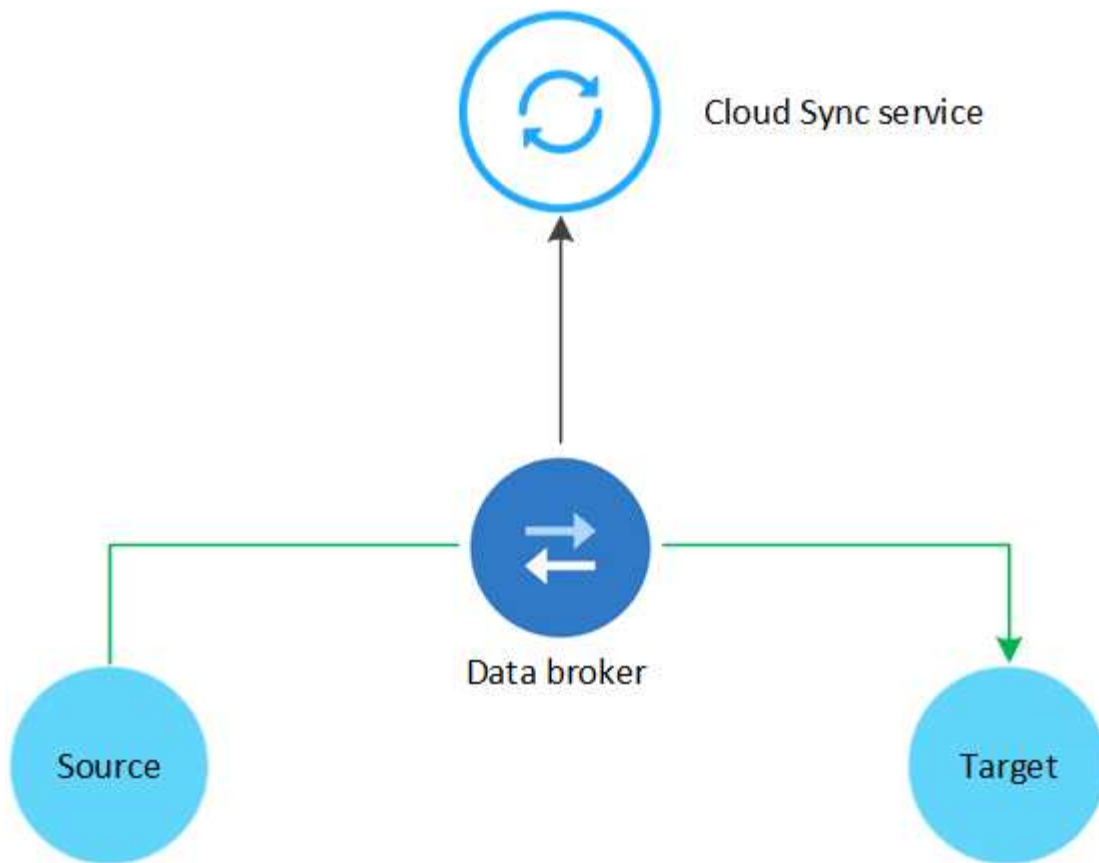
Cloud Sync の概要については、次のビデオをご覧ください。



## Cloud Sync の仕組み

Cloud Sync は、データブローカーグループ、Cloud Manager から提供されるクラウドベースのインターフェイス、ソースとターゲットで構成されるソフトウェアサービス（SaaS）プラットフォームです。

次の図は、Cloud Sync コンポーネント間の関係を示しています。



ネットアップのデータブローカーソフトウェアは、ソースからターゲットへデータを同期します（これを「a\_sync relationship\_」と呼びます）。データブローカーは、AWS、Azure、Google クラウドプラットフォーム、または社内で行うことができます。1 つ以上のデータブローカーで構成されるデータブローカーグループには、Cloud Sync サービスと通信して他のいくつかのサービスやリポジトリに接続するために、ポート 443 経由のアウトバウンドインターネット接続が必要です。"[エンドポイントのリストを表示します。](#)"。

最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。

## サポートされているストレージタイプ

Cloud Sync でサポートされるストレージタイプは次のとおりです。

- 任意の NFS サーバ
- 任意の SMB サーバ
- Amazon EFS
- ONTAP 対応の Amazon FSX
- Amazon S3
- Azure Blob の略
- Azure NetApp Files の特長
- Box （プレビュー版として利用可能）
- Cloud Volumes Service
- Cloud Volumes ONTAP

- 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
- オンプレミスの ONTAP クラスタ
- ONTAP S3 ストレージ
- SFTP（API のみを使用）
- StorageGRID

["サポートされている同期関係を表示します"](#)。

## コスト

Cloud Sync の使用に関連するコストには、リソース料金とサービス料金の 2 種類があります。

### リソース料金

リソースの料金は、1 つ以上のデータブローカーをクラウドで実行する場合のコンピューティングとストレージのコストに関連します。

### サービス料金

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。1 つ目は、AWS または Azure から登録する方法です。AWS または Azure を利用すると、1 時間ごとまたは 1 年ごとに料金を支払うことができます。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。

["ライセンスの仕組みをご確認ください"](#)。

## Cloud Sync のクイックスタート

Cloud Sync サービスを開始するには、いくつかの手順を実行します。

ソースとターゲットがサポートされ、セットアップされていることを確認します。最も重要な要件は、データブローカーグループと、ソースおよびターゲットの場所との間の接続を検証することです。

- ["サポートされている関係を表示する"](#)
- ["ソースとターゲットを準備します"](#)

ネットアップのデータブローカーソフトウェアは、ソースからターゲットへデータを同期します（これを「a\_sync relationship\_」と呼びます）。データブローカーは、AWS、Azure、Google クラウドプラットフォーム、または社内で行うことができます。1 つ以上のデータブローカーで構成されるデータブローカーグループには、Cloud Sync サービスと通信して他のいくつかのサービスやリポジトリに接続するために、ポート 443 経由のアウトバウンドインターネット接続が必要です。 ["エンドポイントのリストを表示します"](#)。

Cloud Sync のインストールプロセスに従って、同期関係を作成します。この段階で、クラウドにデータブローカーを導入したり、ご使用の 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。

- ["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"](#)

にログインします ["クラウドマネージャ"](#)をクリックし、\* 同期 \* をクリックして、ソースとターゲットの選択をドラッグアンドドロップします。プロンプトに従ってセットアップを完了します。 ["詳細はこちら。"](#)。

AWS または Azure から従量課金制または年間の支払いを申し込むことができます。または、ネットアップから直接ライセンスを購入することもできます。Cloud Sync のライセンス設定ページに移動して設定します。 ["詳細はこちら。"](#)。

## サポートされている同期関係

Cloud Sync を使用すると、ソースからターゲットへデータを同期できます。これを同期関係と呼びます。サポートされている関係を理解してから開始する必要があります。

ソースの場所	サポートされるターゲットロケーション
Amazon EFS	<ul style="list-style-type: none"><li>• Amazon EFS</li><li>• ONTAP 対応の Amazon FSX</li><li>• Amazon S3</li><li>• Azure Blob の略</li><li>• Azure NetApp Files の特長</li><li>• Cloud Volumes ONTAP</li><li>• Cloud Volumes Service</li><li>• Google クラウドストレージ</li><li>• IBM クラウドオブジェクトストレージ</li><li>• NFS サーバ</li><li>• オンプレミスの ONTAP クラスタ</li><li>• SMB サーバ</li><li>• StorageGRID</li></ul>

ソースの場所	サポートされるターゲットロケーション
ONTAP 対応の Amazon FSX	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>
Amazon S3	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• ボックス ^1</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>

ソースの場所	サポートされるターゲットロケーション
Azure Blob の略	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>
Azure NetApp Files の特長	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>

ソースの場所	サポートされるターゲットロケーション
ボックス ^1	<ul style="list-style-type: none"> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>
Cloud Volumes ONTAP	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>

ソースの場所	サポートされるターゲットロケーション
Cloud Volumes Service	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>
Google クラウドストレージ	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• ONTAP S3 ストレージ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>



ソースの場所	サポートされるターゲットロケーション
IBM クラウドオブジェクトストレージ	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• ボックス ^1</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>
NFS サーバ	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>

ソースの場所	サポートされるターゲットロケーション
オンプレミスの ONTAP クラスタ	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>
ONTAP S3 ストレージ	<ul style="list-style-type: none"> <li>• Google クラウドストレージ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> <li>• ONTAP S3 ストレージ</li> </ul>
SFTP <sup>2</sup>	S3
SMB サーバ	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• ONTAP S3 ストレージ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>

ソースの場所	サポートされるターゲットロケーション
StorageGRID	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP 対応の Amazon FSX</li> <li>• Amazon S3</li> <li>• Azure Blob の略</li> <li>• Azure NetApp Files の特長</li> <li>• ボックス ^1</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google クラウドストレージ</li> <li>• IBM クラウドオブジェクトストレージ</li> <li>• NFS サーバ</li> <li>• オンプレミスの ONTAP クラスタ</li> <li>• ONTAP S3 ストレージ</li> <li>• SMB サーバ</li> <li>• StorageGRID</li> </ul>

注：

1. Box サポートはプレビューとして利用できます。
2. このソース / ターゲットとの同期関係は、Cloud Sync API のみを使用してサポートされています。
3. BLOB コンテナがターゲットの場合は、特定の Azure BLOB ストレージ階層を選択できます。
  - ホットストレージ
  - 優れたストレージ
4. `[[storage-classes]]` Amazon S3 がターゲットの場合は、特定の S3 ストレージクラスを選択できます。
  - 標準（これがデフォルトクラス）
  - インテリジェント階層化
  - 標準的なアクセス頻度は低い
  - 1 回のアクセスではほとんど発生しません
  - 氷河
  - Glacier Deep Archive
5. Google Cloud Storage バケットがターゲットの場合は、特定のストレージクラスを選択できます。
  - 標準
  - ニアライン
  - コールドライン（Coldline）

## ソースとターゲットを準備します

ソースとターゲットが次の要件を満たしていることを確認します。

### ネットワーキング

- ソースとターゲットに、データブローカーグループへのネットワーク接続が必要です。

たとえば、NFS サーバがデータセンターにあり、データブローカーが AWS にある場合、ネットワークから VPC へのネットワーク接続（VPN または Direct Connect）が必要です。

- ネットワークタイムプロトコル（NTP）サービスを使用するようにソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

### ターゲットディレクトリ

同期関係を作成するときに、Cloud Sync で既存のターゲットディレクトリを選択し、必要に応じてそのディレクトリ内に新しいフォルダを作成できます。そのため、優先ターゲットディレクトリがすでに存在していることを確認してください。

### ディレクトリを読み取るための権限

ソースまたはターゲット内のすべてのディレクトリまたはフォルダを表示するには、Cloud Sync でディレクトリまたはフォルダの読み取り権限が必要です。

#### NFS

ファイルおよびディレクトリに対して、ソース / ターゲットに uid / gid を指定して権限を定義しておく必要があります。

#### オブジェクトストレージ

- AWS と Google Cloud の場合、データブローカーにはリストオブジェクトの権限が必要です（データブローカーのインストール手順を実行する場合、これらの権限はデフォルトで提供されます）。
- Azure 、 StorageGRID 、 IBM の場合は、同期関係のセットアップ時に入力するクレデンシャルに、リストオブジェクトの権限が必要です。

#### SMB

同期関係のセットアップ時に入力する SMB クレデンシャルには、リストフォルダの権限が必要です。



データブローカーでは、デフォルトで、.snapshot 、 ~snapshot 、 .copy-Offload の各ディレクトリが無視されます

## Amazon S3 バケットの要件

Amazon S3 バケットが次の要件を満たしていることを確認します。

## Amazon S3 でサポートされているデータブローカーの場所

S3 ストレージを含む同期関係では、AWS または社内にデータブローカーを導入する必要があります。いずれの場合も、インストール時にデータブローカーを AWS アカウントに関連付けるように求められます。

- ["AWS データブローカーの導入方法について説明します"](#)
- ["Linux ホストにデータブローカーをインストールする方法について説明します"](#)

サポートされている **AWS** リージョン

中国地域を除くすべての地域がサポートされています。

他の **AWS** アカウントの **S3** バケットに必要な権限

同期関係をセットアップする際、データブローカーに関連付けられていない AWS アカウントに配置されている S3 バケットを指定することができます。

["この JSON ファイルに含まれている権限"](#) データブローカーがアクセスできるように、S3 バケットに適用する必要があります。これらの権限を使用すると、データブローカーはバケットとの間でデータをコピーし、バケット内のオブジェクトを一覧表示できます。


JSON ファイルに含まれる権限については、次の点に注意してください。

1. `<BucketName>` は、データブローカーに関連付けられていない AWS アカウントにあるバケットの名前です。
2. `<RoleARN>` は次のいずれかに置き換える必要があります。
  - データブローカーを Linux ホストに手動でインストールした場合、データブローカーの導入時に AWS クレデンシャルを指定した AWS ユーザの ARN を `_RoleARN_` should be the ARN when deploying a AWS credentials
  - CloudFormation テンプレートを使用して AWS にデータブローカーを導入した場合は、テンプレートによって作成された IAM ロールの ARN を `_RoleARN_` にする必要があります。

ロール ARN をを見つけるには、EC2 コンソールに移動し、データブローカーインスタンスを選択して、Description タブから IAM ロールをクリックします。次に、ロール ARN を含む IAM コンソールに概要ページが表示されます。

## Summary

Delete role

**Role ARN** `arn:aws:iam::142281742614:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05`   
**Role description** [Edit](#)

## Azure BLOB ストレージの要件

Azure BLOB ストレージが次の要件を満たしていることを確認します。

**Azure BLOB** でサポートされるデータブローカーの場所

データブローカーは、同期関係に Azure BLOB ストレージが含まれている場合でも、任意の場所に配置でき

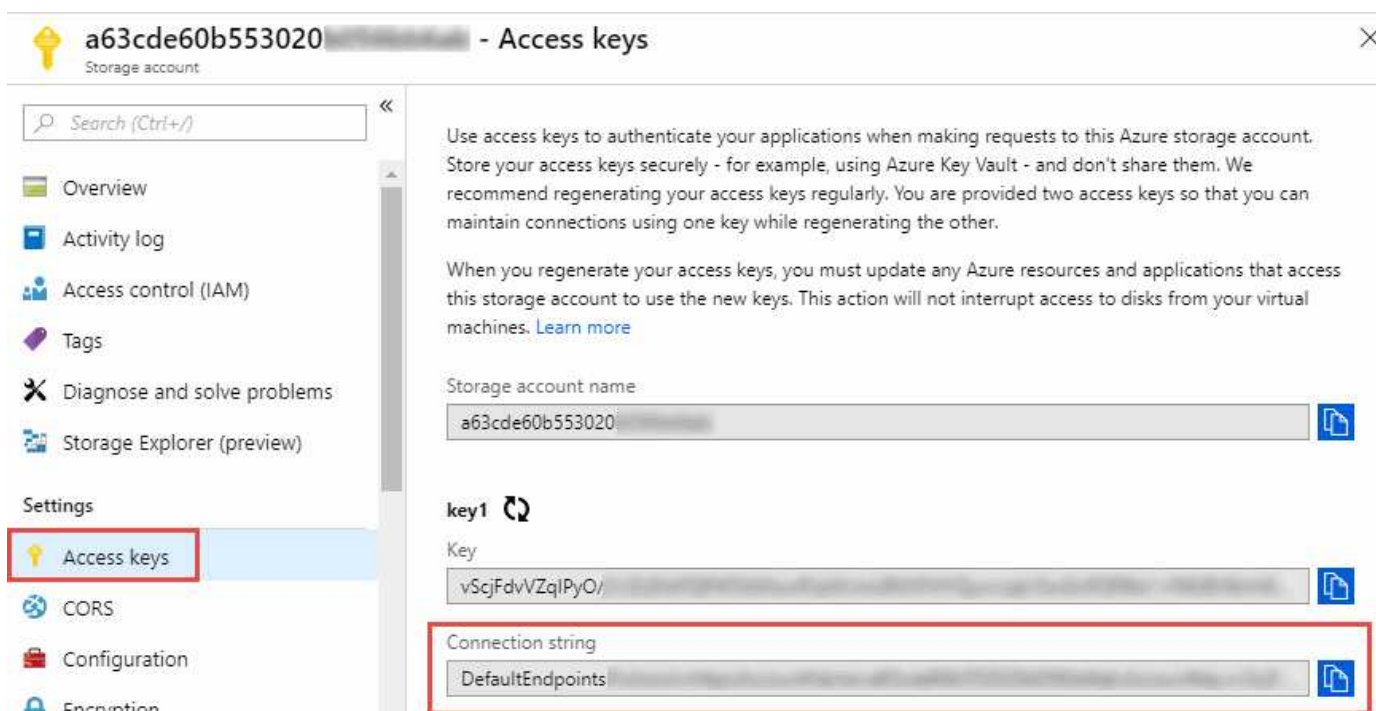
ます。

サポートされている **Azure** リージョン

中国、米国政府、米国国防総省を除くすべての地域がサポートされます。

### Azure Blob および NFS / SMB を含む関係の接続文字列

Azure BLOB コンテナと NFS サーバまたは SMB サーバ間の同期関係を作成する場合は、ストレージアカウント接続文字列を使用してクラウド同期を提供する必要があります。



をクリックすることで使用できます。"]

2 つの Azure Blob コンテナ間でデータを同期する場合は、接続文字列にを含める必要があります **"共有アクセスシグニチャ"**（SAS）。BLOB コンテナと NFS サーバまたは SMB サーバの間で同期する場合は、SAS を使用することもできます。

SA は、BLOB サービスとすべてのリソースタイプ（サービス、コンテナ、オブジェクト）へのアクセスを許可する必要があります。SAS には、次の権限も含まれている必要があります。

- ソース BLOB コンテナの場合： read および list
- ターゲット BLOB コンテナの場合：読み取り、書き込み、一覧表示、追加、作成

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Advanced Threat Protection (pr...

