データブローカーをインストールする

NetApp Copy and Sync

NetApp
November 06, 2025

目次

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

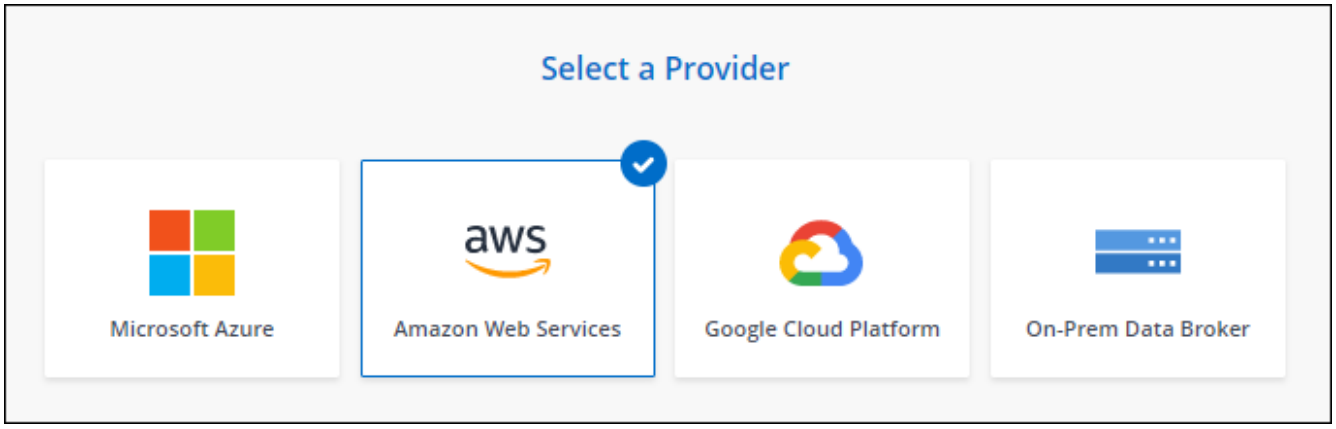
新しいデータ ブローカーを作成するには、いくつかの方法があります。これらの手順では、同期関係を作成するときに AWS にデータブローカーをインストールする方法について説明します。

