データブローカーをインストール

BlueXP copy and sync

NetApp
April 29, 2024

目次

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

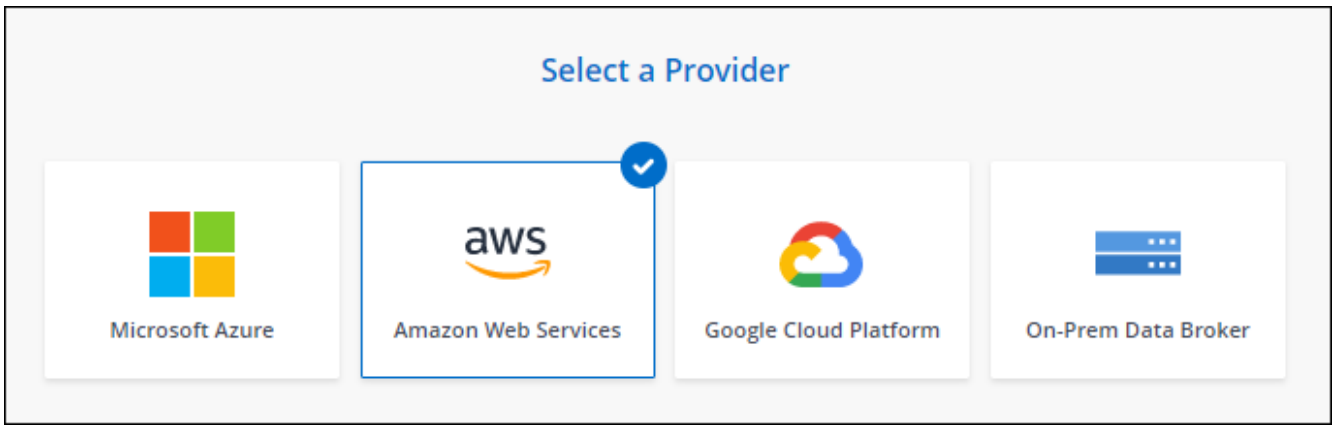
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを AWS にインストールする方法について説明します。

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。

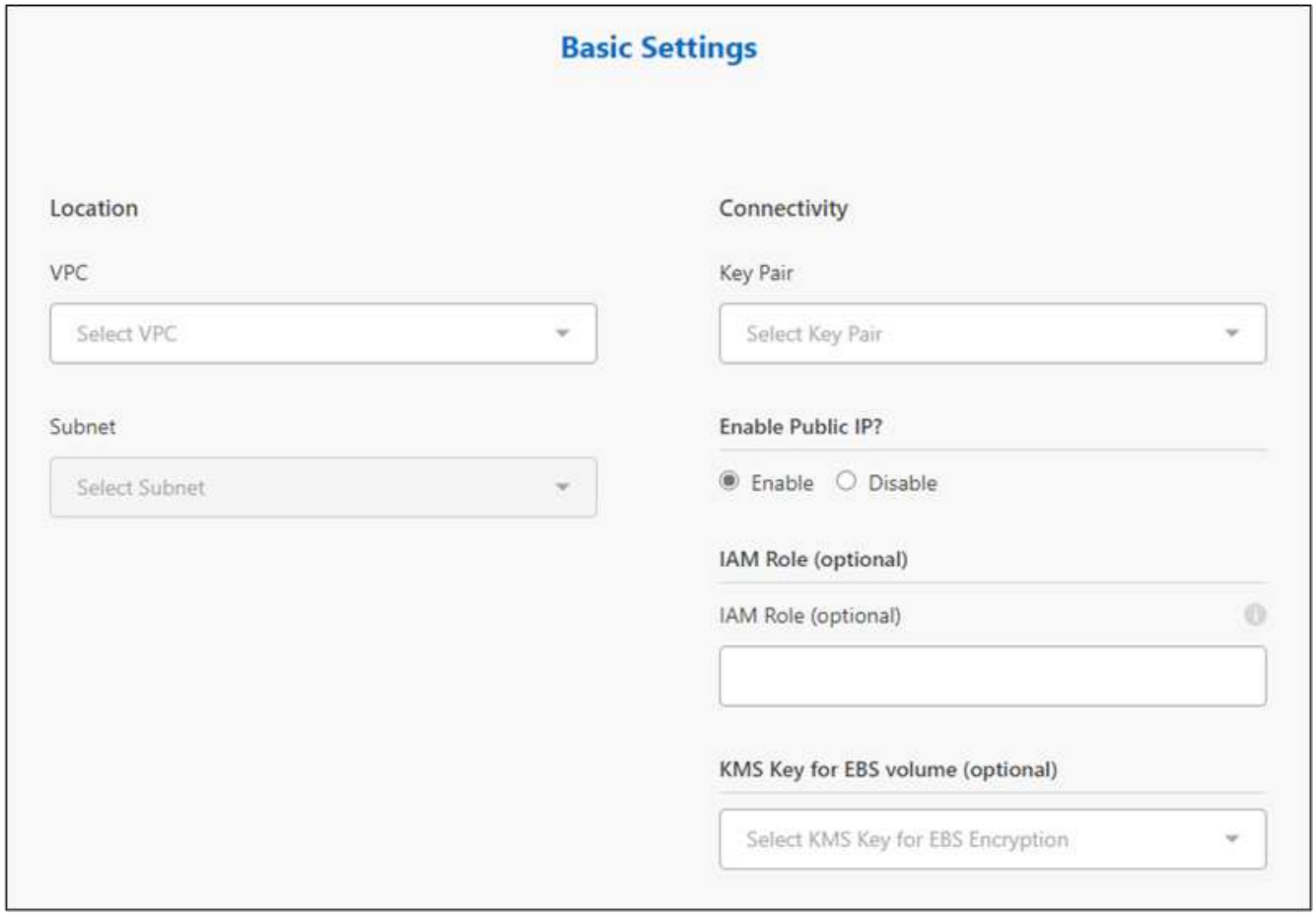
   CloudFormation テンプレートを使用してデータブローカーインスタンスを起動する方法を紹介したビデオを次に示します。