Properties

Locks

Allowed services ⓘ  
☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types ⓘ  
☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ  
☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☐ Update ☐ Process

Start and expiry date/time ⓘ  
Start  
2018-10-23 10:07:32 AM  
End  
2019-10-23 6:07:32 PM  
(UTC-04:00) --- Current Time Zone ---

Allowed IP addresses ⓘ  
for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ  
☒ HTTPS only ☐ HTTPS and HTTP

Signing key ⓘ  
key1

Generate SAS and connection string

## Azure NetApp Files の要件

Azure NetApp Files との間でデータを同期する場合は、Premium または Ultra サービスレベルを使用します。ディスクのサービスレベルが Standard の場合は、エラーやパフォーマンスの問題が発生することがあります。



適切なサービスレベルの決定に支援が必要な場合は、ソリューションアーキテクトに相談してください。取得できるスループットはボリュームサイズとボリューム階層によって決まります。

"Azure NetApp Files のサービスレベルとスループットの詳細については、こちらをご覧ください。"

## Box の要件

- Box を含む同期関係を作成するには、次の資格情報を入力する必要があります。
  - クライアント ID
  - クライアントシークレット
  - 秘密鍵
  - 公開鍵 ID

- パスフレーズ
- エンタープライズ ID
- Amazon S3 から Box への同期関係を作成する場合は、統合構成のデータブローカーグループを使用し、次の設定を 1 にする必要があります。
  - スキャナの同時実行数
  - スキャナ処理の上限
  - 転送元同時実行数
  - 転送元プロセスの制限

["データブローカーグループのユニファイド構成を定義する方法について説明します"](#)。

## Google クラウドストレージバケットの要件

Google クラウドストレージバケットが次の要件を満たしていることを確認します。

### Google クラウドストレージでサポートされるデータブローカーの場所

Google Cloud Storage を含む同期関係を確立するには、Google Cloud または自社運用環境にデータブローカーを導入する必要があります。Cloud Sync では、同期関係を作成する際に、データブローカーのインストールプロセスをガイドします。

- ["Google Cloud データブローカーの導入方法をご確認ください"](#)
- ["Linux ホストにデータブローカーをインストールする方法について説明します"](#)

### サポートされている Google Cloud リージョン

すべてのリージョンがサポートされています。

### 他の Google Cloud プロジェクトのバケットに対する権限

同期関係を設定する際、データブローカーのサービスアカウントに必要な権限を指定している場合は、異なるプロジェクトの Google Cloud バケットから選択できます。 ["サービスアカウントの設定方法について説明します"](#)。

### SnapMirror デスティネーションの権限

同期関係のソースが SnapMirror デスティネーション（読み取り専用）の場合、「読み取り / リスト」権限でソースからターゲットにデータを同期できます。

## NFS サーバの要件

- NFS サーバには、NetApp システムまたは NetApp 以外のシステムを使用できます。
- ファイルサーバは、データブローカーホストが必要なポート経由でエクスポートにアクセスできるようにする必要があります。
  - 111 TCP/UDP
  - 2049 TCP/UDP



- 5555 TCP/UDP

- NFS バージョン 3、4.0、4.1、4.2 がサポートされています。

サーバで目的のバージョンが有効になっている必要があります。

- ONTAP システムから NFS データを同期する場合は、SVM の NFS エクスポートリストへのアクセスが有効になっていることを確認します（`vserver nfs modify -vserver _svm_name _showmount enabled`）。



ONTAP 9.2 以降では、showmount のデフォルト設定は `_enabled_starting` です。

## ONTAP の要件

同期関係に Cloud Volumes ONTAP またはオンプレミスの ONTAP クラスタが含まれており、NFSv4 以降を選択した場合は、ONTAP システムで NFSv4 ACL を有効にする必要があります。これは ACL をコピーするために必要です。

## ONTAP S3 ストレージの要件

を含む同期関係を設定する場合 "[ONTAP S3 ストレージ](#)"を使用するには、次のものを用意する必要があります。

- ONTAP に接続されている LIF の IP アドレス S3
- ONTAP が設定されているアクセスキーとシークレットキー を使用してください

## SMB サーバの要件

- SMB サーバは、NetApp システムまたは他社製システムのいずれかです。
- Cloud Sync には、SMB サーバに対する権限を持つクレデンシャルを指定する必要があります。
  - ソース SMB サーバについては、list および read という権限が必要です。

Backup Operators グループのメンバーは、ソース SMB サーバでサポートされています。

- ターゲット SMB サーバについては、list、read、および write の各権限が必要です。
- ファイルサーバは、データブローカーホストが必要なポート経由でエクスポートにアクセスできるようにする必要があります。
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- SMB バージョン 1.0、2.0、2.1、3.0、および 3.11 がサポートされます。
- 「フルコントロール」権限を持つ「管理者」グループにソースフォルダとターゲットフォルダを付与します。

この権限を付与しないと、データブローカーにファイルまたはディレクトリの ACL を取得するための十分な権限がない可能性があります。この場合、`"getxattr error 95"` というエラーが表示されます。

## 非表示のディレクトリとファイルに関する **SMB** の制限

SMB の制限は、SMB サーバ間でデータを同期する際に非表示のディレクトリとファイルに影響します。ソース SMB サーバ上のディレクトリまたはファイルが Windows で非表示になっていた場合、非表示属性はターゲット SMB サーバにコピーされません。

大文字と小文字の区別がないため、**SMB** 同期の動作が制限されます

SMB プロトコルでは大文字と小文字が区別されないため、大文字と小文字は同じものとして扱われます。この動作により、ターゲットに SMB サーバとデータがすでに存在する同期関係では、ファイルが上書きされ、ディレクトリのコピーでエラーが発生する可能性があります。

たとえば、ソースに「A」という名前のファイルがあり、ターゲットに「A」という名前のファイルがあるとします。Cloud Sync が「A」という名前のファイルをターゲットにコピーすると、ファイル「A」はソースからファイル「A」で上書きされます。

ディレクトリの場合は、ソースに「b」という名前のディレクトリがあり、ターゲットに「B」という名前のディレクトリがあるとします。Cloud Sync が「b」という名前のディレクトリをターゲットにコピーしようとする、Cloud Sync には、そのディレクトリがすでに存在することを示すエラーが表示されます。その結果、Cloud Sync は常に「B」という名前のディレクトリをコピーできません。

この制限を回避する最善の方法は、空のディレクトリにデータを確実に同期させることです。

## Cloud Sync のネットワークの概要

Cloud Sync 用のネットワークでは、データブローカーグループとソースおよびターゲットの場所との間の接続、およびデータブローカーからのポート 443 経由のアウトバウンドインターネット接続が確立されます。

### データブローカーの場所

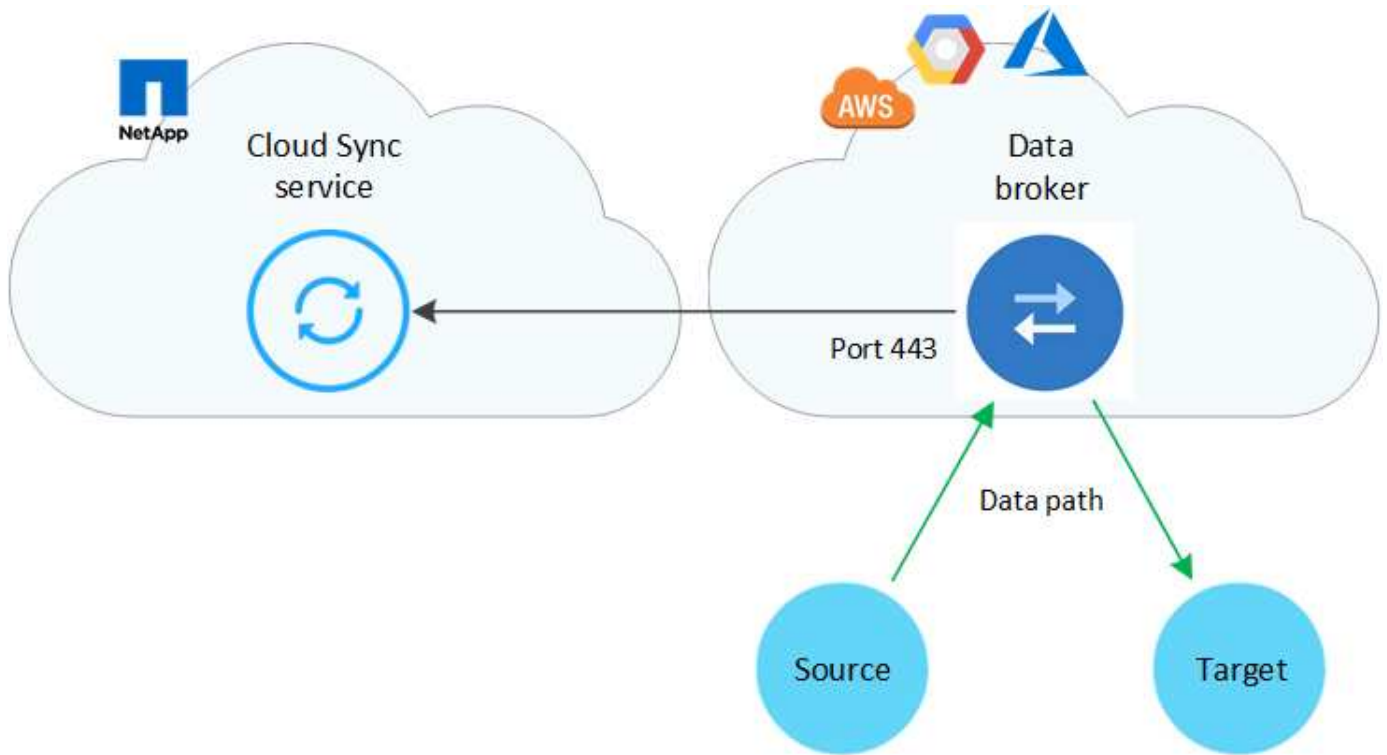
データブローカーグループは、クラウドまたはオンプレミスにインストールされた 1 つ以上のデータブローカーで構成されます。

### クラウド内のデータブローカー

次の図は、クラウド、AWS、Google Cloud、Azure で実行されるデータブローカーを示しています。データブローカーへの接続が確立されていれば、ソースとターゲットはどの場所にも存在できます。たとえば、データセンターからクラウドプロバイダーへの VPN 接続があるとします。

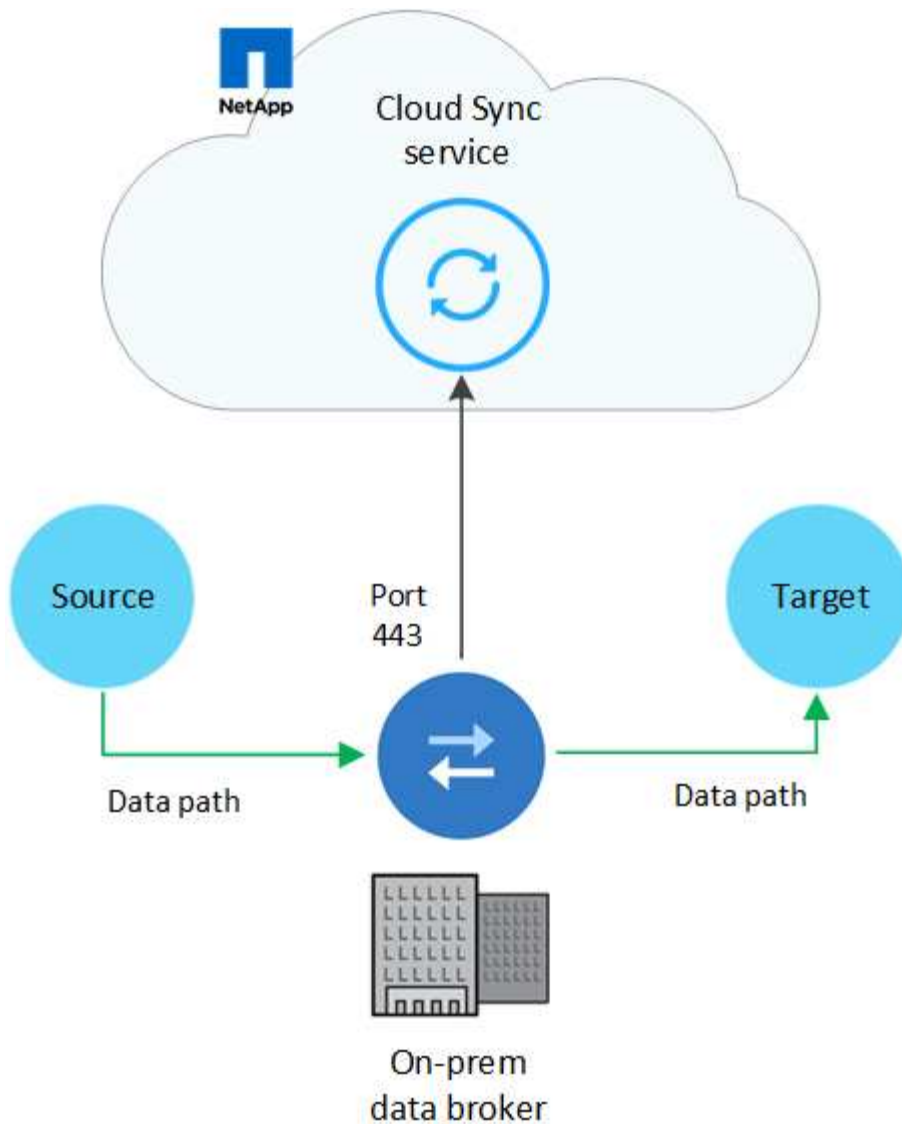


Cloud Sync がデータブローカーを AWS、Azure、または Google Cloud に導入すると、必要なアウトバウンド通信を有効にするセキュリティグループが作成されます。



#### 社内のデータブローカー

次の図は、データセンターでオンプレミスで実行されているデータブローカーを示しています。この場合も、データブローカーに接続が確立されていれば、ソースとターゲットはどの場所にも存在できます。



## ネットワーク要件

- ソースとターゲットに、データブローカーグループへのネットワーク接続が必要です。

たとえば、NFS サーバがデータセンターにあり、データブローカーが AWS にある場合、ネットワークから VPC へのネットワーク接続（VPN または Direct Connect）が必要です。