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。

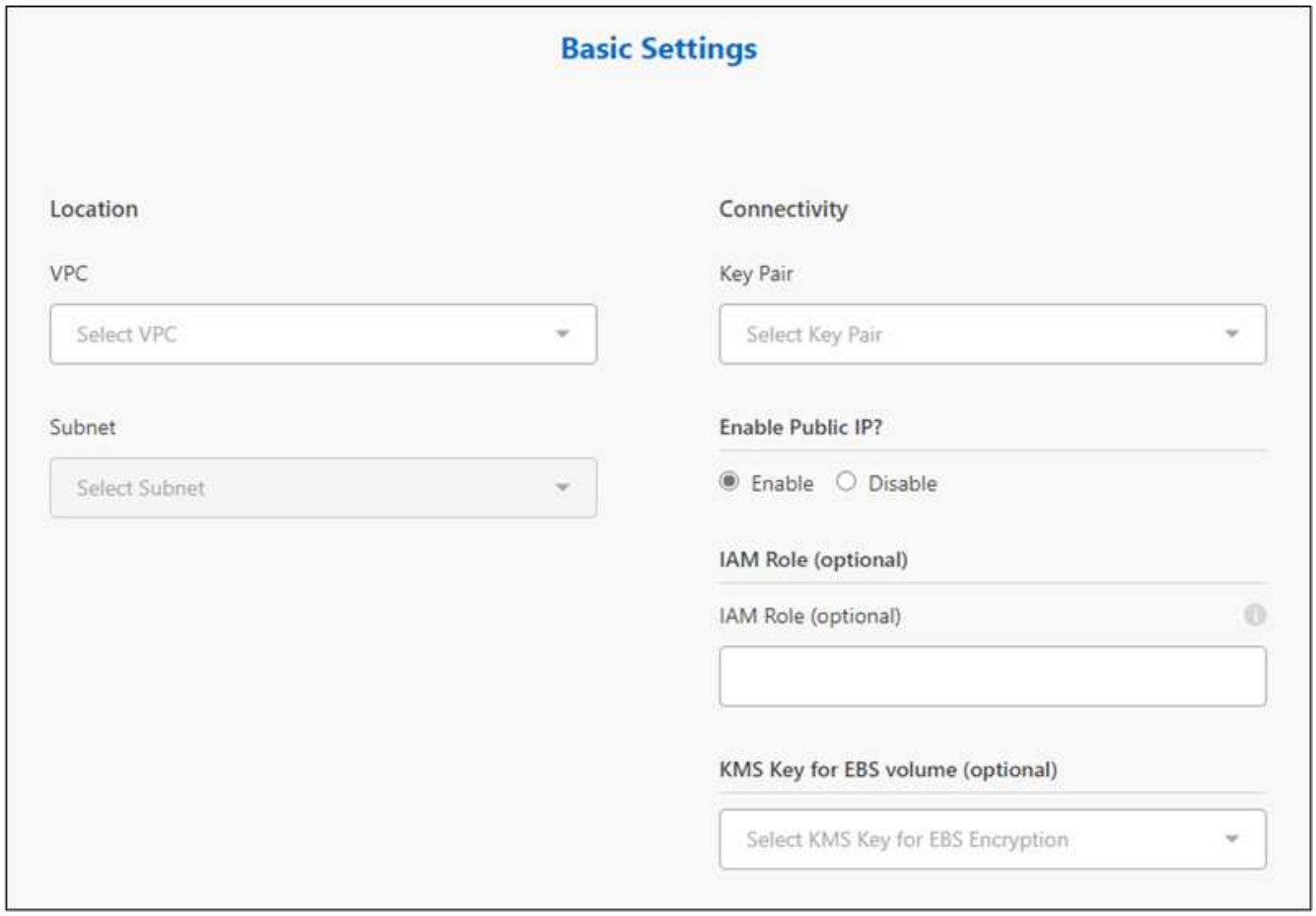
   キーは保存されず、他の目的にも使用されません。

   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。

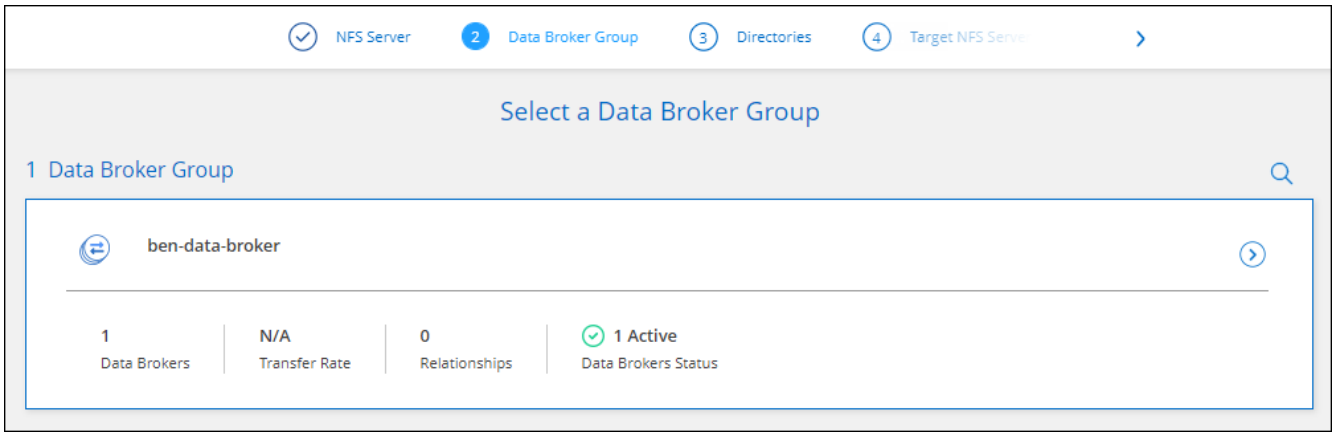
7. AWS アクセスキーを入力した場合は、インスタンスの場所を選択し、キーペアを選択し、パブリック IP アドレスを有効にするかどうかを選択し、既存の IAM ロールを選択するか、フィールドを空白のままにして、コピーと同期によってロールが自動的に作成されるようにします。 KMS キーを使用してデータ ブローカーを暗号化するオプションもあります。

   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/agreemen
ts/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

