はじめに

BlueXP copy and sync

NetApp
April 29, 2024

目次

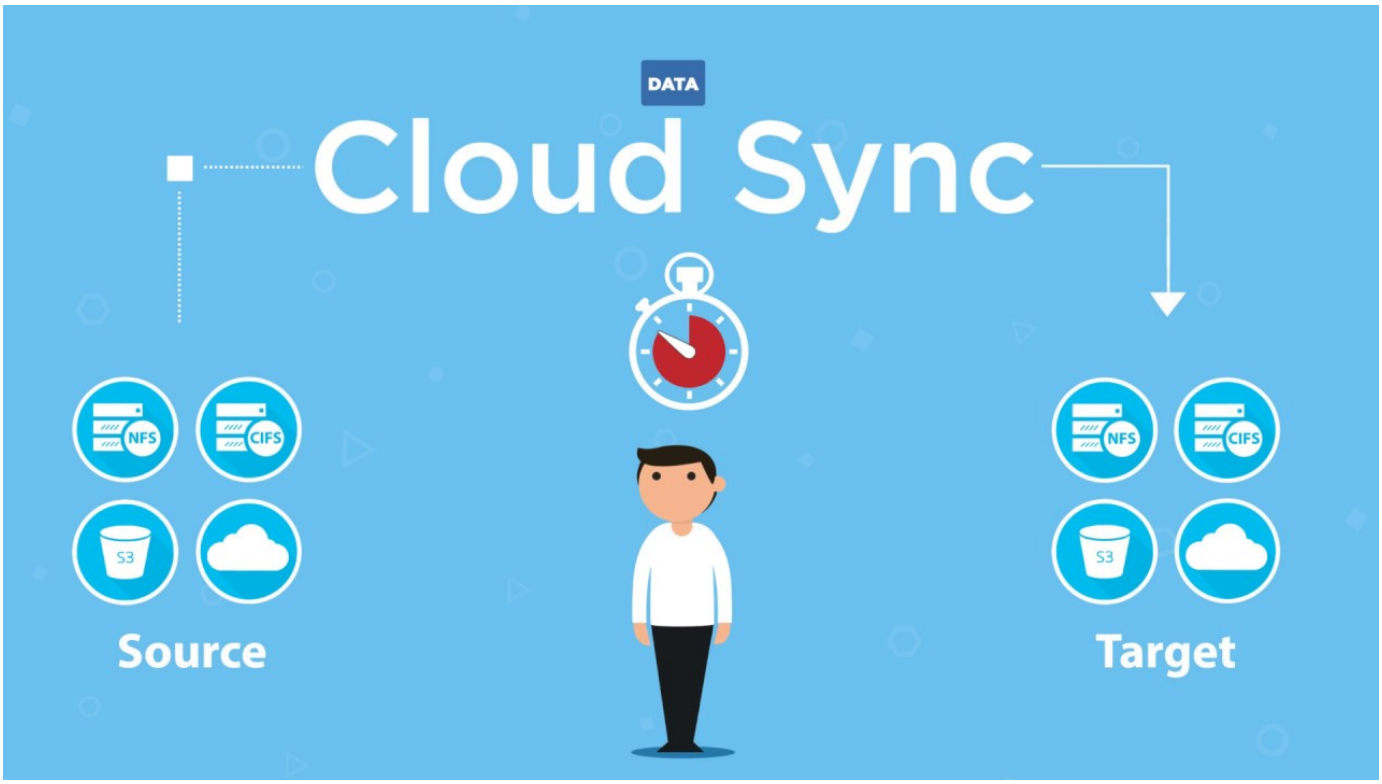
はじめに

BlueXPのコピーと同期の概要

NetApp BlueXPのコピーと同期サービスは、クラウドかオンプレミスかを問わず、シンプルかつセキュアで自動化された方法でデータをあらゆるターゲットに移行します。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）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、BlueXPのコピーと同期を変換して移動できます。

の機能

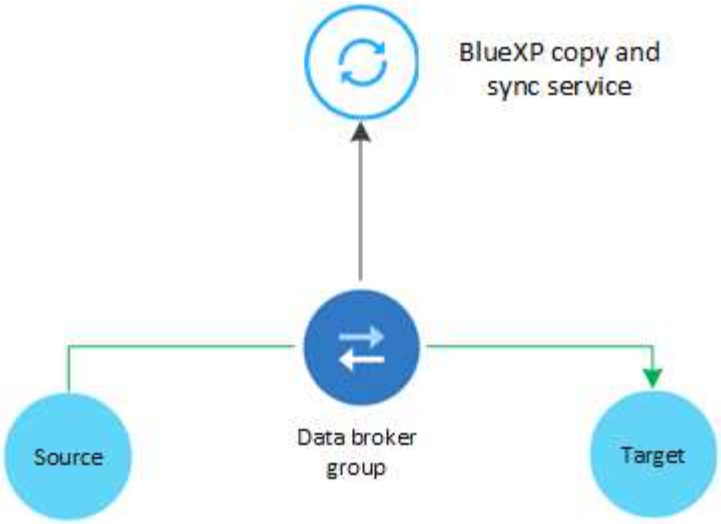
BlueXPのコピーと同期の概要については、次のビデオをご覧ください。



BlueXPのコピーと同期の仕組み

BlueXPのコピーと同期は、データブローカーグループ、BlueXPで利用でき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、BlueXPのコピーコンポーネントと同期コンポーネント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、または社内で実行できます。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は、BlueXPのコピーおよび同期サービスと通信し、他のいくつかのサービスやリポジトリに接続できるように、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

BlueXPのコピーと同期では、次のストレージタイプがサポートされます。

- 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 Data Lake Storage Gen2
- 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
- Googleドライブ
- 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

BlueXPのコピーと同期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"。

BlueXPのコピーと同期のクイックスタート

BlueXPのコピーと同期サービスは、いくつかの手順で開始できます。

1 ログインして**BlueXP**をセットアップします

BlueXPを使い始めました。これにはログイン、アカウントの設定、コネクタの展開、作業環境の作成などが含まれます。

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

Cloud Volumes ONTAP 、オンプレミスONTAP クラスタ、およびONTAP 対応Amazon FSXには、コネクタが必要です。

- "BlueXPの使用を開始する方法について説明します"
- "コネクタの詳細については、こちらをご覧ください"

2 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"

3 ネットアップデータブローカーの設置場所を準備します

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、または社内で実行できます。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は、BlueXPのコピーおよび同期サービスと通信し、他のいくつかのサービスやリポジトリに接続できるように、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。"。

BlueXPのコピーと同期は、ガイドに従ってインストールプロセスを実行して同期関係を作成します。同期関係を作成したら、データブローカーをクラウドに導入したり、自社の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"

4 最初の同期関係を作成します

にログインします "BlueXP"をクリックし、*[同期]*を選択し、ソースとターゲットの選択内容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。"。

5 無料トライアルが終了したら、同期関係の料金をお支払いください

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。BlueXPのコピーの[License Settings]ページに移動して同期するだけでセットアップできます。 "詳細はこちら。"。

サポートされている同期関係

BlueXPのコピーと同期を使用すると、ソースからターゲットに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	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID
ONTAP 対応の Amazon FSX	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