- データブローカーでは、ポート 443 経由で Cloud Sync サービスにタスクをポーリングできるように、アウトバウンドのインターネット接続が必要です。
- ネットワークタイムプロトコル（NTP）サービスを使用するようにソース、ターゲット、データブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

## ネットワークエンドポイント

ネットアップのデータブローカーは、Cloud Sync サービスと通信したり、他のいくつかのサービスやリポジトリと通信したりするために、ポート 443 を介したアウトバウンドインターネットアクセスを必要とします。ローカル Web ブラウザでは、特定の操作を実行するためにエンドポイントへのアクセスも必要です。発信接続を制限する必要がある場合は、発信トラフィック用にファイアウォールを設定する際に、次のエンドポ

イントのリストを参照してください。

## データブローカーエンドポイント

データブローカーは、次のエンドポイントにアクセスします。

エンドポイント	目的
<a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a>	データブローカーホストの CentOS パッケージを更新するためにリポジトリに接続します。このエンドポイントは、CentOS ホストにデータブローカーを手動でインストールした場合にのみ接続されます。
¥ <a href="https://rpm.nodesource.com">https://rpm.nodesource.com</a> ¥ <a href="https://registry.npmjs.org">https://registry.npmjs.org</a> ¥ <a href="https://nodejs.org">https://nodejs.org</a> :	node.js、NPM、および開発に使用されているその他のサードパーティパッケージを更新するためのリポジトリに問い合わせます。
<a href="https://tgz.pm2.io">https://tgz.pm2.io</a>	PM2 を更新するためのリポジトリにアクセスするには、クラウドの同期を監視するために使用されるサードパーティパッケージです。
¥ <a href="https://sqs.us-east-1.amazonaws.com">https://sqs.us-east-1.amazonaws.com</a> ¥ ¥ <a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Cloud Sync が処理に使用する AWS サービスに連絡する（ファイルのキューイング、アクションの登録、データブローカーへの更新の配信）。
¥ <a href="https://s3.region.amazonaws.com">https://s3.region.amazonaws.com</a> （例 ： <a href="https://s3.us-east-2.amazonaws.com">s3.us-east-2.amazonaws.com</a> :443 ） <a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region">https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region</a> ["S3 エンドポイントの一覧については、AWS のドキュメントを参照してください"]	同期関係に S3 バケットが含まれている場合に Amazon S3 に連絡する。
<a href="https://s3.us-east-1.amazonaws.com">https://s3.us-east-1.amazonaws.com</a>	Cloud Sync からデータブローカーログをダウンロードすると、データブローカーは、ログディレクトリを zip で保存し、us-east-1 リージョン内の事前定義された S3 バケットにログをアップロードします。
¥ <a href="https://cf.cloudsync.netapp.com">https://cf.cloudsync.netapp.com</a> ¥ <a href="https://repo.cloudsync.netapp.com">https://repo.cloudsync.netapp.com</a>	Cloud Sync サービスに連絡します。
<a href="https://support.netapp.com">https://support.netapp.com</a>	同期関係に BYOL ライセンスを使用する場合は、ネットアップのサポートにお問い合わせください。
<a href="https://fedoraproject.org">https://fedoraproject.org</a>	インストールおよび更新中にデータブローカー仮想マシンに 7z をインストールするには、AutoSupport メッセージをネットアップテクニカルサポートに送信するには 7z が必要です。
<a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	データブローカーが AWS に導入されたときや、オンプレミスに導入されて AWS のクレデンシャルが指定されたときに、AWS のクレデンシャルを確認することができます。データブローカーは、導入時、更新時、および再起動時にこのエンドポイントにアクセスします。
¥ <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> ¥ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	データセンスを使用して新しい同期関係のソースファイルを選択するときに Cloud Data Sense に連絡するには、次の手順に従います。

## Web ブラウザエンドポイント

トラブルシューティングの目的でログをダウンロードするには、Web ブラウザから次のエンドポイントにアクセスする必要があります。

logs.cloudsync.netapp.com:443

# データブローカーをインストール

## AWS に新しいデータブローカーを作成

新しいデータブローカーグループを作成する場合、Amazon Web Services を選択して、VPC 内の新しい EC2 インスタンスにデータブローカーソフトウェアを導入します。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

また、クラウド内または社内の既存の Linux ホストにデータブローカーをインストールすることもできます。["詳細はこちら。"](#)

サポートされている **AWS** リージョン

中国地域を除くすべての地域がサポートされています。

### ネットワーク要件

- データブローカーは、アウトバウンドインターネット接続を必要としているため、クラウド同期サービスにポート 443 経由のタスクをポーリングできます。

Cloud Sync は、AWS にデータブローカーを導入すると、必要なアウトバウンド通信を有効にするセキュリティグループを作成します。インストールプロセス中にプロキシサーバーを使用するようにデータブローカーを設定できます。

アウトバウンド接続を制限する必要がある場合は、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- ネットワークタイムプロトコル（NTP）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

## AWS にデータブローカーを展開するために必要な権限

の導入に使用する AWS ユーザーアカウント データブローカーの権限は、に含まれている必要があります ["ネットアップが提供するポリシーです"](#)。

## AWS データブローカーで独自の IAM ロールを使用するための要件

Cloud Sync は、データブローカーを導入するときに、データブローカーインスタンスの IAM ロールを作成します。必要に応じて、独自の IAM ロールを使用してデータブローカーを展開できます。組織に厳密なセキュリティポリシーがある場合は、このオプションを使用できます。

IAM ロールは、次の要件を満たす必要があります。

- EC2 サービスは、IAM の役割を信頼できるエンティティとして引き受けることを許可されている必要があります。
- "この JSON ファイルで定義されている権限" データブローカーが正しく機能するように、IAM ロールに関連付ける必要があります。

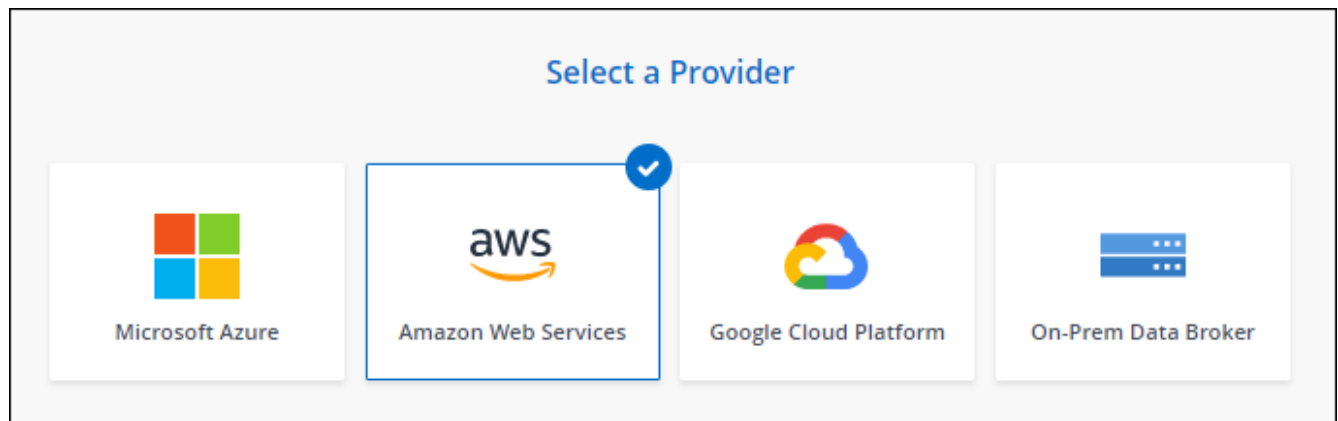
データブローカーを導入する際に IAM ロールを指定するには、次の手順に従います。

## データブローカーの作成

新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを AWS にインストールする方法について説明します。

### 手順

1. [新しい同期の作成 \*] 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、[続行 \*] をクリックします。  
  
「\* データブローカーグループ \*」 ページが表示されるまで、手順を完了します。
3. [\* データブローカーグループ \*] ページで、[\* データブローカーの作成 \*] をクリックし、[\* Amazon Web Services \*] を選択します。



4. データブローカーの名前を入力し、[\* 続行] をクリックします。
5. AWS でデータブローカーを作成するために、Cloud Sync アクセスキーを入力します。

キーは保存されず、他の目的に使用されることもありません。

アクセスキーを指定しない場合は、ページの下部にあるリンクをクリックして CloudFormation テンプレートを使用します。このオプションを使用する場合は、AWS に直接ログインするため、クレデンシャルを指定する必要はありません。

CloudFormation テンプレートを使用してデータブローカーインスタンスを起動する方法を紹介したビデオを次に示します。

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

6. AWS アクセスキーを入力した場合は、インスタンスの場所を選択し、キーペアを選択し、パブリック IP アドレスを有効にするかどうかを選択します。既存の IAM ロールを選択した場合は、Cloud Sync によってロールが作成されるようにこのフィールドを空白のままにします。



独自の IAM ロールを選択した場合は、 [必要な権限を指定する必要があります](#)。

### Basic Settings

#### Location

Region

US West | Oregon

VPC

vpc-3c46c059 - 10.60.21.0/25

Subnet

10.60.21.0/25

#### Connectivity

Key Pair

newKey

Enable Public IP?

☒ Enable ☐ Disable

IAM Role (optional)

7. VPC でのインターネットアクセスにプロキシが必要な場合は、プロキシの設定を指定します。
8. データブローカーが利用可能になったら、Cloud Sync で [\* 続行 ] をクリックします。

次の図は、AWS に正常に導入されたインスタンスを示しています。

NFS Server

2 Data Broker Group

3 Directories

4 Target NFS Server

### Select a Data Broker Group

1 Data Broker Group

ben-data-broker

1 Data Brokers

N/A Transfer Rate

0 Relationships

1 Active

Data Brokers Status

9. ウィザードのページに入力して、新しい同期関係を作成します。

AWS にデータブローカーを導入し、新しい同期関係を作成しました。このデータブローカーグループは、追加の同期関係で使用できます。

データブローカーインスタンスの詳細

Cloud Sync は、次の構成を使用して AWS にデータブローカーを作成します。

インスタンスタイプ

m5n.xlarge （リージョン内で使用可能な場合）。 m5.xlarge （ m5.xlarge



## vCPU

4.

## RAM

16 GB

オペレーティングシステム

Amazon Linux 2.

ディスクのサイズとタイプ

10GB gp2 SSD です

## Azure に新しいデータブローカーを作成

新しいデータブローカーグループを作成する場合は、Microsoft Azure を選択して、VNet 内の新しい仮想マシンにデータブローカーソフトウェアを導入します。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

また、クラウド内または社内の既存の Linux ホストにデータブローカーをインストールすることもできます。["詳細はこちら。"](#)。

サポートされている **Azure** リージョン

中国、米国政府、米国国防総省を除くすべての地域がサポートされます。

ネットワーク要件

- データブローカーは、アウトバウンドインターネット接続を必要としているため、クラウド同期サービスにポート 443 経由のタスクをポーリングできます。

Cloud Sync は、データブローカーを Azure に導入するときに、必要なアウトバウンド通信を有効にするセキュリティグループを作成します。

アウトバウンド接続を制限する必要がある場合は、を参照してください ["データブローカーが連絡するエンドポイントのリスト"](#)。

- ネットワークタイムプロトコル（NTP）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

**Azure** にデータブローカーを導入するための権限が必要です

データブローカーの導入に使用する Azure ユーザーアカウントに、次の権限があることを確認してください。

```
{
  "Name": "Azure Data Broker",
  "Actions": [
    "Microsoft.Resources/subscriptions/read",
```

```

"Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/publicIPAddresses/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Compute/disks/write",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/publicIPAddresses/join/action",
    "Microsoft.Network/networkInterfaces/join/action"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Azure Data Broker",
"IsCustom": "true"
}

```

## 認証方式

データブローカーを導入する場合、仮想マシンの認証方式として、パスワードまたはSSH公開鍵ペアを選択する必要があります。

キー・ペアの作成方法については、を参照してください "[Azure のドキュメント：「Create and use an SSH public-private key pair for Linux VMs in Azure」](#)"。

## データブローカーの作成

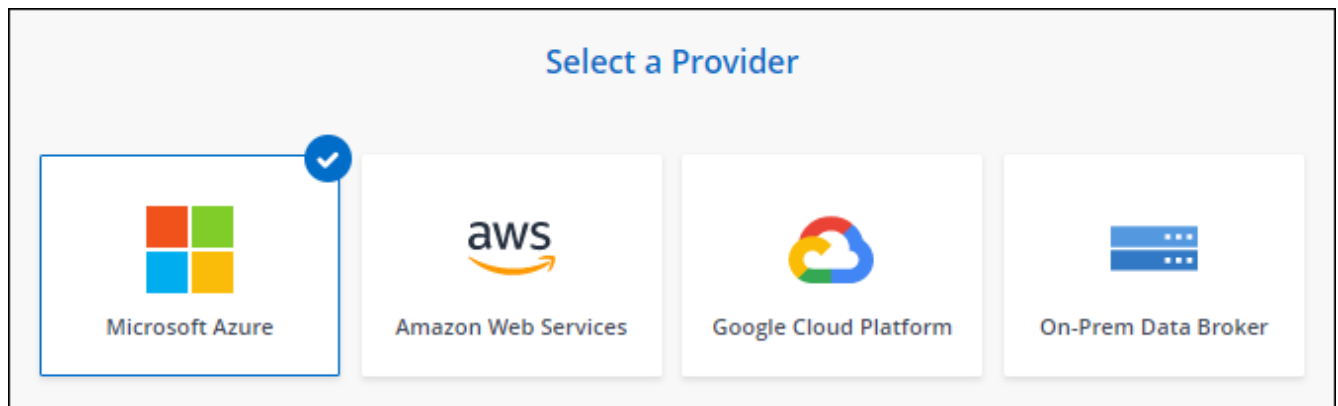
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを Azure にインストールする方法について説明します。

### 手順

1. [新しい同期の作成 \*] 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、[続行 \*] をクリックします。

「\* データブローカーグループ \*」 ページが表示されるまで、手順を完了します。

3. [\* データブローカーグループ \*] ページで、[\* データブローカーの作成 \*] をクリックし、[Microsoft Azure\*] を選択します。



4. データブローカーの名前を入力し、[\* 続行] をクリックします。
5. プロンプトが表示されたら、Microsoft アカウントにログインします。プロンプトが表示されない場合は、\* 「\* Azure へのログイン \*」 をクリックします。

このフォームは、Microsoft が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

6. データブローカーの場所を選択し、仮想マシンに関する基本的な詳細を入力します。

Location	Virtual Machine
<p>Subscription</p> <p>OCCM Dev ▼</p>	<p>VM Name</p> <p>netappdatabroker</p>
<p>Azure Region</p> <p>West US 2 ▼</p>	<p>User Name</p> <p>databroker</p>
<p>VNet</p> <p>Vnet1 ▼</p>	<p>Authentication Method:</p> <p><input checked="" type="radio"/> Password <input type="radio"/> Public Key</p>
<p>Subnet</p> <p>Subnet1 ▼</p>	<p>Enter Password</p> <p>.....</p>
	<p>Resource Group:</p> <p><input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group</p>

7. VNet でのインターネットアクセスにプロキシが必要な場合は、プロキシ設定を指定します。

8. [\* Continue (続行) ] をクリックし、展開が完了するまでページを開いたままにします。

この処理には最大 7 分かかることがあります。

9. Cloud Sync で、データブローカーが利用可能になったら、[\* 続行 ] をクリックします。

10. ウィザードのページに入力して、新しい同期関係を作成します。

Azure にデータブローカーを導入し、新しい同期関係を作成しました。このデータブローカーは、追加の同期関係とともに使用できます。

## 管理者の同意が必要なことを示すメッセージを受信しますか？

Cloud Sync で組織内のリソースに代理でアクセスする権限が必要であるために管理者の承認が必要であることが通知された場合は、次の 2 つのオプションがあります。

1. AD 管理者に次の権限を提供するよう依頼します。

Azure では、[ 管理センター ] > [ Azure AD ] > [ ユーザーとグループ ] > [ ユーザー設定 \* ] の順に選択し、\* ユーザーが代わりに会社のデータにアクセスするアプリに同意できるようにします。\*

2. 次の URL を使用して、\* CloudSync-AzureDataBrokerCreator\* に代わって、AD 管理者に同意するよう依頼してください（これは管理者同意エンドポイントです）。

\ [https://login.microsoftonline.com/{FILL テナント ID }/v2.0/adminconCILINE?client\\_id=8ee4ca3a-BAFA-4831-97cc-5a38923cab85 &redirect\\_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user\\_impersonationhttps://graph.microsoft.com/User.Read](https://login.microsoftonline.com/{FILL テナント ID }/v2.0/adminconCILINE?client_id=8ee4ca3a-BAFA-4831-97cc-5a38923cab85 &redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read) に移動します

URL に示されているように、アプリケーションの URL は <https://cloudsync.netapp.com> で、アプリケーションのクライアント ID は 8ee4ca3a-BAFA-4831-97cc-5a38923cab85 です。

### データブローカー VM の詳細

Cloud Sync は、次の構成を使用して Azure にデータブローカーを作成します。

#### VM タイプ

標準 DS4 v2

#### vCPU

8.

