BlueXPのセットアップと管理に関するドキュメント

Setup and administration

NetApp
April 26, 2024

目次

BlueXPのセットアップと管理に関するドキュメント

リリースノート

新機能

BlueXPの管理機能の新機能（BlueXPアカウント、コネクタ、クラウドプロバイダのクレデンシャルなど）をご確認ください。

2024年4月22日

コネクタ3.9.39

今回のリリースのBlueXP Connectorには、セキュリティが若干改善され、バグが修正されています。

現時点では、3.9.39リリースは標準モードと制限モードで使用できます。

コネクタを作成するためのAWS権限

BlueXPからAWSでコネクタを作成するには、さらに2つの権限が必要になりました。

```
"ec2:DescribeLaunchTemplates",
"ec2:CreateLaunchTemplate",
```

これらの権限は、コネクタのEC2インスタンスでIMDSv2を有効にするために必要です。

これらの権限は、コネクタの作成時にBlueXPユーザインターフェイスに表示されるポリシーと、ドキュメントで提供されているポリシーに含まれています。

> 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。コネクタインスタンスに割り当てられるポリシーとは異なります。

"AWSからコネクタを作成するためのAWS権限を設定する方法"。

2024年4月11日

Docker Engineの更新

Docker Engineの要件を更新して、コネクタでサポートされる最大バージョン（25.0.5）を指定しました。サポートされる最小バージョンは引き続き19.3.1です。

"コネクタホスト要件の表示"。

2024年3月26日

プライベートモードリリース（3.9.38）

BlueXPで新しいプライベートモードリリースが見積もり可能になりました。このリリースには、プライベー

トモードでサポートされる次のバージョンのBlueXPサービスが含まれています。

サービス	含まれるバージョン
コネクタ	3.9.38
バックアップとリカバリ	2024年3月12日
分類	2024年3月4日
Cloud Volumes ONTAP管理	2024年3月8日
デジタルウォレット	2023年7月30日
オンプレミスのONTAPクラスタ管理	2023年7月30日
レプリケーション	2022年9月18日

この新しいリリースは、NetApp Support Siteからダウンロードできます。

- "プライベートモードの詳細"
- "BlueXPのプライベートモードでの利用を開始する方法"
- "プライベートモードの使用時にコネクタをアップグレードする方法について説明します。"

2024年3月8日

コネクタ3.9.38

現時点では、3.9.38リリースは標準モードと制限モードで使用できます。このリリースでは、AWSでのIMDSv2とAWS権限の更新がサポートされます。

IMDSv2のサポート

BlueXPで、コネクタインスタンスとCloud Volumes ONTAPインスタンスでAmazon EC2インスタンスメタデータサービスバージョン2（IMDSv2）がサポートされるようになりました。IMDSv2では、脆弱性に対する保護が強化されています。以前はIMDSv1のみがサポートされていました。

"AWSセキュリティブログでIMDSv2の詳細を確認する"

インスタンスメタデータサービス（IMDS）は、EC2インスタンスで次のように有効になります。

- BlueXPから新規コネクタを導入する場合、または "Terraformスクリプト"IMDSv2はEC2インスタンスでデフォルトで有効になっています。
- AWSで新しいEC2インスタンスを起動し、コネクタソフトウェアを手動でインストールすると、IMDSv2もデフォルトで有効になります。
- AWS Marketplaceからコネクタを起動すると、IMDSv1がデフォルトで有効になります。EC2インスタンスにIMDSv2を手動で設定できます。
- 既存のコネクタについては、IMDSv1は引き続きサポートされますが、必要に応じて、EC2インスタンスでIMDSv2を手動で設定できます。
- Cloud Volumes ONTAPでは、新規および既存のインスタンスでIMDSv1がデフォルトで有効になっています。必要に応じて、EC2インスタンスでIMDSv2を手動で設定できます。

"既存のインスタンスでIMDSv2を設定する方法"。

AWS権限の更新

AWSのコネクタポリシーを更新して、「EC2：DescriptionAvailabilityZones」権限を追加しました。この権限は、今後のリリースで必要になります。リリースノートの詳細については、リリースノートを更新します。

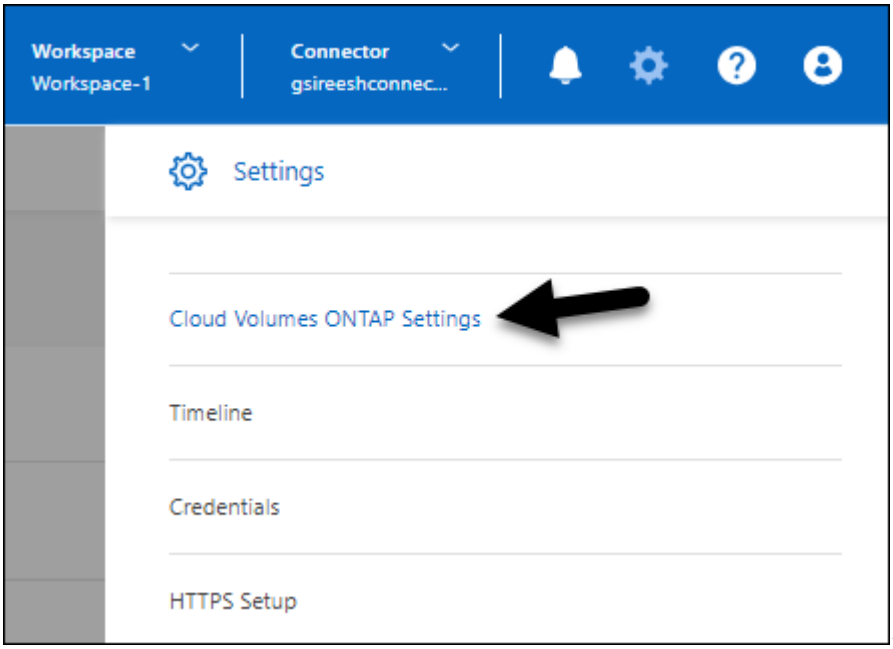
"コネクタのAWS権限を表示する"。

プロキシ設定と**Cloud Volumes ONTAP**設定

コネクターのプロキシサーバー設定は、*コネクターの管理*ページ（標準モード）または*コネクターの編集*ページ（制限モードおよびプライベートモード）から利用できるようになりました。

"プロキシサーバを使用するようにコネクタを設定する方法について説明します。"。

また、コネクター設定*ページの名前を Cloud Volumes ONTAP設定*に変更しました。



メニューから使用できるCloud Volumes ONTAP Settings]オプションを示すスクリーンショット。"]

2024年2月15日

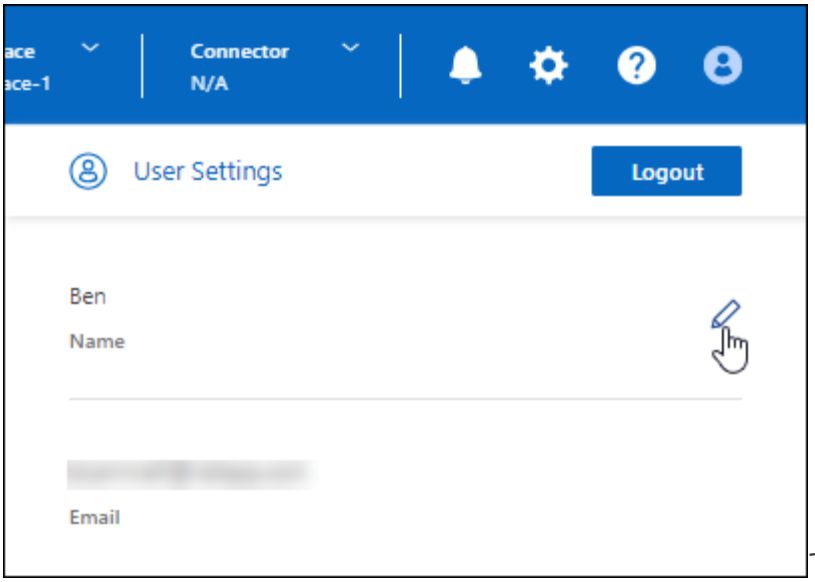
コネクタ**3.9.37**

今回のリリースのBlueXP Connectorには、セキュリティが若干改善され、バグが修正されています。

現時点では、3.9.37リリースは標準モードと制限モードで使用できます。

名前の編集

NetAppのクラウドクレデンシャルを使用してBlueXPにログインすると、*[ユーザ設定]*で名前を編集できるようになりました。



で名前を編集する機能を示すスクリーンショット。"]

フェデレーテッド接続またはNetApp Support Siteアカウントでログインした場合、名前の編集はサポートされません。

2024年1月11日

コネクタ3.9.36

このリリースには、以下のクラウドリージョンでマイナーな改善、バグ修正、コネクタのサポートが含まれています。

- AWSのイスラエル（テルアビブ）リージョン
- Google Cloudのサウジアラビアリージョン

2023年12月5日

プライベートモードリリース（3.9.35）

BlueXPで新しいプライベートモードリリースが見積もり可能になりました。このリリースには、コネクタのバージョン3.9.35と、2023年10月時点でプライベートモードでサポートされるBlueXPサービスのバージョンが含まれています。

この新しいリリースは、NetApp Support Siteからダウンロードできます。

- "プライベートモードに含まれるBlueXPサービスの詳細"
- "BlueXPのプライベートモードでの利用を開始する方法"
- "プライベートモードの使用時にコネクタをアップグレードする方法について説明します。"

2023年11月8日

コネクタ3.9.35

このリリースには、セキュリティのマイナーな改善とバグの修正が含まれています。

2023年10月6日

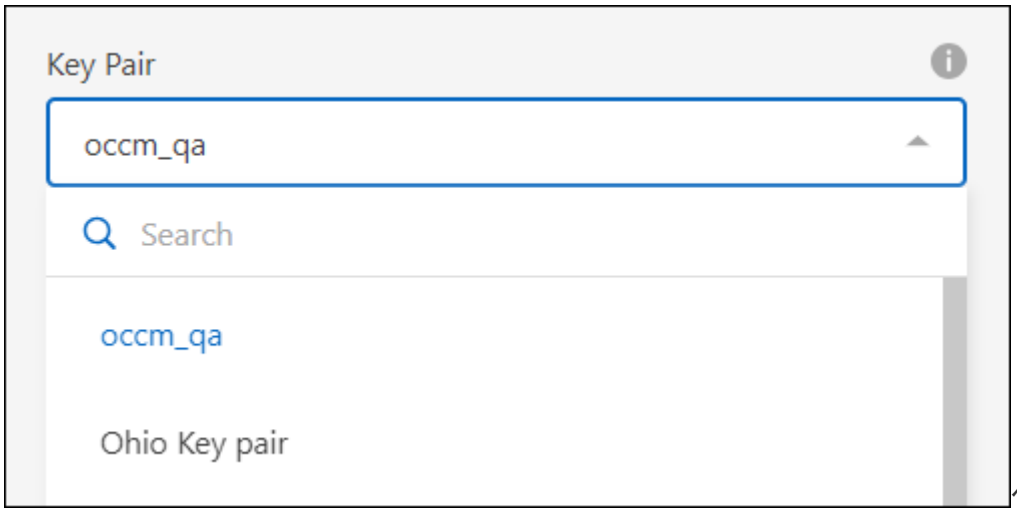
コネクタ3.9.34

このリリースには、マイナーな改善とバグ修正が含まれています。

2023年9月10日

コネクタ3.9.33

- BlueXPからAWSでコネクタを作成するときに、[Key Pair]フィールド内を検索して、コネクタインスタンスで使用するキーペアを簡単に見つけることができるようになりました。



ページに表示される[Key Pair]フィールドの検索オプションのスクリーンショット。"]

- このアップデートにはバグ修正も含まれています。

2023年7月30日

コネクタ3.9.32

- BlueXP監査サービスAPIを使用して監査ログをエクスポートできるようになりました。

  監査サービスには、BlueXPサービスで実行された処理に関する情報が記録されます。これには、ワークスペース、使用されているコネクタ、およびその他のテレメトリデータが含まれます。このデータを使用して、実行されたアクション、実行者、実行日時を確認できます。

  "監査サービスAPIの使用に関する詳細情報"

  このリンクには、BlueXPのユーザインターフェイスの[Timeline]ページからもアクセスできます。

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張とオンプレミスONTAP クラスタの機能拡張も含まれています。

- "Cloud Volumes ONTAP の機能拡張について説明します"
- "ONTAP オンプレミスクラスタの機能拡張について説明します"

2023年7月2日

コネクタ3.9.31

- [My estate]タブ（以前の[My Opportunities]）でオンプレミスのONTAPクラスタを検出できるようになりました。

  "クラスタを検出する方法については、[My estateページを参照してください"]。

- Azure Governmentリージョンでコネクタを使用している場合は、コネクタが次のエンドポイントに接続できることを確認する必要があります。

  https://occmclientinfragov.azurecr.us

  このエンドポイントは、コネクタを手動でインストールし、コネクタとそのDockerコンポーネントをアップグレードするために必要です。

  この変更により、Azure Governmentリージョン内のコネクタは、次のエンドポイントに接続しなくなりました。

  https://cloudmanagerinfraprod.azurecr.io

  このエンドポイントは、他のすべての制限モード設定および標準モードでは引き続き必要であることに注意してください。

2023年6月4日

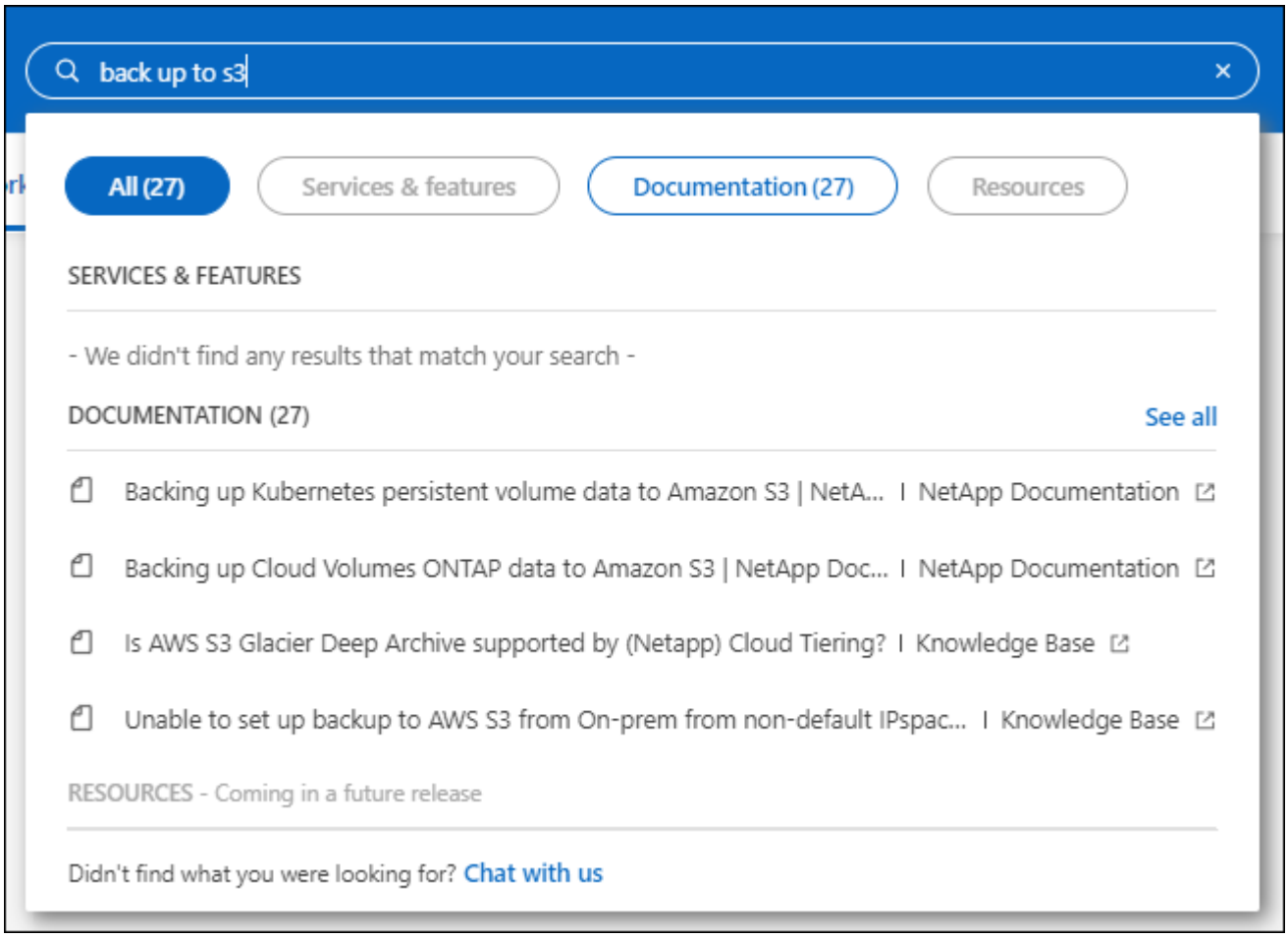
コネクタ3.9.30

- サポートダッシュボードからNetAppサポートケースをオープンすると、BlueXPログインに関連付けられたNetApp Support Siteアカウントを使用してケースがオープンされるようになりました。以前は、BlueXPアカウント全体に関連付けられたNetApp Support Siteアカウントを使用していました。

  この変更に伴い、BlueXPアカウントのサポート登録は、ユーザのBlueXPログインに関連付けられたNetApp Support Siteアカウントを使用して行われるようになりました。これまで、サポートの登録には、BlueXPアカウント全体に関連付けられたNSSアカウントを使用していました。そのため、BlueXPへのログインにNetApp Support Siteアカウントが関連付けられていない場合、他のBlueXPユーザには同じサポート登録ステータスが表示されません。以前にBlueXPアカウントをサポートに登録していても、登録ステータスは引き続き有効です。ステータスを確認するには、ユーザレベルのNSSアカウントを追加するだけです。

  - "NetAppサポートでケースを作成する方法について説明します"
  - "BlueXPログインに関連付けられているクレデンシャルの管理方法について説明します"
  - "サポートに登録する方法について説明します"

- BlueXPからドキュメントを検索できるようになりました。検索結果に、docs.netapp.comおよびkb.netapp.comのコンテンツへのリンクが表示されるようになりました。これは、質問を回答に送信するのに役立つ可能性があります。



- コネクタを使用して、BlueXPからAzureストレージアカウントを追加および管理できるようになりました。

  "BlueXPからAzureサブスクリプションに新しいAzureストレージアカウントを追加する方法をご確認ください"。

- このコネクタが次のAWSリージョンでサポートされるようになりました。
  - ハイデラバード（AP-south-2）
  - メルボルン（AP南東-4）
  - スペイン（EU-south-2）
  - アラブ首長国連邦（ME-CENTRAL-1）
  - チューリッヒ（EU-CENTRAL-2）
- このコネクタは、次のAzureリージョンでサポートされるようになりました。
  - ブラジル南部
  - フランス南部
  - インド中部出身
  - 西インド諸島出身
  - ポーランド中部

- カタール中部

- Connectorは、次のGoogle Cloudリージョンでサポートされるようになりました。
  - コロンバス（us-east5）
  - ダラス（US -サウス1）

  "サポートされているリージョンの完全なリストを表示します"

2023年5月7日

コネクタ**3.9.29**

- Ubuntu 22.04は、BlueXPまたはクラウドプロバイダのマーケットプレイスからコネクタを導入する際のコネクタ用の新しいオペレーティングシステムです。

  また、Ubuntu 22.04を実行している独自のLinuxホストにコネクタを手動でインストールすることもできます。

- Red Hat Enterprise Linux 8.6および8.7は、新しいコネクタの導入ではサポートされなくなりました。

  Red Hatではコネクタに必要なDockerがサポートされなくなるため、新しい環境ではこれらのバージョンはサポートされません。RHEL 8.6または8.7で既存のコネクタを実行している場合、ネットアップは引き続きこの構成をサポートします。

  Red Hat 7.6、7.7、7.8、および7.9は、新規および既存のコネクタで引き続きサポートされます。

- コネクタは現在、Google Cloudのカタール地域でサポートされています。
- このコネクタは、Microsoft AzureのSweden Centralリージョンでもサポートされています。

  "サポートされているリージョンの完全なリストを表示します"

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張が含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

2023年4月4日

展開モード

BlueXP_deployment modes_を使用すると、ビジネス要件やセキュリティ要件に合わせてBlueXPを使用できます。次の3つのモードから選択できます。

- 標準モード
- 制限モード
- プライベートモード

"これらの展開モードの詳細については、こちらをご覧ください"。

制限モードが導入されたことで、SaaSプラットフォームを有効または無効にするオプションが廃止されました。制限モードはアカウント作成時に有効にすることができます。後で有効または無効にすることはできません。

2023年4月3日

コネクタ3.9.28

- Eメール通知がBlueXPデジタルウォレットでサポートされるようになりました。

  通知を設定すると、BYOLライセンスの有効期限が近づいたとき（「警告」通知）、またはすでに有効期限が切れているとき（「エラー」通知）にEメール通知を受け取ることができます。

  "Eメール通知の設定方法については、こちらをご覧ください"。

- Google Cloud Turinリージョンでコネクタがサポートされるようになりました。

  "サポートされているリージョンの完全なリストを表示します"

- BlueXPログインに関連付けられたユーザクレデンシャル（ONTAP クレデンシャルとNetApp Support Site（NSS）クレデンシャル）を管理できるようになりました。

  [設定]>[クレデンシャル]*に移動すると、クレデンシャルを表示したり、更新したり、削除したりできます。たとえば、これらのクレデンシャルのパスワードを変更した場合は、BlueXPでパスワードを更新する必要があります。

  "ユーザクレデンシャルの管理方法について説明します"。

- サポートケースを作成するとき、または既存のサポートケースのケースノートを更新するときに、添付ファイルをアップロードできるようになりました。

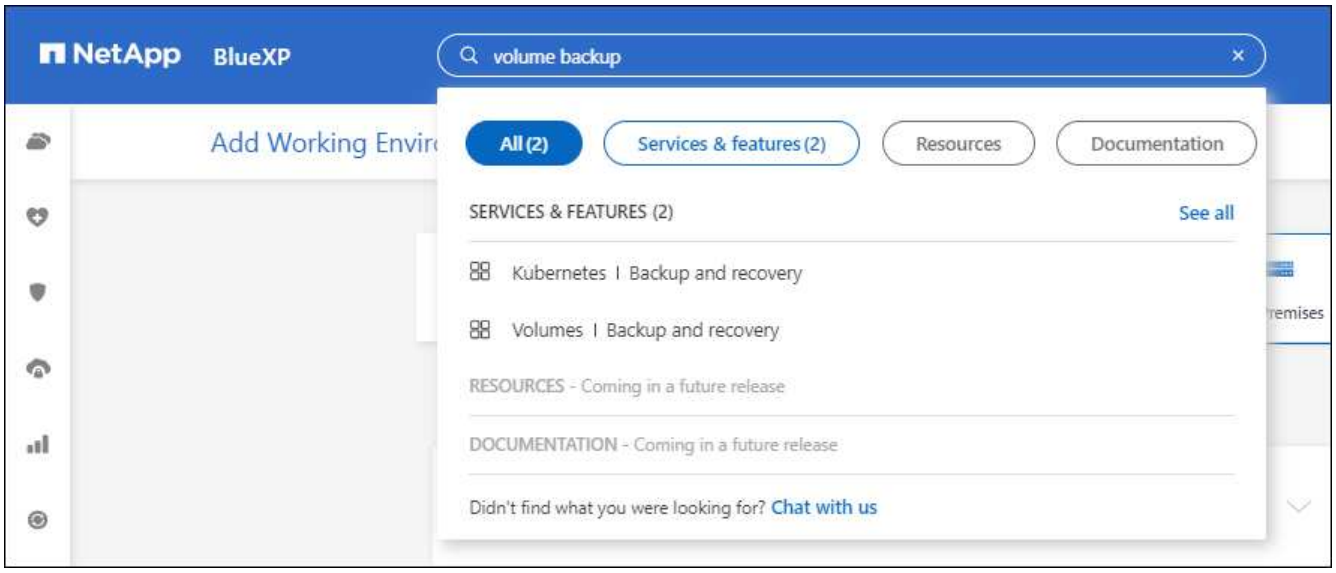
  "サポートケースを作成および管理する方法について説明します"。

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張とオンプレミスONTAP クラスタの機能拡張も含まれています。
  - "Cloud Volumes ONTAP の機能拡張について説明します"
  - "ONTAP オンプレミスクラスタの機能拡張について説明します"

2023年3月5日

コネクタ3.9.27

- BlueXPコンソールで検索できるようになりました。この時点で、検索機能を使用してBlueXPのサービスと機能を検索できます。



- アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと会社に関連付けられたケースを管理できます。

  "サポートケースの管理方法について説明します"。

- このコネクタは、インターネットから完全に分離されたクラウド環境でサポートされるようになりました。その後、コネクタで実行されているBlueXPコンソールを使用して、同じ場所にCloud Volumes ONTAP を導入し、オンプレミスのONTAP クラスタを検出できます（クラウド環境からオンプレミス環境に接続されている場合）。BlueXPのバックアップとリカバリを使用して、AWSとAzureのコマーシャルリージョンのCloud Volumes ONTAP ボリュームをバックアップすることもできます。このタイプの環境では、BlueXPデジタルウォレットを除き、他のBlueXPサービスはサポートされません。

  クラウドリージョンは、AWS Top Secret Cloud、AWS Secret Cloud、Azure IL6、または任意の商用リージョンのような米国の安全な機関のリージョンにすることができます。

  開始するには、コネクタソフトウェアを手動でインストールし、コネクタで実行されているBlueXPコンソールにログインし、BlueXPデジタルウォレットにBYOLライセンスを追加してから、Cloud Volumes ONTAP を導入します。

  - "インターネットにアクセスできない場所にコネクタを取り付けます"
  - "コネクタのBlueXPコンソールにアクセスします"
  - "未割り当てライセンスを追加します"
  - "Cloud Volumes ONTAP の使用を開始します"

- このコネクタで、BlueXPからAmazon S3バケットを追加および管理できるようになりました。

  "BlueXPからAWSアカウントに新しいAmazon S3バケットを追加する方法をご確認ください"。

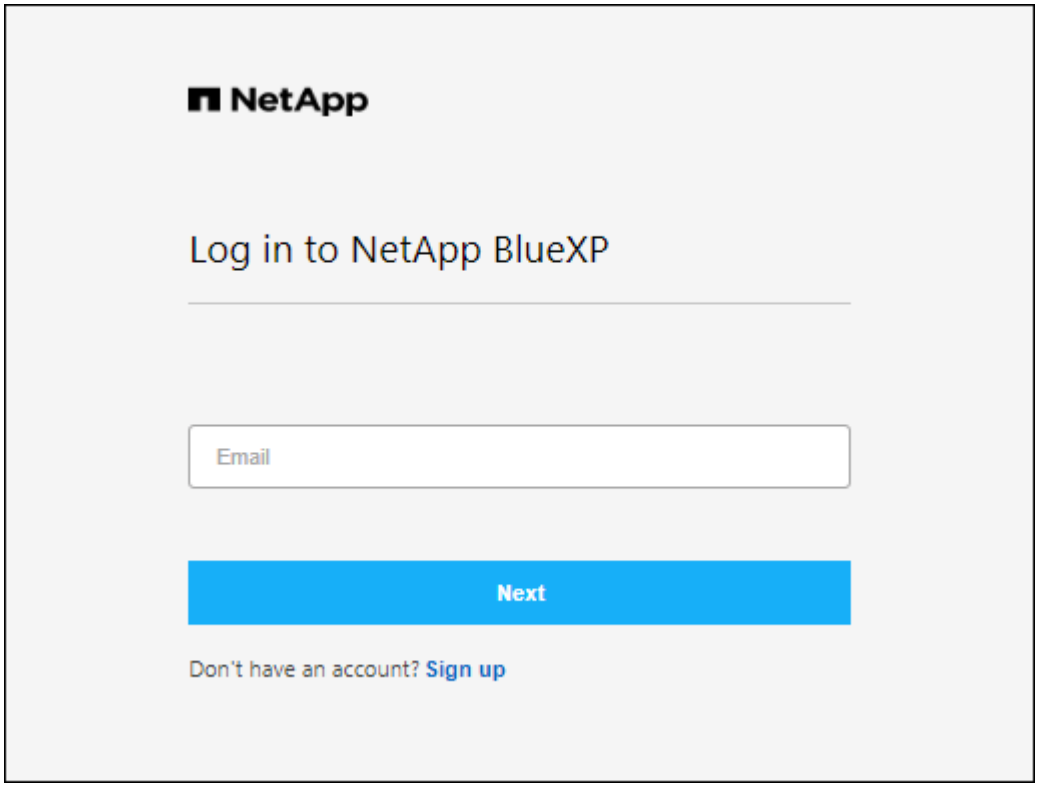
- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張が含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

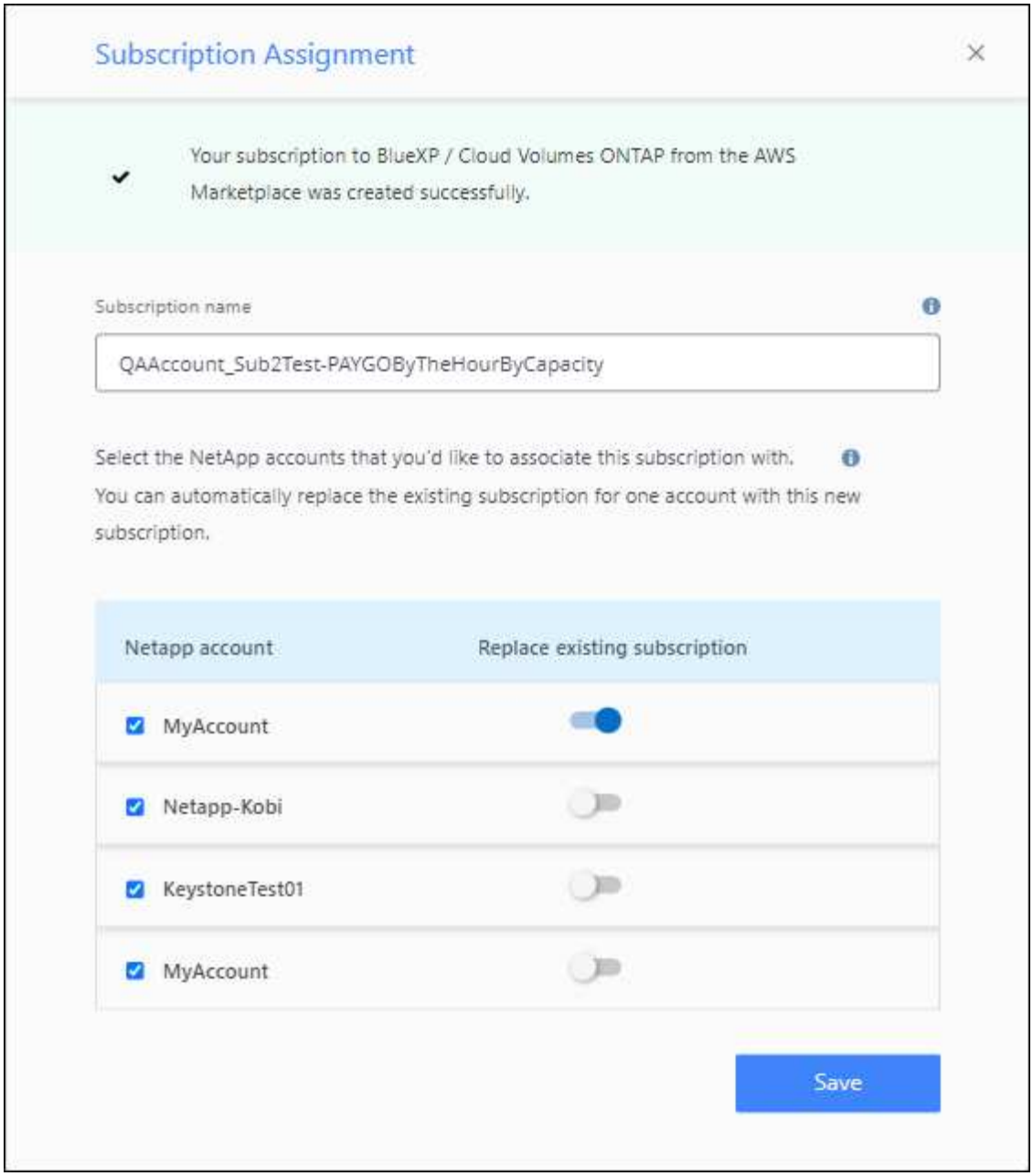
2023年2月5日

コネクタ3.9.26

- ログイン*ページで、ログインに関連付けられたメールアドレスを入力するように求められます。[次へ]*を選択すると、ログインに関連付けられている認証方式を使用して認証するよう求められます。
  - ネットアップクラウドクレデンシャルのパスワード
  - フェデレーテッドアイデンティティのクレデンシャル
  - NetApp Support Site クレデンシャルが必要です



- BlueXPを初めて使用していて、既存のNetApp Support Site (NSS)の資格情報がある場合は、サインアップページをスキップして、ログインページに電子メールアドレスを直接入力できます。この初回ログインの一環として、BlueXPがサインアップします。
- クラウドプロバイダのマーケットプレイスからBlueXPに登録すると、1つのアカウントの既存のサブスクリプションを新しいサブスクリプションに置き換えることができます。



  - "AWSサブスクリプションを関連付ける方法について説明します"
  - "Azureサブスクリプションを関連付ける方法について説明します"
  - "Google Cloudサブスクリプションを関連付ける方法について説明します"
- BlueXPは、コネクタの電源が14日以上切れている場合に通知します。
  - "BlueXP通知についてはこちらをご覧ください"
  - "コネクタの動作を維持する理由について説明します"
- Google Cloudのコネクタポリシーを更新し、Cloud Volumes ONTAP HAペアでStorage VMを作成および管理するために必要な権限を追加しました。

  compute.instances.updateNetworkInterface

  "ConnectorのGoogle Cloud権限を表示します"。

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張が含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

2023年1月1日

コネクタ3.9.25

このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張とバグ修正が含まれています。

"Cloud Volumes ONTAP の機能拡張について説明します"

2022年12月4日

コネクタ3.9.24

- BlueXPコンソールのURLがに更新されました https://console.bluexp.netapp.com
- ConnectorはGoogle Cloudイスラエル地域でサポートされるようになりました。
- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張とオンプレミスONTAP クラスタの機能拡張も含まれています。
  - "Cloud Volumes ONTAP の機能拡張について説明します"
  - "ONTAP オンプレミスクラスタの機能拡張について説明します"

2022年11月6日

コネクタ3.9.23

- BlueXPのPAYGOサブスクリプションと年間契約が、デジタルウォレットで表示、管理できるようになりました。

  "サブスクリプションの管理方法について説明します"

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

2022年11月1日

BlueXPの導入

NetApp BlueXPは、Cloud Managerを通じて提供される機能を拡張、強化します。BlueXPは、オンプレミス環境とクラウド環境のストレージとデータサービスにハイブリッドマルチクラウド環境を提供する統合コントロールプレーンです。

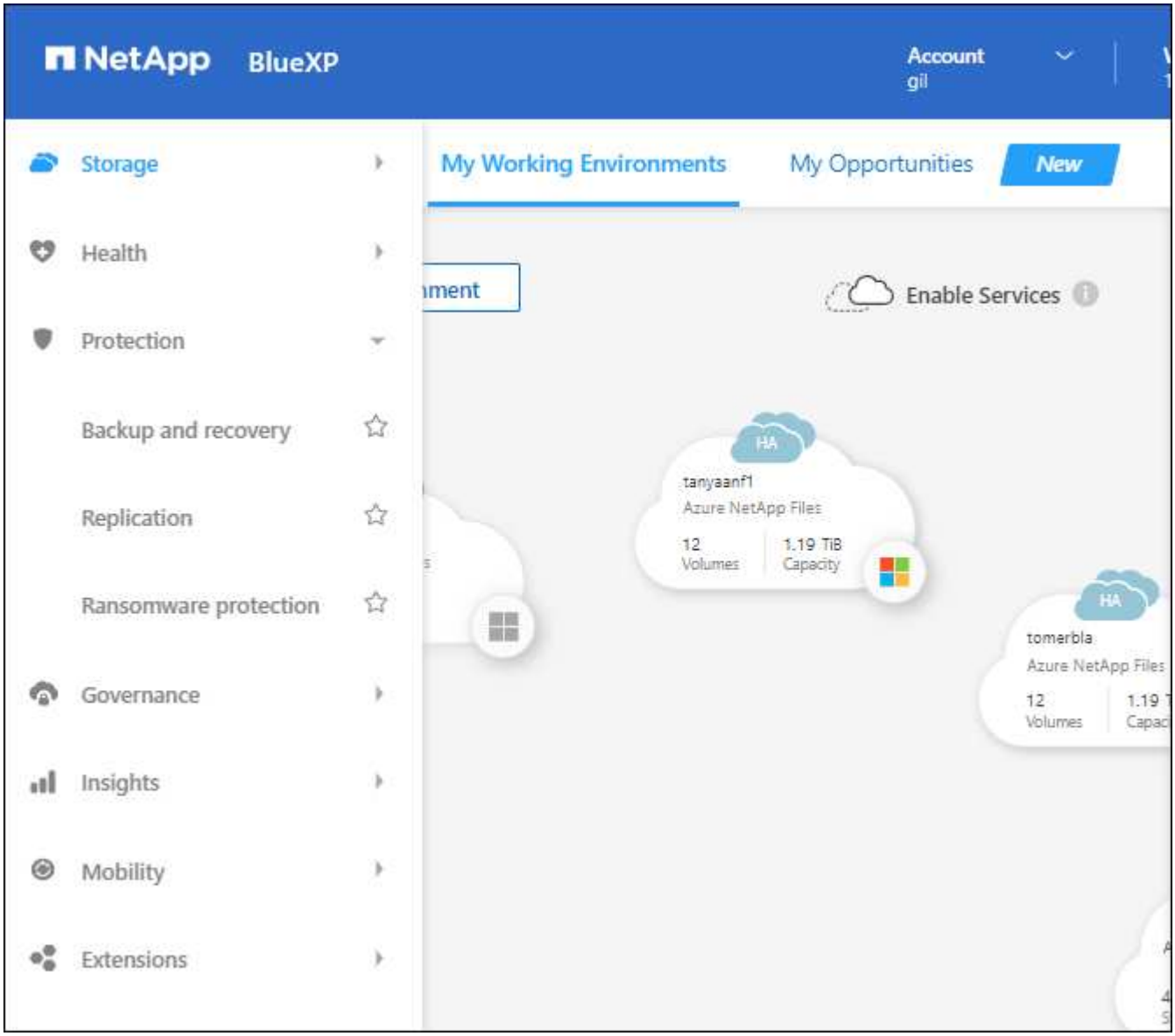
統合された管理エクスペリエンス
: BlueXPを使用すると’すべてのストレージおよびデータ資産を1つのインタフェースから管理できます

BlueXPを使用して、クラウドストレージ（Cloud Volumes ONTAP やAzure NetApp Files など）の作成と管理、データの移動、保護、分析、オンプレミスやエッジの多くのストレージデバイスの管理を行うことができます。

"詳細については、BlueXPのWebサイトをご覧ください"

新しいナビゲーションメニュー

BlueXPのナビゲーションメニューでは、サービスがカテゴリ別に分類され、機能に応じてサービスの名前が付けられます。たとえば、BlueXPのバックアップとリカバリには*[保護]*カテゴリからアクセスできます。



新しい製品統合

- コネクタがインストールされているAWSアカウントでAmazon S3バケットを管理できるようになりました。
- EシリーズやStorageGRID など、オンプレミスのストレージシステムをさらに管理できるようになりました。
- これまでスタンドアロンサービスとしてしか提供されていなかったデータサービスを、別のUIで使用

できるようになりました。たとえば、BlueXP Digital Advisor（Active IQ ）などです。

詳細はこちら。

- "Amazon S3バケットを管理する"
- "Eシリーズストレージシステムを管理"
- "StorageGRID ストレージシステムを管理します"
- "Digital Advisorの統合について"

NSSクレデンシャルの更新を求めるプロンプト

アカウントに関連付けられた更新トークンが3カ月後に期限切れになると、Cloud ManagerはNetApp Support Site アカウントに関連付けられたクレデンシャルの更新を求めます。 "NSS アカウントを管理する方法について説明します"

2022年9月18日

コネクタ**3.9.22**

- Connectorのインストールウィザードを強化しました。このウィザードには、Connectorのインストールに関する最小要件（権限、認証、ネットワーク）を満たすための手順が記載されています。
- ネットアップサポートケースをCloud Managerのサポートダッシュボードで直接作成できるようになりました。

  "ケースを作成する方法について説明します"。

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

2022年7月31日

コネクタ**3.9.21**

- Cloud Managerでまだ管理していない既存のクラウドリソースを検出する新しい方法が導入されました。

  Canvasでは、* My Opportunities *タブを使用して、ハイブリッドマルチクラウド全体で一貫したデータサービスと運用を実現するために、Cloud Managerに追加できる既存のリソースを一元的に検出できます。

  この初回リリースでは、My Opportunitiesを使用して、AWSアカウント内のONTAP ファイルシステム用の既存のFSXを検出できます。

  "ONTAP のFSXを発見する方法については、こちらをご覧ください"

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

2022年7月15日

ポリシーの変更

ドキュメントを更新するには、Cloud Managerのポリシーをドキュメント内に直接追加します。これにより、コネクタとCloud Volumes ONTAP に必要な権限を、設定方法を説明する手順とともに表示できるようになりました。これらのポリシーには、NetApp Support Siteのページからアクセスできます。

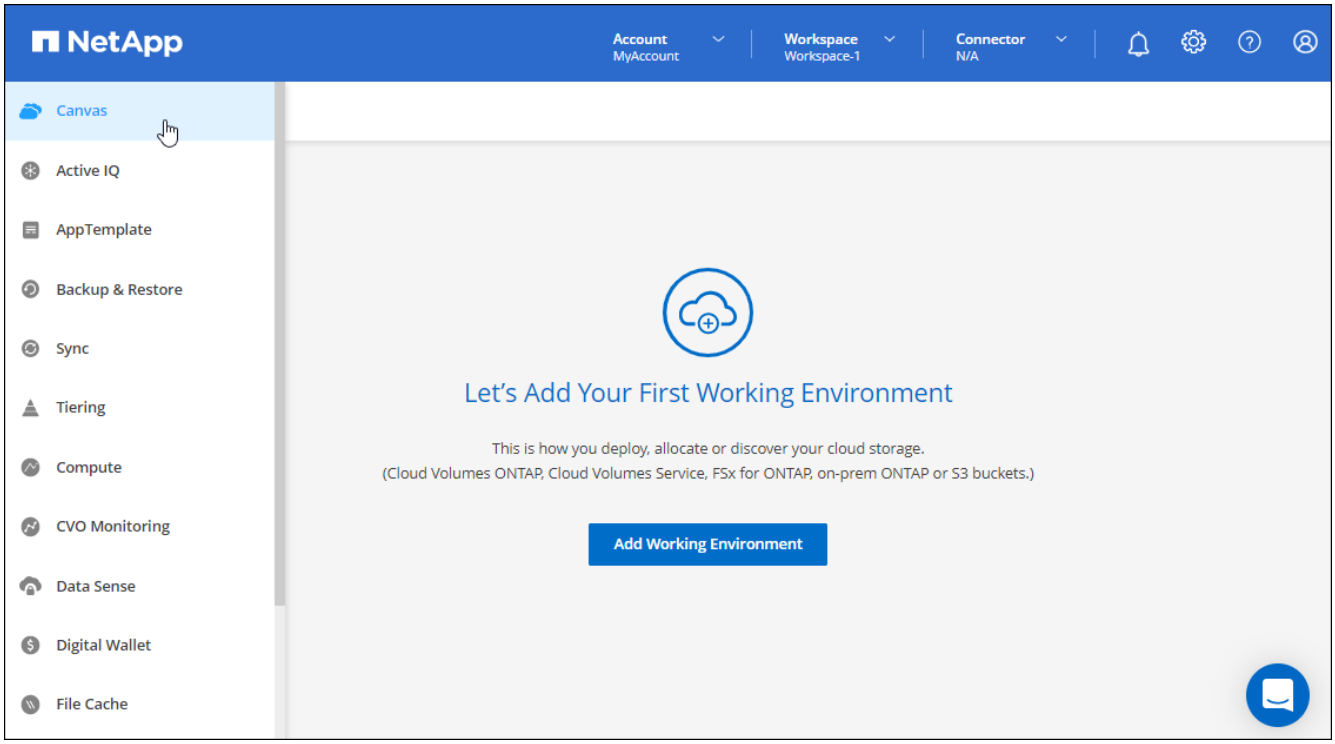
"次の例は、コネクタの作成に使用するAWS IAMロールの権限を示しています"。

また、各ポリシーへのリンクを提供するページも作成しました。 "Cloud Managerの権限の概要を確認します"。

2022年7月3日

コネクタ**3.9.20**

- 拡大する機能のリストへの新しいナビゲート方法が導入されました。左側のパネルにカーソルを合わせると、使い慣れたCloud Managerの機能を簡単に確認できます。



- Cloud ManagerからEメールで通知を送信するように設定できるようになりました。これにより、システムにログインしていないときでも重要なシステムアクティビティを通知できます。

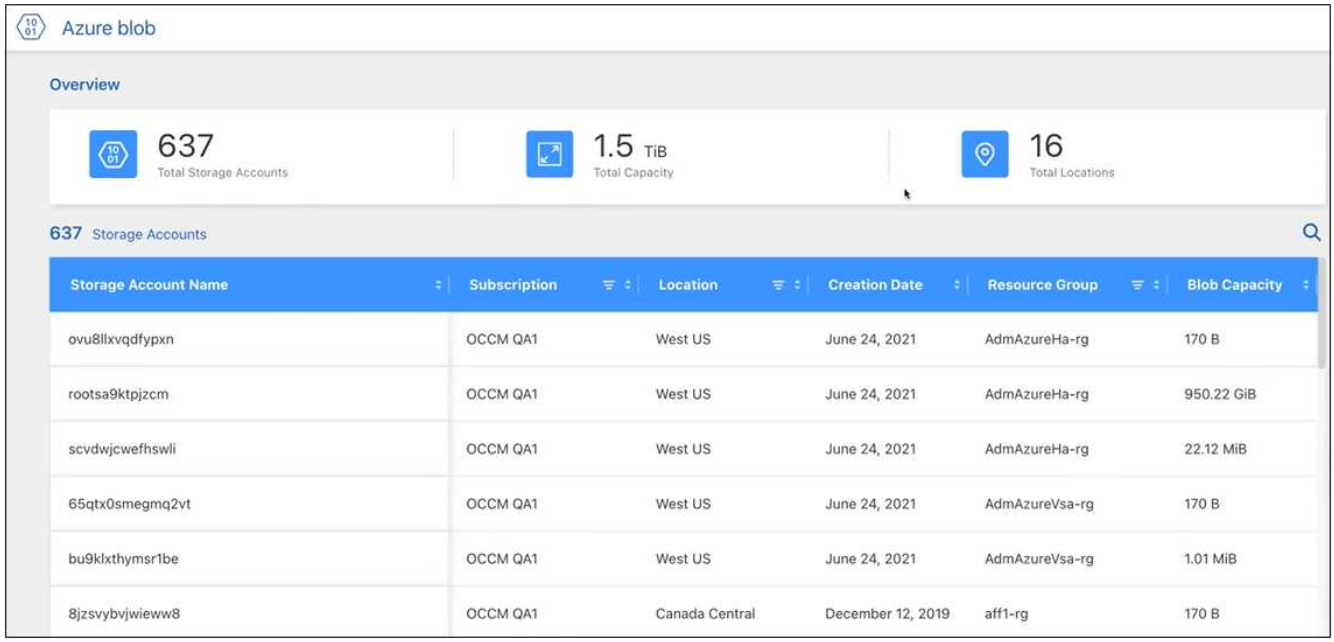
  "アカウントでの操作の監視の詳細については、こちらをご覧ください"。

- Cloud Managerでは、Amazon S3のサポートと同様に、Azure Blob StorageとGoogle Cloud Storageが作業環境としてサポートされるようになりました。

  AzureまたはGoogle Cloudにコネクタをインストールすると、Connectorがインストールされているプロジェクトで、Azureサブスクリプションまたは Google Cloud StorageのAzure Blob Storageに関する情報

がCloud Managerで自動的に検出されるようになりました。Cloud Managerにはオブジェクトストレージが作業環境として表示され、この環境を開いて詳細情報を確認することができます。

Azure Blob作業環境の例は次のとおりです。



- 容量や暗号化の詳細など、S3バケットに関する詳細情報を提供することで、Amazon S3作業環境用のリソースページが再設計されました。
- Connectorは、次のGoogle Cloudリージョンでサポートされるようになりました。
  - マドリード（ヨーロッパ-南西部1）
  - パリ（ヨーロッパ-西9区）
  - ワルシャワ（ヨーロッパ中央部2）
- Azure West US 3リージョンでコネクタがサポートされるようになりました。

  "サポートされているリージョンの完全なリストを表示します"

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。

  "Cloud Volumes ONTAP の機能拡張について説明します"

2022年6月28日

ネットアップのクレデンシャルでログインします

新規ユーザがCloud Centralに登録する際に、「ネットアップでログイン」オプションを選択して、NetApp Support Siteのクレデンシャルを使用してログインできるようになりました。Eメールアドレスとパスワードを入力する代わりに使用できます。

> Eメールアドレスとパスワードを使用する既存のログインでは、このログイン方法を使用し続ける必要があります。ネットアップでログインするオプションは、新規ユーザがサインアップする際に使用できます。

2022年6月7日

コネクタ3.9.19

- このコネクタは、AWSジャカルタリージョン（AP-Southee-3）でサポートされるようになりました。
- このコネクタは、Azureブラジル南東部でサポートされるようになりました。

  "サポートされているリージョンの完全なリストを表示します"

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張とオンプレミスONTAP クラスタの機能拡張も含まれています。
  - "Cloud Volumes ONTAP の機能拡張について説明します"
  - "ONTAP オンプレミスクラスタの機能拡張について説明します"

2022年5月12日

コネクタ3.9.18パッチ

コネクタを更新し、バグ修正を実施しました。最も注目すべき解決策は、問題 が共有VPC内にある場合にGoogle CloudでのCloud Volumes ONTAP の導入に影響するというものです。

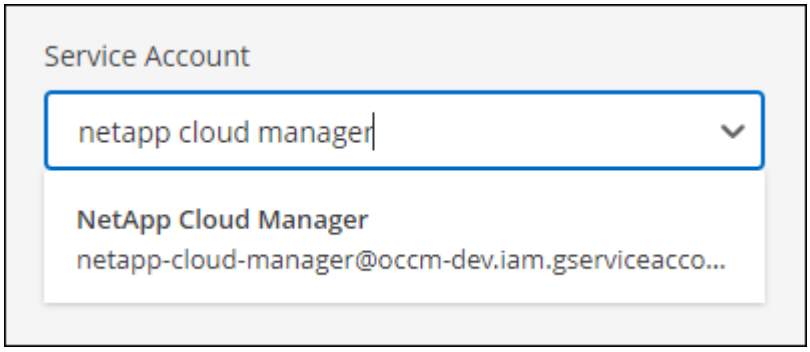
2022年5月2日

コネクタ3.9.18

- Connectorは、次のGoogle Cloudリージョンでサポートされるようになりました。
  - デリー（アジア-サウス2）
  - メルボルン（オーストラリア-スモアカス2）
  - ミラノ（ヨーロッパ-西8）
  - サンティアゴ（サウスメリカ-西1）

  "サポートされているリージョンの完全なリストを表示します"

- Connectorで使用するGoogle Cloudサービスアカウントを選択すると、Cloud Managerに各サービスアカウントに関連付けられているEメールアドレスが表示されるようになりました。メールアドレスを表示すると、同じ名前を共有するサービスアカウントを区別しやすくなります。



- をサポートするOSでVMインスタンス上のGoogle CloudのConnectorを認定しました "シールドVM機能"
- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。 "これらの拡張機能について説明します"
- ConnectorでCloud Volumes ONTAP を導入するには、新しいAWS権限が必要です。

  単一のAvailability Zone（AZ；アベイラビリティゾーン）にHAペアを導入する際にAWS分散配置グループを作成するためには、次の権限が必要です。

  ```
  "ec2:DescribePlacementGroups",
  "iam:GetRolePolicy",
  ```

  これらの権限は、Cloud Managerによる配置グループの作成方法を最適化するために必要になります。

  Cloud Managerに追加したAWSクレデンシャルの各セットに、これらの権限を必ず付与してください。 "コネクタの最新のIAMポリシーを確認します"。

2022年4月3日

コネクタ3.9.17

- Cloud Manager に、環境で設定した IAM ロールを割り当てることでコネクタを作成できるようになりました。この認証方式は、 AWS のアクセスキーとシークレットキーを共有する場合よりも安全です。

  "IAM ロールを使用してコネクタを作成する方法について説明します"。

- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。 "これらの拡張機能について説明します"

(2022年2月27日).

コネクタ3.9.16

- Google Cloud で新しいコネクタを作成すると、 Cloud Manager に既存のすべてのファイアウォールポリシーが表示されるようになります。以前は、 Cloud Manager にはターゲットタグがないポリシーは表示されませんでした。
- このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張も含まれています。 "これらの拡張機能について説明します"

(2022年1月30日).