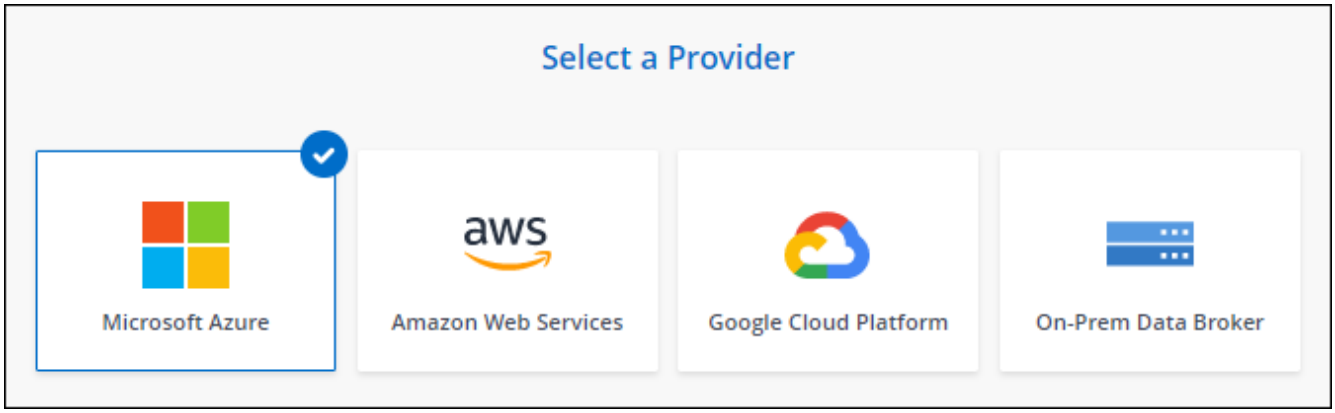
新しいデータ ブローカーを作成するには、いくつかの方法があります。次の手順では、同期関係を作成するときに Azure にデータ ブローカーをインストールする方法について説明します。

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。

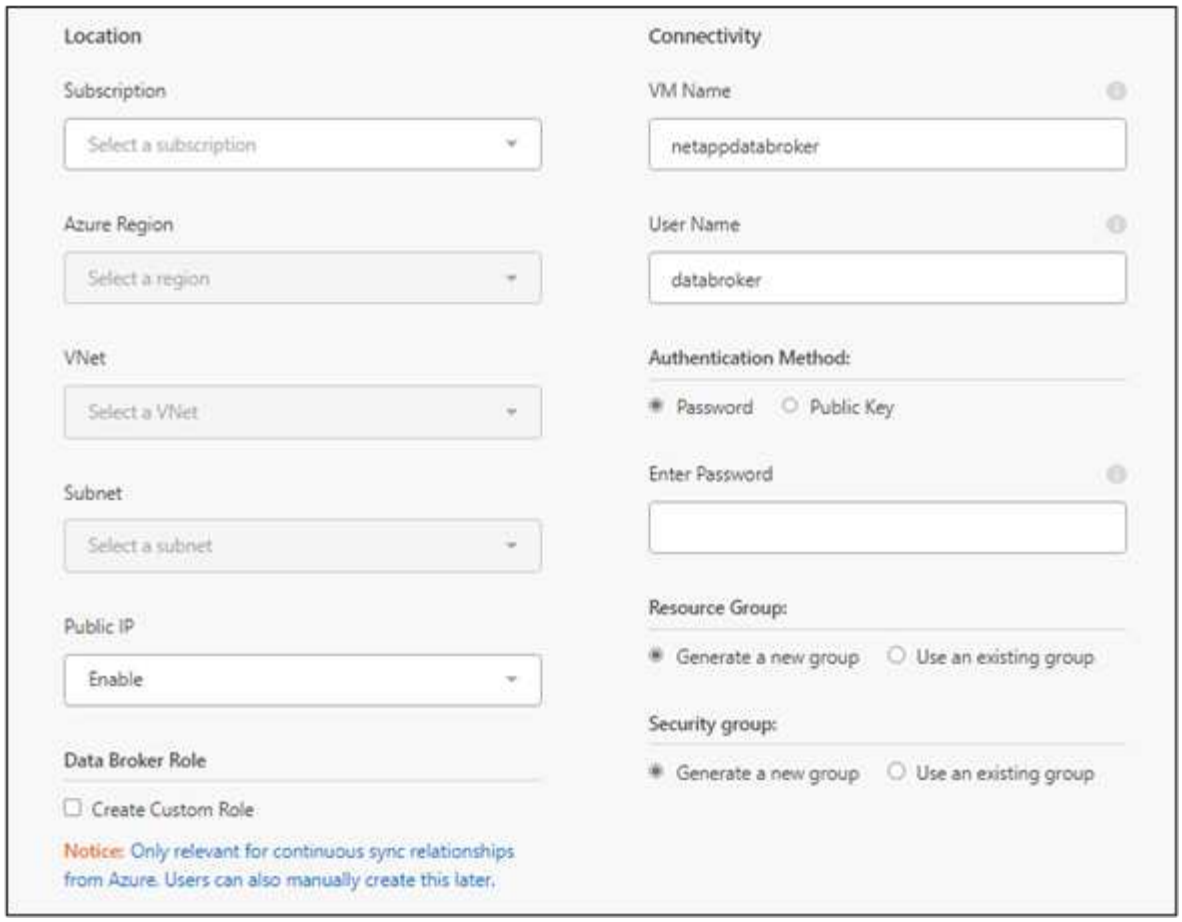
4. データ ブローカー グループ ページで、データ ブローカーの作成 を選択し、**Microsoft Azure** を選択します。



