始めましょう
NetApp Copy and Sync

NetApp
December 16, 2025

目次

始めましょう

NetApp Copy and Syncについて学ぶ

NetApp Copy and Sync は、クラウド内またはオンプレミスの任意のターゲットにデータを移行するためのシンプルで安全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) オブジェクト形式、 NetApp StorageGRIDアプライアンス、またはその他のクラウド プロバイダー オブジェクト ストアのいずれであっても、Copy and Sync を使用すると変換して移動できます。

NetApp Console

NetApp Copy and Sync はNetApp Consoleからアクセスできます。

NetApp Consoleは、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとデータ サービスの集中管理を提供します。NetAppデータ サービスにアクセスして使用するには、コンソールが必要です。管理インターフェースとして、1 つのインターフェースから多数のストレージ リソースを管理できます。コンソール管理者は、企業内のすべてのシステムのストレージとサービスへのアクセスを制御できます。

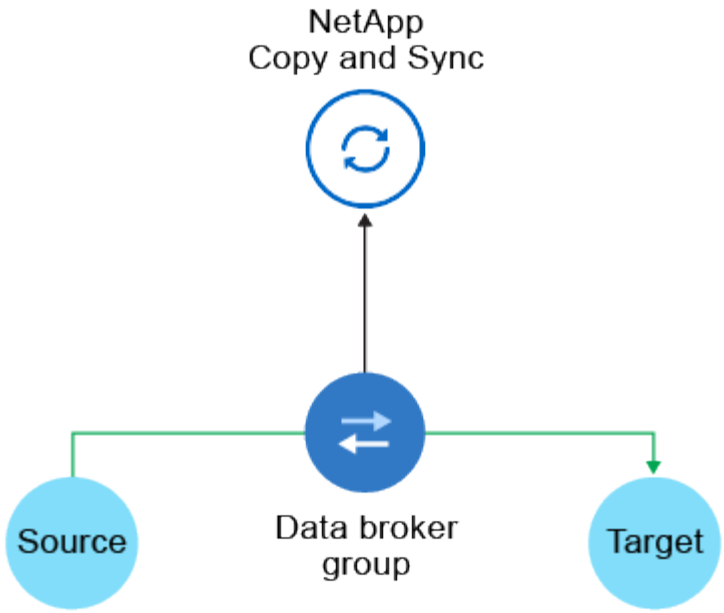
NetApp Consoleの使用を開始するためにライセンスやサブスクリプションは必要ありません。ストレージ システムまたはNetAppデータ サービスへの接続を確保するためにクラウドにコンソール エージェントを展開する必要がある場合にのみ料金が発生します。ただし、コンソールからアクセスできる一部のNetAppデータ サービスは、ライセンスまたはサブスクリプションベースです。

詳細はこちら "NetApp Console"。

NetApp Copy and Syncの仕組み

NetApp Copy and Sync は、データ ブローカー グループ、 NetApp Consoleから利用できるクラウドベースのインターフェイス、およびソースとターゲットで構成される SaaS (Software-as-a-Service) プラットフォームです。

次の図は、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。



NetApp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にデータを同期します (これを 同期関係 と呼びます)。データブローカーは、AWS、Azure、Google Cloud Platform、またはオンプレミスで実行できます。 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 グループには、Copy and Sync 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 経由の送信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する" 。

最初のコピーの後、コピーと同期は設定したスケジュールに基づいて変更されたデータを同期します。

サポートされているストレージ タイプ

コピーと同期は、次のストレージ タイプをサポートします。

- 任意のNFSサーバー
- 任意のSMBサーバー
- アマゾンEFS
- Amazon FSx for ONTAP
- Amazon S3
- Azure ブロブ
- Azure データレイクストレージ Gen2
- Azure NetApp Files
- ボックス（プレビューとして利用可能）
- Cloud Volumes ONTAP
- Google Cloud Storage
- Googleドライブ
- IBM Cloud Object Storage
- オンプレミスのONTAPクラスタ
- ONTAP S3 ストレージ

- SFTP（APIのみ使用）
- StorageGRID

"サポートされている同期関係を表示する" 。

費用

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

リソース料金は、クラウドで 1 つ以上のデータ 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 コストに関連します。

サービス料

14 日間の無料トライアルが終了した後、同期関係の料金を支払う方法は 2 つあります。最初のオプションは、AWS または Azure からサブスクライブすることです。これにより、時間単位または年単位で支払いが可能になります。 2 番目のオプションは、 NetApp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学ぶ" 。

NetApp Copy and Syncのクイックスタート

NetApp Copy and Sync の使用を開始するには、いくつかの手順が必要です。

1 **NetApp Console**にログインして設定する

NetApp Consoleの使用を開始しているはずです。これには、ログイン、アカウントの設定、コンソール エージェントの展開、システム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、まずシステムを作成または検出する必要があります。

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

Cloud Volumes ONTAP、オンプレミスのONTAPクラスター、およびAmazon FSx for ONTAPには、コンソールエージェントが必要です。

- "NetApp Consoleの使い方を学ぶ"
- "コンソールエージェントの詳細"

2 ソースとターゲットを準備する

ソースとターゲットがサポートされ、設定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間の接続を確認することです。

- "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する"

3 **NetApp**データブローカーの場所を準備する

NetApp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にデータを同期します (これを 同期関係 と呼びます)。データブローカーは、AWS、Azure、Google Cloud Platform、またはオンプレミスで実行できます。 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 グループには、 NetApp Copy and Sync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 経由の送信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する" 。

NetApp Copy and Sync は、同期関係を作成するときにインストール プロセスをガイドします。その時点で、クラウドにデータ ブローカーを展開したり、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。

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

4 最初の同期関係を作成する

ログイン "NetApp Console"をクリックし、[同期] を選択して、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。指示に従ってセットアップを完了します。"詳細情報" 。

5 無料トライアル終了後は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支払いでサブスクライブします。または、 NetAppから直接ライセンスを購入します。 NetApp Copy and Syncのライセンス設定ページに移動して設定するだけです。"詳細情報" 。

NetApp Copy and Syncでサポートされている同期関係

NetApp Copy and Sync 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。始める前に、サポートされている関係を理解しておく必要があります。

ソースの場所	サポートされているターゲットの場所
アマゾンEFS	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
Amazon FSx for ONTAP	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
Amazon S3	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • ボックス[1] • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure ブロブ	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
Azure データレイクストレージ Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • ONTAP向け FSx • IBM Cloud Object Storage • NFS サーバ • オンプレミスONTAP • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
Azure NetApp Files	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
ボックス[1]	• Amazon FSx for ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM Cloud Object Storage • NFS サーバ • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
Cloud Volumes ONTAP	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
Google Cloud Storage	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • 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

ソースの場所	サポートされているターゲットの場所
IBM Cloud Object Storage	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • ボックス[1] • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
NFS サーバ	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Googleドライブ • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID

ソースの場所	サポートされているターゲットの場所
オンプレミスのONTAPクラスタ（NFS または SMB）	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • SMB サーバ • StorageGRID
ONTAP S3 ストレージ	• Amazon S3 • Azure データレイクストレージ Gen2 • Google Cloud Storage • NFS サーバ • SMB サーバ • StorageGRID • ONTAP S3 ストレージ
SFTP [2]	S3

ソースの場所	サポートされているターゲットの場所
SMB サーバ	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Googleドライブ • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • ONTAP S3 ストレージ • SMB サーバ • StorageGRID
StorageGRID	• アマゾンEFS • Amazon FSx for ONTAP • Amazon S3 • Azure ブロブ • Azure データレイクストレージ Gen2 • Azure NetApp Files • ボックス[1] • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS サーバ • オンプレミスのONTAPクラスタ（NFS または SMB） • 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、コピーおよび同期 API の使用によってのみサポートされます。
3. BLOB コンテナーがターゲットの場合は、特定の Azure BLOB ストレージ層を選択できます。
    - ホットストレージ
    - クールストレージ
4. 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（これがデフォルトのクラスです）
    - インテリジェントティアリング
    - 標準-低頻度アクセス
    - 1つのゾーン - 低頻度アクセス
    - グレイシャーディープアーカイブ
    - 氷河フレキシブルリトリーバル
    - 氷河の即時検索
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。
    - Standard
    - ニアライン
    - コールドライン
    - アーカイブ

NetApp Copy and Syncでソースとターゲットを準備する

ソースとターゲットがNetApp Copy and Syncの次の要件を満たしていることを確認します。

ネットワーク

- ソースとターゲットは、データ ブローカー グループへのネットワーク接続を持っている必要があります。

  たとえば、NFS サーバーがデータセンターにあり、データブローカーが AWS にある場合は、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。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