コネクタ3.9.15

このリリースのコネクタには、Cloud Volumes ONTAP の機能拡張が含まれています。 "これらの拡張機能について説明します"

2022年1月2日

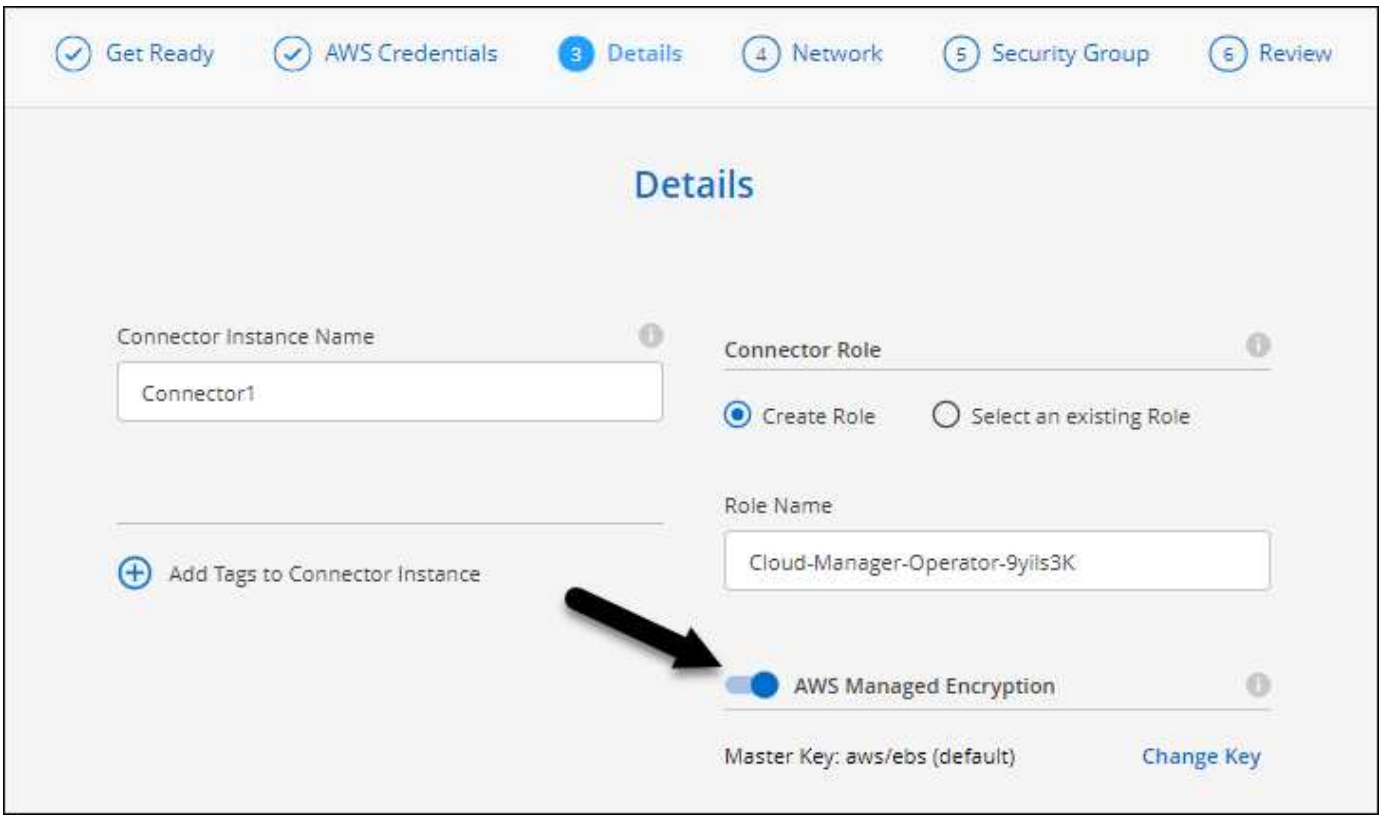
コネクタのエンドポイントが減少しました

パブリッククラウド環境内でリソースやプロセスを管理するためにコネクタが接続する必要があるエンドポイントの数を削減しました。

"必要なエンドポイントのリストを表示します"

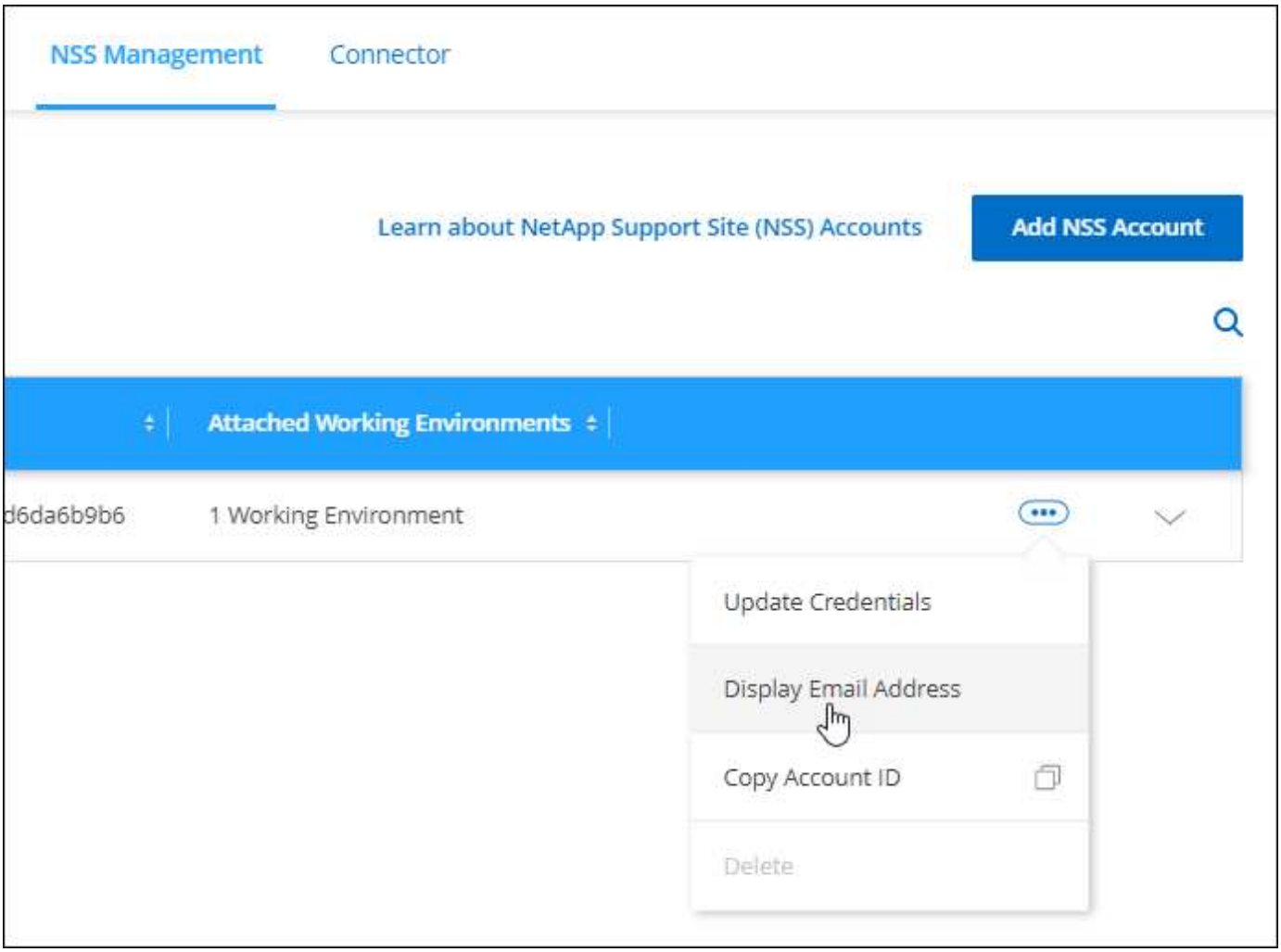
コネクタの **EBS** ディスク暗号化

Cloud Manager から AWS に新しいコネクタを導入する際に、デフォルトのマスターキーまたは管理対象キーを使用してコネクタの EBS ディスクを暗号化できるようになりました。



NSS アカウントの **E** メールアドレス

Cloud Manager に、NetApp Support Siteのアカウントに関連付けられている E メールアドレスが表示されるようになりました。



(2021年11月28日).

NetApp Support Siteのアカウントを更新する必要があります

2021 年 12 月以降、ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用するようになりました。この更新によって、 Cloud Manager は、以前に追加した既存のNetApp Support Siteのアカウントのクレデンシャルの更新を求めます。

NSS アカウントを IDaaS に移行していない場合は、まずアカウントを移行してから、 Cloud Manager でクレデンシャルを更新する必要があります。

"ネットアップによるID管理にMicrosoft Azure Active Directoryを使用する方法の詳細"

Cloud Volumes ONTAP の **NSS** アカウントを変更します

組織内に複数のNetApp Support Siteのアカウントがある場合、 Cloud Volumes ONTAP システムに関連付けられているアカウントを変更できるようになりました。

"作業環境を別の NSS アカウントに接続する方法について説明します"。

(2021年11月4日).

SOC 2 Type 2 認定

独立機関の公認会計士であり、サービス監査役は、 Cloud Manager 、 Cloud Sync 、 Cloud Tiering 、 Cloud Data Sense 、 Cloud Backup （ Cloud Manager プラットフォーム）を調査し、該当する信頼サービス基準に基づいて SOC 2 Type 2 のレポートを達成したことを確認しました。

"ネットアップの SOC 2 レポートをご覧ください"。

コネクタはプロキシとしてサポートされなくなりました

AutoSupport から Cloud Volumes ONTAP メッセージを送信するためのプロキシサーバとして Cloud Manager Connector を使用することはできなくなりました。この機能は削除され、サポートも終了しています。AutoSupport 接続は、 NAT インスタンスまたは環境のプロキシサービスを介して提供する必要があります。

"Cloud Volumes ONTAP による AutoSupport の検証の詳細については、こちらをご覧ください"

2021年10月31日閲覧

サービスプリンシパルを使用した認証

Microsoft Azure で新しいコネクタを作成する際、 Azure アカウントのクレデンシャルではなく Azure サービスプリンシパルで認証できるようになりました。

"Azure サービスプリンシパルでの認証方法について説明します"。

クレデンシャルの機能拡張

クレデンシャルページのデザインを見直し、使いやすく、 Cloud Manager のインターフェイスの外観に合わせて刷新しました。

2021年9月2日

新しい通知サービスが追加されました

通知サービスが導入され、現在のログインセッションで開始した Cloud Manager の処理のステータスを表示できるようになりました。処理が成功したかどうか、または失敗したかどうかを確認できます。 "アカウントの操作を監視する方法については、を参照してください"。

2021 年 7 月 7 日

コネクタの追加ウィザードの機能拡張

新しいオプションを追加して使いやすくするために、 * コネクターの追加 * ウィザードを再設計しました。タグの追加、ロール（ AWS または Azure ）の指定、プロキシサーバのルート証明書のアップロード、Terraform Automation のコードの表示、進捗状況の詳細の表示などが可能になりました。

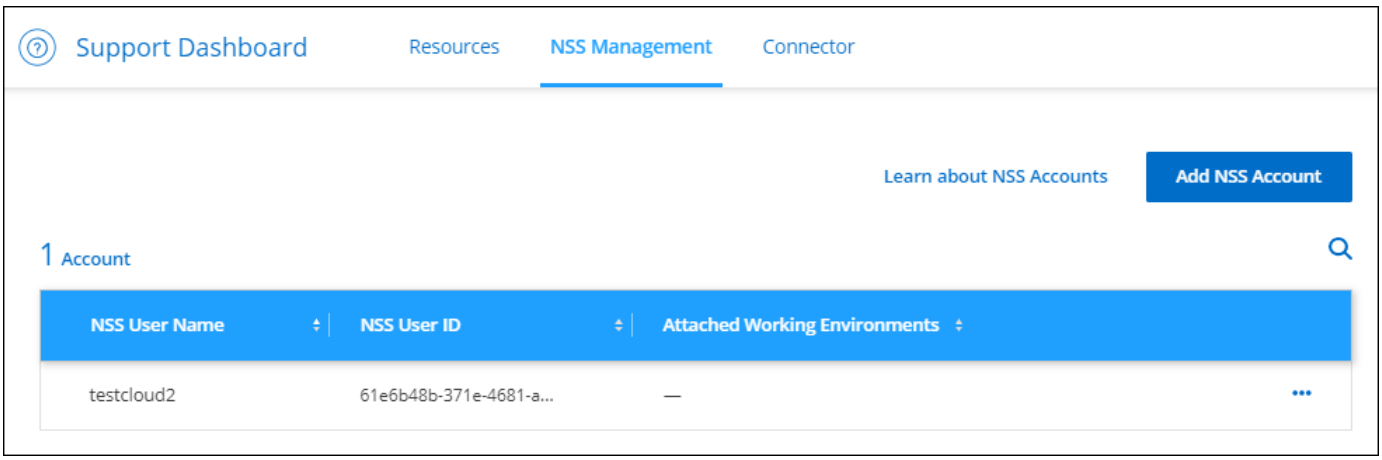
- "AWS でコネクタを作成します"

- "Azure でコネクタを作成します"
- "Google Cloud でコネクターを作成します"

NSS アカウントの管理をサポートダッシュボードから行うこともできます

NetApp Support Site（ NSS ）アカウントは、設定メニューではなくサポートダッシュボードで管理できるようになりました。この変更により、すべてのサポート関連情報を 1 箇所から簡単に検索して管理できるようになります。

"NSS アカウントを管理する方法について説明します"。



2021 年 5 月 5 日

タイムラインのアカウント

Cloud Manager のタイムラインに、アカウント管理に関連する操作とイベントが表示されるようになりました。アクションには、ユーザーの関連付け、ワークスペースの作成、コネクタの作成などがあります。タイムラインのチェックは、特定のアクションを実行したユーザーを特定する必要がある場合や、アクションのステータスを特定する必要がある場合に役立ちます。

"タイムラインをテナンシーサービスにフィルタリングする方法について説明します"。

(2021年4月11日).

Cloud Manager に直接 **API** で呼び出します

プロキシサーバを設定している場合、プロキシを経由せずに Cloud Manager に API 呼び出しを直接送信するオプションを有効にできるようになりました。このオプションは、 AWS または Google Cloud で実行されているコネクタでサポートされます。

"この設定の詳細については、こちらをご覧ください"。

サービスアカウントユーザ

サービスアカウントユーザを作成できるようになりました。

サービスアカウントは「ユーザ」の役割を果たし、 Cloud Manager に対して自動化のための許可された API

呼び出しを実行できます。これにより、自動化スクリプトを作成する必要がなくなります。自動化スクリプトは、会社を離れることができる実際のユーザアカウントに基づいて作成する必要がなくなります。フェデレーションを使用している場合は、クラウドから更新トークンを生成することなくトークンを作成できます。

"サービスアカウントの使用方法の詳細については、こちらをご覧ください"。

プライベートプレビュー

アカウントのプライベートプレビューで、新しい NetApp クラウドサービスが Cloud Manager のプレビューとして利用できるようになりました。

"このオプションの詳細については、こちらをご覧ください"。

サードパーティのサービス

また、アカウント内のサードパーティサービスが Cloud Manager で使用可能なサードパーティサービスにアクセスできるようにすることもできます。

"このオプションの詳細については、こちらをご覧ください"。

2021年3月8日

このアップデートには、いくつかの機能とサービスの機能強化が含まれています。

Cloud Volumes ONTAP の機能拡張

このリリースの Cloud Manager では、 Cloud Volumes ONTAP の管理が強化されています。

すべてのクラウドプロバイダで利用できる機能強化

Cloud Volumes ONTAP 9.9.9..0 を導入および管理できるようになりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

AWS で利用できる機能拡張

- クラウドサービス 9.8 を AWS Commercial Cloud Volumes ONTAP （ C2S ）環境に導入できるようになりました。

  "C2S の使用を開始する方法をご確認ください"

- Cloud Manager では、 AWS Key Management Service （ KMS ）を使用して Cloud Volumes ONTAP データを暗号化できるようになりました。Cloud Volumes ONTAP 9.9.9..0 以降では、お客様が管理する CMK を選択すると、 EBS ディスク上のデータと S3 に階層化されたデータが暗号化されます。これまでは、 EBS データだけが暗号化されていました。

  Cloud Volumes ONTAP IAM ロールに CMK を使用するためのアクセス権を付与する必要があります。

  "Cloud で AWS KMS を設定する方法については、こちらをご覧ください Volume ONTAP の略"

Azure で利用できる機能拡張

Cloud Volumes ONTAP 9.8 を、国防総省（ DoD ）の影響レベル 6 （ IL6 ）に導入できるようになりました。

Google Cloud で利用可能な機能強化

- Google Cloud で Cloud Volumes ONTAP 9.8 以降に必要な IP アドレスの数が削減されました。デフォルトでは、 IP アドレスを 1 つ減らす必要があります（インタークラスタ LIF をノード管理 LIF と統合しました）。また、 API を使用する場合は SVM 管理 LIF の作成を省略でき、追加の IP アドレスが不要になります。

  "Google Cloud の IP アドレス要件の詳細については、こちらをご覧ください"

- Google Cloud で Cloud Volumes ONTAP HA ペアを導入する際に、 VPC -1 、 VPC -2 、および VPC -3 の共有 VPC を選択できるようになりました。以前は、 VPC を共有できるのは VPC のみでした。この変更は Cloud Volumes ONTAP 9.8 以降でサポートされています。

  "Google Cloud のネットワーク要件の詳細については、こちらをご覧ください"

コネクタの機能拡張

- Connector が実行されていない場合に、 Cloud Manager から管理者ユーザに E メールで通知されるようになりました。

  コネクタを常時稼働させておくと、 Cloud Volumes ONTAP やその他の NetApp クラウドサービスを最大限に管理するのに役立ちます。

- コネクタのインスタンスタイプを変更する必要がある場合に、 Cloud Manager に通知が表示されるようになりました。

  インスタンスタイプを変更することで、現在利用できない新しい機能を確実に使用できます。

Cloud Sync の機能拡張

- Cloud Sync で ONTAP S3 ストレージと SMB サーバの同期関係がサポートされるようになりました。
  - ONTAP S3 ストレージから SMB サーバへの移動
  - SMB サーバから ONTAP S3 ストレージ

    "サポートされている同期関係を表示する"

- Cloud Sync では、ユーザインターフェイスからデータブローカーグループの設定を直接統合できるようになりました。

  自分で設定を変更することはお勧めしません。設定を変更するタイミングと変更方法については、ネットアップに相談してください。

  "ユニファイド構成の定義に関する詳細は、こちらをご覧ください"

Cloud Tiering の機能拡張

- Google Cloud Storage に階層化する場合は、ライフサイクルルールを適用して、階層化されたデータを Standard ストレージクラスから 30 日後に低コストの Nearline 、 Coldline 、または Archive ストレージに移行することができます。
- Cloud Tiering Now は、オンプレミスの ONTAP クラスタで検出されていないものがある場合に表示されます。これにより、クラスタへの階層化やその他のサービスを有効にすることができます。

  "これらのクラスタの詳細については、こちらをご覧ください"

Azure NetApp Files の機能拡張

ワークロードのニーズを満たし、コストを最適化するために、ボリュームのサービスレベルを動的に変更できるようになりました。ボリュームは、ボリュームに影響を及ぼすことなく、もう一方の容量プールに移動されます。 "詳細はこちら。"

(2021年2月9日).

サポートダッシュボードの強化

サポートダッシュボードが更新され、NetApp Support Siteのクレデンシャルを追加できるようになりました。このクレデンシャルをサポートに登録してください。ネットアップサポートケースは、ダッシュボードから直接開始することもできます。[ヘルプ] アイコンをクリックして、 [**Support**] をクリックします。

既知の制限

既知の制限事項は、このリリースの製品でサポートされていないプラットフォーム、デバイス、機能、または製品と正しく相互運用できない機能を特定します。これらの制限事項を慎重に確認してください

これらの制限は、BlueXPのセットアップと管理に特有のものです。コネクタ、SaaSプラットフォームなどです。

コネクタの制限

透過プロキシサーバはサポートされない

BlueXPでは、コネクタを備えた透過的プロキシサーバはサポートされていません。

"コネクタでプロキシサーバを使用する方法の詳細"。

172 の範囲の **IP** アドレスと競合する可能性があります

BlueXPは、172.17.0.0/16と172.18.0.0/16の範囲にIPアドレスを持つ2つのインターフェイスを持つコネクタを展開します。

ネットワークにこれらのいずれかの範囲が設定されたサブネットがある場合、BlueXPから接続エラーが発生する可能性があります。たとえば、BlueXPでオンプレミスのONTAP クラスタを検出できない場合があります。

技術情報アーティクルを参照してください "BlueXP ConnectorのIPが既存のネットワークと競合しています" コネクタのインターフェイスのIPアドレスを変更する方法については、を参照してください。

SSL復号化はサポートされていません

BlueXPでは、SSL復号化が有効になっているファイアウォール構成はサポートされていません。SSL復号化が有効になっている場合、BlueXPにエラーメッセージが表示され、コネクタインスタンスが非アクティブとして表示されます。

セキュリティを強化するには、を選択します "認証局（ CA ）が署名した HTTPS 証明書をインストールする"。

ローカル **UI** のロード時に空白ページが表示される

コネクタで実行されているWebベースのコンソールをロードすると、インターフェイスが表示されず、空白のページが表示されることがあります。

この問題は、キャッシュの問題に関連しています。回避策では、 incognito モードまたはプライベート Web ブラウザセッションを使用します。

共有 **Linux** ホストはサポートされません

コネクタは、他のアプリケーションと共有されている VM ではサポートされません。VM は、コネクタソフトウェア専用にする必要があります。

サードパーティのエージェントと内線番号

Connector VM では、サードパーティのエージェントや VM 拡張機能はサポートされません。

はじめに

基本事項をご確認ください

BlueXPの詳細をご覧ください

NetApp BlueXPは、オンプレミス環境とクラウド環境にわたってデータの構築、保護、ガバナンスを支援する単一のコントロールプレーンです。BlueXP SaaSプラットフォームには、ストレージ管理、データモビリティ、データ保護、データ分析と制御を提供するサービスが含まれています。管理機能は、WebベースのコンソールとAPIを介して提供されます。

機能

BlueXPプラットフォームは、データ管理において、ストレージ、モビリティ、保護、分析と制御という4つの主要な柱を提供します。

ストレージ

AWS、Azure、Google Cloud、オンプレミスのいずれであっても、ストレージを検出、導入、管理できます。

- をセットアップして使用します "Cloud Volumes ONTAP" 複数のクラウドにわたって効率的なマルチプロトコルデータ管理を実現します。
- クラウドファイルストレージサービスをセットアップして使用
  - "Azure NetApp Files の特長"
  - "ONTAP 対応の Amazon FSX"
  - "Cloud Volumes Service for Google Cloud"
- 検出と管理 "オンプレミスストレージ"：
  - Eシリーズシステム
  - ONTAP クラスタ
  - StorageGRID システム

モビリティ

データを同期、コピー、階層化、キャッシュすることで、必要な場所にデータを移動できます。

- "コピーと同期"
- "エッジキャッシュ"
- "階層化"

保護

自動化された保護メカニズムを使用して、データ損失、計画外停止、ランサムウェアなどのサイバー脅威からデータを保護します。

- "バックアップとリカバリ"
- "レプリケーション"
- "Kubernetesワークロードのデータ保護"

分析と管理

ツールを使用して、データストレージとインフラを監視、マッピング、最適化できます。実用的な情報を取得して、ストレージの健全性、耐障害性、経済性を最適化します。

- "分類"
- "デジタルアドバイザ"
- "経済効率"
- "運用の耐障害性"

"BlueXPを活用して組織を支援する方法をご紹介します"

サポートされているクラウドプロバイダ

BlueXPを使用すると、クラウドストレージを管理し、Amazon Web Services、Microsoft Azure、Google Cloudで クラウド サービス を使用できます。

コスト

BlueXPの価格は、使用する予定のサービスによって異なります。 "BlueXPの価格設定についてはこちらをご覧ください"

BlueXPの仕組み

BlueXPには、SaaSレイヤを通じて提供されるWebベースのコンソール、マルチテナンシーを提供するアカウント、作業環境を管理してBlueXPクラウドサービスを有効にするコネクタが含まれています。

ソフトウェアサービス

BlueXPには、からアクセスできます "Webベースのコンソール" API を使用できます。このSaaSエクスペリエンスでは、リリースされた最新機能に自動的にアクセスし、BlueXPアカウントとコネクタを簡単に切り替えることができます。

BlueXPアカウント

BlueXPに初めてログインすると、_BlueXPアカウント_を作成するように求められます。このアカウントはマルチテナンシーを提供し、分離されたワークスペース内でユーザとリソースを整理することができます。

"アカウントの詳細については、こちらをご覧ください"。

コネクタ

BlueXPの使用を開始するにはコネクタは必要ありませんが、コネクタを作成してBlueXPのすべての機能とサービスを有効にする必要があります。コネクタにより、オンプレミス環境とクラウド環境にわたってリソースとプロセスを管理できます。作業環境（Cloud Volumes ONTAPクラスタやオンプレミスのONTAPクラスタなど）の管理や、BlueXPの多くのデータサービスの使用が必要です。

"コネクタの詳細については、こちらをご覧ください"。

制限モードとプライベートモード

BlueXPは、セキュリティや接続が制限されている環境でもサポートされます。restricted mode_or_private mode__を使用して、アウトバウンド接続をBlueXP SaaSレイヤへの制限できます。

"BlueXPの導入モードの詳細については、こちらをご覧ください"。

SOC 2 Type 2 認定

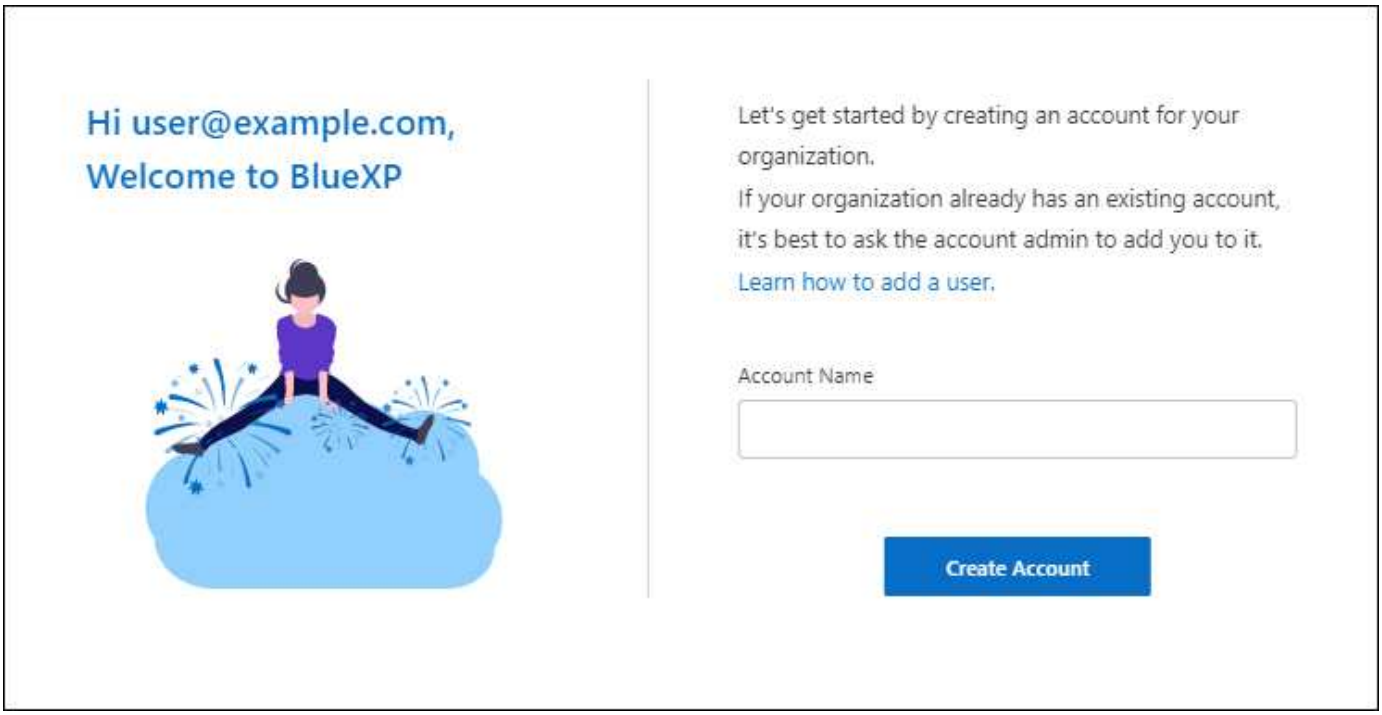
独立した公認会計士事務所およびサービス監査人がBlueXPを調査し、該当するトラストサービスの基準に基づいてSOC 2 Type 2レポートを達成したことを確認しました。

"ネットアップの SOC 2 レポートをご覧ください"

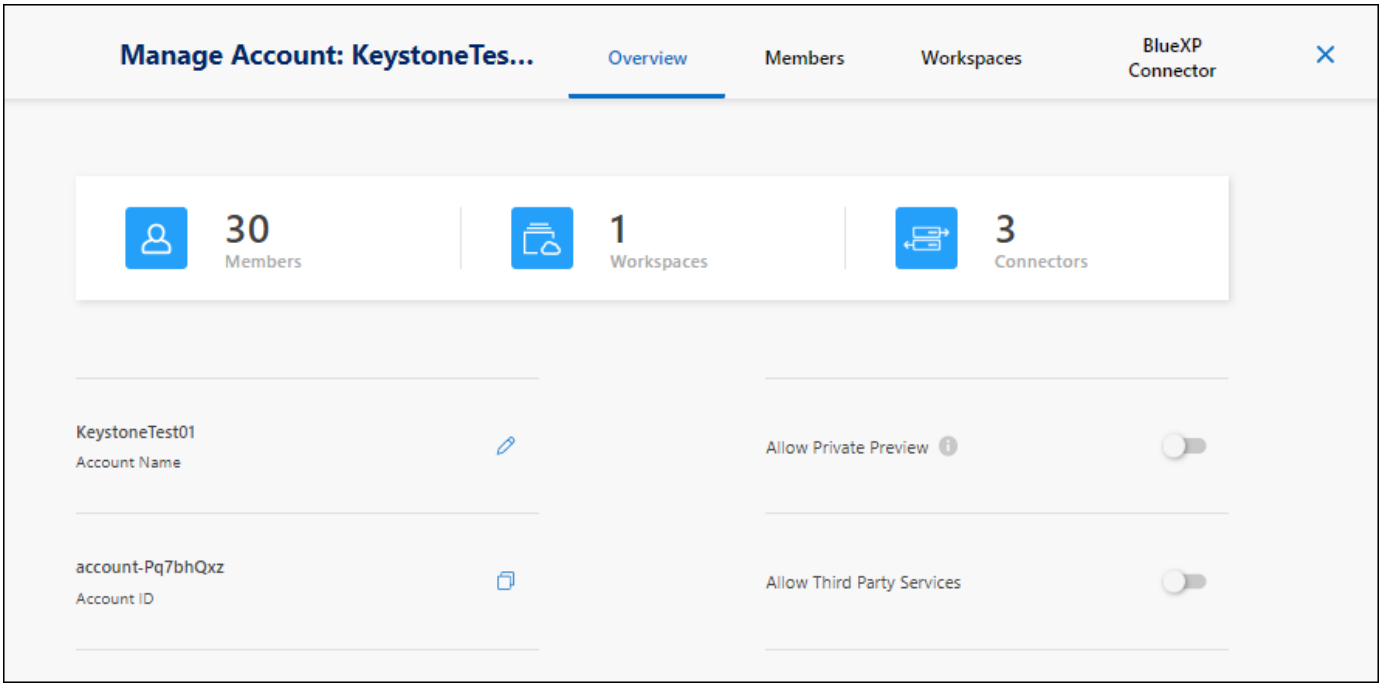
BlueXPアカウントの詳細をご確認ください

A_BlueXPアカウント_は組織にマルチテナンシーを提供するため、isolated_workspaces_でユーザとリソースを整理できます。たとえば、ユーザーのグループは、別のワークスペースで作業環境を管理するユーザーには表示されないワークスペースにCloud Volumes ONTAP作業環境を展開および管理できます。

BlueXPに初めてアクセスすると、アカウントを選択または作成するように求められます。たとえば、まだアカウントを持っていない場合は、次の画面が表示されます。



BlueXPアカウント管理者は'ユーザー(メンバー)'ワークスペース'およびコネクタを管理することで'このアカウントの設定を変更できます



"BlueXPアカウントの管理方法をご紹介します"。

展開モード

BlueXPには、アカウントに標準モード、制限モード、プライベートモードの導入モードが用意されています。これらのモードは、さまざまなレベルのセキュリティおよび接続制限を持つ環境をサポートします。

"BlueXPの導入モードの詳細については、こちらをご覧ください"。

メンバー

メンバーとは、BlueXPアカウントに関連付けるBlueXPユーザです。ユーザーをアカウントと1つ以上のワークスペースに関連付けることで、これらのユーザーは作業環境をBlueXPで作成および管理できます。

ユーザを関連付けると、ユーザにロールが割り当てられます。

- *Account Admin*: BlueXPではどのようなアクションでも実行できます。
- _ ワークスペース管理者 _ ：割り当てられたワークスペースでリソースを作成および管理できます。
- *Compliance Viewer*：BlueXP分類のコンプライアンス情報のみを表示し、アクセス権限があるワークスペースのレポートを生成できます。

"これらの役割の詳細については、こちらをご覧ください"。

ワークスペース

BlueXPでは、ワークスペースによって、_working environments_の数がアカウントの他のユーザから分離されます。アカウント管理者がそのワークスペースに管理者を関連付けないと、ワークスペース管理者はワークスペース内の作業環境にアクセスできません。

作業環境はストレージシステムを表します。例：

- Cloud Volumes ONTAP システム
- オンプレミスのONTAP クラスタ
- Kubernetesクラスタ

"ワークスペースを追加する方法について説明します"。

コネクタ

コネクタは、データインフラを管理するためにBlueXPが実行する必要のあるアクションを実行します。コネクタは、クラウドプロバイダに導入した仮想マシンインスタンス、または設定したオンプレミスホストで実行されます。

コネクタは複数のBlueXPサービスで使用できます。たとえば、Cloud Volumes ONTAP の管理にコネクタを使用している場合は、同じコネクタをBlueXP階層化などの別のサービスで使用できます。

"コネクタの詳細については、こちらをご覧ください"。

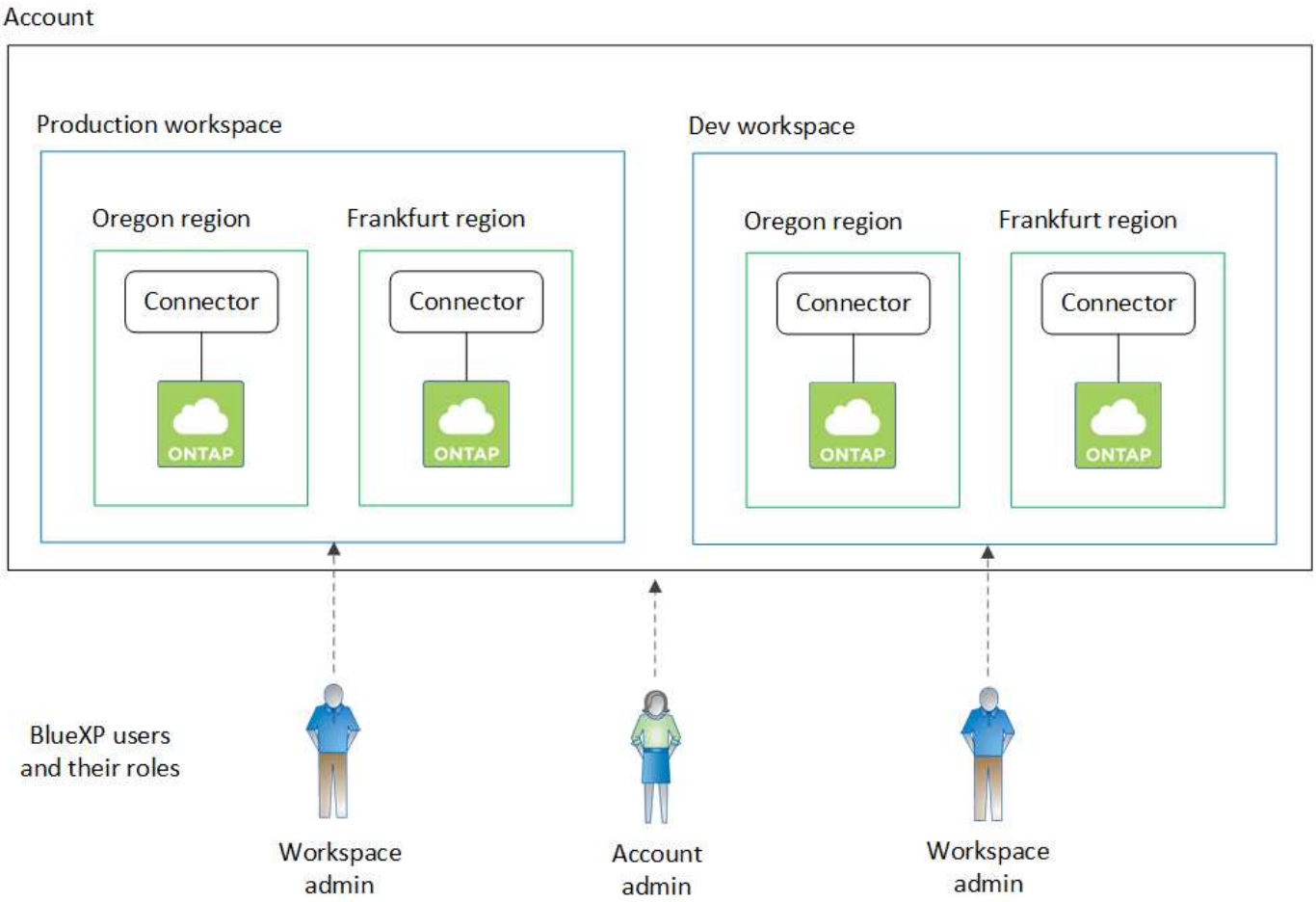
例

次の例は、アカウントの設定方法を示しています。

> 以降の例の画像では、コネクタとCloud Volumes ONTAP システムは実際にはBlueXPアカウントには存在しません。これらはクラウドプロバイダで実行されています。これは、各コンポーネント間の関係の概念図です。

複数のワークスペース

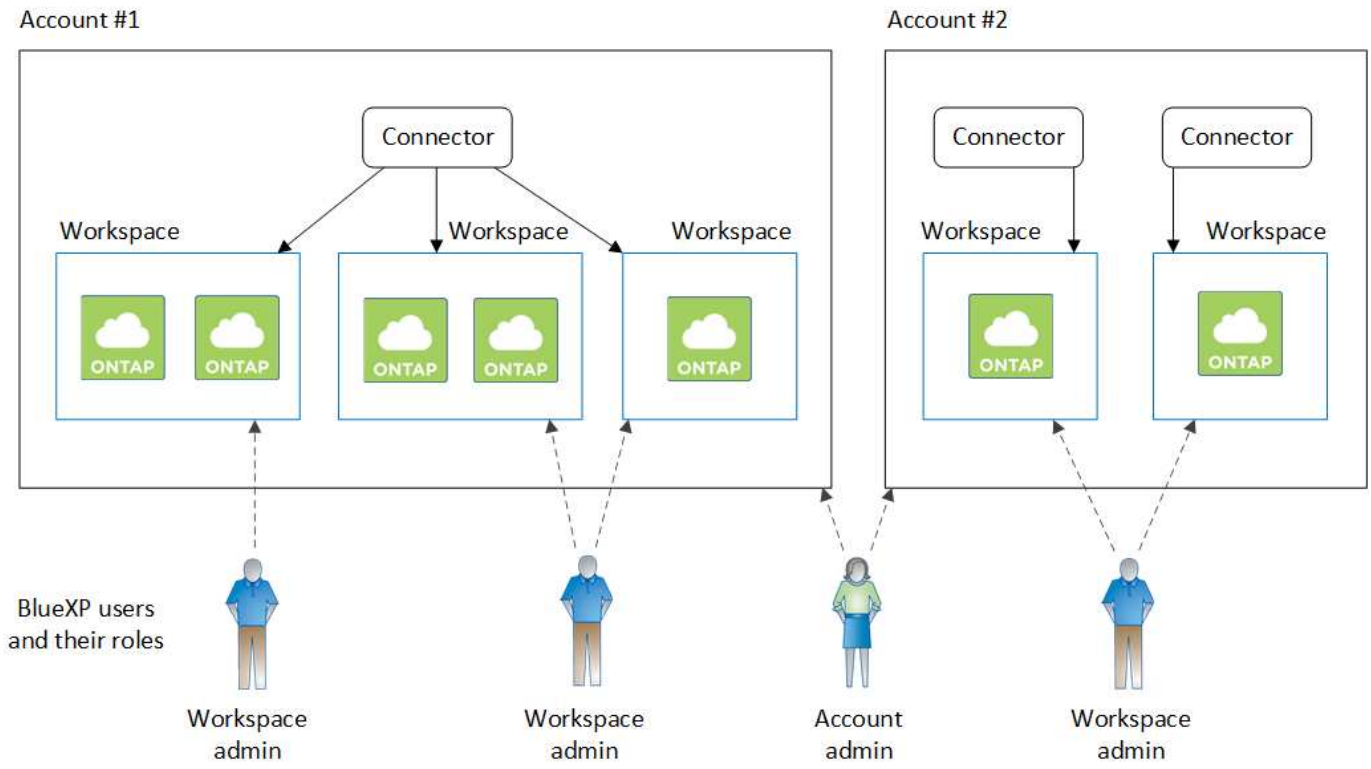
次の例は、 2 つのワークスペースを使用して分離された環境を作成するアカウントを示しています。1 つ目のワークスペースは本番環境用で、 2 つ目のワークスペースは開発環境用です。



複数のアカウント

別の例では、2つのBlueXPアカウントを使用して、最高レベルのマルチテナンシーを実現しています。たとえば、あるアカウントでBlueXPを使用して顧客にサービスを提供しながら、別のアカウントを使用して事業部門の1つにディザスタリカバリを提供することができます。

アカウント 2 には 2 つのコネクタがあります。これは、システムが別々の地域にある場合や、別々のクラウドプロバイダにある場合に発生することがあります。



コネクタについて説明します

A_connector_は、クラウドネットワークまたはオンプレミスネットワークで実行されるネットアップのソフトウェアです。データインフラを管理するためにBlueXPが実行する必要のあるアクションを実行します。Connectorは、必要なアクションについてBlueXP SaaSレイヤを定期的にポーリングします。BlueXPの使用を開始するにはコネクタは必要ありませんが、コネクタを作成してBlueXPのすべての機能とサービスを有効にする必要があります。

コネクタなしでできること

BlueXPの使用を開始するためにコネクタは必要ありません。コネクタを作成することなく、BlueXPで複数の機能やサービスを使用できます。

コネクタなしでBlueXPの次の機能とサービスを使用できます。

- Amazon FSx for NetApp ONTAP 作業環境の作成

  コネクタは作業環境の作成には必要ありませんが、ボリュームの作成と管理、データのレプリケート、FSx for ONTAP とBlueXPの分類やコピーと同期などのサービスの統合を行う必要があります。

- 自動化カタログ
- Azure NetApp Files の特長

  Azure NetApp Files のセットアップと管理にコネクタは必要ありませんが、BlueXP分類を使用してAzure NetApp Files データをスキャンする場合はコネクタが必要です。

- Cloud Volumes Service for Google Cloud
- コピーと同期
- デジタルアドバイザ
- デジタルウォレット

  ほとんどすべての場合、コネクタなしでデジタルウォレットにライセンスを追加できます。

  デジタルウォレットにライセンスを追加するためにコネクタが必要なのは、Cloud Volumes ONTAP _ノードベース_ライセンスのみです。この場合、 Cloud Volumes ONTAP システムにインストールされているライセンスのデータを使用するため、コネクタが必要です。

- オンプレミスのONTAP クラスタを直接検出

  オンプレミスのONTAP クラスタを直接検出する場合はコネクタは必要ありませんが、BlueXPのその他の機能を利用する場合はコネクタが必要です。

  "オンプレミスのONTAP クラスタの検出オプションと管理オプションの詳細については、こちらをご覧ください"

- 持続可能性

コネクタが必要な場合

BlueXPを標準モードで使用する場合、BlueXPの次の機能やサービスにはコネクタが必要です。

- ONTAP 管理機能用の Amazon FSX
- Amazon S3ストレージ
- Azure BLOBストレージ
- バックアップとリカバリ
- 分類
- Cloud Volumes ONTAP
- ディザスタリカバリ
- Eシリーズシステム
- 経済性^ 1^
- エッジキャッシュ
- Google Cloud Storageバケット
- Kubernetes クラスタ
- 移行レポート
- オンプレミスのONTAP クラスタとBlueXPデータサービスの統合
- 運用の耐障害性[1]
- ランサムウェアからの保護
- StorageGRID システム

- 階層化
- ボリュームキャッシュ

[1]コネクタなしでこれらのサービスにアクセスできますが、サービスからアクションを開始するにはコネクタが必要です。

BlueXPを制限モードまたはプライベートモードで使用するには、コネクタが必要です。

コネクタは常に動作している必要があります

コネクタは、BlueXPサービスアーキテクチャの基本要素です。関連するコネクタが常に稼働し、アクセス可能であることを確認するのは、お客様の責任です。このサービスは、コネクタの可用性の短い停止を克服するように設計されていますが、インフラストラクチャの障害を修復するために必要なときにすぐに対処する必要があります。

このドキュメントにはEULAが適用されます。製品がドキュメントに従って操作されていない場合、製品の機能と操作、およびEULAに基づくお客様の権利に悪影響を及ぼす可能性があります。

Cloud Volumes ONTAP への影響

コネクタは、Cloud Volumes ONTAP の正常性と動作における重要なコンポーネントです。コネクタの電源がオフの場合は、Cloud Volumes ONTAP PAYGOシステムと容量ベースのBYOLシステムは、コネクタとの通信を14日以上切断したあとでシャットダウンします。これは、コネクタがシステムのライセンスを毎日更新するためです。

Cloud Volumes ONTAP システムにノードベースのBYOLライセンスがある場合は、ライセンスがCloud Volumes ONTAP システムにインストールされているため、14日後もシステムは実行されたままになります。

サポートされている場所

コネクタは次の場所でサポートされています。

- Amazon Web Services の
- Microsoft Azure

  Azureのコネクタは、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"

- Google Cloud

  BlueXPサービスをGoogle Cloudで使用する場合は、Google Cloudで実行されているコネクタを使用する必要があります。

- オンプレミス

制限モードとプライベートモード

BlueXPを制限モードまたはプライベートモードで使用するには、まずBlueXPでコネクタをインストールし、コネクタでローカルに実行されているユーザインターフェイスにアクセスします。

"BlueXPの導入モードについて説明します"。

コネクタを作成する方法

BlueXPアカウント管理者は、BlueXPまたはクラウドプロバイダのマーケットプレイスから直接コネクタを作成するか、自社のLinuxホストに手動でソフトウェアをインストールしてコネクタを作成できます。BlueXPを標準モード、制限モード、プライベートモードのいずれで使用しているかによって、作業を開始する方法が異なります。

- "BlueXPの導入モードについて説明します"
- "BlueXPを標準モードで開始する"
- "制限モードでのBlueXPの使用を開始する"
- "BlueXPのプライベートモードで開始する"

権限

BlueXPからコネクタを直接作成するには特定の権限が必要です。コネクタインスタンス自体には別の権限セットが必要です。AWSまたはAzureでBlueXPから直接コネクタを作成する場合は、必要な権限でコネクタがBlueXPによって作成されます。

標準モードでBlueXPを使用している場合、権限の付与方法はコネクタの作成方法によって異なります。

アクセス許可の設定方法については、以下を参照してください。

- 標準モード
  - "AWSでのコネクタのインストールオプション"
  - "Azureでのコネクタのインストールオプション"
  - "Google Cloudでのコネクタのインストールオプション"
  - "オンプレミス環境のクラウド権限を設定"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

コネクタが日常的な操作に必要とする正確な権限を表示するには、次のページを参照してください。

- "ConnectorでのAWS権限の使用方法について説明します"
- "ConnectorでのAzure権限の使用方法について説明します"
- "ConnectorでのGoogle Cloud権限の使用方法について説明します"

コネクタのアップグレード

私たちは通常、コネクタソフトウェアを毎月更新して新機能を導入し、安定性を向上させています。BlueXPプラットフォームのサービスと機能のほとんどはSaaSベースのソフトウェアで提供されますが、いくつかの機能はコネクタのバージョンによって異なります。Cloud Volumes ONTAP 管理、オンプレミスの ONTAP クラスタ管理、設定、ヘルプが含まれます。

標準モードまたは制限モードでBlueXPを使用すると、ソフトウェアの更新を取得するためにアウトバウンドのインターネットアクセスが確立されていれば、コネクタは自動的にソフトウェアを最新バージョンに更新し

ます。BlueXPをプライベートモードで使用している場合は、コネクタを手動でアップグレードする必要があります。

"コネクタソフトウェアを手動でアップグレードする方法について説明します"。

オペレーティングシステムと**VM**のメンテナンス

コネクタホストでのオペレーティングシステムの保守はお客様の責任で行ってください。たとえば、オペレーティングシステムの配布に関する会社の標準手順に従って、コネクタホストのオペレーティングシステムにセキュリティ更新プログラムを適用する必要があります。

OSの更新を実行するときは、コネクタホスト上のサービスを停止する必要はありません。

コネクタVMを停止してから起動する必要がある場合は、クラウドプロバイダのコンソールから、またはオンプレミス管理の標準手順を使用して起動する必要があります。

コネクタは常に動作している必要があることに注意してください。

複数の作業環境

コネクタは、BlueXPで複数の作業環境を管理できます。1 つのコネクタで管理できる作業環境の最大数は、環境によって異なります。管理対象は、作業環境の種類、ボリュームの数、管理対象の容量、ユーザの数によって異なります。

大規模な導入の場合は、ネットアップの担当者にご相談のうえ、環境のサイジングを行ってください。途中で問題が発生した場合は、製品内のチャットでお問い合わせください。

複数のコネクタ

コネクタが 1 つしか必要ない場合もありますが、 2 つ以上のコネクタが必要な場合もあります。

次にいくつかの例を示します。

- マルチクラウド環境（AWSやAzureなど）で、コネクタの1つをAWSに、もう1つをAzureに配置したいと考えています。各で、それらの環境で実行される Cloud Volumes ONTAP システムを管理します。
- サービスプロバイダは、1つのBlueXPアカウントを使用してお客様にサービスを提供し、別のアカウントを使用してビジネスユニットのディザスタリカバリを提供することができます。アカウントごとに個別のコネクタがあります。

いつスイッチするか

最初のコネクタを作成すると、作成した追加の作業環境ごとにそのコネクタが自動的に使用されます。コネクタを追加で作成したら、コネクタを切り替えることで各コネクタに固有の作業環境を確認する必要があります。

"コネクタを切り替える方法について説明します"。

ディザスタリカバリ

ディザスタリカバリ目的で、複数のコネクタを備えた作業環境を同時に管理できます。一方のコネクタが停止した場合は、もう一方のコネクタに切り替えて、作業環境をただちに管理できます。

この構成をセットアップするには：

1. "別のコネクタに切り替えます"。
2. 既存の作業環境を検出
   - "既存のCloud Volumes ONTAP システムをBlueXPに追加します"
   - "ONTAP クラスタを検出"
3. を設定します "Capacity Management Mode （容量管理モード）"

   メインコネクターのみ * オートマチックモード * に設定する必要があります。DR 目的で別のコネクタに切り替える場合は、必要に応じて容量管理モードを変更できます。

BlueXPの導入モードについて説明します

BlueXPには複数の_導入モード_が用意されており、ビジネス要件やセキュリティ要件を満たす方法でBlueXPを使用できます。_Standard modeは*BlueXP SaaS*レイヤを活用してすべての機能を提供しますが、*_restricted mode_and_private mode*は接続が制限されている組織で使用できます。

制限モードまたはプライベートモードを使用している場合、BlueXPではトラフィック、通信、データのフローが禁止されますが、環境（オンプレミスとクラウド内）が必要な規制に準拠していることを確認するのはお客様の責任です。

概要

BlueXPには、お客様のアカウントに次の導入モードが用意されています。各モードは、アウトバウンド接続要件、導入場所、インストールプロセス、認証方法、使用可能なデータサービスとストレージサービス、課金方法の点で異なります。

標準モード

BlueXPは、Webベースのコンソールからクラウドサービスとしてアクセスできます。使用するBlueXPサービスに応じて、BlueXP管理者はハイブリッドクラウド環境内のデータを管理するためのコネクタを1つ以上作成します。

このモードでは、パブリックインターネットを介した暗号化されたデータ転送が使用されます。

制限モード

BlueXP Connectorはクラウド（行政リージョン、主権あるクラウドリージョン、商用リージョン）にインストールされ、BlueXPのSaaSレイヤへのアウトバウンド接続に制限があります。BlueXPには、SaaSレイヤではなくコネクタからアクセスできるWebベースのコンソールからローカルにアクセスします。

このモードは通常、州や地方自治体や規制された企業で使用されます。

SaaSレイヤへのアウトバウンド接続の詳細については、こちらをご覧ください。

プライベートモード

BlueXP Connectorはオンプレミスまたはクラウド（セキュアなリージョン、ソブリンクラウドリージョン、商用リージョン）にインストールされ、BlueXP SaaSレイヤへの_no_connectivityがあります。BlueXPには、SaaSレイヤではなくコネクタからアクセスできるWebベースのコンソールからローカ

ルにアクセスします。

セキュアなリージョンには、が含まれます "AWSシークレットクラウド"、 "AWSのトップシークレットクラウド"および "Azure IL6"