#### RAM

28 GB

#### オペレーティングシステム

CentOS 7.7

#### ディスクのサイズとタイプ

64 GB Premium SSD

## Google Cloud で新しいデータブローカーを作成

新しいデータブローカーグループを作成するときは、Google Cloud Platform を選択して、Google Cloud VPC 内の新しい仮想マシンインスタンスにデータブローカーソフトウェアを導入します。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

また、クラウド内または社内の既存の Linux ホストにデータブローカーをインストールすることもできます。

"詳細はこちら。"。

サポートされている **Google Cloud** リージョン

すべてのリージョンがサポートされています。

ネットワーク要件

- データブローカーは、アウトバウンドインターネット接続を必要としているため、クラウド同期サービスにポート 443 経由のタスクをポーリングできます。

Cloud Sync が Google Cloud にデータブローカーを導入すると、必要なアウトバウンド通信を可能にするセキュリティグループが作成されます。

アウトバウンド接続を制限する必要がある場合は、を参照してください "[データブローカーが連絡するエンドポイントのリスト](#)"。

- ネットワークタイムプロトコル（NTP）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

**Google Cloud** にデータブローカーを導入するための権限が必要です

データブローカーを導入する Google Cloud ユーザに、次の権限があることを確認します。

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

サービスアカウントに必要な権限

データブローカーを導入する場合、次の権限を持つサービスアカウントを選択する必要があります。

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
- iam.serviceAccounts.signJwt
```



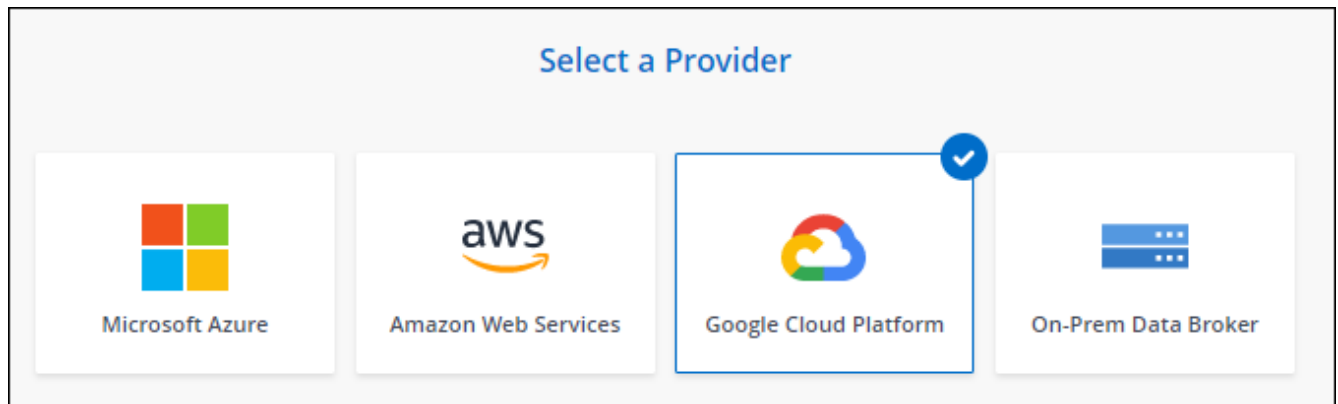
「iam.serviceAccounts.signJwt」権限が必要なのは、外部の橋本ボルトを使用するようにデータブローカーを設定する予定の場合のみです。

## データブローカーの作成

新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成するときにデータブローカーを Google Cloud にインストールする方法について説明します。

### 手順

1. [新しい同期の作成 \*] 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、[続行 \*] をクリックします。  
  
「\* データブローカーグループ \*」 ページが表示されるまで、手順を完了します。
3. [\* データブローカーグループ \*] ページで、[\* データブローカーの作成 \*] をクリックし、[Microsoft Azure\*] を選択します。



4. データブローカーの名前を入力し、[\* 続行] をクリックします。
5. メッセージが表示されたら、Google アカウントでログインします。

このフォームは Google が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

6. プロジェクトとサービスアカウントを選択し、パブリック IP アドレスを有効にするか無効にするかなど、データブローカーの場所を選択します。

パブリック IP アドレスを有効にしない場合は、次の手順でプロキシサーバーを定義する必要があります。

### Basic Settings

<b>Project</b>	<b>Location</b>
Project	Region
<div>OCCM-Dev</div>	<div>us-west1</div>
Service Account	Zone
<div>test</div>	<div>us-west1-a</div>
Select a Service Account that includes <a href="#">these permissions</a>	VPC
	<div>default</div>
	Subnet
	<div>default</div>
	Public IP
	<div>Enable</div>

7. VPC でのインターネットアクセスにプロキシが必要な場合は、プロキシの設定を指定します。

インターネットアクセスにプロキシが必要な場合は、データブローカーと同じサービスアカウントを Google Cloud で使用してプロキシを設定する必要があります。

8. データブローカーが利用可能になったら、Cloud Sync で [\* 続行 ] をクリックします。

このインスタンスの導入には、約 5 ～ 10 分かかります。Cloud Sync サービスから進捗状況を監視できます。このサービスは、インスタンスが使用可能になると自動的に更新されます。

9. ウィザードのページに入力して、新しい同期関係を作成します。

Google Cloud にデータブローカーを導入し、新しい同期関係を作成しました。このデータブローカーは、追加の同期関係とともに使用できます。

#### 他の **Google Cloud** プロジェクトでバケットを使用する権限を付与する

同期関係 Cloud Sync を作成し、ソースまたはターゲットとして Google Cloud Storage を選択すると、データブローカーのサービスアカウントに使用する権限があるバケットから選択できるようになります。デフォルトでは、これにはデータブローカーサービスアカウントと同じ `_PROJECT` に含まれるバケットが含まれます。ただし、必要な権限を指定した場合は、`_other_projects` からバケットを選択できます。

#### 手順

1. Google Cloud Platform コンソールを開き、Cloud Storage サービスをロードします。



2. 同期関係のソースまたはターゲットとして使用するバケットの名前をクリックします。
3. **[Permissions]** をクリックします
4. **[ 追加 (Add) ]** をクリックします。
5. データブローカーのサービスアカウントの名前を入力します。
6. 提供するロールを選択します [上記と同じ権限](#)。
7. **[ 保存 (Save) ]** をクリックします。

同期関係を設定するときに、そのバケットを同期関係のソースまたはターゲットとして選択できるようになりました。

#### データブローカー **VM** インスタンスの詳細

Cloud Sync は、Google Cloud に次の構成でデータブローカーを作成します。

##### マシンのタイプ

N1-standard-4

##### vCPU

4.

##### RAM

15 GB

##### オペレーティングシステム

Red Hat Enterprise Linux 7.7

##### ディスクのサイズとタイプ

20 GB HDD pd-standard

## Linux ホストへのデータブローカーのインストール

新しいデータブローカーグループを作成する場合は、オンプレミスのデータブローカーオプションを選択して、オンプレミスの Linux ホストまたはクラウド内の既存の 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。Cloud Sync ではインストールプロセスがガイドされますが、インストールの準備に役立つように、このページの要件と手順が繰り返されています。

#### Linux ホストの要件

- \* オペレーティング・システム \* :
  - CentOS 7.0、7.7、および 8.0
  - CentOS ストリームはサポートされていません。
  - Red Hat Enterprise Linux 7.7 および 8.0
  - Ubuntu Server 20.04 LTS の場合は

- SUSE Linux Enterprise Server 15 SP1

コマンド 'yum update all' は 'データ・ブローカーをインストールする前に' ホスト上で実行する必要があります

Red Hat Enterprise Linux システムは、Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、システムはインストール中に必要なサードパーティソフトウェアをアップデートするためのリポジトリにアクセスできません。

- \* RAM \* : 16GB
- \* CPU \* : 4 コア
- \* 空きディスク容量 \* : 10 GB
- \* SELinux \* : 無効にすることをお勧めします ["SELinux"](#) ホスト。

SELinux では、データブローカーソフトウェアの更新をブロックし、通常運用に必要なエンドポイントにデータブローカーがアクセスできないようにするポリシーが適用されます。

## ネットワーク要件

- Linux ホストは、ソースとターゲットに接続されている必要があります。
- ファイルサーバが Linux ホストにエクスポートへのアクセスを許可している必要があります。
- AWS へのアウトバウンドトラフィック（データブローカーは常に Amazon SQS サービスと通信）を処理するために、Linux ホストでポート 443 が開いている必要があります。
- ネットワークタイムプロトコル（NTP）サービスを使用するように、ソース、ターゲット、およびデータブローカーを設定することを推奨します。3 つのコンポーネント間の時間差は 5 分を超えないようにしてください。

## AWS へのアクセスを有効化

S3 バケットを含む同期関係でデータブローカーを使用する場合は、Linux ホストで AWS にアクセスする準備をしておく必要があります。データブローカーをインストールする際、プログラム経由のアクセス権と特定の権限を持つ AWS ユーザに対して AWS キーを提供する必要があります。

### 手順

1. を使用して、IAM ポリシーを作成します ["ネットアップが提供するポリシーです"](#)

["AWS の手順を表示します。"](#)

2. プログラムによるアクセス権を持つ IAM ユーザを作成します。

["AWS の手順を表示します。"](#)

データブローカーソフトウェアをインストールするときに AWS キーを指定する必要があるため、必ず AWS キーをコピーしてください。

## Google Cloud へのアクセスを有効にします

Google Cloud Storage バケットを含む同期関係でデータブローカーを使用する場合は、Google Cloud アクセ

ス用の Linux ホストを準備しておく必要があります。データブローカーをインストールする場合、特定の権限を持つサービスアカウントにキーを提供する必要があります。

#### 手順

1. Storage Admin の権限がない Google Cloud サービスアカウントを作成します。
2. JSON 形式で保存されたサービスアカウントキーを作成します。

["Google Cloud の手順をご覧ください"](#)

このファイルには、少なくとも「project\_id」、「private\_key」、および「client\_email」というプロパティを含める必要があります。



キーを作成すると、ファイルが生成され、マシンにダウンロードされます。

3. JSON ファイルを Linux ホストに保存します。

#### Microsoft Azure へのアクセスを有効にしています

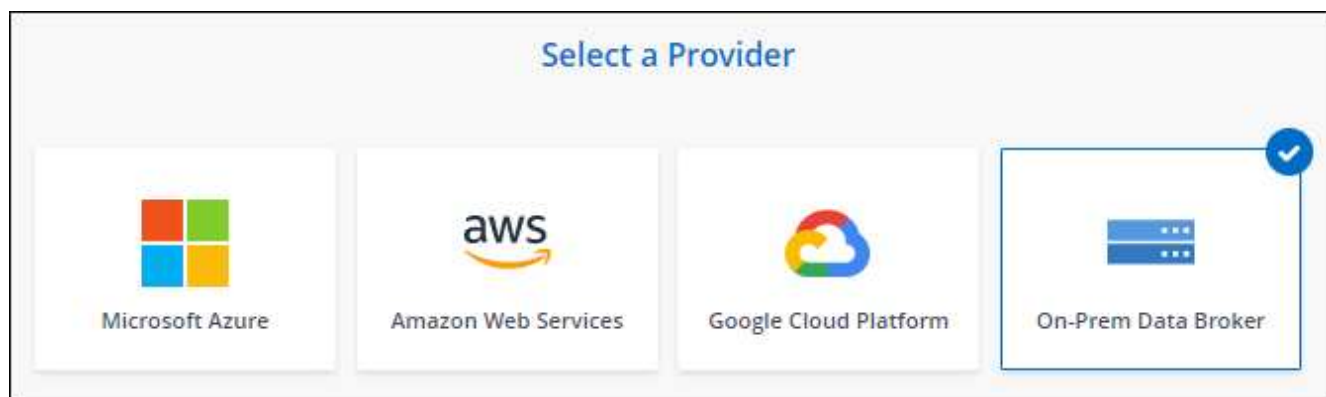
Azure へのアクセスは、関係ごとに定義されます。そのためには、同期関係ウィザードでストレージアカウントと接続文字列を指定します。

#### データブローカーのインストール

同期関係を作成するときに、Linux ホストにデータブローカーをインストールできます。

#### 手順

1. [新しい同期の作成 \*] 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、[続行 \*] をクリックします。
- 「\* データブローカーグループ \*」ページが表示されるまで、手順を完了します。
3. [\* データブローカーグループ \*] ページで、[\* データブローカーの作成 \*] をクリックし、[\* オンプレミスのデータブローカー \*] を選択します。



このオプションには「\*\_オンプレミス\_データブローカー\*」というラベルが付けられていますが、オンプレミスまたはクラウド上の Linux ホストにも該当します。

4. データブローカーの名前を入力し、[\* 続行] をクリックします。

手順ページがすぐにロードされます。これらの手順に従う必要があります。インストーラをダウンロードするための固有のリンクが含まれています。

5. 手順ページで次の手順を実行します。

- a. 「\*AWS\*」、「\*Google Cloud\*」、またはその両方へのアクセスを有効にするかどうかを選択します。
- b. インストールオプションとして、\*プロキシなし\*、\*プロキシサーバーを使用\*、または\*認証付きプロキシサーバーを使用\*を選択します。
- c. データブローカーをダウンロードしてインストールするには、コマンドを使用します。

次の手順では、使用可能な各インストールオプションの詳細を示します。インストールオプションに基づいて正確なコマンドを取得するには、手順ページを参照してください。

d. インストーラをダウンロードします。

- プロキシなし：

```
curl <uri>-o data_broker_installer.sh
```

- プロキシサーバを使用：

```
curl <uri>-o data_broker_installer.sh -x <proxy_host>:<proxy_port>
```

- プロキシサーバで認証を使用する：

```
curl <uri>-o data_broker_installer.sh -x  
<proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
```

#### URI

Cloud Sync の指示ページにインストールファイルの URI が表示され、オンプレミスのデータブローカーを導入するプロンプトに従ってロードされます。この URI はリンクが動的に生成され、1 回しか使用できないため、ここでは繰り返し使用されません。 [Cloud Sync から URI を取得するには、次の手順を実行します。](#)

e. スーパーユーザーに切り替え、インストーラを実行可能にしてソフトウェアをインストールします。



以下に示す各コマンドには、AWS アクセスと Google Cloud アクセスのパラメータが含まれています。インストールオプションに基づいて正確なコマンドを取得するには、手順ページを参照してください。

- プロキシ構成なし：

```
「 sudo -s chmod +x data_broker_installer.sh 」 / data_broker_installer.sh - A <AWS_access_key>  
-s <AWS_secret_key> -g <absolute_path-to-the_json ファイル>
```

- プロキシ設定：

```
「 sudo -s chmod +x data_broker_installer.sh 」 / data_broker_installer.sh - A <AWS_access_key>  
-s <AWS_secret_key> -g <absolute_path-to-the_json ファイル> -h <proxy_host> -p  
<proxy_port>
```

- 認証を使用したプロキシ設定：