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 S3	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • ボックス ^1 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure Blob の略	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

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 Data Lake Storage Gen2	• Azure NetApp Files の特長 • Cloud Volumes ONTAP • FSX for ONTAP の略 • IBM クラウドオブジェクトストレージ • NFS サーバ • On-Prem ONTAP の略 • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure NetApp Files の特長	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID
ボックス ^1	• ONTAP 対応の Amazon FSX • Amazon S3 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • IBM クラウドオブジェクトストレージ • NFS サーバ • SMB サーバ • StorageGRID

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 ONTAP	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID
Cloud Volumes Service	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
Google クラウドストレージ	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Googleドライブ	• NFS サーバ • SMB サーバ
IBM クラウドオブジェクトストレージ	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • ボックス ^1 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

ソースの場所	サポートされるターゲットロケーション
NFS サーバ	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • Googleドライブ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
オンプレミスの ONTAP クラスタ	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • SMB サーバ • StorageGRID

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 S3 ストレージ	• Amazon S3 • Azure Data Lake Storage Gen2 • Google クラウドストレージ • NFS サーバ • SMB サーバ • StorageGRID • ONTAP S3 ストレージ
SFTP[2]	S3
SMB サーバ	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • Cloud Volumes ONTAP • Cloud Volumes Service • Google クラウドストレージ • Googleドライブ • IBM クラウドオブジェクトストレージ • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID

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	• Amazon EFS • ONTAP 対応の Amazon FSX • Amazon S3 • Azure Blob の略 • Azure Data Lake Storage Gen2 • Azure NetApp Files の特長 • ボックス ^1 • Cloud Volumes ONTAP • Cloud Volumes Service • 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 • NFS サーバ • オンプレミスの ONTAP クラスタ • ONTAP S3 ストレージ • SMB サーバ • StorageGRID

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、BlueXPのコピーおよび同期APIでのみサポートされます。
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
   - Glacier Deep Archive
   - Glacierの柔軟な取得
   - Glacier のインスタント検索
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 ）
- Archive サービスの略

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際、BlueXPのコピーと同期を使用して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

BlueXPのコピーと同期には、ソースまたはターゲット内のすべてのディレクトリやフォルダを表示するため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

[s3] 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、BlueXPのコピーと同期で、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

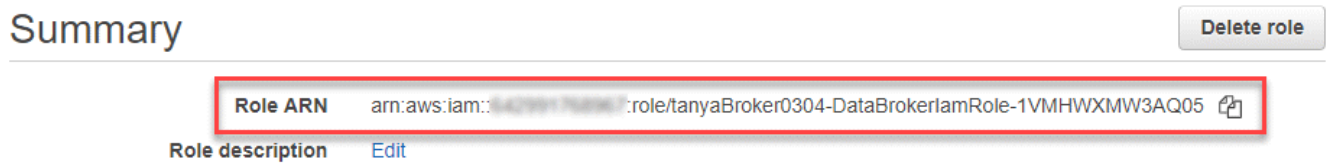
同期関係をセットアップする際、データブローカーに関連付けられていない AWS アカウントに配置されている S3 バケットを指定することができます。

"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. *<Rolear>* 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 _Rolears_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を確認するには、EC2コンソールに移動してデータブローカーインスタンスを選択し、概要タブからIAMロールを選択します。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。



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

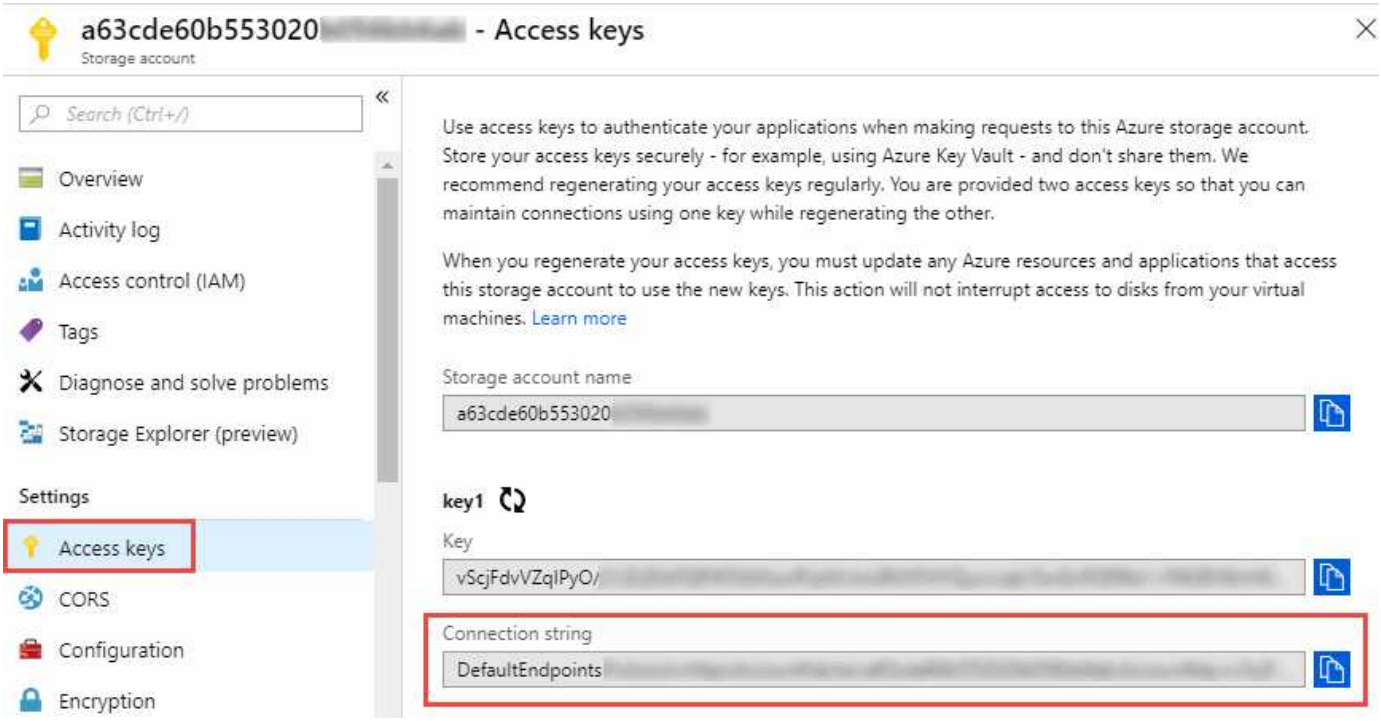
データブローカーは、同期関係に Azure BLOB ストレージが含まれている場合でも、任意の場所に配置できます。

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またはSMBサーバの間の同期関係を作成する場合は、BlueXPのコピーとストレージアカウント接続文字列との同期を指定する必要があります。

