コネクタを作成します

Setup and administration

NetApp
April 26, 2024

目次

コネクタを作成します 1
AWS 1
Azure 22
Google Cloud 66
コネクタをオンプレミスにインストールしてセットアップします 88

コネクタを作成します

AWS

AWSでのコネクタのインストールオプション

AWSでコネクタを作成する方法はいくつかあります。最も一般的な方法はBlueXPから直接実行することです。

次のインストールオプションを使用できます。

- "BlueXPからコネクタを直接作成" （これは標準オプションです）

  この操作により、Linuxを実行するEC2インスタンスとコネクタソフトウェアが、選択したVPCで起動されます。

- "AWS Marketplace からコネクタを作成します"

  また、Linuxを実行するEC2インスタンスとコネクタソフトウェアも起動しますが、導入はBlueXPではなくAWS Marketplaceから直接開始されます。

- "ソフトウェアをダウンロードして、自分のLinuxホストに手動でインストールします"

選択するインストールオプションは、インストールの準備方法に影響します。これには、AWSでリソースの認証と管理に必要な権限をBlueXPに付与する方法も含まれます。

BlueXPからAWSにコネクタを作成します

BlueXPからAWSでコネクタを作成するには、ネットワークを設定し、AWS権限を準備してからコネクタを作成する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順1：ネットワークをセットアップする

コネクタをインストールするネットワークの場所が、次の要件をサポートしていることを確認します。これらの要件を満たすことで、コネクタはハイブリッドクラウド環境内のリソースとプロセスを管理できるようになります。

vPCおよびサブネット

コネクタを作成するときは、コネクタを配置するVPCとサブネットを指定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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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"
\ https://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

BlueXPコンソールからアクセスするエンドポイント

SaaSレイヤで提供されるWebベースのBlueXPコンソールを使用すると、IT部門は複数のエンドポイントと通信してデータ管理タスクを実行します。これには、BlueXPコンソールからコネクタを導入するために接続されるエンドポイントも含まれます。

"BlueXPコンソールからアクセスしたエンドポイントのリストを表示します"。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

コネクタを作成した後で、このネットワーク要件を実装する必要があります。

手順**2**：**AWS**権限を設定する

BlueXPでは、VPCにConnectorインスタンスを導入する前にAWSで認証する必要があります。次のいずれかの認証方式を選択できます。

- 必要な権限を持つIAMロールをBlueXPに割り当てます
- 必要な権限を持つIAMユーザにAWSアクセスキーとシークレットキーを指定します

どちらのオプションを使用する場合も、最初にIAMポリシーを作成します。このポリシーには、BlueXPからAWSでConnectorインスタンスを起動するために必要な権限のみが含まれています。

必要に応じて、IAMを使用してIAMポリシーを制限できます `Condition` 要素（Element）： "AWSドキュメント：Condition要素"

BlueXPでコネクタを作成すると、コネクタインスタンスに新しい権限セットが適用され、コネクタでAWSリソースを管理できるようになります。

手順

1. AWS IAMコンソールに移動します。
2. [Policies]>[Create policy]*を選択します。
3. 「* JSON *」を選択します。
4. 次のポリシーをコピーして貼り付けます。

   なお、このポリシーには、BlueXPからAWSでコネクタインスタンスを起動するために必要な権限のみが含まれています。 "コネクタインスタンス自体に必要な表示権限"。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
```

```
            "ec2:DescribeKeyPairs",
            "ec2:DescribeRegions",
            "ec2:DescribeInstances",
            "ec2:CreateTags",
            "ec2:DescribeImages",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeLaunchTemplates",
            "ec2:CreateLaunchTemplate",
            "cloudformation:CreateStack",
            "cloudformation:DeleteStack",
            "cloudformation:DescribeStacks",
            "cloudformation:DescribeStackEvents",
            "cloudformation:ValidateTemplate",
            "ec2:AssociateIamInstanceProfile",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:DisassociateIamInstanceProfile",
            "iam:GetRole",
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. 必要に応じて、[次へ]*を選択し、タグを追加します。
6. [次へ]*を選択し、名前と概要を入力します。
7. [ポリシーの作成]*を選択します。
8. BlueXPが引き継ぐことができるIAMロールにポリシーを適用するか、BlueXPにアクセスキーを提供できるようにIAMユーザにポリシーを関連付けます。

- （オプション1）BlueXPで想定できるIAMロールを設定します。
  i. ターゲットアカウントの AWS IAM コンソールに移動します。
  ii. [Access Management]で、*[Roles]>[Create Role]*を選択し、手順に従ってロールを作成します。
  iii. 信頼されるエンティティのタイプ * で、 * AWS アカウント * を選択します。
  iv. 別のAWSアカウント*を選択して、BlueXP SaaSアカウントのID 952013314444を入力します
  v. 前のセクションで作成したポリシーを選択します。
  vi. ロールを作成したら、ロールARNをコピーして、コネクタの作成時にBlueXPに貼り付けることができます。
- （オプション2）BlueXPにアクセスキーを提供できるように、IAMユーザの権限を設定します。
  i. AWS IAMコンソールで、*[Users]*を選択し、ユーザ名を選択します。
  ii. [権限の追加]>[既存のポリシーを直接適用]*を選択します。
  iii. 作成したポリシーを選択します。
  iv. を選択し、[権限の追加]*を選択します。
  v. IAMユーザのアクセスキーとシークレットキーがあることを確認します。

結果

これで、必要な権限を持つIAMロールまたは必要な権限を持つIAMユーザが作成されました。BlueXPからコネクタを作成するときに、ロールまたはアクセスキーに関する情報を指定できます。

手順**3**：コネクタを作成する

BlueXPのWebベースのコンソールから直接コネクタを作成します。

このタスクについて

BlueXPでコネクタを作成すると、デフォルト設定を使用してAWSにEC2インスタンスが導入されます。コネクタの作成後は、CPUやRAMの少ない小さいEC2インスタンスタイプに変更しないでください。 "コネクタのデフォルト設定について説明します"。

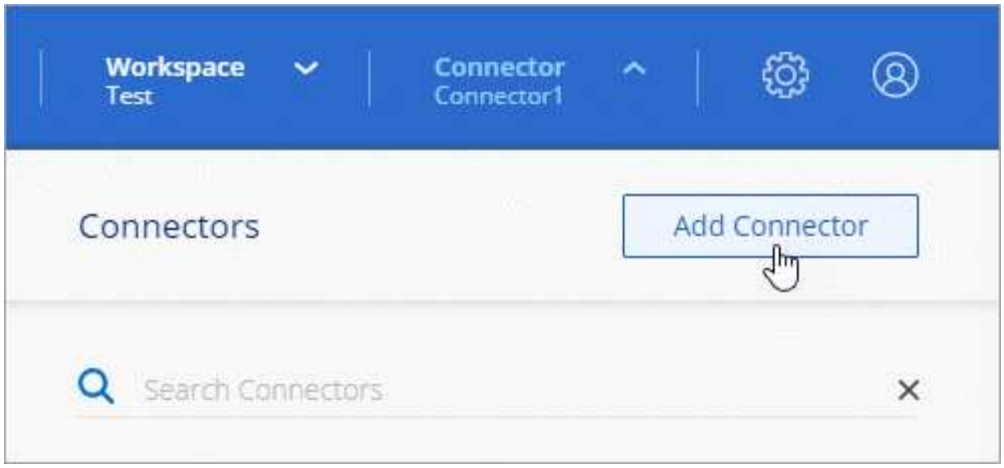
作業を開始する前に

次の情報が必要です。

- AWS認証方式：IAMロールまたは必要な権限を持つIAMユーザのアクセスキー。
- ネットワーク要件を満たすVPCとサブネット。
- EC2インスタンスのキーペア。
- コネクタからのインターネットアクセスにプロキシが必要な場合は、プロキシサーバに関する詳細。

手順

1. ドロップダウンを選択し、[コネクタの追加]*を選択します。



2. クラウドプロバイダとして* Amazon Web Services を選択し、 Continue *を選択します。
3. [*コネクターの配置（Deploying a Connector *）]ページで、必要なものについて詳しく確認してください。次の 2 つのオプションがあります。
   a. 製品内のガイドを使用して導入を準備するには、* Continue *を選択します。製品ガイドの各手順には、このページのドキュメントに記載されている情報が含まれています。
   b. このページの手順に従って準備が完了している場合は、[Skip to Deployment]*を選択します。
4. ウィザードの手順に従って、コネクタを作成します。
   - * 準備をしてください * ：必要なものを確認してください。
   - * AWSクレデンシャル*：AWSリージョンを指定してから認証方式を選択します。認証方式は、BlueXPが引き受けることができるIAMロールか、AWSのアクセスキーとシークレットキーのどちらかです。

     [*Assume Role] を選択した場合は、 Connector 展開ウィザードから最初の資格情報セットを作成できます。クレデンシャルの追加のセットは、 [Credentials] ページから作成する必要があります。ウィザードのドロップダウンリストから使用できるようになります。 "クレデンシャルを追加する方法について説明します"。

   - * 詳細 * ：コネクタの詳細を入力します。
     - インスタンスの名前を入力します。
     - カスタムタグ（メタデータ）をインスタンスに追加します。
     - 必要な権限を持つ新しいロールを作成するか、で設定した既存のロールを選択するかを選択します "必要な権限"。
     - コネクタの EBS ディスクを暗号化するかどうかを選択します。デフォルトの暗号化キーを使用することも、カスタムキーを使用することもできます。
   - * ネットワーク * ：インスタンスに VPC 、サブネット、キーペアを指定し、パブリック IP アドレスを有効にするかどうかを選択し、必要に応じてプロキシ設定を指定します。

     コネクタで使用する正しいキーペアがあることを確認します。キーペアがないと、Connector仮想マシンにアクセスできません。

   - セキュリティグループ:新しいセキュリティグループを作成するか、必要なインバウンドおよびアウトバウンドルールを許可する既存のセキュリティグループを選択するかを選択します。

"AWSのセキュリティグループルールを表示します"。

- * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

5. 「 * 追加」を選択します。

インスタンスの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

結果

プロセスが完了すると、BlueXPからコネクタを使用できるようになります。

コネクタを作成したAWSアカウントにAmazon S3バケットがある場合は、BlueXPキャンバスにAmazon S3の作業環境が自動的に表示されます。 "BlueXPでS3バケットを管理する方法"

AWS Marketplace からコネクタを作成します

AWS Marketplaceからコネクタを作成するには、ネットワークを設定し、AWS権限を準備し、インスタンス要件を確認してから、コネクタを作成する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順**1**：ネットワークをセットアップする

コネクタをインストールするネットワークの場所が、次の要件をサポートしていることを確認します。これらの要件を満たすことで、コネクタはハイブリッドクラウド環境内のリソースとプロセスを管理できるようになります。

vPCおよびサブネット

コネクタを作成するときは、コネクタを配置するVPCとサブネットを指定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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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"
\ https://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。

- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

コネクタを作成した後で、このネットワーク要件を実装する必要があります。

手順**2**：**AWS**権限を設定する

Marketplaceの導入に備えて、AWSでIAMポリシーを作成し、IAMロールに関連付けます。AWS Marketplaceからコネクタを作成すると、そのIAMロールを選択するように求められます。

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、AWS Marketplaceからの導入時にEC2インスタンスに関連付けることができるIAMロールが作成されました。

ステップ**3**：インスタンス要件を確認する

コネクタを作成するときは、次の要件を満たすEC2インスタンスタイプを選択する必要があります。

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。

手順**4**：コネクタを作成する

AWS Marketplaceからコネクタを直接作成します。

このタスクについて

AWS Marketplaceからコネクタを作成すると、デフォルト設定を使用してAWSにEC2インスタンスがデプロイされます。 "コネクタのデフォルト設定について説明します"。

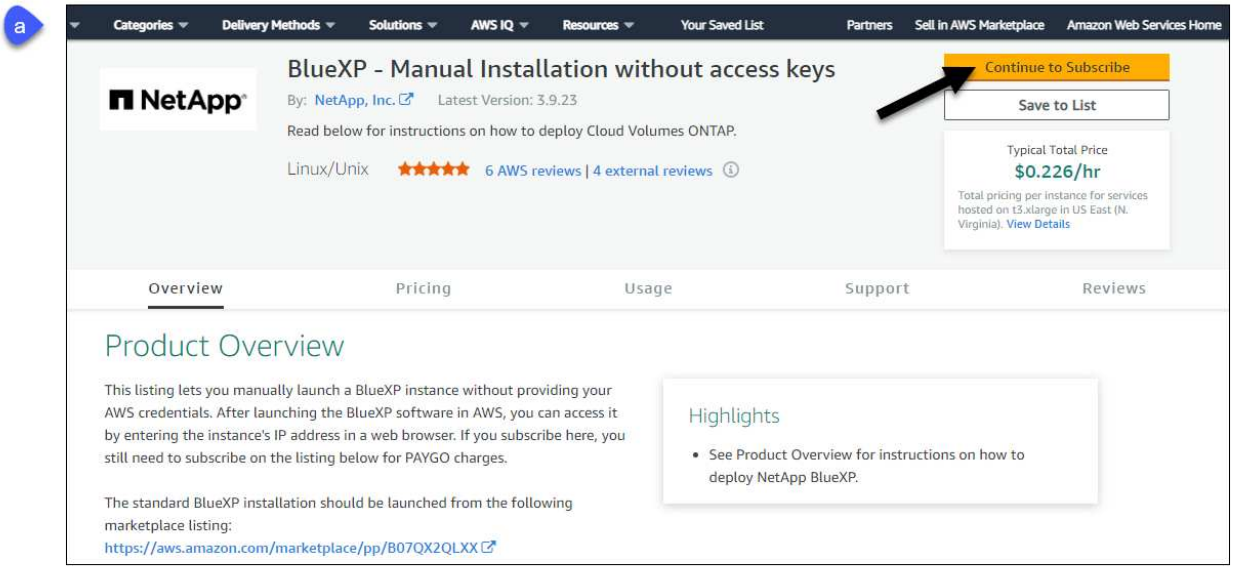
作業を開始する前に

次の情報が必要です。

- ネットワーク要件を満たすVPCとサブネット。
- コネクタに必要な権限を含むポリシーが添付されたIAMロール。
- IAMユーザのAWS Marketplaceをサブスクライブおよびサブスクライブ解除する権限。
- インスタンスのCPUとRAMの要件を理解していること。
- EC2インスタンスのキーペア。

手順

1. にアクセスします "AWS MarketplaceのBlueXPページ"
2. [Marketplace]ページで、**[Continue to Subscribe]***を選択し、[Continue to Configuration]*を選択します。



3. デフォルトのオプションを変更して、*[起動を続行]*を選択します。
4. [Choose Action]*で、[Launch through EC2]*を選択し、[Launch]*を選択します。

   以下の手順では、コンソールからEC2コンソールからインスタンスを起動する方法について説明します。これは、IAMロールをコネクタインスタンスに関連付けることができるためです。これは、 * ウェブサイトからの起動 * アクションを使用しては実行できません。

5. プロンプトに従って、インスタンスを設定および導入します。
   - 名前とタグ：インスタンスの名前とタグを入力します。
   - アプリケーションと**OS**イメージ:このセクションは省略します。コネクタAMIはすでに選択されています。
   - インスタンスタイプ：リージョンの可用性に応じて、RAMとCPUの要件を満たすインスタンスタイプを選択します（T3.xlargeを推奨）。
   - キーペア（ログイン）：インスタンスへのセキュアな接続に使用するキーペアを選択します。
   - ネットワーク設定：必要に応じてネットワーク設定を編集します。
     - 目的のVPCとサブネットを選択します。
     - インスタンスにパブリックIPアドレスを割り当てるかどうかを指定します。

- コネクタインスタンスに必要な接続方法（SSH、HTTP、HTTPS）を有効にするファイアウォール設定を指定します。

  特定の構成にはさらにいくつかのルールが必要です。

  "AWSのセキュリティグループルールを表示します"。

- ストレージの構成：ルートボリュームのデフォルトサイズとディスクタイプを維持します。

  ルートボリュームでAmazon EBS暗号化を有効にする場合は、**[アドバンスト]***を選択し、[ボリューム1]を展開して[暗号化]*を選択し、KMSキーを選択します。

- 詳細情報：*[IAMインスタンスプロファイル]*で、コネクタに必要な権限を含むIAMロールを選択します。
- 概要：概要を確認し、*インスタンスの起動*を選択します。

AWS は、指定した設定でソフトウェアを起動します。コネクタインスタンスとソフトウェアは、約 5 分後に実行される必要があります。

6. Connector 仮想マシンに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

7. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるBlueXPアカウントを指定します。
   b. システムの名前を入力します。
   c. *では、セキュリティ保護された環境で実行していますか？*制限モードを無効にしたままにします。