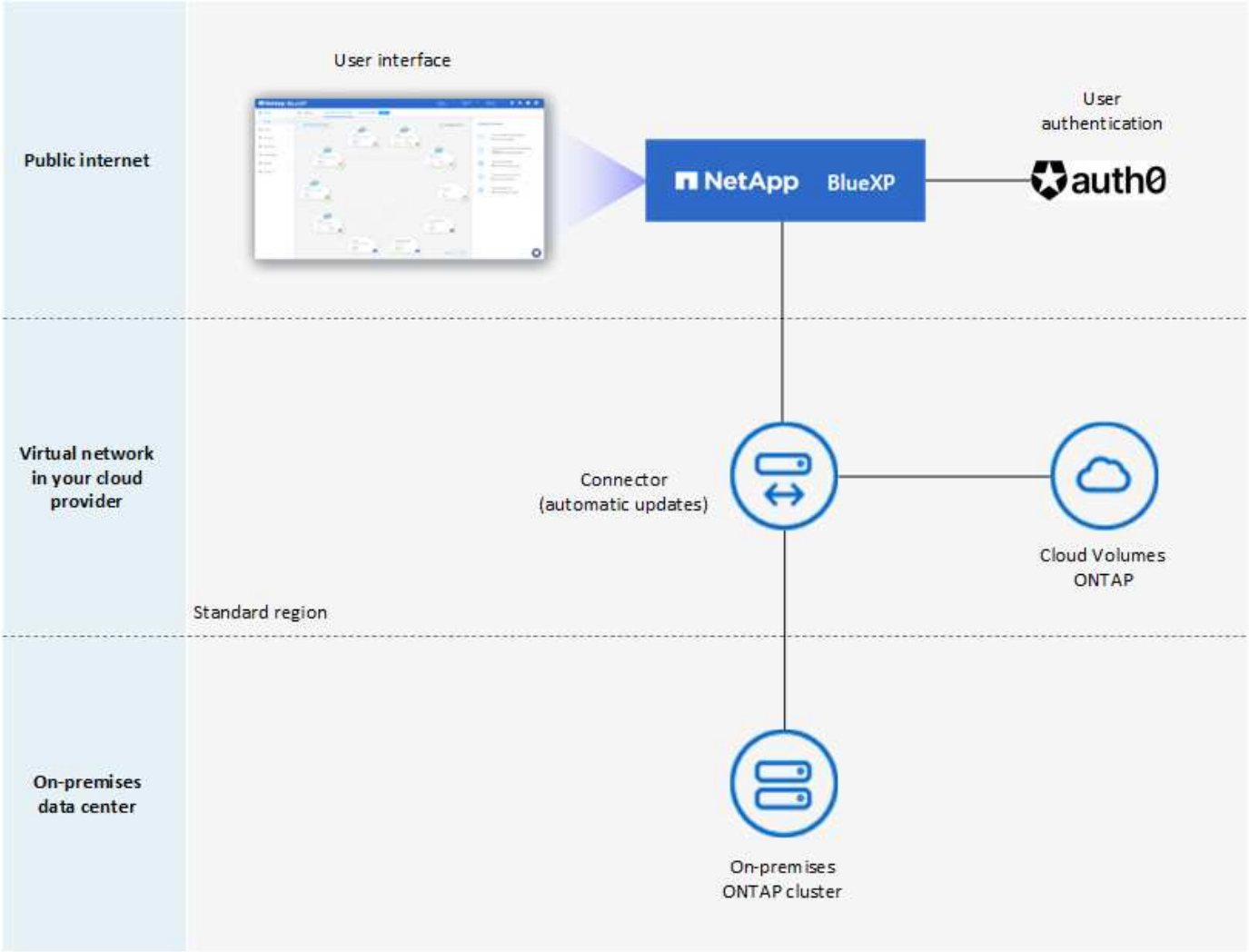
次の表に、これらのモードの比較を示します。

	標準モード	制限モード	プライベートモード
BlueXPの**SaaS**レイヤへの接続が必要ですか？	はい。	アウトバウンドのみ	いいえ
クラウドプロバイダへの接続が必要ですか？	はい。	はい、地域内です	○（リージョン内）（Cloud Volumes ONTAP を使用している場合）
コネクタの取り付け	BlueXP、クラウドマーケットプレイス、手動インストールから選択できます	クラウドマーケットプレイスまたは手動インストール	手動インストール
コネクタのアップグレード	NetApp Connectorソフトウェアの自動アップグレード	NetApp Connectorソフトウェアの自動アップグレード	手動アップグレードが必要です
UIアクセス	BlueXPのSaaSレイヤからアクセスします	コネクタVMからローカルに	コネクタVMからローカルに
APIエンドポイント	BlueXPのSaaSレイヤ	コネクタ	コネクタ
認証	SaaS経由（Auth0、NSSログイン、アイデンティティフェデレーションを使用	Auth0またはアイデンティティフェデレーションを使用してSaaSを介して	ローカルユーザ認証
ストレージサービスとデータサービス	すべてがサポートされています	多数サポートされています	いくつかサポートされています
ライセンスオプション	マーケットプレイスのサブスクリプションとBYOL	マーケットプレイスのサブスクリプションとBYOL	BYOL

これらのモードの詳細（サポートされるBlueXPの機能やサービスなど）については、以降のセクションで確認してください。

標準モード

次の図は、標準モードの配置の例です。



BlueXPは、標準モードで次のように機能します。

アウトバウンド通信

コネクタからBlueXP SaaSレイヤ、クラウドプロバイダが一般に公開しているリソース、および日常業務に欠かせないその他のコンポーネントへの接続が必要です。

- "コネクタがAWSで接続するエンドポイント"
- "コネクタがAzureで接続するエンドポイント"
- "コネクタがGoogle Cloudで接続するエンドポイント"

コネクタのサポートされている場所

標準モードでは、コネクタはクラウドまたはオンプレミスでサポートされます。

コネクタの取り付け

コネクタのインストールは、BlueXPのセットアップウィザード、AWSまたはAzure Marketplaceから実行できます。また、インストーラを使用して、データセンターまたはクラウドの自社のLinuxホストにコネクタを手動でインストールすることもできます。

コネクタのアップグレード

Connectorソフトウェアの自動アップグレードは、毎月更新されるBlueXPから利用できます。

ユーザインターフェイスアクセス

ユーザインターフェイスには、SaaSレイヤを通じて提供されるWebベースのコンソールからアクセスできます。

APIエンドポイント

次のエンドポイントに対してAPI呼び出しが実行されます。
https://cloudmanager.cloud.netapp.com

認証

認証は、BlueXPのクラウドサービスでAuth0またはNetApp Support Site （NSS）ログインを使用して行われます。アイデンティティフェデレーションを使用できます。

サポートされる**BlueXP**サービス

ユーザはすべてのBlueXPサービスを利用できます。

サポートされるライセンスオプション

MarketplaceのサブスクリプションとBYOLはStandardモードでサポートされますが、サポートされるライセンスオプションは、使用しているBlueXPサービスによって異なります。使用可能なライセンスオプションの詳細については、各サービスのドキュメントを参照してください。

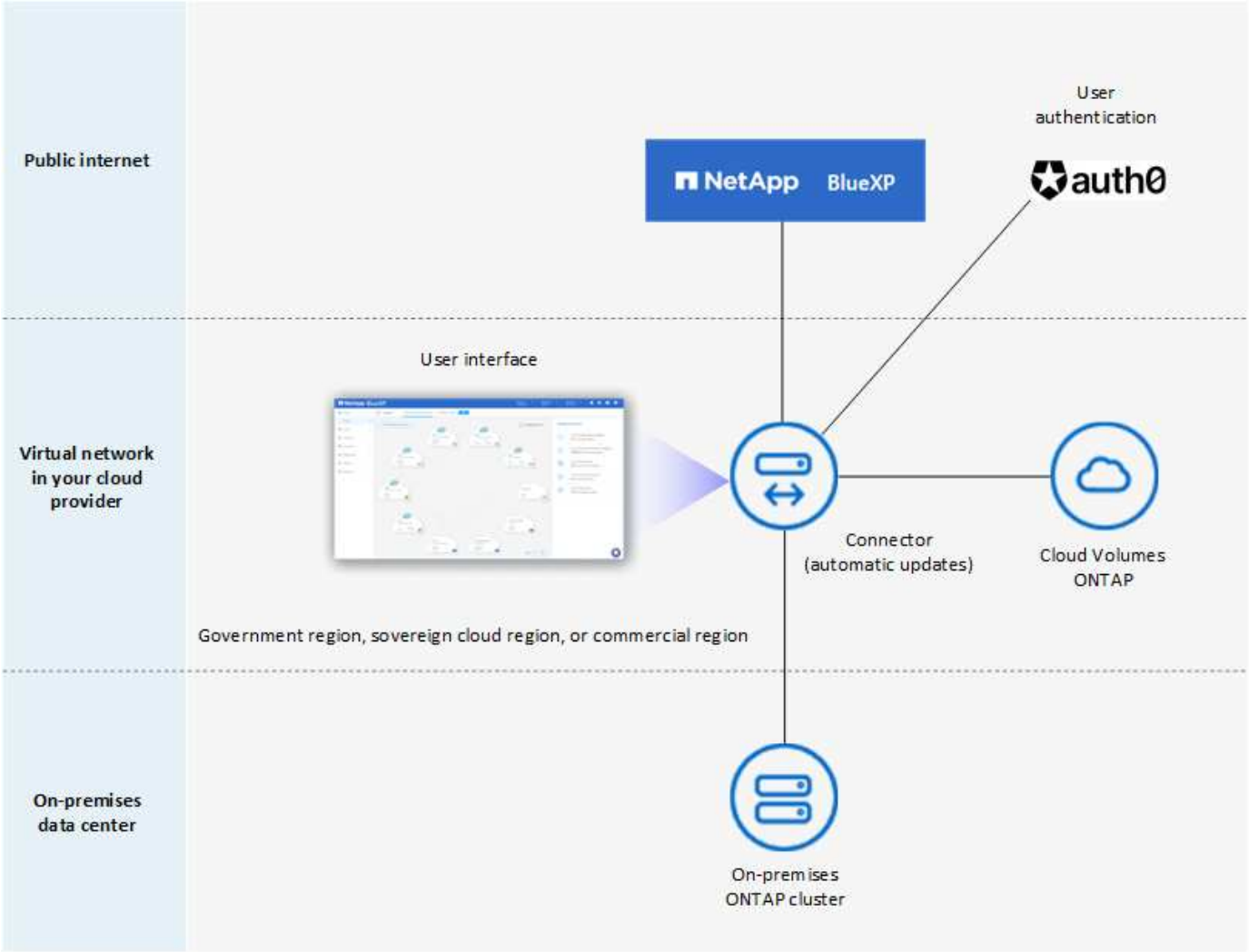
標準モードで開始する方法

にアクセスします "WebベースのBlueXPコンソール" 登録してください。

"標準モードを使用する方法について説明します"。

制限モード

次の図は、制限モードの配置の例です。



BlueXPは、制限モードでは次のように機能します。

アウトバウンド通信

BlueXPデータサービスの使用、コネクタの自動ソフトウェアアップグレードの有効化、Auth0ベースの認証の使用、課金用のメタデータ（Storage VM名、割り当て容量、ボリュームのUUID、タイプ、IOPS）の送信には、コネクタからBlueXP SaaSレイヤへのアウトバウンド接続が必要です。

SaaSレイヤのBlueXPでは、コネクタとの通信は開始されません。すべての通信はコネクタによって開始され、コネクタは必要に応じてSaaSレイヤとの間でデータを取得またはプッシュできます。

リージョン内のクラウドプロバイダリソースへの接続も必要です。

コネクタのサポートされている場所

制限モードでは、コネクタはクラウド（政府地域、主権地域、または商業地域）でサポートされます。

コネクタの取り付け

Connectorのインストールは、AWSまたはAzure Marketplaceから行うことも、手動で独自のLinuxホストにインストールすることもできます。

コネクタのアップグレード

Connectorソフトウェアの自動アップグレードは、毎月更新されるBlueXPから利用できます。

ユーザインターフェイスアクセス

ユーザーインターフェイスには、クラウドリージョンに導入されているコネクタ仮想マシンからアクセスできます。

APIエンドポイント

コネクタ仮想マシンに対してAPI呼び出しが実行されます。

認証

認証は、BlueXPのクラウドサービスを通じて、Auth0を使用して行われます。アイデンティティフェデレーションも使用できます。

サポートされる**BlueXP**サービス

BlueXPでは、制限モードで次のストレージサービスとデータサービスがサポートされます。

サポートされるサービス	注：
ONTAP 対応の Amazon FSX	フルサポート
Azure NetApp Files の特長	フルサポート
バックアップとリカバリ	制限モードの政府地域および商用地域でサポートされています。制限モードの主権領域ではサポートされていません。 制限モードでは、BlueXPのバックアップとリカバリでONTAPボリュームのデータのバックアップとリストアのみがサポートされます。 "ONTAPデータでサポートされるバックアップデスティネーションのリストを表示する" アプリケーションデータ、仮想マシンデータ、およびKubernetesデータのバックアップとリストアはサポートされていません。
分類	制限モードの政府機関地域でサポートされます。商用リージョンまたは制限モードのソブリンリージョンではサポートされていません。 次の制限事項が適用されます。 • OneDriveアカウント、SharePointアカウント、Googleドライブアカウントはスキャンできません。 • Microsoft Azure Information Protection（AIP）ラベル機能を統合できません。
Cloud Volumes ONTAP	フルサポート
デジタルウォレット	デジタルウォレットは、制限モードでサポートされている以下のライセンスオプションで使用できます。

サポートされるサービス	注：
オンプレミスの ONTAP クラスタ	コネクタを使用した検出とコネクタを使用しない検出（直接検出）の両方がサポートされます。 コネクタを備えたオンプレミスクラスタを検出した場合、アドバンストビュー（System Manager）はサポートされません。
レプリケーション	制限モードの政府機関地域でサポートされます。商用リージョンまたは制限モードのソブリンリージョンではサポートされていません。

サポートされるライセンスオプション

制限モードでは、次のライセンスオプションがサポートされます。

- マーケットプレイスのサブスクリプション（時間単位および年単位の契約）

  次の点に注意してください。

  - Cloud Volumes ONTAP では、容量単位のライセンスのみがサポートされます。
  - Azureでは、政府機関の地域との年間契約はサポートされていません。
- BYOL

  Cloud Volumes ONTAP の場合、BYOLでは容量単位のライセンスとノード単位のライセンスの両方がサポートされます。

制限モードの使用を開始する方法

BlueXPアカウントの作成時に制限モードを有効にする必要があります。

まだアカウントをお持ちでない場合は、手動でインストールしたコネクタまたはクラウドプロバイダのマーケットプレイスから作成したコネクタからBlueXPに初めてログインするときに、アカウントを作成して制限モードを有効にするように求められます。

すでにアカウントを持っていて、別のアカウントを作成する場合は、Tenancy APIを使用する必要があります。

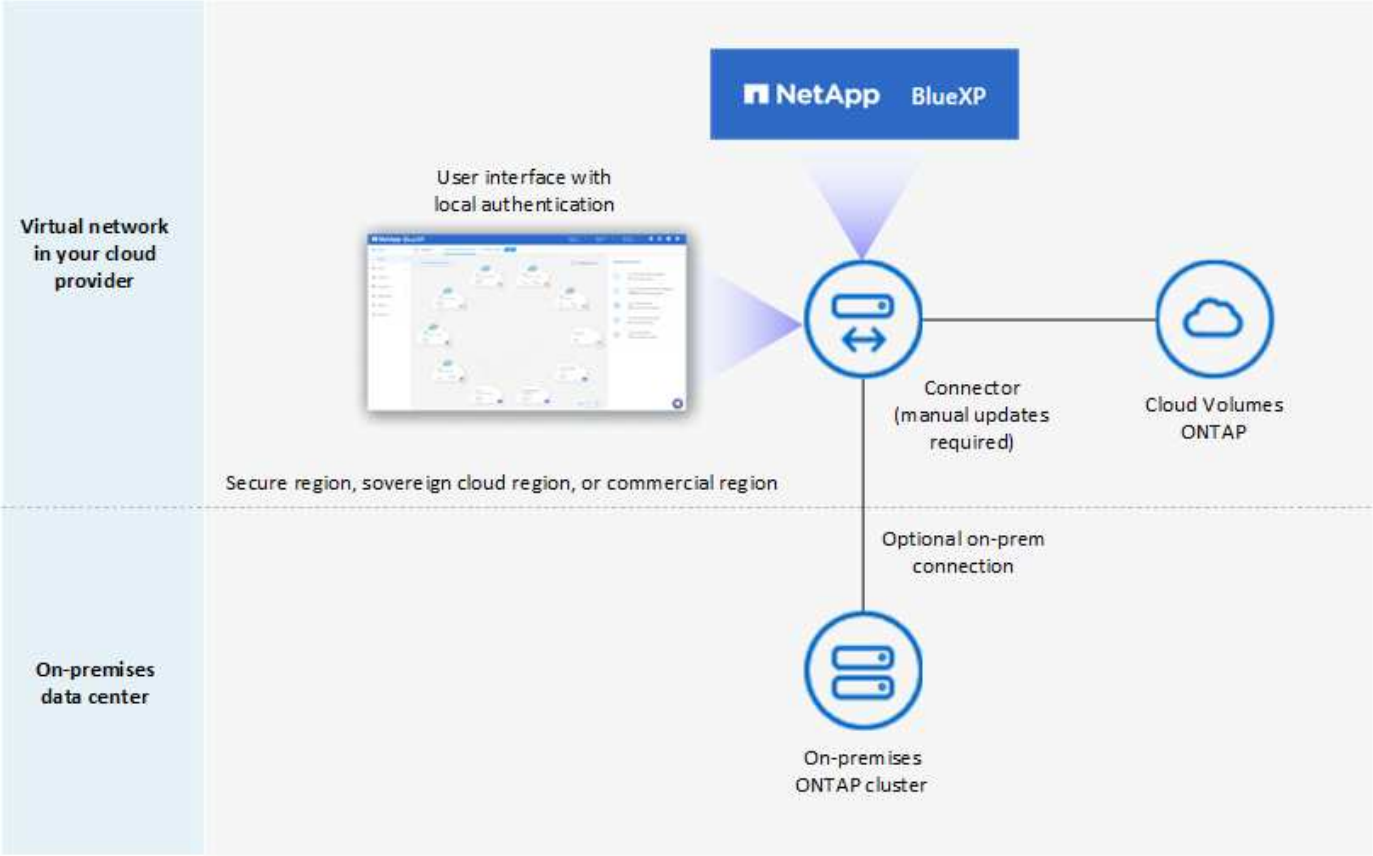
制限モードの設定は、BlueXPでアカウントが作成されたあとは変更できません。制限モードは後で有効にすることも、後で無効にすることもできません。アカウント作成時に設定する必要があります。

- "制限モードの使用を開始する方法について説明します"。
- "BlueXPアカウントを追加で作成する方法をご紹介します"。

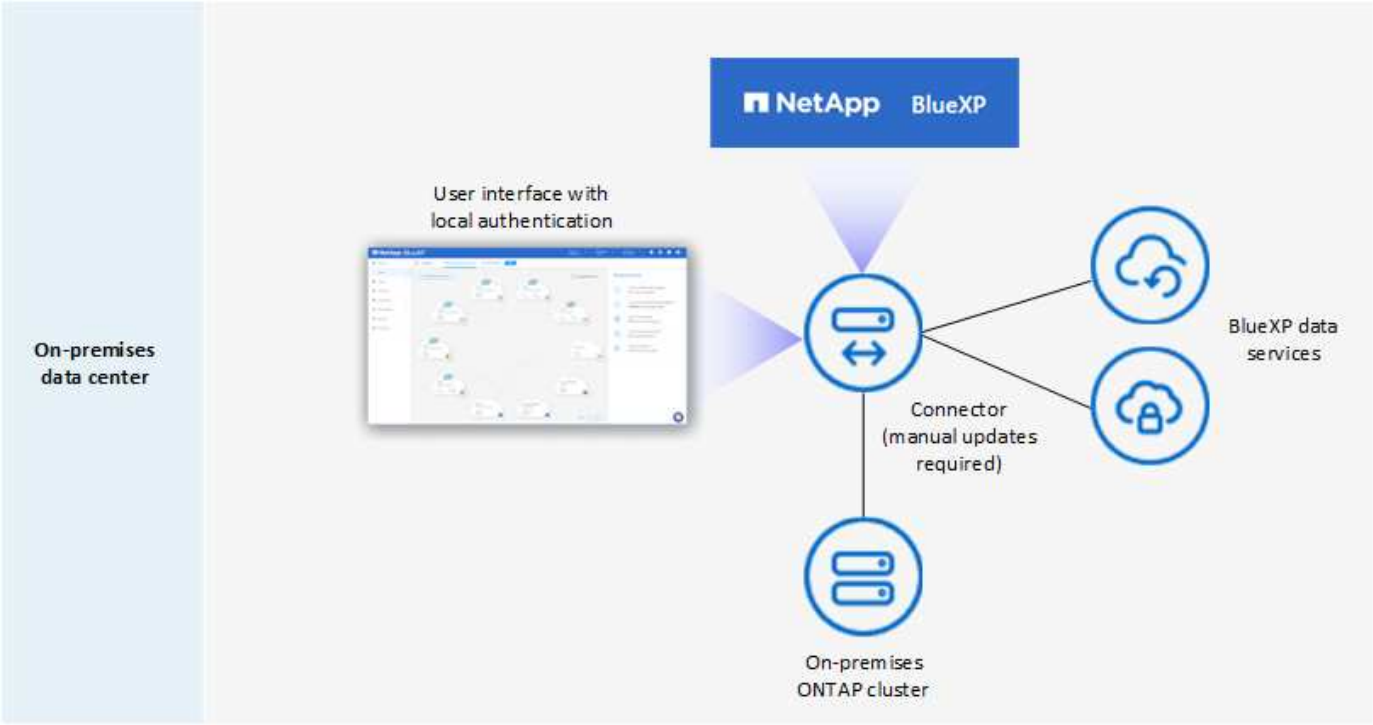
プライベートモード

プライベートモードでは、オンプレミスまたはクラウドにコネクタをインストールし、BlueXPを使用してハイブリッドクラウド全体のデータを管理できます。BlueXP SaaSレイヤへの接続はありません。

次の図は、コネクタをクラウドにインストールし、Cloud Volumes ONTAP とオンプレミスのONTAP クラスタの両方を管理するプライベートモードの導入例を示しています。



一方、2つ目の図はプライベートモードの環境の例を示しています。この環境では、コネクタをオンプレミスにインストールし、オンプレミスのONTAP クラスタを管理し、サポートされているBlueXPデータサービスへのアクセスを提供します。



BlueXPはプライベートモードで次のように機能します。

アウトバウンド通信

BlueXP SaaSレイヤへのアウトバウンド接続は必要ありません。すべてのパッケージ、依存関係、および必須コンポーネントはコネクタとともにパッケージ化され、ローカルマシンから提供されます。クラウドプロバイダの一般に利用可能なリソースへの接続は、Cloud Volumes ONTAP を導入する場合にのみ必要です。

コネクタのサポートされている場所

プライベートモードでは、コネクタはクラウドまたはオンプレミスでサポートされます。

コネクタの取り付け

コネクタの手動インストールは、クラウドまたはオンプレミスの独自のLinuxホストでサポートされています。

コネクタのアップグレード

コネクタソフトウェアを手動でアップグレードする必要があります。コネクターソフトウェアは、未定義の間隔でNetApp Support Site にパブリッシュされます。

ユーザインターフェイスアクセス

ユーザインターフェイスには、クラウドリージョンまたはオンプレミスに導入されているコネクタからアクセスできます。

APIエンドポイント

コネクタ仮想マシンに対してAPI呼び出しが実行されます。

認証

認証は、ローカルユーザの管理とアクセスを通じて提供されます。BlueXPのクラウドサービスでは認証が行われません。

クラウド環境でサポートされる**BlueXP**サービス

BlueXPでは、コネクタがクラウドにインストールされている場合、プライベートモードで次のストレージサービスとデータサービスがサポートされます。

サポートされるサービス	注：
バックアップとリカバリ	AWSとAzureの商用リージョンでサポートされます。 Google Cloudまたはではサポートされていません "AWSシークレットクラウド"、 "AWSのトップシークレットクラウド"または "Azure IL6" プライベートモードでは、BlueXPのバックアップとリカバリでONTAPボリュームのデータのバックアップとリストアのみがサポートされます。 "ONTAPデータでサポートされるバックアップデスティネーションのリストを表示する" アプリケーションデータ、仮想マシンデータ、およびKubernetesデータのバックアップとリストアはサポートされていません。

サポートされるサービス	注：
Cloud Volumes ONTAP	インターネットにアクセスできないため、自動ソフトウェアアップグレードとAutoSupportの機能は使用できません。
デジタルウォレット	デジタルウォレットは、プライベートモードでサポートされている以下のライセンスオプションで使用できます。
オンプレミスの ONTAP クラスタ	クラウド（コネクタがインストールされている場所）からオンプレミス環境への接続が必要 コネクタなしの検出（直接検出）はサポートされていません。

オンプレミス環境で**BlueXP**サービスをサポート

BlueXPでは、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、プライベートモードで次のストレージサービスとデータサービスがサポートされます。

サポートされるサービス	注：
バックアップとリカバリ	プライベートモードでは、BlueXPのバックアップとリカバリでONTAPボリュームのデータのバックアップとリストアのみがサポートされます。 "ONTAPボリュームデータでサポートされるバックアップデスティネーションのリストを表示する" アプリケーションデータ、仮想マシンデータ、およびKubernetesデータのバックアップとリストアはサポートされていません。
分類	• ローカルで検出できるデータソースは、サポートされているデータソースだけです。 "ローカルで検出できるソースを表示します" • アウトバウンドインターネットアクセスを必要とする機能はサポートされていません。 "機能の制限事項を確認します"
デジタルウォレット	デジタルウォレットは、プライベートモードでサポートされている以下のライセンスオプションで使用できます。
オンプレミスの ONTAP クラスタ	コネクタなしの検出（直接検出）はサポートされていません。
レプリケーション	フルサポート

サポートされるライセンスオプション

プライベートモードではBYOLのみがサポートされます。

Cloud Volumes ONTAP のBYOLでは、ノードベースのライセンスのみがサポートされます。容量単位のライセンスはサポートされていません。アウトバウンドのインターネット接続を使用できないため、Cloud Volumes ONTAP ライセンスファイルをBlueXPのデジタルウォレットに手動でアップロードする必要があります。

"BlueXPデジタルウォレットにライセンスを追加する方法をご紹介します"

プライベートモードを開始する方法

プライベートモードは、NetApp Support Site から「オフライン」インストーラをダウンロードすることで利用できます。

"プライベートモードの使用を開始する方法について説明します"。

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

サービスと機能の比較

次の表は、制限モードとプライベートモードでサポートされるBlueXPのサービスと機能を簡単に特定するのに役立ちます。

一部のサービスは制限付きでサポートされる場合があります。これらのサービスが制限モードおよびプライベートモードでどのようにサポートされるかの詳細については、上記の項を参照してください。

製品エリア	**BlueXP**のサービスまたは機能	制限モード	プライベートモード
作業環境 表の次の部分には、BlueXPキャンバスでの作業環境管理のサポートが表示されます。BlueXPのバックアップとリカバリでサポートされるバックアップ先を示すわけではありません。	ONTAP 対応の Amazon FSX	はい。	いいえ
	Amazon S3	いいえ	いいえ
	Azure Blob の略	いいえ	いいえ
	Azure NetApp Files の特長	はい。	いいえ
	Cloud Volumes ONTAP	はい。	はい。
	Cloud Volumes Service for Google Cloud	いいえ	いいえ
	Google クラウドストレージ	いいえ	いいえ
	Kubernetes クラスタ	いいえ	いいえ
	オンプレミスの ONTAP クラスタ	はい。	はい。
	E シリーズ	いいえ	いいえ
	StorageGRID	いいえ	いいえ

製品エリア	**BlueXP**のサービスまたは機能	制限モード	プライベートモード
* サービス *	バックアップとリカバリ	はい。 "ONTAPボリュームデータでサポートされるバックアップデスティネーションのリストを表示する"	はい。 "ONTAPボリュームデータでサポートされるバックアップデスティネーションのリストを表示する"
	分類	はい。	はい。
	クラウド運用	いいえ	いいえ
	コピーと同期	いいえ	いいえ
	デジタルアドバイザ	いいえ	いいえ
	デジタルウォレット	はい。	はい。
	ディザスタリカバリ	いいえ	いいえ
	経済効率	いいえ	いいえ
	エッジキャッシュ	いいえ	いいえ
	移行レポート	いいえ	いいえ
	運用の耐障害性	いいえ	いいえ
	ランサムウェアからの保護	いいえ	いいえ
	レプリケーション	はい。	はい。
	持続可能性	いいえ	いいえ
	階層化	いいえ	いいえ
	ボリュームキャッシュ	いいえ	いいえ
機能	クレデンシャル	はい。	はい。
	NSSアカウント	はい。	いいえ
	通知	はい。	いいえ
	検索	はい。	いいえ
	タイムライン	はい。	はい。

標準モードで開始します

スタートアップワークフロー（標準モード）

BlueXPを標準モードで使い始めるには、BlueXPコンソールのネットワークを準備し、サインアップしてアカウントを作成し、必要に応じてコネクタを作成し、BlueXPにサブスクライブします。

標準モードでは、Webベースのコンソールからクラウドサービスとして BlueXPにアクセスできます。開始する前に、次のことを理解しておく必要があります。 "BlueXPのアカウント"、 "コネクタ"および "導入モード

"。

1 **"BlueXPコンソールを使用するためのネットワークの準備"**

BlueXPコンソールにアクセスするコンピュータは、いくつかの管理タスクを実行するために特定のエンドポイントに接続する必要があります。ネットワークでアウトバウンドアクセスが制限されている場合は、これらのエンドポイントが許可されていることを確認する必要があります。

2 **"サインアップしてアカウントを作成します"**

にアクセスします "BlueXPコンソール" 登録してください。アカウントを作成するオプションが表示されますが、既存のアカウントに招待されている場合は、この手順を省略できます。

これでログインし、デジタルアドバイザ、Amazon FSx for ONTAP 、Azure NetApp Files など、複数のBlueXPサービスの使用を開始できます。 "コネクタなしでできることを学びます"。

3 コネクタを作成します

BlueXPの使用を開始するためにコネクタは必要ありませんが、コネクタを作成してBlueXPのすべての機能とサービスを活用することができます。このコネクタは、BlueXPで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するためのネットアップのソフトウェアです。

BlueXPアカウント管理者は、クラウドまたはオンプレミスのネットワークにコネクタを作成できます。

- "コネクタが必要になる状況とその方法については、こちらをご覧ください 仕事"
- "AWS でコネクタを作成する方法について説明します"
- "Azure でコネクタを作成する方法について説明します"
- "Google Cloud でコネクタを作成する方法について説明します"
- "オンプレミスでコネクタを作成する方法について説明します"

BlueXPサービスを使用してGoogle Cloudのストレージとデータを管理する場合は、コネクタがGoogle Cloudで実行されている必要があります。

4 **"BlueXPにサブスクライブします"**

クラウドプロバイダのマーケットプレイスからBlueXPにサブスクライブして、BlueXPサービスの料金を時間単位（PAYGO）または年間契約でお支払いください。

BlueXPコンソールを使用するためのネットワークの準備

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、いくつかの管理タスクを実行する際に複数のエンドポイントに通信します。BlueXPコンソールにアクセスするコンピュータは、これらのエンドポイントに接続する必要があります。

これらのエンドポイントは、BlueXPコンソールから特定の操作を実行するときに、ユーザのコンピュータからアクセスされます。また、コネクタや特定のBlueXPサービスのネットワーク要件も参照してください。詳

細については、このページの最後にある関連リンクを参照してください。

エンドポイント	目的
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	BlueXPのWebベースのコンソールを使用すると、Webブラウザからこれらの URLにアクセスできます。
https://aiq.netapp.com	BlueXP Digital Advisorにアクセスするには必要です。
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 ） • 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 ）	BlueXPからAWSにコネクタを導入する場合に必要です。正確なエンドポイントは、コネクタを配置するリージョンによって異なります。 "詳細については、AWS のマニュアルを参照してください。"
https://management.azure.com https://login.microsoftonline.com	ほとんどのAzureリージョンでBlueXPからコネクタを導入する場合に必要です。
https://management.microsoftazure.de https://login.microsoftonline.de	Azureドイツ地域でBlueXPからコネクタを導入する場合に必要です。
https://management.usgovcloudapi.net https://login.microsoftonline.com	Azure US Govリージョンで BlueXPからコネクタを導入する場合に必要です。
https://www.googleapis.com	Google CloudでBlueXPからConnectorを展開するために必要です。
https://signin.b2c.netapp.com	NetApp Support Site (NSS)の資格情報を更新するか、新しいNSS資格情報をBlueXPに追加する必要があります。
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Webブラウザはこれらのエンドポイントに接続して、BlueXPを介した集中型ユーザ認証を行います。
https://widget.intercom.io	製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。

これらのエンドポイント以外にも、日常業務のために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アクセスがコネクタにあることを確認する必要があります。これらのエンドポイントのリストは、次のセクションのリンクに従って確認できます。

関連リンク

- コネクタのネットワークを準備します
  - "AWSネットワークをセットアップする"

- "Azureネットワークをセットアップする"
- "Google Cloudネットワークをセットアップする"
- "オンプレミスネットワークをセットアップする"

- BlueXPサービスのネットワークを準備

  各BlueXPサービスのドキュメントを参照してください。

  "BlueXPのマニュアル"

BlueXPにサインアップします

BlueXPにはWebベースのコンソールからアクセスできます。BlueXPの利用を開始するには、まず既存のNetApp Support Site クレデンシャルを使用するか、ネットアップクラウドログインアカウントを作成して登録します。

このタスクについて

次のいずれかのオプションを使用して、BlueXPにサインアップできます。

- 既存のNetApp Support Site （NSS）のクレデンシャルを必要に応じて変更
- Eメールアドレスとパスワードを指定してネットアップクラウドにログインします

どちらのオプションも連携接続をサポートしているため、社内ディレクトリのクレデンシャルを使用してシングルサインオンを実行できます（フェデレーテッドアイデンティティ）。フェデレーション接続は、サインアップ後に設定できます。 "BlueXPでアイデンティティフェデレーションを使用する方法をご紹介します"。

手順

1. Webブラウザを開き、にアクセスします "BlueXPコンソール"
2. NetApp Support Site アカウントをお持ちの場合は、*ログイン*ページでNSSアカウントに関連付けられているメールアドレスを直接入力してください。

   NSSアカウントをお持ちの場合は、サインアップページをスキップできます。この初回ログインの一環として、BlueXPがサインアップします。

3. NSSアカウントをお持ちでなく、ネットアップクラウドログインを作成して登録する場合は、*[Sign Up]*を選択します。
4. [Sign Up]ページで、ネットアップクラウドログインの作成に必要な情報を入力します。

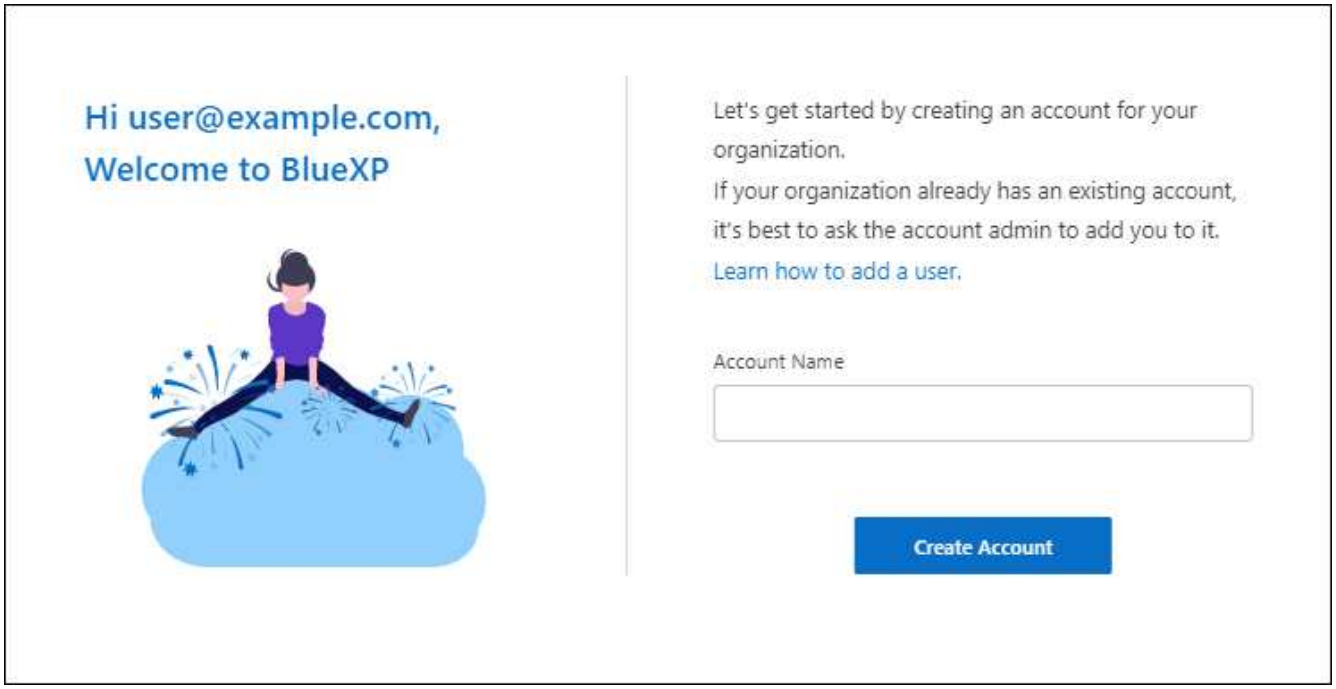
   サインアップフォームでは、英語の文字のみを使用できます。

5. プロンプトが表示されたら、エンドユーザライセンス契約を確認し、条件に同意します。
6. [ようこそ*]ページで、アカウントの名前を入力します。

   すでにアカウントをお持ちで参加をご希望の場合は、BlueXPを終了して所有者にアカウントとの関連付けを依頼してください。オーナーが追加されると、ログインできるようになり、アカウントにアクセスできるようになります。 "既存のアカウントにメンバーを追加する方法について説明します"。

   アカウントは、ネットアップのアイデンティティプラットフォームにおける最上位の要素です。ユーザ、

ロール、権限、作業環境を追加および管理できます。



7. 「 * アカウントの作成 * 」を選択します。

結果

これでBlueXPログインとアカウントが作成されました。ほとんどの場合、次の手順では、BlueXPのサービスをハイブリッドクラウド環境に接続するコネクタを作成します。

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"

エンドポイント	目的
\ 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"。

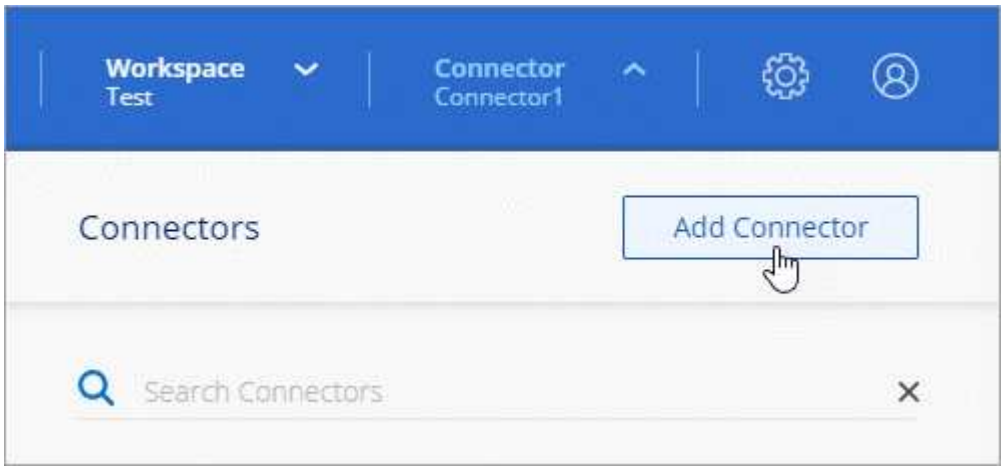
作業を開始する前に

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"。

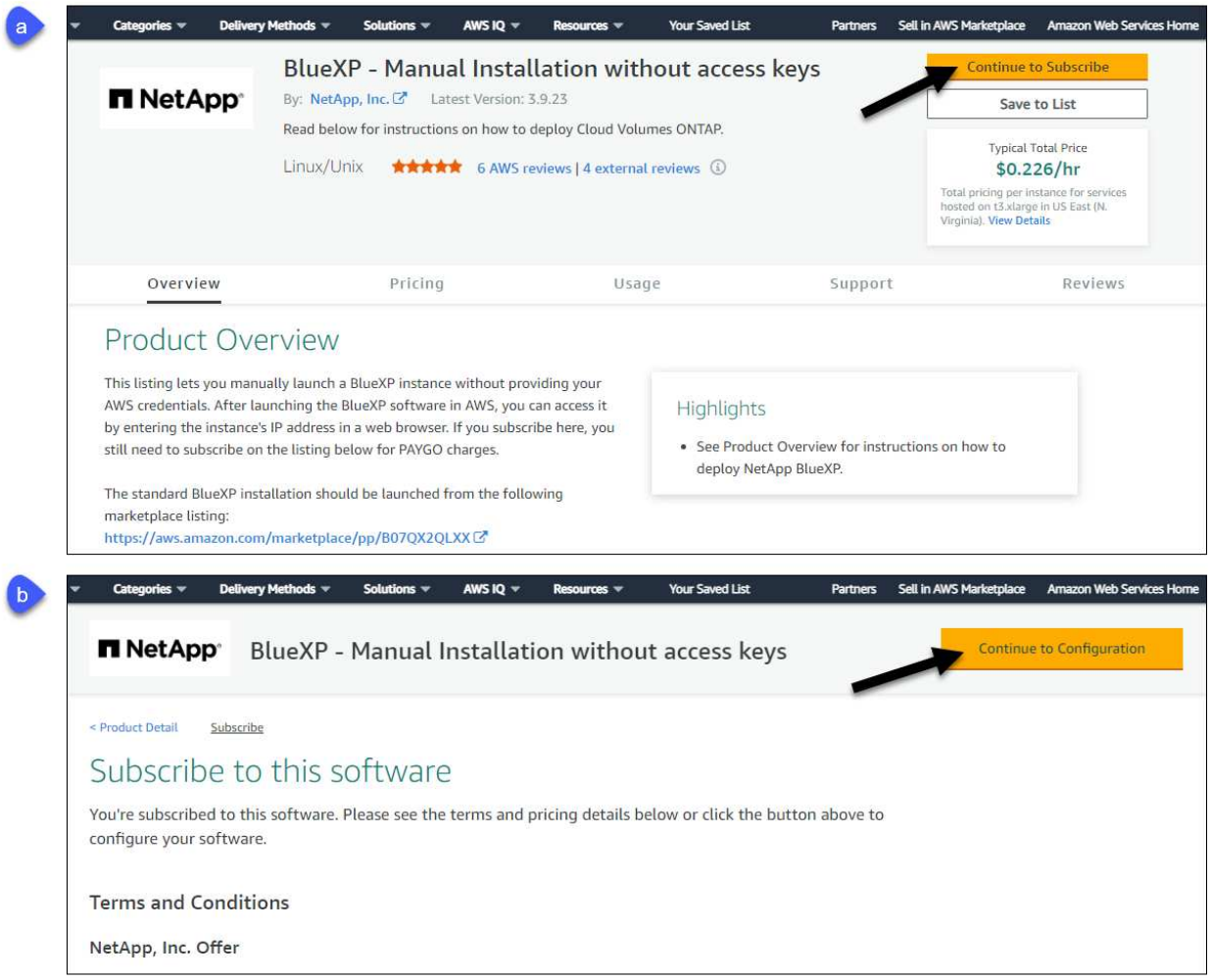
作業を開始する前に

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。

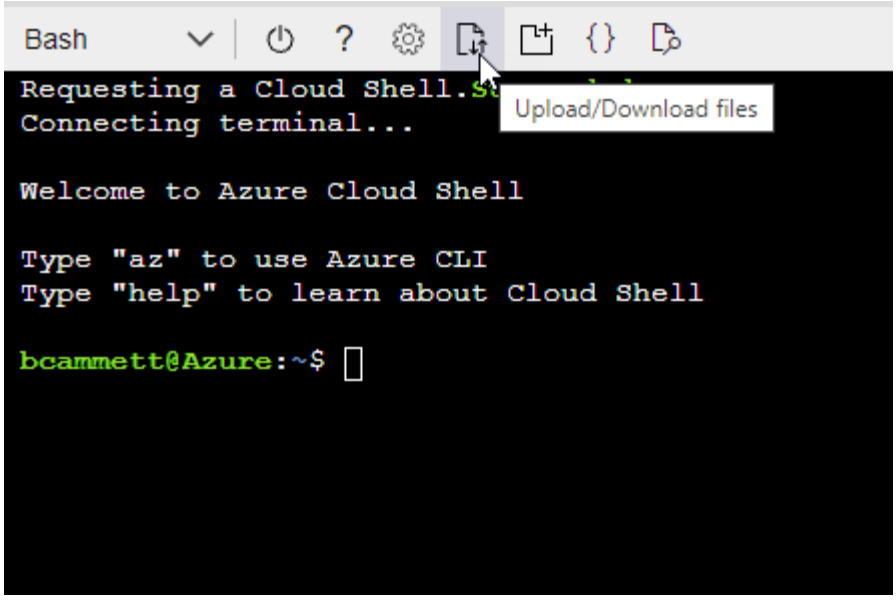
   - 例 *

```
"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。

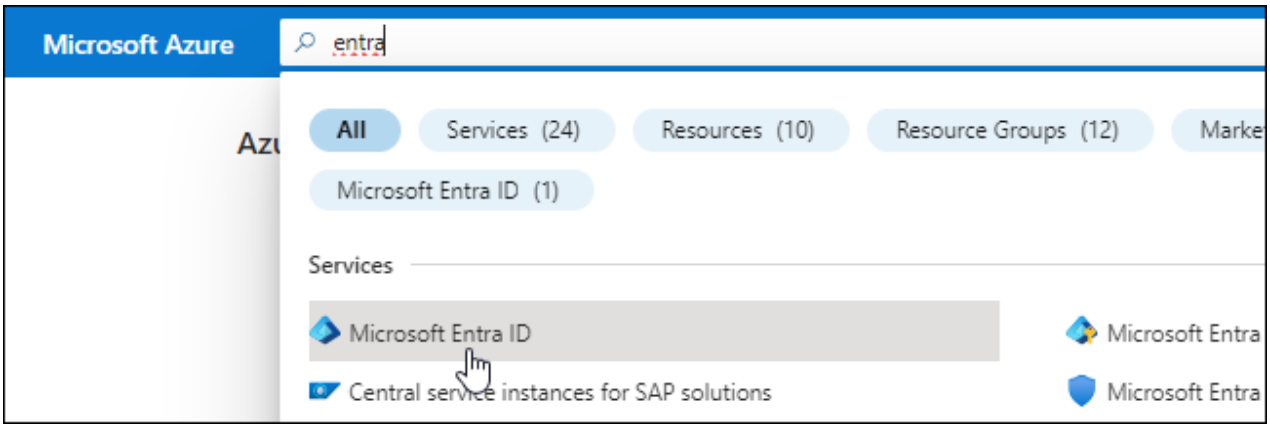
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。

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。

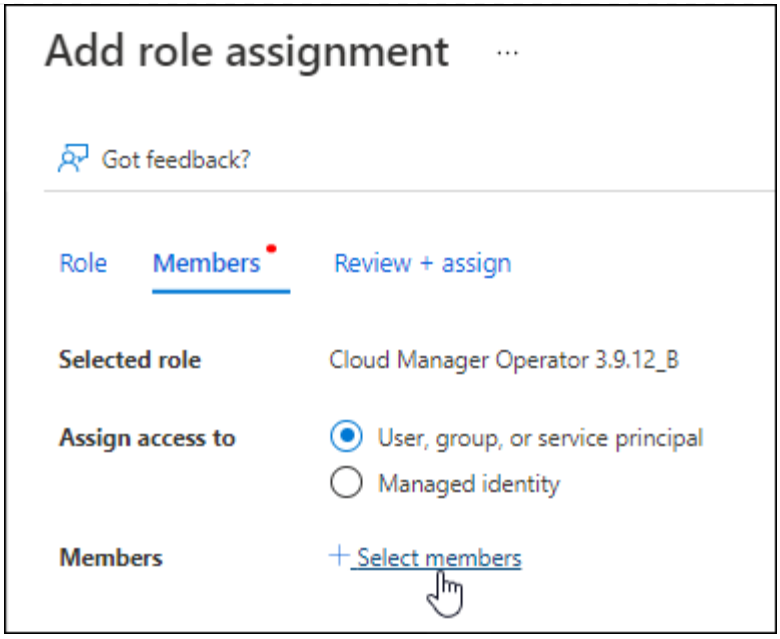


3. メニューで*アプリ登録*を選択します。
4. [New registration]*を選択します。
5. アプリケーションの詳細を指定します。
   - * 名前 * ：アプリケーションの名前を入力します。
   - アカウントの種類:アカウントの種類を選択します(すべてのアカウントはBlueXPで動作します)。
   - * リダイレクト URI *: このフィールドは空白のままにできます。
6. [*Register] を選択します。

   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。

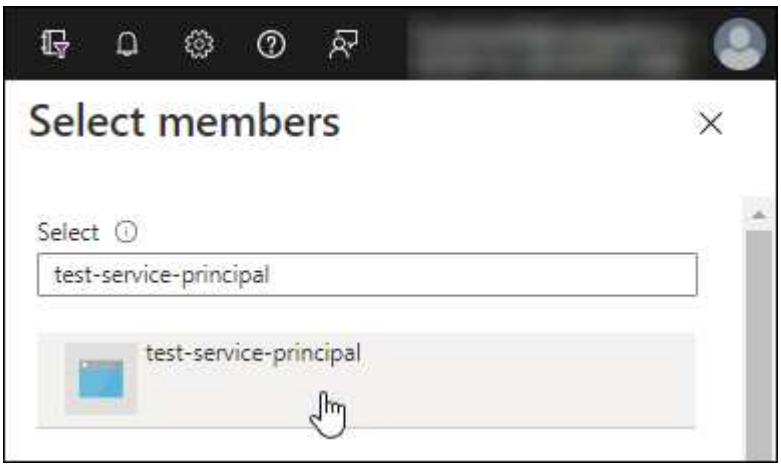
アプリケーションにカスタムロールを割り当てます

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。

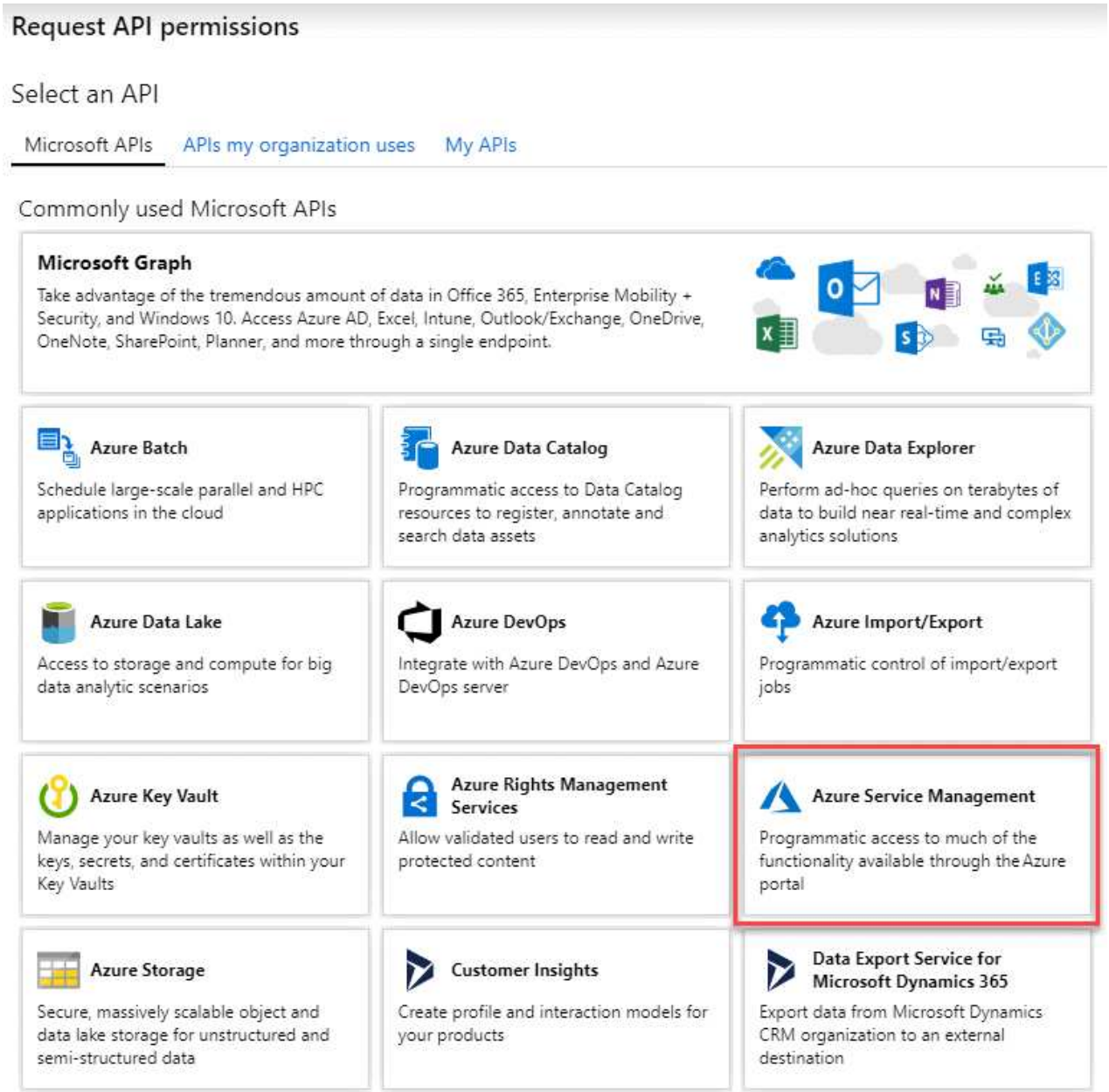
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

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。

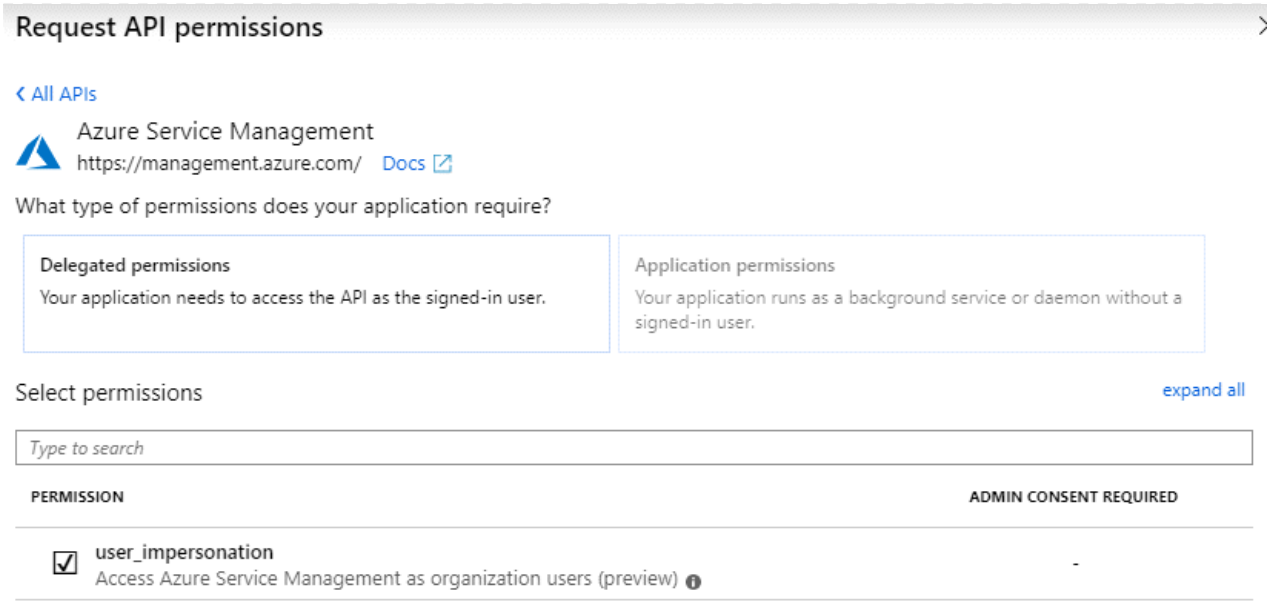
Windows Azure Service Management API 権限を追加します

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。

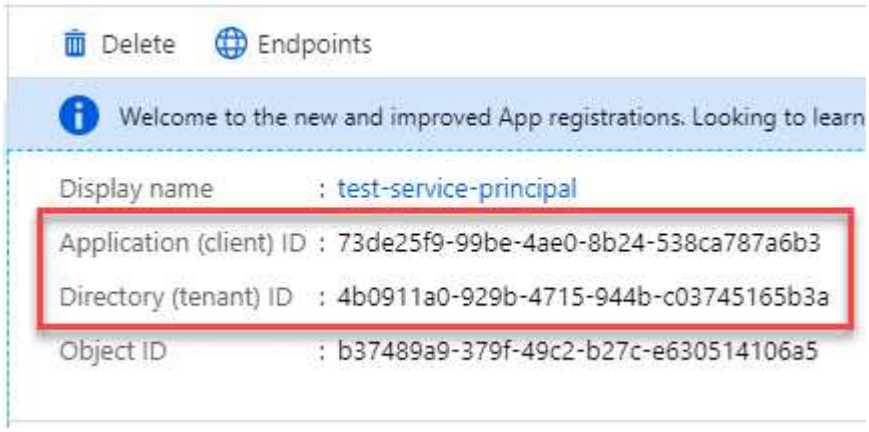


4. を選択し、[Add permissions]*を選択します。



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。

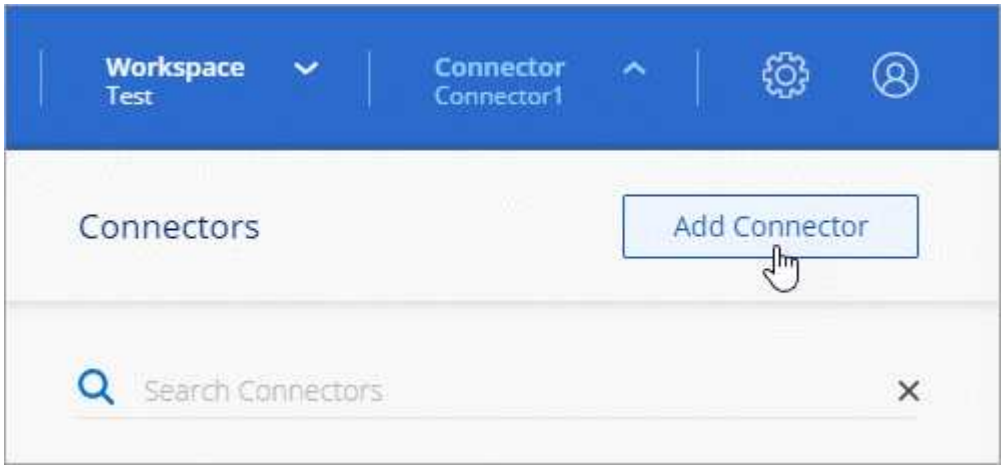
  "AzureでLinux VMに接続する方法について説明します"

- 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。

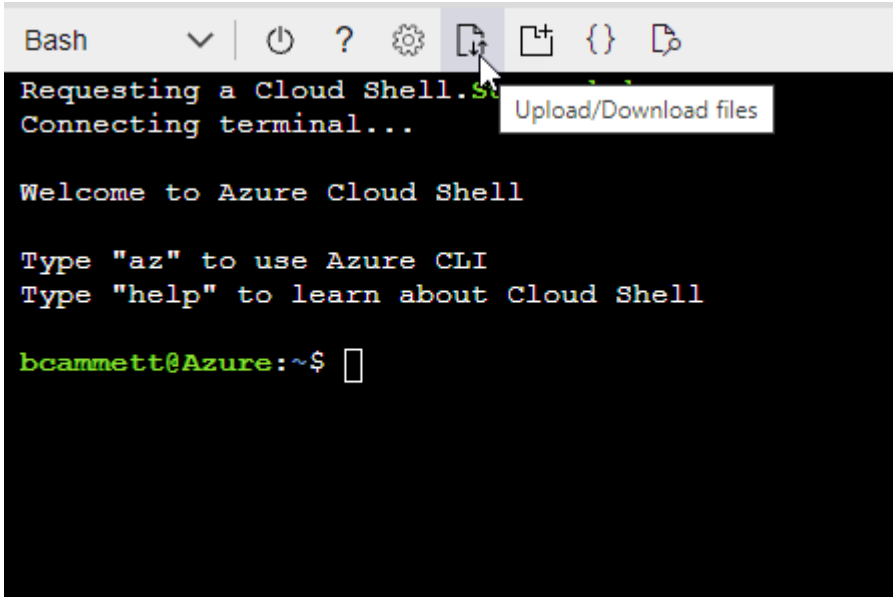
   - 例 *