```
「 sudo -s chmod +x data_broker_installer.sh 」 / data_broker_installer.sh - A <AWS_access_key>  
-s <AWS_secret_key> -g <absolute_path-to-the _json _file> -h <proxy_host> -p <proxy_port> -u  
<proxy_username> -w <proxy_password>
```

### **AWS キー**

これらはユーザに適切なキーです 準備しておきます [次の手順を実行します](#)。AWS のキーはデータブローカーに格納され、オンプレミスネットワークやクラウドネットワークで実行されます。ネットアップでは、データブローカー以外でキーを使用していません。

### **JSON ファイル**

この JSON ファイルにサービスアカウントが含まれています 準備しておく必要があるキー [次の手順を実行します](#)。

6. データブローカーが利用可能になったら、Cloud Sync で [\* 続行] をクリックします。
7. ウィザードのページに入力して、新しい同期関係を作成します。

# 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。

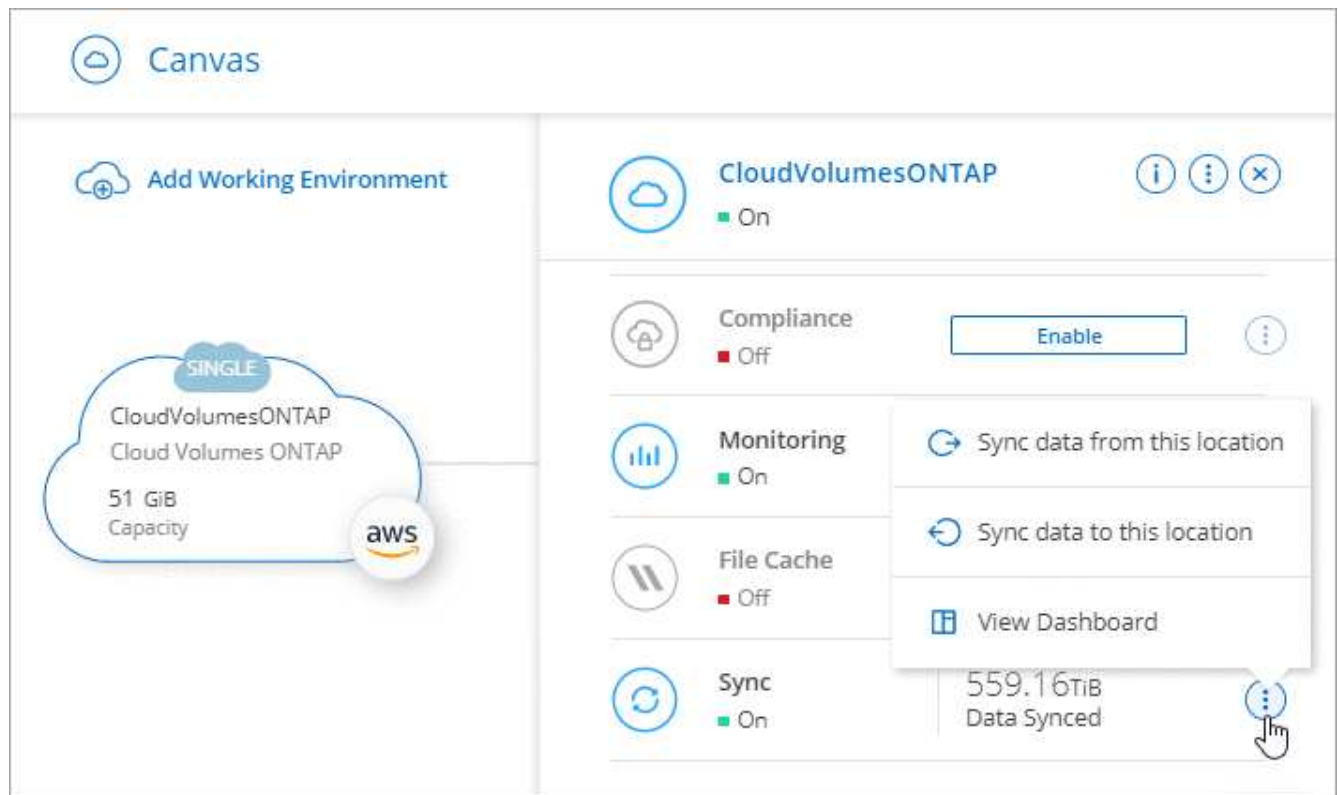
### 特定のタイプの作業環境の同期関係を作成します

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。



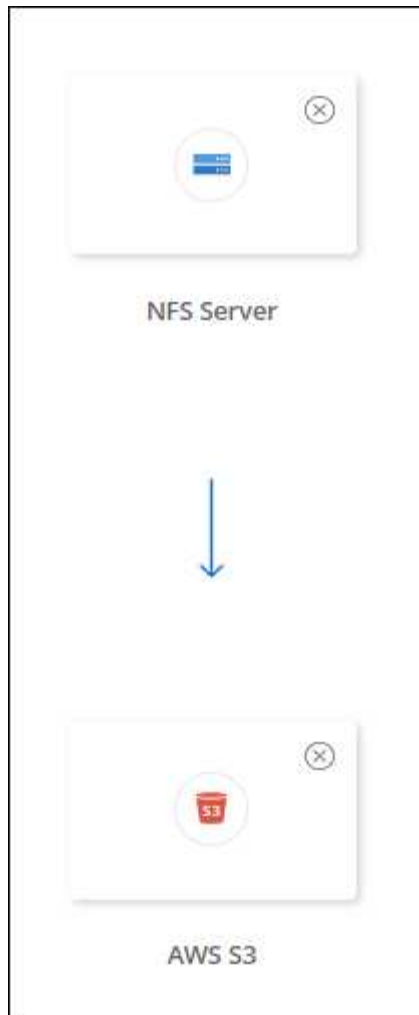
5. この場所から \* データを同期 \* または \* この場所へのデータの同期 \* を選択し、プロンプトに従って同期関係を設定します。

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。



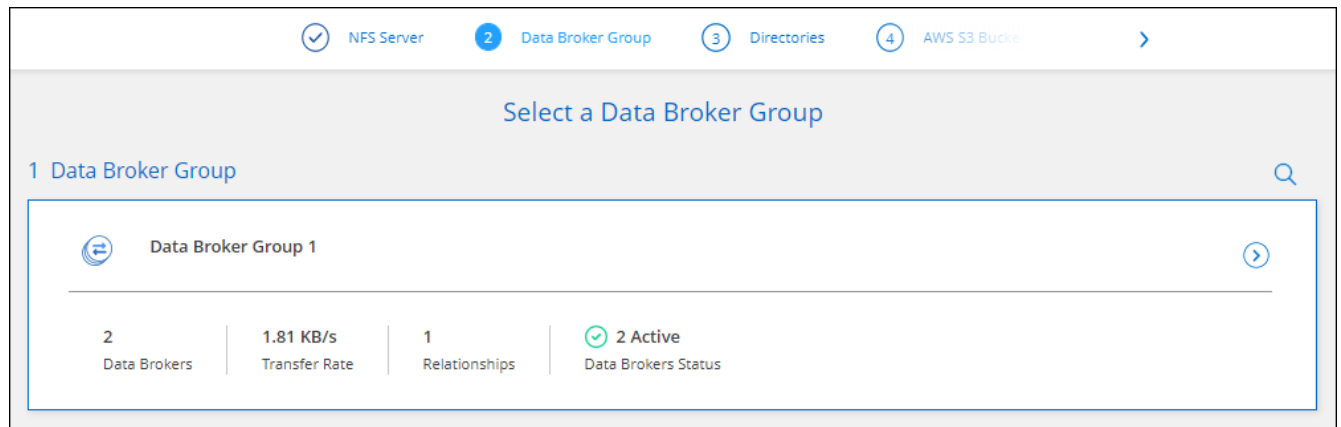
3. NFS Server \* ページで、AWS と同期する NFS サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
4. **[Data Broker Group]** ページで、プロンプトに従って AWS 、 Azure 、または Google Cloud Platform にデータブローカー仮想マシンを作成するか、データブローカーソフトウェアを既存の Linux ホストにインストールします。

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。





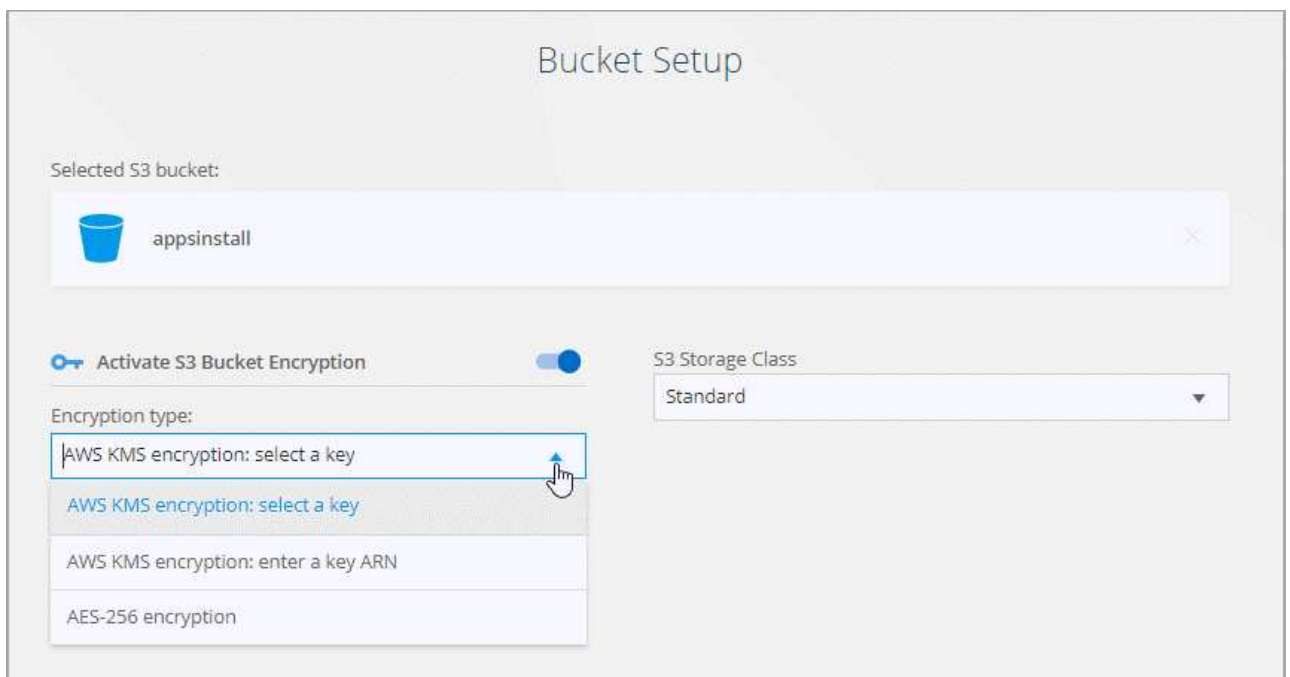
6. [Directories] ページで、最上位のディレクトリまたはサブディレクトリを選択します。

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。

#### 継続的同期

初期データ同期が完了すると、Cloud Sync はソースS3バケットで変更をリスンし、ターゲットへの変更が発生した場合はその変更を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バケットからS3、Google Cloud Storage、Azure BLOBストレージ、StorageGRID、またはIBMストレージに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。
- サイズでフィルタは、コピーイベントに対してのみアクティブになります（削除イベントに対して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。

#### 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

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。

< AWS S3 Bucket Settings 6 Tags/Metadata 7 Review

### Relationship Tags

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.

☒ Save on Object's Tags ☐ Save On Object's Metadata

Tag Key	Tag Value
Up to 128 characters	Up to 256 characters

+ Add Relationship Tag 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す。

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。

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags
 ☒ Save On Object's Metadata

Metadata Key: Up to 128 characters

Metadata Value: Up to 256 characters

+ Add Relationship Metadata

Optional Field | [Up to 5]

#### 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

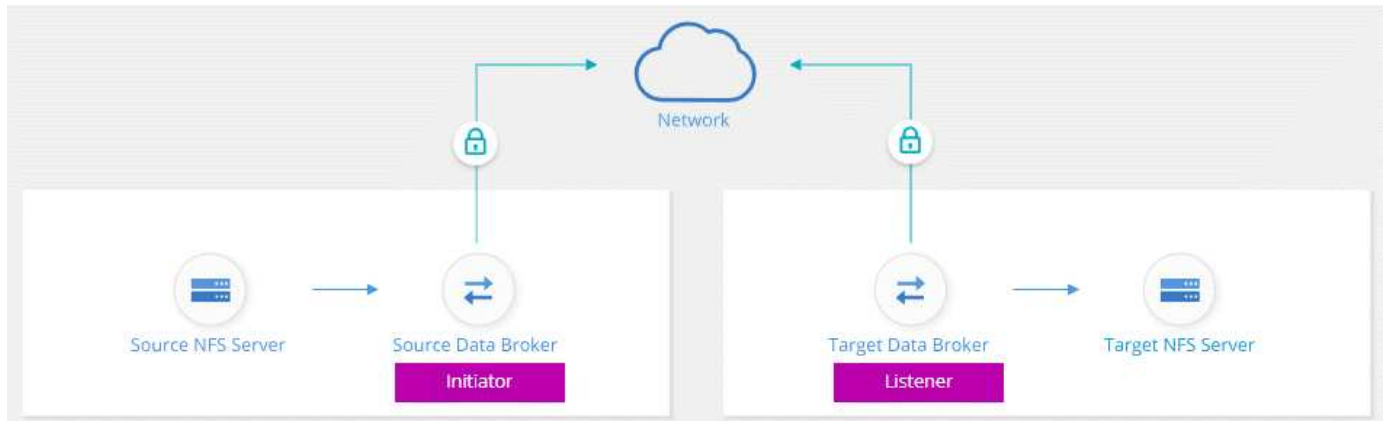
## 転送中のデータ暗号化を使用した **NFS** データの同期

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

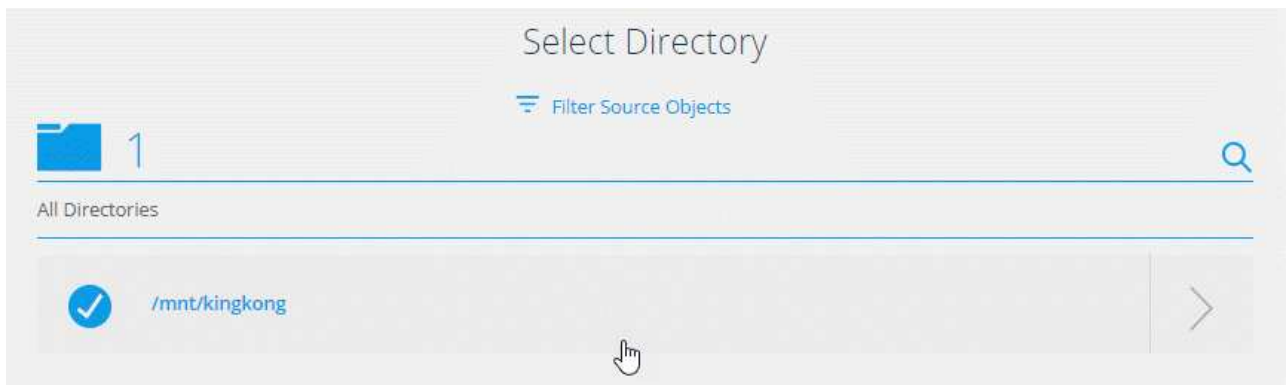
1. [新しい同期の作成 \*] をクリックします。
2. NFS サーバ \* をソースとターゲットの場所にドラッグアンドドロップするか、\* Azure NetApp Files \* をソースとターゲットの場所にドラッグアンドドロップして、\* はい \* を選択して転送中のデータ暗号化を有効にします。
3. プロンプトに従って関係を作成します。
  - a. \* NFS サーバ \* / \* Azure NetApp Files \* : NFS のバージョンを選択し、新しい NFS ソースを指定するか、既存のサーバを選択します。
  - b. \* データブローカー機能の定義 \*: 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。


**Select a Provider**




Microsoft Azure



Amazon Web Services



Google Cloud Platform

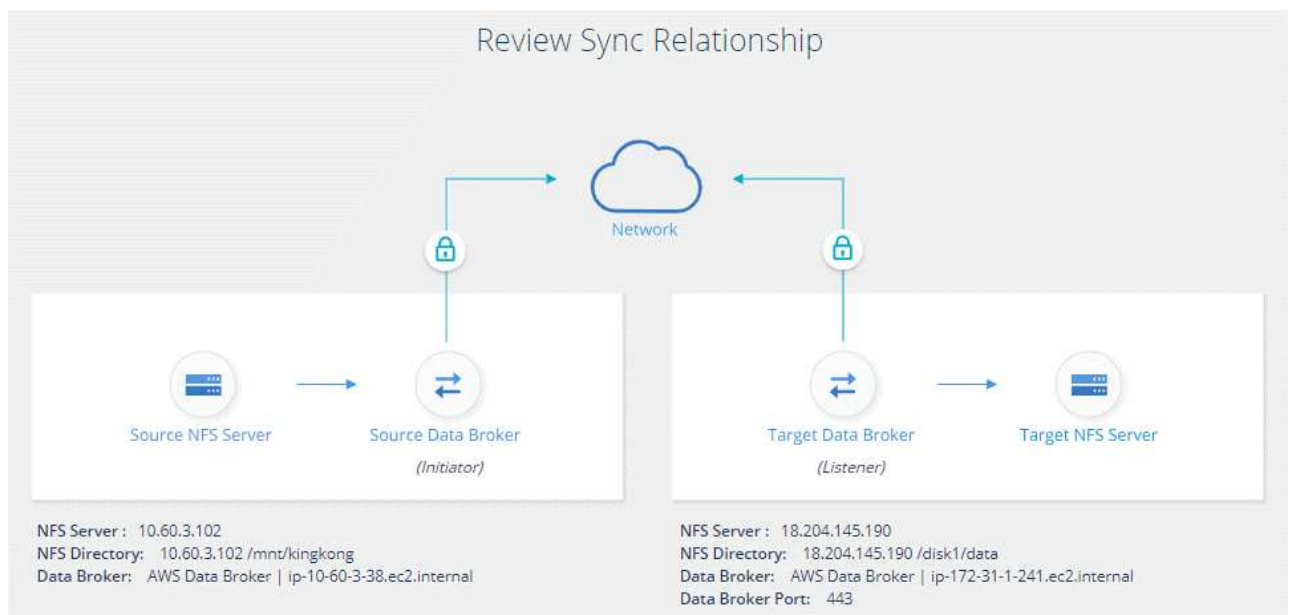


On-Prem Data Broker

Data Broker Name

Port

- 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。

## 外部の橋本社ポ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、外部の橋本社ポ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、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。ヴォ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。

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、外部ヴォー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

ヴォ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 を設定してヴォ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)

#### 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。

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"
    }
  }
}
```