      標準モードでBlueXPを使用する手順について説明しているため、制限モードは無効にしておく必要があります。セキュアな環境でBlueXPバックエンドサービスからこのアカウントを切断する場合にのみ、制限モードを有効にしてください。その場合は、 "制限モードでBlueXPの使用を開始するには、次の手順に従います"。

   d. [* Let’s start]*を選択します。

結果

これで、コネクタのインストールとBlueXPアカウントでのセットアップが完了しました。

Webブラウザを開き、にアクセスします "BlueXPコンソール" BlueXPでコネクタの使用を開始します

コネクタを作成したAWSアカウントにAmazon S3バケットがある場合は、BlueXPキャンバスにAmazon S3の作業環境が自動的に表示されます。 "BlueXPでS3バケットを管理する方法"

AWSにコネクタを手動でインストールする

独自のLinuxホストにコネクタを手動でインストールするには、ホストの要件を確認し、ネットワークをセットアップし、AWS権限を準備してコネクタをインストールし、準備した権限を指定する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順**1**：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。

キーペア

コネクタを作成するときは、インスタンスで使用するEC2キーペアを選択する必要があります。

/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**2**：ネットワークをセットアップする

コネクタをインストールするネットワークの場所が、次の要件をサポートしていることを確認します。これらの要件を満たすことで、コネクタはハイブリッドクラウド環境内のリソースとプロセスを管理できるようになります。

ターゲットネットワークへの接続

コネクタには、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

手動インストール中にエンドポイントに接続しました

独自のLinuxホストにコネクタを手動でインストールする場合、コネクタのインストーラは、インストールプロセス中に次のURLにアクセスする必要があります。

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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"
\ https://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。

- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

手順**3**：権限を設定する

次のいずれかの方法でBlueXPにAWS権限を指定する必要があります。

- オプション1：IAMポリシーを作成し、EC2インスタンスに関連付けることができるIAMロールにポリシーを関連付けます。
- オプション2：必要な権限を持つIAMユーザのAWSアクセスキーをBlueXPに提供します。

BlueXPの権限を準備する手順は次のとおりです。

IAMロール

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、コネクタのインストール後にEC2インスタンスに関連付けることができるIAMロールが作成されました。

AWSアクセスキー

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、必要な権限とBlueXPへのアクセスキーを持つIAMユーザが作成されました。

手順**4**：コネクタを取り付ける

前提条件が完了したら、ソフトウェアを自分のLinuxホストに手動でインストールできます。

作業を開始する前に

次の情報が必要です。

- コネクタをインストールするためのroot権限。
- コネクタからのインターネットアクセスにプロキシが必要な場合は、プロキシサーバに関する詳細。

  インストール後にプロキシサーバを設定することもできますが、その場合はコネクタを再起動する必要があります。

  BlueXPでは透過型プロキシサーバはサポートされません。

- プロキシサーバがHTTPSを使用している場合、またはプロキシが代行受信プロキシの場合は、CA署名証明書。

このタスクについて

NetApp Support Siteで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後、新しいバージョンが利用可能になると、コネクタは自動的に更新されます。

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. ホストに_http_proxy_or_https_proxy_system変数が設定されている場合は、削除します。

   ```
   unset http_proxy
   unset https_proxy
   ```

   これらのシステム変数を削除しないと、インストールは失敗します。

3. からConnectorソフトウェアをダウンロードします "NetApp Support Site"をクリックし、 Linux ホストにコピーします。

   ネットワークまたはクラウドで使用するための「オンライン」コネクタインストーラをダウンロードする必要があります。コネクタには別の「オフライン」インストーラが用意されていますが、プライベートモード展開でのみサポートされています。

