プライベートモードで開始します

Setup and administration

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-setup-admin/task-quick-start-private-mode.html on April 24, 2024. Always check docs.netapp.com for the latest.

目次

プライベートモードで開始します 1
スタートアップワークフロー（プライベートモード） 1
プライベートモードでの導入を準備します 1
コネクタをプライベートモードで展開します 15
次に実行できる操作（プライベートモード） 20

プライベートモードで開始します

スタートアップワークフロー（プライベートモード）

BlueXPをプライベートモードで使用するには、環境を準備してコネクタを導入します。

プライベートモードは通常、インターネットに接続されていないオンプレミス環境や、次のようなセキュアなクラウドリージョンで使用されます。 "AWSシークレットクラウド"、 "AWSのトップシークレットクラウド" および "Azure IL6"

開始する前に、次のことを理解しておく必要があります。 "BlueXPのアカウント"、 "コネクタ"および "導入モード"。

1 "導入を準備"

1. CPU、RAM、ディスクスペース、Docker Engineなどの要件を満たす専用のLinuxホストを準備します。
2. ターゲットネットワークへのアクセスを提供するネットワークをセットアップします。
3. クラウド環境の場合は、ソフトウェアのインストール後にそれらの権限をコネクタに関連付けることができるように、クラウドプロバイダで権限を設定します。

2 "コネクタを展開します"

1. Connectorソフトウェアを独自のLinuxホストにインストールします。
2. Webブラウザを開き、LinuxホストのIPアドレスを入力してBlueXPをセットアップします。
3. クラウド環境の場合は、以前に設定した権限をBlueXPに付与します。

プライベートモードでの導入を準備します

BlueXPをプライベートモードで導入する前に、環境を準備します。たとえば、ホストの要件の確認、ネットワークの準備、権限の設定などが必要になります。

でBlueXPを使用する場合は "AWSシークレットクラウド" または "AWSのトップシークレットクラウド"それらの環境で作業を開始するには、別の手順に従う必要があります。 "AWSシークレットクラウドまたはTop Secret CloudでCloud Volumes ONTAPの使用を開始する方法をご確認ください"

ステップ**1**：プライベートモードの仕組みを理解する

作業を開始する前に、BlueXPがプライベートモードでどのように動作するかを理解しておく必要があります。

たとえば、インストールする必要があるBlueXP Connectorからローカルにアクセスできるブラウザベースのインターフェイスを使用する必要があることを理解しておく必要があります。BlueXPには、SaaSレイヤ経由で提供されるWebベースのコンソールからはアクセスできません。

また、すべてのBlueXPサービスを利用できるわけではありません。

"プライベートモードの仕組みを説明します"。

手順2：インストールオプションを確認する

プライベートモードでは、コネクタを自社のLinuxホストに手動でインストールすることで、コネクタをオンプレミスまたはクラウドにインストールできます。

Google CloudでCloud Volumes ONTAP システムを作成する場合は、コネクタをGoogle Cloudで実行する必要があります。オンプレミスで実行することはできません。

手順3：ホスト要件を確認する

コネクタソフトウェアは、特定のオペレーティングシステム要件、 RAM 要件、ポート要件などを満たすホストで実行する必要があります。

専用ホスト

他のアプリケーションと共有しているホストでは、このコネクタはサポートされていません。専用のホストである必要があります。

サポートされているオペレーティングシステム

- Ubuntu 22.04 LTS
- CentOS 7.6、7.7、7.8、7.9
- Red Hat Enterprise Linux 7.6、7.7、7.8、および7.9

  ホストがRed Hat Subscription Managementに登録されている必要があります。登録されていない場合、ホストはコネクタのインストール時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。

  Connector は、これらのオペレーティングシステムの英語版でサポートされています。

ハイパーバイザー

Ubuntu、CentOS、またはRed Hat Enterprise Linuxの実行が認定されているベアメタルまたはホスト型のハイパーバイザーが必要です。

"Red Hat ソリューション：「 Which hypervisors are certified to run Red Hat Enterprise Linux ？」"

CPU

4 コアまたは 4 個の vCPU

RAM

14GB

AWS EC2 インスタンスタイプ

上記の CPU と RAM の要件を満たすインスタンスタイプ。t3.xlarge をお勧めします。

Azure VM サイズ

上記の CPU と RAM の要件を満たすインスタンスタイプ。DS3 v2 を推奨します。

Google Cloudマシンのタイプ

上記の CPU と RAM の要件を満たすインスタンスタイプ。私たちは、n2規格4をお勧めします。

このコネクタは、OSがサポートされているVMインスタンス上のGoogle Cloudでサポートされます "シールドVM機能"

/opt のディスクスペース

100GiB のスペースが使用可能である必要があります

/var のディスク領域

20GiB のスペースが必要です

Docker Engine の略

コネクタをインストールする前に、ホストにDocker Engineが必要です。

- サポートされる最小バージョンは19.3.1です。
- サポートされる最大バージョンは25.0.5です。

"インストール手順を確認します"

手順**4**：コネクタのネットワークを準備する

コネクタがパブリッククラウド環境内のリソースやプロセスを管理できるように、ネットワークを設定します。コネクタの仮想ネットワークとサブネットを使用する以外に、次の要件が満たされていることを確認する必要があります。

ターゲットネットワークへの接続

コネクタには、ストレージを管理する場所へのネットワーク接続が必要です。たとえば、Cloud Volumes ONTAP を導入するVPCまたはVNet、オンプレミスのONTAP クラスタが配置されているデータセンターなどです。