ターゲット ディレクトリ

同期関係を作成するときに、「コピーと同期」を使用すると、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ーを作成できます。したがって、優先するターゲット ディレクトリがすでに存在することを確認してください。

ディレクトリの読み取り権限

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ーを表示するには、コピーと同期にそのディレクトリまたはフォルダーに対する読み取り権限が必要です。

NFS

ファイルとディレクトリの uid/gid を使用して、ソース/ターゲット上で権限を定義する必要があります。

オブジェクト ストレージ

- AWS および Google Cloud の場合、データ ブローカーにはリスト オブジェクト権限が必要です (データ ブローカーのインストール手順に従うと、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、同期関係を設定するときに入力する資格情報には、オブジェクトの一覧権限が必要です。

SMB

同期関係を設定するときに入力する SMB 資格情報には、リスト フォルダーのアクセス許可が必要です。

データブローカーは、デフォルトで次のディレクトリを無視します: .snapshot、~snapshot、.copy-offload

コピーと同期を使用して SMB データをCloud Volumes ONTAPにコピーする場合、ソース システムのファイルとフォルダーの所有権は保持されません。この動作は、コピーと同期が Linux SMB クライアントを使用し、転送の認証に使用されるユーザーまたはサービス アカウントに所有権を割り当てるために発生します。アクセス制御リストは保持される場合がありますが、所有権と監査情報はソース システムとは異なる場合があります。これは想定される動作です。

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てください。

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には、AWS またはオンプレミスにデプロイされたデータブローカーが必要です。どちらの場合でも、コピーと同期では、インストール中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を学ぶ"
- "Linuxホストにデータブローカーをインストールする方法を学ぶ"

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

同期関係を設定するときに、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 S3 バケットを指定できます。

"このJSONファイルに含まれる権限"データ ブローカーがアクセスできるようにするには、その S3 バケット

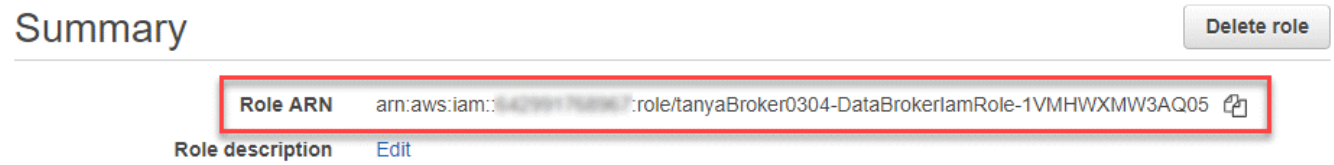
に適用する必要があります。これらの権限により、データ ブローカーはバケットとの間でデータをコピーしたり、バケット内のオブジェクトを一覧表示したりできるようになります。

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。

   - データブローカーが Linux ホストに手動でインストールされた場合、*RoleARN* は、データブローカーのデプロイ時に AWS 認証情報を指定した AWS ユーザーの ARN である必要があります。
   - CloudFormation テンプレートを使用してデータブローカーが AWS にデプロイされた場合、*RoleARN* はテンプレートによって作成された IAM ロールの ARN である必要があります。

     ロール ARN 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、[説明] タブから IAM ロールを選択します。その後、IAM コンソールにロール ARN を含む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てください。

Azure Blob でサポートされているデータ ブローカーの場所

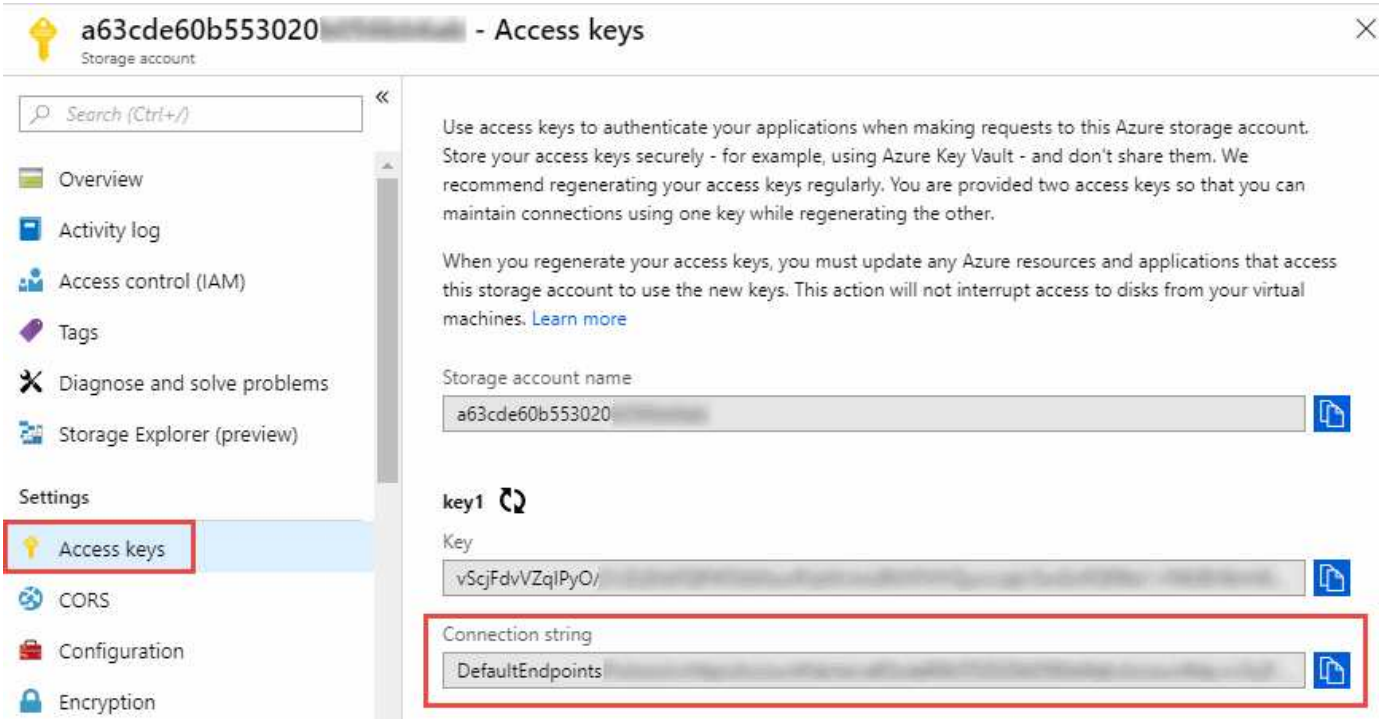
同期関係に Azure Blob Storage が含まれている場合、データ ブローカーは任意の場所に配置できます。