4. スクリプトを実行する権限を割り当てます。

```
chmod +x BlueXP-Connector-Cloud-<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。

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

--proxyパラメータと—cacert.pemパラメータはオプションです。プロキシサーバを使用している場合は、次のようにパラメータを入力する必要があります。プロキシに関する情報の入力を求めるプロンプトは表示されません。

次に、両方のオプションパラメータを使用したコマンドの例を示します。

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxyは、次のいずれかの形式を使用してHTTPまたはHTTPSプロキシサーバを使用するようにコネクタを設定します。

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  次の点に注意してください。

  - ユーザには、ローカルユーザまたはドメインユーザを指定できます。
  - ドメインユーザの場合は、上記のように\にASCIIコードを使用する必要があります。
  - BlueXPでは、@文字を含むパスワードはサポートされていません。

--cacertsは、コネクタとプロキシサーバ間のHTTPSアクセスに使用するCA署名証明書を指定しています。このパラメータは、HTTPSプロキシサーバを指定する場合、または代行受信プロキシを指定する場合にのみ必要です。

6. インストールが完了するまで待ちます。

   プロキシサーバを指定した場合は、インストールの終了時にConnectorサービス（occm）が2回再起動されます。

7. Connector 仮想マシンに接続されているホストから Web ブラウザを開き、次の URL を入力します。

https://ipaddress

8. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるBlueXPアカウントを指定します。
   b. システムの名前を入力します。
   c. *では、セキュリティ保護された環境で実行していますか？*制限モードを無効にしたままにします。

      標準モードでBlueXPを使用する手順について説明しているため、制限モードは無効にしておく必要があります。セキュアな環境でBlueXPバックエンドサービスからこのアカウントを切断する場合にのみ、制限モードを有効にしてください。その場合は、 "制限モードでBlueXPの使用を開始するには、次の手順に従います"。

   d. [* Let’s start]*を選択します。

結果

これでコネクタがインストールされ、BlueXPアカウントでセットアップされました。

コネクタを作成したAWSアカウントにAmazon S3バケットがある場合は、BlueXPキャンバスにAmazon S3の作業環境が自動的に表示されます。 "BlueXPでS3バケットを管理する方法"

手順**5**：**BlueXP**に権限を付与する

コネクタのインストールが完了したら、以前に設定したAWS権限をBlueXPに付与する必要があります。権限を付与することで、BlueXPでAWSのデータとストレージインフラを管理できるようになります。

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。

にアクセスします "BlueXPコンソール" BlueXPでコネクタの使用を開始します

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で正しいコネクタが選択されていることを確認します
2. 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。

3. [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。

にアクセスします "BlueXPコンソール" BlueXPでコネクタの使用を開始します

Azure

Azureでのコネクタのインストールオプション

Azureでコネクタを作成する方法はいくつかあります。最も一般的な方法はBlueXPから直接実行することです。

次のインストールオプションを使用できます。

- "BlueXPからコネクタを直接作成" （これは標準オプションです）

  この操作により、Linuxを実行するVMとコネクタソフトウェアが任意のVNetで起動されます。

- "Azure Marketplace からコネクタを作成します"

  また、Linuxを実行するVMとConnectorソフトウェアも起動しますが、導入はBlueXPではなくAzure Marketplaceから直接開始されます。

- "ソフトウェアをダウンロードして、自分のLinuxホストに手動でインストールします"

選択するインストールオプションは、インストールの準備方法に影響します。これには、Azureのリソースの認証と管理に必要な権限をBlueXPに付与する方法も含まれます。

BlueXPからAzureにコネクタを作成します

BlueXPからAzureでコネクタを作成するには、ネットワークを設定し、Azureの権限を準備してから、コネクタを作成する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順1：ネットワークをセットアップする

コネクタをインストールするネットワークの場所が、次の要件をサポートしていることを確認します。これらの要件を満たすことで、コネクタはハイブリッドクラウド環境内のリソースとプロセスを管理できるようになります。

Azure リージョン

Cloud Volumes ONTAPを使用する場合は、コネクタを管理するCloud Volumes ONTAPシステムと同じAzureリージョンまたはに導入する必要があります "Azure リージョンペア" Cloud Volumes ONTAP システム用。この要件により、 Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間で Azure Private Link 接続が使用されるようになります。

"Cloud Volumes ONTAP での Azure プライベートリンクの使用方法をご確認ください"

VNetおよびサブネット

コネクタを作成するときは、コネクタを配置するVNetとサブネットを指定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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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.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://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

BlueXPコンソールからアクセスするエンドポイント

SaaSレイヤで提供されるWebベースのBlueXPコンソールを使用すると、IT部門は複数のエンドポイントと通信してデータ管理タスクを実行します。これには、BlueXPコンソールからコネクタを導入するために接続されるエンドポイントも含まれます。

"BlueXPコンソールからアクセスしたエンドポイントのリストを表示します"。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

コネクタを作成した後で、このネットワーク要件を実装する必要があります。

手順**2**：カスタムロールを作成する

AzureアカウントまたはMicrosoft Entraサービスプリンシパルに割り当てることができるAzureカスタムロールを作成します。BlueXPはAzureで認証し、これらの権限を使用してコネクタインスタンスを作成します。

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"

手順

1. Azureの新しいカスタムロールに必要な権限をコピーし、JSONファイルに保存します。

   このカスタムロールには、BlueXPからAzureでコネクタVMを起動するために必要な権限のみが含まれています。このポリシーは、他の状況では使用しないでください。BlueXPがコネクタを作成すると、Connector VMに新しい権限セットが適用され、Connectorがパブリッククラウド環境内のリソースを管理できるようになります。

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
```

```
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. JSONを変更して、割り当て可能な範囲にAzureサブスクリプションIDを追加します。

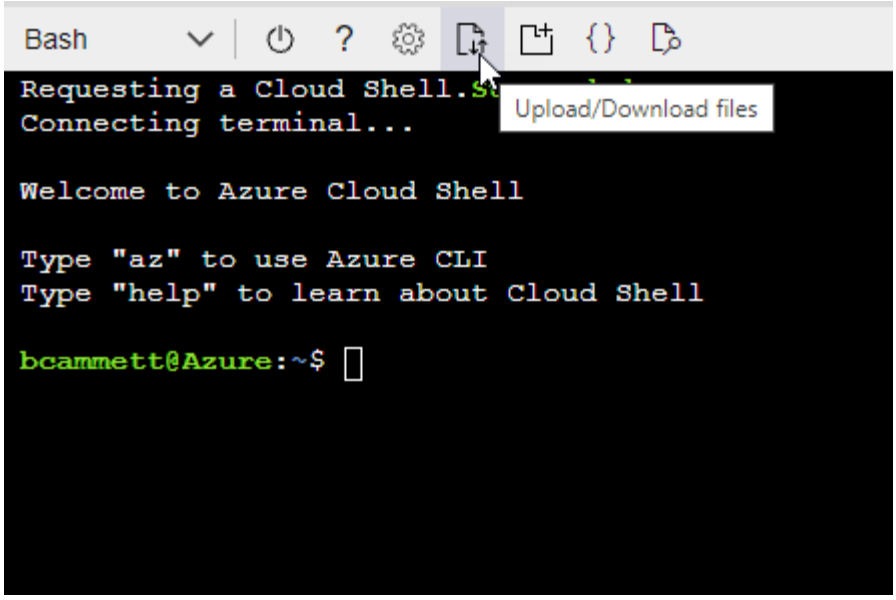
   - 例 *

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

3. 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 で次のコマンドを入力します。

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

これで、 _Azure SetupAsService_という カスタムロールが作成されました。このカスタムロールをユーザーアカウントまたはサービスプリンシパルに適用できるようになりました。

手順**3**：認証を設定する

BlueXPからコネクタを作成するときは、BlueXPがAzureで認証してVMを導入するためのログインを指定する必要があります。次の 2 つのオプションがあります。

1. プロンプトが表示されたら、Azureアカウントでサインインします。このアカウントには Azure 固有の権限が必要です。これがデフォルトのオプションです。
2. Microsoft Entraサービスプリンシパルの詳細を入力します。このサービスプリンシパルには、特定の権限も必要です。

次の手順に従って、いずれかの認証方式をBlueXPで使用できるように準備します。

Azureアカウント

BlueXPからコネクタを導入するユーザにカスタムロールを割り当てます。

手順

1. Azureポータルで、* Subscriptions *サービスを開き、ユーザーのサブスクリプションを選択します。
2. 「 * アクセスコントロール（ IAM ） * 」をクリックします。
3. [* 追加 **>** 役割の割り当ての追加 *] をクリックして、権限を追加します。
   a. Azure SetupAsService * ロールを選択し、 * 次へ * をクリックします。

   > Azure SetupAsServiceは、Azureのコネクタ導入ポリシーで指定されているデフォルトの名前です。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。

   b. [* 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。
   c. [* メンバーの選択 *] をクリックし、ユーザーアカウントを選択して、 [* 選択 *] をクリックします。
   d. 「 * 次へ * 」をクリックします。
   e. [レビュー + 割り当て（ Review + Assign ）] をクリックします。

結果

これで、Azureユーザには、BlueXPからConnectorを導入するために必要な権限が付与されました。

サービスプリンシパル

Azureアカウントでログインする代わりに、必要な権限を持つAzureサービスプリンシパルのクレデンシャルをBlueXPに指定できます。

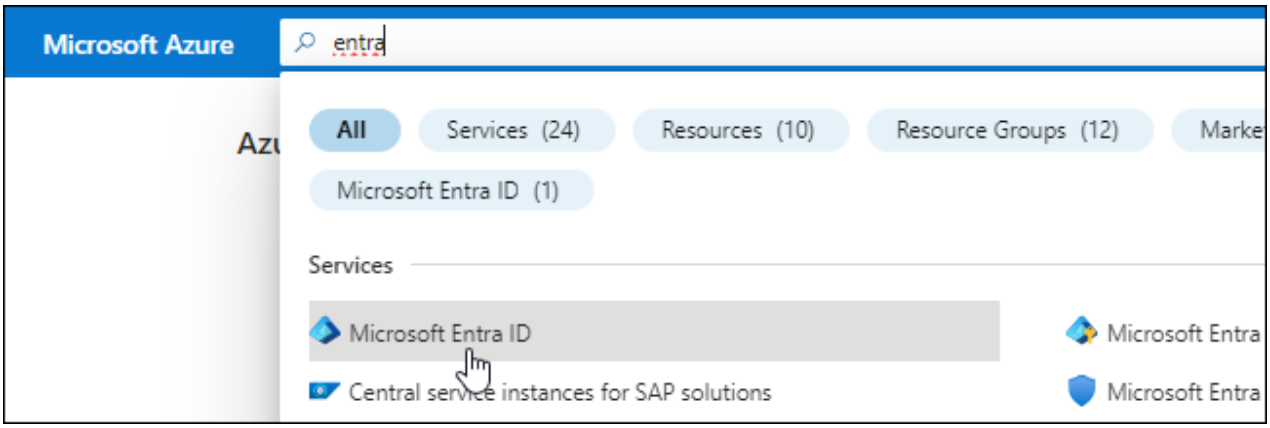
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。

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。

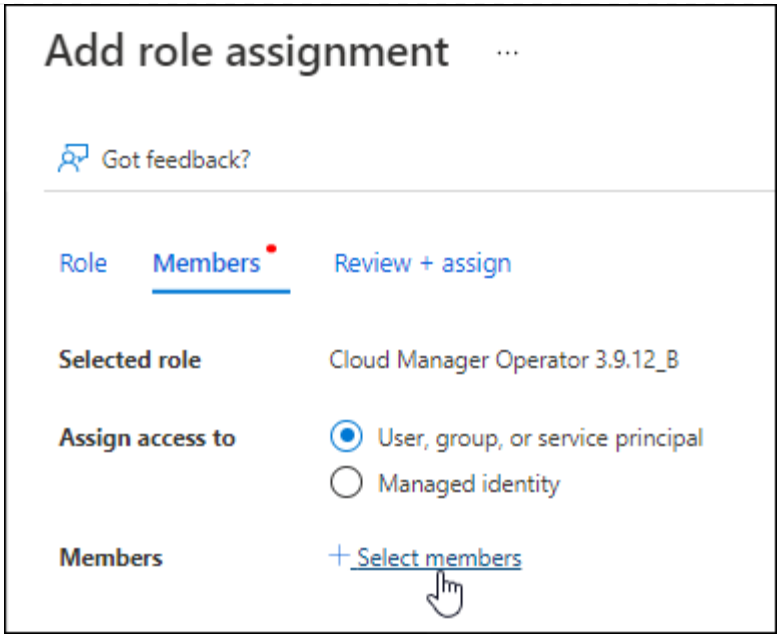


3. メニューで*アプリ登録*を選択します。
4. [New registration]*を選択します。
5. アプリケーションの詳細を指定します。
   - * 名前 * ：アプリケーションの名前を入力します。
   - アカウントの種類:アカウントの種類を選択します(すべてのアカウントはBlueXPで動作します)。
   - * リダイレクト URI *: このフィールドは空白のままにできます。
6. [*Register] を選択します。

   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。

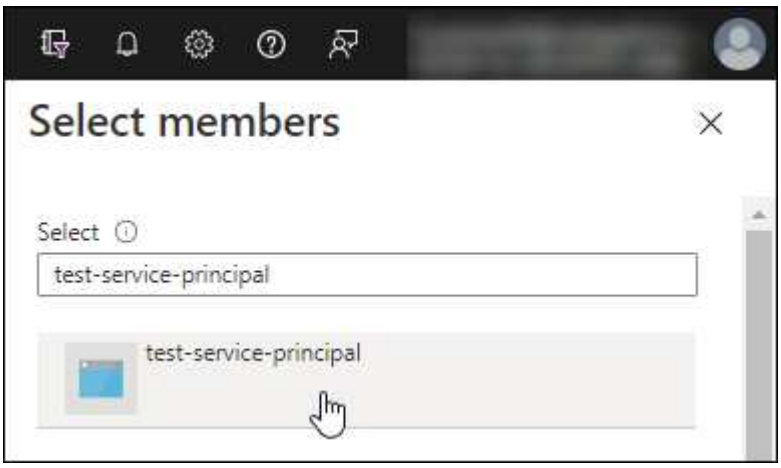
アプリケーションにカスタムロールを割り当てます

1. Azure ポータルで、 * Subscriptions * サービスを開きます。
2. サブスクリプションを選択します。
3. [* アクセス制御 (IAM)] 、 [追加] 、 [役割の割り当ての追加 *] の順にクリックします。
4. [役割]タブで、**[** BlueXP演算子*]役割を選択し、[次へ]をクリックします。
5. [* Members* （メンバー * ）] タブで、次の手順を実行します。
   a. [* 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。
   b. [メンバーの選択] をクリックします。



c. 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。



a. アプリケーションを選択し、 * Select * をクリックします。

b. 「 * 次へ * 」をクリックします。

6. [レビュー + 割り当て（ Review + Assign ）] をクリックします。

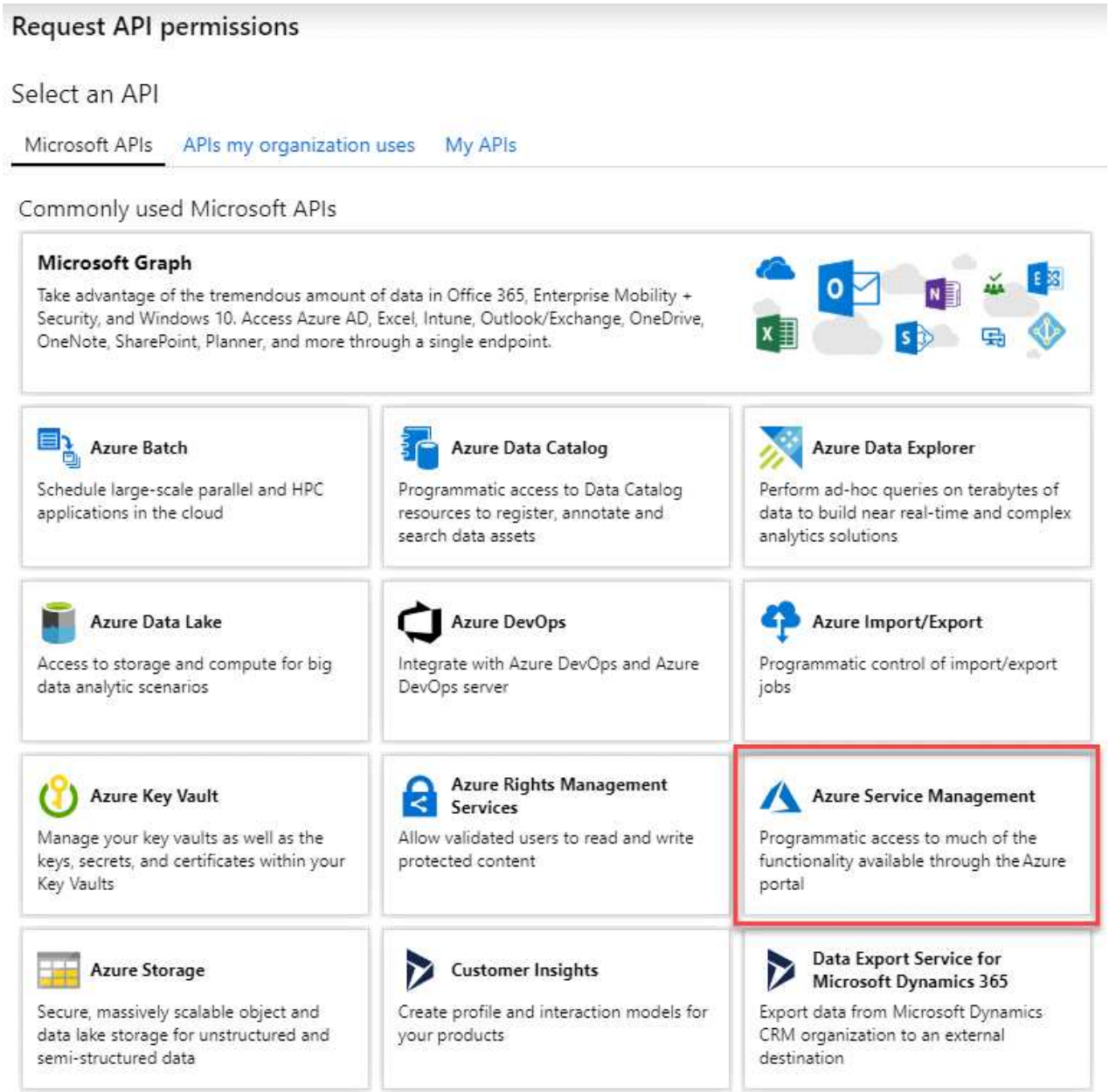
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

複数のAzureサブスクリプションでリソースを管理する場合は、各サブスクリプションにサービスプリンシパルをバインドする必要があります。たとえば、BlueXPでは、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。

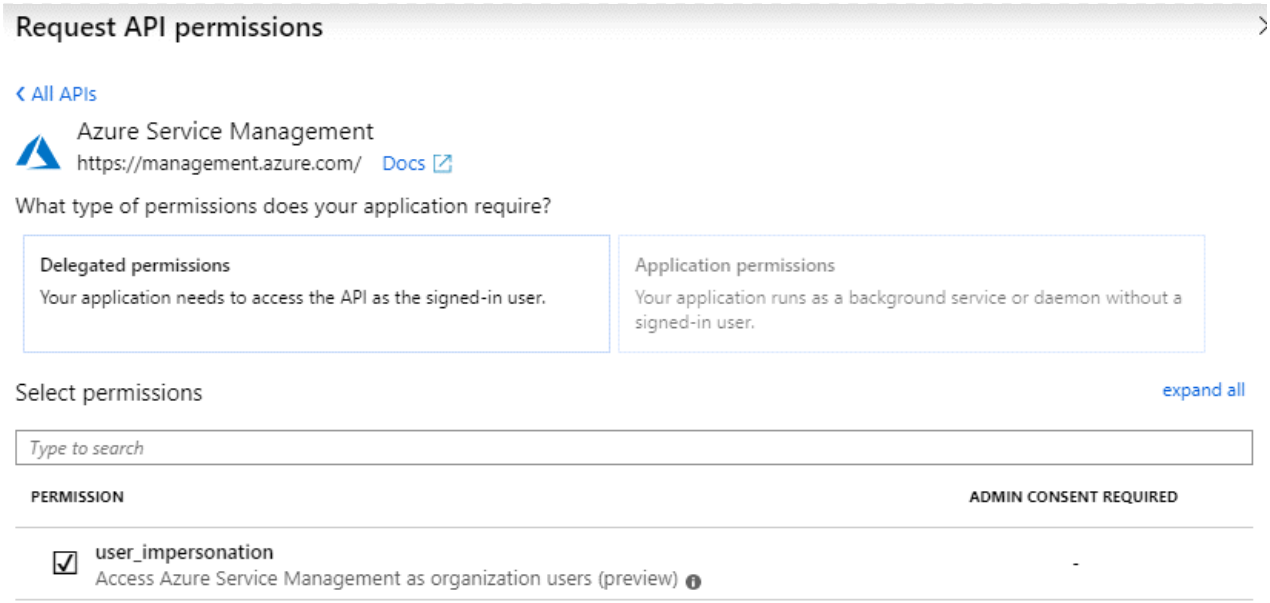
Windows Azure Service Management API 権限を追加します

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。

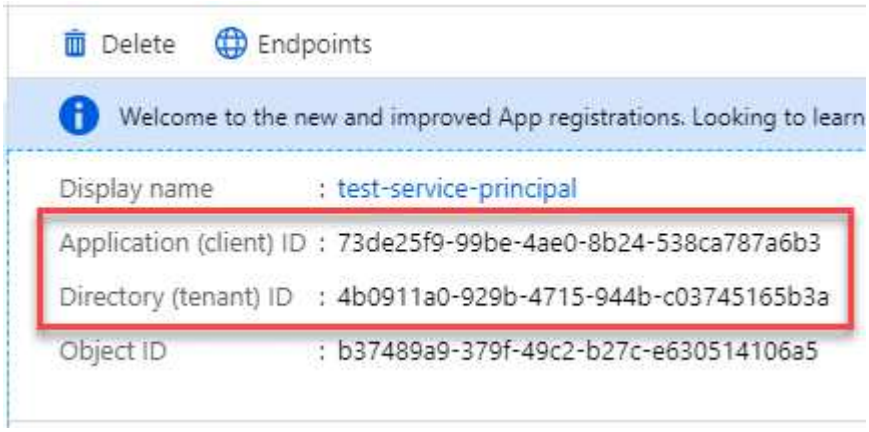


4. を選択し、[Add permissions]*を選択します。



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。コネクタを作成するときに、BlueXPでこの情報を入力する必要があります。

手順4：コネクタを作成する

BlueXPのWebベースのコンソールから直接コネクタを作成します。

このタスクについて

BlueXPからコネクタを作成すると、デフォルトの設定を使用してAzureに仮想マシンが導入されます。コネクタの作成後は、CPUやRAMが少ないVMタイプに変更しないでください。 "コネクタのデフォルト設定について説明します"。

作業を開始する前に

次の情報が必要です。

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet およびサブネット
- すべての発信インターネットトラフィックにプロキシを必要とする場合は、プロキシサーバの詳細を参照してください。
  - IP アドレス
  - クレデンシャル
  - HTTPS証明書
- コネクタ仮想マシンでその認証方法を使用する場合は、SSH公開鍵。認証方法のもう1つのオプションは、パスワードを使用することです。

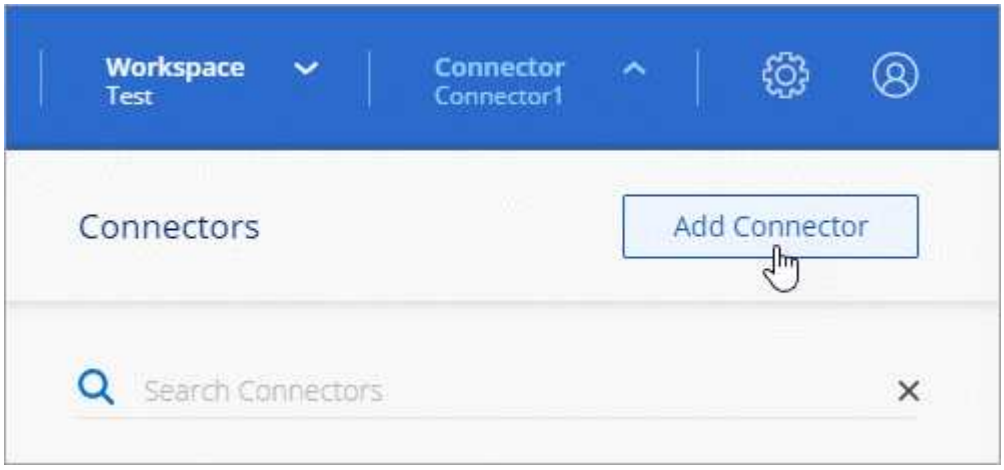
  "AzureでLinux VMに接続する方法について説明します"

- BlueXPでコネクタ用のAzureロールを自動的に作成しない場合は、自分で作成する必要があります "このページのポリシーを使用する"。

  これらの権限はコネクタインスタンス自体に適用されます。これは、コネクタVMを導入するために以前に設定した権限とは異なる権限のセットです。

手順

1. ドロップダウンを選択し、[コネクタの追加]*を選択します。



2. クラウドプロバイダとして「 * Microsoft Azure * 」を選択します。
3. [*コネクターの配置（Deploying a Connector *）]ページ：

   a. [認証]*で、Azure権限の設定方法に一致する認証オプションを選択します。

      - Azureユーザーアカウント*を選択して、必要な権限があるMicrosoftアカウントにログインします。

        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。

        すでにAzureアカウントにログインしている場合は、BlueXPによって自動的にそのアカウントが使用されます。アカウントが複数ある場合は、適切なアカウントを使用するために、最初にログアウトする必要があります。

      - [Active Directory service principal]*を選択して、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

   サービスプリンシパルのこれらの値を取得する方法について説明します。

4. ウィザードの手順に従って、コネクタを作成します。

   - * VM認証*：Azureサブスクリプション、場所、新しいリソースグループ、または既存のリソースグループを選択し、作成するコネクタ仮想マシンの認証方法を選択します。

     仮想マシンの認証方法には、パスワードまたはSSH公開鍵を使用できます。

   "AzureでLinux VMに接続する方法について説明します"

   - 詳細:インスタンスの名前を入力し、タグを指定して、必要な権限を持つ新しいロールを作成するか、またはで設定した既存のロールを選択するかを選択します "必要な権限"。

このロールに関連付けられているAzureサブスクリプションを選択できることに注意してください。選択した各サブスクリプションには、そのサブスクリプション内のリソースを管理するためのコネクタ権限（Cloud Volumes ONTAPなど）が用意されています。

- * ネットワーク * ： VNet とサブネットを選択し、パブリック IP アドレスを有効にするかどうか、および必要に応じてプロキシ設定を指定します。
- セキュリティグループ:新しいセキュリティグループを作成するか、必要なインバウンドおよびアウトバウンドルールを許可する既存のセキュリティグループを選択するかを選択します。

  "Azureのセキュリティグループルールを表示します"。

- * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

5. [追加（ Add ）] をクリックします。

   仮想マシンの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

結果

プロセスが完了すると、BlueXPからコネクタを使用できるようになります。

コネクタを作成したAzureサブスクリプションと同じAzure BLOBストレージがある場合は、BlueXPキャンバスにAzure BLOBストレージの作業環境が自動的に表示されます。 "BlueXPからAzure Blobストレージを管理する方法"

Azure Marketplace からコネクタを作成します

Azure Marketplaceからコネクタを作成するには、ネットワークを設定し、Azureの権限を準備し、インスタンス要件を確認してからコネクタを作成する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順**1**：ネットワークをセットアップする

コネクタをインストールするネットワークの場所が、次の要件をサポートしていることを確認します。これらの要件を満たすことで、コネクタはハイブリッドクラウド環境内のリソースとプロセスを管理できるようになります。

Azure リージョン

Cloud Volumes ONTAPを使用する場合は、コネクタを管理するCloud Volumes ONTAPシステムと同じAzureリージョンまたはに導入する必要があります "Azure リージョンペア" Cloud Volumes ONTAP システム用。この要件により、 Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間で Azure Private Link 接続が使用されるようになります。

"Cloud Volumes ONTAP での Azure プライベートリンクの使用方法をご確認ください"

VNetおよびサブネット

コネクタを作成するときは、コネクタを配置するVNetとサブネットを指定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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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.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://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

コネクタを作成した後で、このネットワーク要件を実装する必要があります。

ステップ**2**：**VM**の要件を確認する

コネクタを作成するときは、次の要件を満たす仮想マシンタイプを選択する必要があります。

CPU

4 コアまたは 4 個の vCPU

RAM

14GB

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。

手順**3**：権限を設定する

権限は次の方法で指定できます。

- オプション1：システム割り当ての管理IDを使用して、Azure VMにカスタムロールを割り当てます。

- オプション2：必要な権限を持つAzureサービスプリンシパルのクレデンシャルをBlueXPに提供します。

BlueXPの権限を設定するには、次の手順を実行します。

カスタムロール

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. 独自のホストにソフトウェアを手動でインストールする場合は、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、VMでシステムが割り当てた管理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。

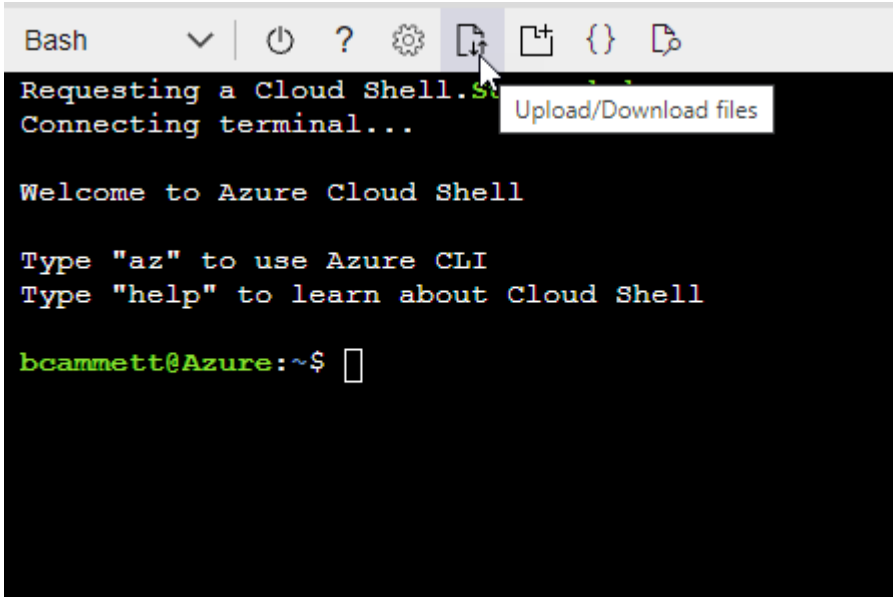
   - 例 *