日常業務のエンドポイント

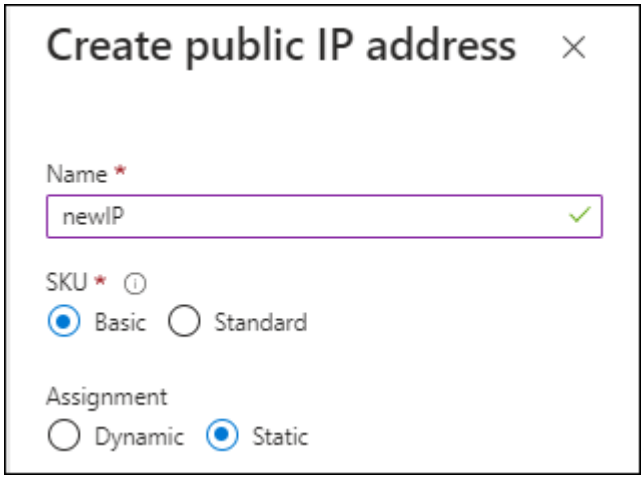
コネクタは、次のエンドポイントに接続して、パブリッククラウド環境内のリソースとプロセスを管理します。

エンドポイント	目的
AWS サービス（ amazonaws.com ）： • クラウド形成 • 柔軟なコンピューティングクラウド（ EC2 ） • IDおよびアクセス管理（IAM） • キー管理サービス（ KMS ） • セキュリティトークンサービス（ STS ） • シンプルなストレージサービス（ S3 ）	AWSでリソースを管理できます。正確なエンドポイントは、使用しているAWSリージョンによって異なります。 "詳細については、AWSのドキュメントを参照してください"

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azureパブリックリージョン内のリソースを管理します。
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	をクリックして、Azure IL6リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	をクリックしてAzure中国地域のリソースを管理してください。
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Google Cloudでリソースを管理します。

Azureのパブリック**IP**アドレス

AzureのコネクタVMでパブリックIPアドレスを使用する場合は、そのIPアドレスでBasic SKUを使用して、BlueXPでこのパブリックIPアドレスが使用されるようにする必要があります。



フィールドで[Basic]を選択できます。"]

Standard SKUのIPアドレスを代わりに使用する場合、BlueXPでは、パブリックIPではなくコネクタの_private_IPアドレスが使用されます。BlueXPコンソールへのアクセスに使用しているマシンがそのプライベートIPアドレスにアクセスできない場合、BlueXPコンソールからの操作が失敗します。

"Azureのドキュメント：パブリックIP SKU"

プロキシサーバ

すべての送信インターネットトラフィック用にプロキシサーバーを導入する必要がある場合は、HTTPまたはHTTPSプロキシに関する次の情報を取得します。この情報は、インストール時に入力する必要があります。

- IP アドレス
- クレデンシャル
- HTTPS証明書

BlueXPでは透過型プロキシサーバはサポートされません。

[+]
プライベートモードの場合、BlueXPがアウトバウンドトラフィックを送信するのは、Cloud Volumes ONTAP システムを作成するためにクラウドプロバイダにしかありません。

ポート

コネクタへの着信トラフィックは、開始しない限りありません。

HTTP（80）およびHTTPS（443）は、BlueXPコンソールへのアクセスを提供します。SSH （ 22 ）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。

NTPを有効にする

BlueXP分類を使用して企業データソースをスキャンする場合は、システム間で時刻が同期されるように、BlueXP ConnectorシステムとBlueXP分類システムの両方でネットワークタイムプロトコル（NTP）サービスを有効にする必要があります。 "BlueXPの分類の詳細については、こちらをご覧ください"

ステップ**5**：クラウドの権限を準備する

Cloud Volumes ONTAP システムの作成を計画している場合は、クラウドプロバイダからBlueXPの権限が必要です。クラウドプロバイダで権限を設定し、インストール後にそれらの権限をコネクタインスタンスに関連付ける必要があります。

必要な手順を表示するには、クラウドプロバイダに使用する認証オプションを選択します。

コネクタをオンプレミスにインストールする場合は、AWSアクセスキーまたはAzureサービスプリンシパルを使用して権限を提供する必要があります。その他のオプションはサポートされていません。

AWS IAMロール

コネクタに権限を付与するには、IAMロールを使用します。コネクタのEC2インスタンスにロールを手動でアタッチする必要があります。

手順

1. AWSコンソールにログインし、IAMサービスに移動します。
2. ポリシーを作成します。
   a. [Policies]>[Create policy]*を選択します。
   b. [*json]*を選択し、の内容をコピーして貼り付けます "コネクタのIAMポリシー"。
   c. 残りの手順を完了してポリシーを作成します。
3. IAMロールを作成します。
   a. [ロール]>[ロールの作成]*を選択します。
   b. [AWS service]>[EC2]*を選択します。
   c. 作成したポリシーを適用して権限を追加します。
   d. 残りの手順を完了してロールを作成します。

結果

これで、コネクタEC2インスタンスのIAMロールが作成されました。

AWSアクセスキー

IAMユーザの権限とアクセスキーを設定します。コネクタをインストールしてBlueXPをセットアップしたら、BlueXPにAWSアクセスキーを指定する必要があります。

手順

1. AWSコンソールにログインし、IAMサービスに移動します。
2. ポリシーを作成します。
   a. [Policies]>[Create policy]*を選択します。
   b. [*json]*を選択し、の内容をコピーして貼り付けます "コネクタのIAMポリシー"。
   c. 残りの手順を完了してポリシーを作成します。

      使用するBlueXPサービスによっては、2つ目のポリシーの作成が必要になる場合があります。

   標準のリージョンでは、権限は2つのポリシーに分散されます。AWSの管理対象ポリシーの最大文字数に制限されているため、2つのポリシーが必要です。 "コネクタのIAMポリシーの詳細については、こちらを参照してください"。
3. IAMユーザにポリシーを適用します。
   - "AWS のドキュメント：「 Creating IAM Roles"
   - "AWS のドキュメント：「 Adding and Removing IAM Policies"
4. コネクタのインストール後にBlueXPに追加できるアクセスキーがユーザに割り当てられていることを確認します。