```
"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

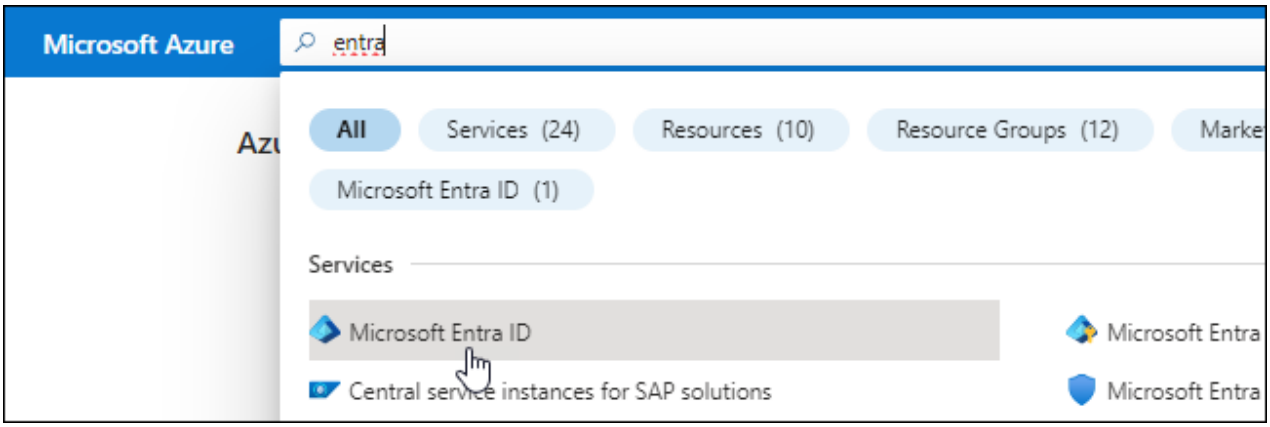
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。

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。

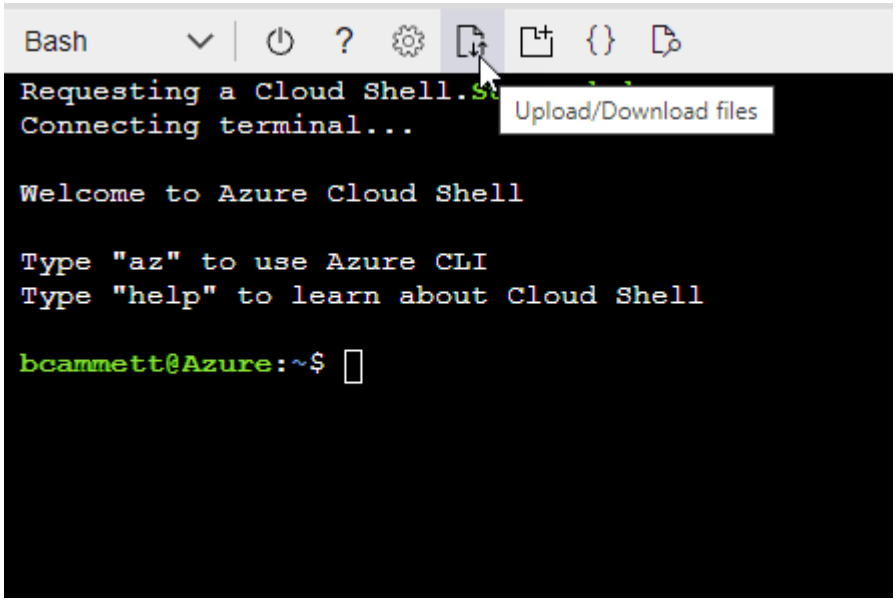
   - 例 *

```
"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
```

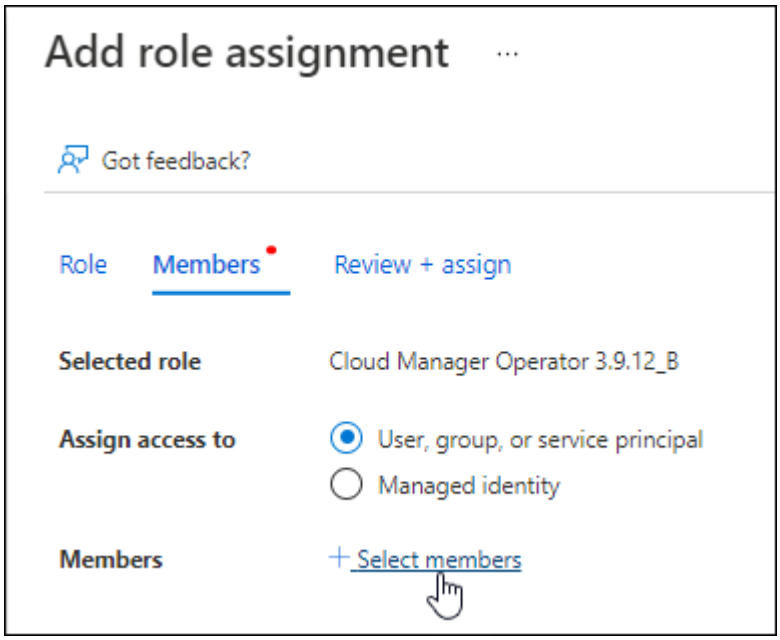
   これで、Connector仮想マシンに割り当てることができるBlueXP Operatorというカスタムロ

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。

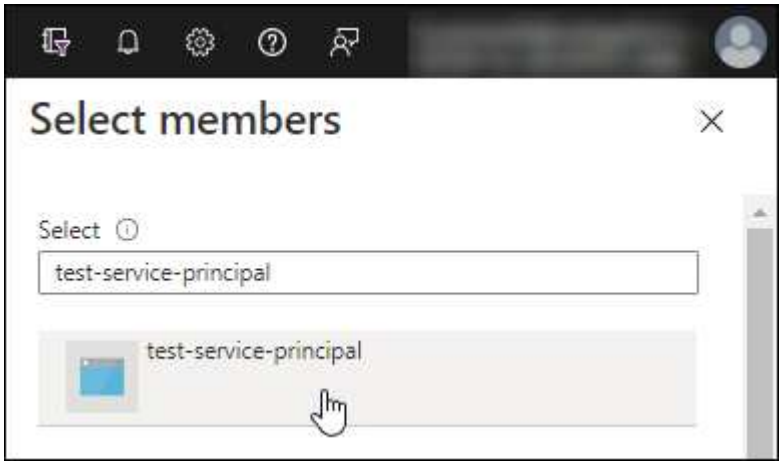
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。

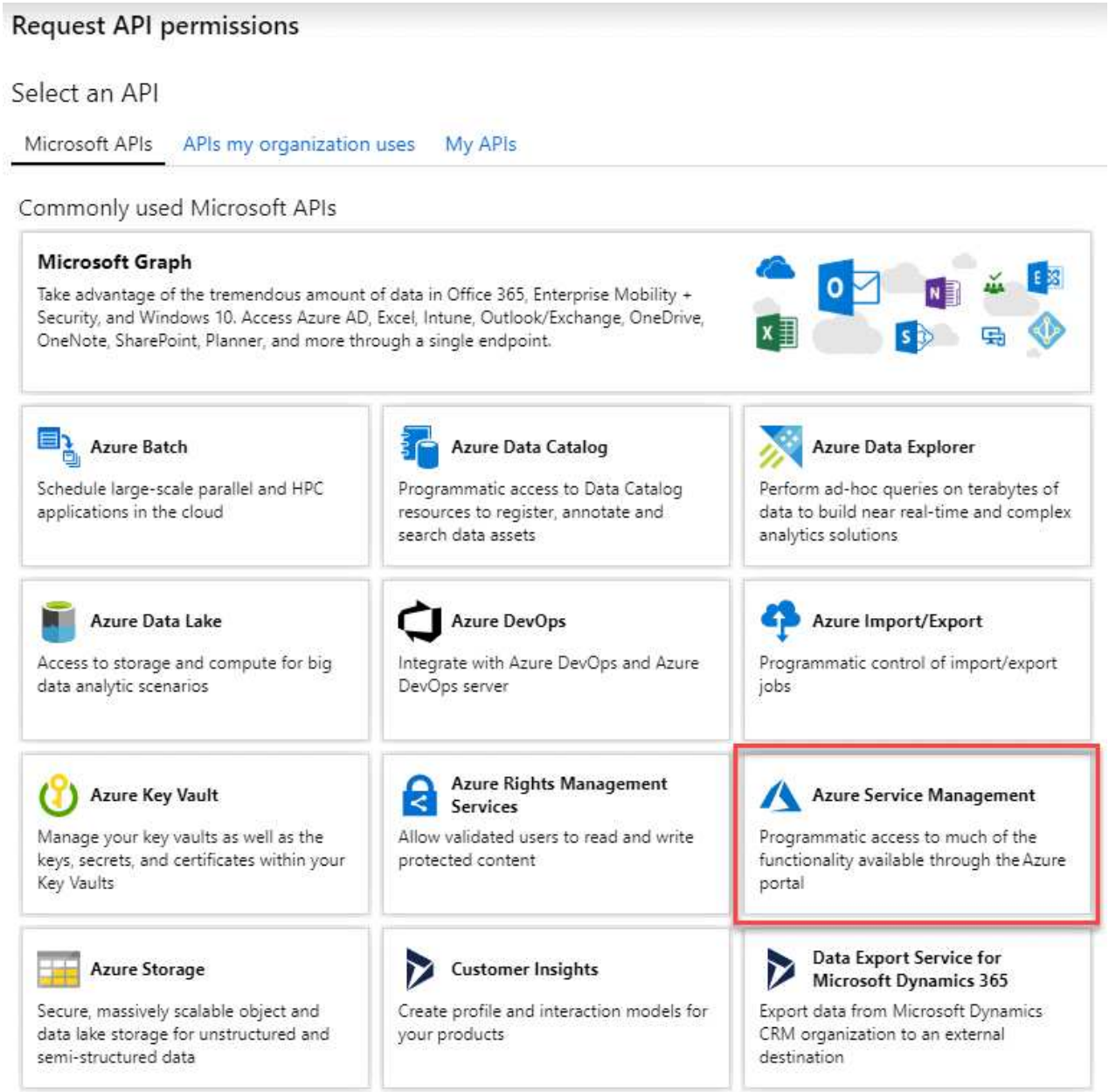
f. [Review + Assign]*を選択します。

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。

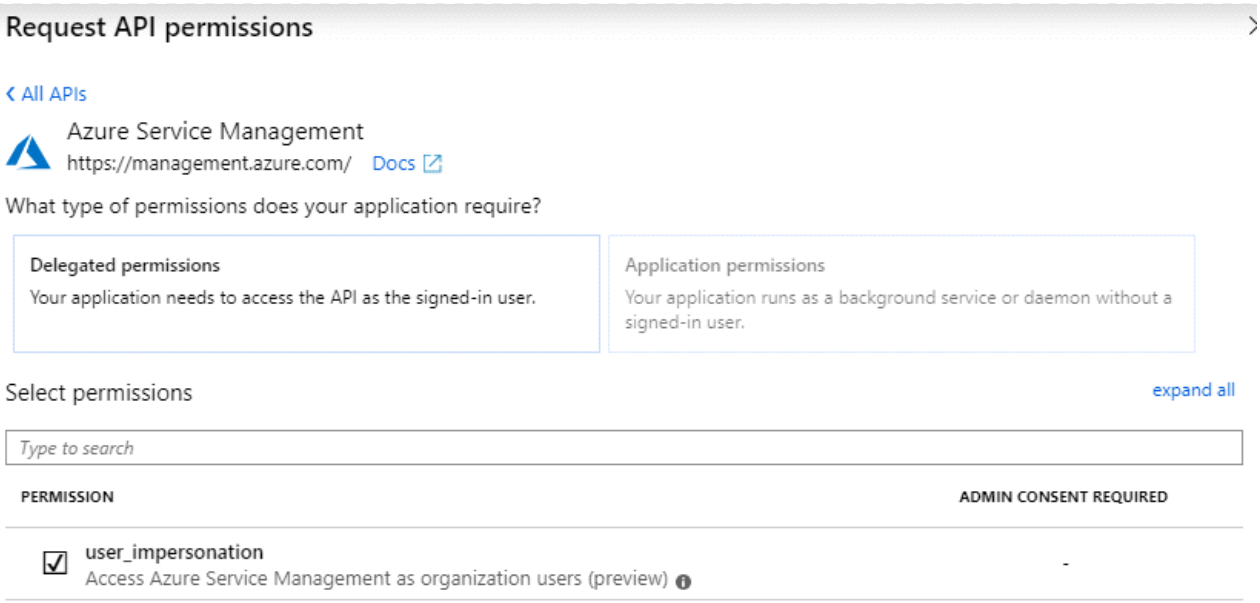
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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。

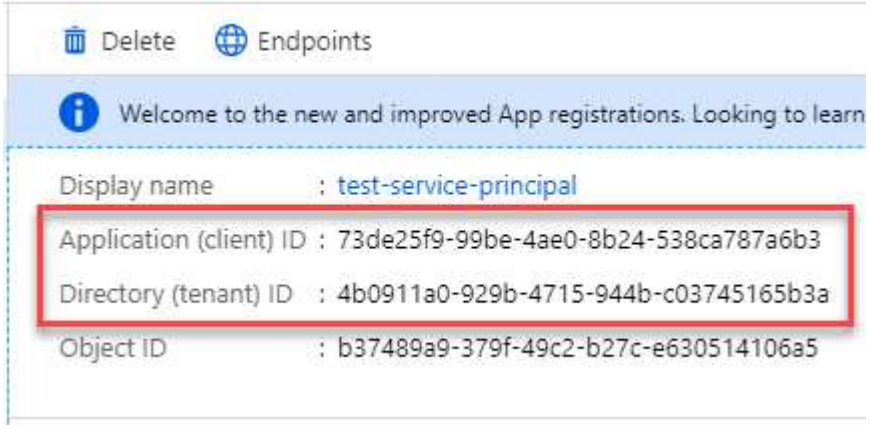


4. を選択し、[Add permissions]*を選択します。



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。

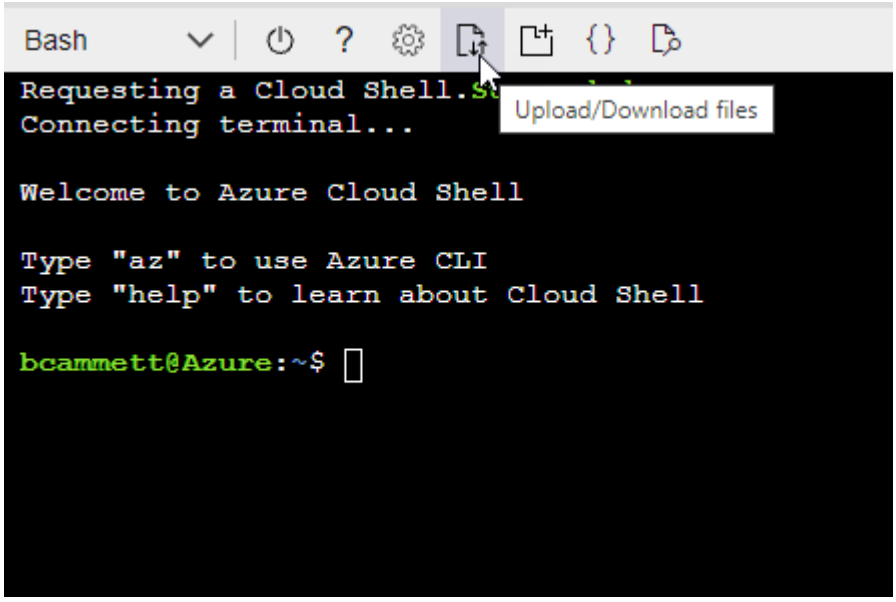
   - 例 *

```
"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

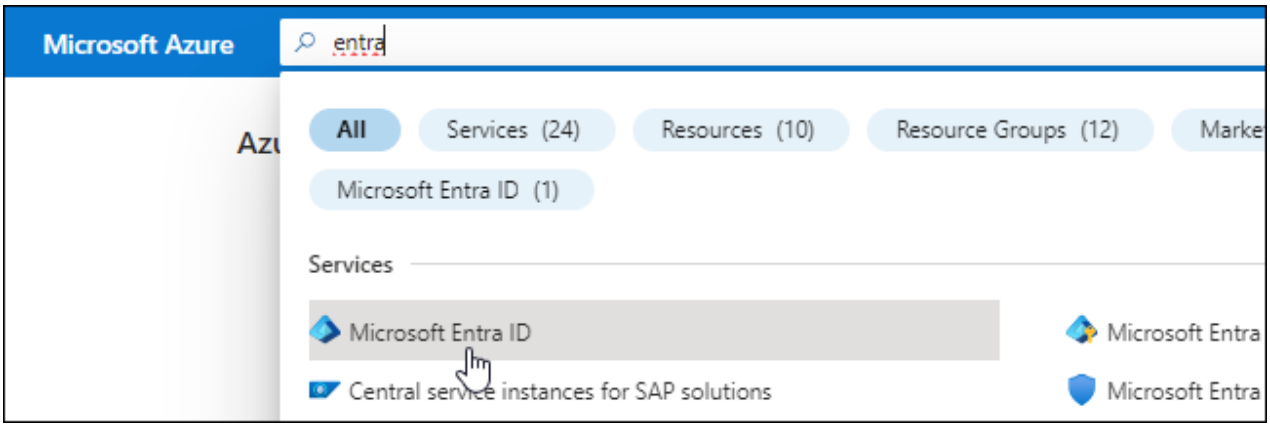
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。

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。

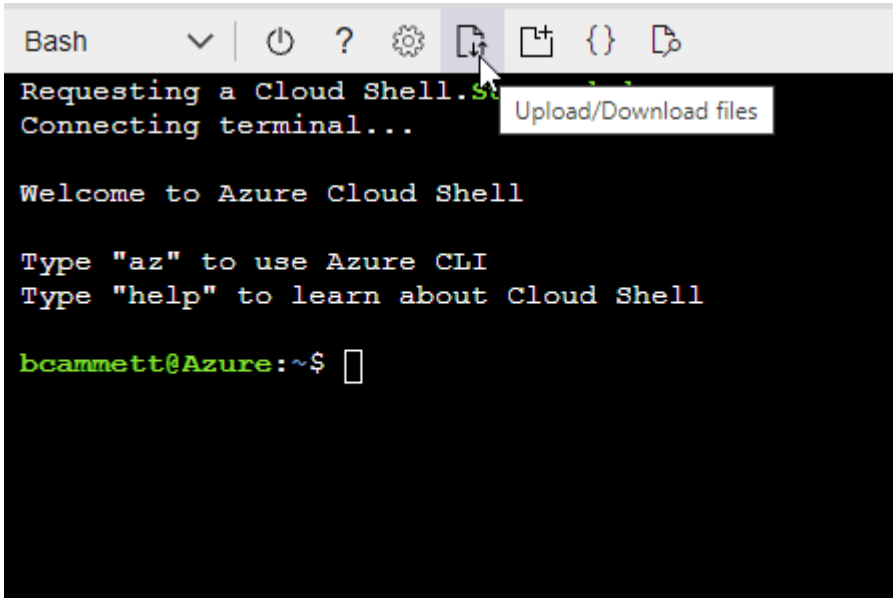
   - 例 *

```
"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
```

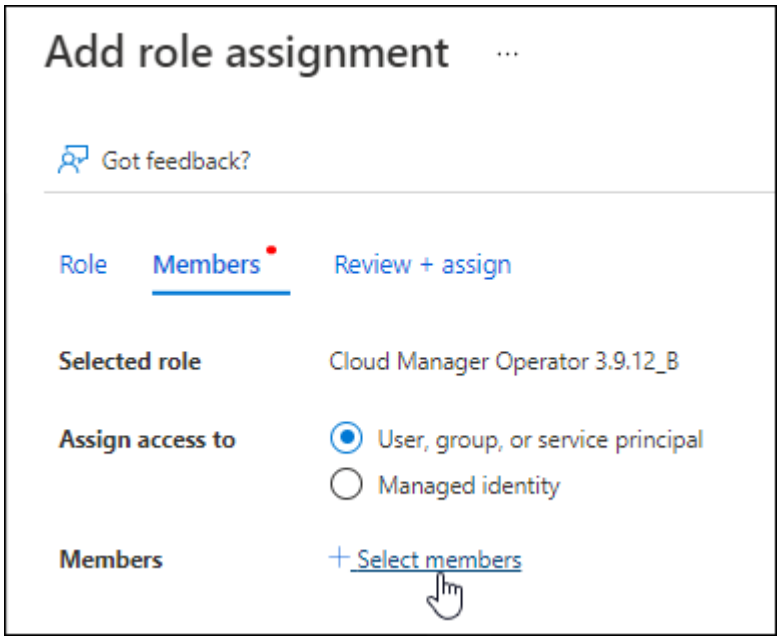
   これで、Connector仮想マシンに割り当てることができるBlueXP Operatorというカスタムロ

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。

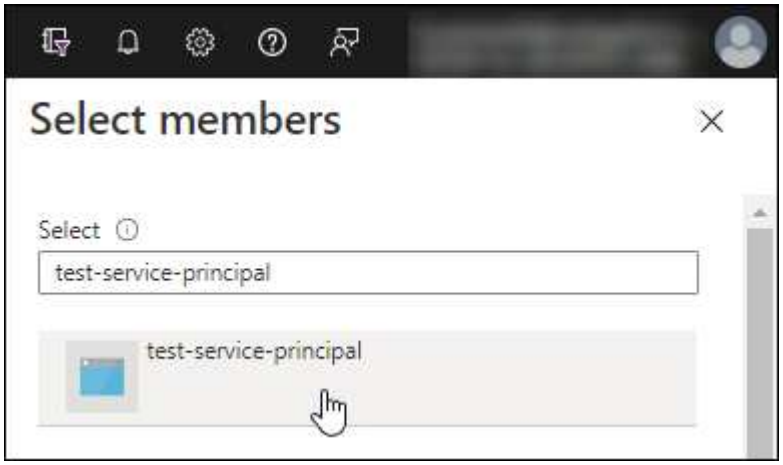
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。

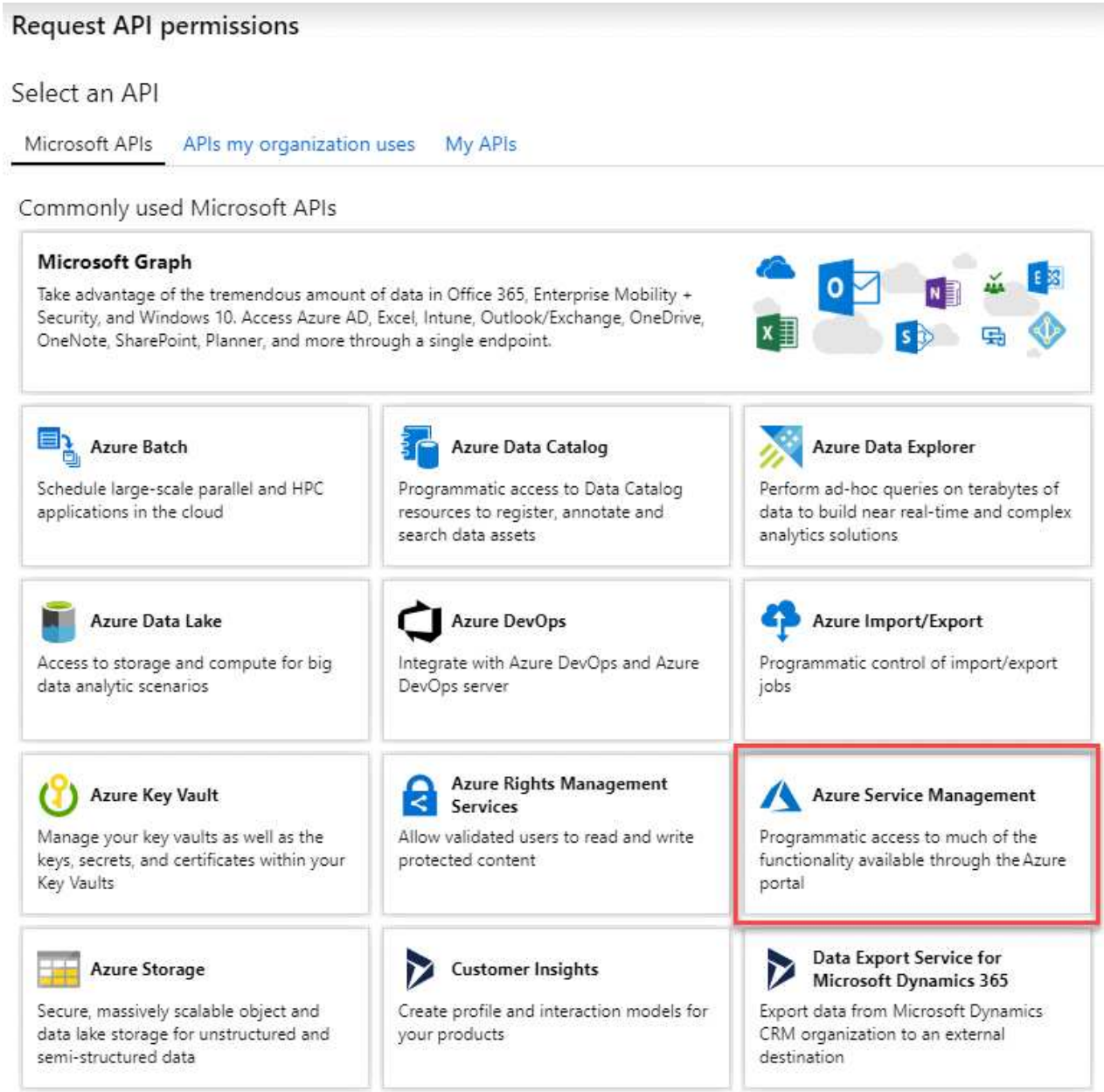
f. [Review + Assign]*を選択します。

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。

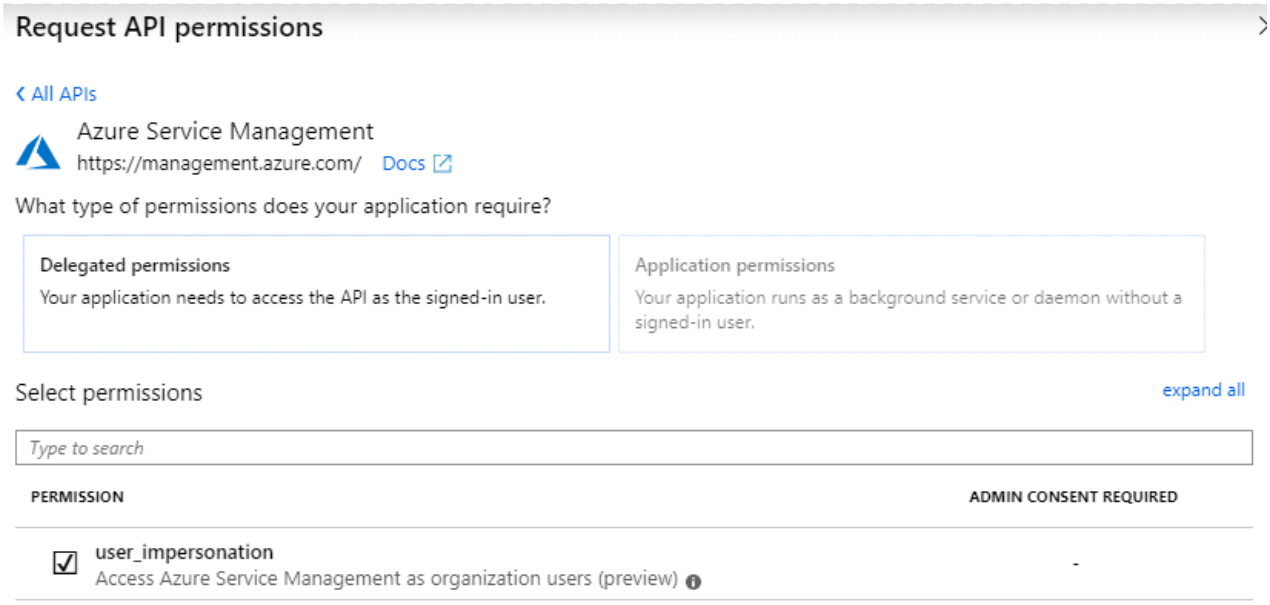
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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。

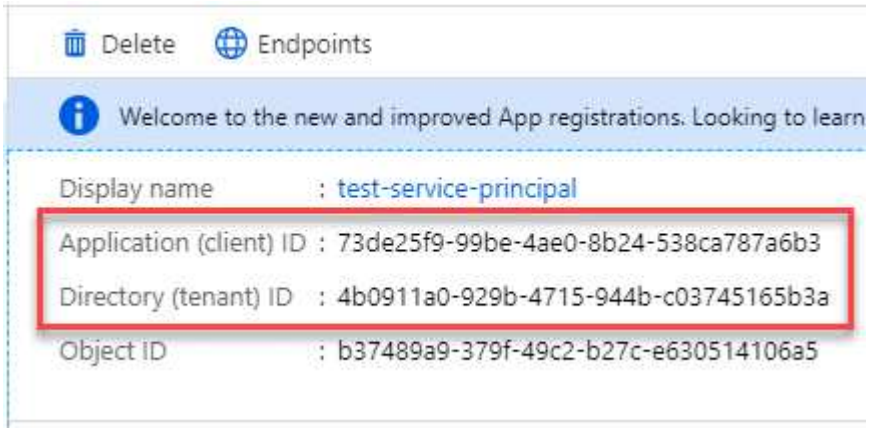


4. を選択し、[Add permissions]*を選択します。



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

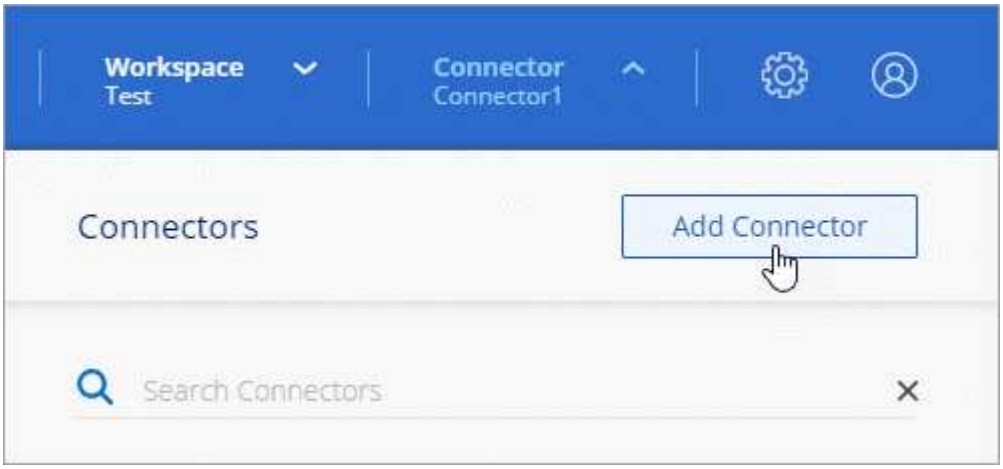
作業を開始する前に

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

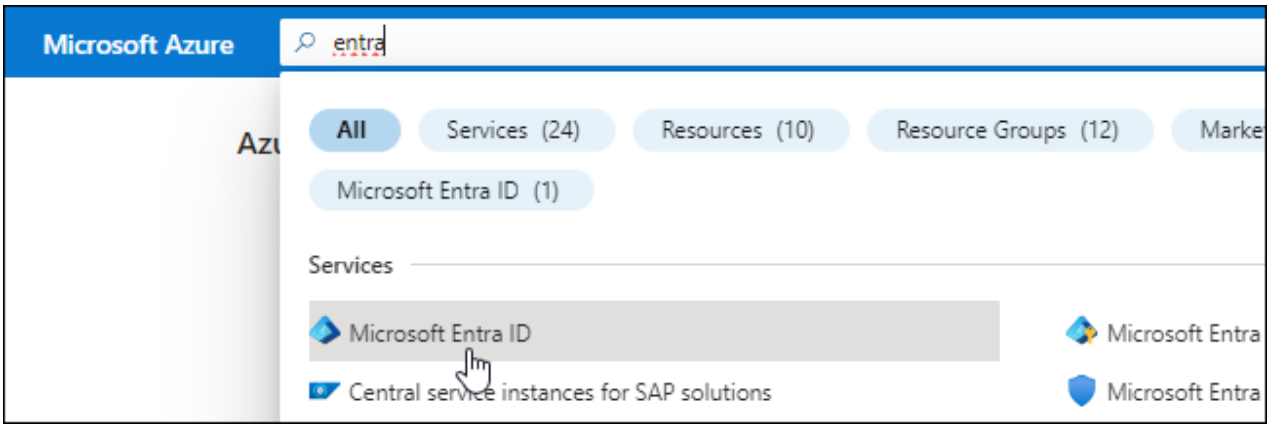
コネクタをオンプレミスにインストールする場合は、Microsoft Entra IDでサービスプリンシパルを設定し、BlueXPに必要なAzureクレデンシャルを取得して、BlueXPにAzure権限を付与する必要があります。

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。

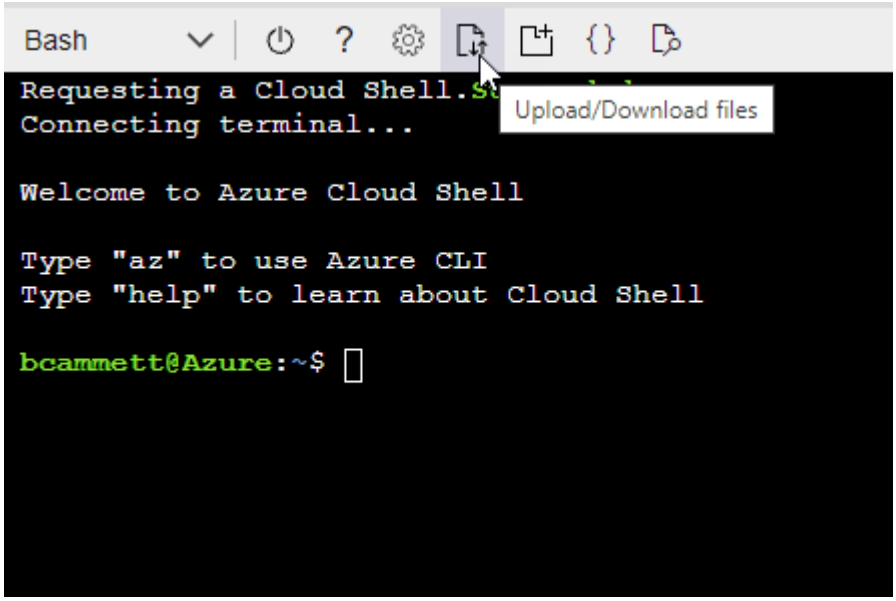
      - 例 *

```
"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。

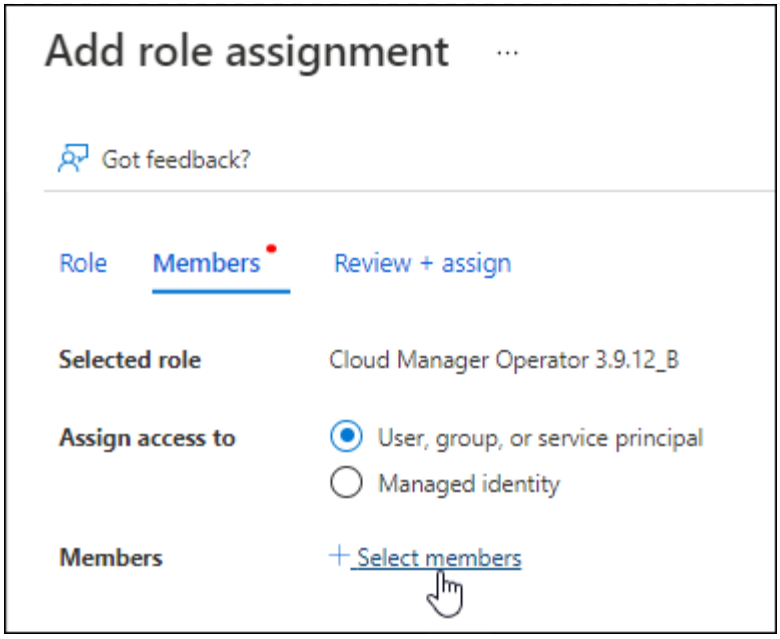
```
az role definition create --role-definition
Connector_Policy.json
```

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。

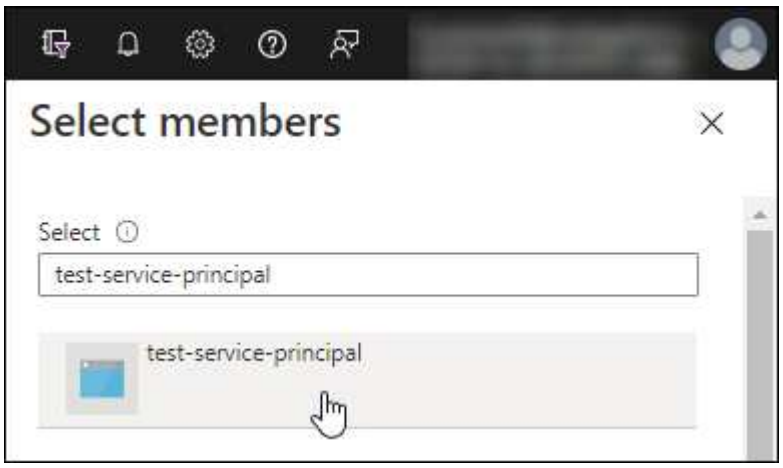
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。

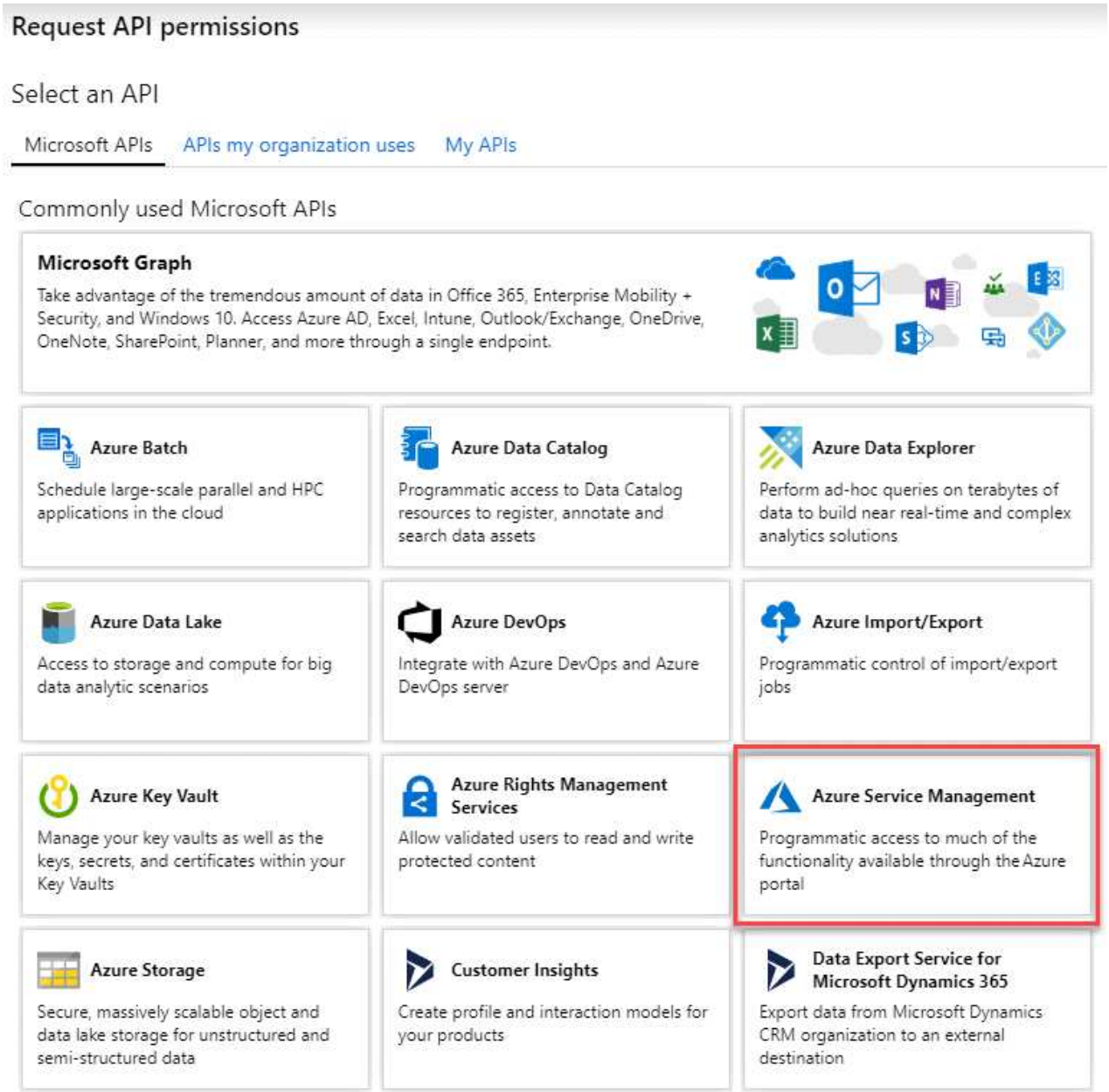
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

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。

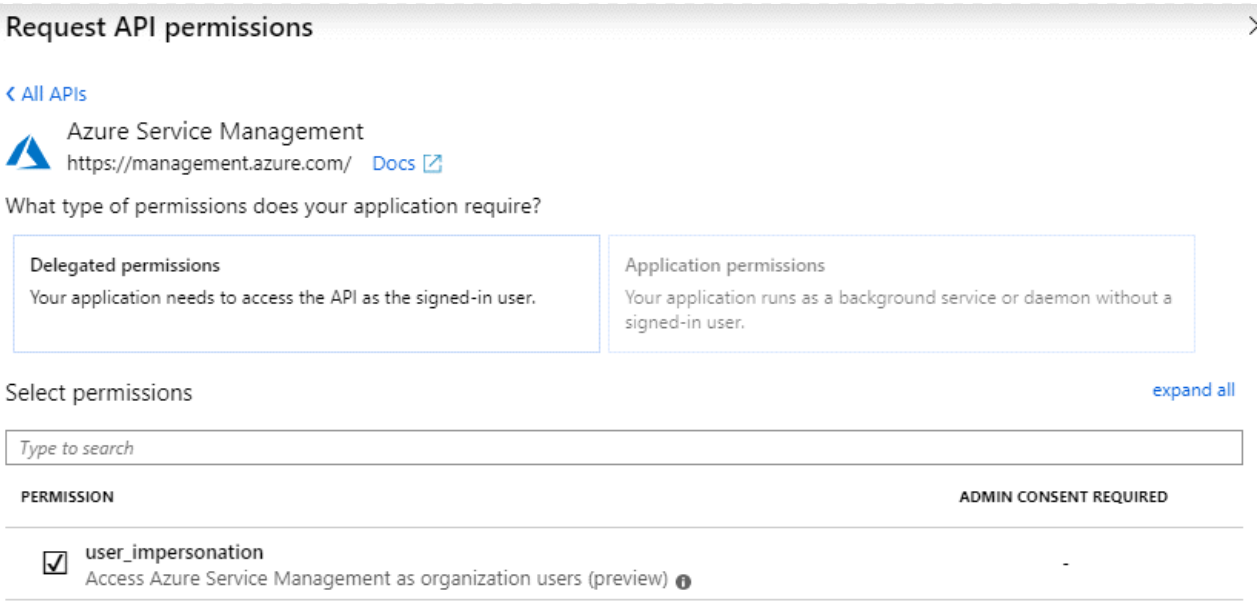
Windows Azure Service Management API 権限を追加します

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。

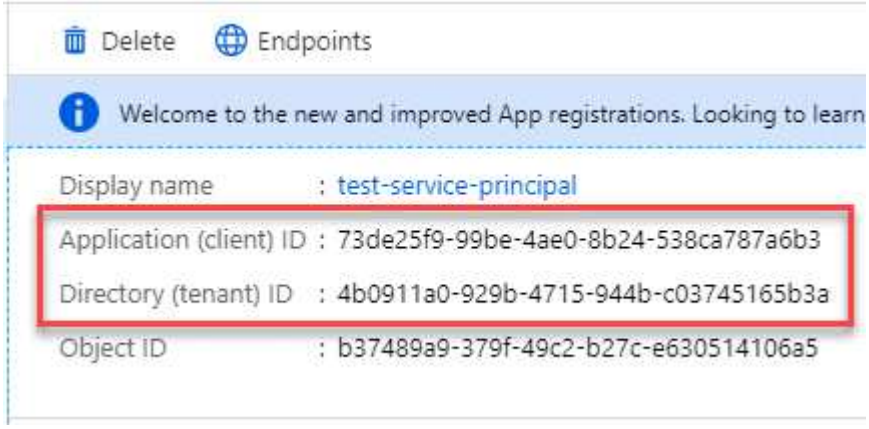


4. を選択し、[Add permissions]*を選択します。



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

BlueXPにサブスクライブ（Standardモード）

クラウドプロバイダのマーケットプレイスからBlueXPにサブスクライブして、BlueXPサービスの料金を時間単位（PAYGO）または年間契約でお支払いください。ネットアップからライセンスを購入した場合（BYOL）は、マーケットプレイスのサービスにも登録する必要があります。ライセンスは常に最初に課金されますが、ライセンス容量を超えた場合やライセンスの有効期限が切れた場合は、時間単位で課金されます。

マーケットプレイスのサブスクリプションでは、次のBlueXPサービスの料金が請求されます。

- バックアップとリカバリ
- 分類
- Cloud Volumes ONTAP
- 階層化

作業を開始する前に

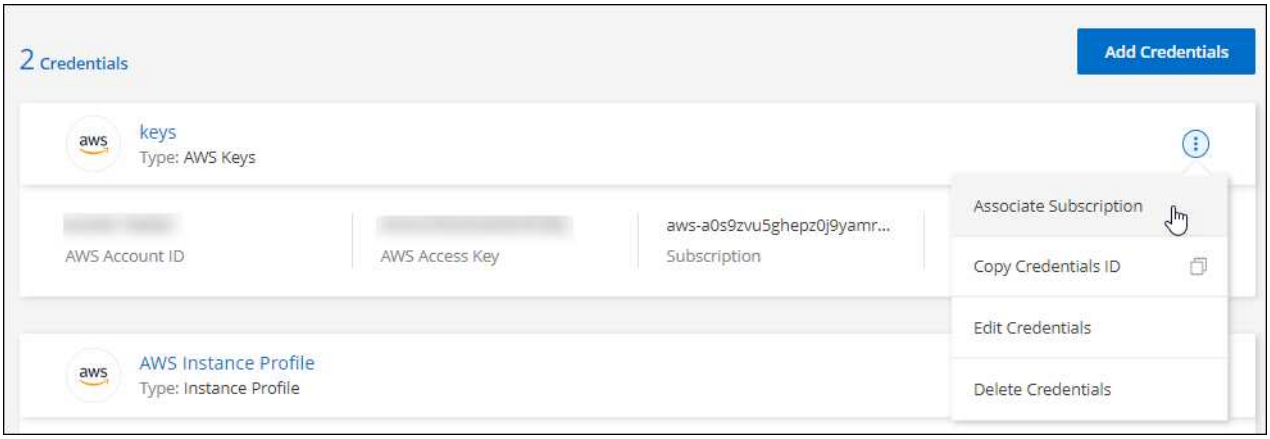
BlueXPにサブスクライブするには、コネクタに関連付けられているクラウドクレデンシャルにマーケットプレイスのサブスクリプションを関連付けます。「標準モードで開始」ワークフローに従っている場合は、コネクタがすでにあるはずです。詳細については、を参照してください "BlueXPを標準モードでクイックスタートできます"。

AWS

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。

   コネクタに関連付けられているクレデンシャルを選択する必要があります。BlueXPに関連付けられているクレデンシャルにMarketplaceサブスクリプションを関連付けることはできません。