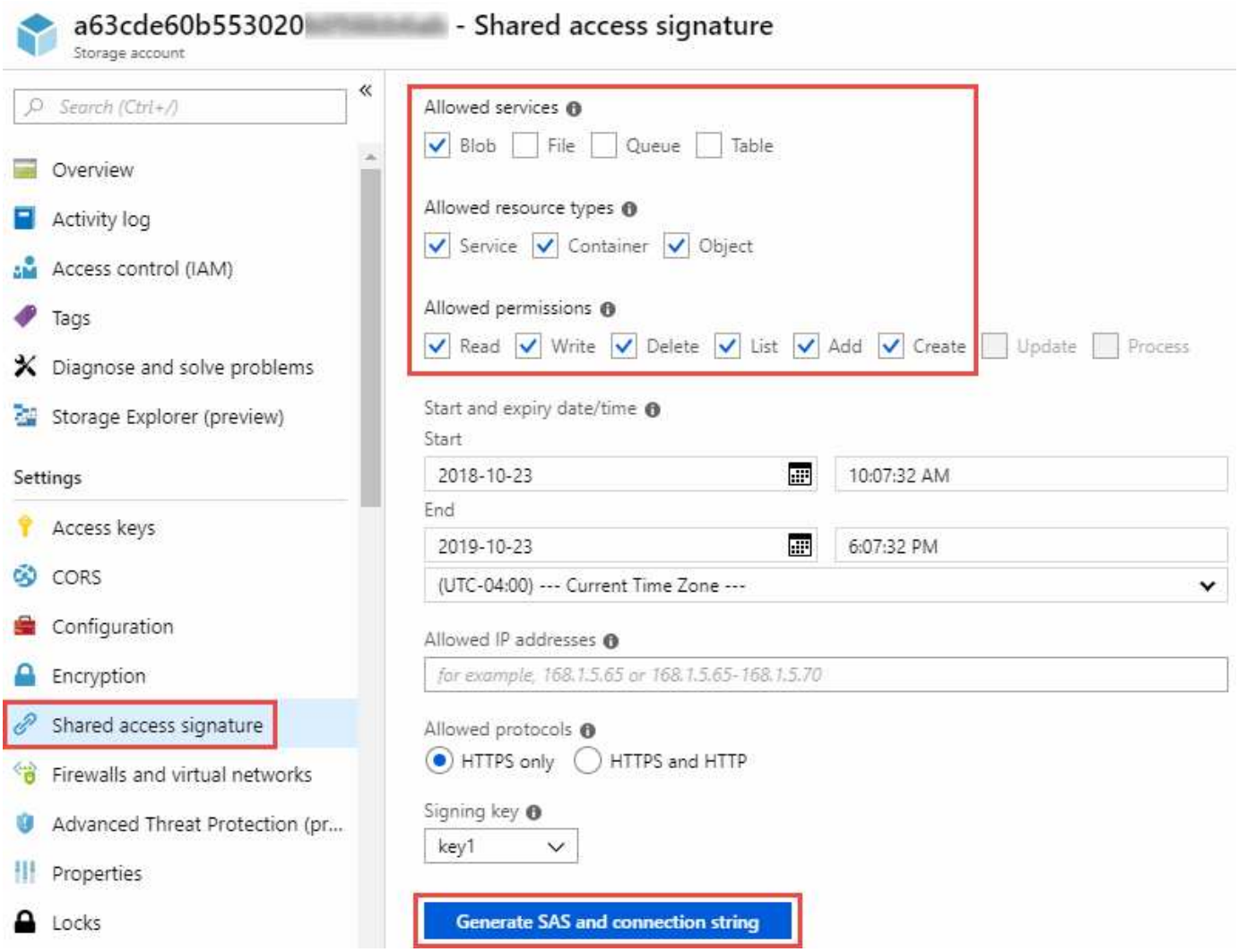


を選択すると表示されます。"]

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



を選択すると表示されます。"]

> Azure BLOBコンテナを含むContinuous Sync関係を実装する場合は、通常の接続文字列またはSAS接続文字列を使用できます。SAS接続文字列を使用している場合は、近い将来有効期限が切れるように設定しないでください。

Azure Data Lake Storage Gen2

Azure Data Lakeを含む同期関係を作成する場合は、BlueXPのコピーとストレージアカウントの接続文字列との同期を指定する必要があります。共有アクセスシグニチャ（SAS）ではなく、通常の接続文字列である必要があります。

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 Cloud Storage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。BlueXPのコピーと同期を使用すると、データブローカーのインストールプロセスに従って同期関係を作成できます。

- "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。

Google Cloudバケットの暗号化

お客様が管理するKMSキーまたはGoogleが管理するデフォルトのキーを使用して、ターゲットのGoogle Cloudバケットを暗号化できます。バケットにKMS暗号化がすでに追加されている場合は、Googleが管理するデフォルトの暗号化よりも優先されます。

お客様が管理するKMSキーを追加するには、 "正しい権限"、およびキーはバケットと同じリージョンに存在する必要があります。

Googleドライブ

Googleドライブを含む同期関係を設定する場合は、次の情報を入力する必要があります。

- データを同期するGoogleドライブの場所にアクセスできるユーザーの電子メールアドレス
- Google Driveへのアクセス権限を持つGoogle CloudサービスアカウントのEメールアドレスです
- サービスアカウントの秘密鍵

サービスアカウントを設定するには、Googleのドキュメントに記載されている手順に従います。

- "サービスアカウントとクレデンシャルを作成します"
- "ドメイン全体の権限をサービスアカウントに委任します"

OAuth Scopesフィールドを編集する場合は、次のスコープを入力します。

- \ https://www.googleapis.com/auth/drive
- \ https://www.googleapis.com/auth/drive.file

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。
- BlueXPのコピーと同期を、SMBサーバに対する権限があるクレデンシャルで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。BlueXPのコピーと同期で「A」という名前のファイルがターゲットにコピーされると、ファイル「A」がソースのファイル「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。BlueXPのコピーと同期で「b」というディレクトリをターゲットにコピーしようとすると、ディレクトリがすでに存在することを示すエラーがBlueXPのコピーと同期に表示されます。そのため、BlueXPのコピーと同期で「B」というディレクトリのコピーが常に失敗します。

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。

BlueXPのコピーと同期のネットワークの概要

BlueXPのコピーと同期のネットワークには、データブローカーグループとソースとターゲットの場所の間の接続、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含まれます。