# 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。

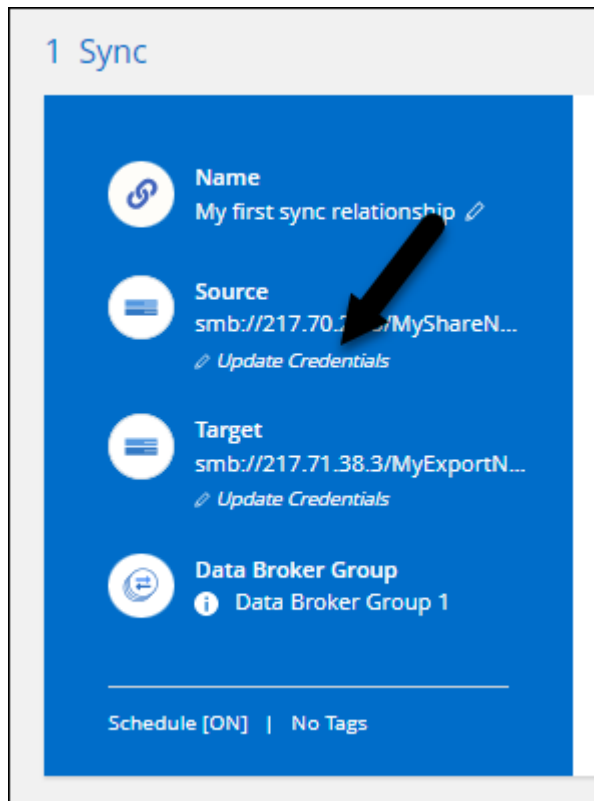
## クレデンシャルを更新し

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

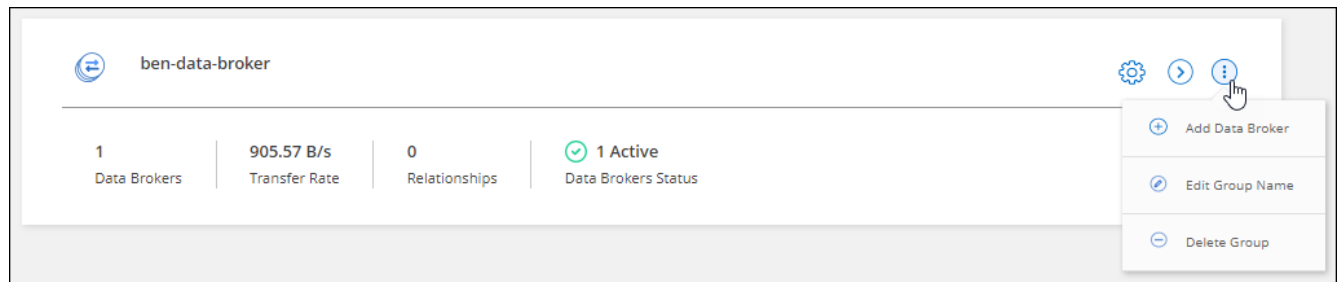
1. [ \* 同期 ] > [ データブローカーの管理 \* ] をクリックします。
2. [ 新しいデータブローカーの追加 ] をクリックします。
3. プロンプトに従ってデータブローカーを作成します。

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。

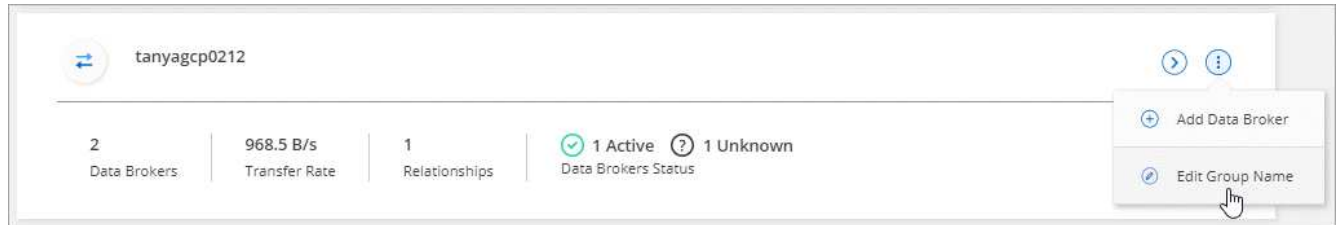
- ["AWS にデータブローカーを作成"](#)
- ["Azure でデータブローカーを作成"](#)
- ["Google Cloud でデータブローカーを作成"](#)
- ["Linux ホストへのデータブローカーのインストール"](#)

## 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。

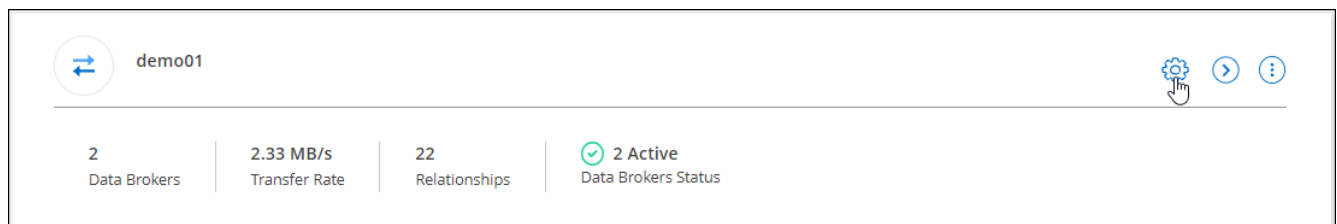
## ユニファイド構成をセットアップする

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。

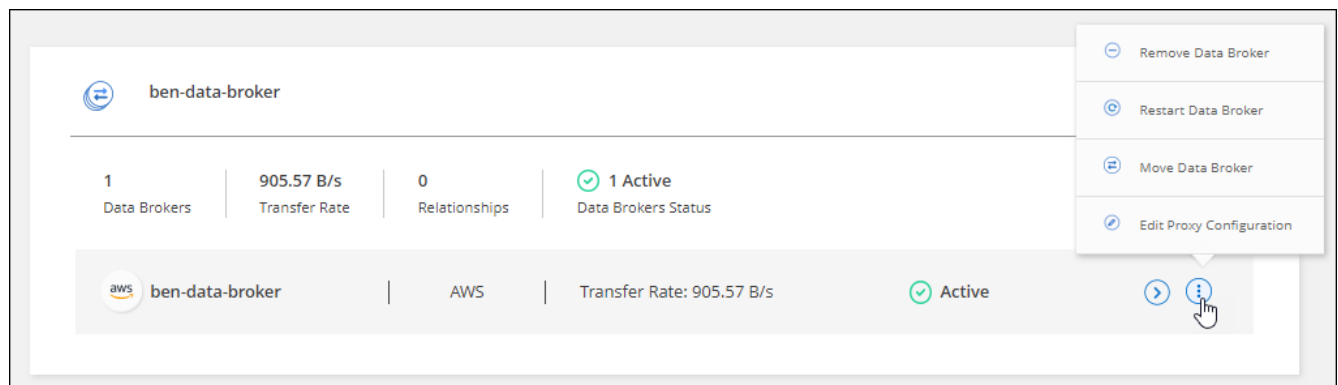
たとえば、データブローカーで同期関係が管理されなくなった場合、同期関係を管理している別のグループに簡単に移動できます。

### 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。

tanyagcp0212   GCP   Transfer Rate: 968.5 B/s   Active				
<b>Information</b>	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project ID
<b>Network</b>	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
<b>Software</b>	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
<b>Hardware</b>	4 Available CPUs	62.22 MB Available RAM		
<b>Configuration</b>	50 Scanner Concurrency	4 Scanner CPUs	50 Transferrer Concurrency	4 Transferrer CPUs

## 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。

tanyagcp0212   GCP   Transfer Rate: 968.5 B/s   Active				
tanya1   ONPREM   Transfer Rate: 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

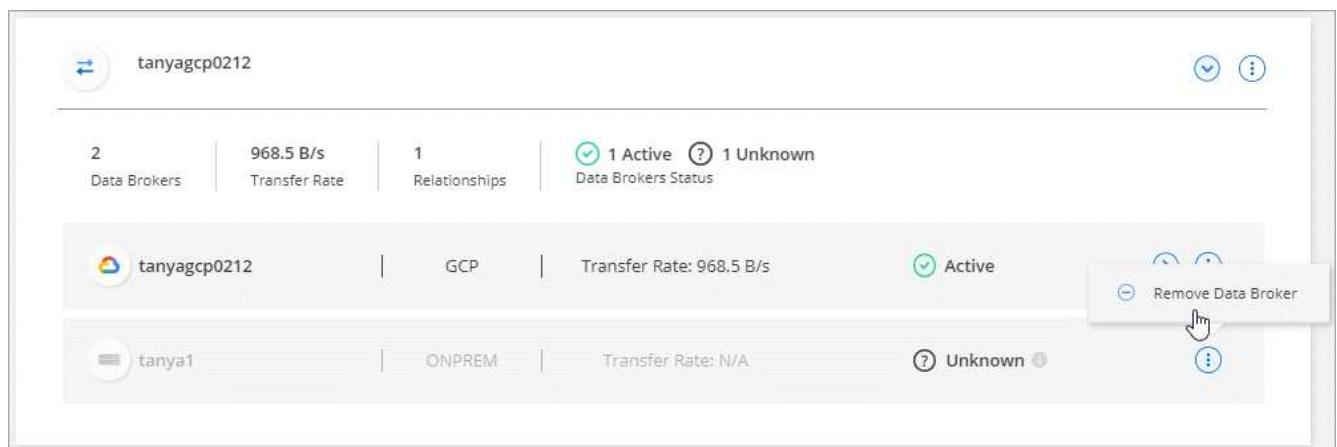
データブローカーが不要になった場合や初期導入に失敗した場合は、グループから削除することができます。この操作では、データブローカーが Cloud Sync のレコードから削除されます。データブローカーとその他のクラウドリソースについては、手動で削除する必要があります。