```
"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。

サービスプリンシパル

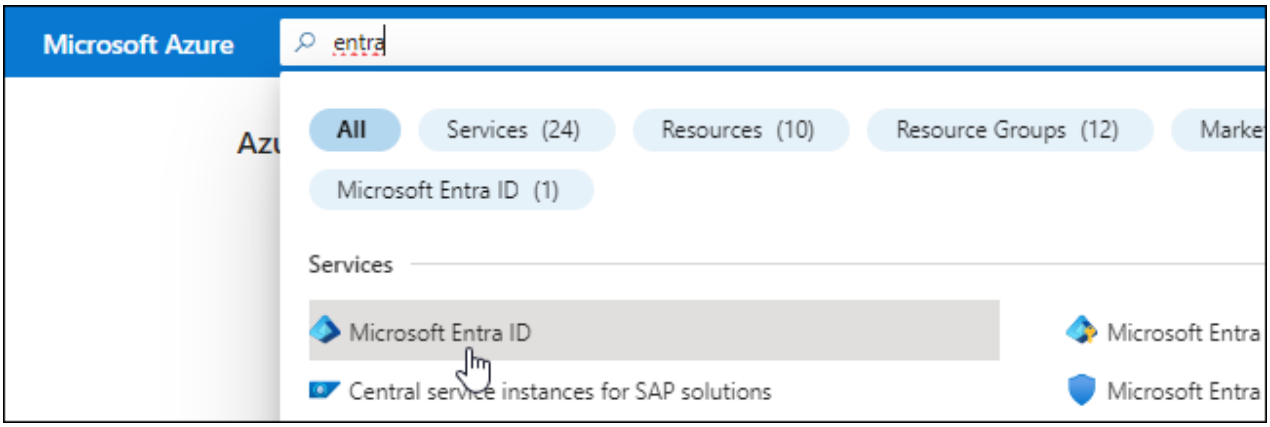
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。

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。

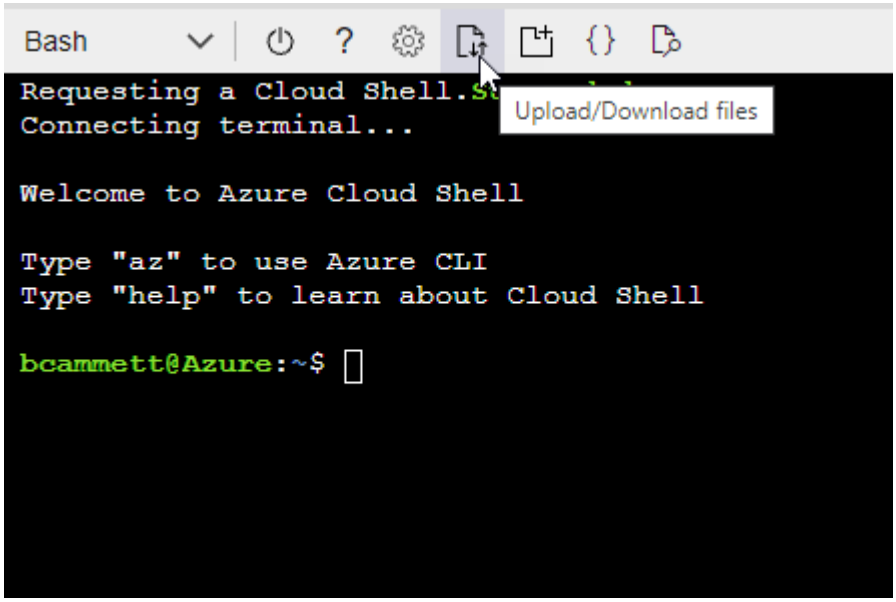
   - 例 *

```
"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
```

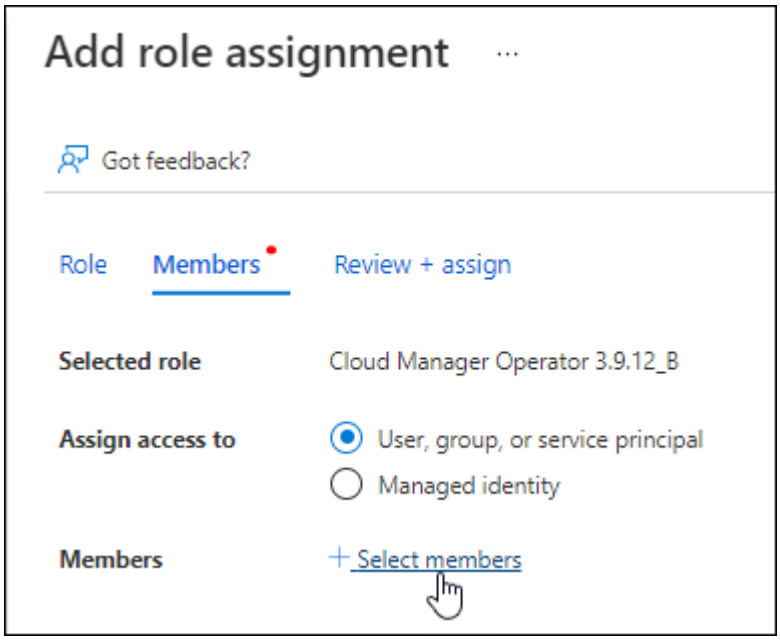
   これで、Connector仮想マシンに割り当てることができるBlueXP Operatorというカスタムロ

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。

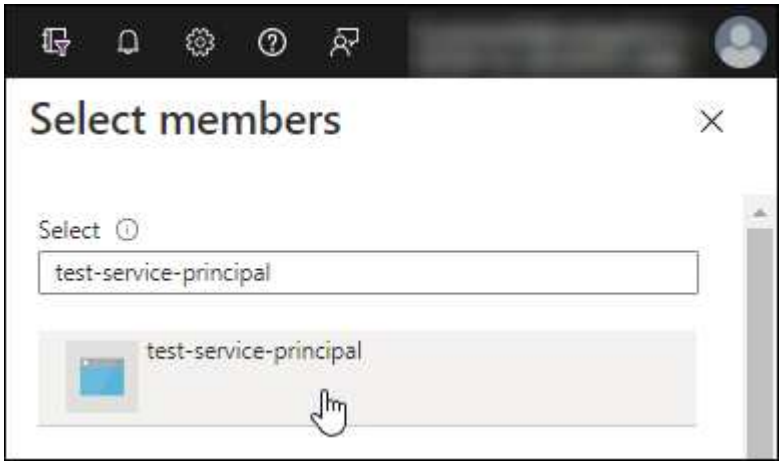
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。

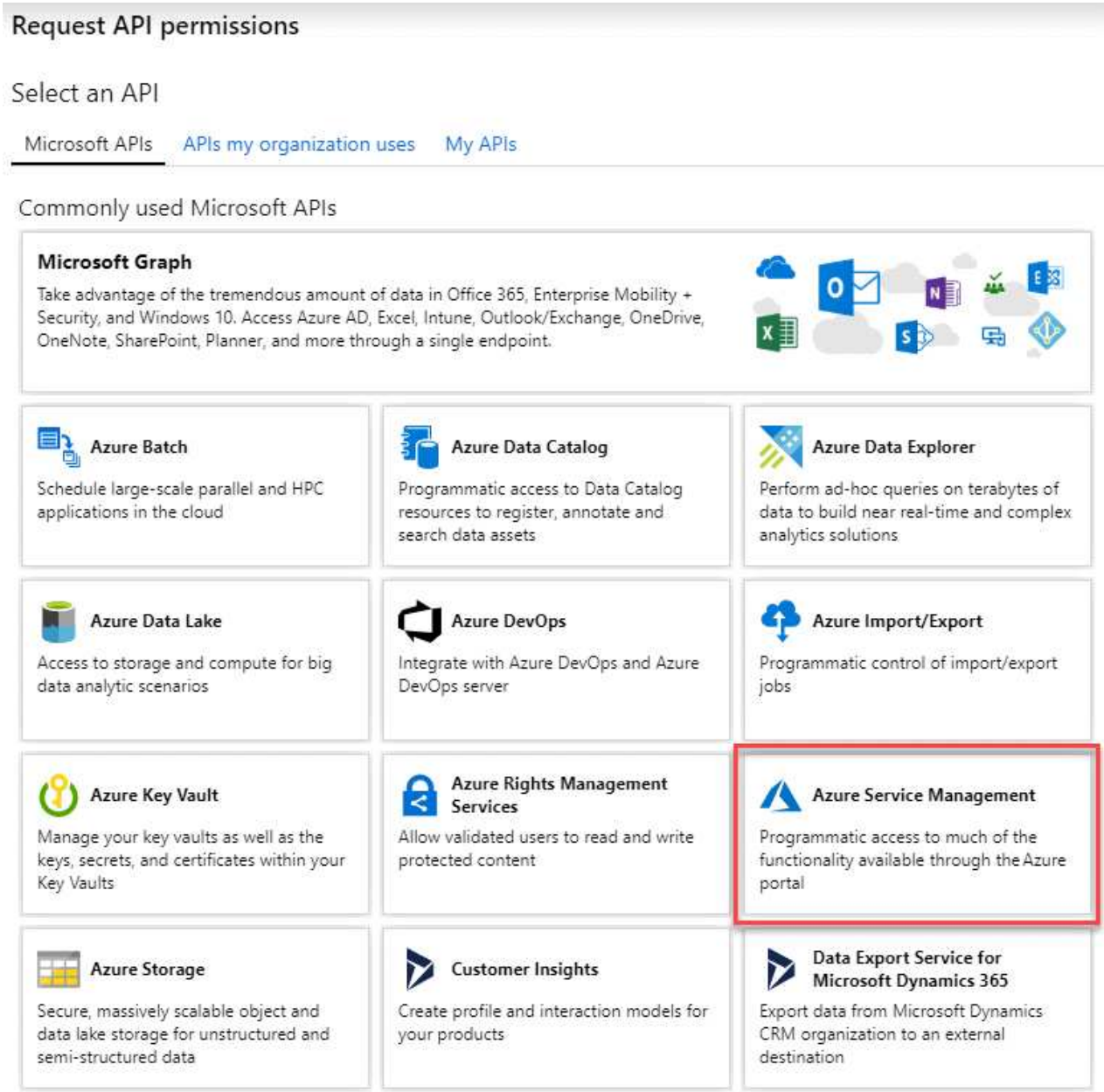
f. [Review + Assign]*を選択します。

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。

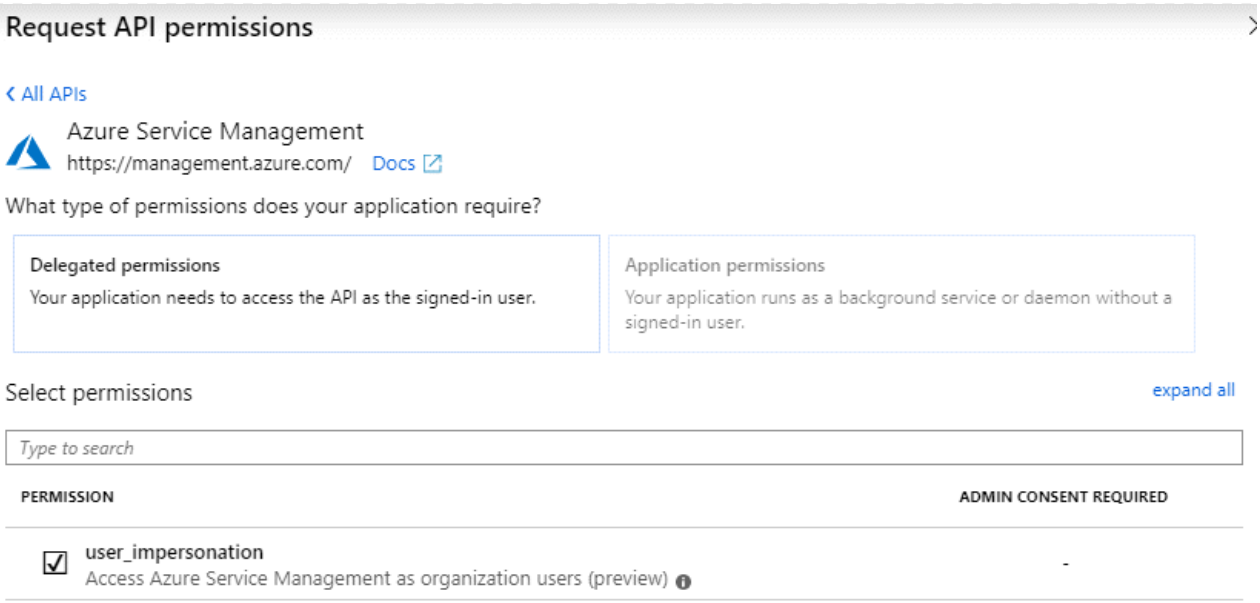
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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。

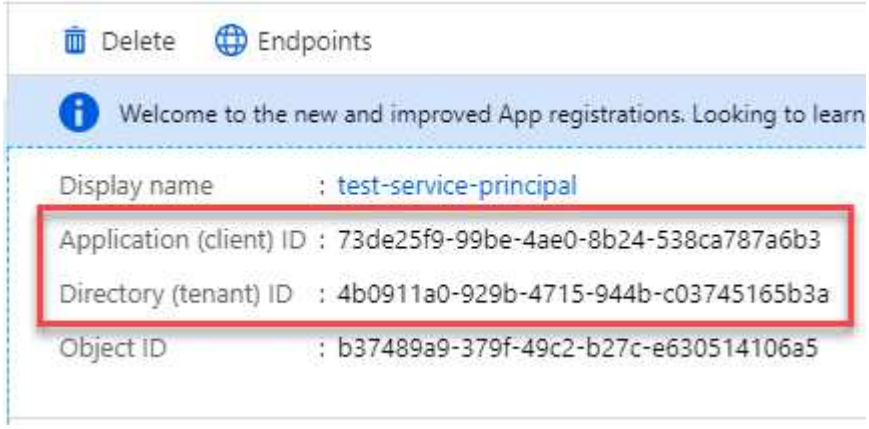


4. を選択し、[Add permissions]*を選択します。



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。

手順**4**：コネクタを作成する

Azure Marketplaceからコネクタを直接起動します。

このタスクについて

Azure Marketplaceからコネクタを作成すると、デフォルト構成を使用してAzureに仮想マシンが導入されます。 "コネクタのデフォルト設定について説明します"。

作業を開始する前に

次の情報が必要です。

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet およびサブネット
- すべての発信インターネットトラフィックにプロキシを必要とする場合は、プロキシサーバの詳細を参照してください。
  - IP アドレス
  - クレデンシャル
  - HTTPS証明書
- コネクタ仮想マシンでその認証方法を使用する場合は、SSH公開鍵。認証方法のもう1つのオプションは、パスワードを使用することです。

  "AzureでLinux VMに接続する方法について説明します"

- BlueXPでコネクタ用のAzureロールを自動的に作成しない場合は、自分で作成する必要があります "このページのポリシーを使用する"。

  これらの権限はコネクタインスタンス自体に適用されます。これは、コネクタVMを導入するために以前に設定した権限とは異なる権限のセットです。

手順

1. Azure MarketplaceのNetApp Connector VMのページに移動します。

   "Azure Marketplaceの一般企業向けページ"

2. を選択し、[続行]*を選択します。
3. Azureポータルで、*[作成]*を選択し、手順に従って仮想マシンを設定します。

   VM を設定する際には、次の点に注意してください。

   - * VMサイズ*：CPUとRAMの要件を満たすVMサイズを選択します。DS3 v2 を推奨します。
   - ディスク：コネクタはHDDまたはSSDディスクで最適なパフォーマンスを発揮します。
   - ネットワークセキュリティグループ：コネクタには、SSH、HTTP、およびHTTPSを使用したインバウンド接続が必要です。

     "Azureのセキュリティグループルールを表示します"。

   - * ID ： Management で Enable system assigned managed identity *を選択します。

     管理されたIDを使用すると、コネクタ仮想マシンは資格情報を提供せずにMicrosoft Entra IDに対して自身を識別できるため、この設定は重要です。 "Azure リソース用の管理対象 ID の詳細については、こちらをご覧ください"。