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

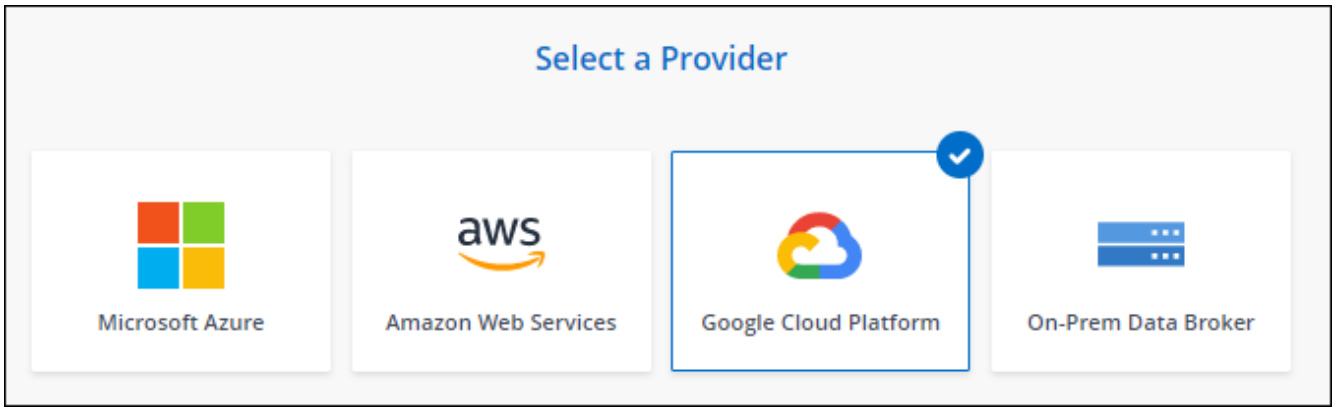
新しいデータ ブローカーを作成するには、いくつかの方法があります。次の手順では、同期関係を作成するときに Google Cloud にデータ ブローカーをインストールする方法について説明します。