サポートされている**Azure**リージョン

中国、米国政府、米国国防総省地域を除くすべての地域がサポートされています。

Azure Blob と **NFS/SMB** を含む関係の接続文字列

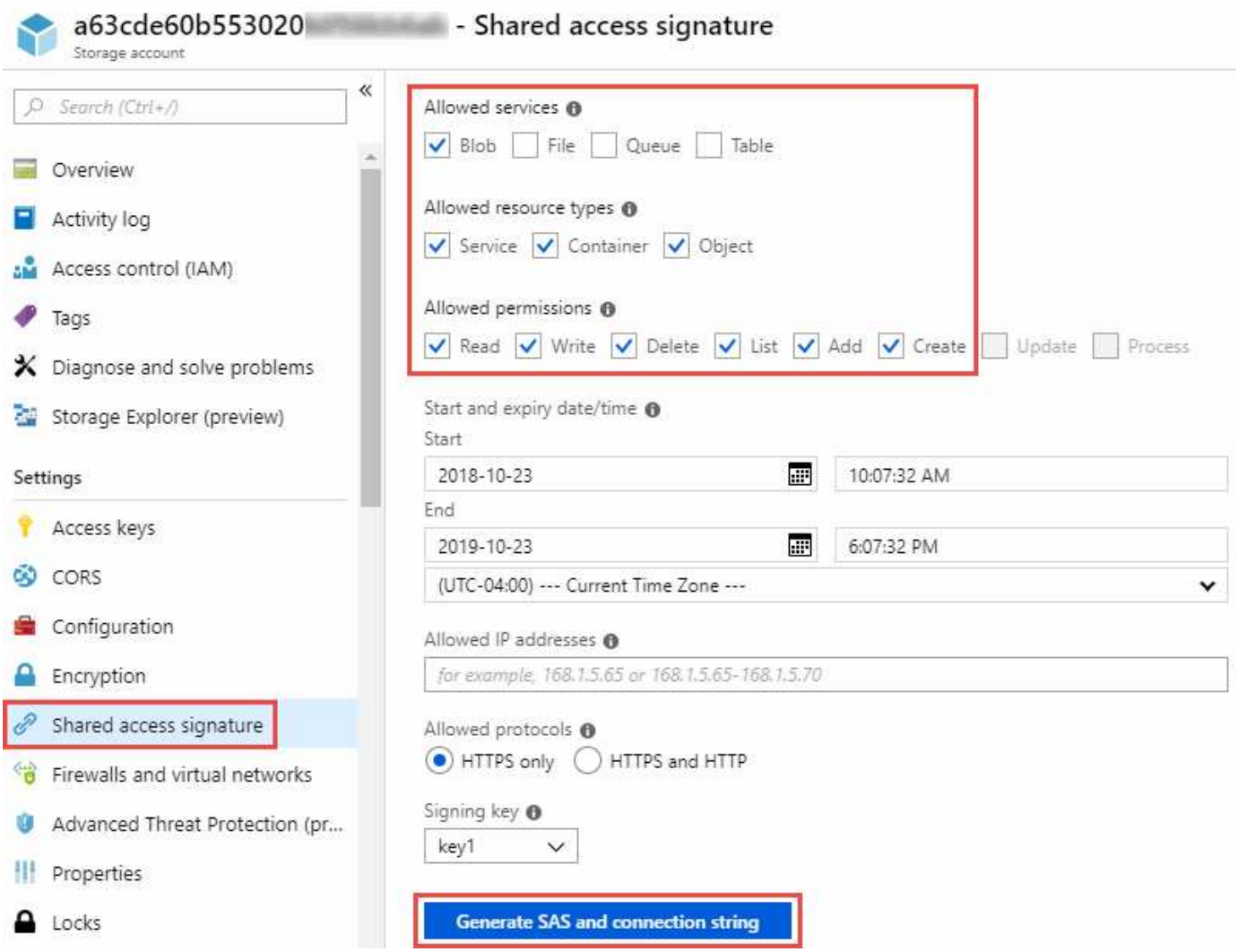
Azure BLOB コンテナーと NFS または SMB サーバー間の同期関係を作成するときは、Copy と Sync にストレージ アカウント接続文字列を指定する必要があります。



2つのAzure Blobコンテナ間でデータを同期したい場合は、接続文字列に "共有アクセス署名"（SAS）。また、Blob コンテナーと NFS または SMB サーバー間で同期するときに SAS を使用するオプションもあります。

SAS は、Blob サービスおよびすべてのリソース タイプ (サービス、コンテナー、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: 読み取りとリスト
- 対象のBLOBコンテナの場合: 読み取り、書き込み、一覧表示、追加、作成



を選択すると利用できます。"]

Azure BLOB コンテナーを含む継続的な同期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 接続文字列を使用する場合は、近い将来に期限切れになるように設定しないでください。

Azure データレイクストレージ Gen2

Azure Data Lake を含む同期関係を作成する場合は、Copy and Sync にストレージ アカウント接続文字列を提供する必要があります。共有アクセス署名 (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 サービス レベルが標準の場合、障害やパフォーマンスの問題が発生する可能性があります。

適切なサービス レベルを決定する際にサポートが必要な場合は、ソリューション アーキテクトにご相談ください。ボリューム サイズとボリューム ティアによって、取得できるスループットが決まります。

"Azure NetApp Files のサービス レベルとスループットの詳細" 。

ボックスの要件

- Box を含む同期関係を作成するには、次の資格情報を提供する必要があります。
  - クライアントID
  - Client secret
  - 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、次の設定が 1 に設定されている統合構成を持つデータ ブローカー グループを使用する必要があります。
  - スキャナの同時実行
  - スキャナプロセス制限
  - 転送者の同時実行
  - 転送プロセス制限

  "データブローカーグループの統一された構成を定義する方法を学びます" 。

Google Cloud Storage バケットの要件

Google Cloud Storage バケットが次の要件を満たしていることを確認してください。

Google Cloud Storage でサポートされているデータ ブローカーの場所

Google Cloud Storage を含む同期関係には、Google Cloud またはオンプレミスにデプロイされたデータ ブローカーが必要です。コピーと同期では、同期関係を作成するときに、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学ぶ"
- "Linuxホストにデータブローカーをインストールする方法を学ぶ"

サポートされている Google Cloud リージョン

すべての地域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ときに、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付与すると、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を学ぶ" 。

SnapMirrorの宛先に対する権限

同期関係のソースがSnapMirror の宛先 (読み取り専用) である場合、ソースからターゲットにデータを同期するには、「読み取り/リスト」権限で十分です。

Google Cloud バケットの暗号化

ターゲットの Google Cloud バケットは、顧客管理の KMS キーまたはデフォルトの Google 管理キーを使用して暗号化できます。バケットにすでに KMS 暗号化が追加されている場合は、デフォルトの Google 管理の暗号化が上書きされます。

顧客管理KMSキーを追加するには、 "正しい権限"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、次の情報を提供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メールアドレス
- Google ドライブにアクセスする権限を持つ Google Cloud サービス アカウントのメールアドレス
- 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 ドキュメントの指示に従ってください。

- "サービスアカウントと資格情報を作成する"
- "ドメイン全体の権限をサービス アカウントに委任する"

OAuth スコープ フィールドを編集するときは、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 サーバーは、 NetAppシステムでも非NetAppシステムでもかまいません。
- ファイル サーバーは、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。

  必要なバージョンをサーバー上で有効にする必要があります。
- 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* になっています。

ONTAPの要件

同期関係にCloud Volumes ONTAPまたはオンプレミスのONTAPクラスターが含まれており、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。 ACL をコピーするにはこれが必要です。

ONTAP S3 ストレージ要件

同期関係を設定すると、 "ONTAP S3 ストレージ" 、以下の情報を提供する必要があります。

- ONTAP S3に接続されているLIFのIPアドレス
- ONTAPが使用するように設定されているアクセス キーと秘密キー

SMBサーバの要件

- SMB サーバーは、 NetAppシステムでも非NetAppシステムでもかまいません。
- SMB サーバーに対する権限を持つ資格情報をコピーおよび同期に提供する必要があります。
  - ソース SMB サーバーには、リストと読み取りの権限が必要です。

    バックアップ オペレーター グループのメンバーは、ソース SMB サーバーでサポートされます。
  - ターゲット SMB サーバーには、リスト、読み取り、および書き込みの権限が必要です。
- ファイル サーバーは、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、3.11 がサポートされています。
- 「Administrators」グループに、ソース フォルダーとターゲット フォルダーに対する「フル コントロール」権限を付与します。

  この権限を付与しないと、データ ブローカーには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。この問題が発生すると、次のエラーが表示されます: 「getxattr error 95」

隠しディレクトリとファイルに対する **SMB** 制限

SMB 制限は、SMB サーバー間でデータを同期するときに隠しディレクトリとファイルに影響します。ソース SMB サーバー上のディレクトリまたはファイルのいずれかが Windows によって非表示になっている場合、非表示属性はターゲット SMB サーバーにコピーされません。

大文字と小文字を区別しない制限による **SMB** 同期の動作

SMB プロトコルは大文字と小文字を区別しません。つまり、大文字と小文字は同じものとして扱われます。同期関係に SMB サーバーが含まれており、ターゲットにデータがすでに存在する場合、この動作によりファイルが上書きされ、ディレクトリのコピー 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。コピーと同期によって「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」はソースのファイル「a」によって上書きされます。

ディレクトリの場合、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。コピーと同期が「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と、ディレクトリがすでに存在するというエラーがコピーと同期によって受信されます。その結果、コピーと同期では常に「b」という名前のディレクトリのコピーに失敗します。

この制限を回避する最善の方法は、データを空のディレクトリに同期することです。

NetApp Copy and Syncのネットワーク概要

NetApp Copy and Syncのネットワークには、データ ブローカー グループとソースおよびターゲットの場所間の接続、およびポート 443 経由のデータ ブローカーからの送信インターネット接続が含まれます。