   ▶ 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

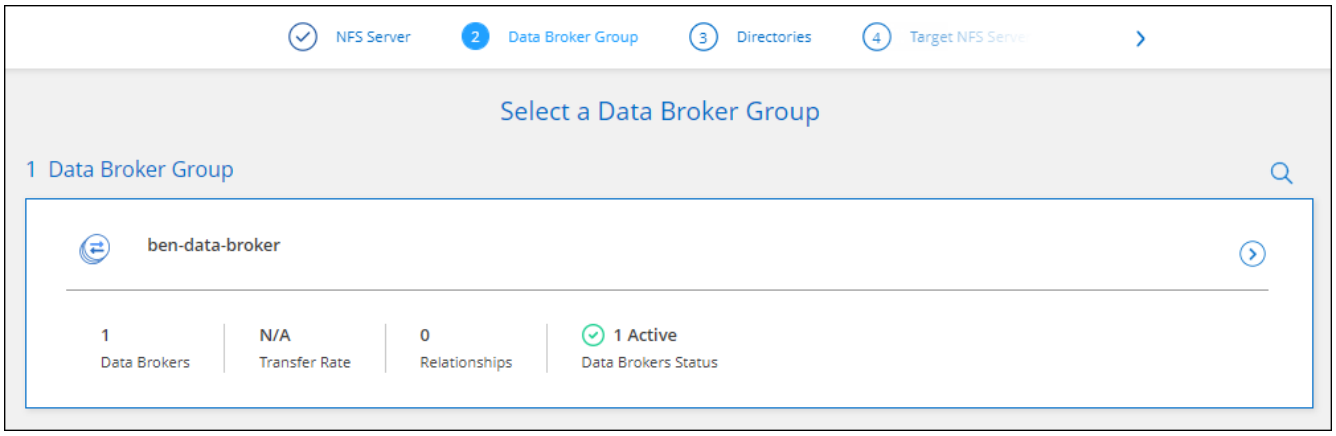
のままにしてBlueXPのコピーと同期でロールが作成されます。また、KMSキーを使用してデータブローカーを暗号化することもできます。