3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからサブスクリプションを選択し、*[関連付け]*を選択します。
4. クレデンシャルを新しいサブスクリプションに関連付けるには、*[Add Subscription]>[Continue]*を選択し、AWS Marketplaceで次の手順を実行します。

   a. [購入オプションの表示]*を選択します。
   b. [サブスクライブ]*を選択します。
   c. [アカウントを設定する]*を選択します。

      BlueXPのWebサイトにリダイレクトされます

   d. [サブスクリプションの割り当て*]ページで、次の操作を行います。

      - このサブスクリプションを関連付けるBlueXPアカウントを選択します。
      - [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

   他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

      - [保存（ Save ）] を選択します。

        次のビデオは、AWS Marketplaceからサブスクライブする手順を示しています。

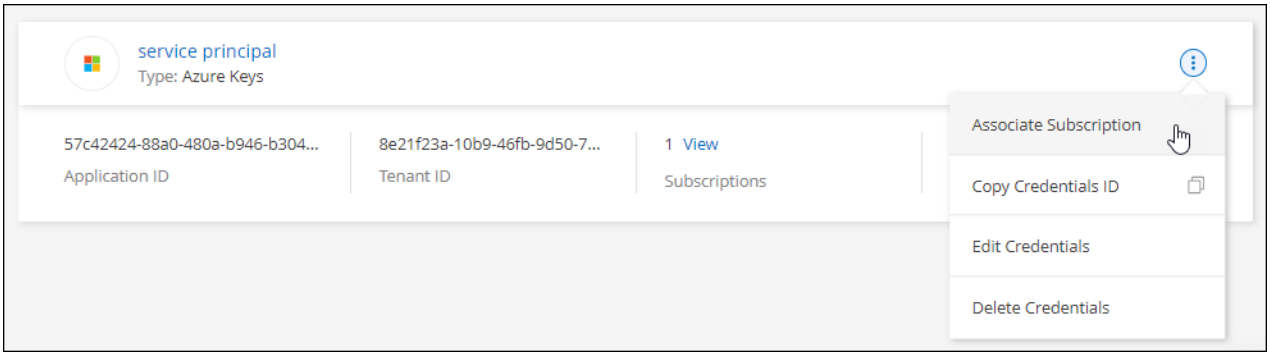
AWS MarketplaceでBlueXPにサブスクライブ

Azure

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。

   コネクタに関連付けられているクレデンシャルを選択する必要があります。BlueXPに関連付けられているクレデンシャルにMarketplaceサブスクリプションを関連付けることはできません。



3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからサブスクリプションを選択し、*[関連付け]*を選択します。
4. クレデンシャルを新しいサブスクリプションに関連付けるには、*[サブスクリプションの追加]>[続行]*を選択し、Azure Marketplaceで次の手順を実行します。

   a. プロンプトが表示されたら、Azureアカウントにログインします。
   b. [サブスクライブ]*を選択します。
   c. フォームに必要事項を入力し、* Subscribe *を選択します。
   d. サブスクリプションプロセスが完了したら、*[今すぐアカウントを設定する]*を選択します。

      BlueXPのWebサイトにリダイレクトされます

   e. [サブスクリプションの割り当て*]ページで、次の操作を行います。

      - このサブスクリプションを関連付けるBlueXPアカウントを選択します。
      - [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

      他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

      - [保存（ Save ）] を選択します。

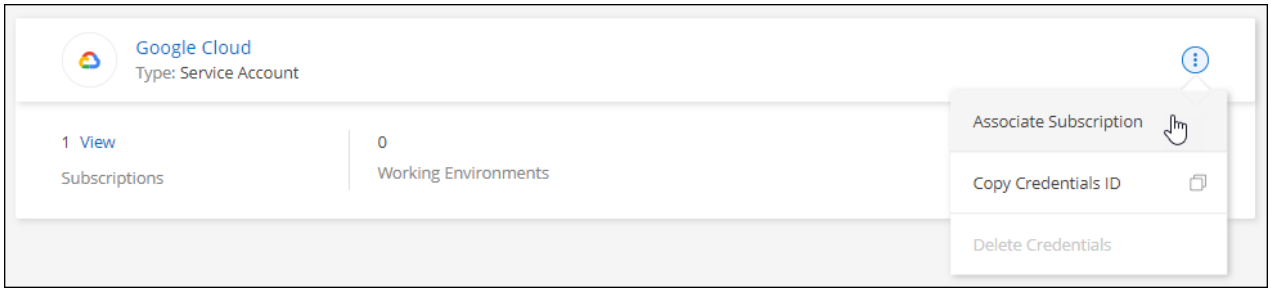
        次のビデオでは、Azure Marketplaceでのサブスクライブ手順を紹介しています。

Azure MarketplaceでBlueXPにサブスクライブ

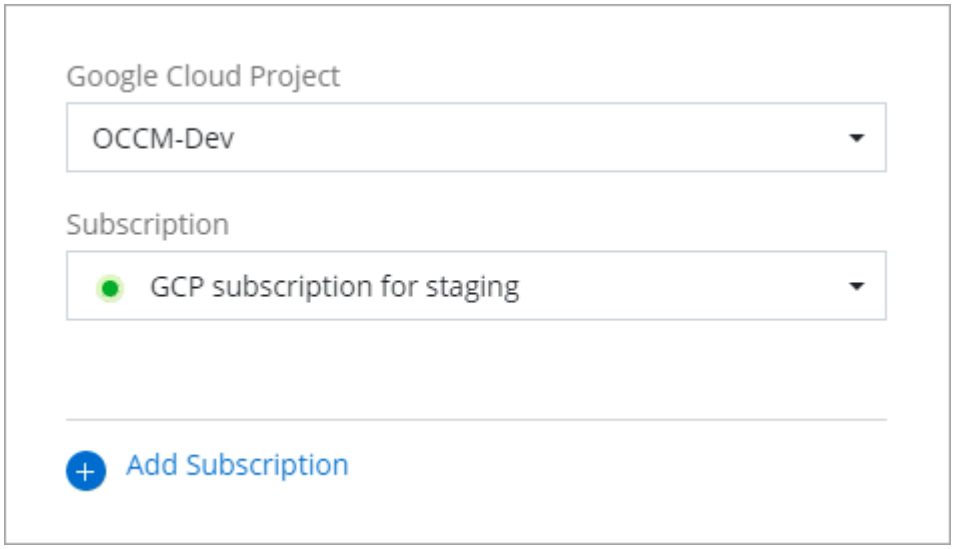
Google Cloud

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。



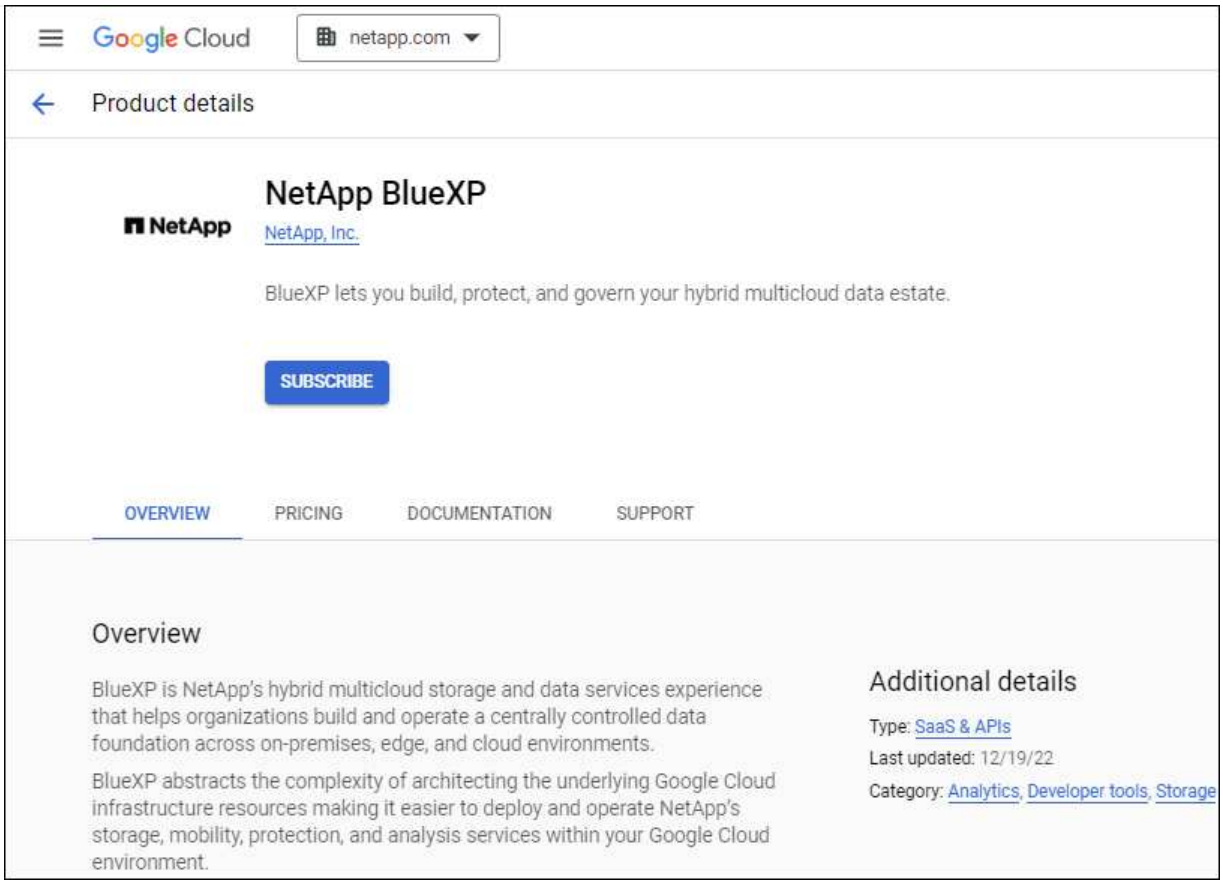
3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからGoogle Cloudプロジェクトとサブスクリプションを選択し、*[関連付け]*を選択します。



4. サブスクリプションをまだお持ちでない場合は、*[サブスクリプションの追加]>[続行]*を選択し、Google Cloud Marketplaceの手順に従います。

> 次の手順を実行する前に、Google CloudアカウントとBlueXPログインの両方に課金管理者権限があることを確認してください。

   a. にリダイレクトされたら "Google Cloud MarketplaceのNetApp BlueXPページ"をクリックし、上部のナビゲーションメニューで正しいプロジェクトが選択されていることを確認します。



b. [サブスクライブ]*を選択します。

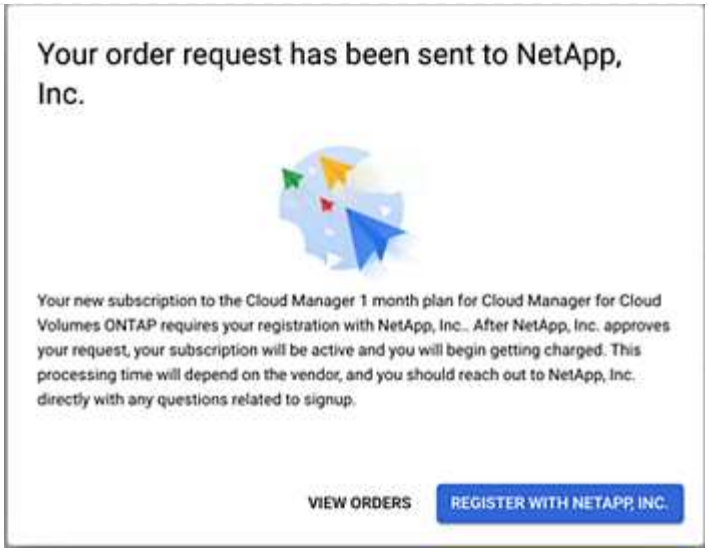
c. 適切な請求先アカウントを選択し、条件に同意します。

d. [サブスクライブ]*を選択します。

   転送要求がネットアップに送信されます。

e. ポップアップダイアログボックスで、* NetApp、Inc.への登録*を選択します

   Google CloudサブスクリプションをBlueXPアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされてBlueXPにサインインするまで、サブスクリプションをリンクするプロセスは完了していません。



f. [サブスクリプションの割り当て*]ページで次の手順を実行します。

> 組織の誰かが請求アカウントからNetApp BlueXPサブスクリプションにすでに登録している場合は、にリダイレクトされます "BlueXP WebサイトのCloud Volumes ONTAP ページ" 代わりに、予想外の場合は、ネットアップの営業チームにお問い合わせください。Google では、 1 つの Google 請求アカウントにつき 1 つのサブスクリプションのみが有効です。

- このサブスクリプションを関連付けるBlueXPアカウントを選択します。
- [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

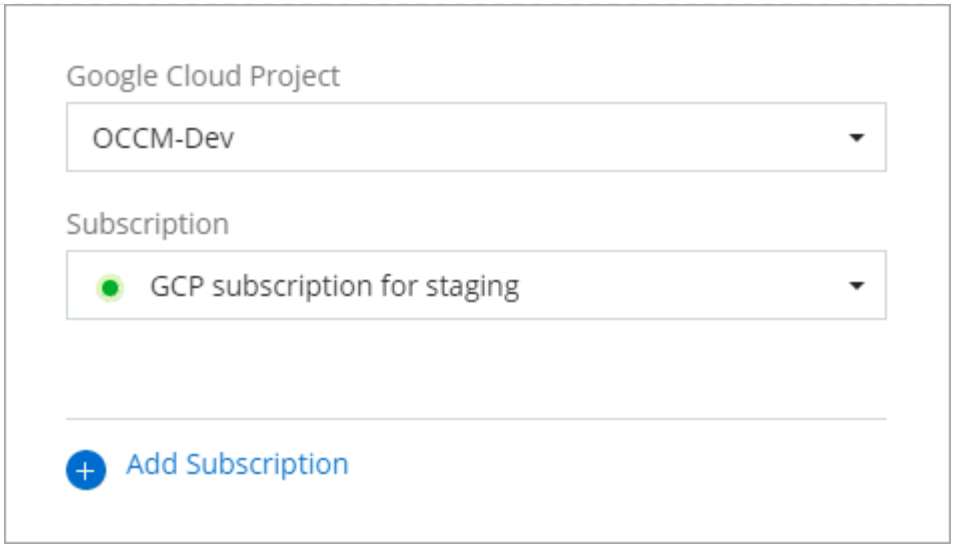
他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

- [保存（ Save ）] を選択します。

  次のビデオでは、Google Cloud Marketplaceから登録する手順を紹介しています。

Google Cloud MarketplaceからBlueXPにサブスクライブ

a. このプロセスが完了したら、BlueXPの[資格情報]ページに戻り、この新しいサブスクリプションを選択します。



関連リンク

- "Cloud Volumes ONTAP のBYOL容量ベースライセンスを管理します"
- "BlueXPデータサービスのBYOLライセンスを管理します"
- "AWSのクレデンシャルとBlueXPのサブスクリプションを管理します"
- "Azureの資格情報とBlueXPのサブスクリプションを管理します"
- "BlueXPのGoogle Cloudクレデンシャルとサブスクリプションを管理します"

次の操作（標準モード）

これでログインして標準モードでBlueXPをセットアップできました。ユーザは作業環境を作成、検出し、BlueXPデータサービスを使用できます。

> AWS、Microsoft Azure、Google Cloudにコネクタをインストールしている場合は、コネクタがインストールされている場所のAmazon S3バケット、Azure BLOBストレージ、またはGoogle Cloud Storageバケットに関する情報がBlueXPで自動的に検出されます。作業環境がBlueXPのキャンバスに自動的に追加されます。

ヘルプが必要な場合は、を参照してください "BlueXPドキュメントのホームページ" をクリックして、すべてのBlueXPサービスのドキュメントを表示してください。

関連リンク

"BlueXPの導入モード"

制限モードの使用を開始します

はじめにワークフロー（制限モード）

環境を準備し、コネクタを導入し、BlueXPにサブスクライブすることで、制限モードでBlueXPを開始できます。

制限モードは通常、州政府や地方自治体、規制対象の企業（AWS GovCloudリージョンやAzure Governmentリージョンへの導入を含む）で使用されます。開始する前に、次のことを理解しておく必要があります。"BlueXPのアカウント"、 "コネクタ"および "導入モード"。

1 **"導入を準備"**

1. CPU、RAM、ディスクスペース、Docker Engineなどの要件を満たす専用のLinuxホストを準備します。
2. ターゲットネットワークへのアクセス、手動インストールの場合はアウトバウンドインターネットアクセス、日常的なアクセスの場合はアウトバウンドインターネットを提供するネットワークをセットアップします。
3. クラウドプロバイダで権限を設定して、導入後にコネクタインスタンスにそれらの権限を関連付けることができるようにします。

2 **"コネクタを展開します"**

1. クラウドプロバイダのマーケットプレイスから、または手動で独自のLinuxホストにソフトウェアをインストールして、コネクタをインストールします。
2. Webブラウザを開き、LinuxホストのIPアドレスを入力してBlueXPをセットアップします。
3. 以前に設定した権限をBlueXPに付与します。

3 **"BlueXPにサブスクライブします"**

クラウドプロバイダのマーケットプレイスからBlueXPにサブスクライブして、BlueXPサービスの料金を時間単位（PAYGO）または年間契約でお支払いください。

制限モードでの展開を準備します

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

手順**1**：制限モードの仕組みを理解する

作業を開始する前に、制限モードでのBlueXPの動作について理解しておく必要があります。

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

また、すべてのBlueXPサービスを利用できるわけではありません。

"制限モードの機能について説明します"。

手順**2**：インストールオプションを確認する

制限モードでは、クラウドにのみコネクタをインストールできます。次のインストールオプションを使用できます。

- AWS Marketplace から入手できます
- Azure Marketplace から入手できます
- AWS、Azure、Google Cloudで実行されている独自のLinuxホストにコネクタを手動でインストールします

手順**3**：ホスト要件を確認する

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

AWSまたはAzure Marketplaceからコネクタを導入する場合、イメージには必要なOSとソフトウェアコンポーネントが含まれています。必要なのは、CPUとRAMの要件を満たすインスタンスタイプを選択することだけです。

専用ホスト

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

サポートされているオペレーティングシステム

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

  ホストがRed Hat Subscription Managementに登録されている必要があります。登録されていない場合、ホストはコネクタのインストール時に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。

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

ハイパーバイザー

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

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

CPU

4 コアまたは 4 個の vCPU

RAM

14GB

AWS EC2 インスタンスタイプ

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

Azure VM サイズ

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

Google Cloudマシンのタイプ

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

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

/opt のディスクスペース

100GiB のスペースが使用可能である必要があります

/var のディスク領域

20GiB のスペースが必要です

Docker Engine の略

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

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

"インストール手順を確認します"

手順**4**：ネットワークを準備する

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

ターゲットネットワークへの接続

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

BlueXPコンソールにユーザがアクセスできるようにネットワークを準備

制限モードでは、コネクタからBlueXPユーザインターフェイスにアクセスできます。BlueXPユーザインターフェイスを使用すると、いくつかのエンドポイントに接続してデータ管理タスクを実行できます。これらのエンドポイントは、BlueXPコンソールから特定の操作を実行するときに、ユーザのコンピュータからアクセスされます。

エンドポイント	目的
https://signin.b2c.netapp.com	NetApp Support Site (NSS)の資格情報を更新するか、新しいNSS資格情報をBlueXPに追加する必要があります。
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Webブラウザはこれらのエンドポイントに接続して、BlueXPを介した集中型ユーザ認証を行います。
https://widget.intercom.io	製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。

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

  このエンドポイントは、Azure Governmentリージョンでは必要ありません。

- https://occmclientinfragov.azurecr.us

  このエンドポイントは、Azure Governmentリージョンでのみ必要です。

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。

日常業務用のアウトバウンドインターネットアクセス

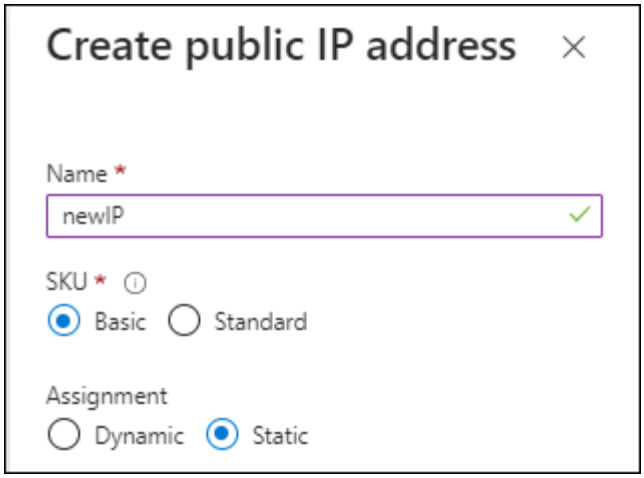
コネクタを配置するネットワークの場所には、アウトバウンドのインターネット接続が必要です。Connector では、パブリッククラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するためにアウトバウンドインターネットアクセスが必要です。

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

エンドポイント	目的
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。
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 このエンドポイントは、Azure Governmentリージョンでは必要ありません。 https://occmclientinfragov.azurecr.us このエンドポイントは、Azure Governmentリージョンでのみ必要です。	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。

Azureのパブリック**IP**アドレス

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



フィールドで[Basic]を選択できます。"]

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

"Azureのドキュメント：パブリックIP SKU"

プロキシサーバ

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

- IP アドレス
- クレデンシャル
- HTTPS証明書

BlueXPでは透過型プロキシサーバはサポートされません。

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"

クラウドプロバイダーのマーケットプレイスからコネクタを作成する場合は、コネクタの作成後に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**5**クラウドの権限を準備する

BlueXPでCloud Volumes ONTAP を仮想ネットワークに導入し、BlueXPデータサービスを使用するには、クラウドプロバイダの権限が必要です。クラウドプロバイダで権限を設定し、それらの権限をコネクタに関連付ける必要があります。

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

AWS IAMロール

コネクタに権限を付与するには、IAMロールを使用します。

AWS Marketplaceからコネクタを作成する場合は、EC2インスタンスの起動時にIAMロールを選択するように求められます。

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は、EC2インスタンスにロールをアタッチする必要があります。

手順

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

結果

これで、コネクタEC2インスタンスのIAMロールが作成されました。

AWSアクセスキー

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

手順

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

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

   標準のリージョンでは、権限は2つのポリシーに分散されます。AWSの管理対象ポリシーの最大文字数に制限されているため、2つのポリシーが必要です。 "コネクタのIAMポリシーの詳細については、こちらを参照してください"。

3. IAMユーザにポリシーを適用します。

- "AWS のドキュメント：「 Creating IAM Roles"
- "AWS のドキュメント：「 Adding and Removing IAM Policies"