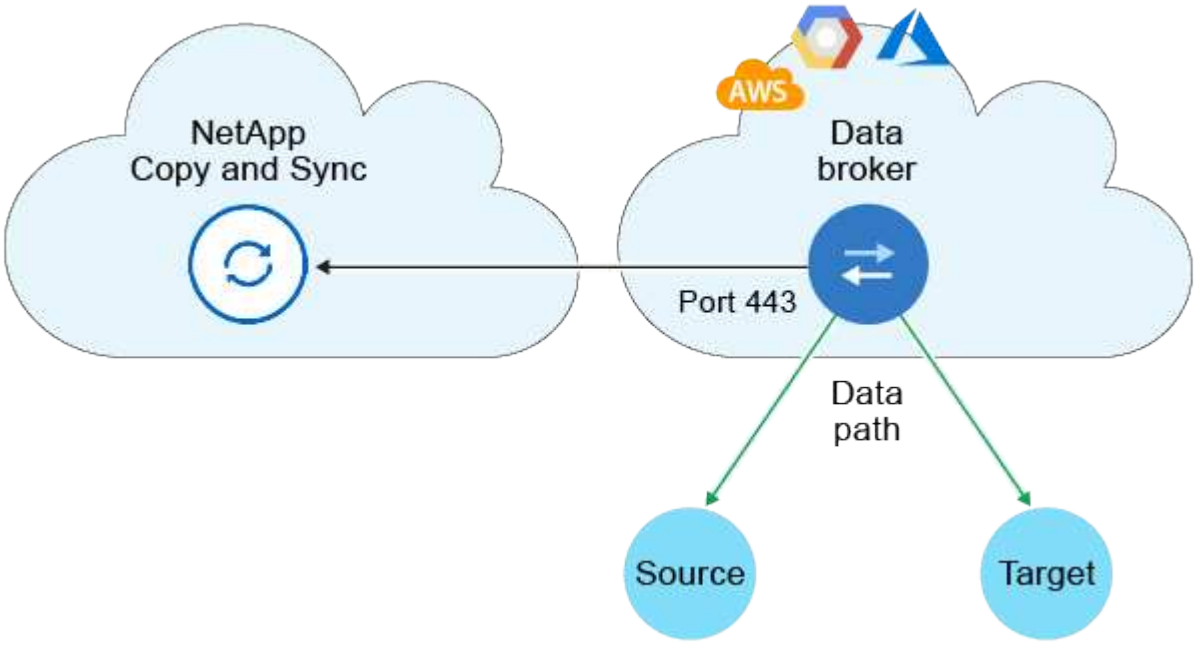
データブローカーの場所

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。

クラウド上のデータブローカー

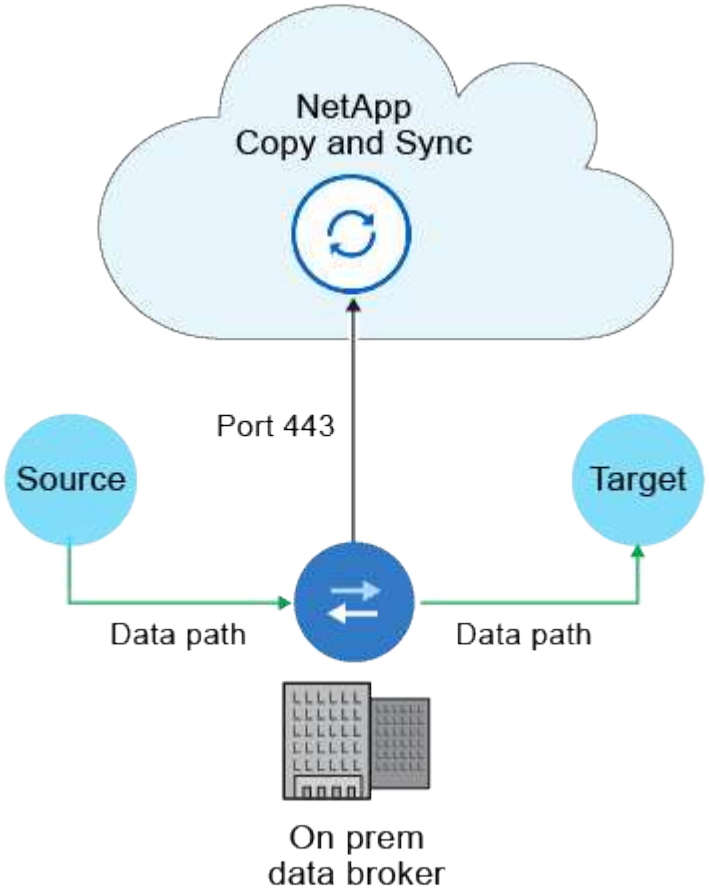
次の画像は、AWS、Google Cloud、または Azure のいずれかのクラウドで実行されているデータ ブローカーを示しています。データ ブローカーに接続している限り、ソースとターゲットは任意の場所に配置できます。たとえば、データセンターからクラウド プロバイダーへの VPN 接続がある場合があります。

Copy and Sync がデータ ブローカーを AWS、Azure、または Google Cloud にデプロイすると、必要な送信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。



オンプレミスのデータブローカー

次の図は、データセンター内の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。繰り返しになりますが、データ ブローカーに接続されていれば、ソースとターゲットは任意の場所に配置できます。



ネットワーク要件

- ソースとターゲットは、データ ブローカー グループへのネットワーク接続を持っている必要があります。

  たとえば、NFS サーバーがデータセンターにあり、データブローカーが AWS にある場合は、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 ブローカーには、ポート 443 経由でタスクのコピーと同期をポーリングできるように、送信インターネット接続が必要です。
- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

ネットワークエンドポイント

NetAppデータ ブローカーでは、コピーおよび同期と通信し、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 経由の送信インターネット アクセスが必要です。ローカル Web ブラウザでも、特定のアクションのためにエンドポイントへのアクセスが必要です。送信接続を制限する必要がある場合は、送信トラフィック用にファイアウォールを構成するときに、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接続します。

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の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:	開発で使用される Node.js、npm、その他のサードパーティ パッケージを更新するためにリポジトリに問い合わせます。
https://tgz.pm2.io	コピーと同期を監視するために使用されるサードパーティ パッケージである PM2 を更新するためのリポジトリにアクセスします。
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com	Copy and Sync が操作 (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 サービスに接続します。
https://s3.*region*.amazonaws.com 例: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["S3エンドポイントのリストについてはAWS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 に接続します。
https://s3.amazonaws.com/	Copy and 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 ファイルに圧縮し、us-east-1 リージョンの定義済み S3 バケットにログをアップロードします。
https://storage.googleapis.com/	同期関係で GCP バケットが使用されるときに Google Cloud に接続します。
https://storage-account.blob.core.windows.netAzure Data Lake Gen2 を使用する場合:https://storage-account.dfs.core.windows.net[]ここで、storage-account はユーザーのソース ストレージ アカウントです。	ユーザーの 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	Copy and Sync に連絡するには。
https://support.netapp.com	同期関係に BYOL ライセンスを使用する場合は、 NetApp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 をインストールします。 AutoSupportメッセージをNetAppテクニカル サポートに送信するには、7z が必要です。

エンドポイント	目的
https://sts.amazonaws.com https://sts.us-east-1.amazonaws.com	データブローカーが AWS にデプロイされている場合、またはオンプレミスにデプロイされていて AWS 認証情報が提供されている場合に、AWS 認証情報を検証します。データ ブローカーは、デプロイ中、更新時、および再起動時にこのエンドポイントに接続します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com	分類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、 NetApp Data Classificationに問い合わせます。
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</ em>.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ブラウザのエンドポイント

トラブルシューティングのためにログをダウンロードするには、Web ブラウザが次のエンドポイントにアクセスできる必要があります。

ログ.cloudsync.netapp.com:443

NetApp Copy and Syncにログイン

NetApp Consoleを使用してNetApp Copy and Syncにログインします。

コンソールにログインするには、 NetAppサポート サイトの認証情報を使用するか、電子メールとパスワードを使用してNetAppクラウド ログインにサインアップすることができます。 "ログインについて詳しくはこちら" 。

NetApp Copy and Sync は、アイデンティティ アクセス管理を使用して、各ユーザーの特定のアクションへのアクセスを制御します。

必要な**NetApp Console**ロール 組織管理者ロール。 "NetApp Consoleのアクセスロールについて学ぶ" 。

手順

1. ウェブブラウザを開いて、 "NetApp Console" 。

   NetApp Consoleのログイン ページが表示されます。

2. コンソールにログインします。
3. コンソールの左側のナビゲーションから、モビリティ > *コピーと同期*を選択します。

データブローカーをインストールする

NetApp Copy and Sync用の新しいデータブローカーを AWS に作成する

NetApp Copy and Syncの新しいデータ ブローカー グループを作成するときは、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 ソフトウェアをデプロイします。 NetApp Copy and Sync はインストール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

クラウド内またはオンプレミスの既存の 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。"詳細情報" 。

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。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- データ ブローカーには、ポート 443 経由でタスクのコピーと同期をポーリングできるように、送信インターネット接続が必要です。

  Copy and Sync が AWS にデータブローカーをデプロイすると、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。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 ブローカーを構成できることに注意してください。

  アウトバウンド接続を制限する必要がある場合は、"データブローカーが接続するエンドポイントのリスト" 。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