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

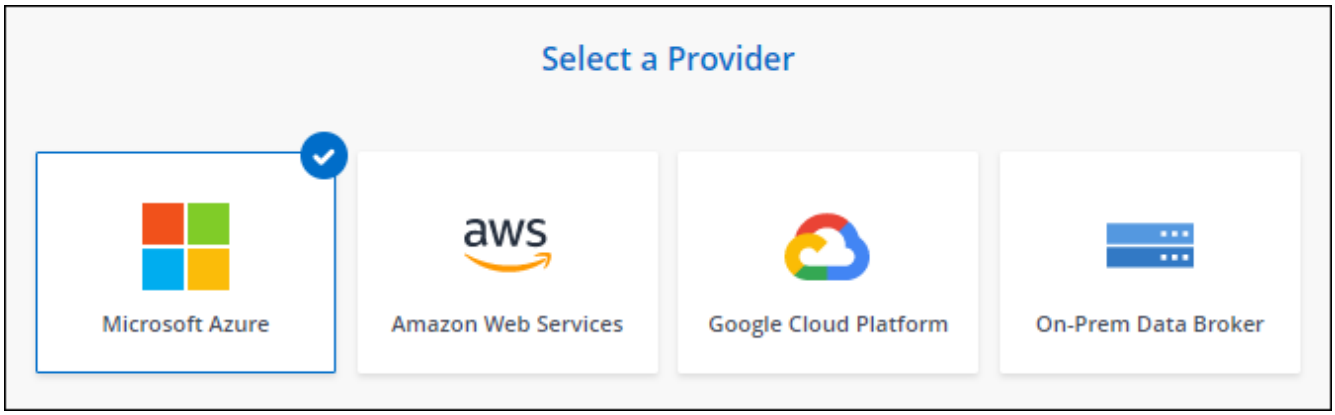
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成する際にデータブローカーを Azure にインストールする方法について説明します。

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。

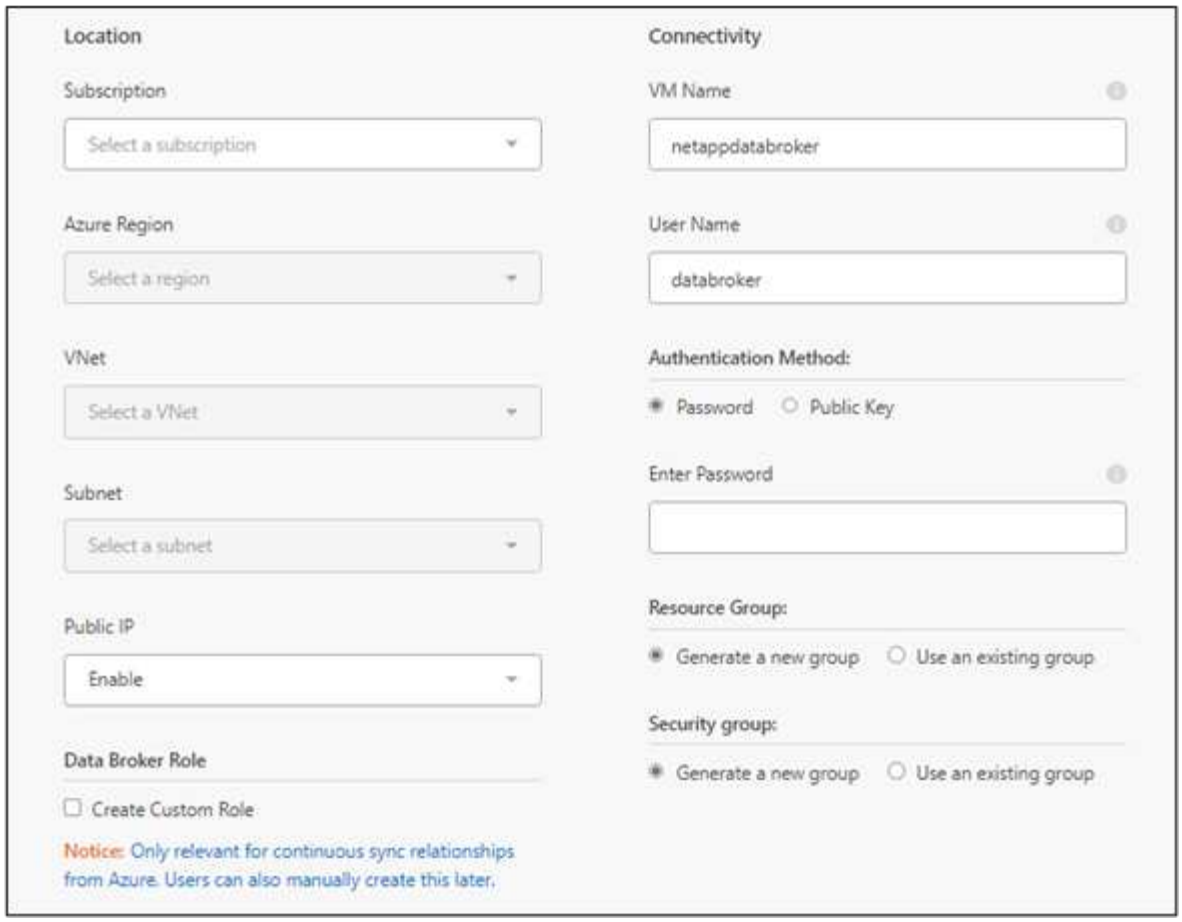
3. [データブローカーグループ]ページで、**[**データブローカーの作成**]***を選択し、[Microsoft Azure]*を選択します。