4. コネクタのインストール後にBlueXPに追加できるアクセスキーがユーザに割り当てられていることを確認します。

結果

これで、アカウントに必要な権限が付与されました。

Azureロール

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

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

手順

1. 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。

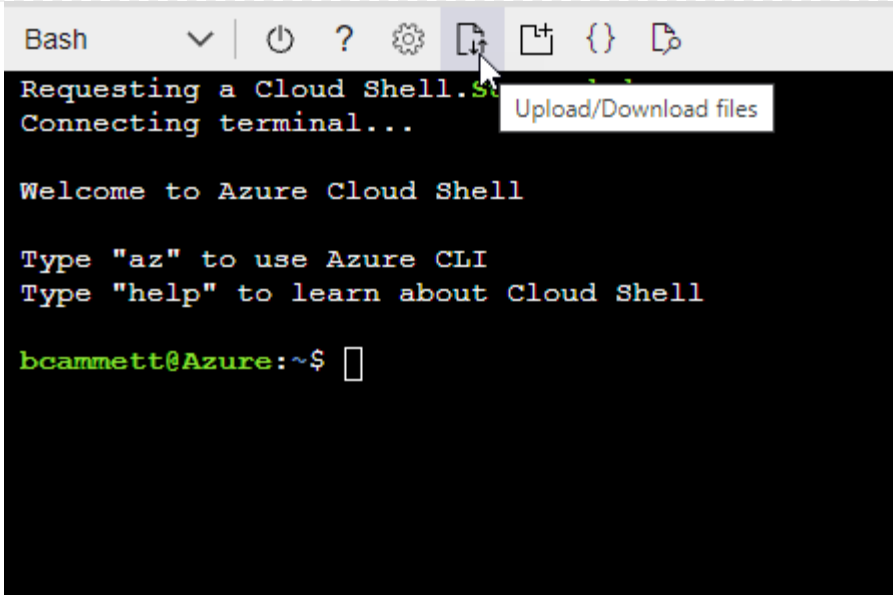
   - 例 *

```
"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。

Azureサービスプリンシパル

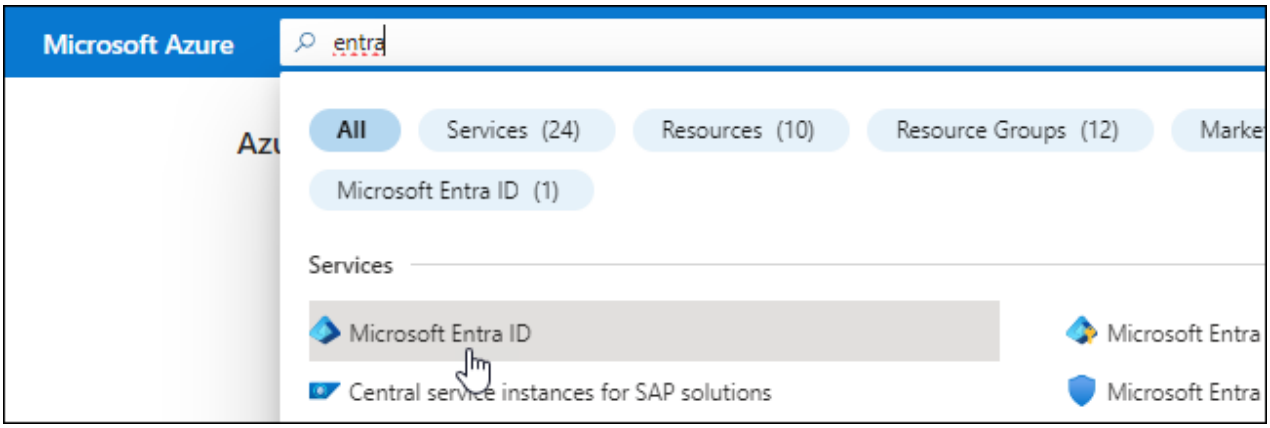
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。これらのクレデンシャルは、コネクタをインストールしてBlueXPをセットアップしたあとにBlueXPに提供する必要があります。

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

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

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

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



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

   AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

1. カスタムロールを作成します。

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

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

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

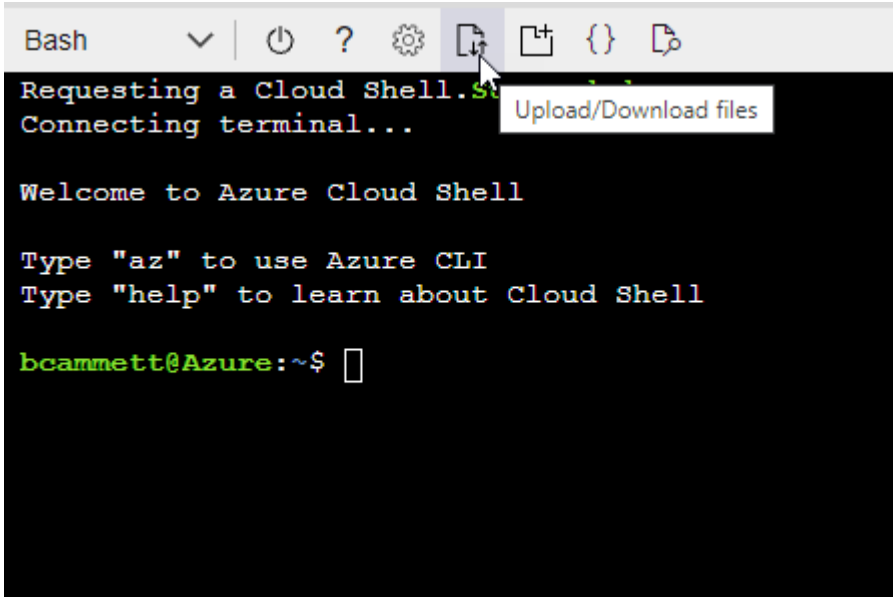
      - 例 *

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

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

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

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



- Azure CLIを使用してカスタムロールを作成します。

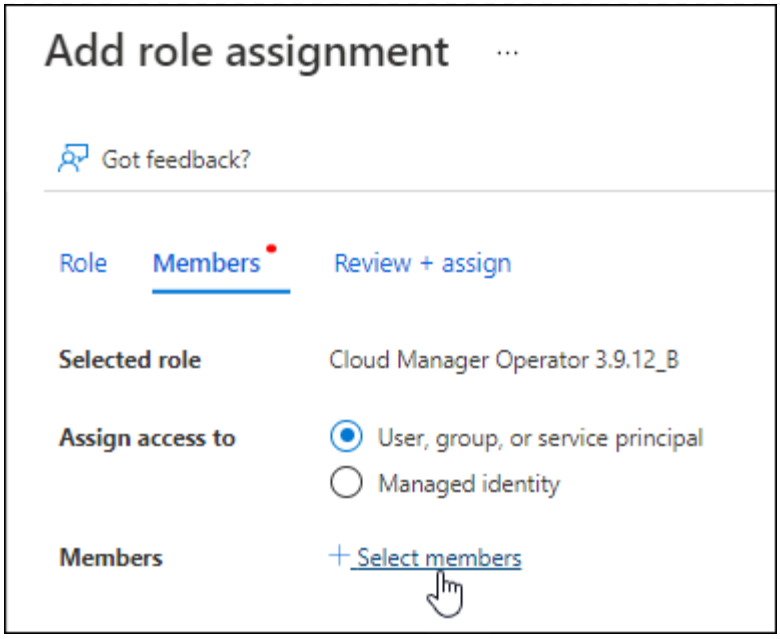
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. ロールにアプリケーションを割り当てます。

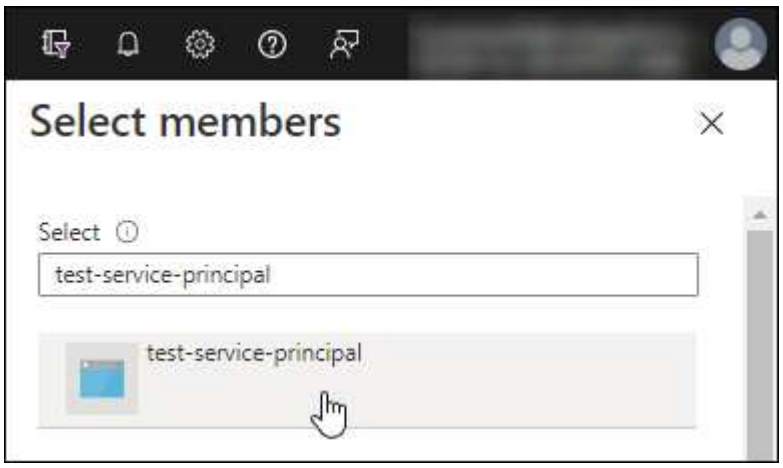
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

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



- アプリケーションの名前を検索します。

  次に例を示します。



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

f. [Review + Assign]*を選択します。

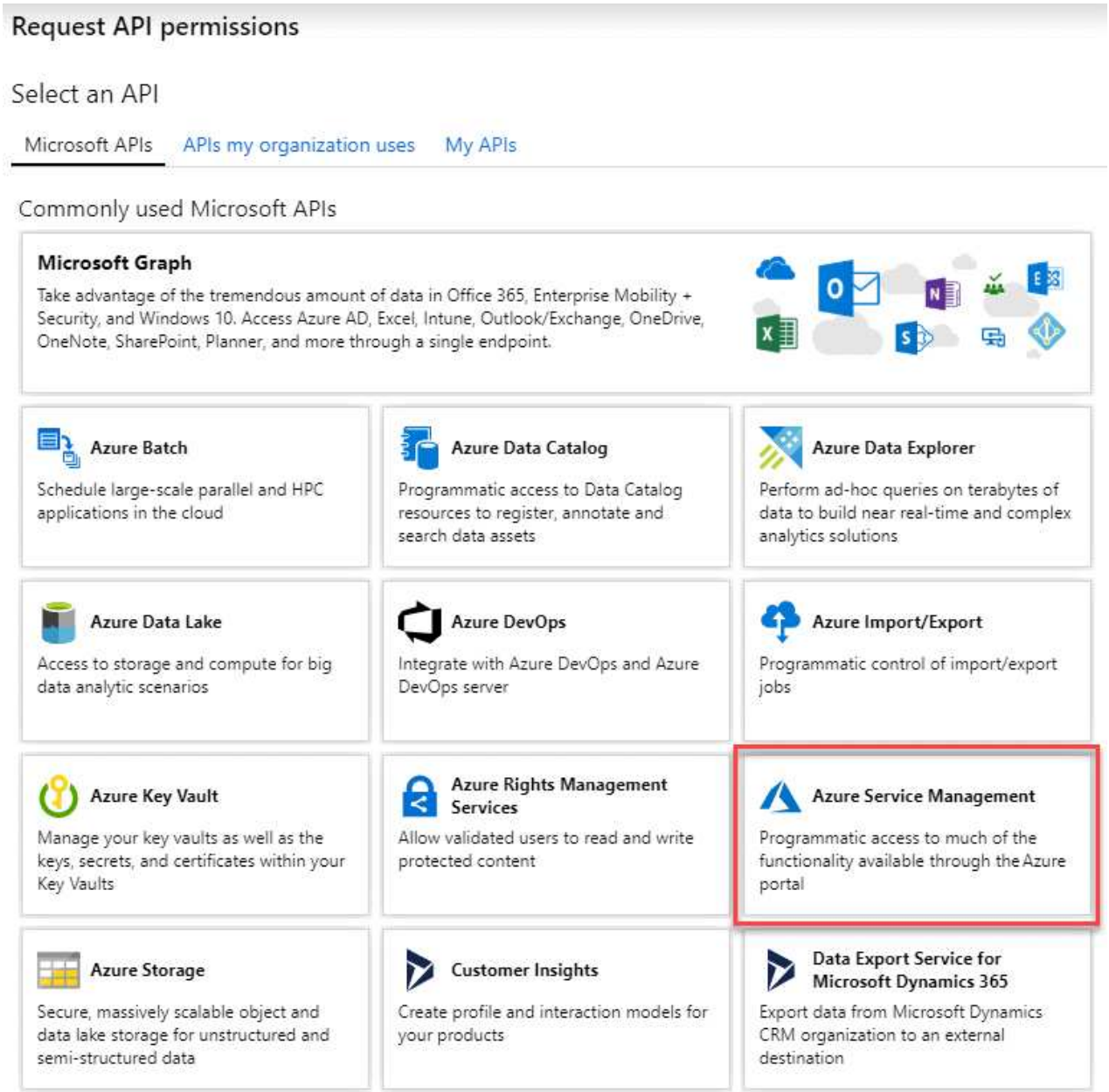
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

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

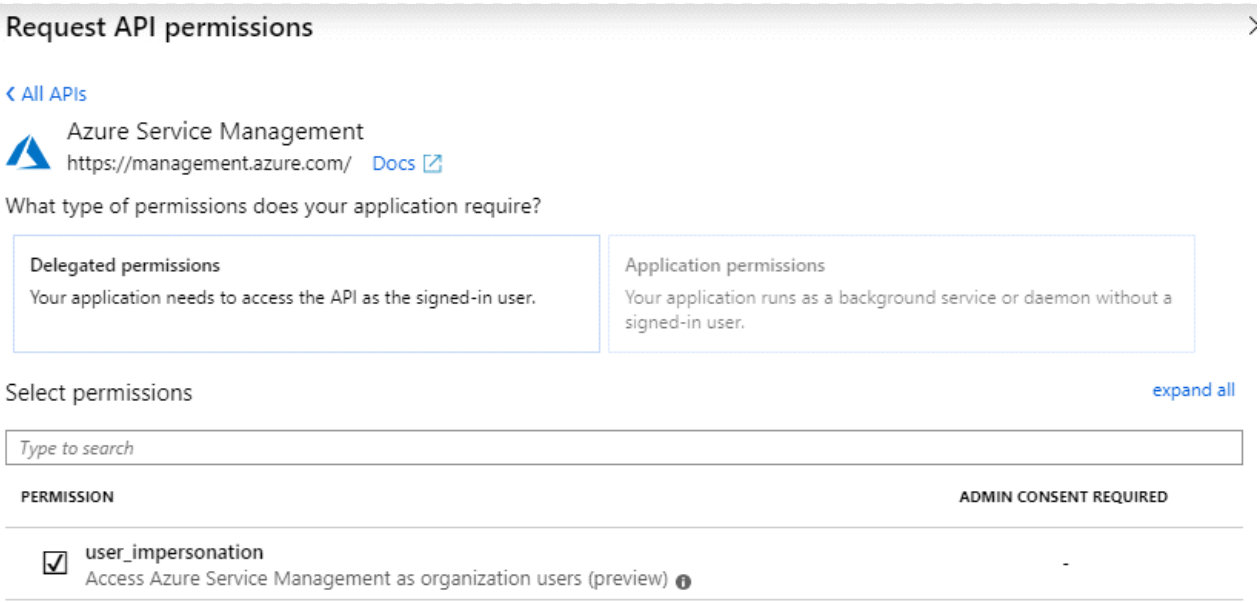
Windows Azure Service Management API 権限を追加します

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

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

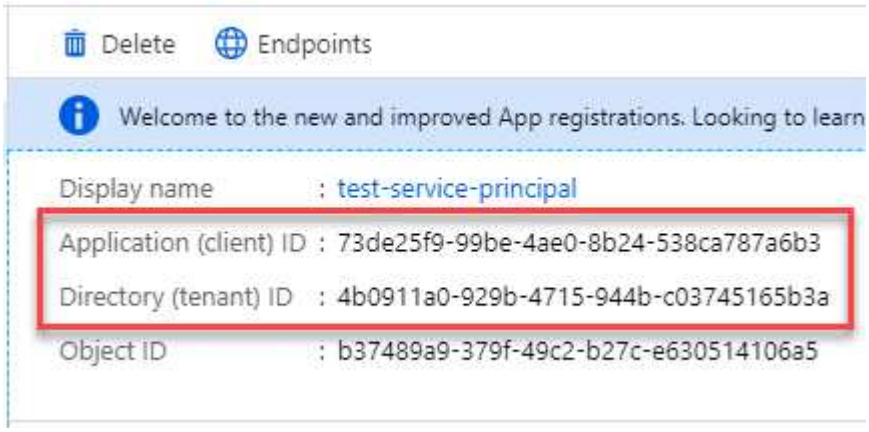


4. を選択し、[Add permissions]*を選択します。



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

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



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

クライアントシークレットを作成します

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

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

結果

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

Google Cloudサービスアカウント

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

手順

1. Google Cloudでカスタムロールを作成します。

   a. で定義された権限を含むYAMLファイルを作成します "Google Cloudのコネクタポリシー"。

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

   c. コネクタに必要な権限を含むYAMLファイルをアップロードします。

   d. を使用して、カスタムロールを作成します `gcloud iam roles create` コマンドを実行します

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

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

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

2. Google Cloudでサービスアカウントを作成します。

   a. IAMおよび管理サービスから、*サービスアカウント>サービスアカウントの作成*を選択します。

   b. サービスアカウントの詳細を入力し、*作成して続行*を選択します。

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

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

結果

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

ステップ**6**：**Google Cloud API**を有効にする

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

ステップ

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

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

コネクタを制限モードで展開します

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

手順**1**：コネクタを取り付ける

クラウドプロバイダのマーケットプレイスから、または手動で独自のLinuxホストにソフトウェアをインストールして、コネクタをインストールします。

AWS Commercial Marketplaceの略

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。

  "ネットワーク要件について説明します"

- 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。

  "AWS権限の設定方法をご確認ください"

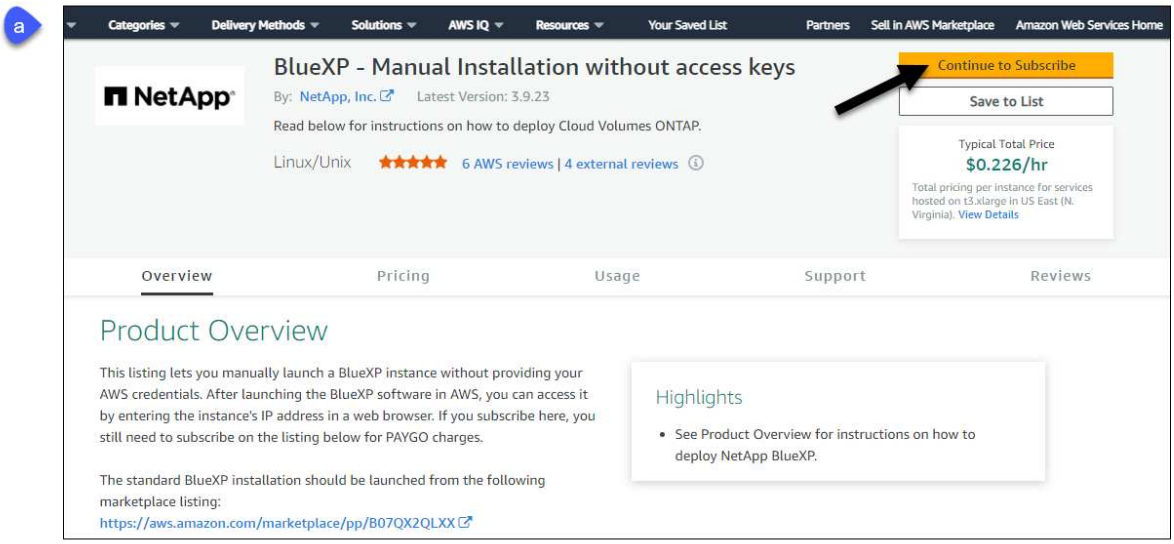
- IAMユーザのAWS Marketplaceをサブスクライブおよびサブスクライブ解除する権限。
- インスタンスのCPUとRAMの要件を理解していること。

  "インスタンス要件を確認します"。

- 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。

結果

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。

次の手順

BlueXPをセットアップします。

AWS Gov Marketplaceの略

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。

  "ネットワーク要件について説明します"

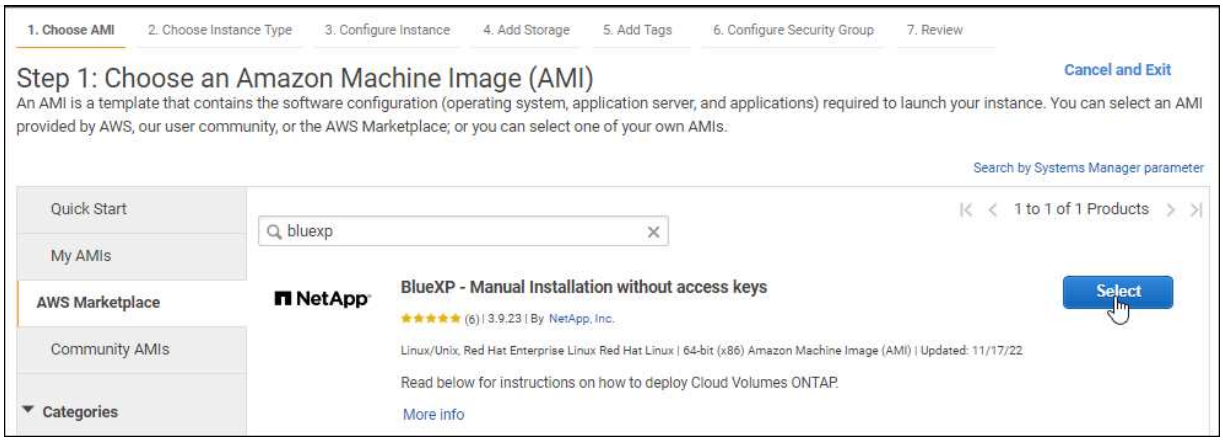
- コネクタに必要な権限を含むポリシーが添付されたIAMロール。

  "AWS権限の設定方法をご確認ください"

- 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。
- EC2インスタンスのキーペア。

手順

1. AWS MarketplaceのBlueXP製品にアクセスします。
   a. EC2サービスを開き、*インスタンスの起動*を選択します。
   b. 「AWS Marketplace *」を選択します。
   c. BlueXPを検索して、製品を選択します。

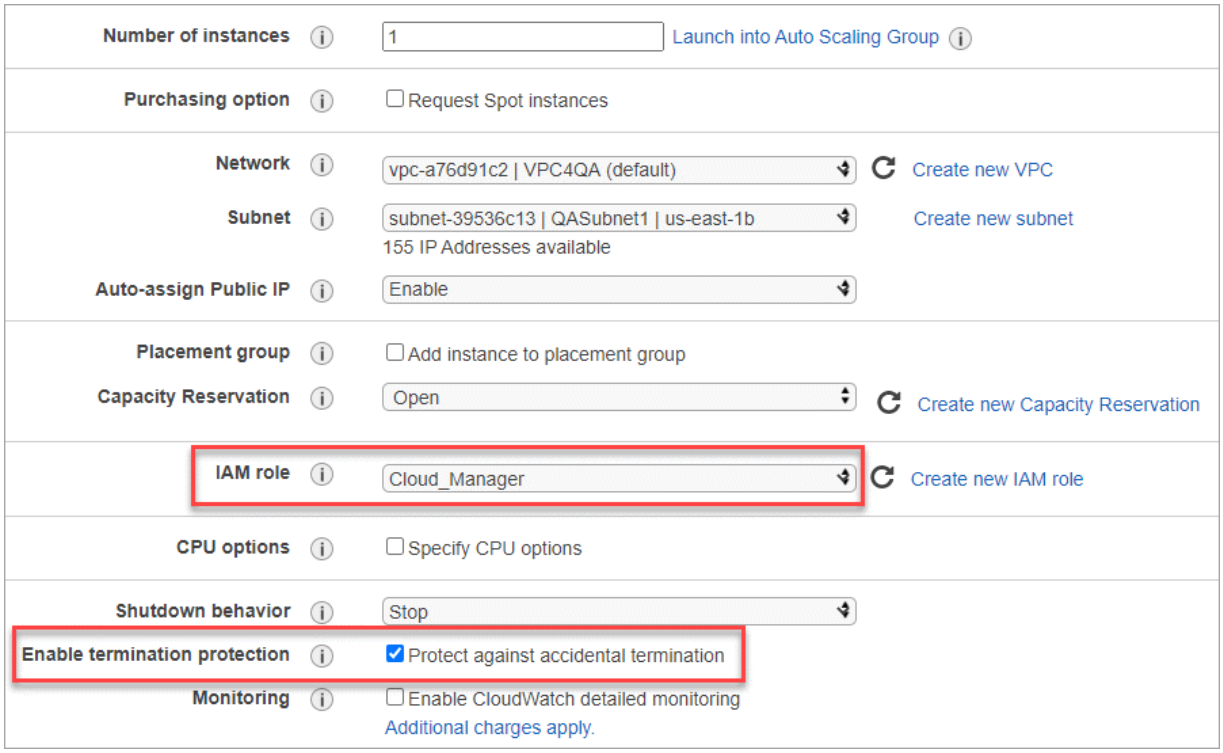


d. 「 * Continue * 」を選択します。

2. 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。
   - インスタンスタイプを選択：リージョンの可用性に応じて、サポートされているインスタンスタイプ（t3.xlargeを推奨）のいずれかを選択します。

     "インスタンスの要件を確認します"。

   - * Configure Instance Details*：VPCとサブネットを選択し、手順1で作成したIAMロールを選択して、終了保護を有効にし（推奨）、要件を満たす他の設定オプションを選択します。



   - * Add Storage* ：デフォルトのストレージ・オプションをそのまま使用します。
   - * Add Tags* ：必要に応じて、インスタンスのタグを入力します。
   - * セキュリティグループの設定 * ：コネクタインスタンスに必要な接続方法（ SSH 、 HTTP 、 HTTPS ）を指定します。
   - 確認：選択内容を確認し、*起動*を選択します。

結果

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。

次の手順

BlueXPをセットアップします。

Azure Marketplace で入手できます

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VNetとサブネット。

  "ネットワーク要件について説明します"

- コネクタに必要な権限を含むAzureのカスタムロール。

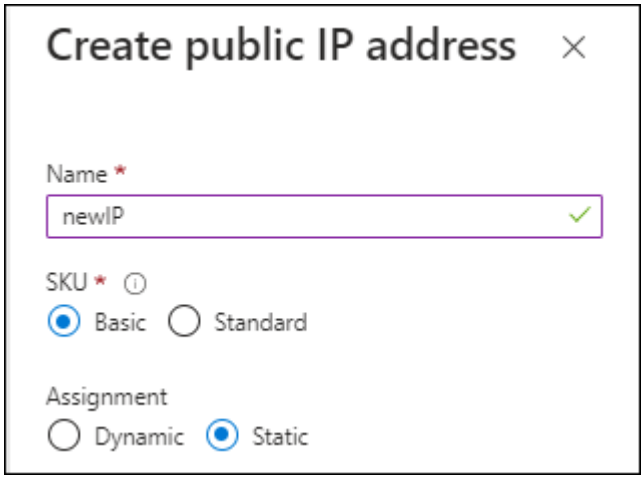
  "Azure権限の設定方法については、こちらをご覧ください"

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"
   - "Azure GovernmentリージョンのAzure Marketplaceのページ"
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。
   - *パブリックIP *：コネクタVMでパブリックIPアドレスを使用する場合、BlueXPでこのパブリックIPアドレスが確実に使用されるように、そのIPアドレスでBasic SKUを使用する必要があります。



フィールドで[Basic]を選択できます。"]

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

"Azureのドキュメント：パブリックIP SKU"

- 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。

結果

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。

次の手順

BlueXPをセットアップします。

手動インストール

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。

次の手順

BlueXPをセットアップします。

ステップ**2**：**BlueXP**をセットアップする

BlueXPコンソールに初めてアクセスすると、コネクタを関連付けるアカウントを選択するように求められ、制限モードを有効にする必要があります。

> すでにアカウントを持っていて、別のアカウントを作成する場合は、Tenancy APIを使用する必要があります。 "BlueXPアカウントを追加で作成する方法をご紹介します"。

手順

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. BlueXPに登録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. コネクタの名前を入力します。
   b. 新しいBlueXPアカウントの名前を入力するか、既存のアカウントを選択します。

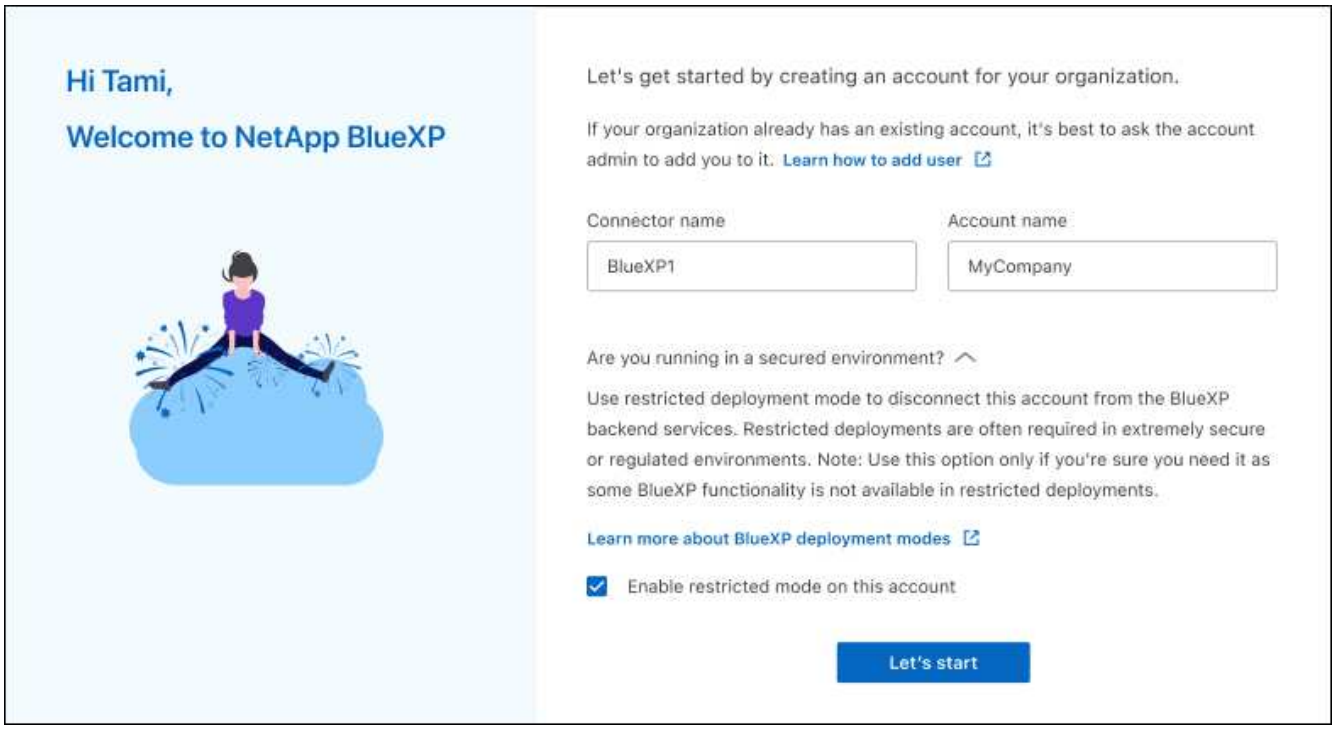
      ログインがすでにBlueXPアカウントに関連付けられている場合は、既存のアカウントを選択できます。

   c. [セキュリティ保護された環境で実行していますか？]*を選択します
   d. *このアカウントで制限モードを有効にする*を選択します。

      BlueXPでアカウントが作成されると、この設定を変更することはできません。制限モードは後で有効

にすることも、後で無効にすることもできません。

コネクタを政府地域に配置した場合、このチェックボックスはすでに有効になっており、変更することはできません。これは、制限モードが政府地域でサポートされている唯一のモードであるためです。



a. [* 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。すべてのユーザがコネクタインスタンスのIPアドレスを使用してBlueXPにアクセスする必要があります。

次の手順

以前に設定した権限をBlueXPに付与します。

ステップ**3**：**BlueXP**への権限を付与する

Azure Marketplaceからコネクタを導入した場合やコネクタソフトウェアを手動でインストールした場合は、BlueXPサービスを使用できるように、以前に設定した権限を指定する必要があります。

AWS Marketplaceからコネクタをデプロイした場合、デプロイ時に必要なIAMロールを選択したため、これらの手順は適用されません。

"クラウドへのアクセス許可を準備する方法をご確認ください"。

AWS IAMロール

以前に作成したIAMロールを、コネクタをインストールしたEC2インスタンスにアタッチします。

これらの手順は、コネクタをAWSに手動でインストールした場合にのみ該当します。AWS Marketplace環境の場合は、コネクタインスタンスに必要な権限を含むIAMロールがすでに関連付けられています。

手順

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

結果

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

AWSアクセスキー

必要な権限を持つIAMユーザのAWSアクセスキーをBlueXPに渡します。

手順

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

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

結果

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

Azureロール

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

手順

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

   サブスクリプションレベルでのロール割り当ての範囲が指定されるため、* Subscriptions *サービス

からロールを割り当てることが重要です。_scope_は、環境にアクセスするリソースセットを定義します。別のレベル（仮想マシンレベルなど）でスコープを指定すると、BlueXPで操作を実行できなくなります。

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

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

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

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

結果

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

Azureサービスプリンシパル

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

手順

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

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

d. 確認：新しいクレデンシャルの詳細を確認し、*[追加]*を選択します。

結果

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

Google Cloudサービスアカウント

サービスアカウントをコネクタVMに関連付けます。

手順

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

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

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

結果

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

BlueXPにサブスクライブ（制限モード）

クラウドプロバイダのマーケットプレイスからBlueXPにサブスクライブして、BlueXPサービスの料金を時間単位（PAYGO）または年間契約でお支払いください。ネットアップからライセンスを購入した場合（BYOL）は、マーケットプレイスのサービスにも登録する必要があります。ライセンスは常に最初に課金されますが、ライセンス容量を超えた場合やライセンスの有効期限が切れた場合は、時間単位で課金されます。

マーケットプレイスのサブスクリプションでは、制限モードで次のBlueXPサービスの料金が請求されます。

- バックアップとリカバリ
- 分類
- Cloud Volumes ONTAP

作業を開始する前に

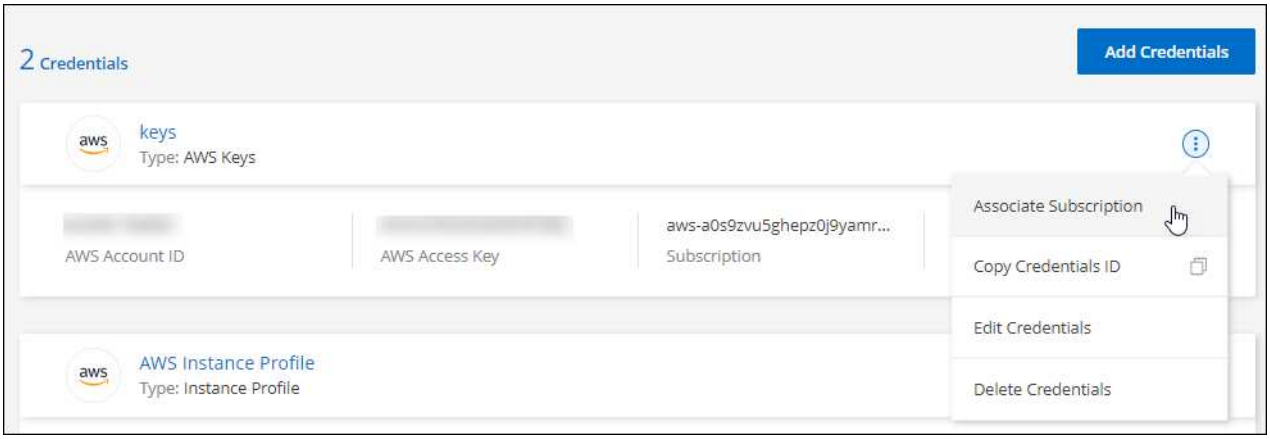
BlueXPにサブスクライブするには、コネクタに関連付けられているクラウドクレデンシャルにマーケットプレイスのサブスクリプションを関連付けます。「制限モードで開始する」ワークフローに従っている場合は、コネクタがすでに用意されている必要があります。詳細については、を参照してください "制限モードのBlueXPのクイックスタート"。

AWS

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。

   コネクタに関連付けられているクレデンシャルを選択する必要があります。BlueXPに関連付けられているクレデンシャルにMarketplaceサブスクリプションを関連付けることはできません。



3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからサブスクリプションを選択し、*[関連付け]*を選択します。
4. クレデンシャルを新しいサブスクリプションに関連付けるには、*[Add Subscription]>[Continue]*を選択し、AWS Marketplaceで次の手順を実行します。

   a. [購入オプションの表示]*を選択します。
   b. [サブスクライブ]*を選択します。
   c. [アカウントを設定する]*を選択します。

      BlueXPのWebサイトにリダイレクトされます

   d. [サブスクリプションの割り当て*]ページで、次の操作を行います。

      - このサブスクリプションを関連付けるBlueXPアカウントを選択します。
      - [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

   他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

      - [保存（ Save ）] を選択します。

        次のビデオは、AWS Marketplaceからサブスクライブする手順を示しています。

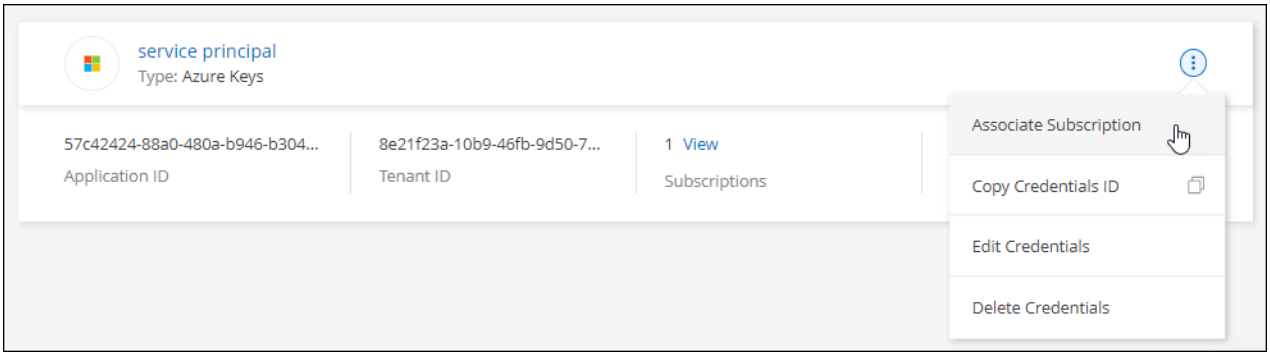
AWS MarketplaceでBlueXPにサブスクライブ

Azure

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。

   コネクタに関連付けられているクレデンシャルを選択する必要があります。BlueXPに関連付けられているクレデンシャルにMarketplaceサブスクリプションを関連付けることはできません。



3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからサブスクリプションを選択し、*[関連付け]*を選択します。
4. クレデンシャルを新しいサブスクリプションに関連付けるには、*[サブスクリプションの追加]>[続行]*を選択し、Azure Marketplaceで次の手順を実行します。

   a. プロンプトが表示されたら、Azureアカウントにログインします。
   b. [サブスクライブ]*を選択します。
   c. フォームに必要事項を入力し、* Subscribe *を選択します。
   d. サブスクリプションプロセスが完了したら、*[今すぐアカウントを設定する]*を選択します。

      BlueXPのWebサイトにリダイレクトされます

   e. [サブスクリプションの割り当て*]ページで、次の操作を行います。

      - このサブスクリプションを関連付けるBlueXPアカウントを選択します。
      - [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

      他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

      - [保存（ Save ）] を選択します。

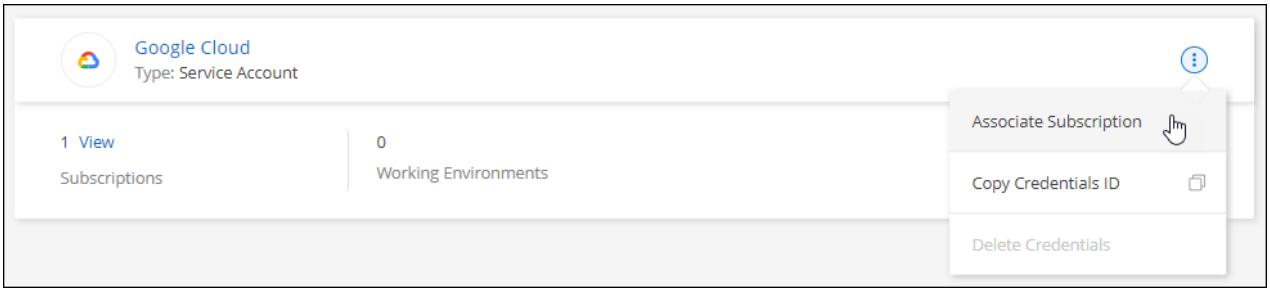
        次のビデオでは、Azure Marketplaceでのサブスクライブ手順を紹介しています。

Azure MarketplaceでBlueXPにサブスクライブ

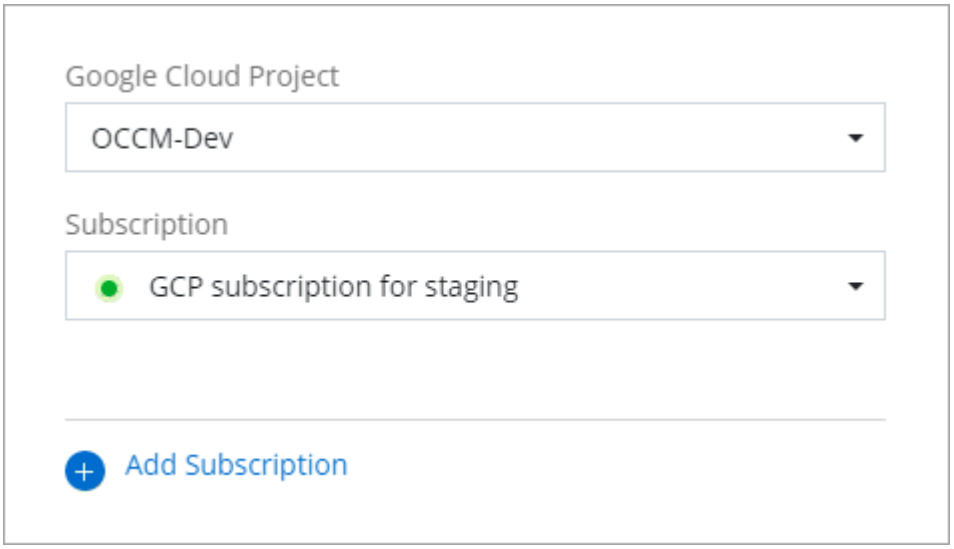
Google Cloud

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。



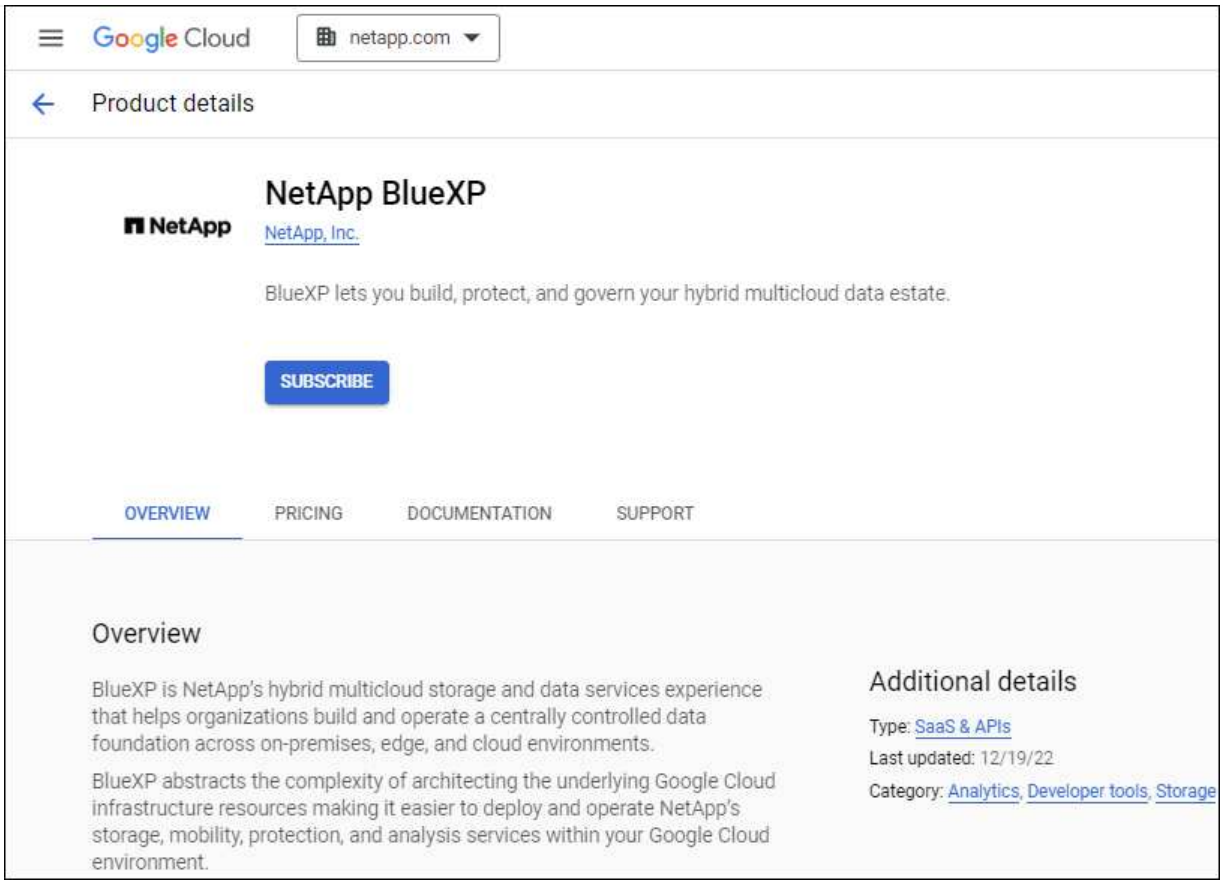
3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからGoogle Cloudプロジェクトとサブスクリプションを選択し、*[関連付け]*を選択します。



4. サブスクリプションをまだお持ちでない場合は、*[サブスクリプションの追加]>[続行]*を選択し、Google Cloud Marketplaceの手順に従います。

> 次の手順を実行する前に、Google CloudアカウントとBlueXPログインの両方に課金管理者権限があることを確認してください。

   a. にリダイレクトされたら "Google Cloud MarketplaceのNetApp BlueXPページ"をクリックし、上部のナビゲーションメニューで正しいプロジェクトが選択されていることを確認します。



b. [サブスクライブ]*を選択します。

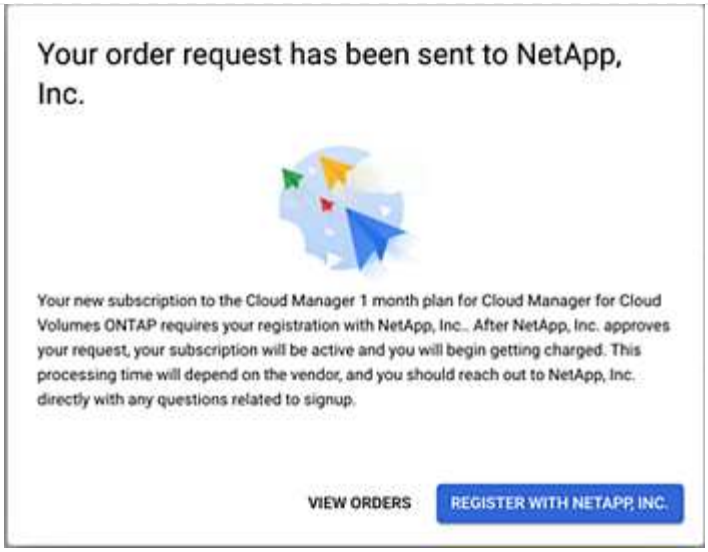
c. 適切な請求先アカウントを選択し、条件に同意します。

d. [サブスクライブ]*を選択します。

   転送要求がネットアップに送信されます。

e. ポップアップダイアログボックスで、* NetApp、Inc.への登録*を選択します

   Google CloudサブスクリプションをBlueXPアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされてBlueXPにサインインするまで、サブスクリプションをリンクするプロセスは完了していません。



f. [サブスクリプションの割り当て*]ページで次の手順を実行します。

> 組織の誰かが請求アカウントからNetApp BlueXPサブスクリプションにすでに登録している場合は、にリダイレクトされます "BlueXP WebサイトのCloud Volumes ONTAP ページ" 代わりに、予想外の場合は、ネットアップの営業チームにお問い合わせください。Google では、 1 つの Google 請求アカウントにつき 1 つのサブスクリプションのみが有効です。

- このサブスクリプションを関連付けるBlueXPアカウントを選択します。
- [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

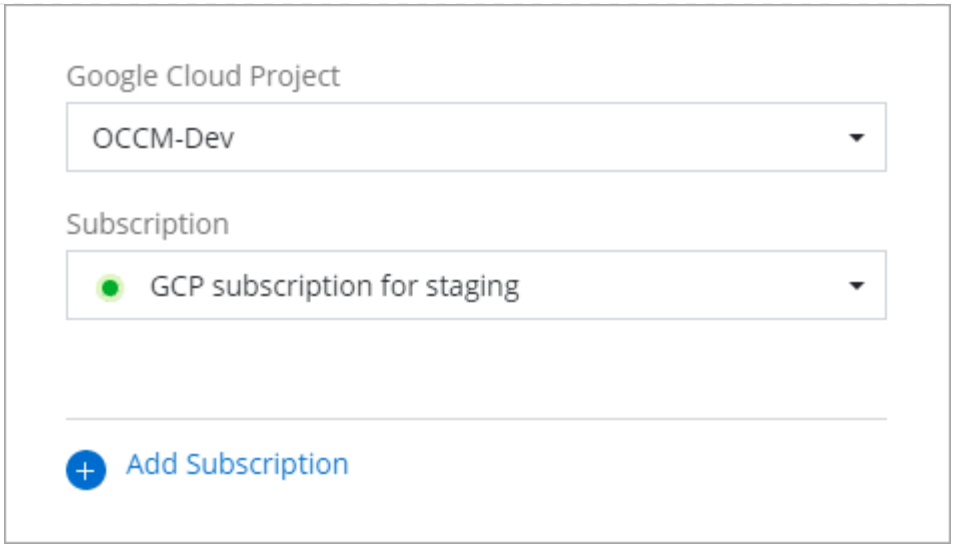
他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

- [保存（ Save ）] を選択します。

  次のビデオでは、Google Cloud Marketplaceから登録する手順を紹介しています。

Google Cloud MarketplaceからBlueXPにサブスクライブ

a. このプロセスが完了したら、BlueXPの[資格情報]ページに戻り、この新しいサブスクリプションを選択します。



関連リンク

- "Cloud Volumes ONTAP のBYOL容量ベースライセンスを管理します"
- "BlueXPデータサービスのBYOLライセンスを管理します"
- "AWSのクレデンシャルとBlueXPのサブスクリプションを管理します"
- "Azureの資格情報とBlueXPのサブスクリプションを管理します"
- "BlueXPのGoogle Cloudクレデンシャルとサブスクリプションを管理します"

次に実行できる処理（制限モード）

制限モードでBlueXPを起動して実行したら、制限モードでサポートされるBlueXPサービスの使用を開始できます。

ヘルプについては、次のサービスのマニュアルを参照してください。

- "ONTAP ドキュメント： Amazon FSX"
- "Azure NetApp Files のドキュメント"
- "バックアップとリカバリのドキュメント"
- "分類ドキュメント"
- "Cloud Volumes ONTAP のドキュメント"
- "オンプレミスのONTAP クラスタのドキュメント"
- "レプリケーションドキュメント"

関連リンク

"BlueXPの導入モード"

プライベートモードで開始します

スタートアップワークフロー（プライベートモード）

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

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

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

1 "導入を準備"

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

2 "コネクタを展開します"

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

プライベートモードでの導入を準備します

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

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

ステップ**1**：プライベートモードの仕組みを理解する

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

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

また、すべてのBlueXPサービスを利用できるわけではありません。

"プライベートモードの仕組みを説明します"。

手順**2**：インストールオプションを確認する

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

コネクタのインストール先によって、プライベートモードの使用時に使用できるBlueXPのサービスと機能が決まります。たとえば、Cloud Volumes ONTAPを導入して管理する場合は、コネクタをクラウドにインストールする必要があります。 "プライベートモードの詳細"。

手順**3**：ホスト要件を確認する

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

専用ホスト

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

サポートされているオペレーティングシステム

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

  ホストがRed Hat Subscription Managementに登録されている必要があります。登録されていない場合、ホストはコネクタのインストール時に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。

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

ハイパーバイザー

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

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

CPU

4 コアまたは 4 個の vCPU

RAM

14GB

AWS EC2 インスタンスタイプ

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

Azure VM サイズ

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

Google Cloudマシンのタイプ

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

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

/opt のディスクスペース

100GiB のスペースが使用可能である必要があります

/var のディスク領域

20GiB のスペースが必要です

Docker Engine の略

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

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

"インストール手順を確認します"

手順**4**：コネクタのネットワークを準備する

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

ターゲットネットワークへの接続

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

日常業務のエンドポイント

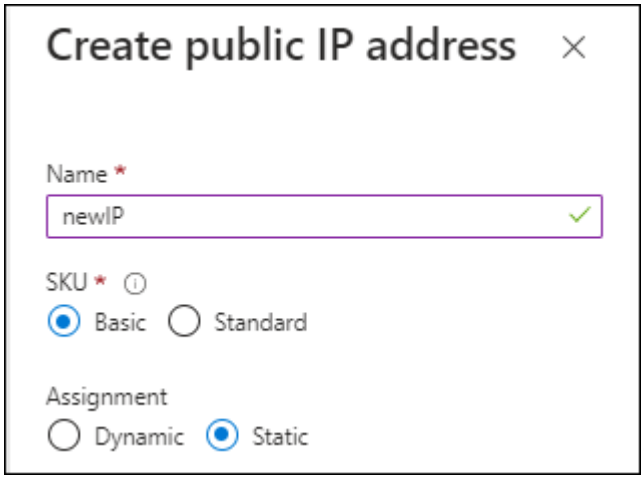
コネクタは、次のエンドポイントに接続して、パブリッククラウド環境内のリソースとプロセスを管理します。

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

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

Azureのパブリック**IP**アドレス

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



フィールドで[Basic]を選択できます。"]

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

"Azureのドキュメント：パブリックIP SKU"

プロキシサーバ

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

- IP アドレス
- クレデンシャル
- HTTPS証明書

BlueXPでは透過型プロキシサーバはサポートされません。

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

ポート

コネクタへの着信トラフィックは、開始しない限りありません。

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

NTPを有効にする

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

ステップ**5**：クラウドの権限を準備する

コネクタがクラウドにインストールされていて、Cloud Volumes ONTAPシステムを作成する場合は、クラウドプロバイダからBlueXPの権限が必要です。クラウドプロバイダで権限を設定し、インストール後にそれらの権限をコネクタインスタンスに関連付ける必要があります。

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

AWS IAMロール

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

手順

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

結果

これで、コネクタEC2インスタンスのIAMロールが作成されました。

AWSアクセスキー

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

手順

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

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

   標準のリージョンでは、権限は2つのポリシーに分散されます。AWSの管理対象ポリシーの最大文字数に制限されているため、2つのポリシーが必要です。 "コネクタのIAMポリシーの詳細については、こちらを参照してください"。

3. IAMユーザにポリシーを適用します。
   - "AWS のドキュメント：「 Creating IAM Roles"
   - "AWS のドキュメント：「 Adding and Removing IAM Policies"
4. コネクタのインストール後にBlueXPに追加できるアクセスキーがユーザに割り当てられていることを確認します。

結果

これで、アカウントに必要な権限が付与されました。

Azureロール

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

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

手順

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

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

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

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

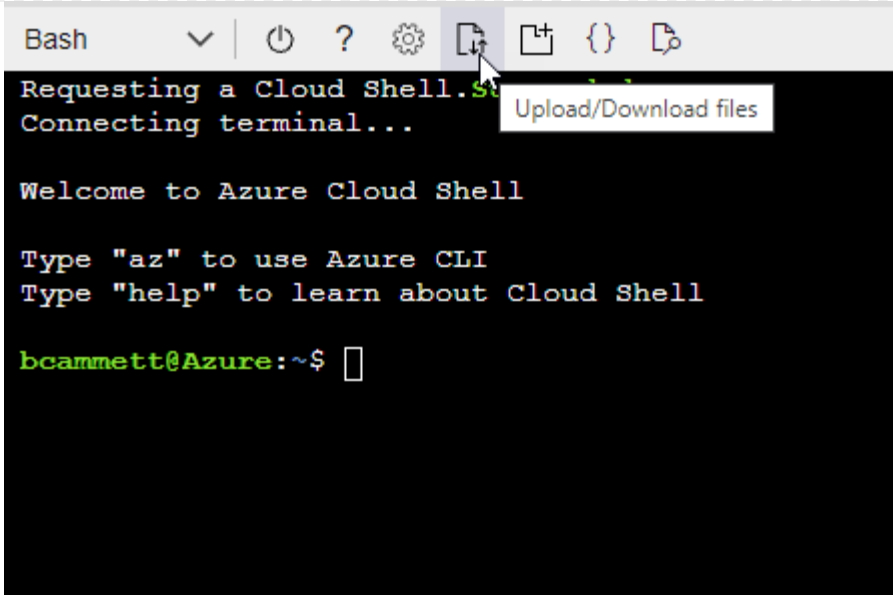
   - 例 *

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

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

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

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



c. Azure CLIを使用してカスタムロールを作成します。

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

結果

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

Azureサービスプリンシパル

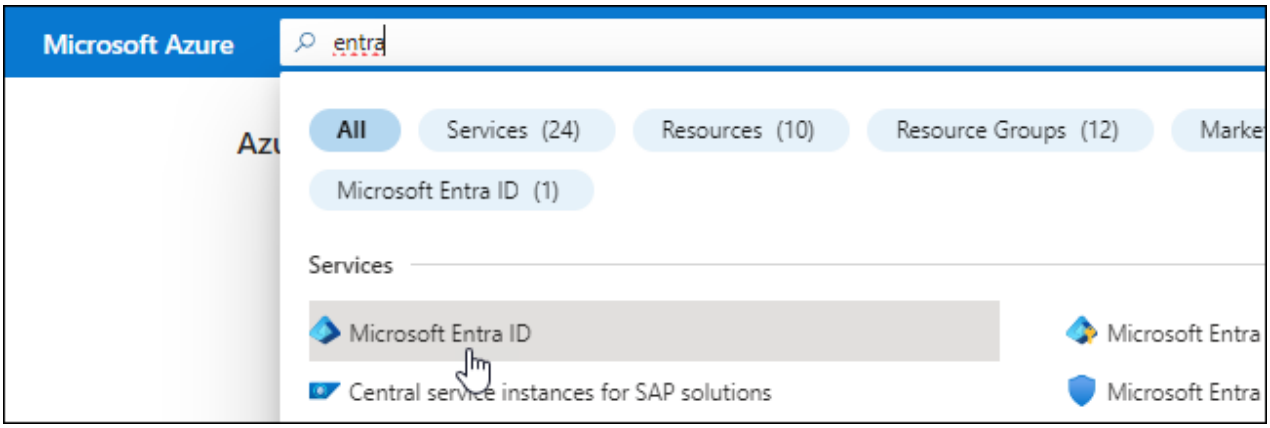
Microsoft Entra IDでサービスプリンシパルを作成してセットアップし、BlueXPに必要なAzureクレデンシャルを取得します。これらのクレデンシャルは、コネクタをインストールしてBlueXPをセットアップしたあとにBlueXPに提供する必要があります。

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

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

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

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



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

   AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

1. カスタムロールを作成します。

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

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

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

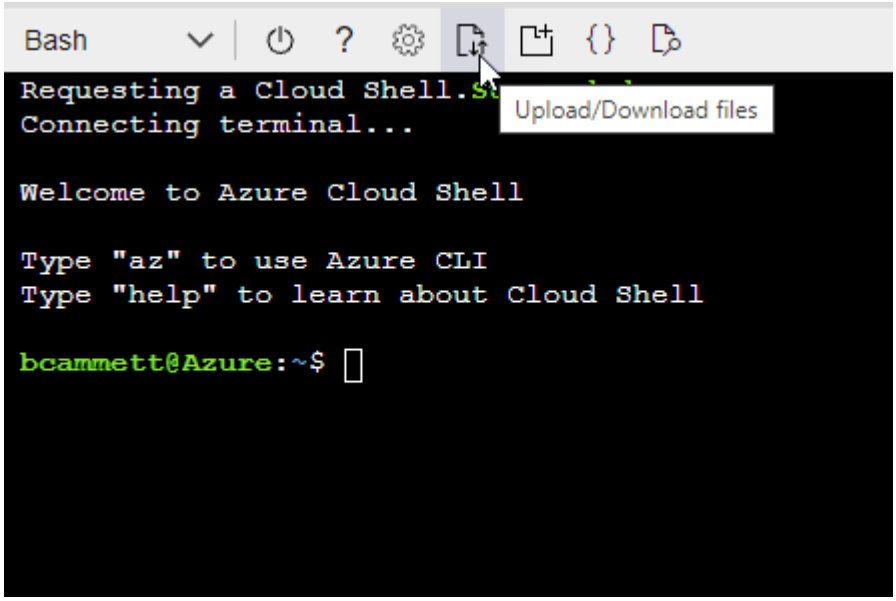
      - 例 *

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

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

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

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



- Azure CLIを使用してカスタムロールを作成します。

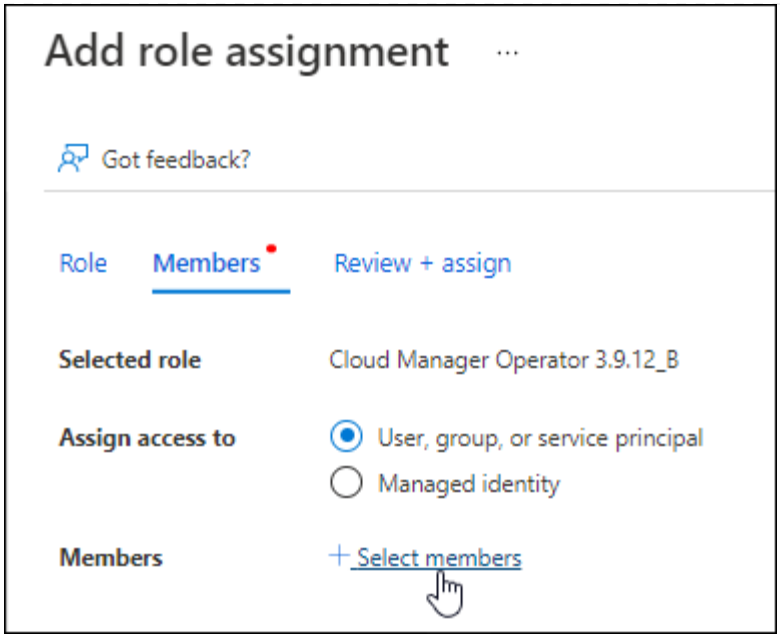
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. ロールにアプリケーションを割り当てます。

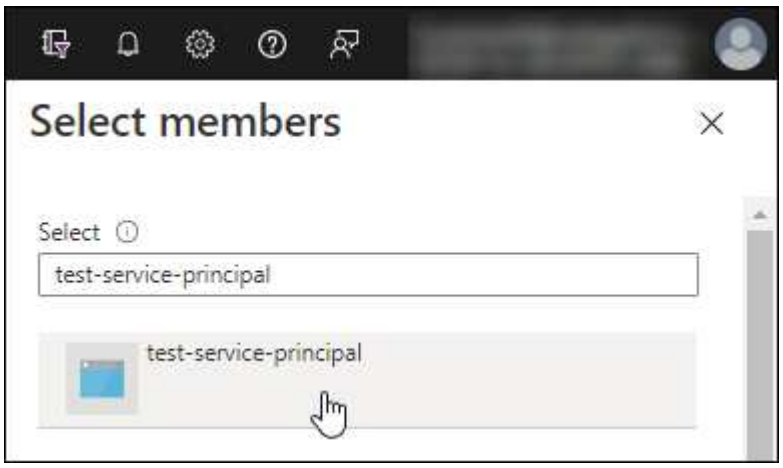
   a. Azure ポータルで、 * Subscriptions * サービスを開きます。
   b. サブスクリプションを選択します。
   c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。
   d. [ロール]タブで、**[BlueXP Operator]***ロールを選択し、[次へ]*を選択します。
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

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



- アプリケーションの名前を検索します。

  次に例を示します。



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

f. [Review + Assign]*を選択します。

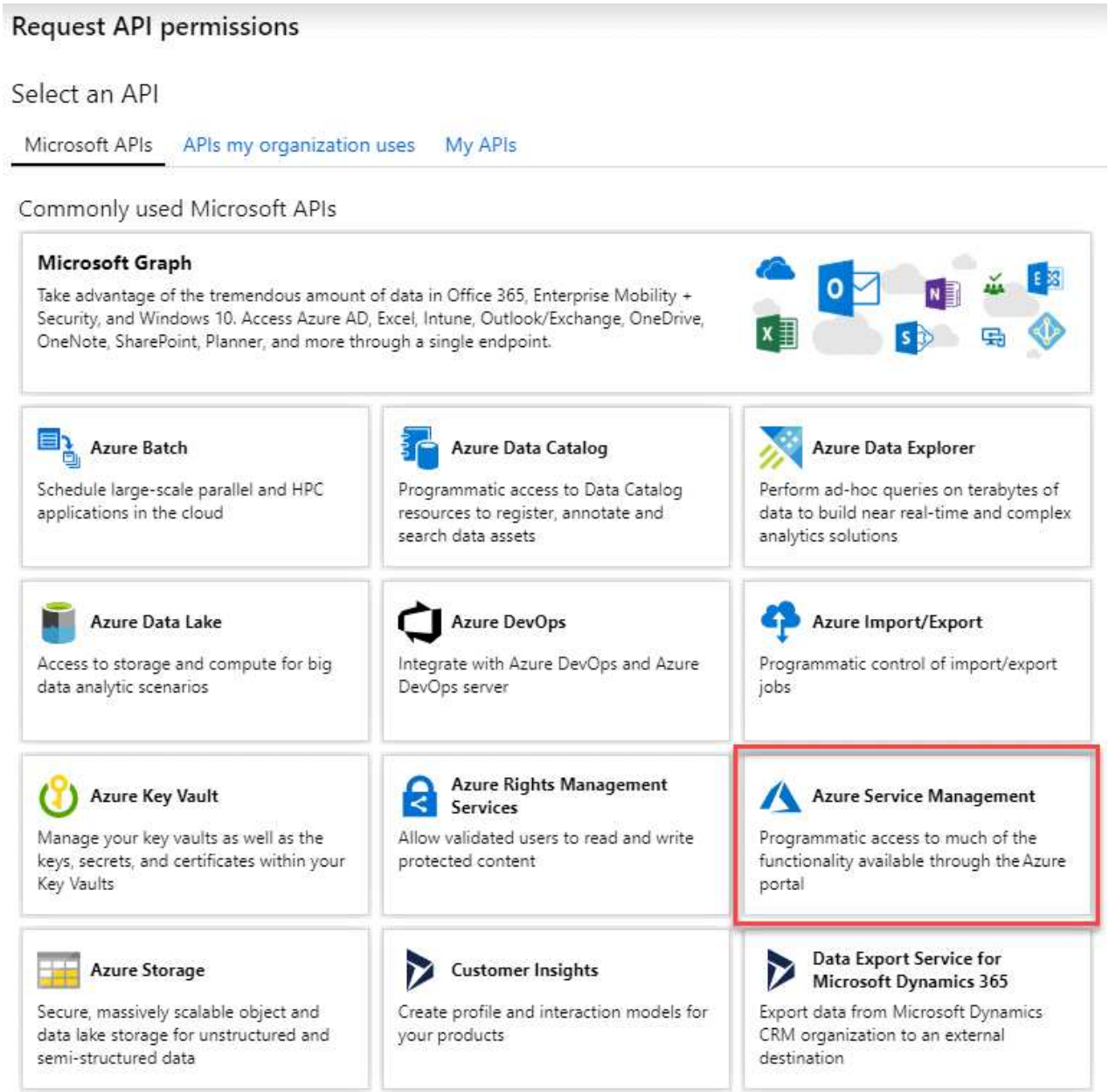
サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

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

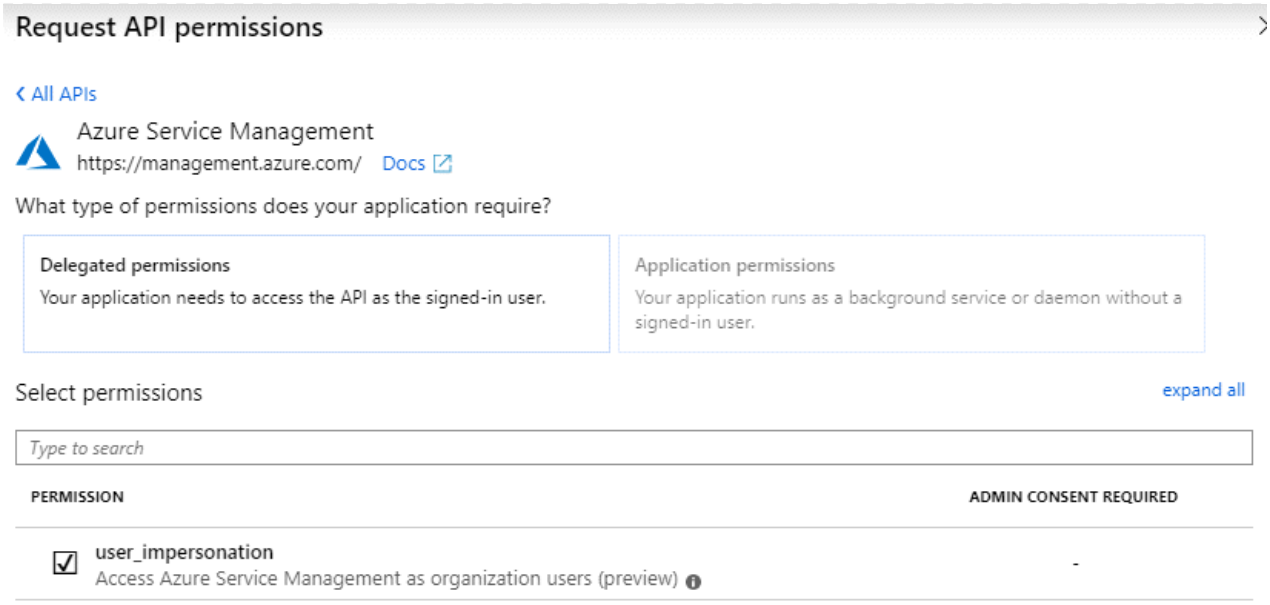
Windows Azure Service Management API 権限を追加します

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

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

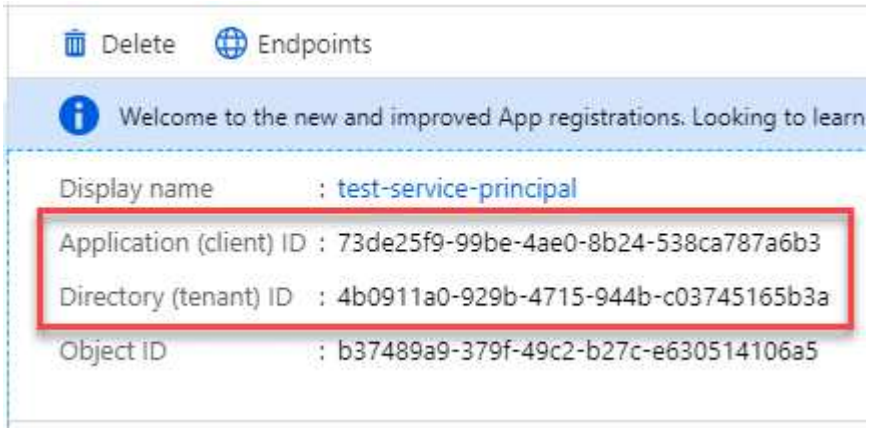


4. を選択し、[Add permissions]*を選択します。



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

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



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

クライアントシークレットを作成します

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

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

結果

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

Google Cloudサービスアカウント

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