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。

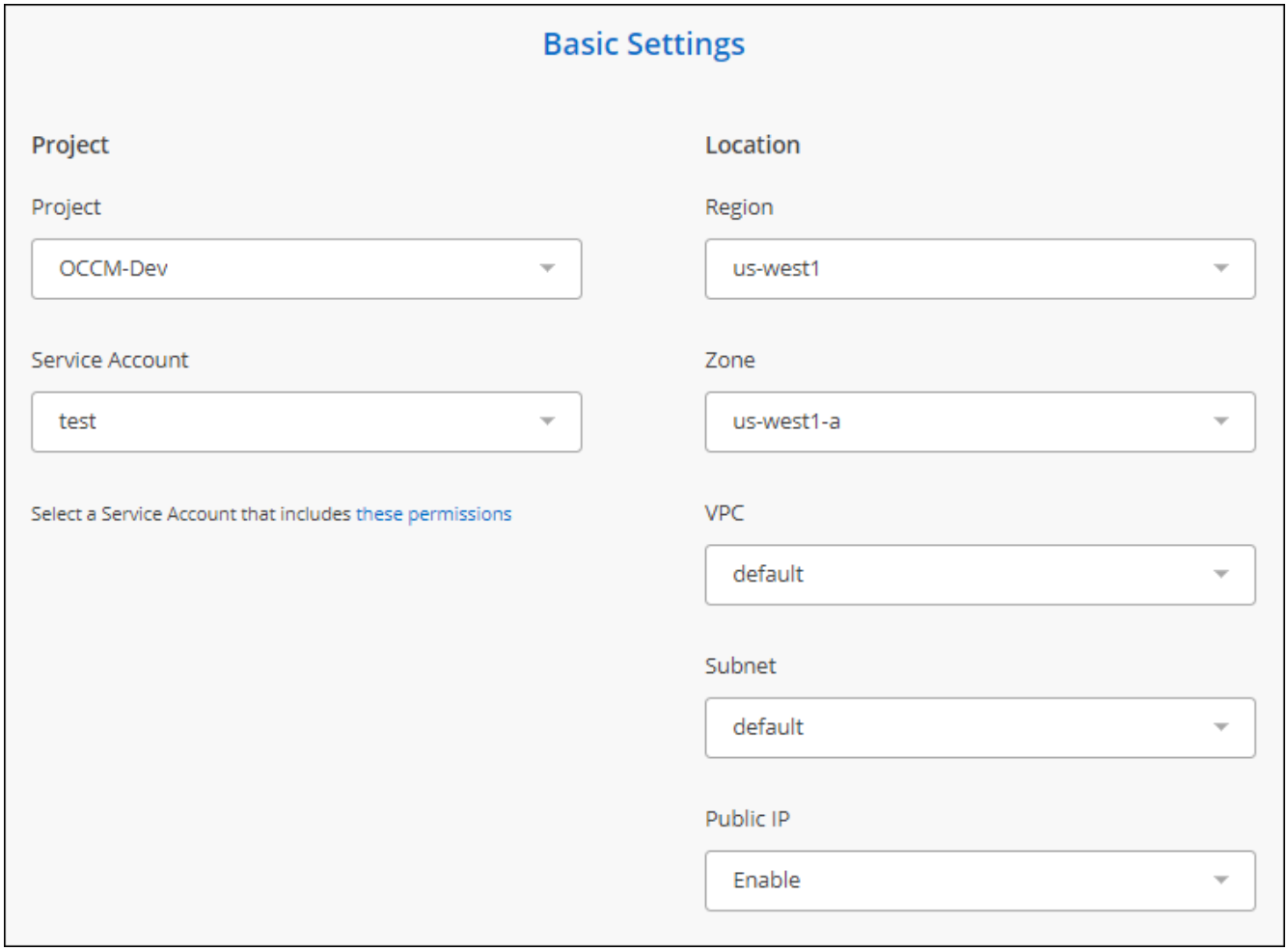


5. データ ブローカーの名前を入力し、[続行] を選択します。
6. プロンプトが表示されたら、Google アカウントでログインします。

   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。

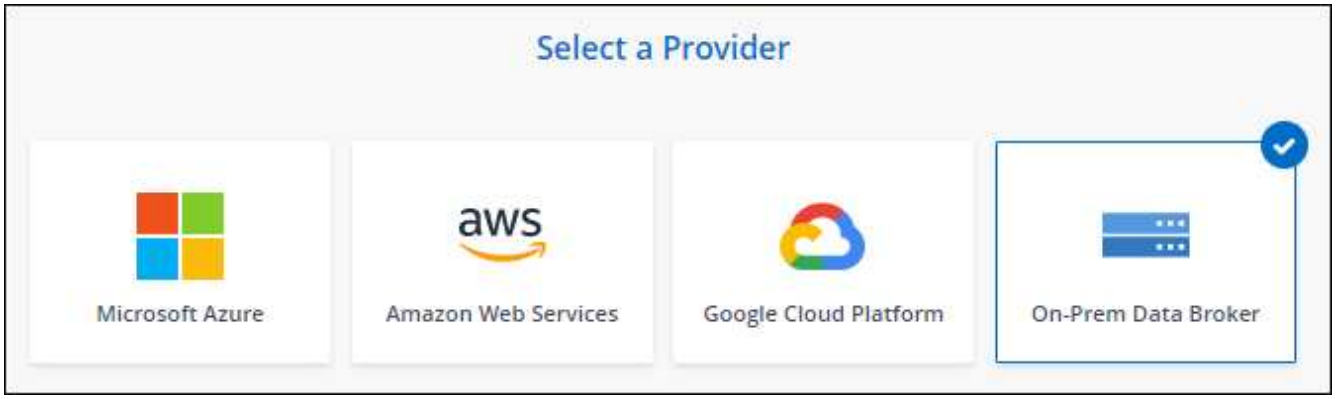
手順

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。

著作権に関する情報

商標に関する情報