結果

これで、アカウントに必要な権限が付与されました。

Azureロール

必要な権限を持つAzureカスタムロールを作成します。このロールをコネクタVMに割り当てます。

Azureカスタムロールは、Azureポータル、Azure PowerShell、Azure CLI、またはREST APIを使用して作成できます。Azure CLIを使用してロールを作成する手順を次に示します。別の方法を使用する場合は、を参照してください。 "Azure に関するドキュメント"

手順

1. カスタムロールを使用して必要なAzure権限を提供できるように、コネクタをインストールするVMでシステム割り当ての管理IDを有効にします。

   "Microsoft Azureのドキュメント：Azureポータルを使用して、VM上のAzureリソースの管理IDを設定します"

2. の内容をコピーします "Connectorのカスタムロールの権限" JSONファイルに保存します。
3. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、 JSON ファイルを変更します。

   BlueXPで使用する各AzureサブスクリプションのIDを追加する必要があります。

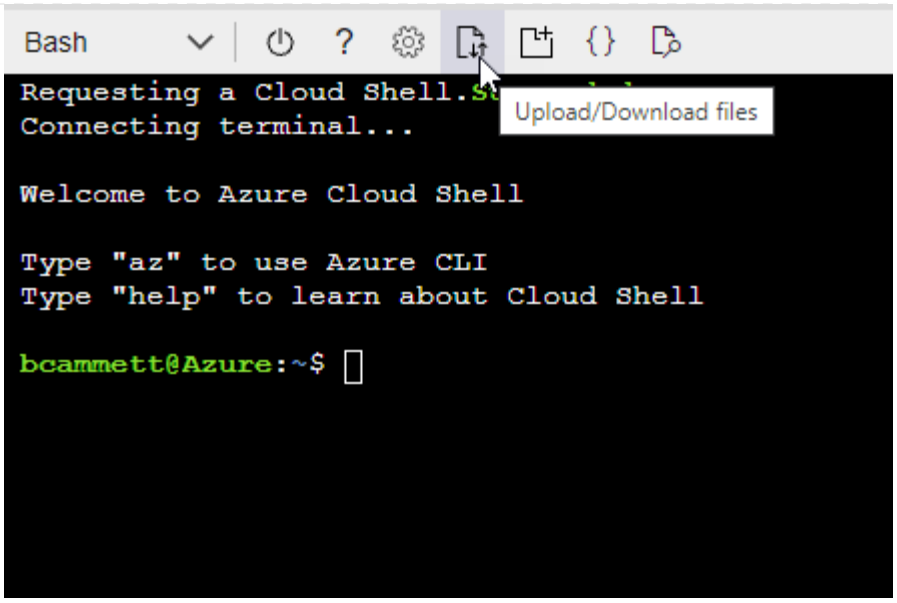
   ◦ 例 *

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. JSON ファイルを使用して、 Azure でカスタムロールを作成します。

   次の手順は、 Azure Cloud Shell で Bash を使用してロールを作成する方法を示しています。

   a. 開始 "Azure Cloud Shell の略" Bash 環境を選択します。
   b. JSON ファイルをアップロードします。



c. Azure CLIを使用してカスタムロールを作成します。

```
az role definition create --role-definition Connector_Policy.json
```

結果

これで、Connector仮想マシンに割り当てることができるBlueXP Operatorというカスタムロールが作成されました。

Azureサービスプリンシパル

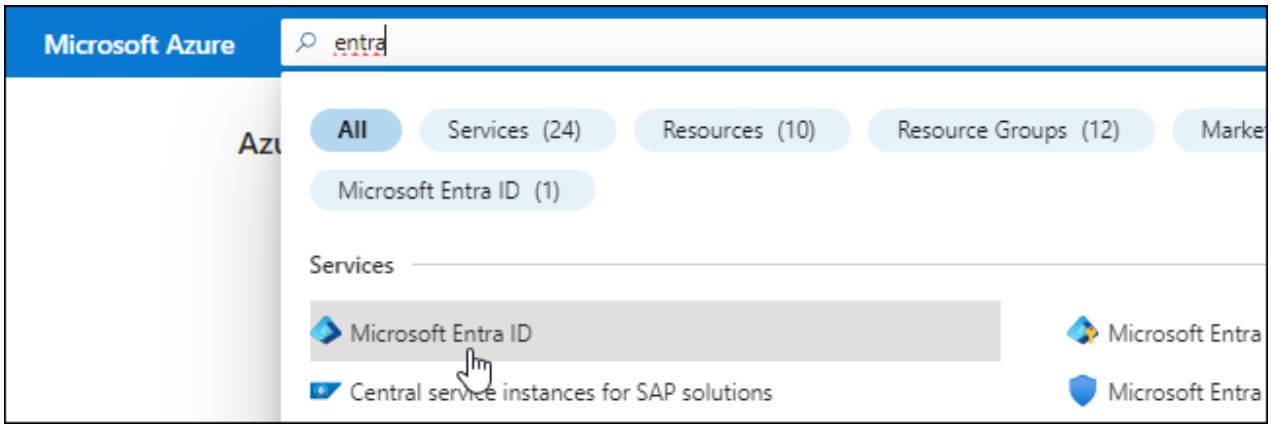
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。これらのクレデンシャルは、コネクタをインストールしてBlueXPをセットアップしたあとにBlueXPに提供する必要があります。

ロールベースアクセス制御用の**Microsoft Entra**アプリケーションの作成

1. Active Directoryアプリケーションを作成し、そのアプリケーションをロールに割り当てる権限がAzureにあることを確認します。

   詳細については、を参照してください "Microsoft Azure のドキュメント：「 Required permissions"

2. Azureポータルで、* Microsoft Entra ID *サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. [New registration]*を選択します。
5. アプリケーションの詳細を指定します。
   - * 名前 * ：アプリケーションの名前を入力します。
   - アカウントの種類:アカウントの種類を選択します(すべてのアカウントはBlueXPで動作します)。
   - * リダイレクト URI *: このフィールドは空白のままにできます。
6. [*Register] を選択します。

   AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

1. カスタムロールを作成します。

   Azureカスタムロールは、Azureポータル、Azure PowerShell、Azure CLI、またはREST APIを使用して作成できます。Azure CLIを使用してロールを作成する手順を次に示します。別の方法を使用する場合は、を参照してください。 "Azure に関するドキュメント"

   a. の内容をコピーします "Connectorのカスタムロールの権限" JSONファイルに保存します。

   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、 JSON ファイルを変更します。

      ユーザが Cloud Volumes ONTAP システムを作成する Azure サブスクリプションごとに ID を追加する必要があります。

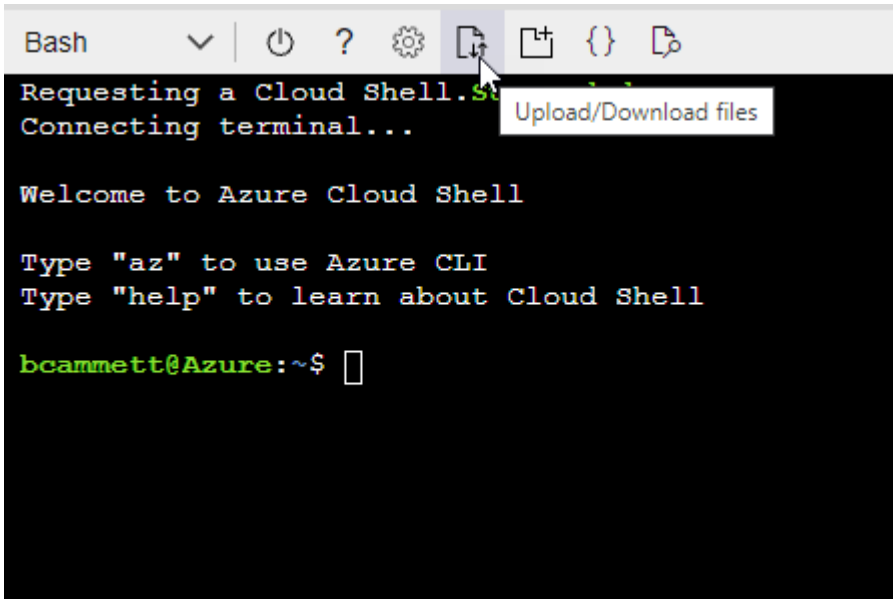
      ▪ 例 *

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

   c. JSON ファイルを使用して、 Azure でカスタムロールを作成します。

      次の手順は、 Azure Cloud Shell で Bash を使用してロールを作成する方法を示しています。

- 開始 "Azure Cloud Shell の略" Bash 環境を選択します。
- JSON ファイルをアップロードします。



- Azure CLIを使用してカスタムロールを作成します。

```
az role definition create --role-definition
Connector_Policy.json
```

これで、Connector仮想マシンに割り当てることができるBlueXP Operatorというカスタムロールが作成されました。

2. ロールにアプリケーションを割り当てます。

a. Azure ポータルで、 * Subscriptions * サービスを開きます。

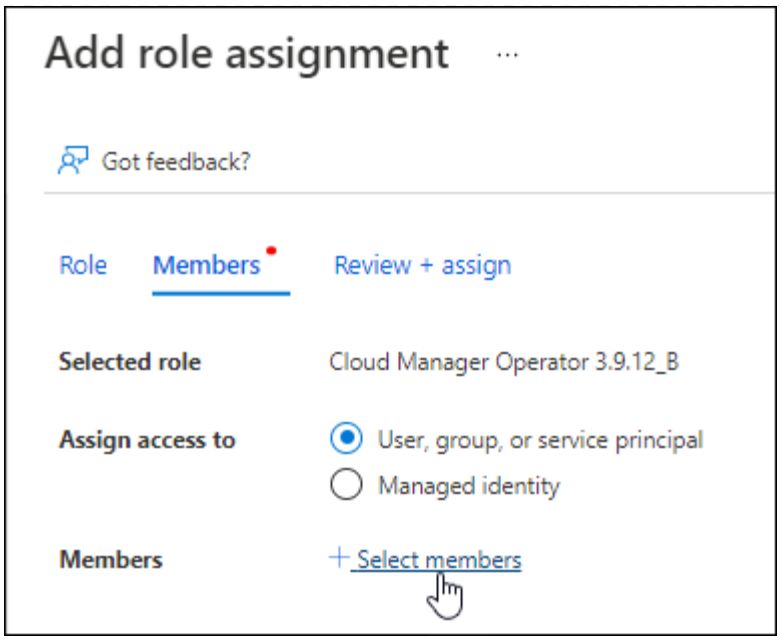
b. サブスクリプションを選択します。

c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。

d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。

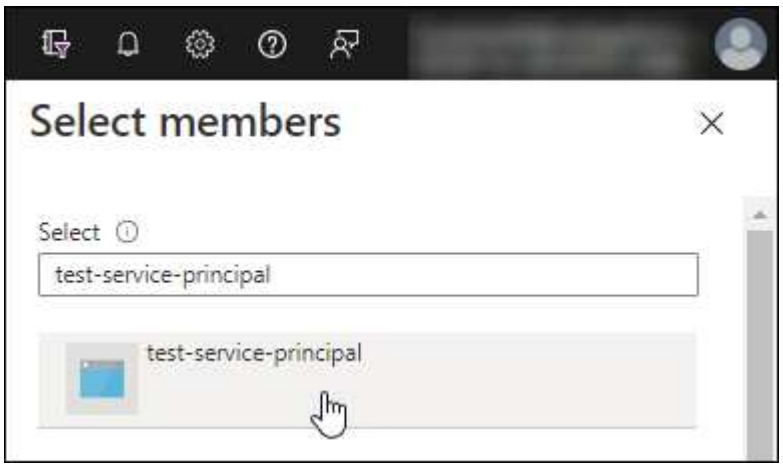
e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