### 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

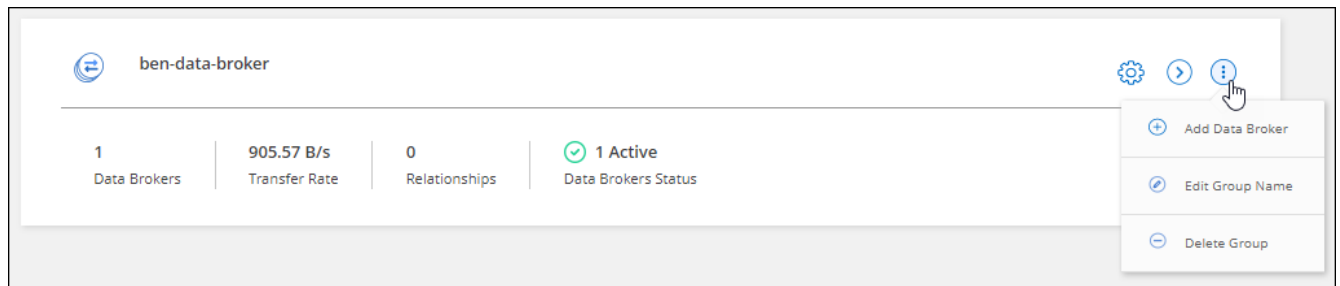
## データブローカーグループを削除

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。

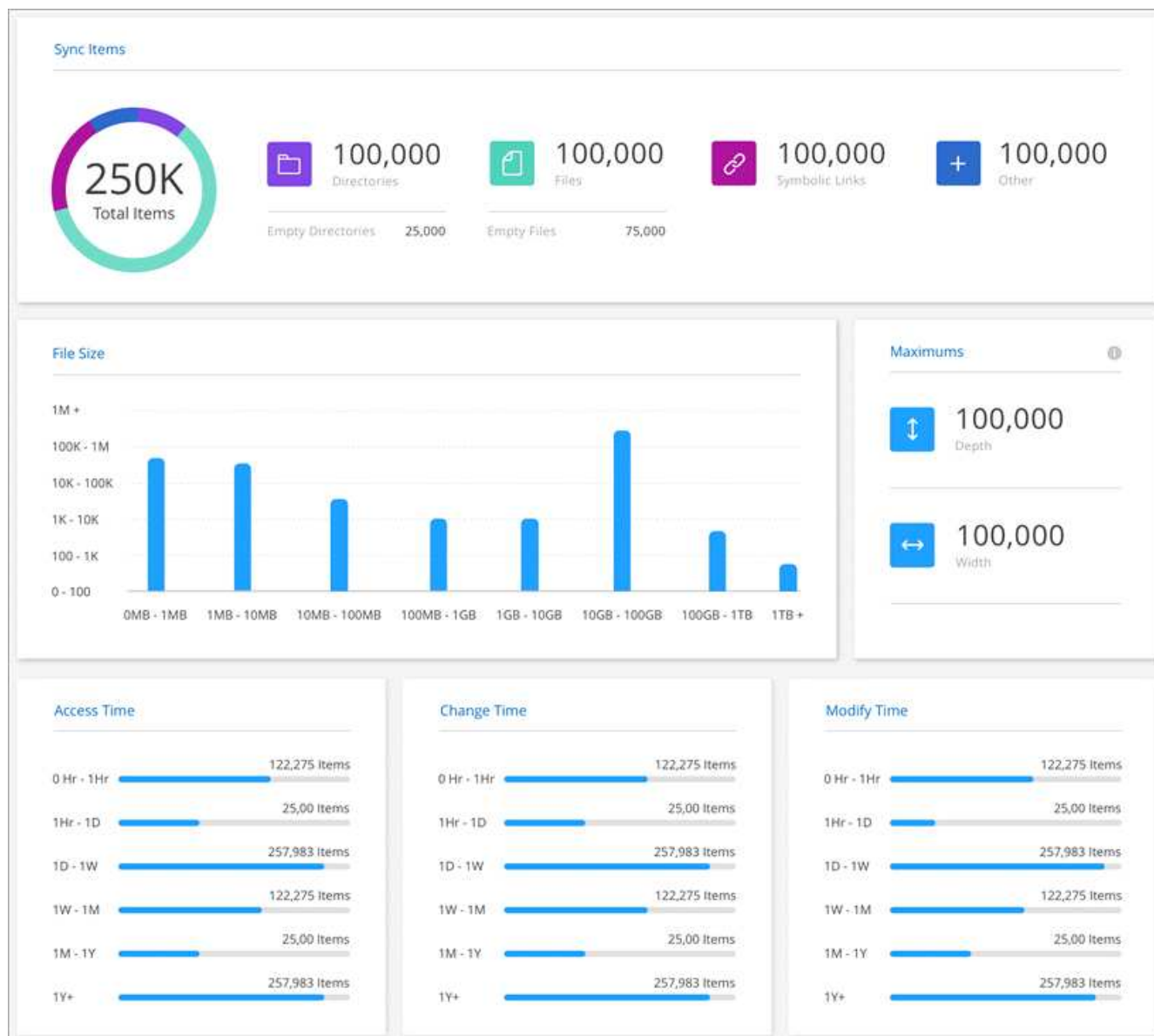
同期関係のそれぞれのパス（ソースまたはターゲット）が表形式で表示されます。

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。

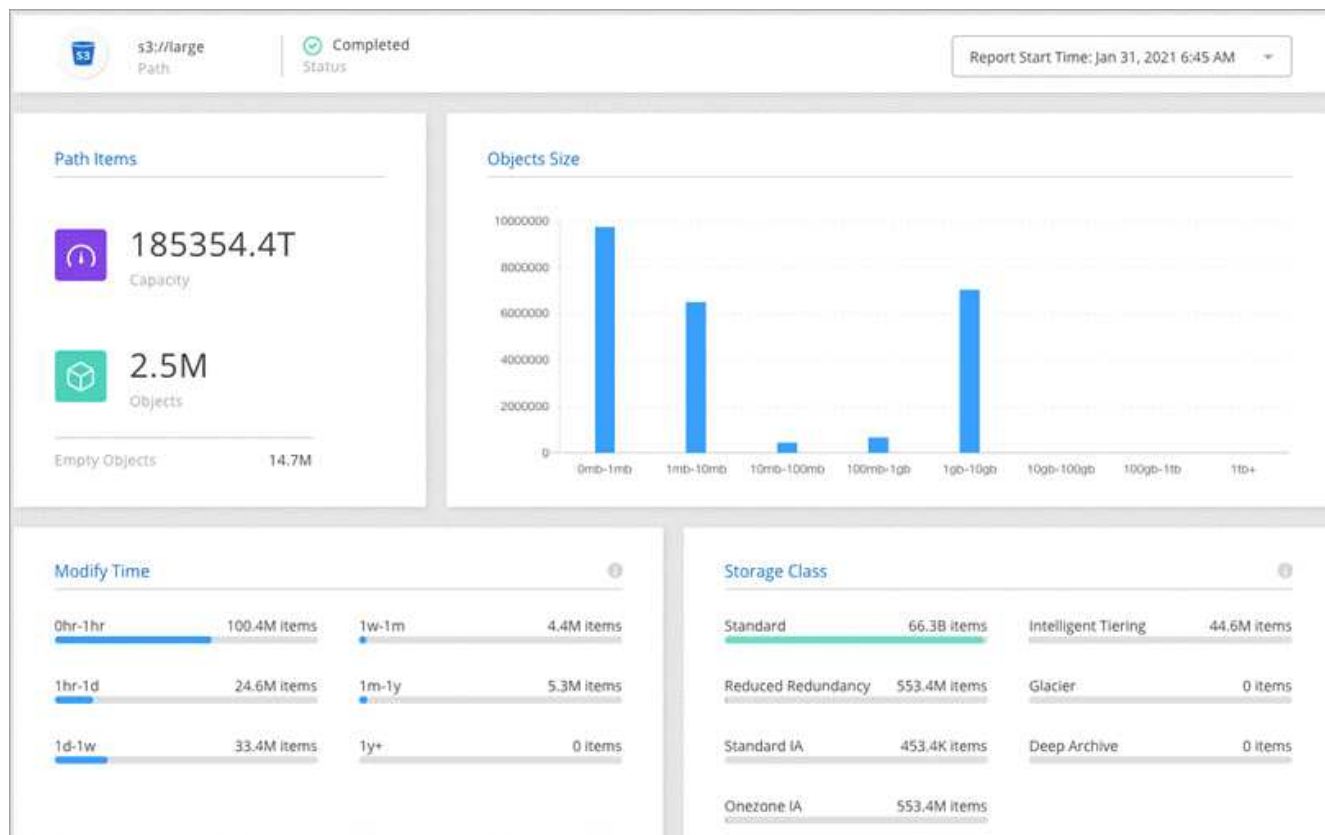
3. レポートの準備ができたなら、アクションメニューをクリックし、\* 表示 \* を選択します。

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。

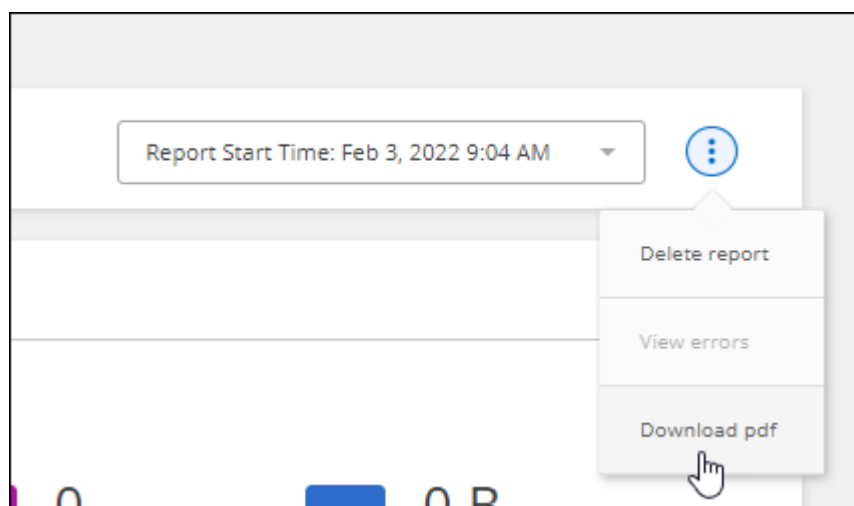


## レポートのダウンロード

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

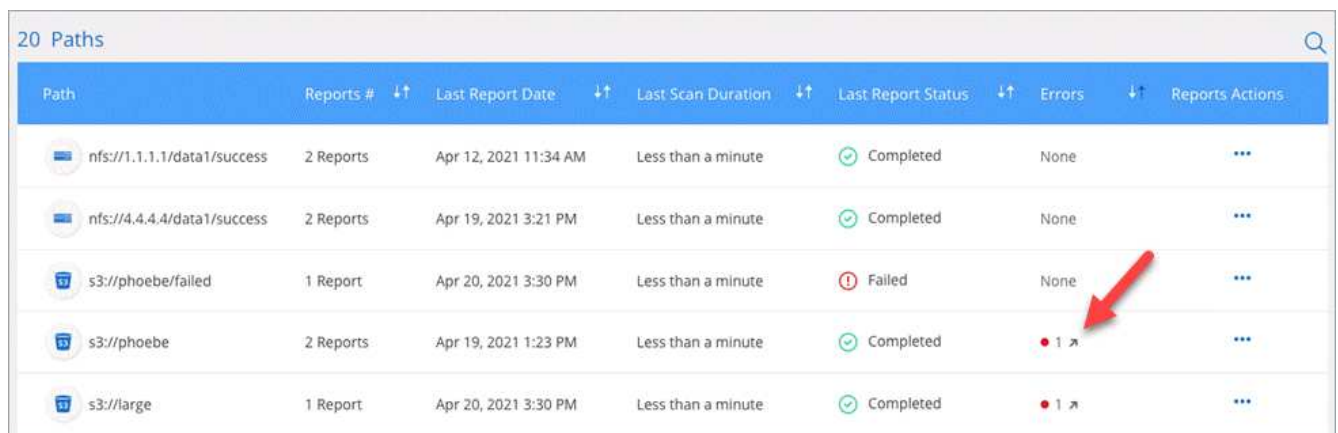
Paths テーブルは、最新のレポートにエラーがあるかどうかを示します。エラーは、Cloud Sync がパスのスキャン時に直面した問題を示します。

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。

# クラウド同期 API

Web UI から使用できる Cloud Sync 機能は、RESTful API から也可以使用できます。

## はじめに

Cloud Sync API を使用するには、ユーザトークンと Cloud Central アカウント ID を取得する必要があります。API 呼び出しを行うときは、トークンとアカウント ID を Authorization ヘッダーに追加する必要があります。

### 手順

1. NetApp Cloud Central からユーザトークンを取得します。

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
  "username": "<user_email>",
  "scope": "profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```

2. Cloud Central アカウント ID を取得します。

```
GET https://api.cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

この API は、次のような応答を返します。

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. 各 API 呼び出しの Authorization ヘッダーにユーザトークンとアカウント ID を追加します。

◦ 例 \*

次の例は、Microsoft Azure でデータブローカーを作成するための API 呼び出しを示しています。<user\_token> と <accountId> は、前の手順で取得したトークンと ID で置き換えます。

```
POST https://api.cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

トークンの有効期限が切れた場合はどうすればよいですか。

NetApp Cloud Central のユーザトークンの有効期限が切れています。トークンを更新するには、手順 1 から API を再度呼び出す必要があります。

API 応答には、トークンの有効期限を示す「expires\_in」フィールドが含まれています。

## API リファレンス

各 Cloud Sync API のドキュメントは、から入手できます <https://api.cloudsync.netapp.com/docs>。

## List API の使用

list API は非同期 API であるため、結果はすぐには返されません (たとえば 'get/data-colders/{id}/list-nfs-export-folders' と 'get/data-colders/{id}/list-s3-bas' など) サーバからの応答は、HTTP ステータス 202 だけです。実際の結果を得るには 'get/mmessaging/client' API を使用する必要があります

手順

1. 使用するリスト API を呼び出します。
2. オペレーションの結果を表示するには 'get/mmessaging/client' API を使用します
3. 受信した ID を付加して、同じ API を使用します。「  
get/http://api.cloudsync.netapp.com/api/messaging/client?last=<id\_from\_step\_2>」

ID は 'get/mmessaging/client' API を呼び出すたびに更新されることに注意してください

◦ 例 \*

'list-s3-buckets' API を呼び出すと、結果はすぐには返されません

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

その結果、HTTP ステータスコード 202 が生成されます。これは、メッセージが受け入れられたが、まだ処理されていないことを意味します。

操作の結果を取得するには、次の API を使用する必要があります。

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

結果は、ID フィールドを含む 1 つのオブジェクトを持つ配列になります。ID フィールドは、サーバが最後に送信したメッセージを表します。例：

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

次に、受信した ID を使用して、次の API コールを実行します。

```
GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

結果はメッセージの配列です。各メッセージ内にはペイロードオブジェクトがあります。ペイロードオブジェクトは、動作の名前（キー）とその結果（値）で構成されます。例：