AWS にデータブローカーをデプロイするために必要な権限

データブローカーをデプロイするために使用するAWSユーザーアカウントには、次の権限が必要です。"NetAppが提供するこのポリシー" 。

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

Copy and Sync がデータ ブローカーをデプロイすると、データ ブローカー インスタンスの 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 ブローカーをデプロイすることもできます。組織に厳格なセキュリティ ポリシーがある場合は、このオプションを使用することをお勧めします。

IAM ロールは次の要件を満たしている必要があります。

- EC2 サービスには、信頼できるエンティティとして IAM ロールを引き受ける権限が必要です。
- "このJSONファイルで定義された権限"データブローカーが適切に機能するには、IAM ロールに添付する必要があります。

データブローカーをデプロイするときに IAM ロールを指定するには、以下の手順に従います。

データブローカーを作成する

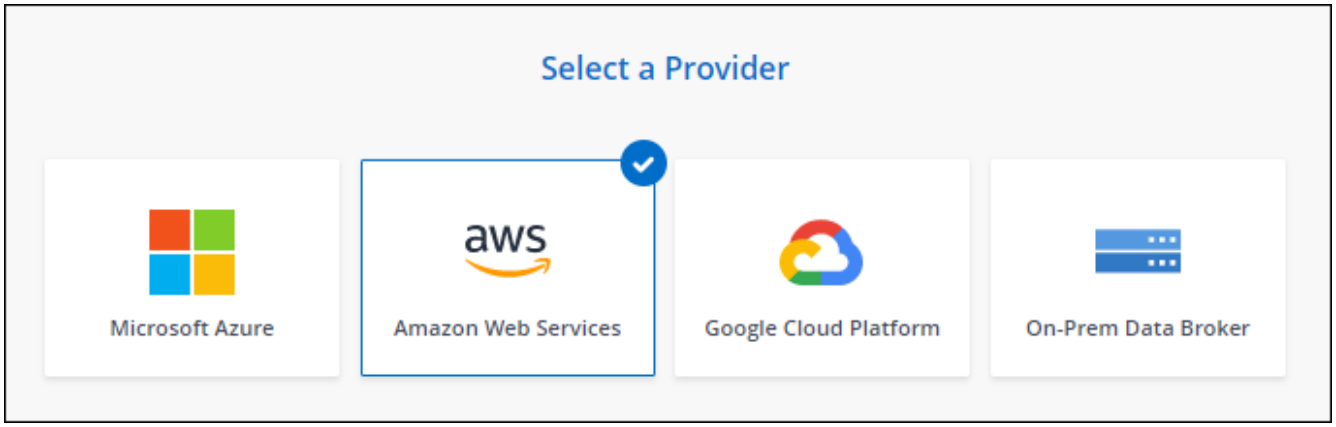
新しいデータ ブローカーを作成するには、いくつかの方法があります。これらの手順では、同期関係を作成するときに AWS にデータブローカーをインストールする方法について説明します。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *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 ページに到達するまで手順を完了します。

4. 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。



5. データ ブローカーの名前を入力し、[続行] を選択します。
6. AWS アクセスキーを入力すると、Copy and Sync がユーザーに代わって AWS にデータブローカーを作成できるようになります。

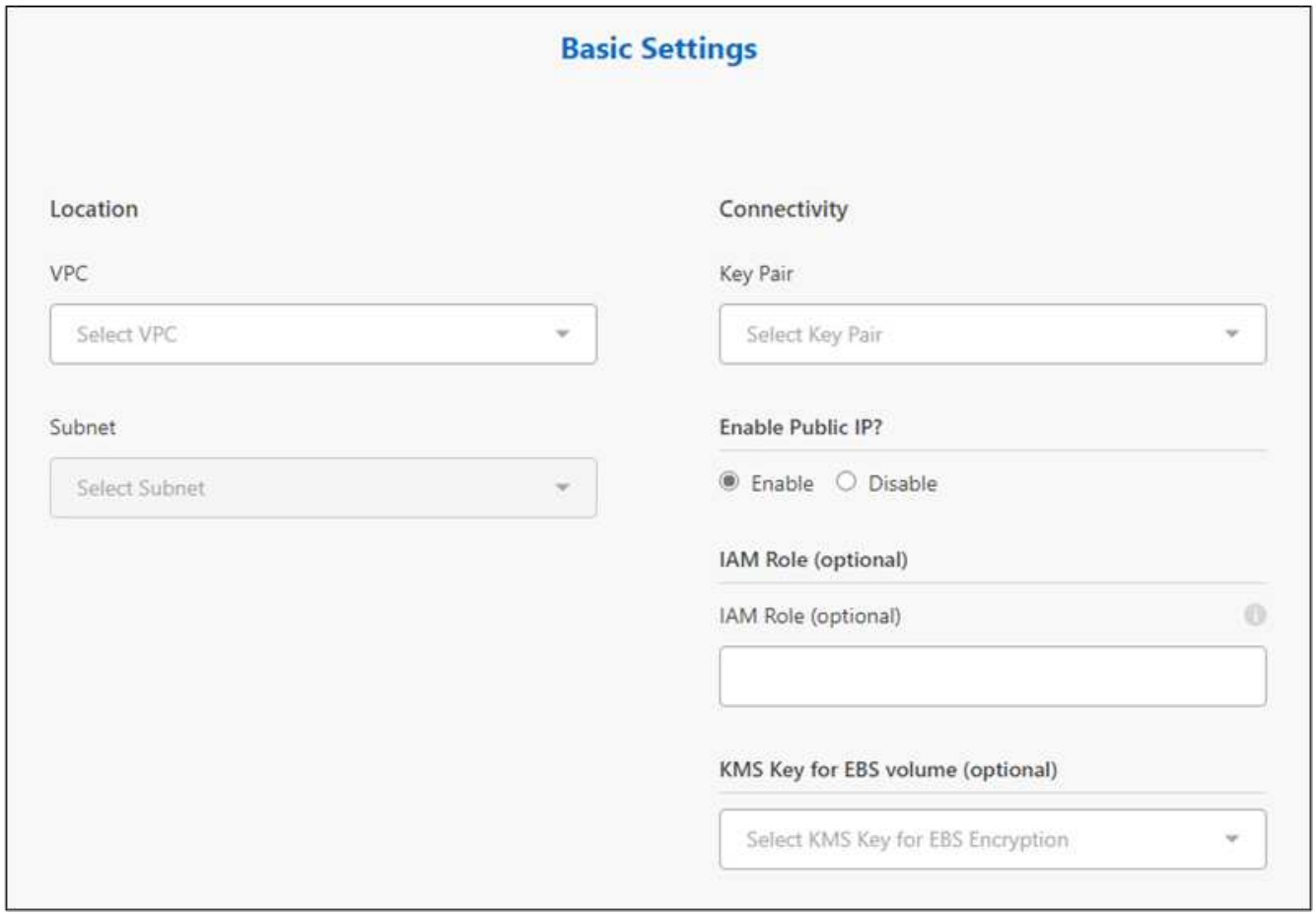
   キーは保存されず、他の目的にも使用されません。

   アクセス キーを提供したくない場合は、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、認証情報を提供する必要はありません。

   次のビデオでは、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示します。

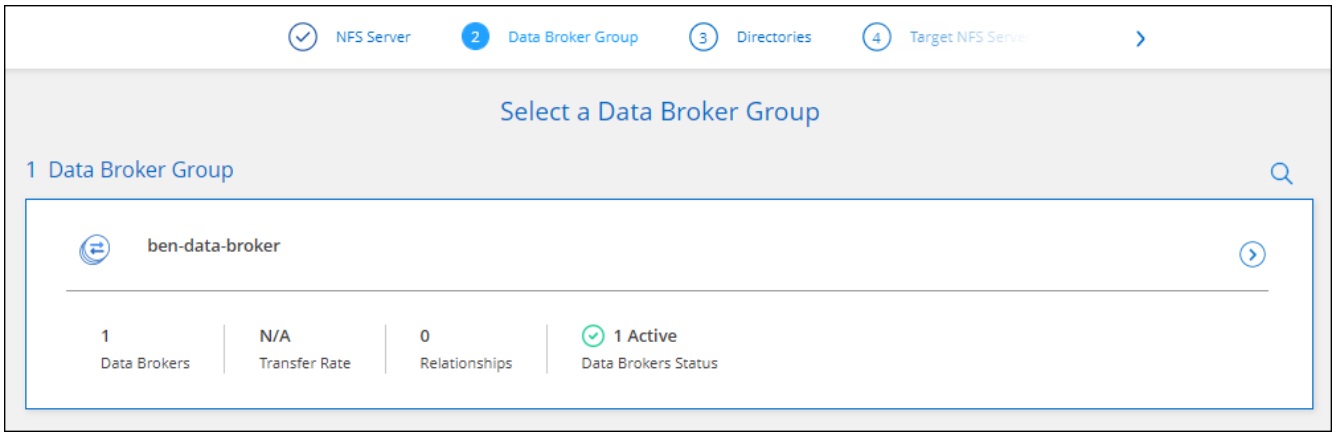
7. AWS アクセスキーを入力した場合は、インスタンスの場所を選択し、キーペアを選択し、パブリック IP アドレスを有効にするかどうかを選択し、既存の IAM ロールを選択するか、フィールドを空白のままにして、コピーと同期によってロールが自動的に作成されるようにします。 KMS キーを使用してデータ ブローカーを暗号化するオプションもあります。