- [* ユーザー、グループ、またはサービスプリンシパル *] を選択したままにします。
- [メンバーの選択]*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、*選択*を選択します。
- 「 * 次へ * 」を選択します。

f. [Review + Assign]*を選択します。

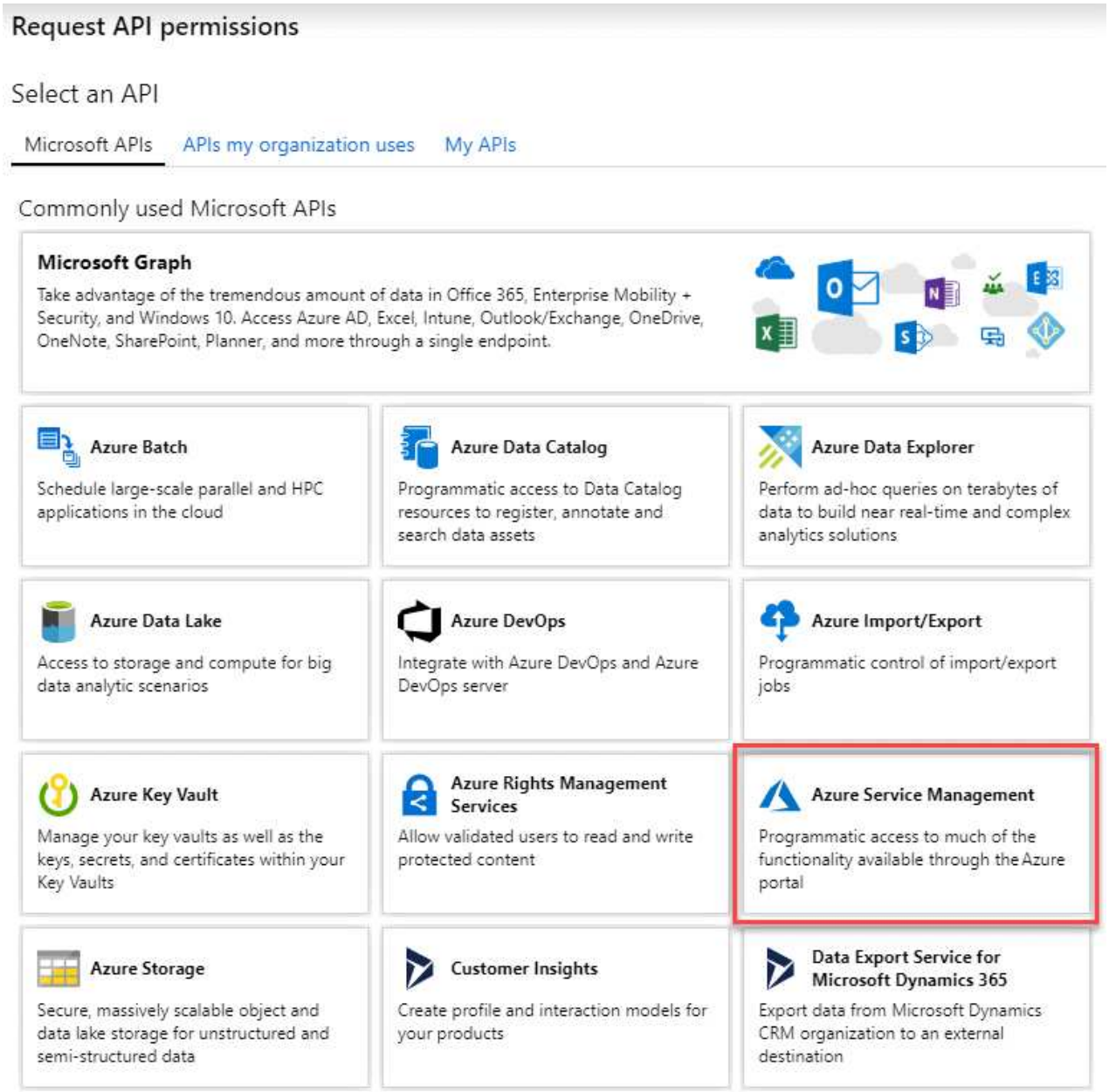
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

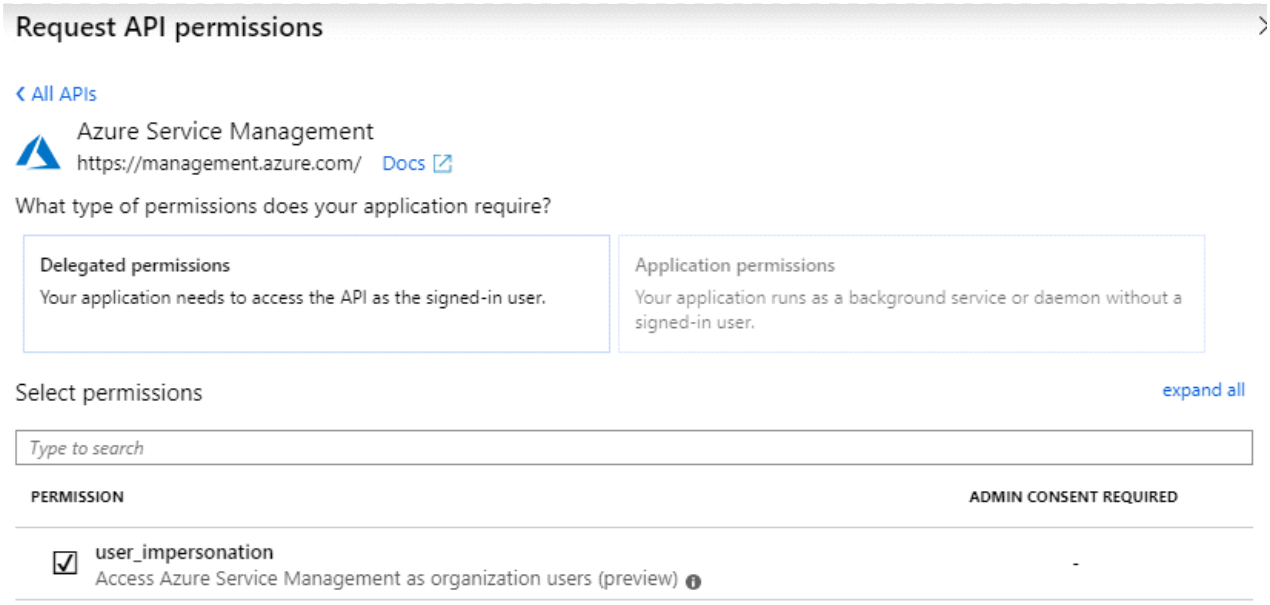
Windows Azure Service Management API 権限を追加します