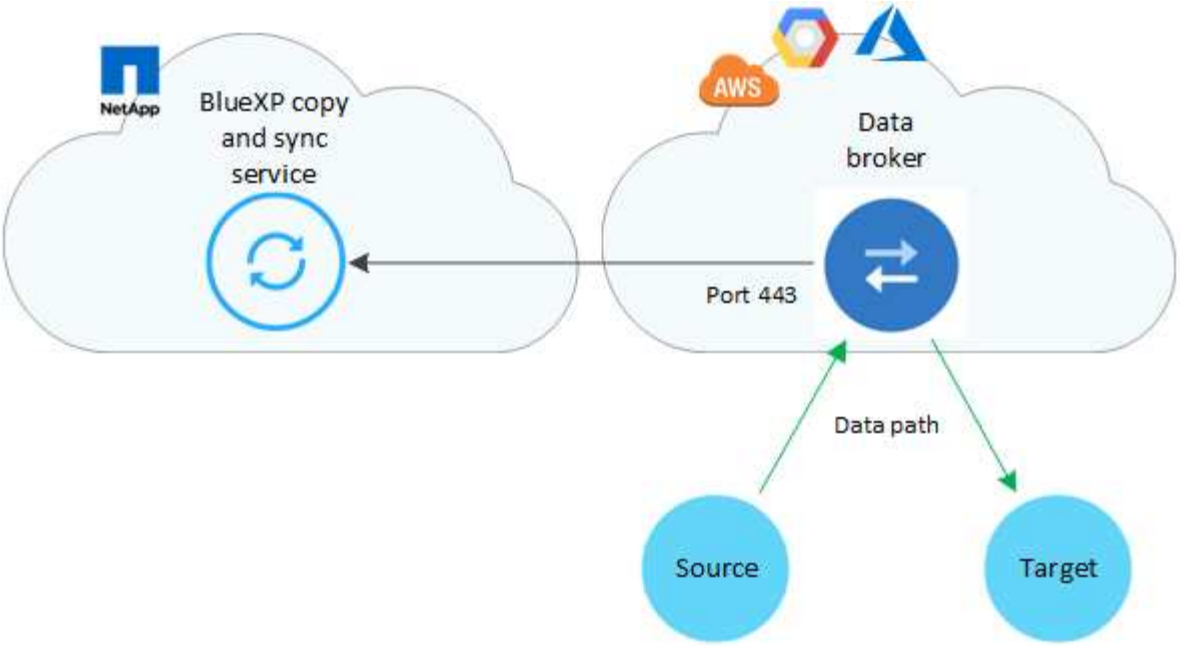
データブローカーの場所

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

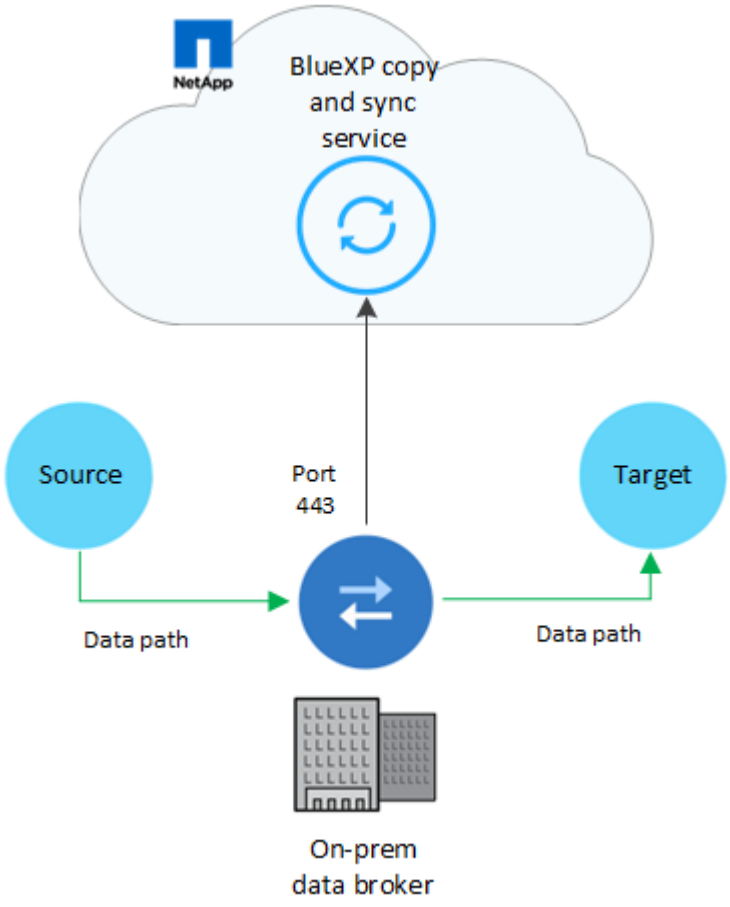
次の図は、クラウド、 AWS 、 Google Cloud 、 Azure で実行されるデータブローカーを示しています。データブローカーへの接続が確立されていれば、ソースとターゲットはどの場所にも存在できます。たとえば、データセンターからクラウドプロバイダーへの VPN 接続があるとします。

> BlueXPのコピーと同期でデータブローカーをAWS、Azure、Google Cloudに導入すると、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。



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。

- データブローカーがBlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるようにするには、アウトバウンド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がBlueXPのコピーおよび同期サービスと通信し、他のいくつかのサービスやリポジトリにアクセスするには、ポート443経由のアウトバウンドインターネットアクセスが必要です。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
\ https://olcentgbl.trafficmanager.net	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。
¥ https://rpm.nodesource.com ¥ https://registry.npmjs.org ¥ https://nodejs.org:	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。
\ https://tgz.pm2.io	では、PM2を更新するためのリポジトリにアクセスします。PM2は、BlueXPのコピーと同期の監視に使用するサードパーティパッケージです。
¥ https://sqs.us-east-1.amazonaws.com ¥ https://kinesis.us-east-1.amazonaws.com	BlueXPのコピーと同期が処理（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）に使用するAWSのサービスにアクセスするため。
¥ https://s3.*region*.amazonaws.com （例： s3.us-east-2.amazonaws.com:443 ）https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["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。
\ https://s3.amazonaws.com/	BlueXPのコピーと同期からデータブローカーの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圧縮し、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。

エンドポイント	目的
\ https://storage.googleapis.com/	同期関係でGCPバケットを使用している場合にGoogle Cloudに連絡するには、次の手順に従います。
https://storage-account.blob.core.windows.netAzure Data Lake Gen2を使用する場合：https://storage-account.dfs.core.windows.net[]storage-account_はユーザのソースストレージアカウントです。	ユーザのAzureストレージアカウントアドレスへのプロキシを開きます。
¥ https://cf.cloudsync.netapp.com ¥ https://repo.cloudsync.netapp.com	BlueXPのコピーと同期サービスにお問い合わせください。
\ https://support.netapp.com	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。
\ https://fedoraproject.org	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。
https://sts.amazonaws.com https://sts.us-east-1.amazonaws.com	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。
¥https://console.bluexp.netapp.com/¥https://netapp-cloud-account.auth0.com	新しい同期関係のソースファイルを分類を使用して選択する場合に、BlueXPの分類に連絡します。
\ https://pubsub.googleapis.com	Googleストレージアカウントから継続的な同期関係を作成する場合。
https://storage-account.queue.core.windows.net\https://management.azure.com/subscriptions/${subscriptionId}/resourceGroups/${resourcegroup}/providers /microsoft.EventGrid/*ここで、_storage-account_はユーザーのソースストレージアカウント、_SubscriptionID_は ソースサブスクリプションID、_resourcegroup_は ソースリソースグループです。	Azureストレージアカウントから継続的な同期関係を作成する場合。

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。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

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。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

ネットワーク要件

- データブローカーは、BlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるように、アウトバウンドインターネット接続を必要とします。

  BlueXPのコピーと同期で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可能にするセキュリティグループが作成されます。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"。

[IAM] AWSデータブローカーで独自の**IAM**ロールを使用する必要があります

BlueXPのコピーと同期でデータブローカーを導入すると、データブローカーインスタンス用のIAMロールが作成されます。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