4. [確認と作成]ページで、選択内容を確認し、*[作成]*を選択して導入を開始します。

   指定した設定で仮想マシンが展開されます。仮想マシンと Connector ソフトウェアが起動するまでの所要時間は約 5 分です。

5. Connector 仮想マシンに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

6. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるBlueXPアカウントを指定します。
   b. システムの名前を入力します。
   c. *では、セキュリティ保護された環境で実行していますか？*制限モードを無効にしたままにします。

      標準モードでBlueXPを使用する手順について説明しているため、制限モードは無効にしておく必要があります。セキュアな環境でBlueXPバックエンドサービスからこのアカウントを切断する場合にのみ、制限モードを有効にしてください。その場合は、 "制限モードでBlueXPの使用を開始するには、次の手順に従います"。

   d. [* Let’s start]*を選択します。

結果

これでコネクタがインストールされ、BlueXPアカウントでセットアップされました。

コネクタを作成したAzureサブスクリプションと同じAzure BLOBストレージがある場合は、BlueXPキャンバスにAzure BLOBストレージの作業環境が自動的に表示されます。 "BlueXPからAzure Blobストレージを管理する方法"

手順**5**：**BlueXP**に権限を付与する

コネクタの作成が完了したら、以前に設定した権限をBlueXPに付与する必要があります。権限を付与することで、AzureのデータとストレージインフラをBlueXPで管理できるようになります。

カスタムロール

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。

次の手順

にアクセスします "BlueXPコンソール" BlueXPでコネクタの使用を開始します

サービスプリンシパル

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。

Azureへのコネクタの手動インストール

独自のLinuxホストにコネクタを手動でインストールするには、ホストの要件を確認し、ネットワークをセットアップし、Azureの権限を準備してから、コネクタをインストールし、準備した権限を指定する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順**1**：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

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。

/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**2**：ネットワークをセットアップする

コネクタをインストールするネットワークの場所が、次の要件をサポートしていることを確認します。これらの要件を満たすことで、コネクタはハイブリッドクラウド環境内のリソースとプロセスを管理できるようになります。

Azure リージョン

Cloud Volumes ONTAPを使用する場合は、コネクタを管理するCloud Volumes ONTAPシステムと同じAzureリージョンまたはに導入する必要があります "Azure リージョンペア" Cloud Volumes ONTAP システム用。この要件により、 Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間で Azure Private Link 接続が使用されるようになります。

"Cloud Volumes ONTAP での Azure プライベートリンクの使用方法をご確認ください"

ターゲットネットワークへの接続

コネクタには、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

手動インストール中にエンドポイントに接続しました

独自のLinuxホストにコネクタを手動でインストールする場合、コネクタのインストーラは、インストールプロセス中に次のURLにアクセスする必要があります。

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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.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://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。

エンドポイント	目的
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

手順**3**：権限を設定する

次のいずれかのオプションを使用して、BlueXPにAzure権限を設定する必要があります。

- オプション1：システム割り当ての管理IDを使用して、Azure VMにカスタムロールを割り当てます。
- オプション2：必要な権限を持つAzureサービスプリンシパルのクレデンシャルをBlueXPに提供します。

BlueXPの権限を準備する手順は次のとおりです。

カスタムロール

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. 独自のホストにソフトウェアを手動でインストールする場合は、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、VMでシステムが割り当てた管理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。

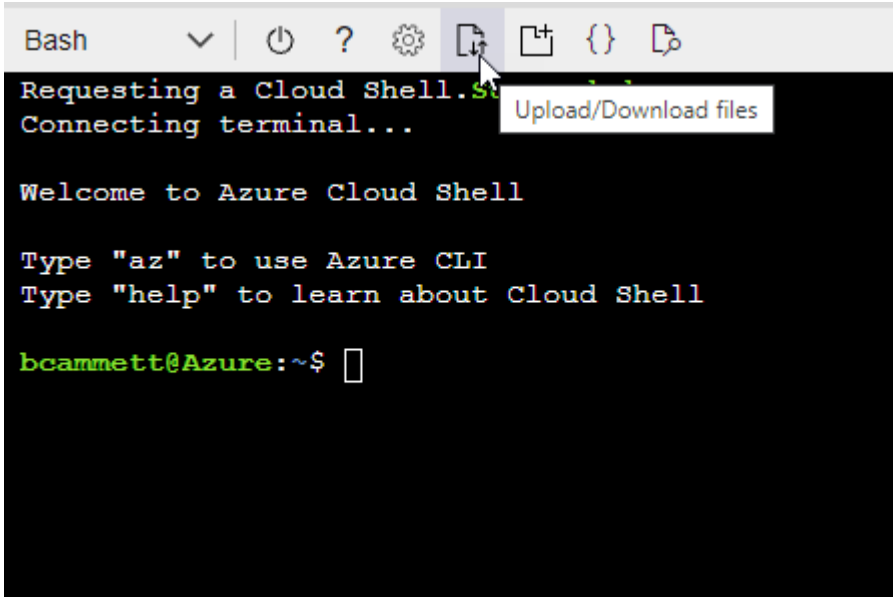
   - 例 *

```
"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。

サービスプリンシパル

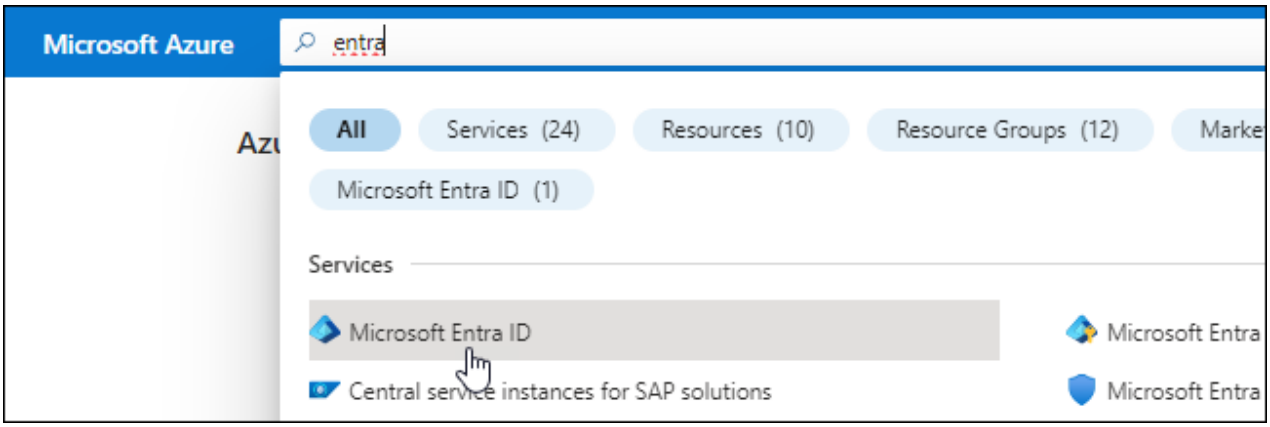
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。

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。

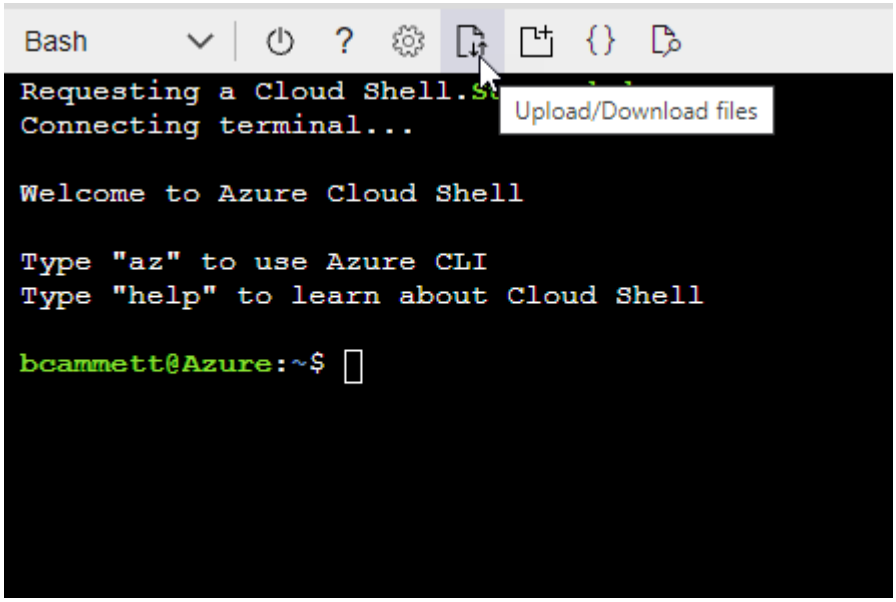
   - 例 *

```
"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
```

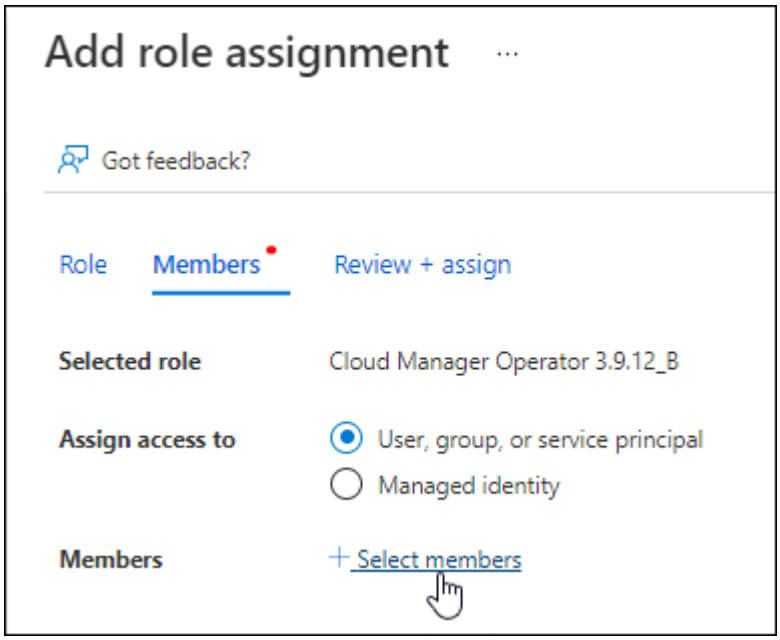
   これで、Connector仮想マシンに割り当てることができるBlueXP Operatorというカスタムロ

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。

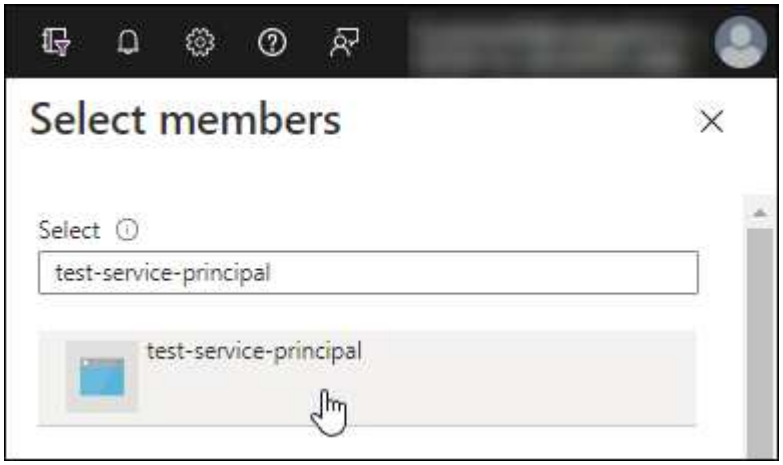
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。

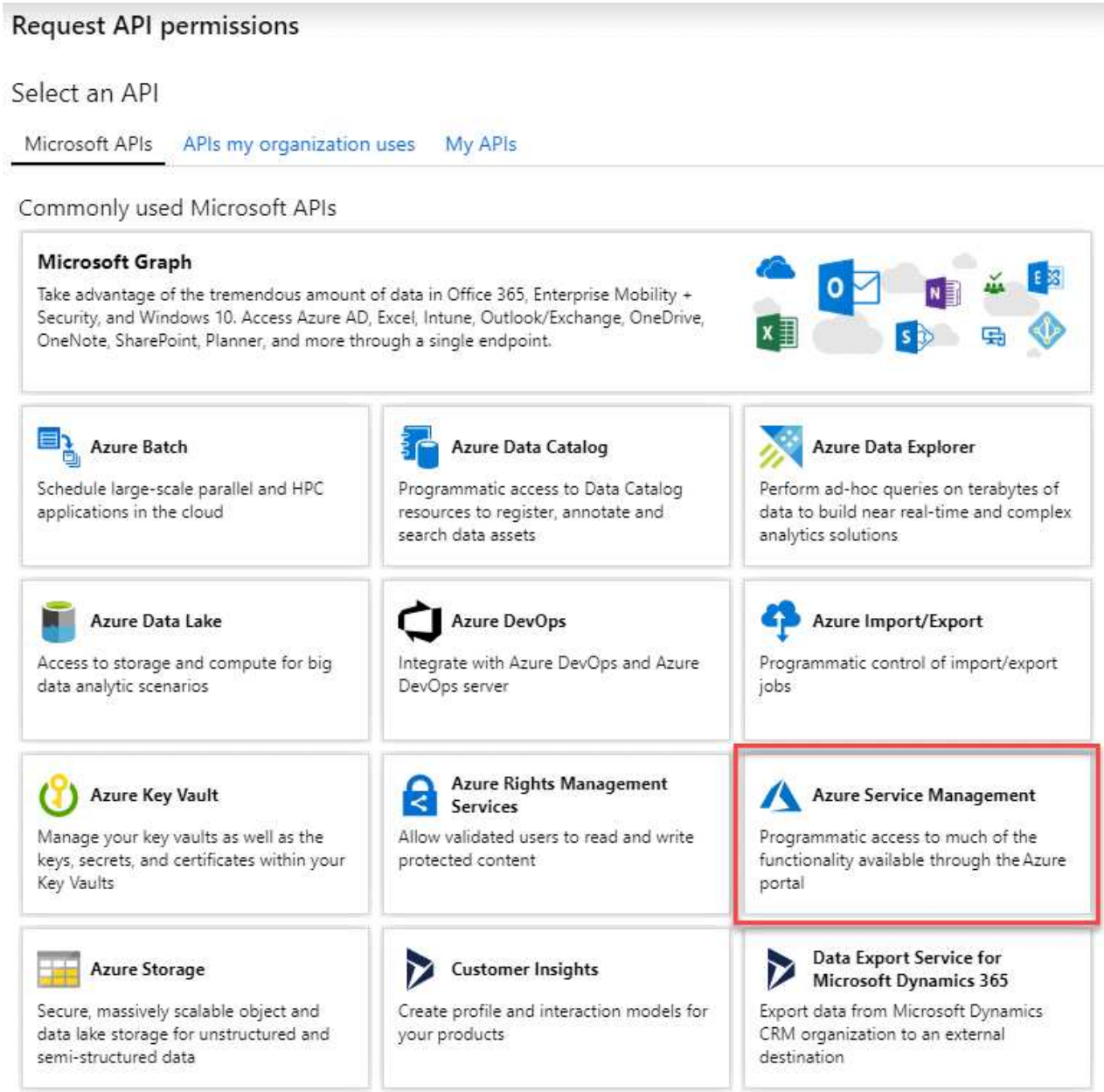
f. [Review + Assign]*を選択します。

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。

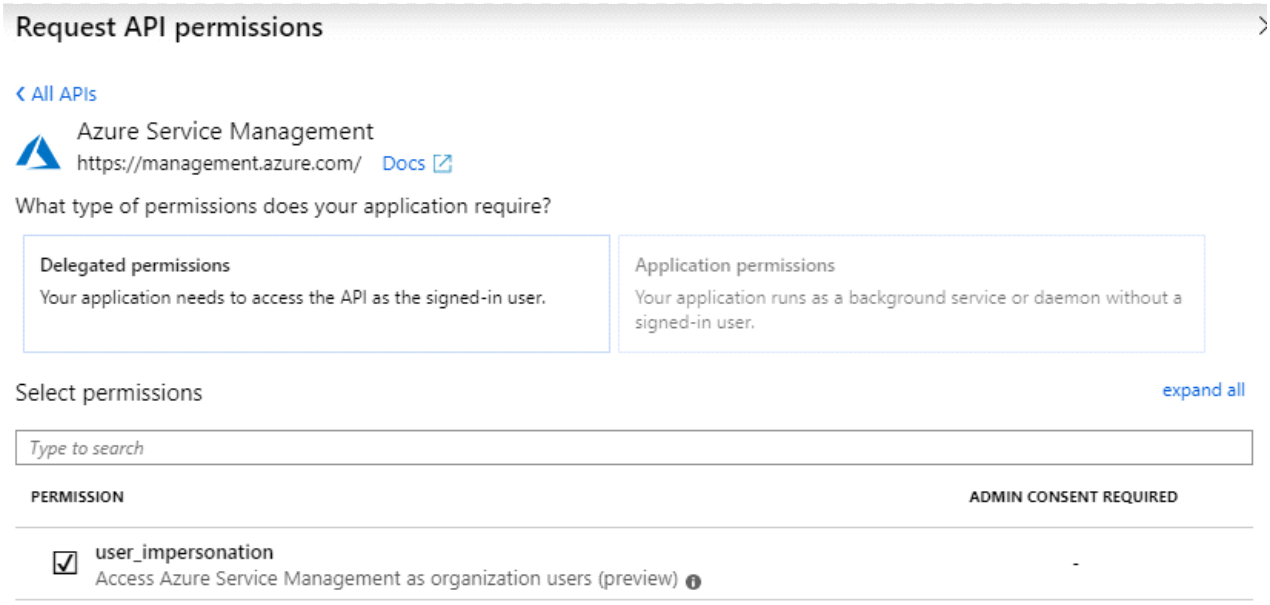
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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。

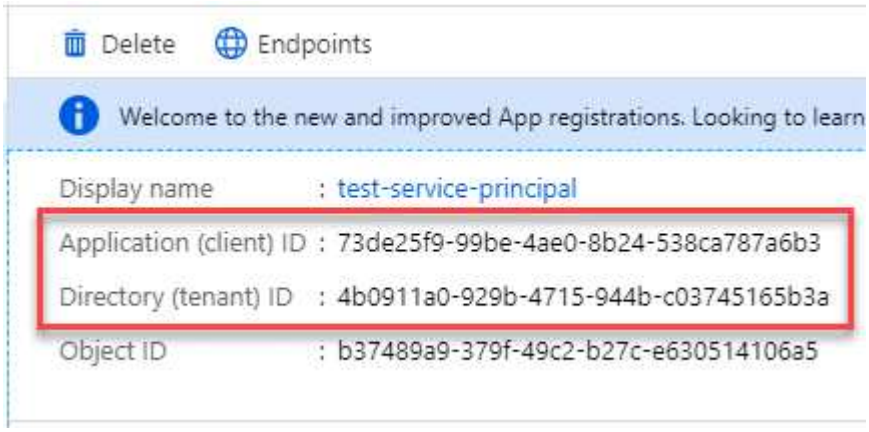


4. を選択し、[Add permissions]*を選択します。



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。

手順**4**：コネクタを取り付ける

前提条件が完了したら、ソフトウェアを自分のLinuxホストに手動でインストールできます。

作業を開始する前に

次の情報が必要です。

- コネクタをインストールするためのroot権限。
- コネクタからのインターネットアクセスにプロキシが必要な場合は、プロキシサーバに関する詳細。

  インストール後にプロキシサーバを設定することもできますが、その場合はコネクタを再起動する必要があります。

  BlueXPでは透過型プロキシサーバはサポートされません。

- プロキシサーバがHTTPSを使用している場合、またはプロキシが代行受信プロキシの場合は、CA署名証明書。
- カスタムロールを使用して必要なAzure権限を指定できるように、AzureのVMで有効になっている管理対象ID。

  "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"

このタスクについて

NetApp Support Siteで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後、新しいバージョンが利用可能になると、コネクタは自動的に更新されます。

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. ホストに_http_proxy_or_https_proxy_system変数が設定されている場合は、削除します。

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

3. からConnectorソフトウェアをダウンロードします "NetApp Support Site"をクリックし、 Linux ホストにコピーします。

ネットワークまたはクラウドで使用するための「オンライン」コネクタインストーラをダウンロードする必要があります。コネクタには別の「オフライン」インストーラが用意されていますが、プライベートモード展開でのみサポートされています。

4. スクリプトを実行する権限を割り当てます。