1. Microsoft Entra ID *サービスで、*アプリ登録*を選択し、アプリケーションを選択します。
2. [API permissions]>[Add a permission]*を選択します。

3. Microsoft API* で、 * Azure Service Management * を選択します。

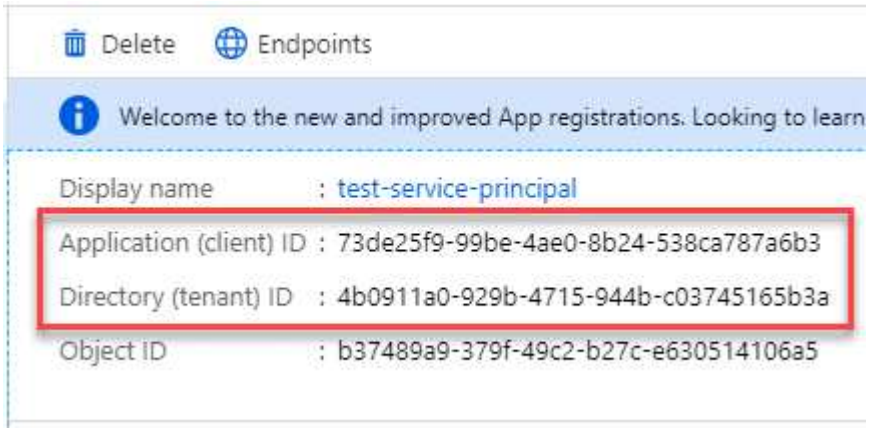


4. を選択し、[Add permissions]*を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

1. Microsoft Entra ID *サービスで、*アプリ登録*を選択し、アプリケーションを選択します。
2. アプリケーション（クライアント） ID * とディレクトリ（テナント） ID * をコピーします。



AzureアカウントをBlueXPに追加するときは、アプリケーション（クライアント）IDとディレクトリ（テナント）IDを指定する必要があります。BlueXPでは、プログラムでサインインするためにIDが使用されます。

クライアントシークレットを作成します

1. Microsoft Entra ID *サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. [Certificates & secrets]>[New client secret]*を選択します。
4. シークレットと期間の説明を入力します。
5. 「 * 追加」を選択します。
6. クライアントシークレットの値をコピーします。

BlueXPでクライアントシークレットを使用してMicrosoft Entra IDで認証できるようになりました。

結果

これでサービスプリンシパルが設定され、アプリケーション（クライアント） ID 、ディレクトリ（テナント） ID 、およびクライアントシークレットの値をコピーしました。Azureアカウントを追加する場合は、BlueXPでこの情報を入力する必要があります。

Google Cloudサービスアカウント

ロールを作成し、コネクタVMインスタンスに使用するサービスアカウントに適用します。

手順

1. Google Cloudでカスタムロールを作成します。
   a. で定義された権限を含むYAMLファイルを作成します "Google Cloudのコネクタポリシー"。
   b. Google CloudからCloud Shellをアクティブ化します。
   c. コネクタに必要な権限を含むYAMLファイルをアップロードします。
   d. を使用して、カスタムロールを作成します `gcloud iam roles create` コマンドを実行します

      次の例では、プロジェクトレベルで「Connector」という名前のロールを作成します。

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloudのドキュメント：カスタムロールの作成と管理"

2. Google Cloudでサービスアカウントを作成します。
   a. IAMおよび管理サービスから、*サービスアカウント>サービスアカウントの作成*を選択します。
   b. サービスアカウントの詳細を入力し、*作成して続行*を選択します。
   c. 作成したロールを選択します。
   d. 残りの手順を完了してロールを作成します。

      "Google Cloudドキュメント：サービスアカウントの作成"

結果

これで、Connector VMインスタンスに割り当てることができるサービスアカウントが作成されました。

ステップ6：Google Cloud APIを有効にする

Google CloudにCloud Volumes ONTAP を導入するには、いくつかのAPIが必要です。

ステップ

1. "プロジェクトで次の Google Cloud API を有効にします"
    - Cloud Deployment Manager V2 API
    - クラウドロギング API
    - Cloud Resource Manager API の略
    - Compute Engine API
    - ID およびアクセス管理（ IAM ） API
    - Cloud Key Management Service（KMS）APIの略

      （お客様が管理する暗号化キー（CMEK）でBlueXPのバックアップとリカバリを使用する場合にのみ必要）

コネクタをプライベートモードで展開します

コネクタをプライベートモードで導入し、BlueXP SaaSレイヤへのアウトバウンド接続なしでBlueXPを使用できるようにします。まず、コネクタをインストールし、コネクタで実行されているユーザインターフェイスにアクセスしてBlueXPをセットアップし、以前に設定したクラウド権限を指定します。