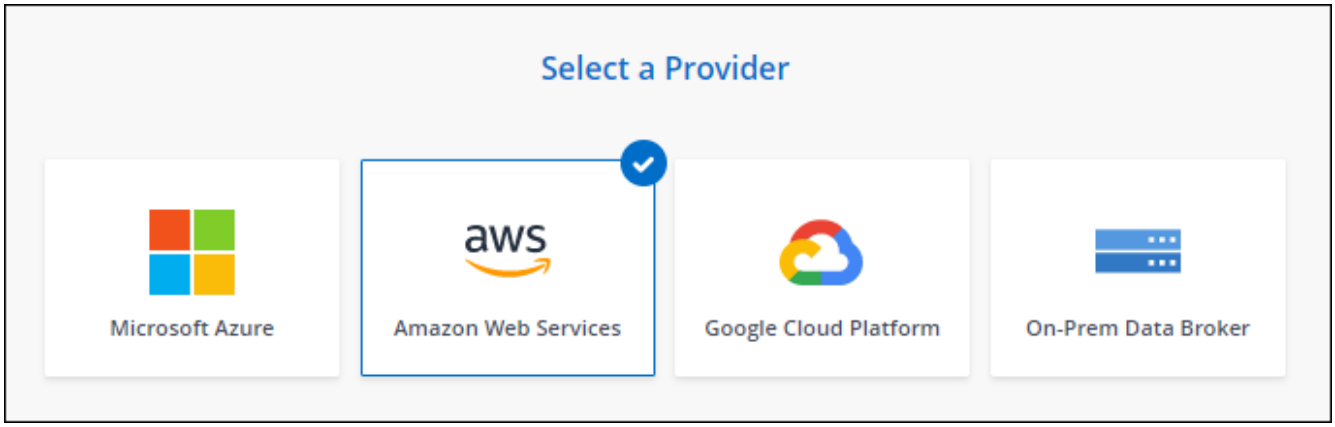
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを AWS にインストールする方法について説明します。

手順

1. [新しい同期の作成]*を選択します。
2. [同期関係の定義]ページで、ソースとターゲットを選択し、*[続行]*を選択します。

   「 * 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**]***を選択し、[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]*を選択します。
5. AWSアクセスキーを入力して、BlueXPのコピーと同期がお客様に代わってAWSでデータブローカーを作成できるようにします。

   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。

   アクセスキーを提供しない場合は、ページの下部にあるリンクを選択して、代わりに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。

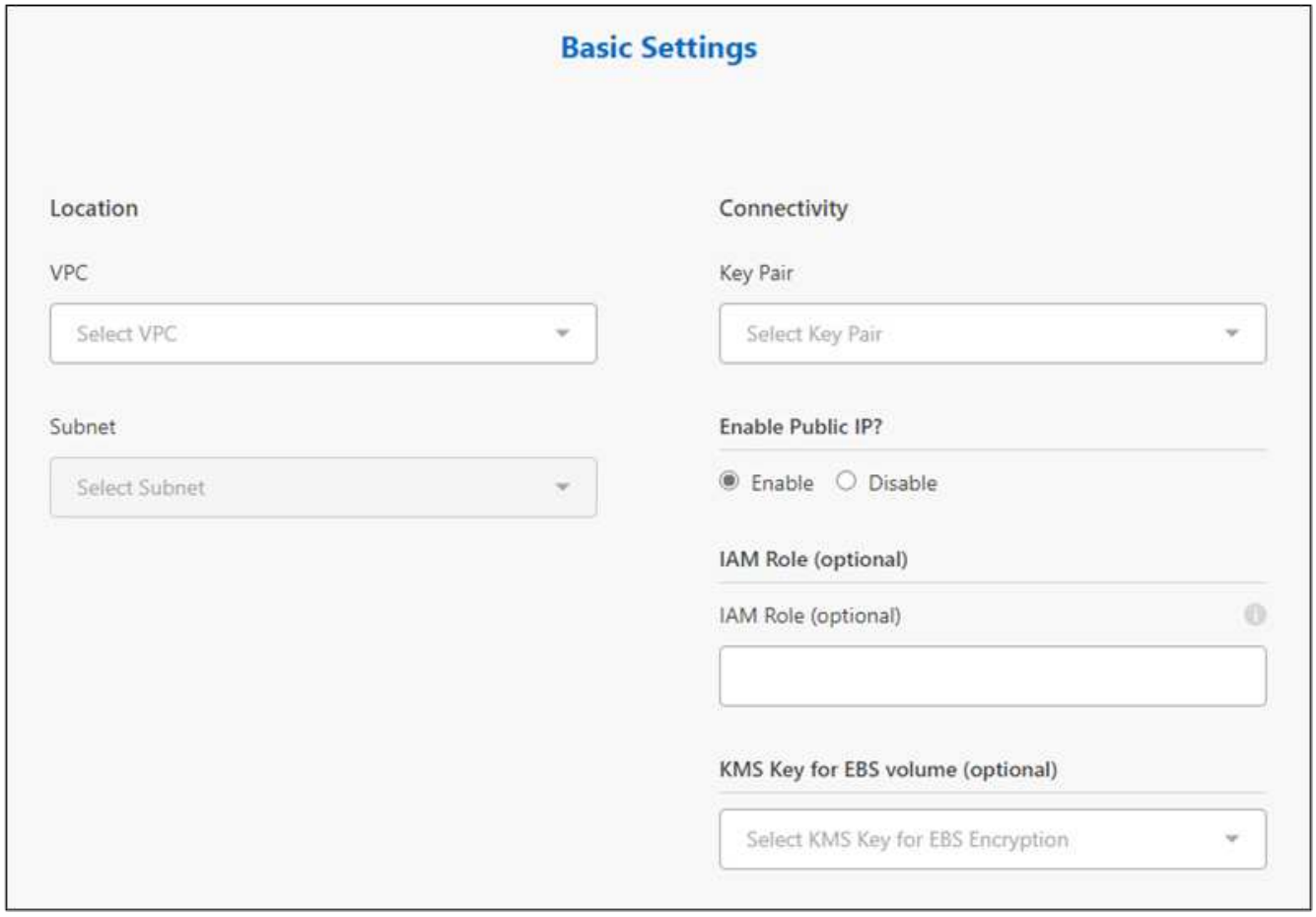
   CloudFormation テンプレートを使用してデータブローカーインスタンスを起動する方法を紹介したビデオを次に示します。

   ▶ https://docs.netapp.com/ja-jp/bluexp-copy-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て既存のIAMロールを選択します。または、このフィールドを空白