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

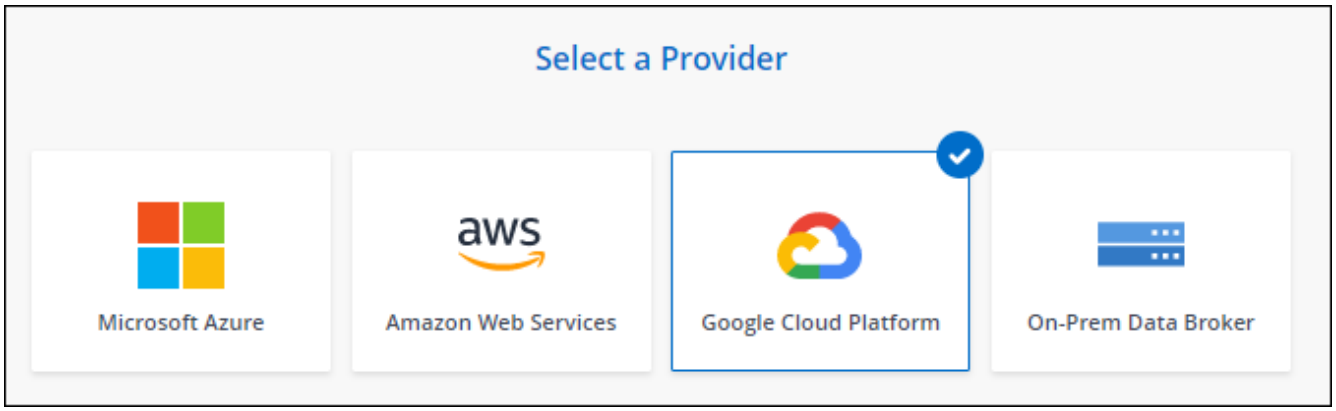
新しいデータブローカーを作成する方法はいくつかあります。以下の手順では、同期関係を作成するときにデータブローカーを Google Cloud にインストールする方法について説明します。