```
chmod +x BlueXP-Connector-Cloud-<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。

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

--proxyパラメータと—cacert.pemパラメータはオプションです。プロキシサーバを使用している場合は、次のようにパラメータを入力する必要があります。プロキシに関する情報の入力を求めるプロンプトは表示されません。

次に、両方のオプションパラメータを使用したコマンドの例を示します。

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxyは、次のいずれかの形式を使用してHTTPまたはHTTPSプロキシサーバを使用するようにコネクタを設定します。

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port

- https://domain-name%92user-name:password@address:port

  次の点に注意してください。

  - ユーザには、ローカルユーザまたはドメインユーザを指定できます。
  - ドメインユーザの場合は、上記のように\にASCIIコードを使用する必要があります。
  - BlueXPでは、@文字を含むパスワードはサポートされていません。

--cacertsは、コネクタとプロキシサーバ間のHTTPSアクセスに使用するCA署名証明書を指定しています。このパラメータは、HTTPSプロキシサーバを指定する場合、または代行受信プロキシを指定する場合にのみ必要です。

6. インストールが完了するまで待ちます。

   プロキシサーバを指定した場合は、インストールの終了時にConnectorサービス（occm）が2回再起動されます。

7. Connector 仮想マシンに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

8. ログイン後、コネクタを設定します。

   a. コネクタに関連付けるBlueXPアカウントを指定します。

   b. システムの名前を入力します。

   c. *では、セキュリティ保護された環境で実行していますか？*制限モードを無効にしたままにします。

      標準モードでBlueXPを使用する手順について説明しているため、制限モードは無効にしておく必要があります。セキュアな環境でBlueXPバックエンドサービスからこのアカウントを切断する場合にのみ、制限モードを有効にしてください。その場合は、 "制限モードでBlueXPの使用を開始するには、次の手順に従います"。

   d. [* Let’s start]*を選択します。

結果

これでコネクタがインストールされ、BlueXPアカウントでセットアップされました。

コネクタを作成したAzureサブスクリプションと同じAzure BLOBストレージがある場合は、BlueXPキャンバスにAzure BLOBストレージの作業環境が自動的に表示されます。 "BlueXPからAzure Blobストレージを管理する方法"

手順**5**：**BlueXP**に権限を付与する

コネクタのインストールが完了したら、以前に設定したAzure権限をBlueXPに付与する必要があります。権限を付与することで、AzureのデータとストレージインフラをBlueXPで管理できるようになります。

カスタムロール

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。

次の手順

にアクセスします "BlueXPコンソール" BlueXPでコネクタの使用を開始します

サービスプリンシパル

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

Google Cloudでのコネクタのインストールオプション

Google Cloudでコネクタを作成する方法はいくつかあります。最も一般的な方法はBlueXPから直接実行することです。

次のインストールオプションを使用できます。

- "BlueXPからコネクタを直接作成" （これは標準オプションです）

  この操作により、Linuxを実行するVMインスタンスとコネクタソフトウェアが、選択したVPCで起動されます。

- "gcloudを使用してコネクターを作成します"

  また、Linuxを実行するVMインスタンスとConnectorソフトウェアも起動しますが、導入はBlueXPではなくGoogle Cloudから直接開始されます。

- "ソフトウェアをダウンロードして、自分のLinuxホストに手動でインストールします"

選択するインストールオプションは、インストールの準備方法に影響します。これには、Google Cloudのリソースの認証と管理に必要な権限をBlueXPに付与する方法も含まれます。

BlueXPやgcloudからGoogle Cloudでコネクタを作成

BlueXPまたはgcloudを使用してGoogle Cloudでコネクタを作成するには、ネットワークを設定し、Google Cloud権限を準備し、Google Cloud APIを有効にしてから、コネクタを作成する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順**1**：ネットワークをセットアップする

コネクタがハイブリッドクラウド環境内のリソースとプロセスを管理できるように、ネットワークをセットアップします。たとえば、ターゲットネットワークへの接続が可能で、アウトバウンドのインターネットアクセスが利用可能であることを確認する必要があります。

vPCおよびサブネット

コネクタを作成するときは、コネクタを配置するVPCとサブネットを指定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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

エンドポイント	目的
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。
\ https://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。

エンドポイント	目的
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

BlueXPコンソールからアクセスするエンドポイント

SaaSレイヤで提供されるWebベースのBlueXPコンソールを使用すると、IT部門は複数のエンドポイントと通信してデータ管理タスクを実行します。これには、BlueXPコンソールからコネクタを導入するために接続されるエンドポイントも含まれます。

"BlueXPコンソールからアクセスしたエンドポイントのリストを表示します"。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

コネクタを作成した後で、このネットワーク要件を実装する必要があります。

手順**2**：コネクタを作成するための権限を設定する

BlueXPまたはgcloudを使用してコネクタを導入する前に、コネクタVMを導入するGoogle Cloudユーザの権限を設定する必要があります。

手順

1. Google Cloudでカスタムロールを作成します。

   a. 次の権限を含むYAMLファイルを作成します。

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
```

```
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Google CloudからCloud Shellをアクティブ化します。

c. 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、「connectorDeployment」という名前のロールをプロジェクトレベルで作成します。

gcloud IAMロールcreate connectorDeployment --project=myproject --file=connector-deployment.yaml

"Google Cloudのドキュメント：カスタムロールの作成と管理"

2. このカスタムロールを、BlueXPから、またはgcloudを使用してコネクタを導入するユーザに割り当てます。

"Google Cloudドキュメント：ロールを1つだけ指定します"

結果

Google Cloudユーザに、Connectorの作成に必要な権限が付与されるようになりました。

手順**3**：コネクタの権限を設定する

Google CloudでリソースをBlueXPで必要な権限を管理するためにBlueXPで必要な権限をコネクタに付与するには、Google Cloudサービスアカウントが必要です。コネクタを作成するときは、このサービスアカウントをコネクタVMに関連付

ける必要があります。

手順

1. Google Cloudでカスタムロールを作成します。

   a. の内容を含むYAMLファイルを作成します "コネクタのサービスアカウント権限"。

   b. Google CloudからCloud Shellをアクティブ化します。

   c. 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、ロールをサービスアカウントに割り当てます。

   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"

3. Cloud Volumes ONTAP システムを、Connectorが存在するプロジェクトとは異なるプロジェクトに導入する場合は、Connectorのサービスアカウントにこれらのプロジェクトへのアクセスを提供する必要があります。

   たとえば、コネクタがプロジェクト1にあり、プロジェクト2でCloud Volumes ONTAP システムを作成するとします。プロジェクト2のサービスアカウントへのアクセス権を付与する必要があります。

   a. IAMと管理サービスで、Cloud Volumes ONTAPシステムを作成するGoogle Cloudプロジェクトを選択します。

   b. [* iAM*（* IAM）]ページで、[*アクセスを許可（Grant Access）]を選択し、必要な詳細を入力します。

      - コネクタのサービスアカウントのEメールを入力します。
      - コネクタのカスタムロールを選択します。
      - [保存（ Save ）] を選択します。

   詳細については、を参照してください "Google Cloudのドキュメント"

結果

Connector VMのサービスアカウントが設定されます。

手順**4**：共有**VPC**権限を設定する

共有VPCを使用してサービスプロジェクトにリソースを導入する場合は、権限を準備する必要があります。

IAM の設定が完了したら、この表を参考にして権限の表を環境に反映させる必要があります。

共有**VPC**権限の表示

ID	作成者	でホストされています	サービスプロジェクトの権限	ホストプロジェクトの権限	目的
コネクタを展開するためのGoogleアカウント	カスタム	サービスプロジェクト	"コネクタ展開ポリシー"	compute.networkUser	サービスプロジェクトへのコネクタの配置
Connectorサービスアカウント	カスタム	サービスプロジェクト	"コネクタサービスアカウントポリシー"	compute.networkUser deploymentmanager. editor	サービスプロジェクトへの Cloud Volumes ONTAP とサービスの導入と保守
Cloud Volumes ONTAP サービスアカウント	カスタム	サービスプロジェクト	storagec.admin メンバー：BlueXPサービスアカウントをserviceAccount.userとして登録します	該当なし	（オプション）データ階層化とBlueXPのバックアップとリカバリに使用します
Google API サービスエージェント	Google Cloud	サービスプロジェクト	（デフォルト）Editor	compute.networkUser	導入に代わってGoogle Cloud APIと対話します。BlueXPが共有ネットワークを使用できるようにします
Google Compute Engineのデフォルトのサービスアカウント	Google Cloud	サービスプロジェクト	（デフォルト）Editor	compute.networkUser	導入に代わってGoogle Cloudインスタンスとコンピューティングインフラストラクチャを導入します。BlueXPが共有ネットワークを使用できるようにします

注：

1. deploymentmanager. editorは、ファイアウォール規則を配備に渡していない場合にのみホストプロジェクトで必要です。BlueXPで作成することを選択している場合にのみ必要です。ルールが指定されていない場合、ホストプロジェクトにVPC0ファイアウォールルールが含まれているデプロイメントがBlueXPによって作成されます。
2. ファイアウォールの作成とfirewall.deleteは、ファイアウォールルールを配布に渡しておらず、BlueXPで作成することを選択している場合にのみ必要です。これらの権限はBlueXPアカウント.yamlファイルにあります。共有 VPC を使用して HA ペアを導入する場合は、これらの権限を使用して VPC1 、 2 、および 3 のファイアウォールルールが作成されます。他のすべての展開では、これらの権限は VPC0 のルールの作成にも使用されます。
3. データ階層化の場合、階層化サービスアカウントは、プロジェクトレベルだけでなく、サービスアカウントに対して serviceAccount.user ロールを持つ必要があります。現在、プロジェクトレベルで serviceAccount.user を割り当てている場合、 getIAMPolicy でサービスアカウントを照会しても権限

は表示されません。

ステップ5：Google Cloud APIを有効にする

コネクタとCloud Volumes ONTAP をGoogle Cloudに導入する前に、いくつかのGoogle Cloud APIを有効にする必要があります。

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）

"Google Cloudドキュメント：APIの有効化"

手順6：コネクタを作成する

BlueXPのWebベースのコンソールから直接、またはgcloudを使用してコネクタを作成します。

このタスクについて

コネクタを作成すると、デフォルトの構成を使用してGoogle Cloudに仮想マシンインスタンスが導入されます。コネクタの作成後は、CPUやRAMが少ないVMインスタンスに変更しないでください。 "コネクタのデフォルト設定について説明します"。

BlueXP

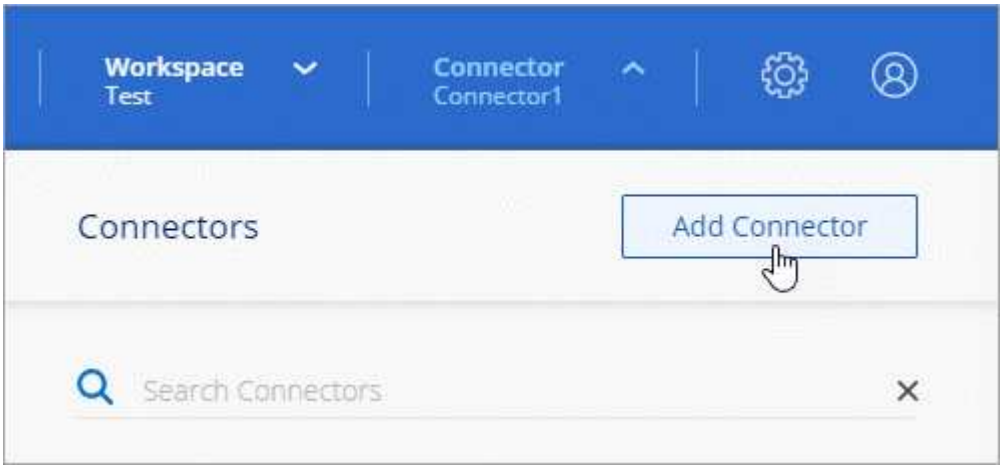
作業を開始する前に

次の情報が必要です。

- コネクタVMのコネクタとサービスアカウントを作成するために必要なGoogle Cloud権限。
- ネットワーク要件を満たすVPCとサブネット。
- コネクタからのインターネットアクセスにプロキシが必要な場合は、プロキシサーバに関する詳細。

手順

1. ドロップダウンを選択し、[コネクタの追加]*を選択します。



2. クラウドプロバイダとして * Google Cloud Platform * を選択します。
3. [*コネクターの配置（Deploying a Connector *）]ページで、必要なものについて詳しく確認してください。次の 2 つのオプションがあります。
   a. 製品内のガイドを使用して導入を準備するには、* Continue *を選択します。製品ガイドの各手順には、このページのドキュメントに記載されている情報が含まれています。
   b. このページの手順に従って準備が完了している場合は、[Skip to Deployment]*を選択します。
4. ウィザードの手順に従って、コネクタを作成します。
   - プロンプトが表示されたら、 Google アカウントにログインします。このアカウントには、仮想マシンインスタンスを作成するために必要な権限が付与されている必要があります。

     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。

   - 詳細：仮想マシンインスタンスの名前を入力し、タグを指定してプロジェクトを選択し、必要な権限を持つサービスアカウントを選択します（詳細については、上のセクションを参照してください）。
   - * 場所 * ：インスタンスのリージョン、ゾーン、 VPC 、およびサブネットを指定します。
   - * ネットワーク * ：パブリック IP アドレスを有効にするかどうかを選択し、必要に応じてプロキシ設定を指定します。
   - ファイアウォールポリシー：新しいファイアウォールポリシーを作成するか、必要なインバウンドおよびアウトバウンドルールを許可する既存のファイアウォールポリシーを選択するかを選択