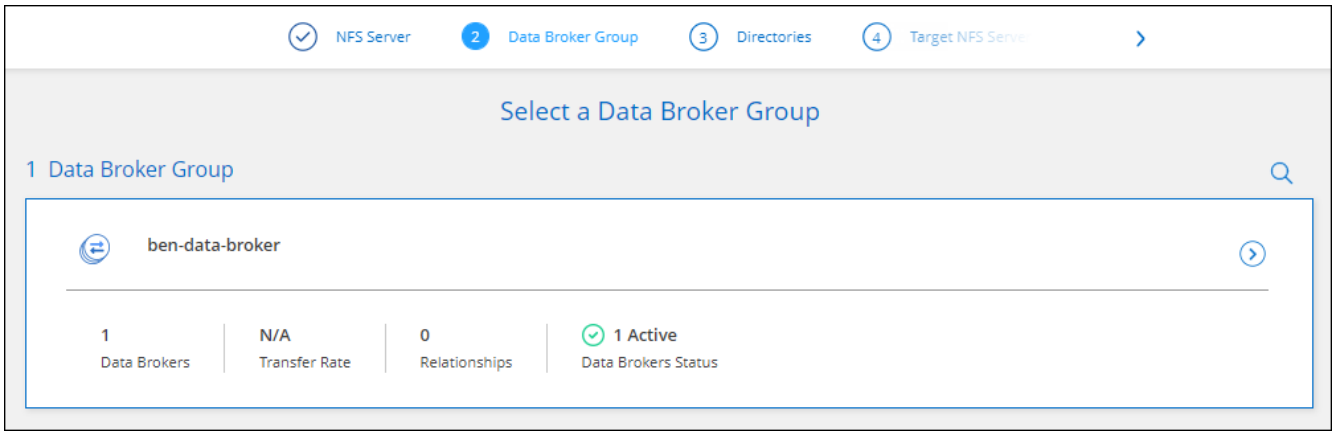
のままにしてBlueXPのコピーと同期でロールが作成されます。また、KMSキーを使用してデータブローカーを暗号化することもできます。

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。



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、BlueXPのコピーと同期で*[続行]*を選択します。

   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。



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。

結果

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

BlueXPのコピーと同期では、次の構成を使用してAWSにデータブローカーが作成されます。

Node.jsとの互換性
: v21.2.0

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 2023

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。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

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。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

ネットワーク要件

- データブローカーは、BlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるように、アウトバウンドインターネット接続を必要とします。

BlueXPのコピーと同期でAzure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。

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",
                    "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",
                    "Microsoft.EventGrid/systemTopics/read",
                    "Microsoft.EventGrid/systemTopics/write",
                    "Microsoft.EventGrid/systemTopics/delete",
                    "Microsoft.EventGrid/eventSubscriptions/write",
                    "Microsoft.Storage/storageAccounts/write"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

"Microsoft.Network/networkSecurityGroups/securityRules/read",
                    "Microsoft.Network/networkSecurityGroups/read",
```