手順1：コネクタを取り付ける

NetApp Support Site から製品のインストーラをダウンロードし、手動でコネクタを自分のLinuxホストにインストールします。

でBlueXPを使用する場合は "AWSシークレットクラウド" または "AWSのトップシークレットクラウド"それらの環境で作業を開始するには、別の手順に従う必要があります。 "AWSシークレットクラウドまたはTop Secret CloudでCloud Volumes ONTAPの使用を開始する方法をご確認ください"

作業を開始する前に

コネクタをインストールするには root 権限が必要です。

手順

1. Docker が有効で実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. からConnectorソフトウェアをダウンロードします "NetApp Support Site"

   インターネットにアクセスできないプライベートネットワーク用のオフラインインストーラを必ずダウンロードしてください。

3. インストーラを Linux ホストにコピーします。
4. スクリプトを実行する権限を割り当てます。

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

<version> は、ダウンロードしたコネクタのバージョンです。

5. インストールスクリプトを実行します。

```
sudo /path/BlueXP-Connector-offline-<version>
```

<version> は、ダウンロードしたコネクタのバージョンです。

結果

コネクタソフトウェアがインストールされます。BlueXPをセットアップできるようになりました。

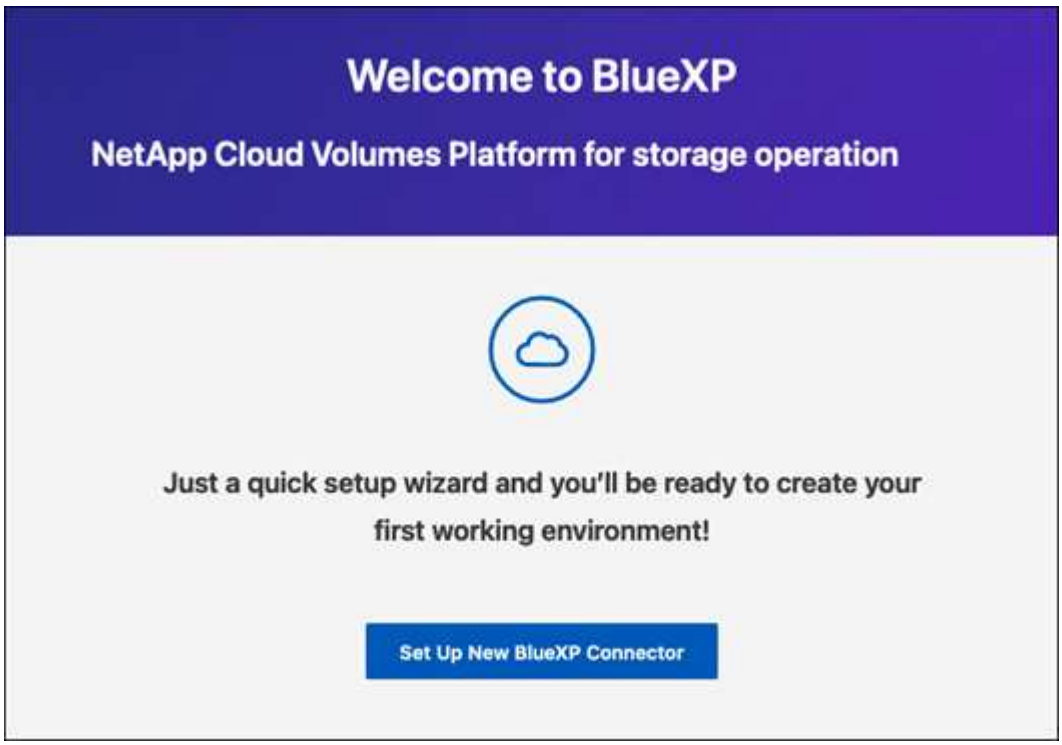
ステップ2：BlueXPをセットアップする

BlueXPコンソールに初めてアクセスすると、BlueXPをセットアップするように求められます。

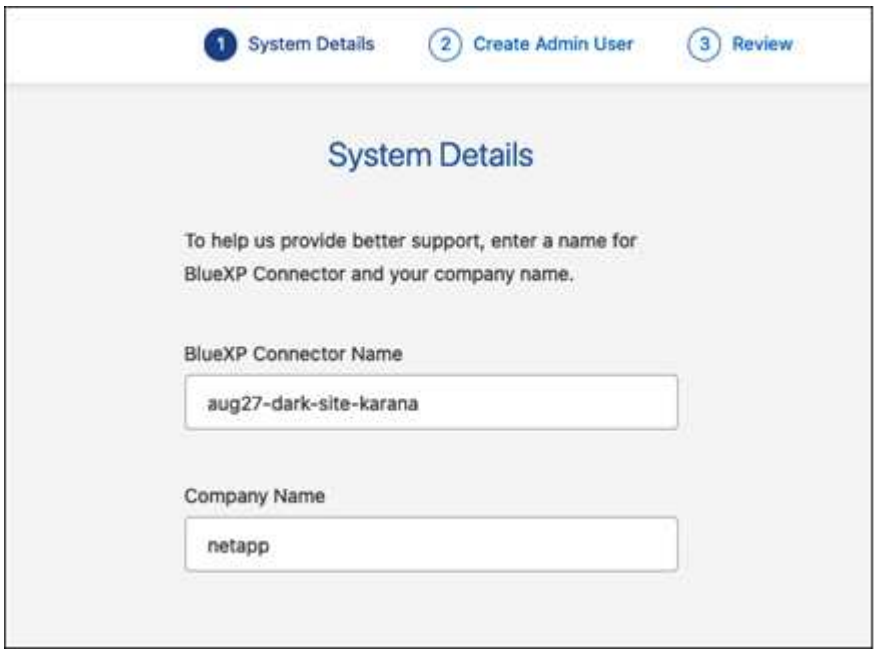
手順

1. Web ブラウザを開き、と入力します https://ipaddress _ipaddress_は、コネクタをインストールしたLinuxホストのIPアドレスです。

   次の画面が表示されます。



2. [新しいBlueXPコネクタのセットアップ]*を選択し、画面の指示に従ってシステムをセットアップします。
   - システムの詳細：コネクタの名前と会社名を入力します。