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。

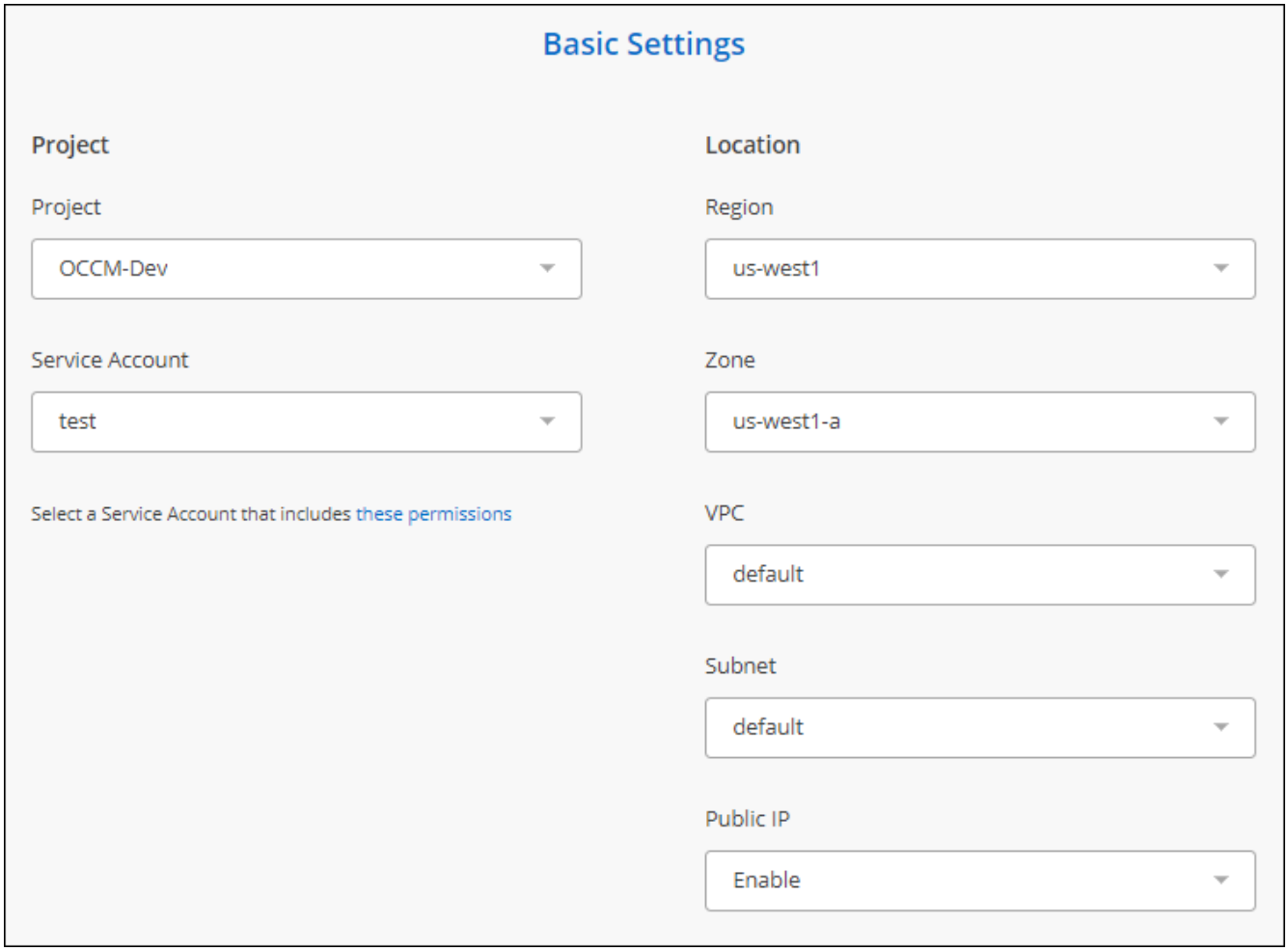


4. データブローカーの名前を入力し、*[続行]*を選択します。
5. メッセージが表示されたら、 Google アカウントでログインします。

   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

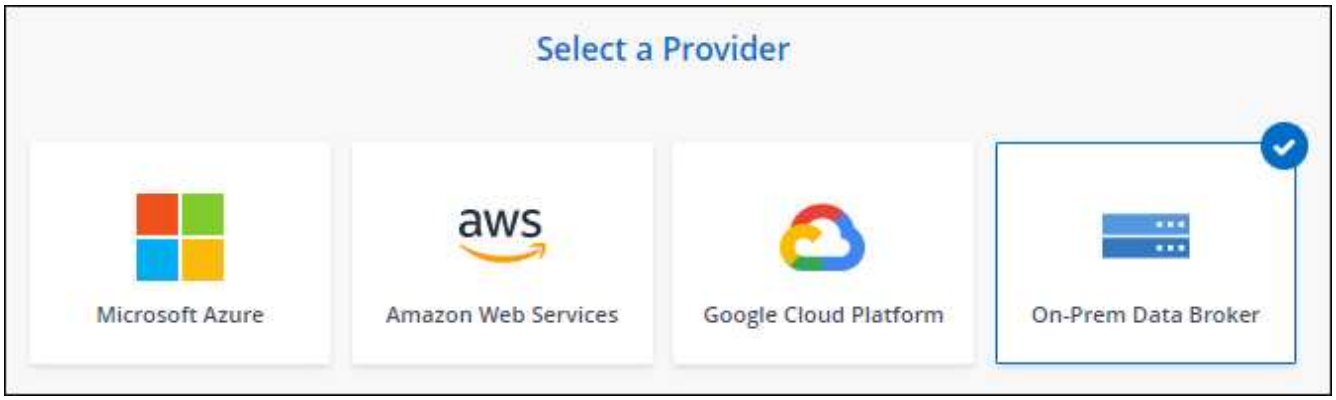
同期関係を作成するときに、 Linux ホストにデータブローカーをインストールできます。

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。