手順

1. Google Cloudでカスタムロールを作成します。

   a. で定義された権限を含むYAMLファイルを作成します "Google Cloudのコネクタポリシー"。

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

   c. コネクタに必要な権限を含むYAMLファイルをアップロードします。

   d. を使用して、カスタムロールを作成します `gcloud iam roles create` コマンドを実行します

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

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

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

2. Google Cloudでサービスアカウントを作成します。

   a. IAMおよび管理サービスから、*サービスアカウント>サービスアカウントの作成*を選択します。

   b. サービスアカウントの詳細を入力し、*作成して続行*を選択します。

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

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

結果

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

ステップ**6**：**Google Cloud API**を有効にする

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

ステップ

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

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

コネクタをプライベートモードで展開します

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

手順**1**：コネクタを取り付ける

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

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

作業を開始する前に

コネクタをインストールするには root 権限が必要です。

手順

1. Docker が有効で実行されていることを確認します。

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

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

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

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

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

<version> は、ダウンロードしたコネクタのバージョンです。

5. インストールスクリプトを実行します。

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

<version> は、ダウンロードしたコネクタのバージョンです。

結果

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

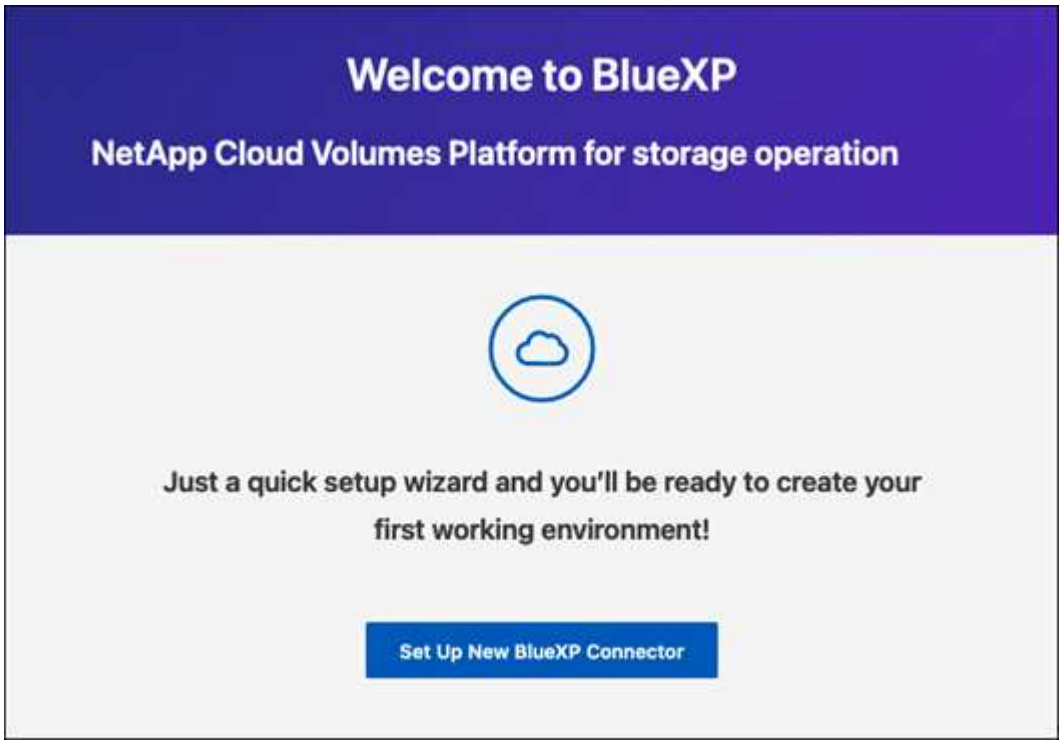
ステップ**2**：**BlueXP**をセットアップする

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

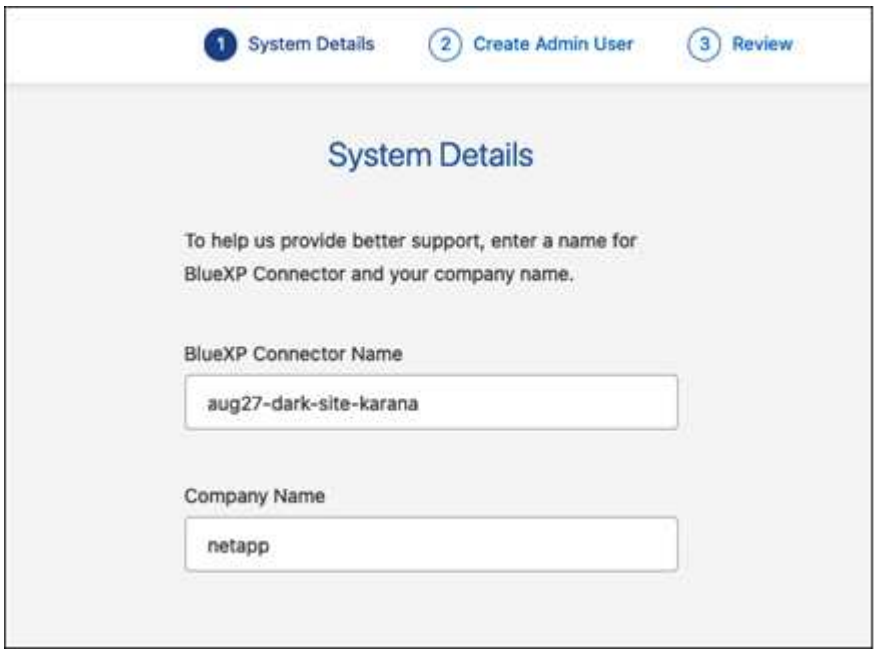
手順

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

   次の画面が表示されます。



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



   - 管理者ユーザーの作成：システムの管理者ユーザーを作成します。

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

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

結果

これでコネクタがインストールされ、セットアップされました。

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

次の手順

以前に設定した権限をBlueXPに付与します。

ステップ**3**：**BlueXP**への権限を付与する

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

"クラウドへのアクセス許可を準備する方法をご確認ください"。

AWS IAMロール

以前に作成したIAMロールをコネクタEC2インスタンスにアタッチします。

手順

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

結果

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

AWSアクセスキー

必要な権限を持つIAMユーザのAWSアクセスキーをBlueXPに渡します。

手順

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

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

結果

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

Azureロール

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

手順

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

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

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

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

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

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

結果

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

Azureサービスプリンシパル

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

手順

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

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

結果

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

Google Cloudサービスアカウント

サービスアカウントをコネクタVMに関連付けます。

手順

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

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

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

結果

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

次に実行できる操作（プライベートモード）

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

ヘルプについては、次のドキュメントを参照してください。

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

関連リンク

"BlueXPの導入モード"

BlueXPにログインします

BlueXPへのログイン方法は、アカウントで使用しているBlueXP導入モードによって異なります。

標準モード

BlueXPに登録すると、Webベースのコンソールからログインしてデータとストレージインフラの管理を開始できます。

このタスクについて

BlueXPのWebベースのコンソールには、次のいずれかの方法でログインできます。

- 既存のNetApp Support Site （NSS）のクレデンシャルを必要に応じて変更
- Eメールアドレスとパスワードを使用したネットアップクラウドへのログイン
- フェデレーテッド接続

  シングルサインオンを使用して、社内ディレクトリ（フェデレーション ID ）からのクレデンシャルを使用してログインできます。 "BlueXPでアイデンティティフェデレーションを使用する方法をご紹介します"。

手順

1. Webブラウザを開き、にアクセスします "BlueXPコンソール"
2. [ログイン*]ページで、ログインに関連付けられている電子メールアドレスを入力します。
3. ログインに関連付けられている認証方法に応じて、クレデンシャルの入力を求められます。
   - ネットアップクラウドクレデンシャル：パスワードを入力します
   - フェデレーテッドユーザ：フェデレーテッドアイデンティティクレデンシャルを入力します
   - NetApp Support Site アカウント：NetApp Support Site クレデンシャルを入力します

結果

ログインして、BlueXPを使用してハイブリッドマルチクラウドインフラを管理できるようになりました。

制限モード

制限モードでBlueXPを使用する場合は、コネクタでローカルに実行されるユーザインターフェイスからBlueXPコンソールにログインする必要があります。

このタスクについて

BlueXPでは、アカウントが制限モードで設定されている場合、次のいずれかの方法でログインできます。

- Eメールアドレスとパスワードを使用したネットアップクラウドへのログイン
- フェデレーテッド接続

  シングルサインオンを使用して、社内ディレクトリ（フェデレーション ID ）からのクレデンシャルを使用してログインできます。 "BlueXPでアイデンティティフェデレーションを使用する方法をご紹介します"。

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、コネクタをインストールしたホストの構成に応じて、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、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る場合があります。

2. ログインするためのユーザ名とパスワードを入力します。

結果

ログインして、BlueXPを使用してハイブリッドマルチクラウドインフラを管理できるようになりました。

プライベートモード

BlueXPをプライベートモードで使用する場合は、コネクタでローカルに実行されるユーザインターフェイスからBlueXPコンソールにログインする必要があります。

このタスクについて

プライベートモードでは、ローカルユーザの管理とアクセスがサポートされます。BlueXPのクラウドサービスでは認証が行われません。

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、コネクタをインストールしたホストの構成に応じて、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、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る場合があります。

2. ログインするためのユーザ名とパスワードを入力します。

結果

ログインして、BlueXPを使用してハイブリッドマルチクラウドインフラを管理できるようになりました。

BlueXPを管理します

BlueXPでアイデンティティフェデレーションを使用

アイデンティティフェデレーション_ BlueXPとのシングルサインオンを有効にして、ユーザが自社のアイデンティティのクレデンシャルを使用してログインできるようにします。まず、アイデンティティフェデレーションとBlueXPの連携について説明し、セットアッププロセスの概要を確認してください。

NSSクレデンシャルを使用したアイデンティティフェデレーション

NetApp Support Site （NSS）クレデンシャルを使用してBlueXPにログインする場合は、このページの手順に従ってアイデンティティフェデレーションを設定しないでください。代わりに、次の手順を実行してください。

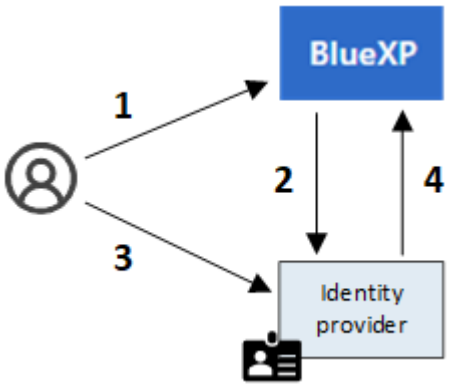
- をダウンロードして実行します "ネットアップフェデレーションリクエストフォーム"
- フォームに指定されたメールアドレスにフォームを送信します

ネットアップのIDおよびアクセス管理チームがリクエスト内容を確認します。

アイデンティティフェデレーションの仕組み

アイデンティティフェデレーションを設定すると、BlueXPの認証サービスプロバイダ（Auth0）と独自のアイデンティティ管理プロバイダの間に信頼関係が確立されます。

次の図は、アイデンティティフェデレーションとBlueXPの連携を示しています。



1. ユーザがBlueXPのログインページでEメールアドレスを入力します。
2. BlueXPは、Eメールドメインがフェデレーテッド接続の一部であることを特定し、信頼された接続を使用して認証要求をアイデンティティプロバイダに送信します。

   フェデレーテッド接続を設定すると、BlueXPでは常にそのフェデレーテッド接続が認証に使用されます。

3. ユーザは、社内ディレクトリのクレデンシャルを使用して認証されます。
4. アイデンティティプロバイダがユーザのIDを認証し、ユーザがBlueXPにログインします。

アイデンティティフェデレーションでは、Security Assertion Markup Language 2.0（SAML）やOpenID Connect（OIDC）などのオープン標準が使用されます。

サポートされている**IDプロバイダ**

BlueXPは次のIDプロバイダをサポートしています。

- Security Assertion Markup Language（SAML）アイデンティティプロバイダ
- MicrosoftエントラID
- Active Directory フェデレーションサービス（ ADFS ）
- PingFederate

BlueXPでは、サービスプロバイダ主導（SP主導）のSSOのみがサポートされます。アイデンティティプロバイダが開始する（IdPが開始する）SSOはサポートされていません。

セットアッププロセスの概要

BlueXPとアイデンティティ管理プロバイダの間の接続をセットアップする前に、必要な準備手順を理解しておく必要があります。

以下の手順は、ネットアップのクラウドログインを使用してBlueXPにログインするユーザに固有のものです。NSSクレデンシャルを使用してBlueXPにログインする場合は、 NSSクレデンシャルを使用してアイデンティティフェデレーションを設定する方法について説明します。

SAMLアイデンティティプロバイダ

概要として、BlueXPとSAMLアイデンティティプロバイダの間にフェデレーテッド接続を設定する手順は次のとおりです。

ステップ	完了者	説明
1.	Active Directory（AD）管理者	SAMLアイデンティティプロバイダを設定して、BlueXPとのアイデンティティフェデレーションを有効にします。 SAML IDプロバイダの手順を表示します。 • "ADFS （ADFS）" • "オクタ" • "OneLogin" • "PingFederate" • "Salesforce" • "SiteMinder" • "SSOCircleの略" お使いのアイデンティティプロバイダが上記のリストに表示されない場合は、 "以下の一般的な手順に従ってください" DO_NOT_Auth0で接続を作成する方法を説明する手順を完了します。この接続は次のステップで作成します。
2.	BlueXPの管理者	にアクセスします "[NetApp Federation Setupページ"^] BlueXPとの接続を確立します。 この手順を完了するには、アイデンティティプロバイダに関する次の情報をAD管理者から入手する必要があります。 • サインインURL • X509署名証明書（PEMまたはCER形式） • サインアウトURL（オプション） この情報を使用して接続を作成すると、[フェデレーションセットアップ]ページに、次の手順で設定を完了するためにAD管理者に送信できるパラメータが一覧表示されます。 証明書の有効期限をメモします。[フェデレーションセットアップ]ページに戻り、証明書_before_itの有効期限を更新する必要があります。これはあなたの責任です。BlueXPでは有効期限は追跡されません。ADチームと協力して、時間通りにアラートを受け取ることをお勧めします。
3.	AD管理者	手順2が完了したら、[フェデレーションセットアップ]ページに表示されたパラメータを使用してアイデンティティプロバイダで設定を完了します。
4.	BlueXPの管理者	から接続をテストして有効にします "[NetApp Federation Setupページ"^] 接続をテストしてから接続を有効にするまでの間に、ページが更新されることに注意してください。

Microsoftエントラ**ID**

概して、BlueXPとMicrosoft Entra IDの間にフェデレーテッド接続を設定する手順は次のとおりです。

ステップ	完了者	説明
1.	AD管理者	BlueXPでアイデンティティフェデレーションを有効にするには、Microsoft Entra IDを設定します。 "Microsoft Entra IDにアプリケーションを登録する手順を表示する" DO_NOT_Auth0で接続を作成する方法を説明する手順を完了します。この接続は次のステップで作成します。
2.	BlueXPの管理者	にアクセスします "[NetApp Federation Setupページ"^] BlueXPとの接続を確立します。 この手順を完了するには、AD管理者から次の情報を入手する必要があります。 • クライアント ID • クライアントシークレット値 • Microsoft Entra IDドメイン この情報を使用して接続を作成すると、[フェデレーションセットアップ]ページに、次の手順で設定を完了するためにAD管理者に送信できるパラメータが一覧表示されます。 シークレットキーの有効期限をメモします。[フェデレーションセットアップ]ページに戻り、証明書_before_itの有効期限を更新する必要があります。これはあなたの責任です。BlueXPでは有効期限は追跡されません。ADチームと協力して、時間通りにアラートを受け取ることをお勧めします。
3.	AD管理者	手順2が完了したら、[フェデレーションセットアップ]ページに表示されているパラメータを使用して、Microsoft Entra IDで設定を完了します。
4.	BlueXPの管理者	から接続をテストして有効にします "[NetApp Federation Setupページ"^] 接続をテストしてから接続を有効にするまでの間に、ページが更新されることに注意してください。

ADFS （ADFS）

BlueXPとADFSの間にフェデレーテッド接続を設定する手順の概要は次のとおりです。

ステップ	完了者	説明
1.	AD管理者	BlueXPとのアイデンティティフェデレーションを有効にするようにADFSサーバを設定します。 "Auth0を使用してADFSサーバを構成する手順を表示します"
2.	BlueXPの管理者	にアクセスします "[NetApp Federation Setupページ"^] BlueXPとの接続を確立します。 この手順を完了するには、AD管理者からADFSサーバーまたはフェデレーションメタデータファイルのURLを取得する必要があります。 この情報を使用して接続を作成すると、[フェデレーションセットアップ]ページに、次の手順で設定を完了するためにAD管理者に送信できるパラメータが一覧表示されます。 証明書の有効期限をメモします。[フェデレーションセットアップ]ページに戻り、証明書_before_itの有効期限を更新する必要があります。これはあなたの責任です。BlueXPでは有効期限は追跡されません。ADチームと協力して、時間通りにアラートを受け取ることをお勧めします。
3.	AD管理者	手順2が完了したら、[フェデレーションセットアップ]ページに表示されているパラメータを使用して、ADFSサーバーで設定を完了します。
4.	BlueXPの管理者	から接続をテストして有効にします "[NetApp Federation Setupページ"^] 接続をテストしてから接続を有効にするまでの間に、ページが更新されることに注意してください。

PingFederate

BlueXPとPingFederateサーバの間にフェデレーテッド接続を設定するには、次の手順を実行します。

ステップ	完了者	説明
1.	AD管理者	BlueXPでアイデンティティフェデレーションを有効にするようにPingFederateサーバを設定します。 "接続の作成手順を表示します" DO_NOT_Auth0で接続を作成する方法を説明する手順を完了します。この接続は次のステップで作成します。

ステップ	完了者	説明
2.	BlueXPの管理者	にアクセスします "[NetApp Federation Setupページ"^] BlueXPとの接続を確立します。 この手順を完了するには、AD管理者から次の情報を入手する必要があります。 • PingFederateサーバのURL • X509署名証明書（PEMまたはCER形式） この情報を使用して接続を作成すると、[フェデレーションセットアップ]ページに、次の手順で設定を完了するためにAD管理者に送信できるパラメータが一覧表示されます。 ⓘ 証明書の有効期限をメモします。[フェデレーションセットアップ]ページに戻り、証明書_before_itの有効期限を更新する必要があります。これはあなたの責任です。BlueXPでは有効期限は追跡されません。ADチームと協力して、時間通りにアラートを受け取ることをお勧めします。
3.	AD管理者	手順2が完了したら、[フェデレーションセットアップ]ページに表示されたパラメータを使用して、PingFederateサーバーで設定を完了します。
4.	BlueXPの管理者	から接続をテストして有効にします "[NetApp Federation Setupページ"^] 接続をテストしてから接続を有効にするまでの間に、ページが更新されることに注意してください。

フェデレーテッド接続を更新しています

BlueXP管理者が接続を有効にすると、管理者はからいつでも接続を更新できます "[NetApp Federation Setupページ"^]

たとえば、新しい証明書をアップロードして接続を更新する必要がある場合があります。

接続を更新できるのは、接続を作成したBlueXP管理者のみです。管理者を追加する場合は、ネットアップサポートにお問い合わせください。

BlueXPのアカウント

BlueXPアカウントを管理します

BlueXPアカウントの作成時には、管理者ユーザとワークスペースが1人だけ含まれます。ユーザーの追加、自動化を目的としたサービスアカウントの作成、ワークスペースの追加など、組織のニーズに合わせてアカウントを管理できます。

"BlueXPアカウントの仕組みをご紹介します"。

Tenancy APIを使用してアカウントを管理します

API 要求を送信してアカウント設定を管理する場合は、 _Tenancy _API を使用する必要があります。このAPIは、Cloud Volumes ONTAP 作業環境の作成と管理に使用するBlueXP APIとは異なります。

"テナンシー API のエンドポイントを表示します"

ユーザを作成および管理します

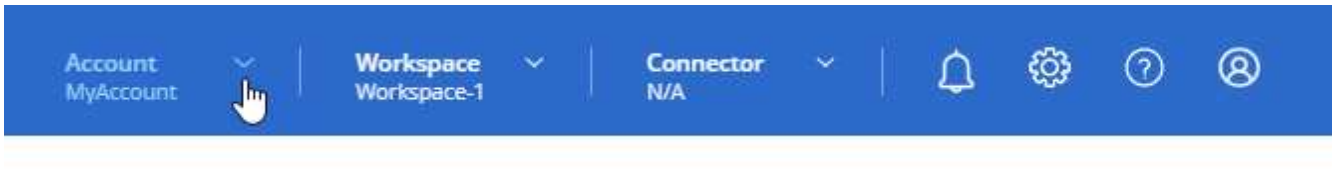
アカウントのユーザーは、特定のワークスペースのリソースにアクセスして管理できます。

ユーザを追加します

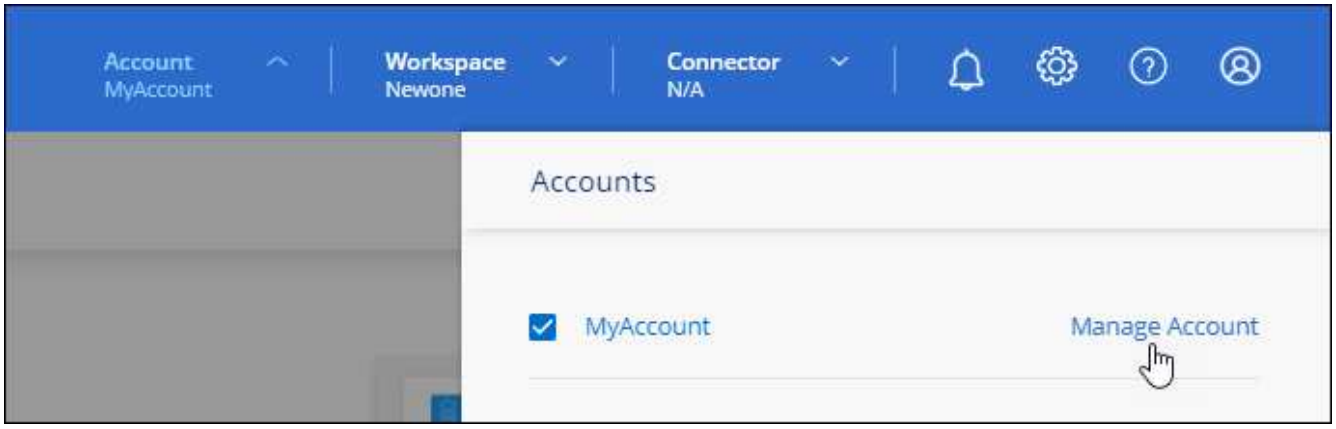
ユーザをBlueXPアカウントに関連付けて、BlueXPで作業環境を作成、管理できるようにします。

手順

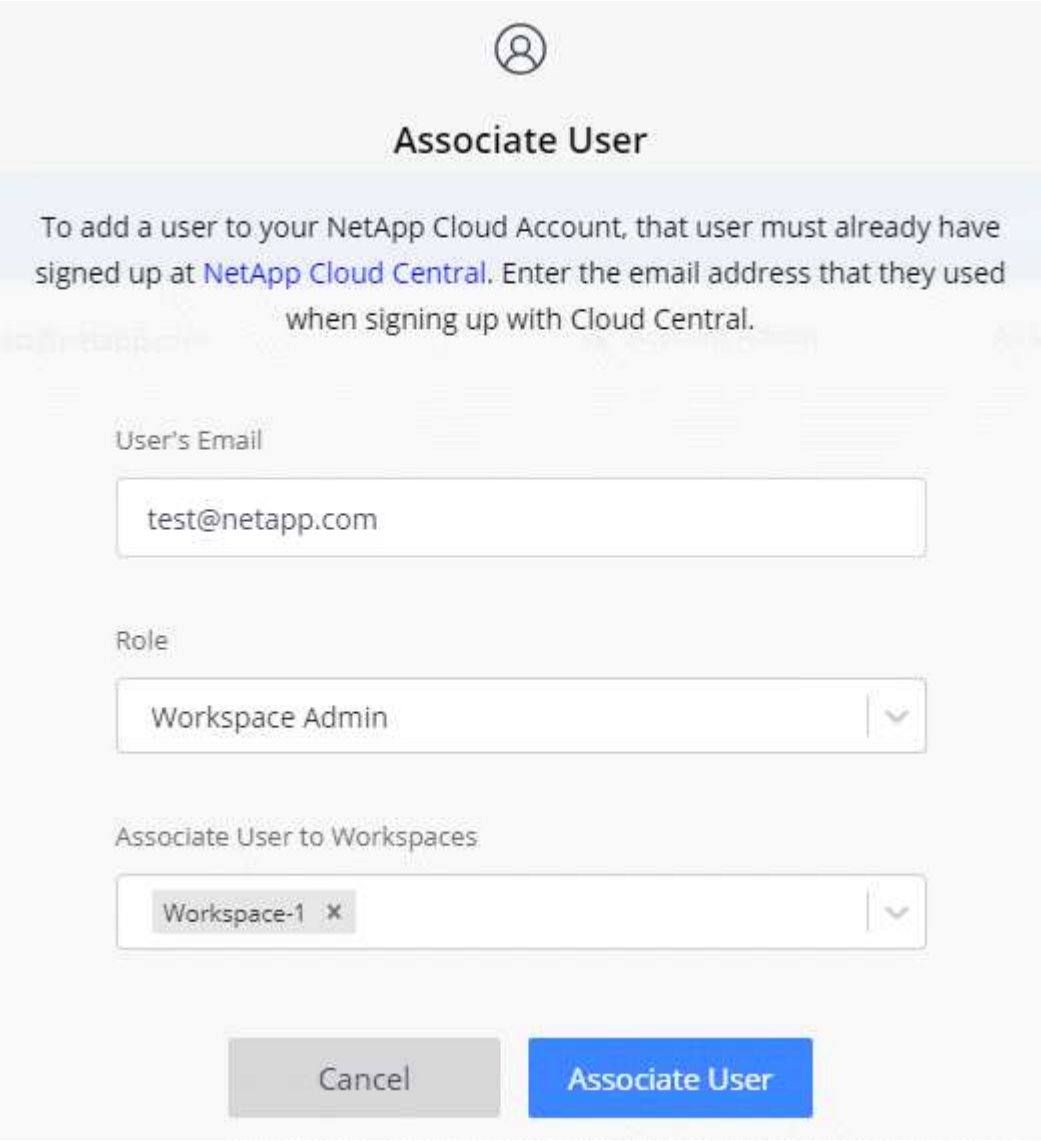
1. ユーザーがまだ行っていない場合は、にアクセスするようにユーザーに依頼します "NetApp BlueXP のWebサイト" 登録してください。
2. BlueXPの上部で、*[Account]*ドロップダウンを選択します。



3. 現在選択されているアカウントの横にある*[アカウントの管理]*を選択します。



4. [メンバー]タブで、*[ユーザーの関連付け]*を選択します。
5. ユーザの E メールアドレスを入力し、ユーザのロールを選択します。
   - **Account Admin**: BlueXPではどのようなアクションでも実行できます。
   - * ワークスペース管理者 * ：割り当てられたワークスペースでリソースを作成および管理できます。
   - * Compliance Viewer *：BlueXPの分類に関するコンプライアンス情報の表示と、アクセス権を持つワークスペースのレポートの生成のみが可能です。
6. Workspace Admin または Compliance Viewer を選択した場合は、 1 つ以上のワークスペースを選択してそのユーザーに関連付けます。



7. [関連付け]*を選択します。

結果

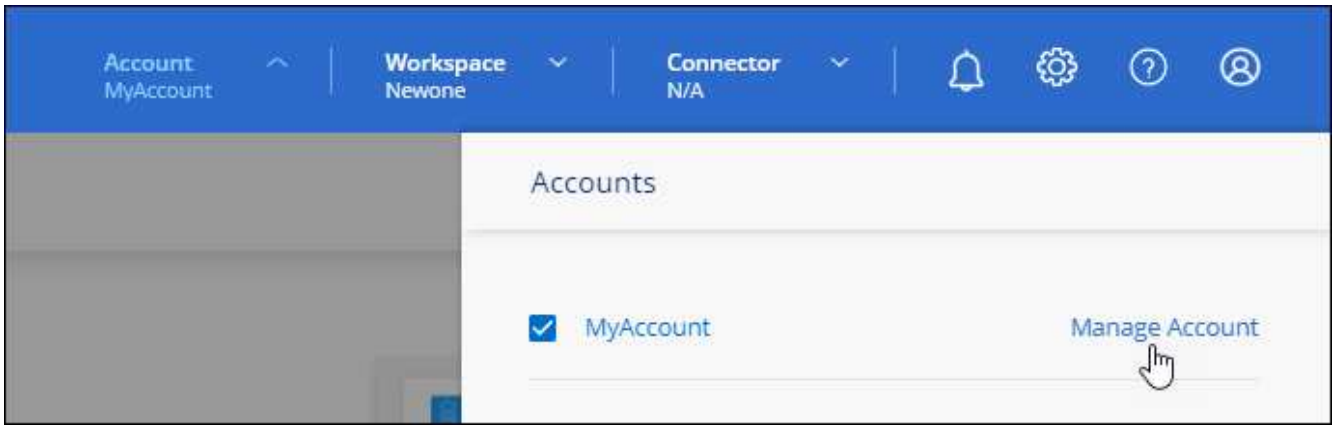
ユーザには、NetApp BlueXPの「Account Association」というタイトルのEメールが送信されます。 このメールには、BlueXPにアクセスするために必要な情報が記載されています。

ユーザを削除します

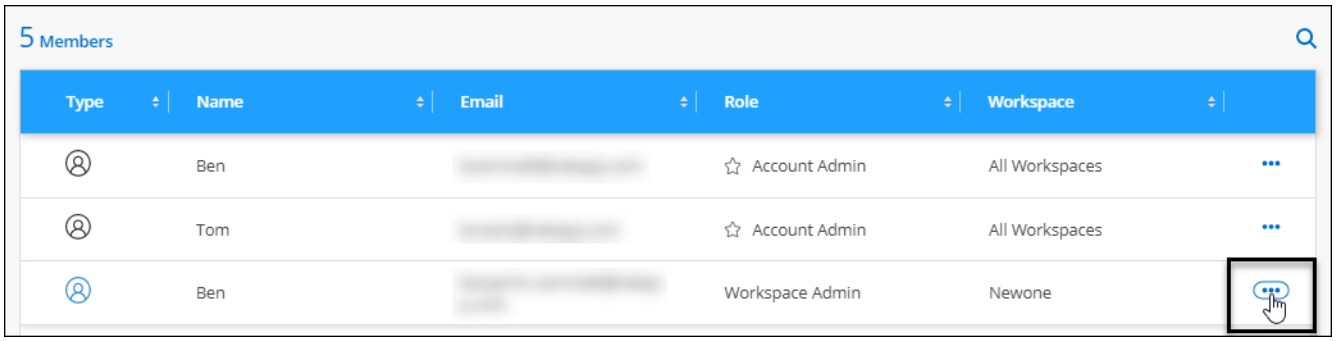
関連付けを解除すると、ユーザはBlueXPアカウントのリソースにアクセスできなくなります。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。



2. [メンバー]タブで、ユーザに対応する行のアクションメニューを選択します。



3. を選択し、[関連付けを解除]*を選択して確定します。

結果

ユーザはこのBlueXPアカウントのリソースにアクセスできなくなります。

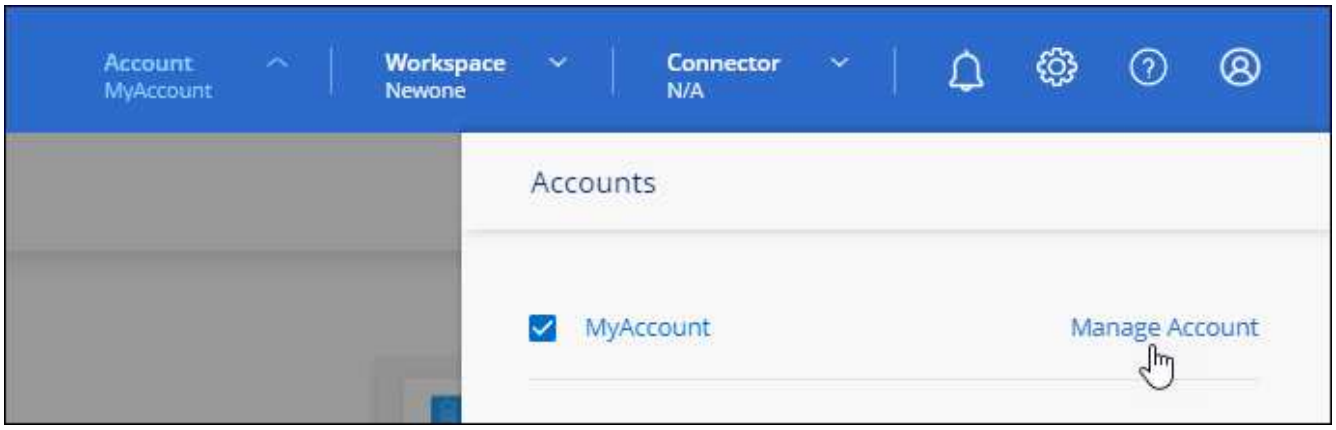
ワークスペース管理者のワークスペースを管理します

ワークスペース管理者は、いつでもワークスペースに関連付けたり、ワークスペースと関連付けを解除したりできます。ユーザーを関連付けると、ワークスペース内の作業環境を作成して表示できます。

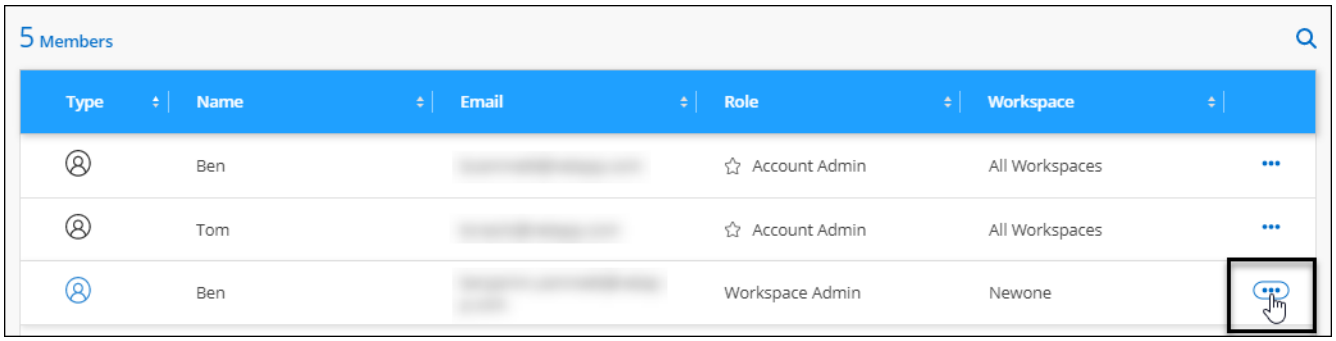
> ワークスペース管理者がBlueXPからこれらのワークスペースにアクセスできるように、コネクタをワークスペースに関連付ける必要もあります。 "コネクターのワークスペースを管理する方法について説明します。"。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。



2. [メンバー]タブで、ユーザに対応する行のアクションメニューを選択します。



3. [ワークスペースの管理]*を選択します。
4. ユーザーに関連付けるワークスペースを選択し、*適用*を選択します。

結果

コネクタがワークスペースにも関連付けられていれば、ユーザはBlueXPからこれらのワークスペースにアクセスできるようになりました。

サービスアカウントを作成および管理します

サービスアカウントは、自動化のために承認されたAPIコールをBlueXPに発信できる「ユーザ」として機能します。これにより、自動化スクリプトを作成する必要がなくなります。自動化スクリプトは、会社を離れることができる実際のユーザアカウントに基づいて作成する必要がなくなります。

サービスアカウントに権限を付与するには、他のBlueXPユーザーと同様に、サービスアカウントにロールを割り当てます。サービスアカウントを特定のワークスペースに関連付けることで、サービスがアクセスできる作業環境（リソース）を制御することもできます。

サービスアカウントを作成すると、サービスアカウントのクライアントIDとクライアントシークレットをコピーまたはダウンロードできます。このキーペアは、BlueXPでの認証に使用されます。

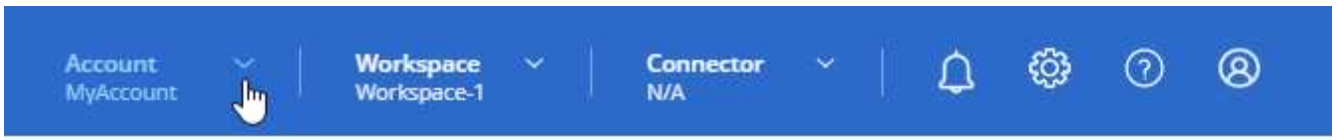
サービスアカウントを使用する場合、API処理に更新トークンは必要ありません。 "リフレッシュトークンの詳細"

サービスアカウントを作成します

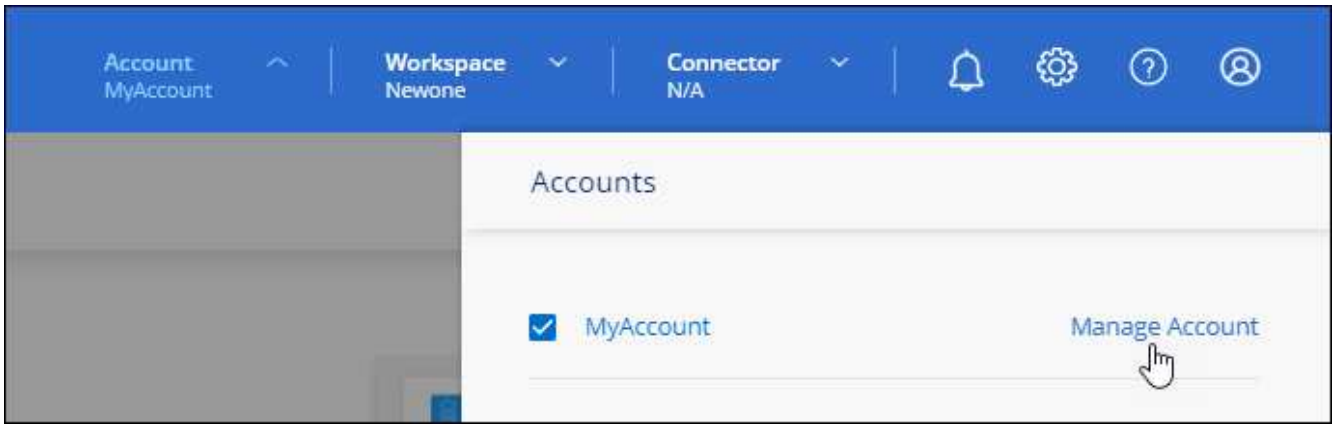
作業環境でリソースを管理するために必要な数のサービスアカウントを作成します。

手順

1. BlueXPの上部で、*[Account]*ドロップダウンを選択します。



2. 現在選択されているアカウントの横にある*[アカウントの管理]*を選択します。



3. [メンバー]タブで、*[サービスアカウントの作成]*を選択します。
4. 名前を入力し、ロールを選択します。Account Admin 以外のロールを選択した場合は、このサービスアカウントに関連付けるワークスペースを選択します。
5. 「 * Create * 」を選択します。
6. クライアント ID とクライアントシークレットをコピーまたはダウンロードします。

   クライアントシークレットは1回だけ表示され、BlueXPによってどこにも保存されません。シークレットをコピーまたはダウンロードして安全に保管します。

7. [閉じる（ Close ）] を選択します。

サービスアカウントのベアラートークンを取得します

への API 呼び出しを実行するため "テナンシー API"サービスアカウントのベアラートークンを取得する必要があります。

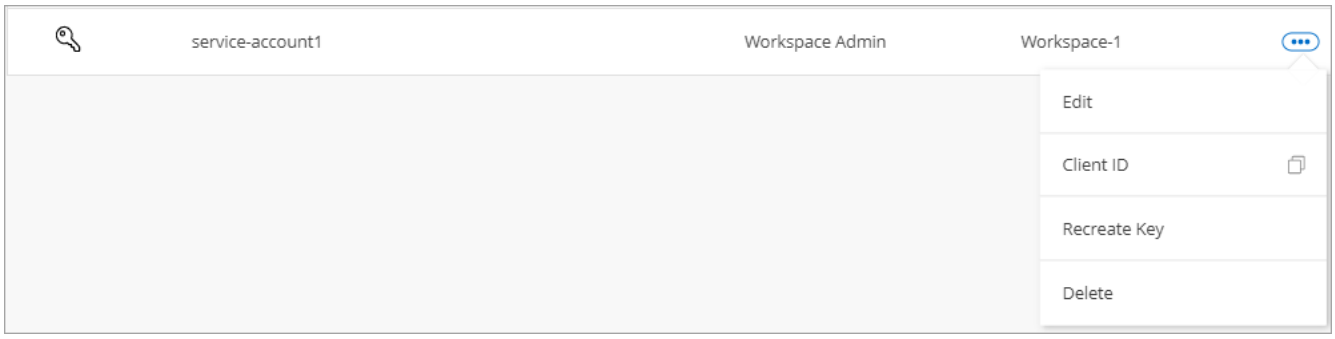
"サービスアカウントトークンの作成方法について説明します"

クライアント**ID**をコピーします

サービスアカウントのクライアント ID はいつでもコピーできます。

手順

1. [メンバー]タブで、サービスアカウントに対応する行のアクションメニューを選択します。



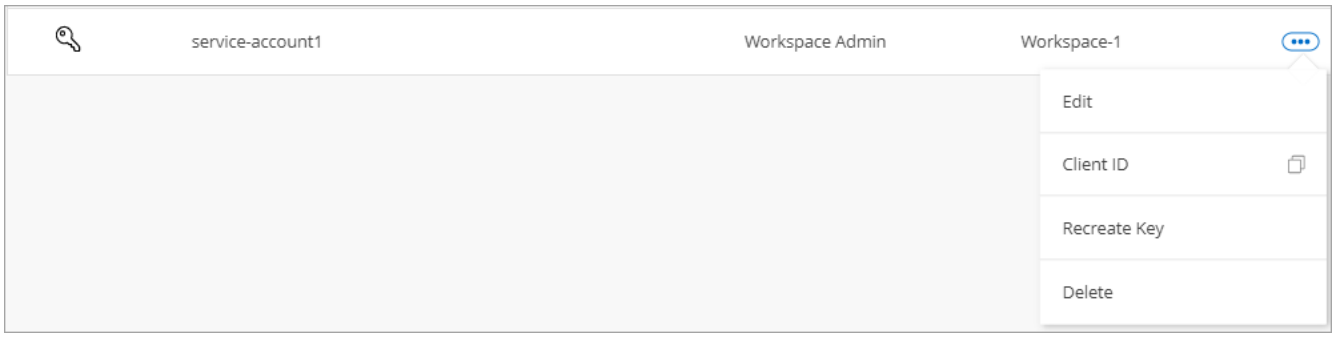
2. [Client ID]*を選択します。
3. ID がクリップボードにコピーされます。

キーを再作成します

キーを再作成すると、このサービスアカウントの既存のキーが削除され、新しいキーが作成されます。前のキーは使用できません。

手順

1. [メンバー]タブで、サービスアカウントに対応する行のアクションメニューを選択します。



2. [キーの再作成]*を選択します。
3. [再作成]*を選択して確定します。
4. クライアント ID とクライアントシークレットをコピーまたはダウンロードします。

   クライアントシークレットは1回だけ表示され、BlueXPによってどこにも保存されません。シークレットをコピーまたはダウンロードして安全に保管します。

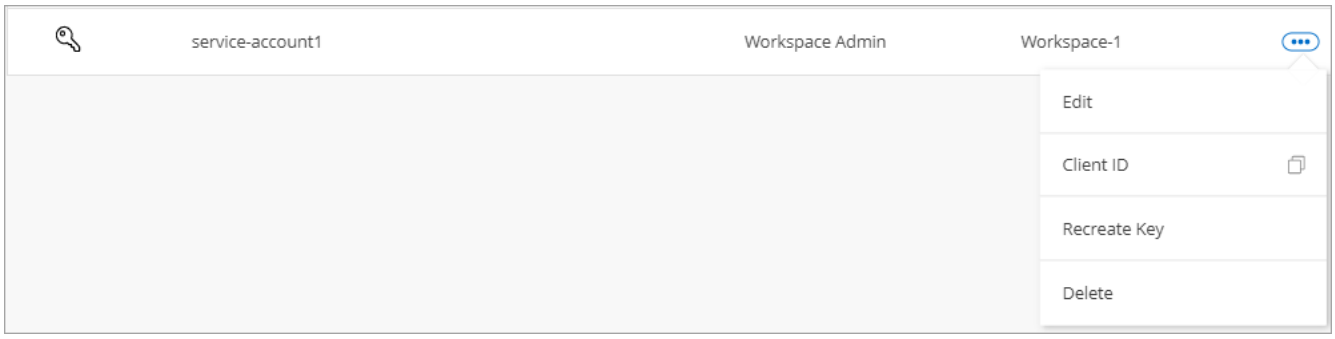
5. [閉じる（ Close ）] を選択します。

サービスアカウントを削除します

不要になったサービスアカウントを削除します。

手順

1. [メンバー]タブで、サービスアカウントに対応する行のアクションメニューを選択します。



2. 「* 削除」を選択します。
3. もう一度*[削除]*を選択して確定します。

ワークスペースを管理します

ワークスペースの作成、名前の変更、および削除により、ワークスペースを管理します。ワークスペースにリソースが含まれている場合、ワークスペースは削除できません。空である必要があります。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。
2. [ワークスペース]*を選択します。
3. 次のいずれかのオプションを選択します。
   - [新しいワークスペースの追加]*を選択して、新しいワークスペースを作成します。
   - ワークスペースの名前を変更するには、[名前の変更]*を選択します。
   - ワークスペースを削除するには、*削除*を選択します。

   新しいワークスペースを作成した場合は、そのワークスペースにコネクタも追加する必要があります。コネクタを追加しないと、ワークスペース管理者はワークスペース内のどのリソースにもアクセスできません。詳細については、次のセクションを参照してください。

コネクターのワークスペースを管理します

ワークスペース管理者がBlueXPからワークスペースにアクセスできるように、コネクタをワークスペースに関連付ける必要があります。

アカウント管理者のみがいる場合は、コネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、既定でBlueXPのすべてのワークスペースにアクセスできます。

"ユーザー、ワークスペース、コネクターの詳細をご覧ください"。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。
2. [コネクタ]*を選択します。
3. 関連付けるコネクタの*[ワークスペースの管理（Manage Workspaces）]*を選択します。
4. コネクターに関連付けるワークスペースを選択し、*適用*を選択します。

アカウント名を変更します

アカウント名はいつでも変更して、わかりやすいものに変更してください。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。
2. [概要]*タブで、アカウント名の横にある編集アイコンを選択します。
3. 新しいアカウント名を入力し、*[保存]*を選択します。

プライベートプレビューを許可します

アカウントでプライベートプレビューを許可すると、BlueXPでプレビューとして提供される新しいサービスにアクセスできます。

プライベートプレビューのサービスは、期待どおりに動作することが保証されておらず、サービスが停止したり、機能しなくなったりする可能性があります。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。
2. [* 概要 *] タブで、 [* プライベートプレビューを許可する *] 設定を有効にします。

サードパーティのサービスを許可します

アカウントのサードパーティサービスがBlueXPで利用可能なサードパーティサービスにアクセスできるようにします。サードパーティのサービスはクラウドサービスとネットアップが提供するサービスに似ていますが、サードパーティが管理とサポートを行っています。

手順

1. BlueXPの上部で、**[Account]***ドロップダウンを選択し、[Manage Account]*を選択します。
2. [* 概要 *] タブで、 [* サードパーティサービスを許可する *] 設定を有効にします。

アカウントでの処理を監視します

BlueXPが実行中の操作のステータスを監視して、対処が必要な問題がないかどうかを確認できます。通知センター、タイムラインでステータスを表示したり、メールに通知を送信したりすることができます。

次の表に、通知センターとタイムラインの比較を示します。これにより、それぞれの機能を理解できます。

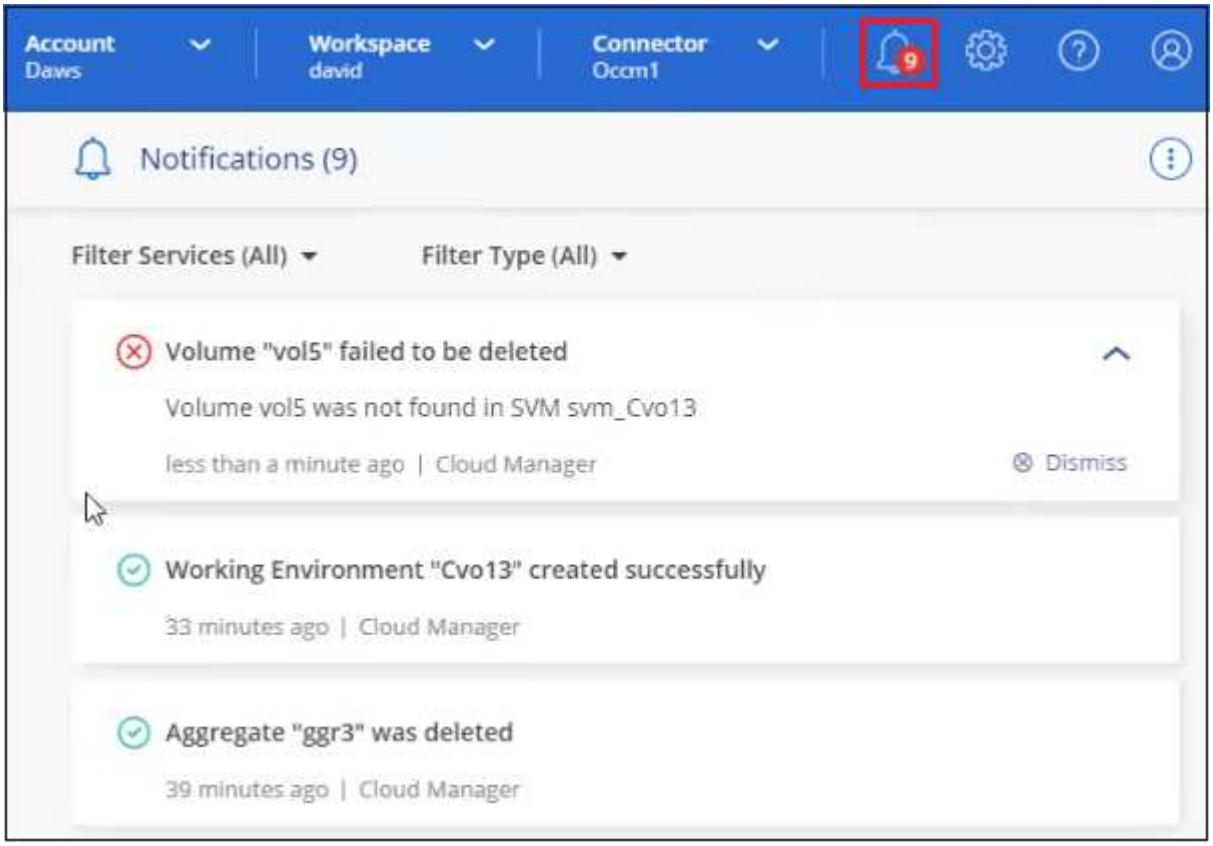
通知センター	タイムライン
イベントとアクションのステータスの概要が表示されます	各イベントまたはアクションの詳細を表示し、詳細な調査を行います
現在のログインセッションのステータスを表示します（ログオフ後、この情報は通知センターに表示されません）。	過去1カ月間のステータスを保持します
ユーザインターフェイスで開始されたアクションのみを表示します	UI または API からのすべての操作が表示されます

通知センター	タイムライン
ユーザが開始した操作を表示します	ユーザが開始したアクションとシステムが開始したアクションの両方が表示されます
結果を重要度でフィルタリングします	サービス、アクション、ユーザー、ステータスなどでフィルタリングします
アカウントユーザーおよび他のユーザーに通知を電子メールで送信する機能を提供します	Eメール機能はありません

通知センターを使用してアクティビティを監視します

通知は、BlueXPで開始した操作の進捗状況を追跡するため、操作が成功したかどうかを確認できます。これらを使用すると、現在のログインセッションで開始した多くのBlueXPアクションのステータスを表示できます。現時点では、すべてのBlueXPサービスが通知センターに情報を報告するわけではありません。

通知ベル（  ）をクリックします。ベルの小さなバブルの色は、アクティブな最上位レベルの重大度通知を示します。赤いバブルが表示されている場合は、重要な通知があることを意味します。



また、特定の種類の通知をEメールで送信するようにBlueXPを設定することで、システムにログインしていないときでも重要なシステムアクティビティを通知することができます。Eメールは、BlueXPアカウントに参加しているすべてのユーザや、特定の種類のシステムアクティビティについて注意が必要なその他の受信者に送信できます。方法を参照してください Eメール通知を設定します。

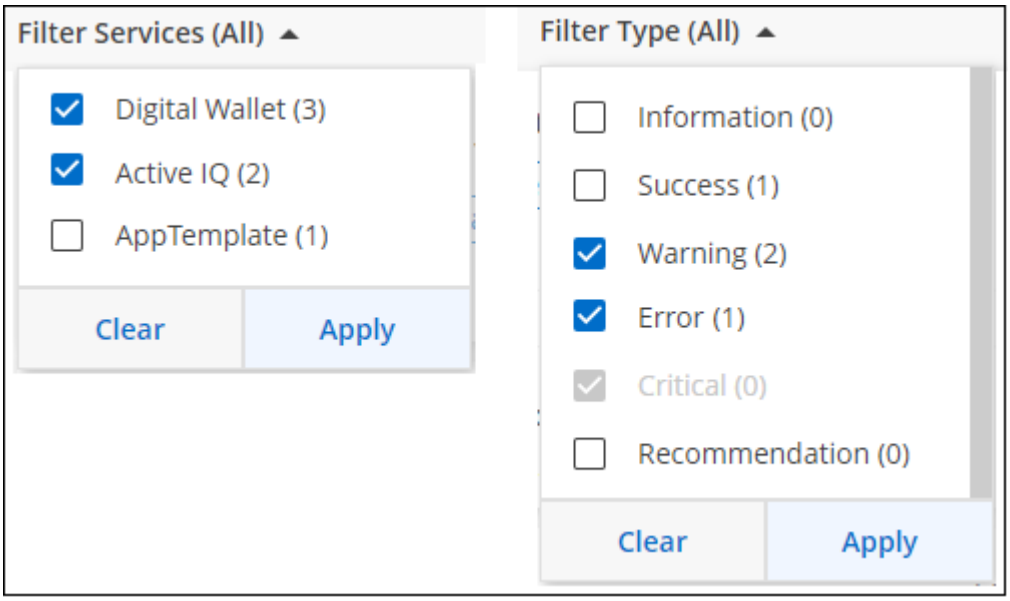
通知タイプ

通知は次のカテゴリに分類されます。

通知のタイプ	説明
重要	問題が発生しており、すぐに対処しないとサービスが停止する可能性があります。
エラー	処理またはプロセスが失敗したために終了したか、修正措置を取らなかった場合にエラーになる可能性があります。
警告	重大度に達しないことを確認するために注意が必要な問題 。この重大度の通知では原因 サービスは停止しません。早急な対処も不要です。
推奨事項	システムまたは特定のサービスを改善するためのアクションを実行することを推奨します。たとえば、コストの節約、新しいサービスの提案、推奨されるセキュリティ設定などです
情報	アクションまたはプロセスに関する追加情報 を提供するメッセージ。
成功	アクションまたはプロセスが正常に完了しました。

通知をフィルタリングします

デフォルトでは、すべてのアクティブな通知が通知センターに表示されます。表示される通知をフィルタリングして、重要な通知のみを表示できます。BlueXPの「サービス」と通知の「タイプ」でフィルタリングできます。



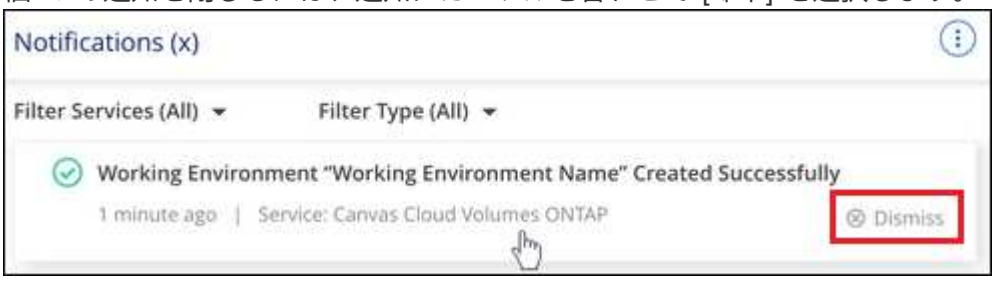
たとえば、BlueXP操作の「エラー」および「警告」通知のみを表示する場合は、これらのエントリを選択すると、これらの通知タイプのみが表示されます。

通知を却下します

通知が不要になった場合は、ページから削除できます。すべての通知を一度に却下することも、個々の通知を却下することもできます。

すべての通知を閉じるには、通知センターでを選択します ⋮ をクリックして、 [すべてを却下] を選択します。

個 々 の通知を閉じるには、通知にカーソルを合わせて*[却下]*を選択します。



Eメール通知を設定します

特定の種類の通知を電子メールで送信することで、BlueXPにログインしていない場合でも重要なシステムアクティビティを通知できます。Eメールは、BlueXPアカウントに参加しているすべてのユーザや、特定の種類のシステムアクティビティについて注意が必要なその他の受信者に送信できます。

- 現時点では、コネクタ、BlueXPデジタルウォレット、BlueXPのコピーと同期、BlueXPのバックアップとリカバリ、BlueXP階層化、BlueXP移行レポートなど、BlueXPの機能とサービスに関する通知がEメールで送信されます。サービスは今後のリリースで追加される予定です。
- Connectorがインターネットにアクセスできないサイトにインストールされている場合は、Eメール通知の送信はサポートされません。

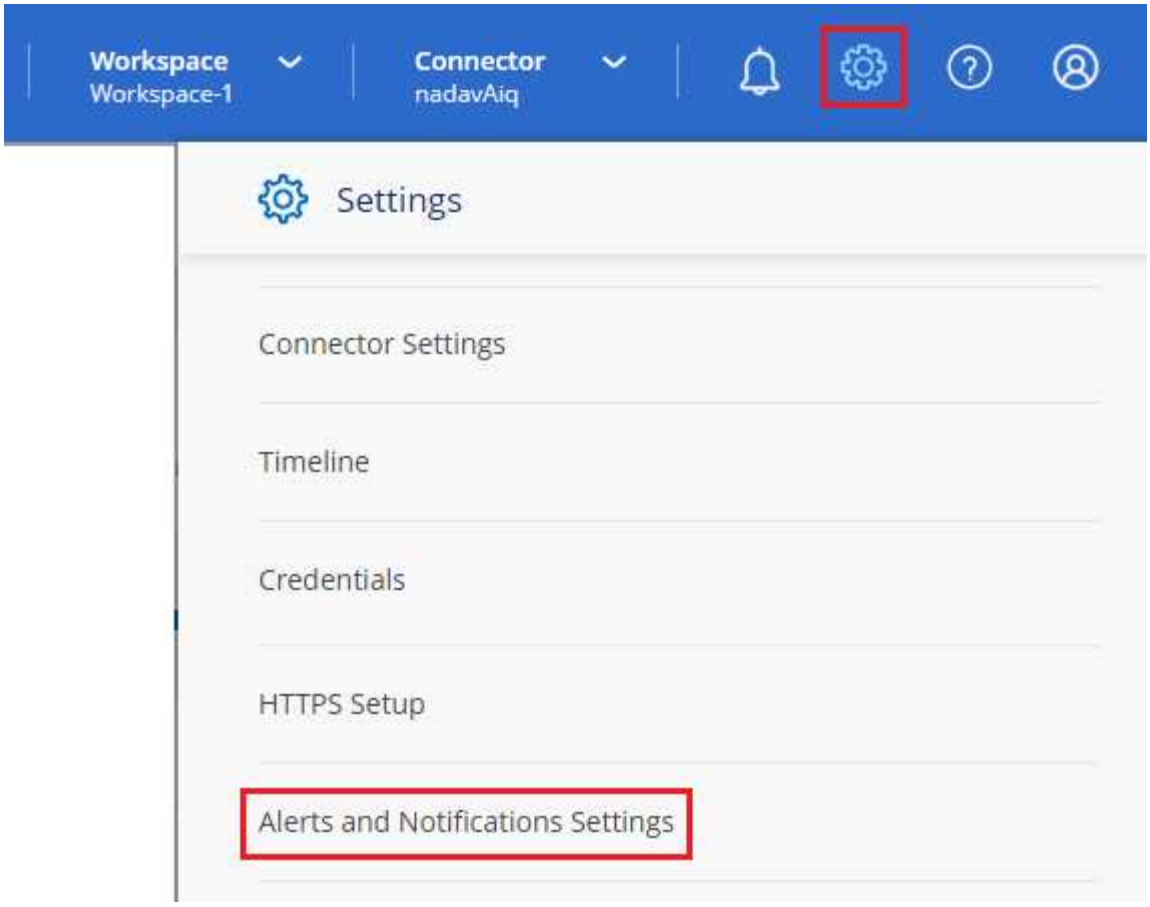
通知センターで設定したフィルタは、電子メールで受信する通知の種類を決定するものではありません。既定では、BlueXPアカウント管理者はすべての「重要」および「推奨」通知の電子メールを受信します。これらの通知はすべてのサービスに適用されます。コネクタやBlueXPのバックアップとリカバリなど、特定のサービスについてのみ通知を受け取ることはできません。

他のすべてのユーザーと受信者は、通知メールを受信しないように設定されているため、追加のユーザーの通知設定を構成する必要があります。

通知設定をカスタマイズするには、アカウント管理者である必要があります。

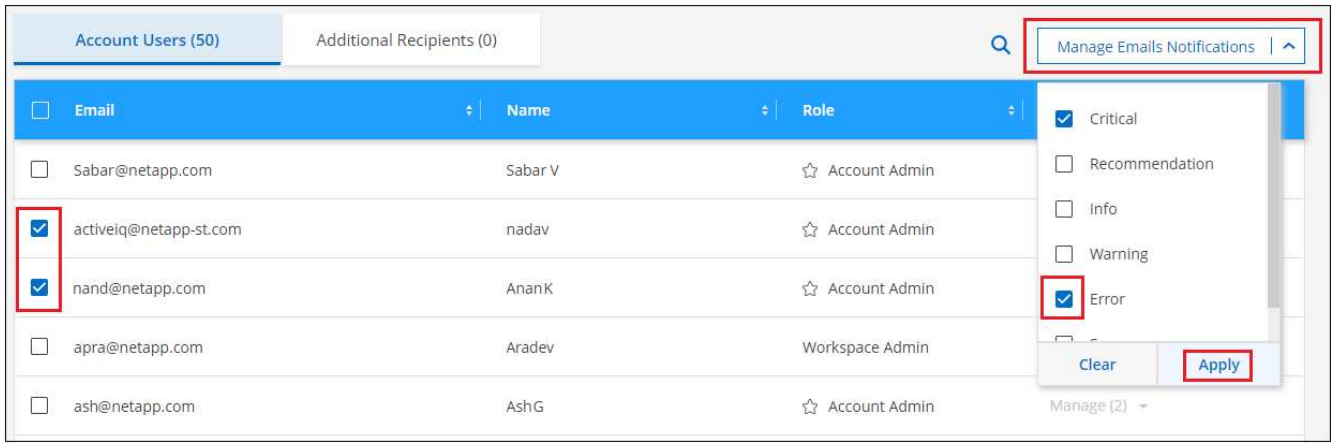
手順

1. BlueXPのメニューバーで、*[設定]>[アラートと通知の設定]*を選択します。



2. _Account Users_タブまたは_Additional Recipients_tabのいずれかからユーザーまたは複数のユーザーを選択し、送信する通知のタイプを選択します。

   - 1人のユーザーに対して変更を行うには、そのユーザーの[通知]列のメニューを選択し、送信する通知の種類を確認して、*[適用]*を選択します。
   - 複数のユーザーに変更を加えるには、各ユーザーのチェックボックスをオンにし、*メール通知の管理*を選択し、送信する通知の種類をチェックして*適用*を選択します。



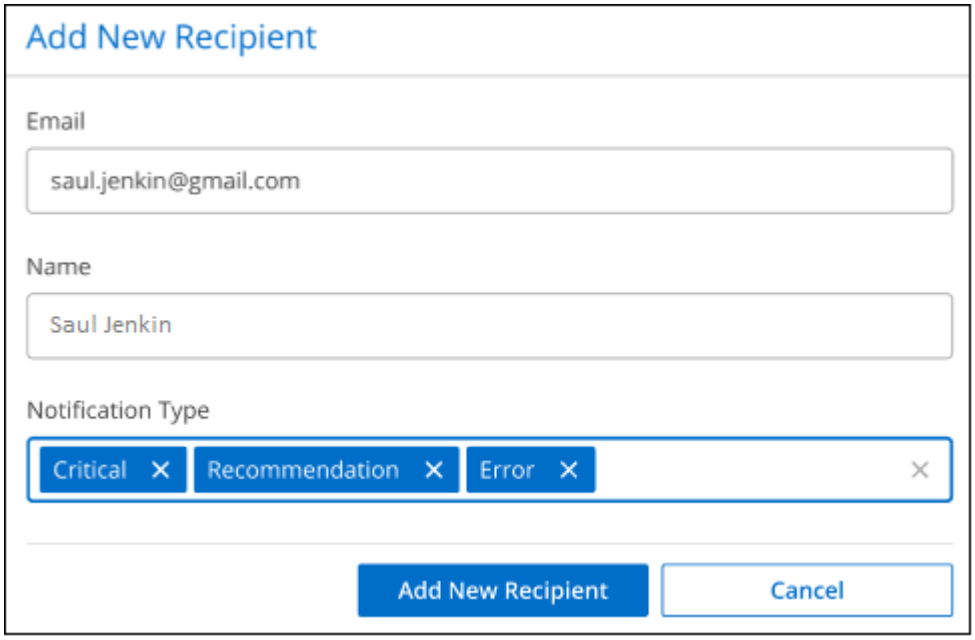
Eメール受信者を追加します

[_Account Users]タブに表示されるユーザは、（から）BlueXPアカウントのユーザから自動的に入力されます"［アカウントの管理］ページ"）。BlueXPにアクセスできないが、特定の種類のアラートや通知について通知する必要がある他のユーザーまたはグループの場合は、_追加の受信者_タブに電子メールアドレスを追加で

きます。

手順

1. [アラートと通知の設定]ページで、*[新しい受信者の追加]*を選択します。



2. 名前とEメールアドレスを入力し、受信者が受信する通知の種類を選択して、*[新しい受信者の追加]*を選択します。

アカウントのユーザーアクティビティを監査します

BlueXPのタイムラインには、ユーザーがアカウントを管理するために完了したアクションが表示されます。これには、ユーザの関連付け、ワークスペースの作成、コネクタの作成などの管理操作が含まれます。

タイムラインのチェックは、特定のアクションを実行したユーザーを特定する必要がある場合や、アクションのステータスを特定する必要がある場合に役立ちます。

手順

1. BlueXPのメニューバーで、*[設定]>[タイムライン]*を選択します。
2. [Filters]で、**[Service]***を選択し、[Tenancy]を有効にして、[Apply]*を選択します。

結果

タイムラインが更新され、アカウント管理アクションが表示されます。

BlueXPアカウントをもう1つ作成します

BlueXPにサインアップすると、組織のアカウントを作成するように求められます。このアカウントだけが必要な場合もありますが、ビジネスで複数のアカウントが必要な場合は、Tenancy APIを使用して追加のアカウントを作成する必要があります。

次のAPI呼び出しを使用して、追加のBlueXPアカウントを作成します。

投稿（Post） `/tenancy/account/{accountName}`

制限モードを有効にする場合は、要求の本文に次の項目を含める必要があります。