します。

"Google Cloudのファイアウォールルール"

- * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

5. 「 * 追加」を選択します。

   インスタンスの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

結果

プロセスが完了すると、BlueXPからコネクタを使用できるようになります。

コネクタを作成したのと同じGoogle CloudアカウントにGoogle Cloud Storageバケットがある場合は、BlueXPキャンバスにGoogle Cloud Storageの作業環境が自動的に表示されます。 "BlueXPからGoogle Cloud Storageを管理する方法をご確認ください"

gcloud

作業を開始する前に

次の情報が必要です。

- コネクタVMのコネクタとサービスアカウントを作成するために必要なGoogle Cloud権限。
- ネットワーク要件を満たすVPCとサブネット。
- VMインスタンスの要件の理解
  - * CPU *：4コアまたは4 vCPU
  - * RAM *：14 GB
  - マシンタイプ：n2-standard-4をお勧めします。

    このコネクタは、シールドされたVM機能をサポートするOSを持つVMインスタンス上のGoogle Cloudでサポートされています。

手順

1. ご希望の方法で gcloud SDK にログインします。

   この例では、gcloud SDKがインストールされたローカルシェルを使用しますが、Google Cloudコンソールでネイティブのの Google Cloud Shellを使用できます。

   Google Cloud SDK の詳細については、を参照してください "Google Cloud SDK ドキュメントページ"。

2. 上のセクションで定義した必要な権限を持つユーザとしてログインしていることを確認します。

   ```
   gcloud auth list
   ```

   出力には次のように表示されます。ここで、 * user account はログインに使用するユーザアカウントです。

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. を実行します `gcloud compute instances create` コマンドを実行します

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

インスタンス名
: VM インスタンスに必要なインスタンス名。

プロジェクト
: （オプション） VM を導入するプロジェクト。

service-account のことです
: 手順 2 の出力で指定したサービスアカウント。

ゾーン
: VM を導入するゾーン

no-address
: （オプション）外部 IP アドレスは使用されません（パブリックインターネットにトラフィックをルーティングするには、クラウド NAT またはプロキシが必要です）。

ネットワークタグ

（オプション）タグを使用してファイアウォールルールをコネクタインスタンスにリンクするには、ネットワークタグを追加します

network-path

（オプション）コネクタを配置するネットワークの名前を追加します（共有 VPC の場合は完全パスが必要です）。

subnet-path 」を指定します

（オプション）コネクタを導入するサブネットの名前を追加します（共有 VPC の場合は完全パスが必要です）。

kms -key-path

（オプション） KMS キーを追加してコネクタのディスクを暗号化する（ IAM 権限も適用する必要があります）

これらの旗についてのより多くの情報のために、訪問しなさい "Google Cloud Compute SDK ドキュメント"。

+
コマンドを実行すると、ネットアップのゴールデンイメージを使用してコネクタが導入されます。コネクタインスタンスとソフトウェアは、約 5 分後に実行される必要があります。

1. コネクタインスタンスに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

2. ログイン後、コネクタを設定します。

   a. コネクタに関連付けるBlueXPアカウントを指定します。

      "BlueXPアカウントの詳細をご確認ください"。

   b. システムの名前を入力します。

結果

これで、コネクタのインストールとBlueXPアカウントでのセットアップが完了しました。

Webブラウザを開き、にアクセスします "BlueXPコンソール" BlueXPでコネクタの使用を開始します

Google Cloudにコネクタを手動でインストールする

独自のLinuxホストにコネクタを手動でインストールするには、ホストの要件を確認し、ネットワークをセットアップし、Google Cloudの権限を準備し、Google Cloud APIを有効にしてから、コネクタをインストールし、準備した権限を指定する必要があります。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順**1**：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

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**2**：ネットワークをセットアップする

コネクタがハイブリッドクラウド環境内のリソースとプロセスを管理できるように、ネットワークをセットアップします。たとえば、ターゲットネットワークへの接続が可能で、アウトバウンドのインターネットアクセスが利用可能であ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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

手動インストール中にエンドポイントに接続しました

独自のLinuxホストにコネクタを手動でインストールする場合、コネクタのインストーラは、インストールプロセス中に次のURLにアクセスする必要があります。

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

エンドポイント	目的
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。
\ https://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。

- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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"

手順**3**：コネクタの権限を設定する

Google Cloudでリソースを管理するためにBlueXPで必要な権限をコネクタに付与するには、Google Cloudサービスアカウントが必要です。コネクタを作成するときは、このサービスアカウントをコネクタVMに関連付ける必要があります。

手順

1. Google Cloudでカスタムロールを作成します。

   a. の内容を含むYAMLファイルを作成します "コネクタのサービスアカウント権限"。

   b. Google CloudからCloud Shellをアクティブ化します。

   c. 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、ロールをサービスアカウントに割り当てます。

   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"

3. Cloud Volumes ONTAP システムを、Connectorが存在するプロジェクトとは異なるプロジェクトに導入する場合は、Connectorのサービスアカウントにこれらのプロジェクトへのアクセスを提供する必要があります。

   たとえば、コネクタがプロジェクト1にあり、プロジェクト2でCloud Volumes ONTAP システムを作成するとします。プロジェクト2のサービスアカウントへのアクセス権を付与する必要があります。

a. IAMと管理サービスで、Cloud Volumes ONTAPシステムを作成するGoogle Cloudプロジェクトを選択します。

b. [* iAM*（* IAM）]ページで、[*アクセスを許可（Grant Access）]を選択し、必要な詳細を入力します。

   - コネクタのサービスアカウントのEメールを入力します。
   - コネクタのカスタムロールを選択します。
   - [保存（ Save ）] を選択します。

詳細については、を参照してください "Google Cloudのドキュメント"

結果

Connector VMのサービスアカウントが設定されます。

手順**4**：共有**VPC**権限を設定する

共有VPCを使用してサービスプロジェクトにリソースを導入する場合は、権限を準備する必要があります。

IAM の設定が完了したら、この表を参考にして権限の表を環境に反映させる必要があります。

共有**VPC**権限の表示

ID	作成者	でホストされています	サービスプロジェクトの権限	ホストプロジェクトの権限	目的
コネクタを展開するためのGoogleアカウント	カスタム	サービスプロジェクト	"コネクタ展開ポリシー"	compute.networkUser	サービスプロジェクトへのコネクタの配置
Connectorサービスアカウント	カスタム	サービスプロジェクト	"コネクタサービスアカウントポリシー"	compute.networkUser deploymentmanager. editor	サービスプロジェクトへの Cloud Volumes ONTAP とサービスの導入と保守
Cloud Volumes ONTAP サービスアカウント	カスタム	サービスプロジェクト	storagec.admin メンバー：BlueXPサービスアカウントをserviceAccount.userとして登録します	該当なし	（オプション）データ階層化とBlueXPのバックアップとリカバリに使用します
Google API サービスエージェント	Google Cloud	サービスプロジェクト	（デフォルト）Editor	compute.networkUser	導入に代わってGoogle Cloud APIと対話します。BlueXPが共有ネットワークを使用できるようにします
Google Compute Engineのデフォルトのサービスアカウント	Google Cloud	サービスプロジェクト	（デフォルト）Editor	compute.networkUser	導入に代わってGoogle Cloudインスタンスとコンピューティングインフラストラクチャを導入します。BlueXPが共有ネットワークを使用できるようにします

注：

1. deploymentmanager. editorは、ファイアウォール規則を配備に渡していない場合にのみホストプロジェクトで必要です。BlueXPで作成することを選択している場合にのみ必要です。ルールが指定されていない場合、ホストプロジェクトにVPC0ファイアウォールルールが含まれているデプロイメントがBlueXPによって作成されます。
2. ファイアウォールの作成とfirewall.deleteは、ファイアウォールルールを配布に渡しておらず、BlueXPで作成することを選択している場合にのみ必要です。これらの権限はBlueXPアカウント.yamlファイルにあります。共有 VPC を使用して HA ペアを導入する場合は、これらの権限を使用して VPC1 、 2 、および 3 のファイアウォールルールが作成されます。他のすべての展開では、これらの権限は VPC0 のルールの作成にも使用されます。
3. データ階層化の場合、階層化サービスアカウントは、プロジェクトレベルだけでなく、サービスアカウントに対して serviceAccount.user ロールを持つ必要があります。現在、プロジェクトレベルで serviceAccount.user を割り当てている場合、 getIAMPolicy でサービスアカウントを照会しても権限

は表示されません。

ステップ5：Google Cloud APIを有効にする

Cloud Volumes ONTAPシステムをGoogle Cloudに導入する前に、いくつかのGoogle Cloud APIを有効にする必要があります。

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）

"Google Cloudドキュメント：APIの有効化"

手順6：コネクタを取り付ける

前提条件が完了したら、ソフトウェアを自分のLinuxホストに手動でインストールできます。

作業を開始する前に

次の情報が必要です。

- コネクタをインストールするためのroot権限。
- コネクタからのインターネットアクセスにプロキシが必要な場合は、プロキシサーバに関する詳細。

  インストール後にプロキシサーバを設定することもできますが、その場合はコネクタを再起動する必要があります。

  BlueXPでは透過型プロキシサーバはサポートされません。

- プロキシサーバがHTTPSを使用している場合、またはプロキシが代行受信プロキシの場合は、CA署名証明書。

このタスクについて

NetApp Support Siteで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後、新しいバージョンが利用可能になると、コネクタは自動的に更新されます。

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. ホストに_http_proxy_or_https_proxy_system変数が設定されている場合は、削除します。

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

3. からConnectorソフトウェアをダウンロードします "NetApp Support Site"をクリックし、 Linux ホストにコピーします。

ネットワークまたはクラウドで使用するための「オンライン」コネクタインストーラをダウンロードする必要があります。コネクタには別の「オフライン」インストーラが用意されていますが、プライベートモード展開でのみサポートされています。

4. スクリプトを実行する権限を割り当てます。

```
chmod +x BlueXP-Connector-Cloud-<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。

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

--proxyパラメータと—cacert.pemパラメータはオプションです。プロキシサーバを使用している場合は、次のようにパラメータを入力する必要があります。プロキシに関する情報の入力を求めるプロンプトは表示されません。

次に、両方のオプションパラメータを使用したコマンドの例を示します。

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxyは、次のいずれかの形式を使用してHTTPまたはHTTPSプロキシサーバを使用するようにコネクタを設定します。

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port

- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  次の点に注意してください。

  - ユーザには、ローカルユーザまたはドメインユーザを指定できます。
  - ドメインユーザの場合は、上記のように\にASCIIコードを使用する必要があります。
  - BlueXPでは、@文字を含むパスワードはサポートされていません。

--cacertsは、コネクタとプロキシサーバ間のHTTPSアクセスに使用するCA署名証明書を指定しています。このパラメータは、HTTPSプロキシサーバを指定する場合、または代行受信プロキシを指定する場合にのみ必要です。

6. インストールが完了するまで待ちます。

   プロキシサーバを指定した場合は、インストールの終了時にConnectorサービス（occm）が2回再起動されます。

7. Connector 仮想マシンに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

8. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるBlueXPアカウントを指定します。
   b. システムの名前を入力します。
   c. *では、セキュリティ保護された環境で実行していますか？*制限モードを無効にしたままにします。

      標準モードでBlueXPを使用する手順について説明しているため、制限モードは無効にしておく必要があります。セキュアな環境でBlueXPバックエンドサービスからこのアカウントを切断する場合にのみ、制限モードを有効にしてください。その場合は、 "制限モードでBlueXPの使用を開始するには、次の手順に従います"。

   d. [* Let’s start]*を選択します。

結果

これでコネクタがインストールされ、BlueXPアカウントでセットアップされました。

コネクタを作成したのと同じGoogle CloudアカウントにGoogle Cloud Storageバケットがある場合は、BlueXPキャンバスにGoogle Cloud Storageの作業環境が自動的に表示されます。 "BlueXPからGoogle Cloud Storageを管理する方法をご確認ください"

手順**7**：**BlueXP**に権限を付与する

以前に設定したGoogle Cloud権限をBlueXPに付与する必要があります。権限を付与することで、BlueXPでGoogle Cloudのデータとストレージインフラを管理できるようになります。

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Google Cloud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。

コネクタをオンプレミスにインストールしてセットアップします

コネクタをオンプレミスにインストールし、ログインしてBlueXPアカウントと連携するように設定します。

作業を開始する前に

確認が必要です "コネクタの制限"。

手順1：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。コネクタを取り付ける前に、ホストがこれらの要件を満たしていることを確認してください。

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

/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**2**：ネットワークをセットアップする

コネクタがハイブリッドクラウド環境内のリソースとプロセスを管理できるように、ネットワークをセットアップします。たとえば、ターゲットネットワークへの接続が可能で、アウトバウンドのインターネットアクセスが利用可能であ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、作業環境を作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムやストレージシステムを作成するネットワークなどです。

アウトバウンドインターネットアクセス

コネクタを展開するネットワークの場所には、特定のエンドポイントに接続するためのアウトバウンドインターネット接続が必要です。

手動インストール中にエンドポイントに接続しました

独自のLinuxホストにコネクタを手動でインストールする場合、コネクタのインストーラは、インストールプロセス中に次のURLにアクセスする必要があります。

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

コネクタから接続されたエンドポイント

このコネクタは、パブリッククラウド環境内のリソースとプロセスを日常的に管理するために、次のエンドポイントに接続するためのアウトバウンドインターネットアクセスを必要とします。

次に示すエンドポイントはすべてCNAMEエントリであることに注意してください。

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"
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.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。
\ https://support.netapp.com https://mysupport.netapp.com をご覧ください	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。

エンドポイント	目的
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXPでSaaSの機能とサービスを提供するため。 コネクタは現在「cloudmanager.cloud.netapp.com"」に連絡していますが、今後のリリースでは「api.bluexp.netapp.com"」に連絡を開始します。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

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。

ポート

コネクタを起動するか、コネクタがCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用されている場合を除き、コネクタへの受信トラフィックはありません。

- HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。
- 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。
- アウトバウンドインターネット接続を使用できないサブネットにCloud Volumes ONTAP システムを導入する場合は、ポート3128経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムでAutoSupportメッセージを送信するためのアウトバウンドインターネット接続が確立されていない場合は、コネクタに付属のプロキシサーバを使用するように自動的に設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128を介したインバウンド接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

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3：クラウドの権限を設定する

AWSまたはAzureでBlueXPサービスをオンプレミスコネクタで使用する場合は、インストール後にコネクタにクレデンシャルを追加できるように、クラウドプロバイダで権限を設定する必要があります。

> Google Cloudではない理由コネクタがオンプレミスにインストールされている場合、Google Cloudでリソースを管理することはできません。Google Cloudに存在するすべてのリソースを管理するには、コネクタをGoogle Cloudにインストールする必要があります。

AWS

コネクタをオンプレミスにインストールする場合は、必要な権限を持つIAMユーザのアクセスキーを追加して、BlueXPにAWS権限を設定する必要があります。

コネクタがオンプレミスにインストールされている場合は、この認証方法を使用する必要があります。IAMロールは使用できません。

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、必要な権限を持つIAMユーザのアクセスキーが作成されました。コネクタをインストールしたら、これらのクレデンシャルをBlueXPのコネクタに関連付ける必要があります。

Azure

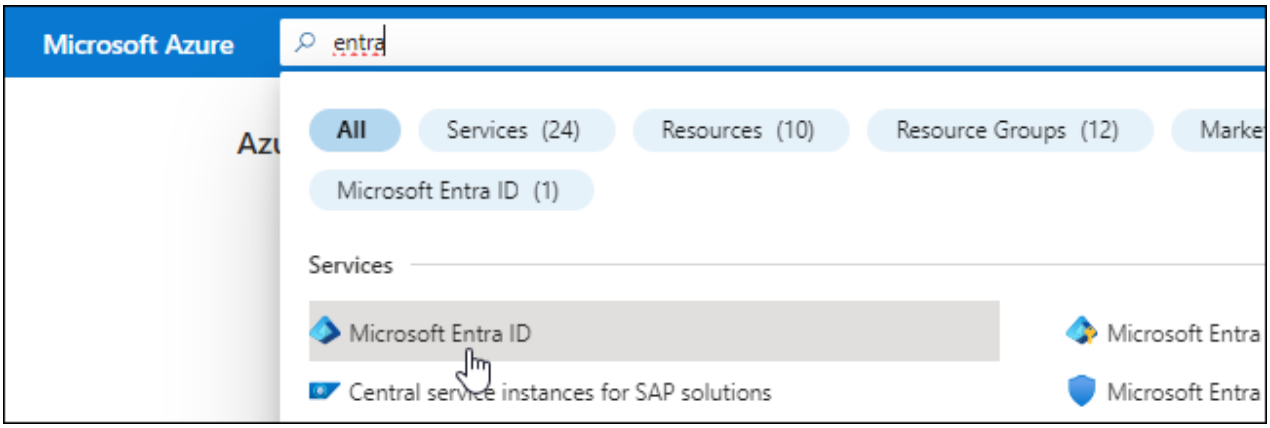
コネクタをオンプレミスにインストールする場合は、Microsoft Entra IDでサービスプリンシパルを設定し、BlueXPに必要なAzureクレデンシャルを取得して、BlueXPにAzure権限を付与する必要があります。

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。

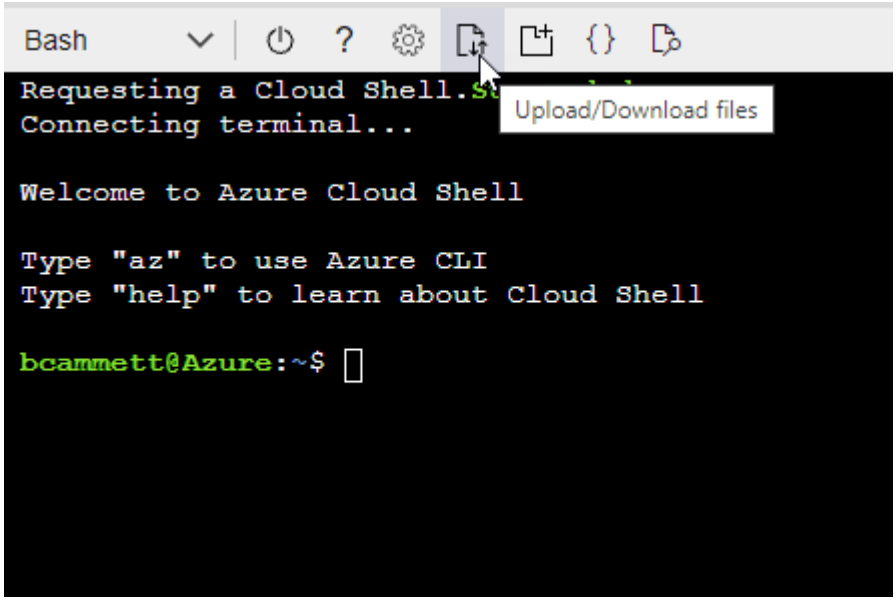
      - 例 *