```
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}
```

注：

1. 次の権限は、 "連続同期設定" Azureから別のクラウドストレージの場所への同期関係で次の手順を実行します。

    - 'microsoft.StorageAccounts/read'、
    - 'microsoft.EventGrid/systemTopics/eventSubscriptions/write'、
    - 'microsoft.EventGrid/systemTopics/eventSubscriptions/read'、
    - 'microsoft.EventGrid/systemTopics/eventSubscripts/delete'、
    - 'microsoft.EventGrid/systemTopics/eventSubscripts/getFullUrl/action'、
    - 'microsoft.EventGrid/systemTopics/eventSubscripts/getDeliveryAttributes/action'、
    - 'microsoft.EventGrid/systemTopics/read'、
    - 'microsoft.EventGrid/systemTopics/write'、
    - 'microsoft.EventGrid/systemTopics/delete'、
    - 'microsoft.EventGrid/eventSubscriptions/write'、
    - 'microsoft.StorageAccounts/write'

    また、AzureにContinuous Syncを実装する場合は、割り当て可能な範囲をサブスクリプションの範囲に設定し、*リソースグループの範囲ではない*に設定する必要があります。

2. 次の権限は、データブローカーの作成に独自のセキュリティを選択する場合にのみ必要です。
    - Microsoft.Network/networkSecurityGroups/securityRules/read"
    - Microsoft.Network/networkSecurityGroups/read"

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

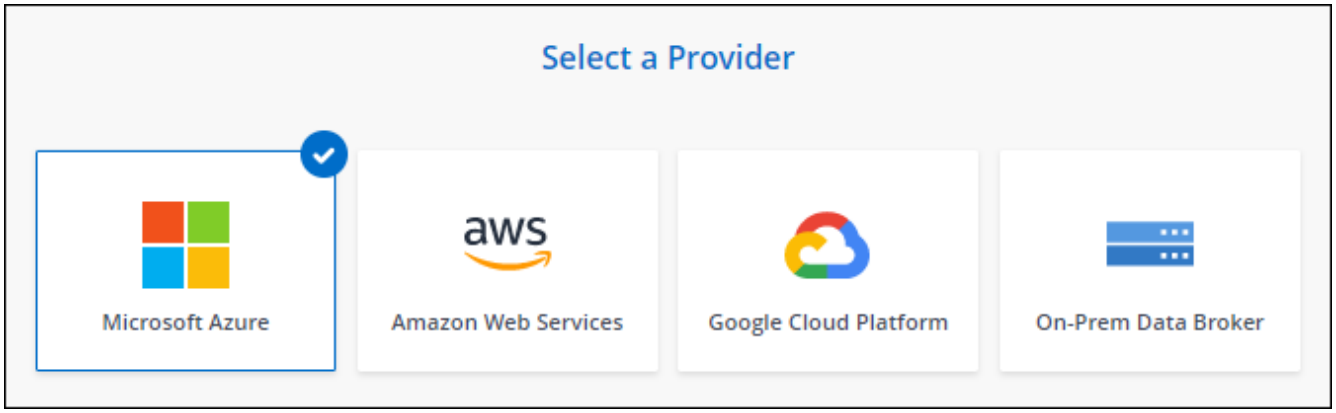
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを Azure にインストールする方法について説明します。

手順

1. [新しい同期の作成]*を選択します。
2. [同期関係の定義]ページで、ソースとターゲットを選択し、*[続行]*を選択します。

    「 * 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。

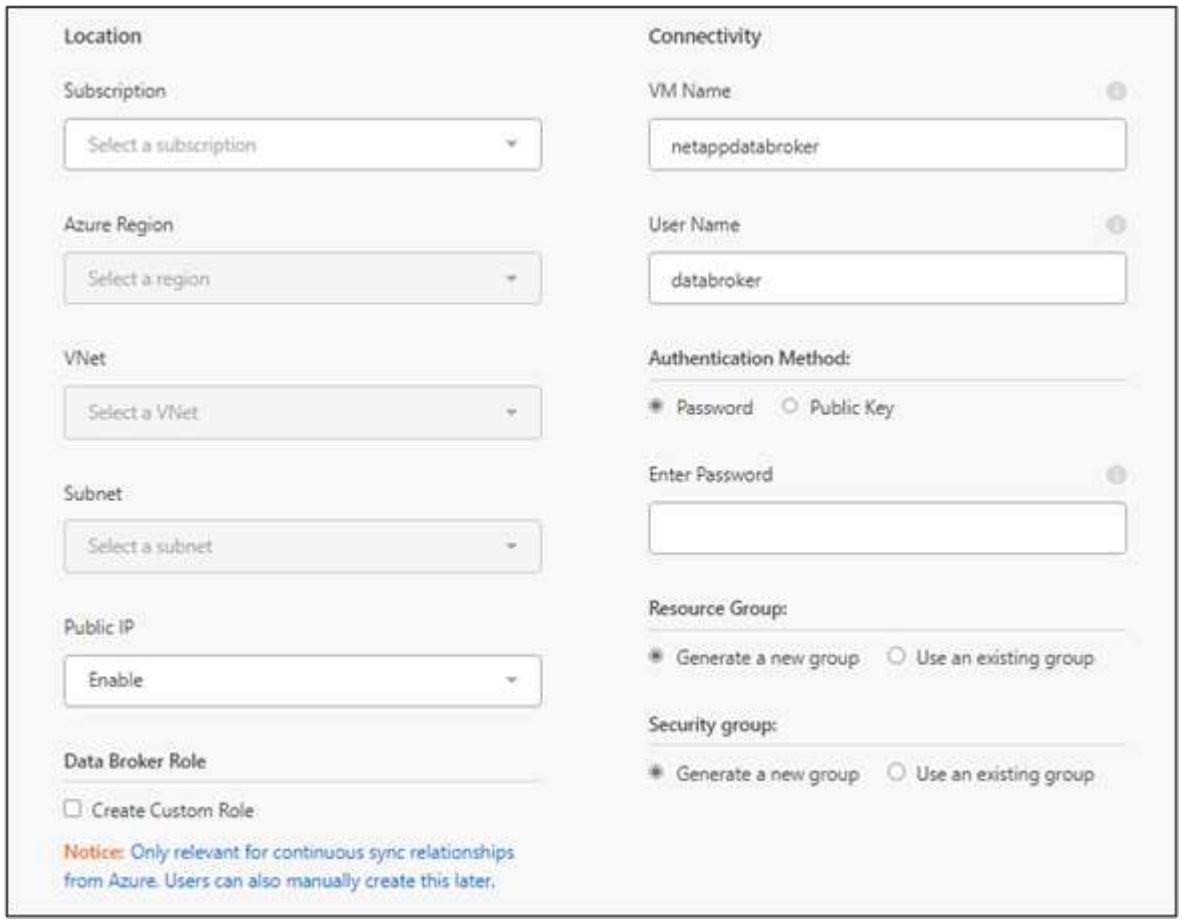
3. [データブローカーグループ]ページで、**[**データブローカーの作成**]***を選択し、[Microsoft Azure]*を選択します。



4. データブローカーの名前を入力し、*[続行]*を選択します。
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にログイン*を選択します。

   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。



Continuous Sync関係を実装する場合は、データブローカーにカスタムロールを割り当てる必要があります。これは、ブローカーの作成後に手動で行うこともできます。

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 * 」を選択します。データブローカーにS3権限を追加する場合は、AWSのアクセスキーとシークレットキーを入力します。
9. [続行]*を選択し、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。

10. BlueXPのコピーと同期で、データブローカーが利用可能になったら*[続行]*を選択します。
11. 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。

結果

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？

BlueXPのコピーと同期には組織内のリソースにユーザに代わってアクセスする権限が必要であるため、管理者の承認が必要であることをMicrosoftから通知された場合は、次の2つの方法があります。

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 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

BlueXPのコピーと同期では、Azureで次の構成を使用してデータブローカーが作成されます。

Node.jsとの互換性
: v21.2.0

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

Rocky Linux 9.0

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。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

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。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

ネットワーク要件

- データブローカーは、BlueXPのコピーと同期サービスにポーリングしてポート443経由のタスクを実行できるように、アウトバウンドインターネット接続を必要とします。

  BlueXPのコピーと同期で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.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

注：