   - 管理者ユーザーの作成：システムの管理者ユーザーを作成します。

     このユーザアカウントはシステム上でローカルに実行されます。BlueXPからはAuth0サービスに接続できません。

   - 確認：詳細を確認し、使用許諾契約に同意して、*セットアップ*を選択します。
3. 作成した管理者ユーザを使用してBlueXPにログインします。

結果

これでコネクタがインストールされ、セットアップされました。

新しいバージョンの Connector ソフトウェアが利用可能になると、ソフトウェアはNetApp Support Siteにアップロードされます。 "コネクタをアップグレードする方法について説明します"。

次の手順

以前に設定した権限をBlueXPに付与します。

ステップ3：BlueXPへの権限を付与する

Cloud Volumes ONTAP 作業環境を作成する場合は、以前に設定したクラウド権限をBlueXPに付与する必要があります。

"クラウドへのアクセス許可を準備する方法をご確認ください"。

AWS IAMロール

以前に作成したIAMロールをコネクタEC2インスタンスにアタッチします。

手順

1. Amazon EC2コンソールに移動します。
2. [インスタンス]*を選択します。
3. コネクターインスタンスを選択します。
4. [アクション]>[セキュリティ]>[IAMロールの変更]*を選択します。
5. IAMロールを選択し、*[IAMロールの更新]*を選択します。

結果

BlueXPに、AWSでユーザに代わって操作を実行するために必要な権限が付与されました。

AWSアクセスキー

必要な権限を持つIAMユーザのAWSアクセスキーをBlueXPに渡します。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [クレデンシャルの追加]*を選択し、ウィザードの手順に従います。
   a. * 資格情報の場所 * ：「 * Amazon Web Services > Connector * 」を選択します。
   b. クレデンシャルを定義：AWSアクセスキーとシークレットキーを入力します。
   c. * Marketplace サブスクリプション *: 今すぐ登録するか、既存のサブスクリプションを選択して、 Marketplace サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認：新しいクレデンシャルの詳細を確認し、*[追加]*を選択します。

結果

BlueXPに、AWSでユーザに代わって操作を実行するために必要な権限が付与されました。

Azureロール

Azureポータルに移動し、1つ以上のサブスクリプションのコネクタ仮想マシンにAzureカスタムロールを割り当てます。

手順

1. Azure Portalで、* Subscriptions *サービスを開き、サブスクリプションを選択します。

   サブスクリプションレベルでのロール割り当ての範囲が指定されるため、* Subscriptions *サービスからロールを割り当てることが重要です。_scope_は、環境にアクセスするリソースセットを定義します。別のレベル（仮想マシンレベルなど）でスコープを指定すると、BlueXPで操作を実行できなくなります。

"Microsoft Azureのドキュメント：「Azure RBACの範囲を理解する」"

2. >[追加]>[ロール割り当ての追加]*を選択します。
3. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。

> BlueXP Operatorは'BlueXPポリシーで指定されているデフォルト名ですロールに別の名前を選択した場合は、代わりにその名前を選択します。

4. [* Members* （メンバー * ）] タブで、次の手順を実行します。
   a. * 管理対象 ID * へのアクセス権を割り当てます。
   b. * Select members を選択し、コネクター仮想マシンが作成されたサブスクリプションを選択します。 Managed identity で Virtual machine *を選択し、コネクター仮想マシンを選択します。
   c. [選択]*を選択します。
   d. 「 * 次へ * 」を選択します。
   e. [Review + Assign]*を選択します。
   f. 追加のAzureサブスクリプションでリソースを管理する場合は、そのサブスクリプションに切り替えてから、上記の手順を繰り返します。

結果

BlueXPに、Azureで処理を実行するために必要な権限が付与されました。

Azureサービスプリンシパル

以前にセットアップしたAzureサービスプリンシパルのクレデンシャルをBlueXPに指定します。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [クレデンシャルの追加]*を選択し、ウィザードの手順に従います。
   a. * 資格情報の場所 * ： Microsoft Azure > Connector * を選択します。
   b. 資格情報の定義:必要な権限を付与するMicrosoft Entraサービスプリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID
      - クライアントシークレット
   c. * Marketplace サブスクリプション *: 今すぐ登録するか、既存のサブスクリプションを選択して、 Marketplace サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認：新しいクレデンシャルの詳細を確認し、*[追加]*を選択します。

結果

BlueXPに、Azureで処理を実行するために必要な権限が付与されました。

Google Cloudサービスアカウント

サービスアカウントをコネクタVMに関連付けます。

手順

1. Google Cloudポータルに移動し、コネクタVMインスタンスにサービスアカウントを割り当てます。

   "Google Cloudドキュメント：インスタンスのサービスアカウントとアクセス範囲の変更"

2. 他のプロジェクトのリソースを管理する場合は、BlueXPロールを持つサービスアカウントをそのプロジェクトに追加してアクセスを許可します。プロジェクトごとにこの手順を繰り返す必要があります。

結果

BlueXPに、Google Cloudでユーザに代わって操作を実行するために必要な権限が付与されました。

次に実行できる操作（プライベートモード）

プライベートモードでBlueXPを起動して実行したら、プライベートモードでサポートされているBlueXPサービスの使用を開始できます。

ヘルプについては、次のドキュメントを参照してください。

- "Cloud Volumes ONTAP システムの作成"
- "オンプレミスのONTAP クラスタを検出"
- "データのレプリケート"
- "BlueXPの分類を使用してオンプレミスのONTAP ボリュームのデータをスキャンします"
- "BlueXPのバックアップとリカバリを使用して、オンプレミスのONTAP ボリュームのデータをStorageGRID にバックアップします"

関連リンク

"BlueXPの導入モード"

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

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

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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