```
"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。

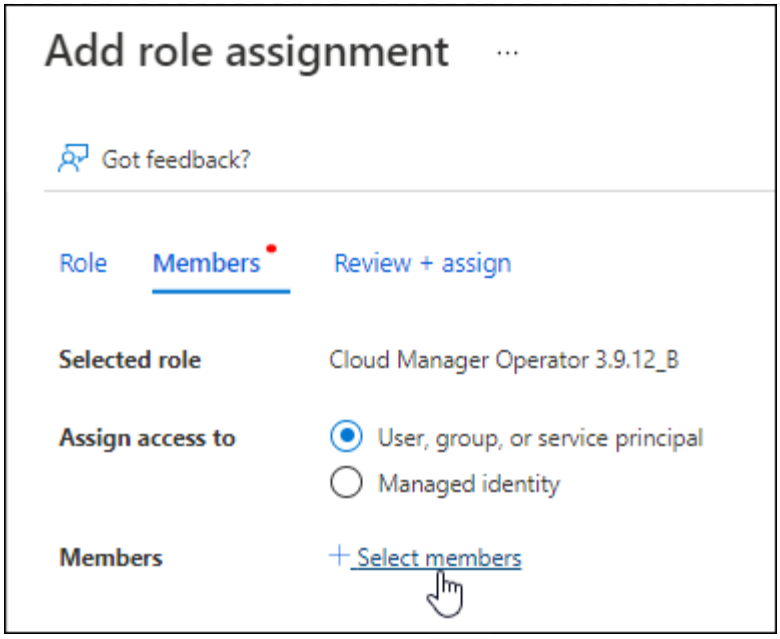
```
az role definition create --role-definition
Connector_Policy.json
```

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。

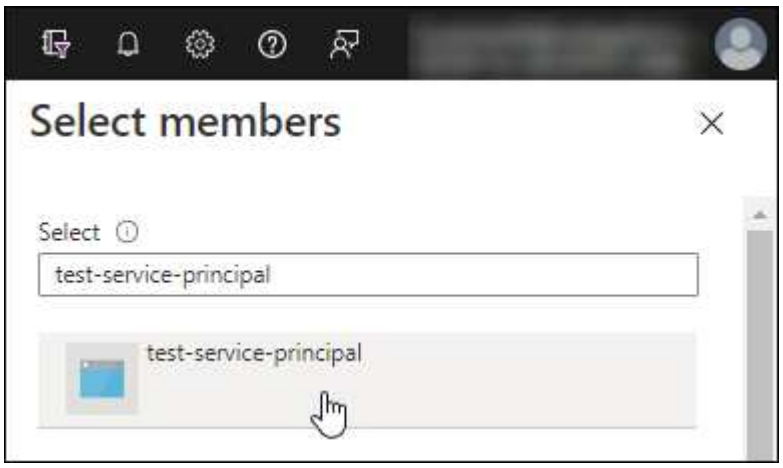
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。

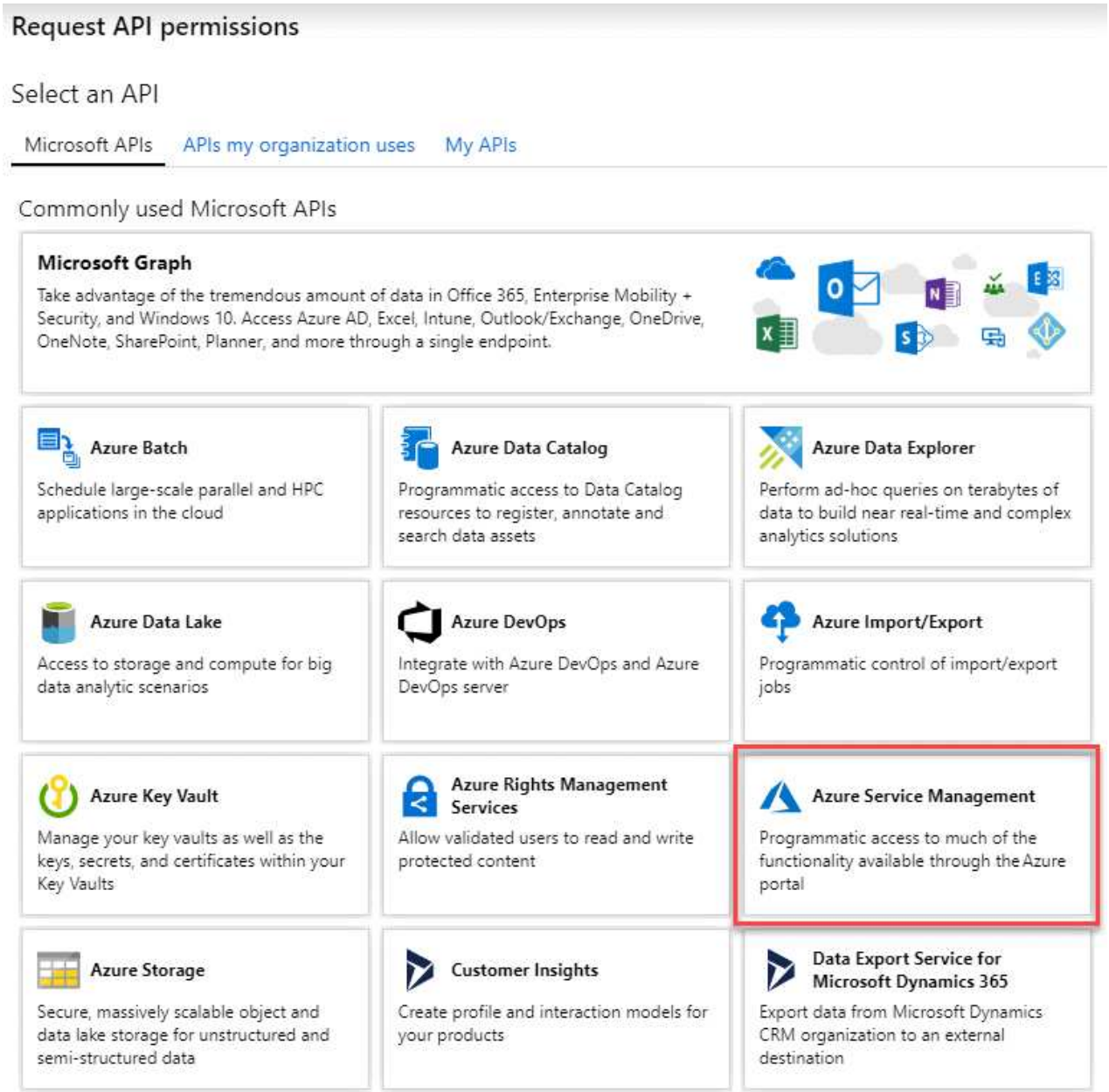
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

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。

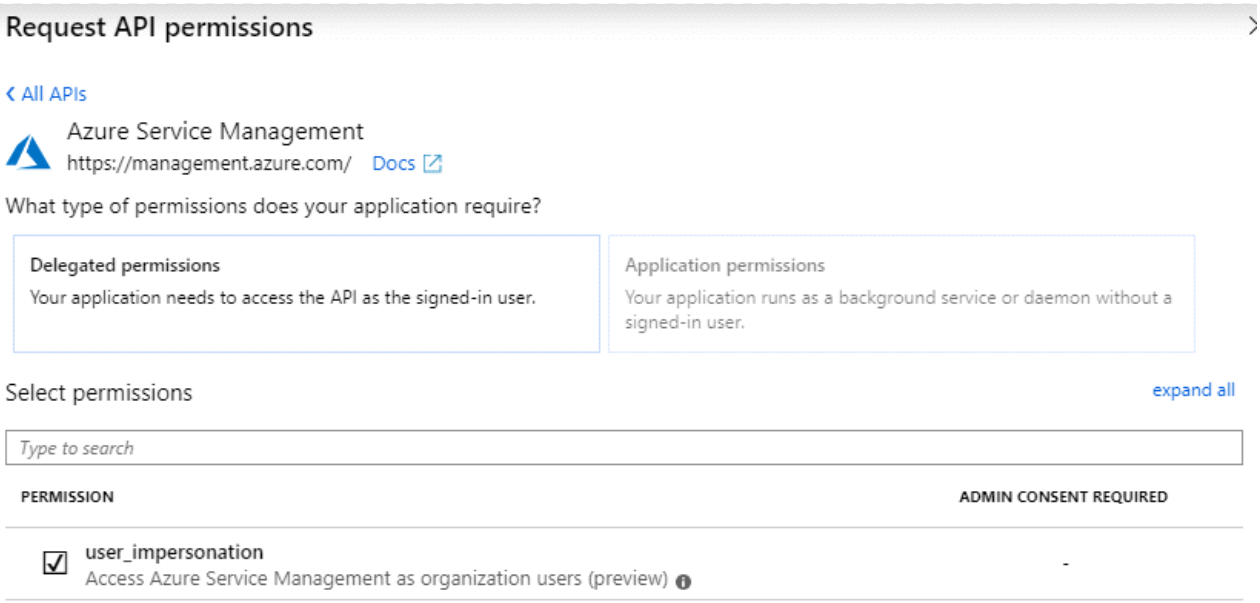
Windows Azure Service Management API 権限を追加します

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。

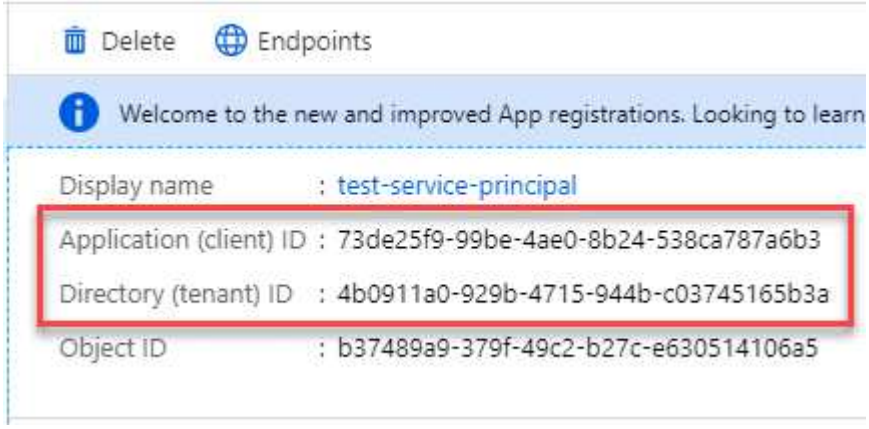


4. を選択し、[Add permissions]*を選択します。



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。コネクタをインストールしたら、これらのクレデンシャルをBlueXPのコネクタに関連付ける必要があります。

手順4：コネクタを取り付ける

コネクタソフトウェアをオンプレミスの既存のLinuxホストにダウンロードしてインストールします。

作業を開始する前に

次の情報が必要です。

- コネクタをインストールするためのroot権限。
- コネクタからのインターネットアクセスにプロキシが必要な場合は、プロキシサーバに関する詳細。

  インストール後にプロキシサーバを設定することもできますが、その場合はコネクタを再起動する必要があります。

  BlueXPでは透過型プロキシサーバはサポートされません。

- プロキシサーバがHTTPSを使用している場合、またはプロキシが代行受信プロキシの場合は、CA署名証明書。

このタスクについて

NetApp Support Siteで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後、新しいバージョンが利用可能になると、コネクタは自動的に更新されます。

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. ホストに_http_proxy_or_https_proxy_system変数が設定されている場合は、削除します。

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

3. からConnectorソフトウェアをダウンロードします "NetApp Support Site"をクリックし、 Linux ホストにコピーします。

   ネットワークまたはクラウドで使用するための「オンライン」コネクタインストーラをダウンロードする必要があります。コネクタには別の「オフライン」インストーラが用意されていますが、プライベートモード展開でのみサポートされています。

4. スクリプトを実行する権限を割り当てます。

```
chmod +x BlueXP-Connector-Cloud-<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。

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

   --proxyパラメータと—cacert.pemパラメータはオプションです。プロキシサーバを使用している場合は、次のようにパラメータを入力する必要があります。プロキシに関する情報の入力を求めるプロンプトは表示されません。

   次に、両方のオプションパラメータを使用したコマンドの例を示します。

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --proxyは、次のいずれかの形式を使用してHTTPまたはHTTPSプロキシサーバを使用するようにコネクタを設定します。

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     次の点に注意してください。

- ユーザには、ローカルユーザまたはドメインユーザを指定できます。
- ドメインユーザの場合は、上記のように\にASCIIコードを使用する必要があります。
- BlueXPでは、@文字を含むパスワードはサポートされていません。

--cacertsは、コネクタとプロキシサーバ間のHTTPSアクセスに使用するCA署名証明書を指定しています。このパラメータは、HTTPSプロキシサーバを指定する場合、または代行受信プロキシを指定する場合にのみ必要です。

結果

これでコネクタがインストールされました。プロキシサーバを指定した場合は、インストールの終了時にConnectorサービス（occm）が2回再起動されます。

手順5：コネクタを設定する

サインアップまたはログインして、BlueXPアカウントと連携するようにConnectorを設定します。

手順

1. Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

   _ipaddress _ には、ホストの設定に応じて、 localhost 、プライベート IP アドレス、またはパブリック IP アドレスを指定できます。たとえば、パブリック IP アドレスのないパブリッククラウドにコネクタがある場合は、コネクタホストに接続されているホストからプライベート IP アドレスを入力する必要があります。

2. サインアップまたはログインします。
3. ログインしたら、BlueXPをセットアップします。
   a. コネクタに関連付けるBlueXPアカウントを指定します。
   b. システムの名前を入力します。
   c. *では、セキュリティ保護された環境で実行していますか？*制限モードを無効にしたままにします。

      標準モードでBlueXPを使用する手順について説明しているため、制限モードは無効にしておく必要があります。(また、コネクタがオンプレミスにインストールされている場合、制限モードはサポートされません)。

   d. [* Let’s start]*を選択します。

結果

これで、先ほどインストールしたコネクタでBlueXPがセットアップされました。

手順6：BlueXPに権限を付与する

コネクタのインストールとセットアップが完了したら、クラウドクレデンシャルを追加して、AWSまたはAzureで操作を実行するために必要な権限をBlueXPに付与します。

AWS

作業を開始する前に

AWSでクレデンシャルを作成したばかりの場合は、クレデンシャルが使用可能になるまでに数分かかることがあります。数分待ってから、BlueXPに資格情報を追加します。

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。

これで、に移動できます "BlueXPコンソール" BlueXPでコネクタの使用を開始します

Azure

作業を開始する前に

これらのクレデンシャルをAzureで作成したばかりの場合は、クレデンシャルが使用可能になるまでに数分かかることがあります。数分待ってから、BlueXPに資格情報を追加します。

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。これで、に移動できます "BlueXPコンソール" BlueXPでコネクタの使用を開始します