1. 「 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。
2. 「pubsub.*」権限と「storage.enable」は、Google Cloud Storageから別のクラウドストレージ上の同期関係に対してContinuous Sync設定を有効にする場合にのみ必要です。 "継続的同期オプションの詳細については、こちらをご覧ください"。
3. 「cloudkms.cryptoKeys.list」権限と「cloudkms.keyrings.list」権限は、ターゲットのGoogle Cloud

Storageバケットで顧客管理KMSキーを使用する場合にのみ必要です。

データブローカーの作成

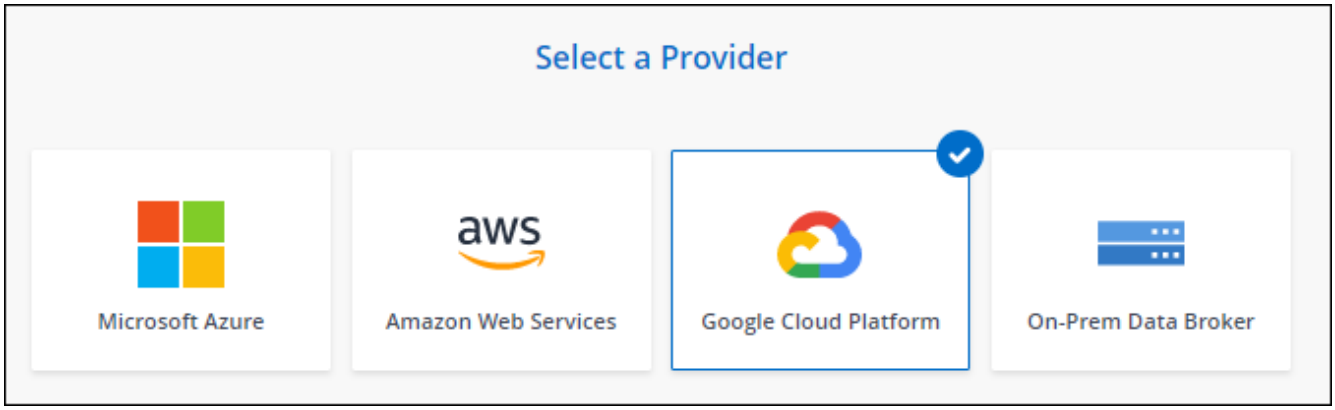
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成するときにデータブローカーを Google Cloud にインストールする方法について説明します。

手順

1. [新しい同期の作成]*を選択します。
2. [同期関係の定義]ページで、ソースとターゲットを選択し、*[続行]*を選択します。

   「 * 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**]***を選択し、[Google Cloud Platform]*を選択します。

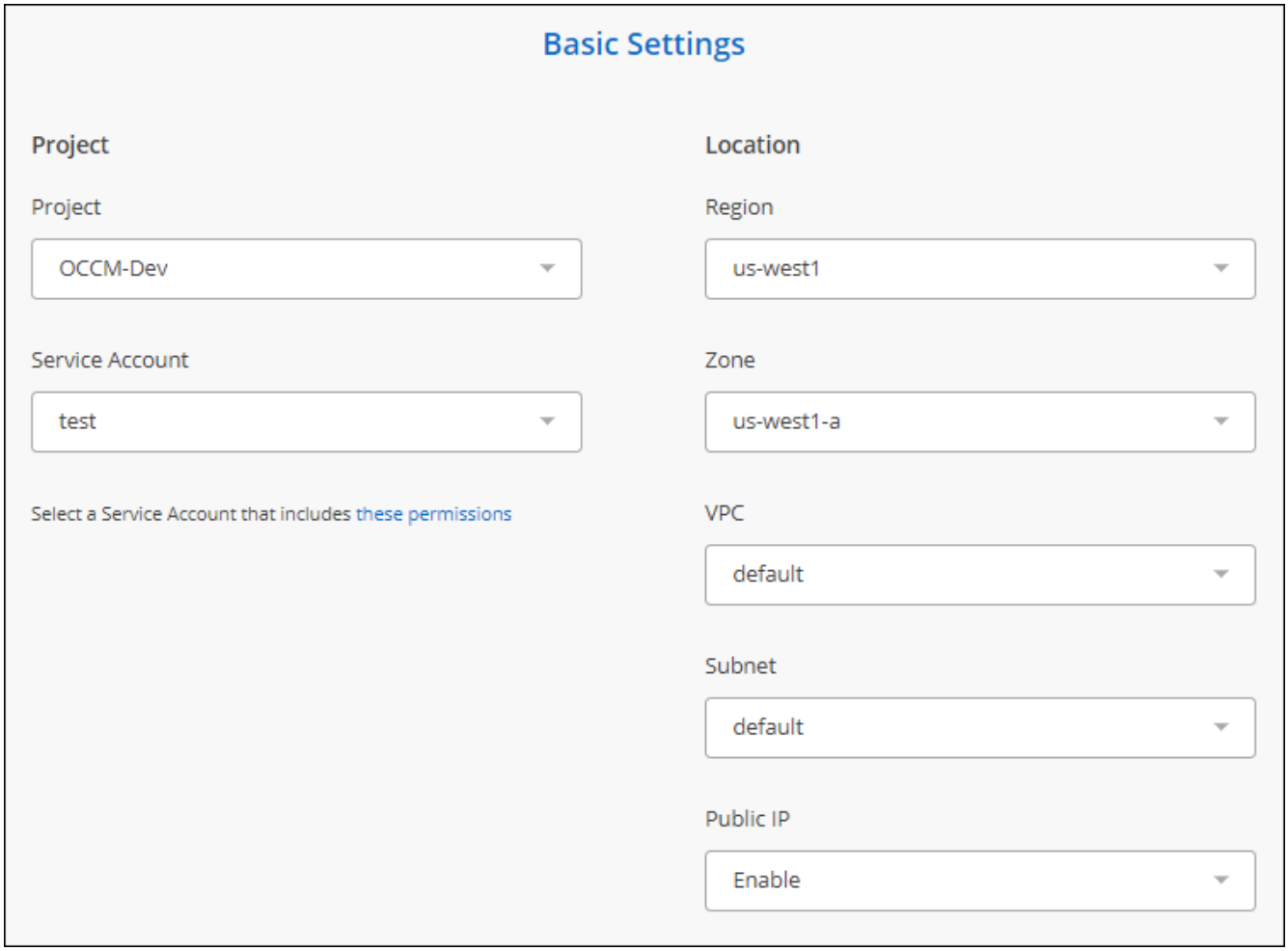


4. データブローカーの名前を入力し、*[続行]*を選択します。
5. メッセージが表示されたら、 Google アカウントでログインします。

   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。



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、BlueXPのコピーと同期で*[続行]*を選択します。

   このインスタンスの導入には、約 5 〜 10 分かかります。進捗状況はBlueXPのコピーおよび同期サービスで監視できます。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。

結果

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、BlueXPのコピーと同期では、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選択します。
3. [権限]*を選択します。
4. 「 * 追加」を選択します。
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 ）] を選択します。

結果

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

BlueXPのコピーと同期では、以下の構成を使用してGoogle Cloudにデータブローカーが作成されます。

Node.jsとの互換性
: v21.2.0

マシンのタイプ
: N2 - 標準 -4

vCPU
: 4.

RAM
: 15 GB

オペレーティングシステム
: Rocky Linux 9.0

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。BlueXPのコピーと同期の手順に従ってインストールプロセスを実行できますが、インストールの準備に役立つように、このページでは要件と手順を繰り返します。

Linux ホストの要件

- * Node.jsとの互換性*：v21.2.0
- * オペレーティング・システム * ：

- CentOS 8.0および8.5

  CentOS ストリームはサポートされていません。

- Red Hat Enterprise Linux 8.5、8.8、および8.9
- Rocky Linux 9
- Ubuntu Server 20.04 LTS の場合は
- SUSE Linux Enterprise Server 15 SP1

  データ・ブローカーをインストールする前に'yum updateコマンドをホスト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。

root権限

データブローカーソフトウェアは、Linuxホストで自動的にルートとして実行されます。データブローカーの処理では、rootとして実行する必要があります。たとえば、共有をマウントするには、のように指定します

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

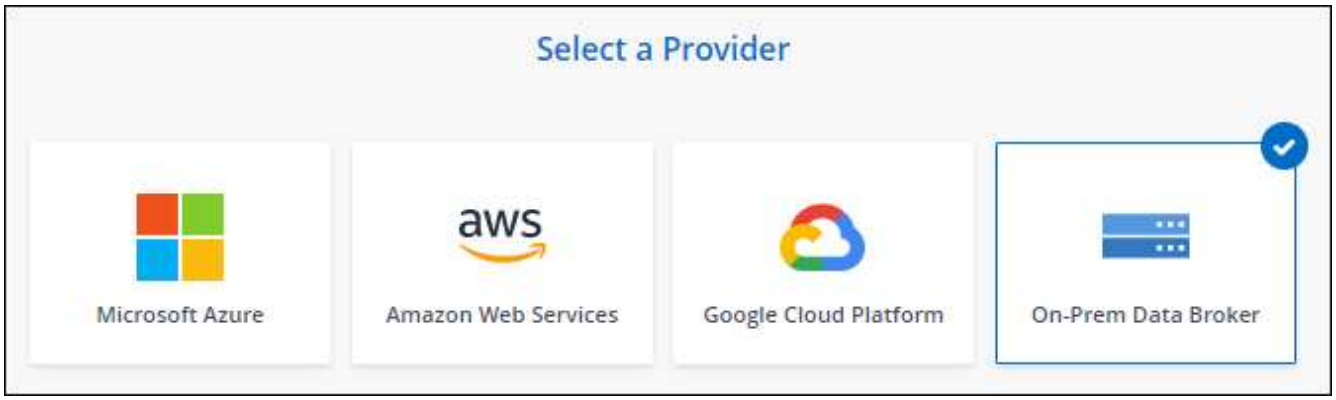
同期関係を作成するときに、 Linux ホストにデータブローカーをインストールできます。

手順

1. [新しい同期の作成]*を選択します。
2. [同期関係の定義]ページで、ソースとターゲットを選択し、*[続行]*を選択します。

   「 * 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. ページで、[データブローカーの作成]を選択し、[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]*を選択します。

   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。

      ユーザはローカルユーザである必要があります。ドメインユーザはサポートされません。

   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

        BlueXPのコピーと同期の手順ページにインストールファイルのURIが表示されます。プロンプトに従ってオンプレミスのデータブローカーを導入すると、このURIがロードされます。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。 BlueXPのコピーと同期から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、BlueXPのコピーと同期で*[続行]*を選択します。
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。