   独自のIAMロールを選択した場合は、必要な権限を与える必要があります 。



8. 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、プロキシ設定を指定します。
9. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。

   次の画像は、AWS に正常にデプロイされたインスタンスを示しています。



10. ウィザードのページを完了して、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デプロイし、新しい同期関係を作成しました。このデータ ブローカー グループを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

コピーと同期は、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。

Node.js の互換性
: バージョン21.2.0

インスタンスタイプ
: リージョンで利用可能な場合は m5n.xlarge、そうでない場合は 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種類
: 10 GB GP2 SSD

Azure でNetApp Copy and Sync用の新しいデータ ブローカーを作成する

NetApp Copy and Syncの新しいデータ ブローカー グループを作成するときは、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 ソフトウェアを展開します。 NetApp Copy and Sync はインストール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

クラウド内またはオンプレミスの既存の 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。"詳細情報" 。

サポートされている**Azure**リージョン

中国、米国政府、米国国防総省地域を除くすべての地域がサポートされています。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- データ ブローカーには、ポート 443 経由でタスクのコピーおよび同期サービスをポーリングできるように、送信インターネット接続が必要です。

  コピーと同期によって Azure にデータ ブローカーがデプロイされると、必要な送信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。

  アウトバウンド接続を制限する必要がある場合は、"データブローカーが接続するエンドポイントのリスト" 。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