```
[
  {
    "payload": {
      "list-s3-buckets": [
        {
          "tags": [
            {
              "Value": "100$",
              "Key": "price"
            }
          ],
          "region": {
            "displayName": "US West (Oregon)",
            "name": "us-west-2"
          },
          "name": "small"
        }
      ]
    },
    "header": {
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
      "clientId": "5beb032f548e6e35f4ed1ba9",
      "agentId": "5bed61f4489fb04e34a9aac6"
    },
    "id": "5802"
  }
]
```



# 概念

## ライセンスの概要

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。

### Marketplace サブスクリプション

AWS または Azure から Cloud Sync サービスに加入すると、1 時間あたりの料金を支払うか、年間の料金を支払うことができます。"[AWS または Azure でサブスクライブできます](#)"、どこに課金するかによって異なります。

#### 時間単位のサブスクリプション

時間単位の従量課金制サブスクリプションでは、作成した同期関係の数に基づいて 1 時間ごとに課金されます。

- "[Azure で価格を表示します](#)"
- "[AWS で従量課金制の価格を確認できます](#)"

#### 年間サブスクリプション

年間サブスクリプションでは、事前に支払う 20 の同期関係のライセンスが提供されます。同期関係を 20 個以上に設定し、AWS から登録した場合は、追加の関係分を 1 時間単位で支払います。

"[AWS の年間価格を確認します](#)"

## ネットアップのライセンス

同期関係のコストを事前に支払うもう 1 つの方法は、ネットアップからライセンスを直接購入することです。各ライセンスでは、最大 20 の同期関係を作成できます。

これらのライセンスは、AWS または Azure サブスクリプションで使用できます。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。

"[ライセンスを購入して Cloud Sync に追加する方法について説明します。](#)"

### ライセンス条項

Cloud Sync サービスに Bring Your Own License (BYOL) を購入されたお客様は、ライセンス資格に関連する制限事項に注意する必要があります。

- お客様は、納品日から 1 年を超えない期間、BYOL ライセンスを利用できます。
- お客様は、BYOL ライセンスを利用して、ソースとターゲットの間の合計 20 個の個別接続を確立するこ

とができます（それぞれ「同期関係」）。

- お客様の利用資格は、お客様が 20 件の同期関係の制限に達したかどうかに関係なく、1 年間のライセンス期間の終了時に期限切れとなります。
- お客様がライセンスの更新を選択した場合、以前のライセンス付与から関連付けられた未使用の同期関係は、ライセンスの更新には引き継がれません。

## データのプライバシー

ネットアップには、Cloud Sync サービスの使用中に指定したクレデンシャルへのアクセス権がありません。クレデンシャルは、ネットワーク内のデータブローカーマシンに直接保存されます。

選択した設定によっては、新しい関係を作成するときに Cloud Sync によってクレデンシャルの入力が求められる場合があります。たとえば、SMB サーバを含む関係を設定する場合や、AWS にデータブローカーを導入する場合などです。

これらのクレデンシャルは、常にデータブローカー自体に直接保存されます。データブローカーは、オンプレミスでもクラウドアカウントでも、ネットワーク上のマシンに配置されます。クレデンシャルがネットアップに提供されることはありません。

クレデンシャルは、HanCorp Vault を使用してデータブローカーマシンでローカルに暗号化されます。

## Cloud Sync テクニカル FAQ

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

### はじめに

次の質問は、クラウド同期の導入に関連しています。

#### クラウド同期の仕組み

Cloud Sync では、ネットアップデータブローカーソフトウェアを使用して、ソースからターゲット（「a\_sync relationship\_」）にデータを同期します。

データブローカーグループは、ソースとターゲットの同期関係を制御します。同期関係を設定すると、Cloud Sync はソースシステムを分析し、選択したターゲットデータにプッシュするために複数のレプリケーションストリームに分割します。

最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。

#### 14 日間の無料トライアルはどのように機能しますか？

14 日間の無料トライアルは、Cloud Sync サービスにサインアップすると開始されます。14 日間にわたって作成した Cloud Sync 関係については、ネットアップが料金を支払う必要はありません。ただし、導入するデータブローカーのすべてのリソース料金は引き続き適用されます。

クラウド同期のコストはいくらですか。

Cloud Sync の使用に関連するコストには、サービス料金とリソース料金の 2 種類があります。

- サービス料金 \*

従量課金制の場合、Cloud Sync サービス料金は、作成する同期関係の数に基づいて 1 時間ごとに課金されます。

- ["AWS で従量課金制の価格を確認できます"](#)
- ["AWS の年間価格を確認します"](#)
- ["Azure で価格を表示します"](#)

Cloud Sync ライセンスは、ネットアップの担当者からも入手できます。各ライセンスでは、12 カ月間で 20 の同期関係が有効になります。

["ライセンスの詳細については、こちらをご覧ください。"](#)



Cloud Volumes Service と Azure NetApp Files には Cloud Sync 関係が無償で用意されています。

- リソース料金 \*

リソース料金は、クラウドでデータブローカーを実行するためのコンピューティングコストとストレージコストに関連しています。

**Cloud Sync** の料金はどのように設定されますか

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 から購読することです。AWS または Azure を使用すると、従量課金制または年払いが可能になります。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。

クラウドの外部でクラウド同期を使用できますか。

はい。クラウド同期は非クラウドアーキテクチャで使用できます。ソースとターゲットはオンプレミスに配置できるため、データブローカーソフトウェアを使用することもできます。

Cloud Sync をクラウドの外部で使用する場合、次の点に注意してください。

- データブローカーグループには、Cloud Sync サービスと通信するためのインターネット接続が必要です。
- ネットアップからライセンスを直接購入しない場合は、従量課金制の Cloud Sync サービスを利用する AWS または Azure のアカウントが必要です。

**Cloud Sync** へのアクセス方法を教えてください。

Cloud Sync は、Cloud Manager の \* Sync \* タブで使用できます。

データブローカーグループとは何ですか？

各データブローカーは、データブローカーグループに属しています。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が向上します。

## サポートされているソースとターゲット

同期関係でサポートされているソースとターゲットに関連する次の質問。

**Cloud Sync** がサポートするソースとターゲットはどれですか。

クラウド同期では、さまざまな種類の同期関係がサポートされています。 "[リスト全体を表示します。](#)"。

クラウド同期でサポートされる **NFS** と **SMB** のバージョンを教えてください。

クラウド同期では、NFS バージョン 3 以降、SMB バージョン 1 以降がサポートされます。

"[同期の要件の詳細については、こちらをご覧ください。](#)"。

**Amazon S3** がターゲットである場合、特定の **S3** ストレージクラスにデータを階層化できますか。

はい。AWS S3 がターゲットである場合は、特定の S3 ストレージクラスを選択できます。

- 標準（これがデフォルトクラス）
- インテリジェント階層化
- 標準的なアクセス頻度は低い
- 1 回のアクセスではほとんど発生しません
- 氷河
- Glacier Deep Archive

**Azure BLOB** ストレージのストレージ階層について教えてください。

BLOB コンテナがターゲットの場合は、特定の Azure BLOB ストレージ階層を選択できます。

- ホットストレージ
- 優れたストレージ

**Google Cloud** のストレージ階層をサポートしていますか？

はい。Google Cloud Storage バケットがターゲットの場合は、特定のストレージクラスを選択できます。

- 標準
- ニアライン
- コールドライン（Coldline）
- Archive サービスの略

## ネットワーキング

次の質問は、クラウド同期のネットワーク要件に関連しています。

クラウドの同期に必要なネットワーク要件は何ですか？

Cloud Sync 環境では、選択したプロトコルまたはオブジェクトストレージ API（Amazon S3、Azure Blob、IBM Cloud Object Storage）を使用して、データブローカーグループがソースとターゲットに接続されている必要があります。

また、データブローカーグループには、Cloud Sync サービスと通信して他のいくつかのサービスやリポジトリに接続するために、ポート 443 経由のアウトバウンドインターネット接続が必要です。

詳細： ["ネットワーク要件を確認します。"](#)。

データブローカーでプロキシサーバを使用できますか。

はい。

Cloud Sync は、ベーシック認証を使用するかどうかに関係なく、プロキシサーバをサポートします。データブローカーの導入時にプロキシサーバを指定した場合、データブローカーからの HTTP および HTTPS トラフィックはすべてプロキシ経由でルーティングされます。NFS や SMB などの HTTP 以外のトラフィックは、プロキシサーバ経由でルーティングできないことに注意してください。

プロキシサーバの唯一の制限は、NFS または Azure NetApp Files 同期関係で転送中のデータ暗号化を使用する場合です。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。

## データの同期

次の質問は、データ同期の仕組みに関連しています。

同期はどのくらいの頻度で行われますか。

デフォルトのスケジュールは、毎日の同期に設定されています。初期同期化の後、次の操作を実行できます。

- 同期スケジュールを、希望する日数、時間数、分数に変更します
- 同期スケジュールを無効にします
- 同期スケジュールを削除します（データは失われません。同期関係のみが削除されます）。

最小同期スケジュールは何ですか？

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。

データブローカーグループは、ファイルの同期に失敗したときに再試行しますか。またはタイムアウトしますか？

データブローカーグループは、1 つのファイルの転送が失敗してもタイムアウトしません。代わりに、データブローカーグループは、ファイルをスキップする前に 3 回再試行します。再試行値は、同期関係の設定で設定できます。

["同期関係の設定を変更する方法について説明します。"](#)。

非常に大規模なデータセットがある場合はどうすればよいですか。

1 つのディレクトリに 60 万以上のファイルが含まれている場合は、データブローカーグループを設定してペイロードを処理できるように、mailto : [ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com) [ お問い合わせ ] をご利用ください。データブローカーグループにメモリを追加しなければならない場合があります。

マウントポイント内のファイルの総数に制限はありません。上位ディレクトリやサブディレクトリの階層のレベルに関係なく、600、000 以上のファイルを含む大規模なディレクトリには、追加のメモリが必要です。

## セキュリティ

セキュリティに関する次の質問

クラウドの同期は安全ですか？

はい。すべての Cloud Sync サービスのネットワーク接続には、を使用します "[Amazon Simple Queue Service \(SQS\)](#)"。

データブローカーグループと Amazon S3、Azure Blob、Google Cloud Storage、IBM Cloud Object Storage の間の通信は、すべて HTTPS プロトコルを使用して行われます。

オンプレミス（ソースまたはデスティネーション）システムで Cloud Sync を使用している場合、推奨される接続オプションは次のとおりです。

- AWS Direct Connect、Azure ExpressRoute、または Google Cloud Interconnect 接続。インターネット経由ではない（指定したクラウドネットワークとのみ通信可能）
- オンプレミスゲートウェイデバイスとクラウドネットワーク間の VPN 接続
- S3 バケット、Azure BLOB ストレージ、または Google クラウドストレージを使用した安全なデータ転送のために、Amazon Private S3 エンドポイント、Azure Virtual Network サービスエンドポイント、またはプライベート Google アクセスを確立できます。

これらの方法を使用すると、オンプレミスの NAS サーバと Cloud Sync データブローカーグループの間にセキュアな接続が確立されます。

データはクラウド同期で暗号化されていますか？

- クラウド同期では、ソースとターゲットの NFS サーバ間のデータインフライト暗号化がサポートされます。 "[詳細はこちら](#)。"。
- SMB の場合、Cloud Sync は、サーバ側で暗号化した SMB 3.0 および 3.11 データをサポートします。Cloud Sync は、暗号化されたデータをソースからターゲットにコピーします。ターゲットはデータが暗号化されたままです。

Cloud Sync は SMB データ自体を暗号化できません。

- Amazon S3 バケットが同期関係のターゲットである場合は、AWS KMS の暗号化と AES-256 暗号化を使用してデータ暗号化を有効にするかどうかを選択できます。

## 権限

次の質問は、データ権限に関連しています。

**SMB** データの権限はターゲットの場所に同期されていますか？

Cloud Sync を設定して、ソース SMB 共有とターゲット SMB 共有の間、およびソース SMB 共有からオブジェクトストレージ（ONTAP S3 を除く）へのアクセス制御リスト（ACL）を保持することができます。



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。

["SMB 共有間で ACL をコピーする方法について説明します。"](#)

**NFS** データの権限はターゲットの場所に同期されていますか。

クラウド同期では、NFS サーバ間で次のように NFS 権限が自動的にコピーされます。

- NFS バージョン 3 : Cloud Sync は権限とユーザグループ所有者をコピーします。
- NFS バージョン 4 : Cloud Sync は ACL をコピーします。

## オブジェクトストレージのメタデータ

Cloud Sync は、次のタイプの同期関係について、オブジェクトストレージのメタデータをソースからターゲットにコピーします。

- Amazon S3 → Amazon S3 ^1
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID の順にクリックします
- StorageGRID → Google Cloud Storage
- Google Cloud Storage → StorageGRID ^1
- Google Cloud Storage → IBM Cloud Object Storage ^1
- Google Cloud Storage → Amazon S3 ^1
- Amazon S3 → Google Cloud Storage
- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → IBM クラウドオブジェクトストレージ
- IBM Cloud Object Storage → StorageGRID の順にクリックします
- IBM Cloud Object Storage → IBM Cloud Object Storage

^1 この同期関係には、以下が必要です ["同期関係を作成するときに、\[オブジェクトのコピー設定を有効にします\]"](#)。

## パフォーマンス

クラウド同期のパフォーマンスに関する質問は次のとおりです。



同期関係の進行状況インジケータは何を表していますか。

同期関係は、データブローカーグループのネットワークアダプタのスループットを示しています。複数のデータブローカーを使用して同期パフォーマンスを高速化した場合、スループットはすべてのトラフィックの合計になります。このスループットは 20 秒ごとに更新されます。

パフォーマンスの問題が発生しています。同時転送の数を制限できますか。

大容量のファイル（それぞれ複数の TiB）がある場合は、転送プロセスが完了するまでに時間がかかることがあり、パフォーマンスに影響する可能性があります。

同時転送の数を制限すると効果的です。mailto : [ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com) [ お問い合わせ ]

**Azure NetApp Files** でパフォーマンスが低いのはなぜですか？

Azure NetApp Files との間でデータを同期する際、ディスクのサービスレベルが Standard の場合は障害やパフォーマンスの問題が発生することがあります。

同期パフォーマンスを向上させるには、サービスレベルを Premium または Ultra に変更します。

"[Azure NetApp Files のサービスレベルとスループットの詳細については、こちらをご覧ください](#)".

**Cloud Volumes Service for AWS** でパフォーマンスが低下するのはなぜですか。

クラウドボリュームとの間でデータを同期する場合、クラウドボリュームのパフォーマンスレベルが標準の場合は、障害やパフォーマンスの問題が発生することがあります。

サービスレベルを Premium または Extreme に変更して、同期のパフォーマンスを向上させます。

## 1 つのグループに必要なデータブローカーの数

新しい関係を作成する場合は、1 つのデータブローカーを 1 つのグループで開始します（アクセラレーション同期関係に属する既存のデータブローカーを選択した場合を除く）。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。同期されていない場合は、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。

データ転送のパフォーマンスには、複数の要因が影響します。全体的な同期パフォーマンスは、ネットワーク帯域幅、レイテンシ、ネットワークトポロジ、データブローカー VM の仕様、ストレージシステムのパフォーマンスによって影響を受ける可能性があります。たとえば、グループ内の単一のデータブローカーが 100MB/s に達することはありますが、ターゲットのディスクスループットでは 64MB/s しか許可されません。その結果、データブローカーグループはデータのコピーを試行し続けますが、ターゲットではデータブローカーグループのパフォーマンスを達成できません。

そのため、ネットワークのパフォーマンスとターゲットのディスクスループットを確認してください。

次に、グループにデータブローカーを追加してその関係の負荷を共有することで、同期パフォーマンスを高速化することを検討します。"[同期のパフォーマンスを高速化する方法について説明します](#)".

## 項目を削除する

次の質問は、ソースとターゲットから同期関係とデータを削除することに関連しています。



クラウドの同期関係を削除するとどうなりますか。

関係を削除すると、以降のすべてのデータの同期が停止し、支払いが終了します。ターゲットに同期されたデータはそのまま残ります。

ソースサーバから何かを削除するとどうなりますか。ターゲットからも削除されていますか？

デフォルトでは、Active Sync 関係がある場合、ソースサーバ上で削除されたアイテムは、次の同期時にターゲットから削除されません。ただし、各関係の同期設定にはオプションがあり、ソースから削除されたファイルは Cloud Sync によってターゲットロケーションから削除されるように定義できます。

["同期関係の設定を変更する方法について説明します。"](#)

ターゲットから何かを削除するとどうなりますか？ソースからも削除されていますか？

ターゲットから削除されたアイテムは、ソースから削除されません。ソースからターゲットへの関係は一方方向です。次の同期サイクルでは、クラウド同期によってソースとターゲットが比較され、アイテムが見つからないことが特定され、クラウド同期によってソースからターゲットに再度コピーされます。

## トラブルシューティング

["ネットアップナレッジベース：Cloud Sync FAQ：Support and Troubleshooting"](#)

## データブローカーのディープダイブ

次の質問は、データブローカーに関連しています。

データブローカーのアーキテクチャについて説明できますか？

確かに。最も重要なポイントは次のとおりです。

- データブローカーは、Linux ホスト上で実行されている Node.js アプリケーションです。
- Cloud Sync は、次のようにデータブローカーを導入します。
  - AWS：AWS Cloudformation テンプレートから
  - Azure：Azure Resource Manager から
  - Google：Google Cloud Deployment Manager から
  - 独自の Linux ホストを使用する場合は、ソフトウェアを手動でインストールする必要があります
- データブローカーソフトウェアは、自動的に最新バージョンにアップグレードします。
- データブローカーは、AWS SQS を信頼性の高い安全な通信チャネルとして使用し、制御と監視を行います。SQS は永続性レイヤも提供します。
- データブローカーをグループに追加することで、転送速度を向上させ、高可用性を追加することができます。1 つのデータブローカーに障害が発生した場合、サービスの耐障害性があります

# 知識とサポート

## サポートに登録します

ネットアップテクニカルサポートでサポートケースをオープンするには、事前に Cloud Manager にネットアップサポートサイトのアカウントを追加し、サポートに登録しておく必要があります。

### NSS アカウントを追加します

サポートダッシュボードを使用すると、すべてのネットアップサポートサイトのアカウントを 1 箇所から追加および管理できます。

#### 手順

1. ネットアップサポートサイトのアカウントがない場合は、**"1 名で登録します"**。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、**\* Support \*** を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

3. **[NSS Management] > [Add NSS Account]** をクリックします。
4. メッセージが表示されたら、**[\* Continue (続行) ]** をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

Cloud Manager で NSS アカウントを使用することができます。

注：お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。

## アカウントを登録してサポートを受けてください

サポートの登録は、Cloud Manager のサポートダッシュボードで実行できます。

### 手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、\* Support \* を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [\* リソース ] タブで、[\* サポートに登録 \* ] をクリックします。
3. 登録する NSS 資格情報を選択し、\* 登録 \* をクリックします。

## ヘルプを表示します

ネットアップでは、Cloud Manager とその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（KB）記事やコミュニティフォーラムなど、24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

### セルフサポート

次のオプションは、1 日 24 時間、週 7 日間無料でご利用いただけます。

- ["ナレッジベース"](#)

Cloud Manager のナレッジベースで問題のトラブルシューティングに役立つ記事を検索してください。

- ["コミュニティ"](#)

Cloud Manager コミュニティに参加して、進行中のディスカッションに参加したり、新しいコミュニティを作成したりできます。

- [ドキュメント](#)

現在表示している Cloud Manager のドキュメント。

- mailto : [ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com) [ フィードバックメール ]

お客様のご意見をお考えください。Cloud Manager の改善に役立つフィードバックを送信します。

## ネットアップサポート

上記のセルフサポートオプションに加え、サポートを有効にしたあとに問題が発生した場合は、ネットアップサポートエンジニアと協力して解決できます。

### 手順

1. Cloud Manager で、 \* Help > Support \* の順にクリックします。
2. テクニカルサポートで利用可能なオプションのいずれかを選択します。
  - a. [ \* お問い合わせ \* ] をクリックして、ネットアップ・テクニカル・サポートの電話番号を検索してください。
  - b. [ \* 問題 を開く \* ] をクリックし、いずれかのオプションを選択して、[ \* 送信 \* ] をクリックします。

ネットアップの担当者がケースを確認し、すぐに対応を開始します。

# 法的通知

著作権に関する声明、商標、特許などにアクセスできます。

## 著作権

<http://www.netapp.com/us/legal/copyright.aspx>

## 商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/us/media/patents-page.pdf>

## プライバシーポリシー

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

["クラウドの同期に関する注意事項"](#)

## 著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、またはその他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1 つ以上の米国特許、その他の国の特許、および出願中の特許により特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

## 商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> は、NetApp、Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。