Azure にデータ ブローカーをデプロイするために必要な権限

データ ブローカーをデプロイするために使用する Azure ユーザー アカウントに次のアクセス許可があることを確認します。

```
{
    "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/agreements/write"

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

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

注：

1. 以下の権限は、 "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について:
    - '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/アクション',
    - 'Microsoft.EventGrid/systemTopics/read'、
    - 'Microsoft.EventGrid/systemTopics/write',
    - 'Microsoft.EventGrid/systemTopics/削除',
    - 'Microsoft.EventGrid/eventSubscriptions/write',
    - 'Microsoft.Storage/storageAccounts/write'

    さらに、Azure で継続的な同期を実装する予定の場合は、割り当て可能なスコープをリソース グループ スコープではなくサブスクリプション スコープ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/ネットワークセキュリティグループ/セキュリティルール/読み取り」
    - 「Microsoft.Network/networkSecurityGroups/読み取り」

認証方式

データ ブローカーをデプロイするときに、仮想マシンの認証方法 (パスワードまたは SSH 公開キーと秘密キーのペア) 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、以下を参照してください。 "Azure ドキュメント: Azure の Linux VM 用の SSH 公開キーと秘密キーのペアを作成して使用する" 。

データブローカーを作成する

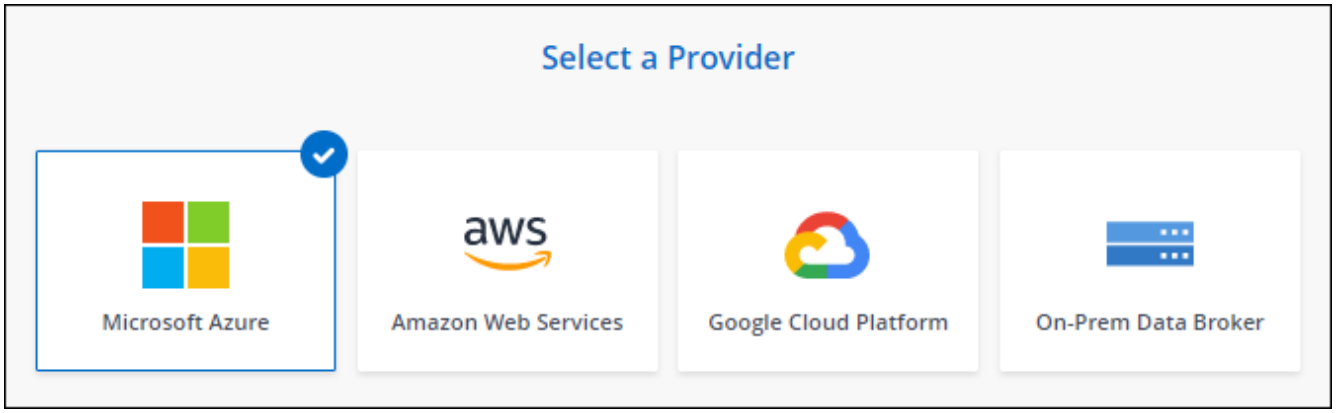
新しいデータ ブローカーを作成するには、いくつかの方法があります。次の手順では、同期関係を作成するときに Azure にデータ ブローカーをインストールする方法について説明します。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *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 ページに到達するまで手順を完了します。

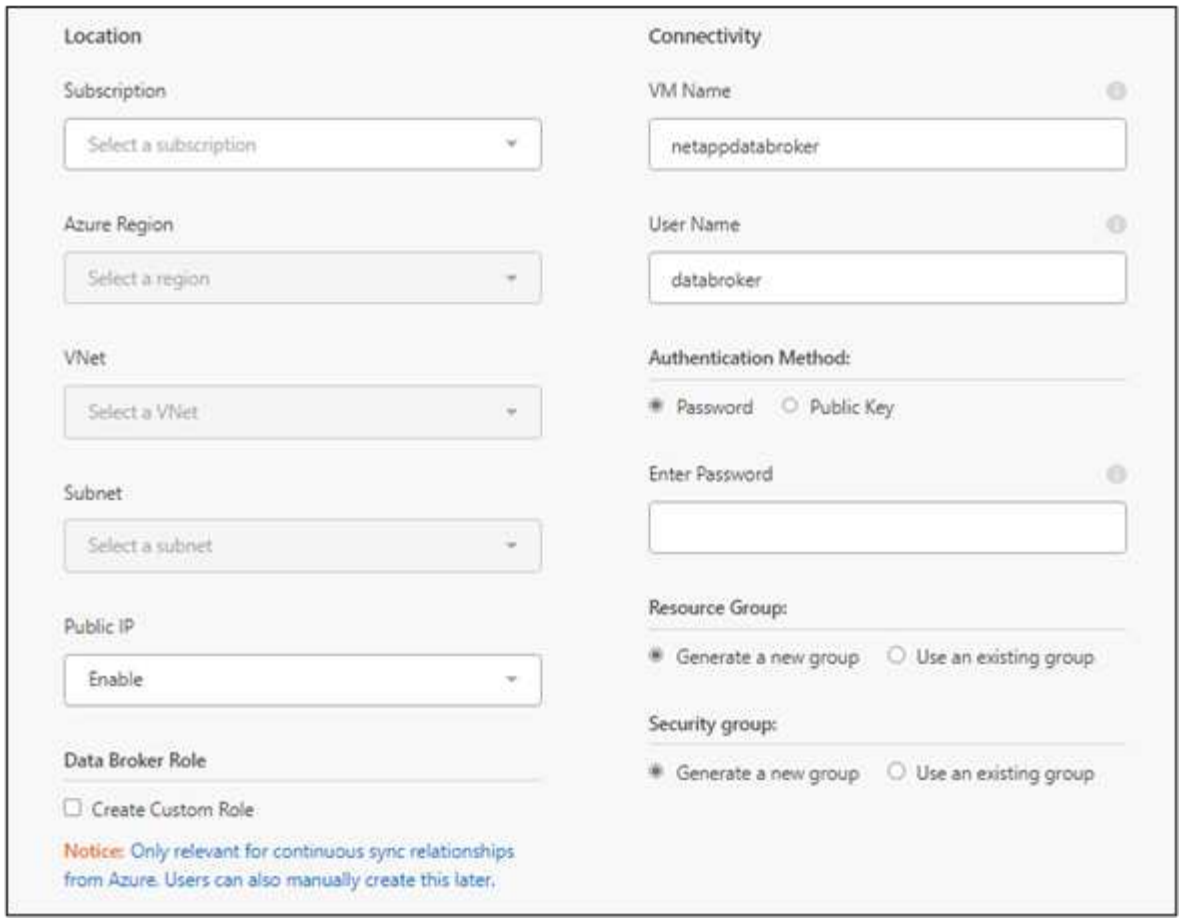
4. データ ブローカー グループ ページで、データ ブローカーの作成 を選択し、**Microsoft Azure** を選択します。



5. データ ブローカーの名前を入力し、[続行] を選択します。
6. 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 によって所有およびホストされています。資格情報がNetAppに提供されていません。

7. 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。



継続的な同期関係を実装する予定の場合は、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。

8. 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、プロキシ構成を指定します。
9. *続行*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 アクセスキーとシークレットキーを入力します。
10. *続行*を選択し、デプロイメント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 分かかる場合があります。

11. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。
12. ウィザードのページを完了して、新しい同期関係を作成します。

結果

Azure にデータ ブローカーをデプロイし、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で使用できます。

管理者の同意が必要であるというメッセージが表示されていますか?

コピーと同期にはユーザーに代わって組織内のリソースに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と Microsoft から通知された場合は、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付与するよう依頼してください。

   Azure で、管理センター **> Azure AD >** ユーザーとグループ **>** ユーザー設定 に移動し、ユーザーはアプリが自分に代わって会社のデータにアクセスすることに同意できます を有効にします。

2. 次の URL (管理者の同意エンドポイント) を使用して、AD 管理者に代わって **CloudSync-AzureDataBrokerCreator** に同意するよう依頼します。

   https://login.microsoftonline.com/{テナントIDを入力してください}/v2.0/adminconsent?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

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

データブローカー**VM**の詳細

コピーと同期は、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。

Node.js の互換性
: バージョン21.2.0

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
: ロッキーLinux 9.0

ディスクのサイズと種類
: 64 GB プレミアム SSD

Google Cloud で**NetApp Copy and Sync**用の新しいデータ ブローカーを作成する

NetApp Copy and Syncの新しいデータ 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 ソフトウェアをデプロイします。 NetApp Copy and Sync はインスト

ール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

クラウド内またはオンプレミスの既存の 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。"詳細情報" 。

サポートされている **Google Cloud** リージョン

すべての地域がサポートされています。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、root として実行する必要があります。たとえば、共有をマウントします。

ネットワーク要件

- データ ブローカーには、ポート 443 経由でタスクのコピーと同期をポーリングできるように、送信インターネット接続が必要です。

  Copy and Sync が Google Cloud にデータ ブローカーをデプロイすると、必要な送信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。

  アウトバウンド接続を制限する必要がある場合は、"データブローカーが接続するエンドポイントのリスト" 。

- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

Google Cloud にデータブローカーをデプロイするために必要な権限

データ ブローカーをデプロイする Google Cloud ユーザー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 ブローカーをデプロイするときは、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」権限は、外部の HashiCorp ボールトを使用するようにデータ ブローカーを設定する場合にのみ必要です。
2. 「pubsub.*」および「storage.buckets.update」権限は、Google Cloud Storage から別のクラウド ストレージの場所への同期関係で継続的な同期設定を有効にする場合にのみ必要です。"継続同期オプションの詳細" 。
3. 「cloudkms.cryptoKeys.list」および「cloudkms.keyRings.list」権限は、ターゲットの Google Cloud Storage バケットで顧客管理の KMS キーを使用する予定の場合にのみ必要です。

データブローカーを作成する

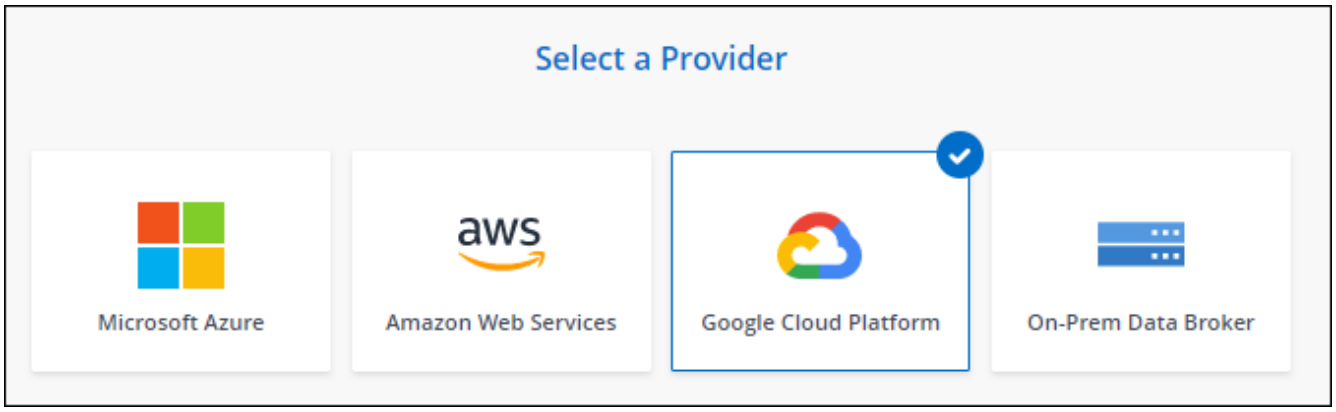
新しいデータ ブローカーを作成するには、いくつかの方法があります。次の手順では、同期関係を作成するときに Google Cloud にデータ ブローカーをインストールする方法について説明します。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *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 ページに到達するまで手順を完了します。

4. 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。

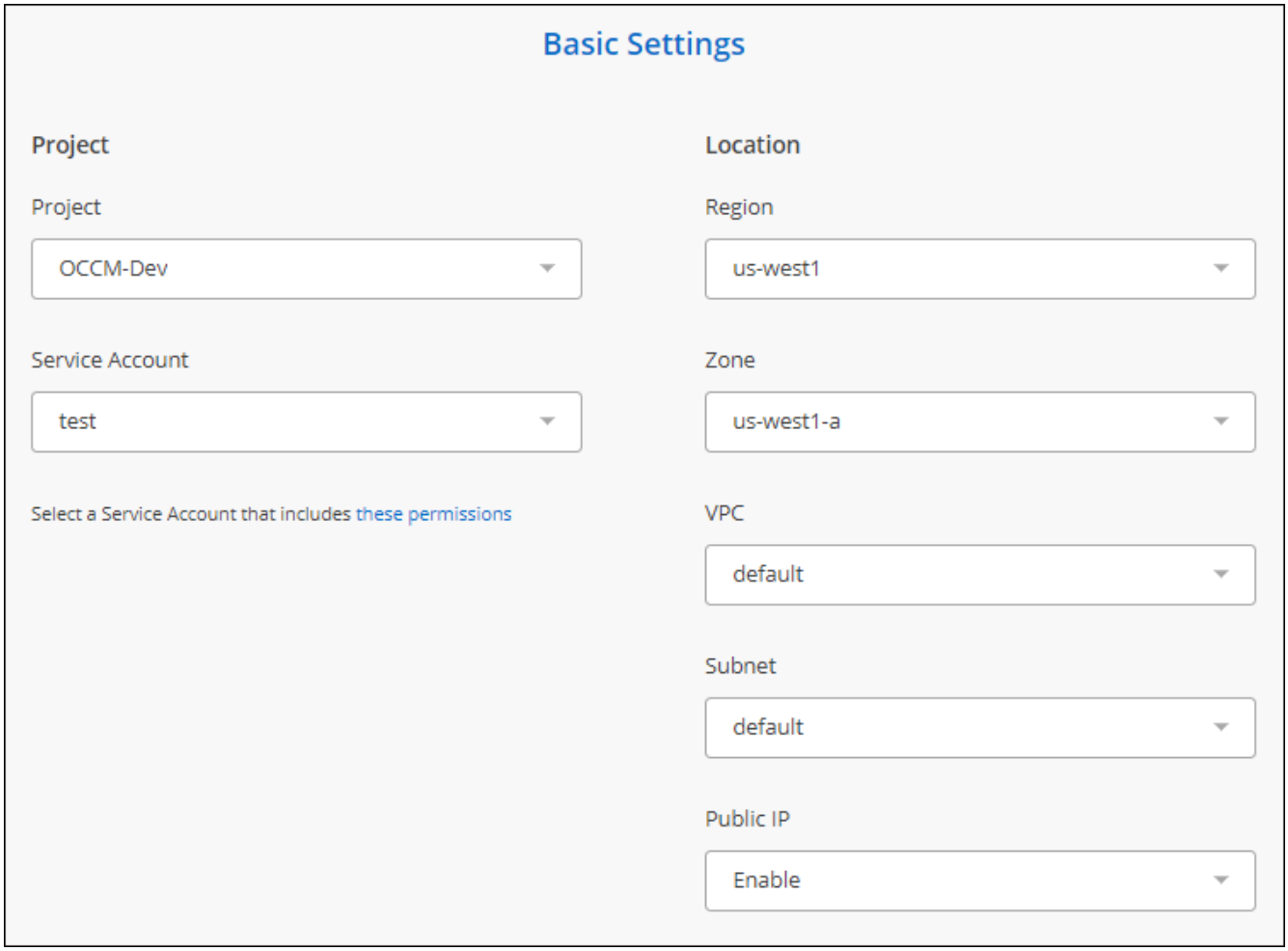


5. データ ブローカーの名前を入力し、[続行] を選択します。
6. プロンプトが表示されたら、Google アカウントでログインします。

   このフォームは Google が所有し、ホストしています。資格情報がNetAppに提供されていません。

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

   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。



8. 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、プロキシを Google Cloud 内に配置して、データ ブローカーと同じサービス アカウントを使用する必要があります。

9. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。

   インスタンスのデプロイには約 5 ～ 10 分かかります。コピーと同期の進行状況を監視できます。インスタンスが利用可能になると、自動的に更新されます。

10. ウィザードのページを完了して、新しい同期関係を作成します。

結果

Google Cloud にデータ ブローカーをデプロイし、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で使用できます。

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、コピーと同期により、データブローカーのサービス アカウントが使用権限を持つ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、データ ブローカー サービス アカウントと同じプロジェクトにあるバケットが含まれます。ただし、必要な権限を付与すれば、他のプロジェクト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 サービスを読み込みます。
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. 提供する役割を選択してください上記と同じ権限。
7. *保存*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

コピーと同期は、次の構成を使用して Google Cloud にデータ ブローカーを作成します。

Node.js の互換性
: バージョン21.2.0

機械の種類
: n2-標準-4

vCPU
: 4

RAM
: 15 GB

オペレーティング システム
: ロッキーLinux 9.0

ディスクのサイズと種類
: 20 GB HDD PD標準

NetApp Copy and Sync用のデータ ブローカーを **Linux** ホストにインストールします。

NetApp Copy and Syncの新しいデータ ブローカー グループを作成する場合は、オンプレミス 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。 NetApp Copy and Sync はインストール プロセスをガイドしますが、インストールの準備に役立つように、このページに要件と手順が繰り返し記載されています。

Linuxホストの要件

- **Node.js** 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 Streamはサポートされていません。
  - Red Hat Enterprise Linux 8.5、8.8、8.9、および 9.4
  - ロッキーLinux 9
  - Ubuntu Server 20.04 LTS、23.04 LTS、および 24.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    コマンド `yum update`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 Subscription Management 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製ソフトウェアを更新するためのリポジトリにアクセスできません。
- **RAM**: 16 GB
- **CPU**: 4コア
- 空きディスク容量: 10 GB
- **SELinux**: ホスト上で SELinux を無効にすることをお勧めします。

  SELinux は、データ ブローカー ソフトウェアの更新をブロックするポリシーを適用し、通常の操作に必要なエンドポイントへのデータ ブローカーの接続をブロックできます。

ルート権限

データ ブローカー ソフトウェアは、Linux ホスト上で自動的に root として実行されます。データ ブローカーを操作するには、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 サーバーは、Linux ホストが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。
- AWS への送信トラフィック用に、Linux ホストでポート 443 が開いている必要があります (データブローカーは Amazon SQS サービスと常に通信します)。
- NetApp、ソース、ターゲット、およびデータ ブローカーをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。 3 つのコンポーネント間の時間差は 5 分を超えてはなりません。

AWSへのアクセスを有効にする

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予定の場合は、AWS アクセス用に Linux ホストを準備する必要があります。データブローカーをインストールするときは、プログラムによるアクセスと特定の権限を持つ AWS ユーザーに AWS キーを提供する必要があります。

手順

1. IAMポリシーを作成する "NetAppが提供するこのポリシー"

   "AWS の手順を見る"

2. プログラムによるアクセス権を持つ IAM ユーザーを作成します。

   "AWS の手順を見る"

   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ので、必ずコピーしてください。

Google Cloudへのアクセスを有効にする

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予定の場合は、Google Cloud アクセス用に Linux ホストを準備する必要があります。データ ブローカーをインストールするときは、特定の権限を持つサービス アカウントのキーを指定する必要があります。

手順

1. ストレージ管理者権限を持つ Google Cloud サービス アカウントをまだお持ちでない場合は作成します。
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 の手順を見る"

   ファイルには少なくとも次のプロパティが含まれている必要があります: "project_id"、"private_key"、および "client_email"

   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する

Azure へのアクセスは、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することにより、関係ごとに定義されます。

データブローカーをインストールする

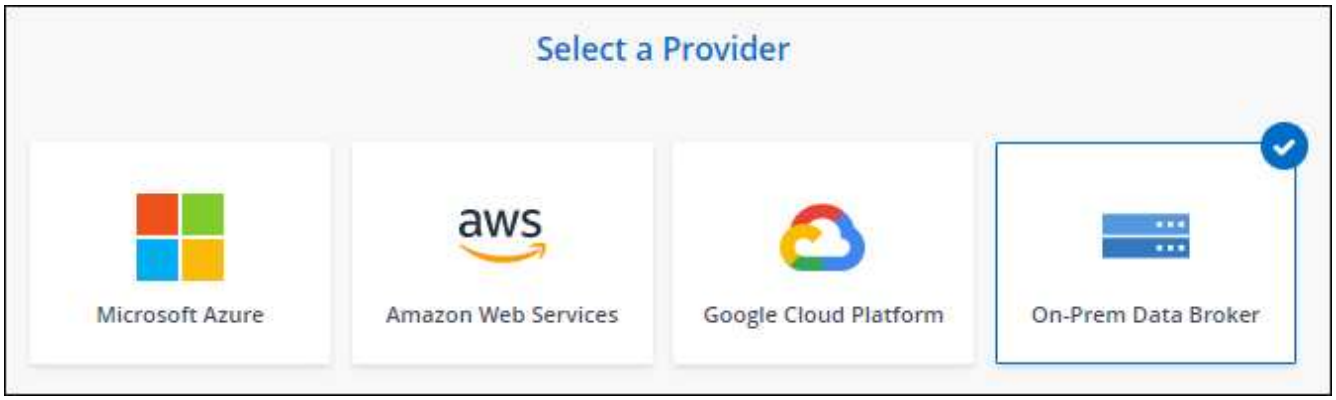
同期関係を作成するときに、Linux ホストにデータ ブローカーをインストールできます。

手順

1. "コピーと同期にログイン" 。
2. *新しい同期を作成*を選択します。
3. *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 ページに到達するまで手順を完了します。

4. 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、オンプレミス データ ブローカー を選択します。



このオプションには ***On-Prem*** **Data Broker** というラベルが付いていますが、オンプレミスまたはクラウド内の Linux ホストに適用されます。

5. データ ブローカーの名前を入力し、[続行] を選択します。

   説明ページがすぐに読み込まれます。以下の手順に従う必要があります。手順にはインストーラー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。

6. 説明ページで：

   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 オプションを選択します: プロキシなし、プロキシ サーバーを使用する、または 認証付きプロキシ サーバーを使用する。

      ユーザーはローカル ユーザーである必要があります。ドメイン ユーザーはサポートされていません。

   c. コマンドを使用して、データ ブローカーをダウンロードしてインストールします。

      次の手順では、可能な各インストール オプションの詳細について説明します。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、指示ページに従ってください。

   d. インストーラーをダウンロードしてください:

      - プロキシなし:

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

      - プロキシサーバーを使用する:

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

      - 認証付きプロキシサーバーを使用する:

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

        URI

        「コピーと同期」では、指示ページにインストール ファイルの URI が表示されます。この URI は、プロンプトに従ってオンプレミス データ ブローカーを展開すると読み込まれます。

リンクは動的に生成され、一度しか使用できないため、この URI はここでは繰り返されません。コピーと同期からURIを取得するには、次の手順に従います。 。

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

> 以下にリストされている各コマンドには、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、指示ページに従ってください。

- プロキシ設定なし:

```
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_file>
```

- 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>
```

- 認証付きプロキシ構成:

```
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、ユーザーが準備しておくべきキーです以下の手順に従ってください。 AWS キーは、オンプレミスまたはクラウド ネットワークで実行されるデータ ブローカーに保存されます。 NetApp はデータ ブローカーの外部ではキーを使用しません。

JSONファイル

これは、準備しておくべきサービスアカウントキーを含むJSONファイルです。以下の手順に従ってください 。

7. データ ブローカーが利用可能になったら、[コピーと同期] で [続行] を選択します。
8. ウィザードのページを完了して、新しい同期関係を作成します。