```
{
  "isSaasDisabled": true
}
```

> 制限モードの設定は、BlueXPがアカウントを作成したあとに変更することはできません。制限モードは後で有効にすることも、後で無効にすることもできません。アカウント作成時に設定する必要があります。

"このAPI呼び出しの使用方法について説明します"

関連リンク

- "BlueXPアカウントの詳細をご確認ください"
- "BlueXPの導入モードについて説明します"

ユーザロール

アカウント管理者、ワークスペース管理者、コンプライアンスビューア、および SnapCenter 管理者の各ロールは、ユーザーに特定の権限を提供します。BlueXPアカウントに新しいユーザを関連付けるときに、これらのロールのいずれかを割り当てることができます。

Compliance Viewerロールは、BlueXPの分類への読み取り専用アクセス用です。

タスク	アカウント管理者	ワークスペース管理者	**Compliance Viewer**（コンプライアンスビューア）	**SnapCenter** 管理者
作業環境の管理	はい。	はい。	いいえ	いいえ
作業環境でサービスを有効にします	はい。	はい。	いいえ	いいえ
ワークスペースからの作業環境の削除	はい。	はい。	いいえ	いいえ
作業環境を削除します	はい。	はい。	いいえ	いいえ
データ複製ステータスを表示します	はい。	はい。	いいえ	いいえ
タイムラインを表示します	はい。	はい。	いいえ	いいえ
ワークスペースを切り替えます	はい。	はい。	はい。	いいえ

タスク	アカウント管理者	ワークスペース管理者	**Compliance Viewer**（コンプライアンスビューア）	**SnapCenter** 管理者
BlueXPの分類スキャン結果を表示します	はい。	はい。	はい。	いいえ
Cloud Volumes ONTAP レポートを受信します	はい。	いいえ	いいえ	いいえ
コネクタを作成します	はい。	いいえ	いいえ	いいえ
BlueXPアカウントの管理	はい。	いいえ	いいえ	いいえ
クレデンシャルを管理する	はい。	いいえ	いいえ	いいえ
BlueXPの設定を変更します	はい。	いいえ	いいえ	いいえ
サポートダッシュボードを表示および管理します	はい。	いいえ	いいえ	いいえ
HTTPS 証明書をインストールします	はい。	いいえ	いいえ	いいえ

関連リンク

- "BlueXPアカウントでのワークスペースとユーザのセットアップ"
- "BlueXPアカウントでのワークスペースとユーザの管理"

コネクタ

コネクタのシステム **ID** を確認します

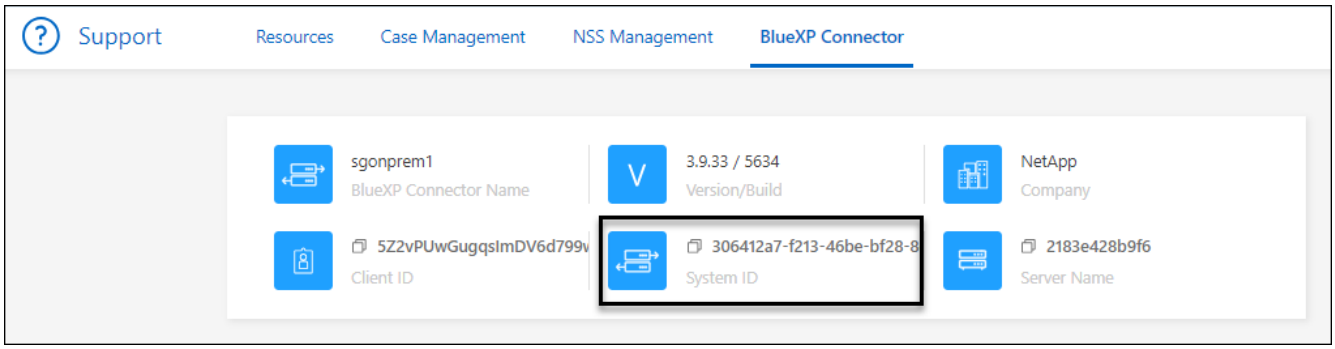
使用を開始するにあたり、ネットアップの担当者からコネクタのシステムIDを尋ねられることがあります。この ID は通常、ライセンスの取得やトラブルシューティングの目的で使用されます。

手順

1. BlueXPコンソールの右上にある[Help]アイコンを選択します。
2. [サポート]>[BlueXP Connector]*を選択します。

   システムIDがページの上部に表示されます。

   - 例 *



既存のコネクタを管理します

コネクタの作成後は、コネクタの管理が必要になる場合があります。たとえば、複数のコネクタがある場合は、コネクタを切り替えることができます。または、BlueXPをプライベートモードで使用している場合は、コネクタの手動アップグレードが必要になることがあります。

"コネクタの仕組みを説明します"。

> コネクタには、コネクタホストからアクセスできるローカルUIが含まれています。このUIは、BlueXPを制限モードまたはプライベートモードで使用しているお客様向けに提供されます。標準モードでBlueXPを使用する場合は、からユーザインターフェイスにアクセスする必要があります。 "BlueXP SaaSコンソール"
>
> "BlueXPの導入モードについて説明します"。

オペレーティングシステムと**VM**のメンテナンス

コネクタホストでのオペレーティングシステムの保守はお客様の責任で行ってください。たとえば、オペレーティングシステムの配布に関する会社の標準手順に従って、コネクタホストのオペレーティングシステムにセキュリティ更新プログラムを適用する必要があります。

OSの更新を実行するときは、コネクタホスト上のサービスを停止する必要はありません。

コネクタVMを停止してから起動する必要がある場合は、クラウドプロバイダのコンソールから、またはオンプレミス管理の標準手順を使用して起動する必要があります。

"コネクタは常に動作している必要があることに注意してください"。

VMまたはインスタンスタイプ

コネクタをBlueXPから直接作成した場合は、デフォルトの設定を使用してクラウドプロバイダに仮想マシンインスタンスを導入しました。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。

CPUとRAMの要件は次のとおりです。

CPU

4 コアまたは 4 個の vCPU

RAM

14GB

"コネクタのデフォルト設定について説明します"。

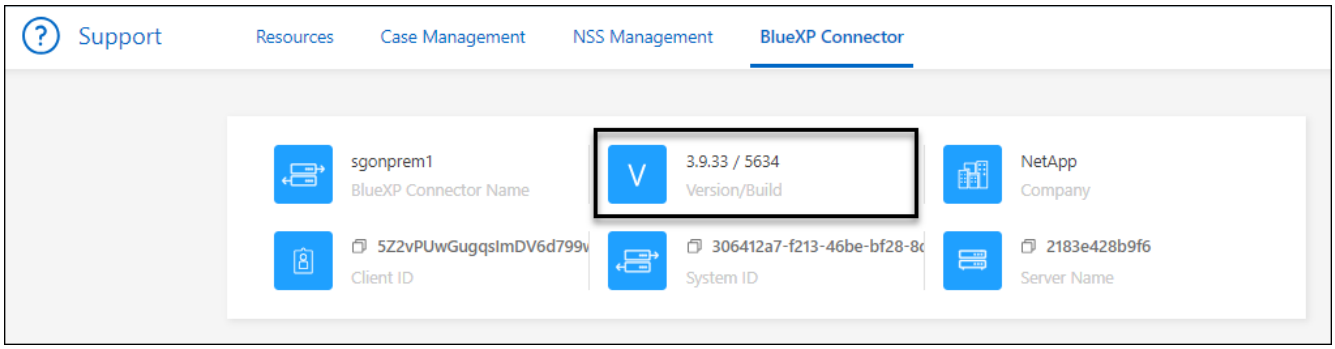
コネクタのバージョンの表示

コネクタのバージョンを表示して、コネクタが自動的に最新リリースにアップグレードされたこと、またはNetApp担当者と共有する必要があることを確認できます。

手順

1. BlueXPコンソールの右上にある[Help]アイコンを選択します。
2. [サポート]>[BlueXP Connector]*を選択します。

   ページの上部にバージョンが表示されます。



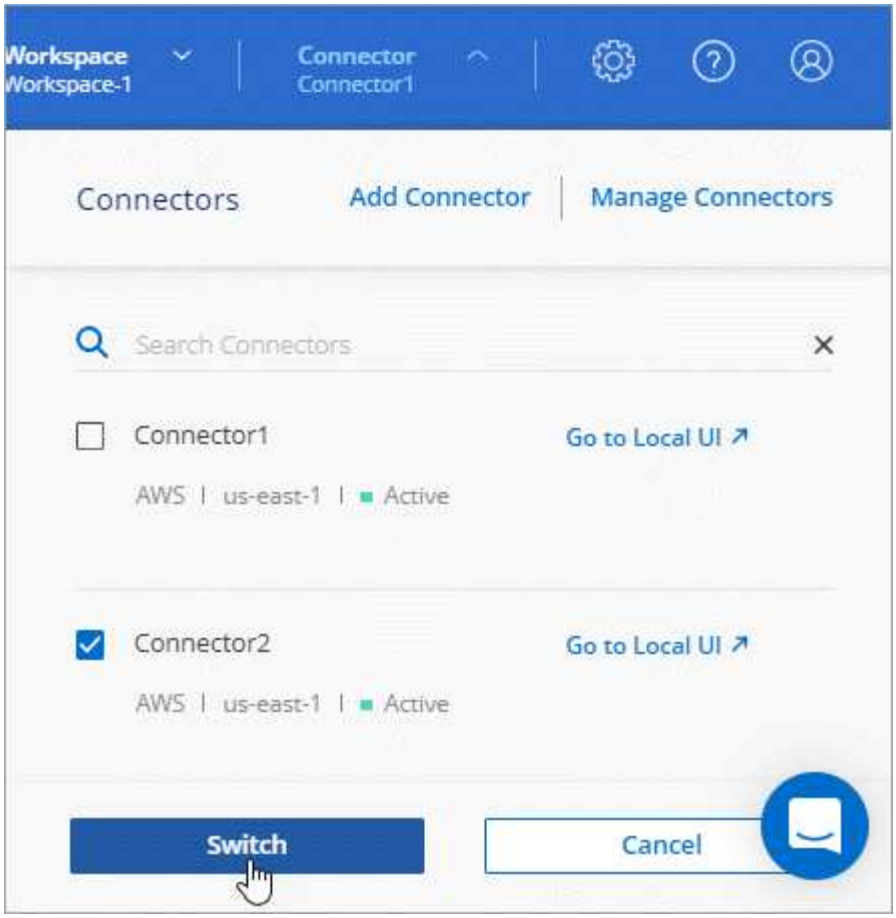
コネクタを切り替えます

複数のコネクタがある場合は、コネクタを切り替えることで特定のコネクタに関連付けられている作業環境を確認できます。

たとえば、マルチクラウド環境で作業しているとします。AWS にコネクタが 1 つ、 Google Cloud にコネクタが 1 つあるとします。これらのクラウドで実行されている Cloud Volumes ONTAP システムを管理するには、これらのコネクタを切り替える必要があります。

ステップ

1. ドロップダウンを選択し、別のコネクタを選択して、[Switch]*を選択します。



結果

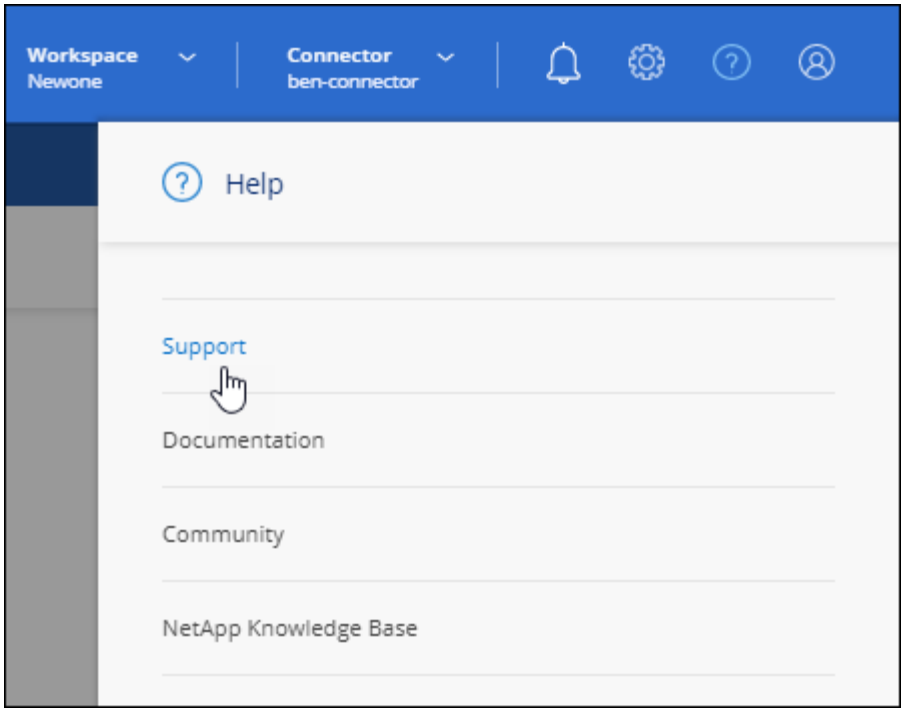
BlueXPが更新され'選択したコネクタに関連付けられている作業環境が表示されます

AutoSupport メッセージをダウンロードまたは送信します

問題が発生した場合、ネットアップの担当者から、トラブルシューティングの目的で AutoSupport メッセージをネットアップサポートに送信するように依頼されることがあります。

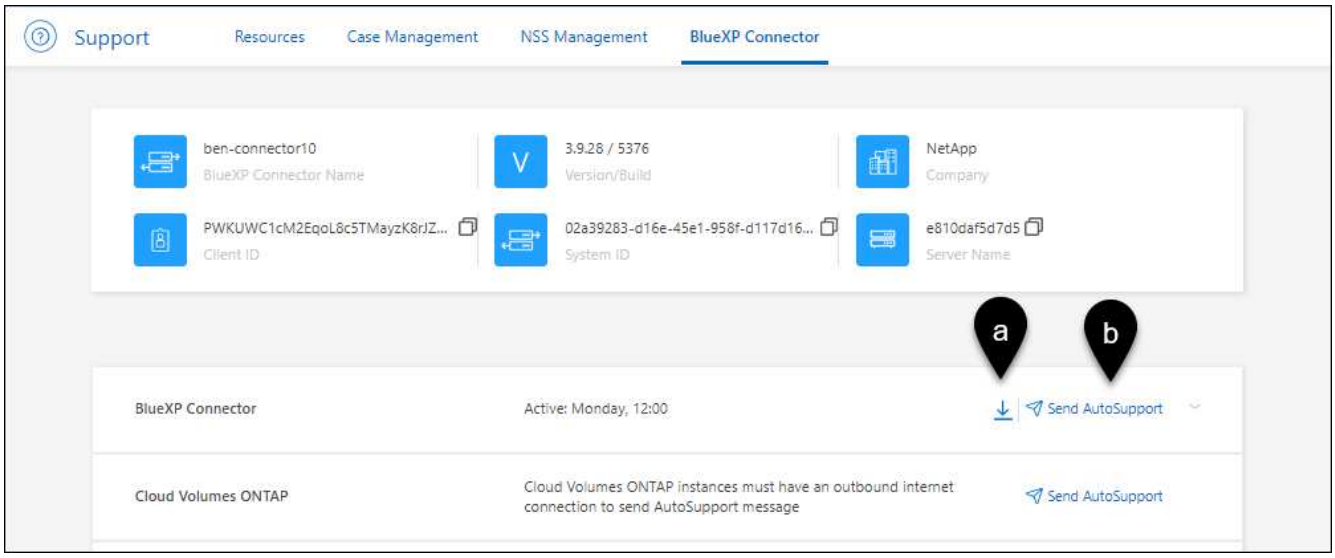
手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

2. [BlueXP Connector]*を選択します。
3. ネットアップサポートへの情報の送信方法に応じて、次のいずれかを実行します。
   a. AutoSupport メッセージをローカルマシンにダウンロードするオプションを選択します。登録したら、任意の方法でネットアップサポートに送信できます。
   b. ネットアップサポートにメッセージを直接送信するには、* Send AutoSupport *を選択します。



Linux VM に接続します

コネクタが実行されている Linux VM に接続する必要がある場合は、クラウドプロバイダから提供されている接続オプションを使用できます。

AWS

AWS でコネクタインスタンスを作成する際に、 AWS のアクセスキーとシークレットキーを指定しました。このキーペアを使用して、 SSH でインスタンスに接続できます。EC2 Linuxインスタンスのユーザ名はUbuntuです（2023年5月より前に作成されたコネクタの場合、ユーザ名はEC2-user）。

"AWS Docs ： Linux インスタンスに接続します"

Azure

AzureでコネクタVMを作成するときに、ユーザ名を指定し、パスワードまたはSSH公開鍵で認証することを選択しました。選択した認証方式を使用して VM に接続します。

"Azure Docs ： SSH を使用して VM を接続します"

Google Cloud

Google Cloud でコネクタを作成するときに認証方法を指定することはできません。ただし、 Google Cloud Console または Google Cloud CLI （ gcloud ）を使用して Linux VM インスタンスに接続することができます。

"Google Cloud Docs ： Linux VM に接続します"

Amazon EC2インスタンスで**IMDSv2**を使用する必要がある

2024年3月より、BlueXPで、コネクタとCloud Volumes ONTAP（HA環境のメディエーターを含む）でAmazon EC2インスタンスメタデータサービスバージョン2（IMDSv2）がサポートされるようになりました。ほとんどの場合、IMDSv2は新しいEC2インスタンスで自動的に設定されます。IMDSv1は2024年3月より前に有効になっています。セキュリティポリシーで必要な場合は、EC2インスタンスでIMDSv2を手動で設定する必要があります。

このタスクについて

IMDSv2では、脆弱性に対する保護が強化されています。 "AWSセキュリティブログでIMDSv2の詳細を確認する"

インスタンスメタデータサービス（IMDS）は、EC2インスタンスで次のように有効になります。

- BlueXPから新規コネクタを導入する場合、または "Terraformスクリプト"IMDSv2はEC2インスタンスでデフォルトで有効になっています。
- AWSで新しいEC2インスタンスを起動し、コネクタソフトウェアを手動でインストールすると、IMDSv2もデフォルトで有効になります。
- AWS Marketplaceからコネクタを起動すると、IMDSv1がデフォルトで有効になります。EC2インスタンスにIMDSv2を手動で設定できます。
- 既存のコネクタについては、IMDSv1は引き続きサポートされますが、必要に応じて、EC2インスタンスでIMDSv2を手動で設定できます。
- Cloud Volumes ONTAPでは、新規および既存のインスタンスでIMDSv1がデフォルトで有効になっています。必要に応じて、EC2インスタンスでIMDSv2を手動で設定できます。

作業を開始する前に

- コネクタのバージョンは3.9.38以降である必要があります。
- Cloud Volumes ONTAPで次のいずれかのバージョンが実行されている必要があります。

- 9.12.1 P2（またはそれ以降のパッチ）
- 9.13.0 P4（またはそれ以降のパッチ）
- 9.13.1以降のすべてのバージョン

- この変更を行うには、Cloud Volumes ONTAPインスタンスを再起動する必要があります。

このタスクについて

応答ホップの制限を3に変更する必要があるため、この手順ではAWS CLIを使用する必要があります。

手順

1. コネクタインスタンスでIMDSv2を使用する必要があります。

   a. コネクタのLinux VMに接続します。

      AWS でコネクタインスタンスを作成する際に、 AWS のアクセスキーとシークレットキーを指定しました。このキーペアを使用して、 SSH でインスタンスに接続できます。EC2 Linuxインスタンスのユーザ名はUbuntuです（2023年5月より前に作成されたコネクタの場合、ユーザ名はEC2-user）。

      "AWS Docs ： Linux インスタンスに接続します"

   b. AWS CLIをインストールします。

      "AWSドキュメント：最新バージョンのAWS CLIをインストールまたは更新する"

   c. を使用します `aws ec2 modify-instance-metadata-options` IMDSv2の使用を要求し、PUT応答ホップ制限を3に変更するコマンド。

      - 例 *

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

> 。 `http-tokens` パラメータはIMDSv2を必須に設定します。いつ `http-tokens` は必須です。次の項目も設定する必要があります。 `http-endpoint` を有効にします。

2. Cloud Volumes ONTAPインスタンスでIMDSv2を使用する必要があります。

   a. にアクセスします "Amazon EC2コンソール"

   b. ナビゲーションペインで、*[インスタンス]*を選択します。

   c. Cloud Volumes ONTAPインスタンスを選択します。

   d. [Actions]>[Instance settings]>[Modify instance metadata options]*を選択します。

   e. インスタンスメタデータオプションの変更*（Modify instance metadata options *）ダイアログボックスで、次のオプションを選択します。

      - で、[有効化]*を選択します。

- IMDSv2 *で、*必須*を選択します。
- [保存（ Save ）] を選択します。

f. HAメディエーターを含む他のCloud Volumes ONTAPインスタンスについて、上記の手順を繰り返します。

g. "Cloud Volumes ONTAPインスタンスの停止と開始"

結果

コネクタインスタンスとCloud Volumes ONTAPインスタンスがIMDSv2を使用するように構成されました。

プライベートモードを使用する場合は、コネクタをアップグレードします

BlueXPをプライベートモードで使用している場合は、NetApp Support Site から新しいバージョンが利用可能になったらコネクタをアップグレードできます。

アップグレード中にWebベースのコンソールを使用できなくなるように、アップグレードプロセス中にコネクタを再起動する必要があります。

> 標準モードまたは制限モードでBlueXPを使用すると、ソフトウェアの更新を取得するためにアウトバウンドのインターネットアクセスが確立されていれば、コネクタは自動的にソフトウェアを最新バージョンに更新します。

手順

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

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

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

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

   <version> は、ダウンロードしたコネクタのバージョンです。

4. インストールスクリプトを実行します。

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

   <version> は、ダウンロードしたコネクタのバージョンです。

5. アップグレードが完了したら、 * Help > Support > Connector * を選択してコネクタのバージョンを確認できます。

コネクタの **IP** アドレスを変更します

ビジネスに必要な場合は、クラウドプロバイダによって自動的に割り当てられたコネクタインスタンスの内部

IP アドレスとパブリック IP アドレスを変更できます。

手順

1. クラウドプロバイダからの指示に従って、 Connector インスタンスのローカル IP アドレスまたはパブリック IP アドレス（またはその両方）を変更します。
2. パブリックIPアドレスを変更した場合、コネクタで実行されているローカルユーザインターフェイスに接続する必要があるときは、コネクタインスタンスを再起動して、新しいIPアドレスをBlueXPに登録します。
3. プライベート IP アドレスを変更した場合は、 Cloud Volumes ONTAP 構成ファイルのバックアップ先を更新して、コネクタ上の新しいプライベート IP アドレスにバックアップが送信されるようにします。

   各Cloud Volumes ONTAPシステムのバックアップ場所を更新する必要があります。

   a. Cloud Volumes ONTAP CLIから次のコマンドを実行して、現在のバックアップターゲットを表示します。

   ```
   system configuration backup show
   ```

   b. 次のコマンドを実行して、バックアップターゲットのIPアドレスを更新します。

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

コネクターの**URI**を編集します

コネクタのUniform Resource Identifier（URI）を追加および削除します。

手順

1. BlueXPヘッダーの* Connector *ドロップダウンを選択します。
2. [コネクタの管理]*を選択します。
3. コネクタのアクションメニューを選択し、* URIの編集*を選択します。
4. URIを追加および削除し、*適用*を選択します。

Google Cloud NAT ゲートウェイを使用しているときのダウンロードエラーを修正します

コネクタは、 Cloud Volumes ONTAP のソフトウェアアップデートを自動的にダウンロードします。設定で Google Cloud NAT ゲートウェイを使用している場合、ダウンロードが失敗することがあります。この問題を修正するには、ソフトウェアイメージを分割するパーツの数を制限します。この手順は、BlueXP APIを使用して実行する必要があります。

ステップ

1. 次の JSON を本文として /occm/config に PUT 要求を送信します。

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions の値は 1 または 1 より大きい任意の整数です。値が 1 の場合、ダウンロードされたイメージは分割されません。

32 は値の例です。使用する値は、 NAT の設定と同時に使用できるセッションの数によって異なります。

"/occm/config API 呼び出しの詳細を確認してください"

BlueXPからコネクタを取り外します

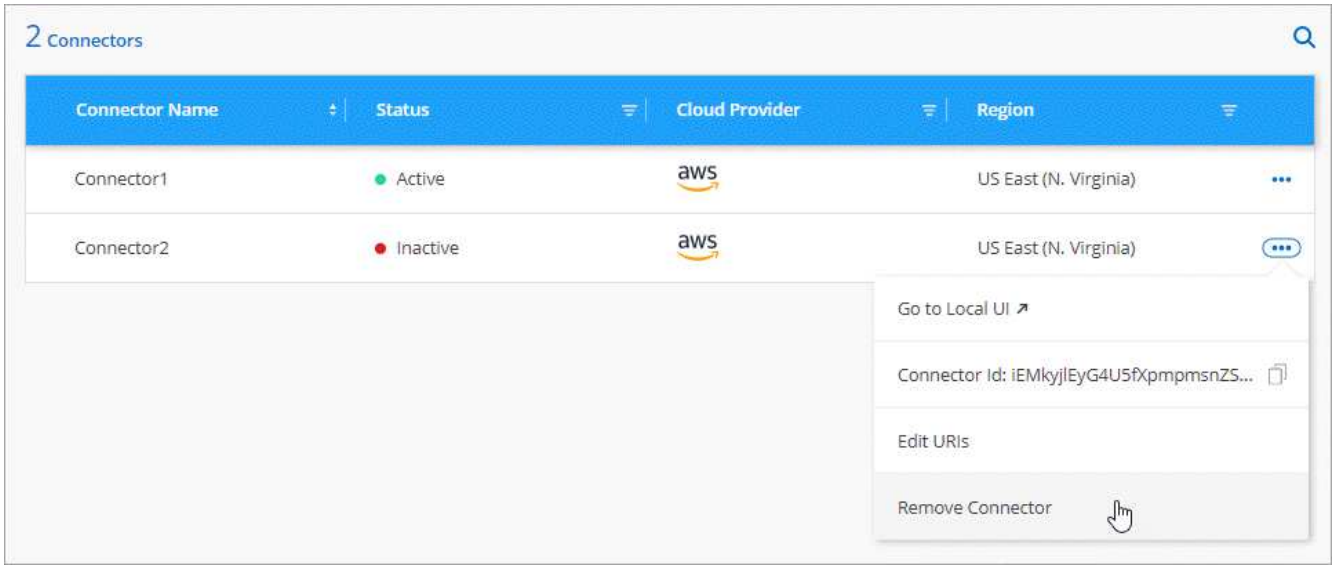
コネクタがアクティブでない場合は、BlueXPのコネクタのリストから削除できます。この処理は、Connector 仮想マシンを削除した場合や Connector ソフトウェアをアンインストールした場合に実行できます。

コネクタの取り外しについては、次の点に注意してください。

- この操作で仮想マシンが削除されることはありません。
- この操作を元に戻すことはできません。BlueXPからコネクタを削除すると、再度追加することはできません。

手順

1. BlueXPヘッダーの* Connector *ドロップダウンを選択します。
2. [コネクタの管理]*を選択します。
3. 非アクティブなコネクターのアクションメニューを選択し、*コネクターの除去*を選択します。



4. 確認するコネクタの名前を入力し、*[削除]*を選択します。

結果

BlueXPはコネクタをレコードから削除します。

Connector ソフトウェアをアンインストールします

問題のトラブルシューティングを行う場合や、ソフトウェアをホストから完全に削除する場合は、コネクタソフトウェアをアンインストールします。必要な手順は、コネクタをインターネットにアクセスできるホスト（標準モードまたは制限モード）にインストールしたか、インターネットにアクセスできないネットワーク内のホスト（プライベートモード）にインストールしたかによって異なります。

標準モードまたは制限モードを使用する場合のアンインストール

標準モードまたは制限モードでBlueXPを使用している場合は、以下の手順でコネクタソフトウェアをアンインストールできます。

手順

1. コネクタのLinux VMに接続します。
2. Linux ホストからアンインストールスクリプトを実行します。

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent_ 確認を求めずにスクリプトを実行します。

プライベートモード使用時のアンインストール

次の手順では、BlueXPをプライベートモードで使用している場合にインターネットアクセスを使用できないときにコネクタソフトウェアをアンインストールできます。

手順

1. コネクタのLinux VMに接続します。
2. Linux ホストから、次のコマンドを実行します。

   ```
   ./opt/application/netapp/ds/cleanup.sh
   rm -rf /opt/application/netapp/ds
   ```

セキュアなアクセスのための**HTTPS**証明書をインストールします

デフォルトでは、BlueXPはWebコンソールへのHTTPSアクセスに自己署名証明書を使用します。ビジネスで必要な場合は、認証局（CA）によって署名された証明書をインストールできます。これにより、自己署名証明書よりもセキュリティ保護が強化されます。

作業を開始する前に

BlueXP設定を変更する前にコネクタを作成する必要があります。 "詳細をご確認ください"。

HTTPS 証明書をインストールします

セキュアなアクセスのために、 CA によって署名された証明書をインストールします。

手順

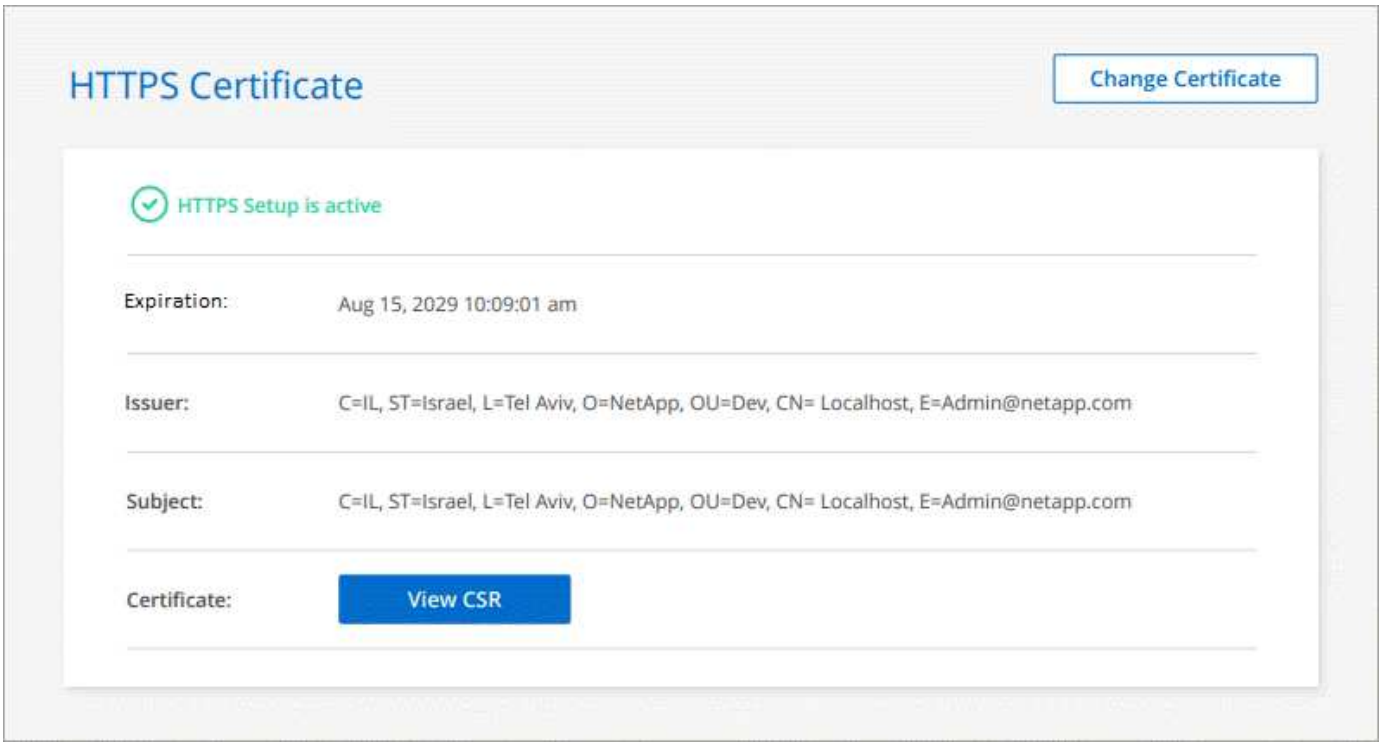
1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[HTTPSセットアップ]*を選択します。

2. [HTTPS Setup] ページで、証明書署名要求（ CSR ）を生成するか、独自の CA 署名付き証明書をインストールして、証明書をインストールします。

オプション	説明
CSR を生成します	a. コネクタホストのホスト名またはDNS（共通名）を入力し、*[CSRの生成]*を選択します。 証明書署名要求が表示されます。 b. CSR を使用して、 SSL 証明書要求を CA に送信します。 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。 c. 証明書ファイルをアップロードし、*[インストール]*を選択します。
独自の CA 署名付き証明書をインストールします	a. 「 CA 署名証明書のインストール」を選択します。 b. 証明書ファイルと秘密鍵の両方をロードし、*[インストール]*を選択します。 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。

結果

BlueXPでは、CA署名証明書を使用してセキュアなHTTPSアクセスが提供されるようになりました。次の図は、セキュアなアクセスが設定されたBlueXPアカウントを示しています。



BlueXP HTTPS証明書を更新します

BlueXPコンソールへの安全なアクセスを確保するために、有効期限が切れる前にBlueXP HTTPS証明書を更新する必要があります。有効期限が切れる前に証明書を更新しないと、ユーザがHTTPSを使用してWebコンソールにアクセスしたときに警告が表示されます。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[HTTPSセットアップ]*を選択します。

   BlueXP証明書の詳細が、有効期限を含めて表示されます。

2. [証明書の変更]*を選択し、手順に従ってCSRを生成するか、独自のCA署名証明書をインストールします。

結果

BlueXPは、新しいCA署名証明書を使用してセキュアなHTTPSアクセスを提供します。

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

社内ポリシーで、インターネットへのすべての通信にプロキシサーバを使用する必要がある場合は、そのプロキシサーバを使用するようにコネクタを設定する必要があります。インストール時にプロキシサーバを使用するようにコネクタを設定していない場合は、いつでもそのプロキシサーバを使用するようにコネクタを設定できます。

プロキシサーバを使用するようにコネクタを設定すると、パブリックIPアドレスまたはNATゲートウェイを使用できない場合に、アウトバウンドインターネットアクセスが提供されます。このプロキシサーバは、アウトバウンド接続を持つコネクタのみを提供します。Cloud Volumes ONTAP システムへの接続は提供しません。

Cloud Volumes ONTAP システムに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

接続がない場合、コネクタに含まれているプロキシサーバを使用するようにCloud Volumes ONTAP システムが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。

サポートされている構成

- BlueXPはHTTPとHTTPSをサポートしています
- プロキシサーバは、クラウドまたはネットワークに配置できます。
- BlueXPでは、透過型プロキシサーバはサポートされていません。

コネクタでプロキシを有効にします

プロキシサーバ、そのコネクタ、および管理対象の Cloud Volumes ONTAP システム（ HA メディエーターを含む）を使用するようにコネクタを設定すると、すべてのでプロキシサーバが使用されます。

この操作により、コネクタが再起動されます。続行する前に、コネクタが操作を実行していないことを確認してください。

手順

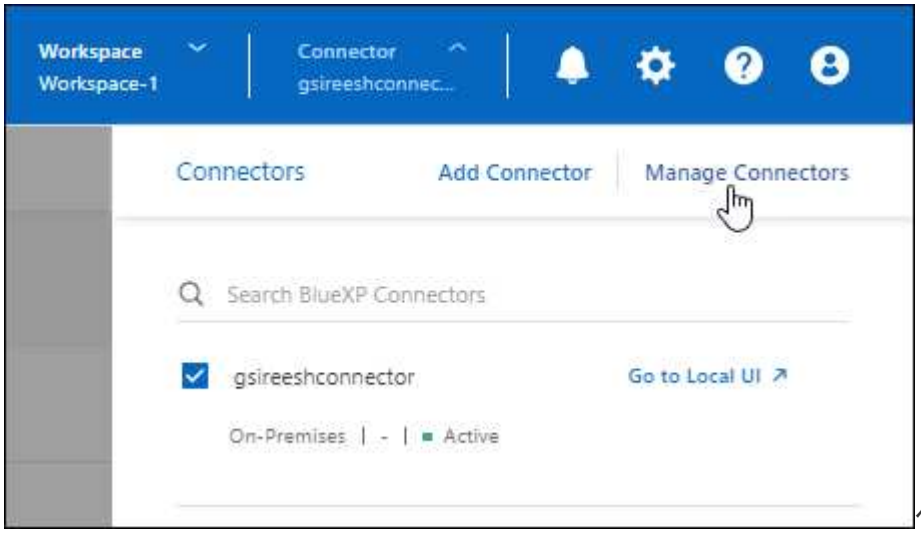
1. [BlueXPコネクタの編集]*ページに移動します。

   操作方法は、BlueXPを標準モード（SaaS WebサイトからBlueXPインターフェイスにアクセス）で使用しているか、制限モードとプライベートモード（コネクタホストからローカルにBlueXPインターフェイスにアクセス）で使用しているかによって異なります。

標準モード

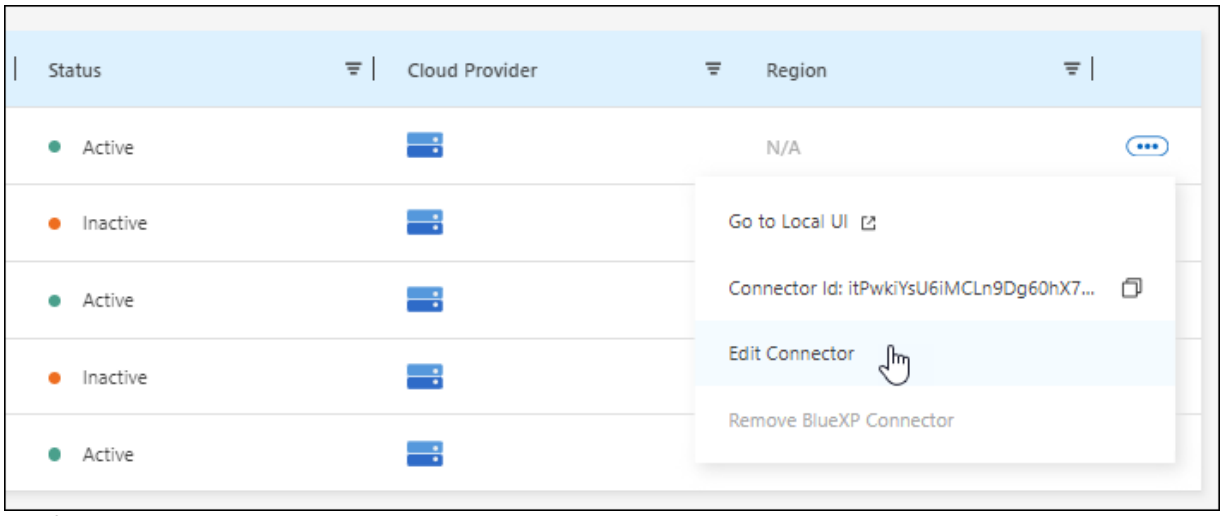
a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

b. [コネクタの管理]*を選択します。



ページのスクリーンショット。"]

c. コネクターのアクションメニューを選択し、*コネクターを編集*を選択します。

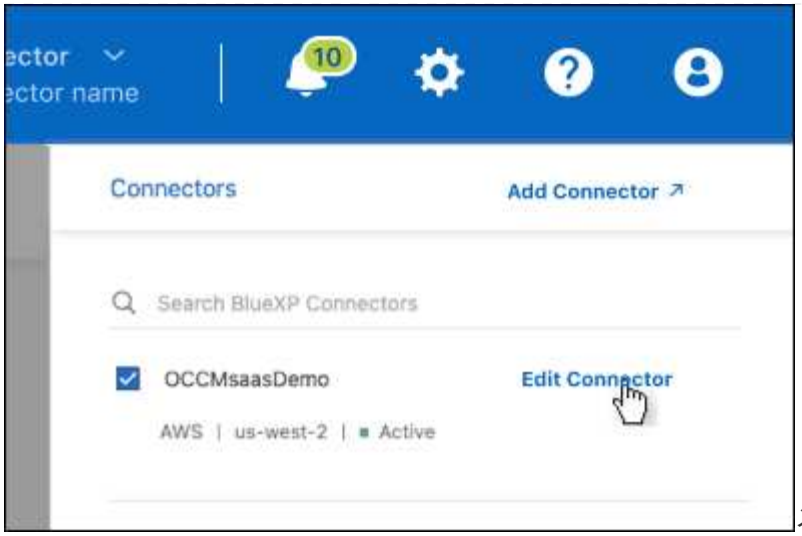


オプションを示すスクリーンショット。"]

制限モードまたはプライベートモード

a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

b. [Edit Connector]*を選択します。



メニューを展開すると使用できる[Edit Connector]オプションを示すスクリーンショット。"]

2. [HTTP Proxy Configuration]*を選択します。
3. プロキシを設定します。
   a. [Enable Proxy]*を選択します。
   b. 構文を使用してサーバを指定します http://address:port または https://address:port
   c. サーバでベーシック認証が必要な場合は、ユーザ名とパスワードを指定します。

      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、\のASCIIコードを次のように入力する必要があります。domain-name%92user-name

        例：NetApp%92proxy

      - 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。
   d. [保存（ Save ）] を選択します。

API の直接トラフィックを有効にします

プロキシサーバを使用するようにコネクタを設定した場合は、コネクタで直接APIトラフィックを有効にして、プロキシを経由せずにAPI呼び出しをクラウドプロバイダサービスに直接送信できます。このオプションは、 AWS 、 Azure 、または Google Cloud で実行されているコネクタでサポートされます。

Cloud Volumes ONTAP でAzureプライベートリンクの使用を無効にし、代わりにサービスエンドポイントを使用している場合は、ダイレクトAPIトラフィックを有効にする必要があります。そうしないと、トラフィックは適切にルーティングされません。

"Azure Private LinkまたはサービスエンドポイントをCloud Volumes ONTAP で使用する方法の詳細については、こちらをご覧ください"

手順

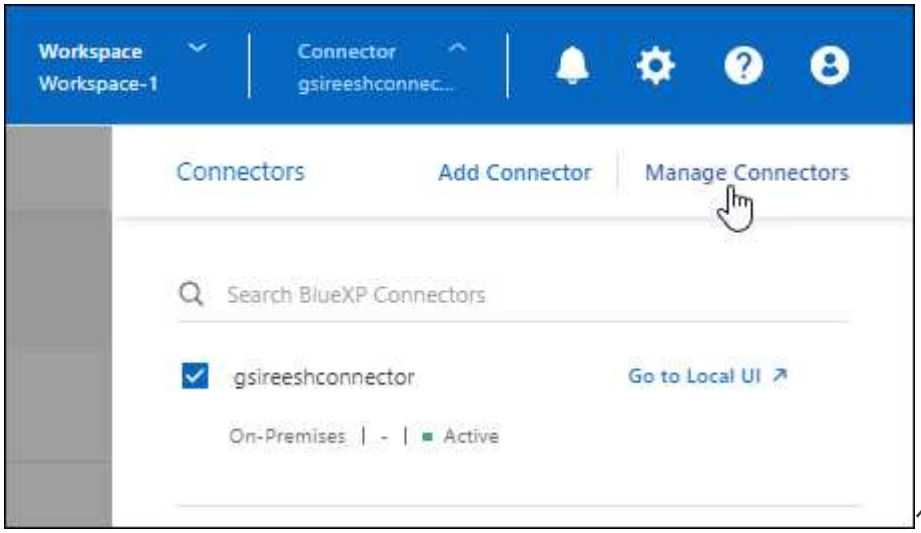
1. [BlueXPコネクタの編集]*ページに移動します。

   操作方法は、BlueXPを標準モード（SaaS WebサイトからBlueXPインターフェイスにアクセス）で使用しているか、制限モードとプライベートモード（コネクタホストからローカルにBlueXPインターフェイスにアクセス）で使用しているかによって異なります。

標準モード

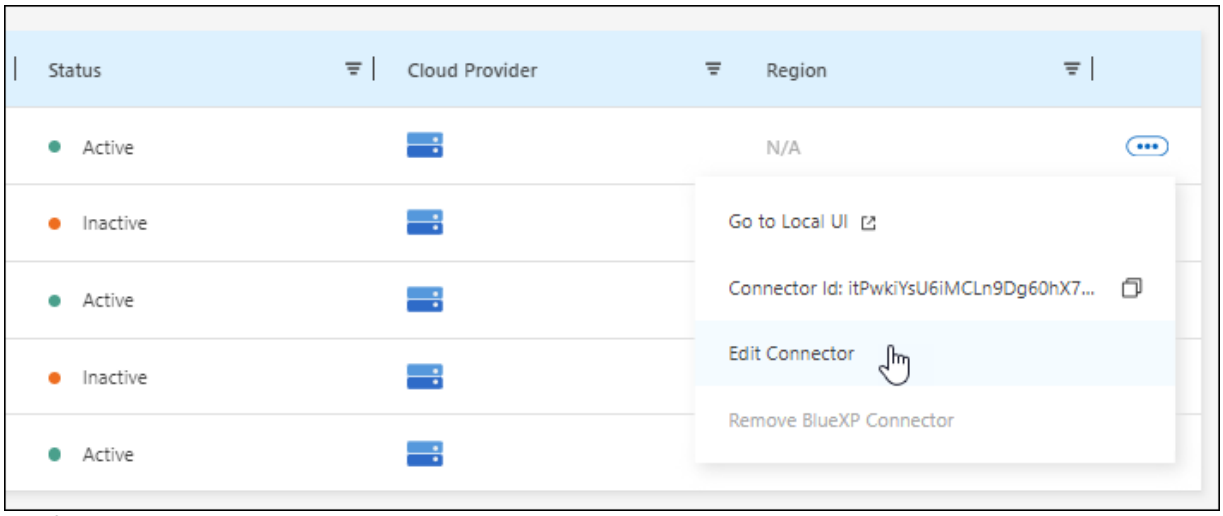
a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

b. [コネクタの管理]*を選択します。



ページのスクリーンショット。"]

c. コネクターのアクションメニューを選択し、*コネクターを編集*を選択します。

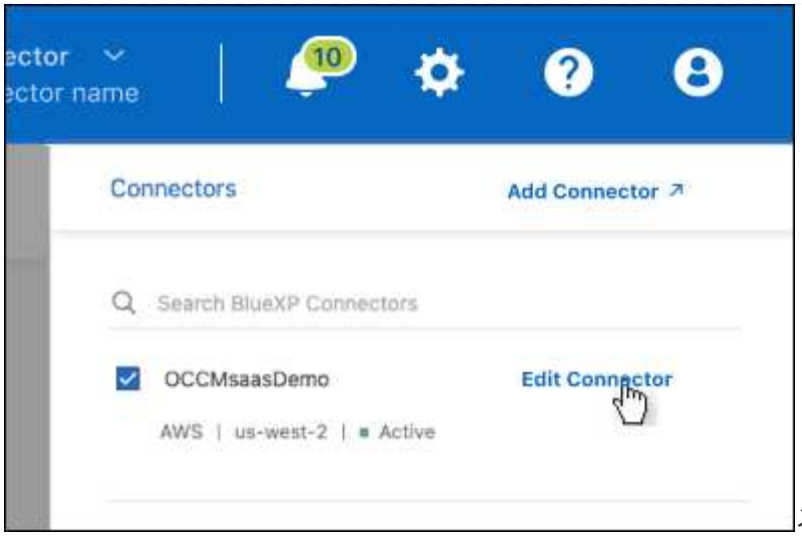


オプションを示すスクリーンショット。"]

制限モードまたはプライベートモード

a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

b. [Edit Connector]*を選択します。



メニューを展開すると使用できる[Edit Connector]オプションを示すスクリーンショット。"]

2. [サポート][Direct API Traffic]*を選択します。
3. チェックボックスをオンにしてオプションを有効にし、*[保存]*を選択します。

コネクタのデフォルト設定

コネクタを導入する前に、または問題のトラブルシューティングが必要な場合は、コネクタの設定に関する詳細を確認しておくことを推奨します。

インターネットアクセスを使用するデフォルト設定

次の構成の詳細は、BlueXPからコネクタを導入した場合、クラウドプロバイダのマーケットプレイスからコネクタを導入した場合、またはインターネットにアクセスできるオンプレミスのLinuxホストにコネクタを手動でインストールした場合に適用されます。

AWSの詳細

BlueXPまたはクラウドプロバイダのマーケットプレイスからコネクタを導入した場合は、次の点に注意してください。

- EC2インスタンスタイプはt3.xlargeです。
- イメージのオペレーティングシステムはUbuntu 22.04 LTSです。

  オペレーティングシステムには GUI は含まれていません。システムにアクセスするには、端末を使用する必要があります。

- EC2 Linuxインスタンスのユーザ名はUbuntuです（2023年5月より前に作成されたコネクタの場合、ユーザ名はEC2-user）。
- デフォルトのシステムディスクは100GiBのgp2ディスクです。

Azureの詳細

BlueXPまたはクラウドプロバイダのマーケットプレイスからコネクタを導入した場合は、次の点に注意して

ください。

- VMタイプはDS3 v2です。
- イメージのオペレーティングシステムはUbuntu 22.04 LTSです。

  オペレーティングシステムには GUI は含まれていません。システムにアクセスするには、端末を使用する必要があります。

- デフォルトのシステムディスクは100GiBのPremium SSDディスクです。

Google Cloudの詳細

BlueXPからコネクタを導入した場合は、次の点に注意してください。

- VMインスタンスがn2 -標準-4である。
- イメージのオペレーティングシステムはUbuntu 22.04 LTSです。

  オペレーティングシステムには GUI は含まれていません。システムにアクセスするには、端末を使用する必要があります。

- デフォルトのシステムディスクは100GiBのSSD永続ディスクです。

インストールフォルダ

Connector インストールフォルダは、次の場所にあります。

/opt/application/netapp/cloudmanager です

ログファイル

ログファイルは次のフォルダに格納されます。

- /opt/application/netapp/cloudmanager/log を選択します
  または
- /opt/application/netapp/service-manager-2 /ログ（新規インストール3.9.23以降）

  これらのフォルダのログには、ConnectorイメージとDockerイメージの詳細が記載されています。

- /opt/application/NetApp/cloudmanager/docx_occm/data/log

  このフォルダのログには、コネクタで実行されている クラウド サービス およびBlueXPサービスの詳細が表示されます。

コネクタサービス

- BlueXPサービスの名前はoccmです
- OCCM サービスは MySQL サービスに依存します。

  MySQL サービスがダウンしている場合は、 OCCM サービスもダウンしています。

ポート

このコネクタは Linux ホストで次のポートを使用します。

- HTTP アクセスの場合は 80
- 443 ： HTTPS アクセス用

インターネットアクセスを使用しないデフォルトの設定

インターネットにアクセスできないオンプレミスの Linux ホストにコネクタを手動でインストールした場合、次の構成が適用されます。 "このインストールオプションの詳細については、こちらをご覧ください"。

- Connector インストールフォルダは、次の場所にあります。

  /opt/application/NetApp/DS

- ログファイルは次のフォルダに格納されます。

  /var/lib/docker /volumes /DS_occmdata/_data/log

  このフォルダのログには、 Connector イメージと Docker イメージの詳細が記録されます。

- すべてのサービスが Docker コンテナ内で実行されています

  サービスは、実行されている Docker ランタイムサービスに依存します

- このコネクタは Linux ホストで次のポートを使用します。
  - HTTP アクセスの場合は 80
  - 443 ： HTTPS アクセス用

クレデンシャルとサブスクリプション

AWS

AWS のクレデンシャルと権限について説明します

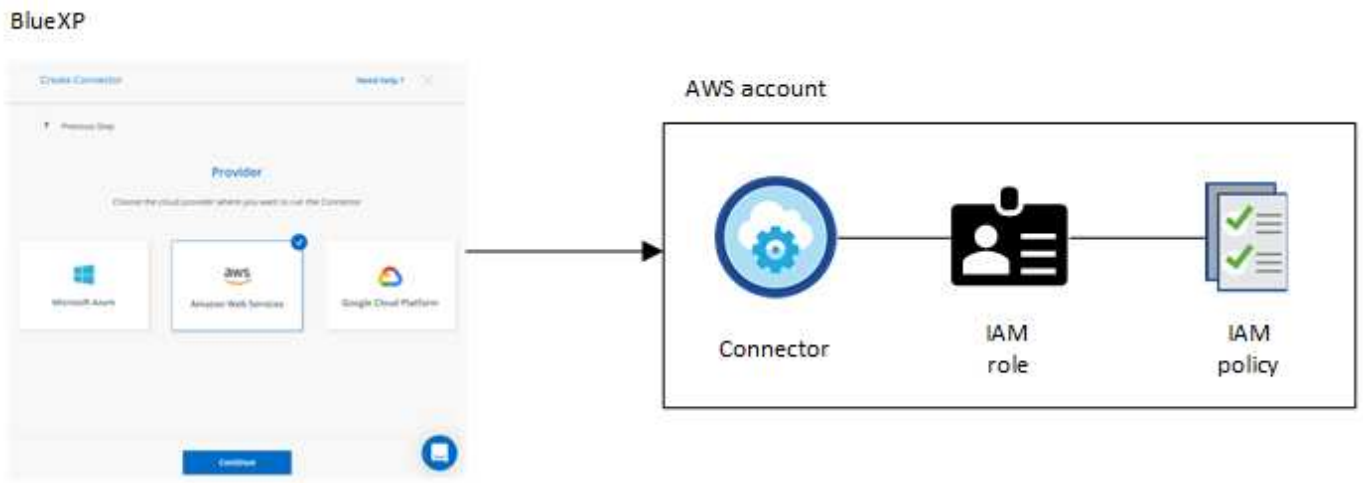
BlueXPがAWSクレデンシャルを使用してユーザに代わって操作を実行する方法と、それらのクレデンシャルがマーケットプレイスのサブスクリプションにどのように関連付けられているかをご確認くださいこれらの詳細を理解しておくと、BlueXPで1つ以上のAWSアカウントのクレデンシャルを管理する際に役立ちます。たとえば、AWSクレデンシャルをBlueXPに追加するタイミングを把握できます。

AWS の初期クレデンシャル

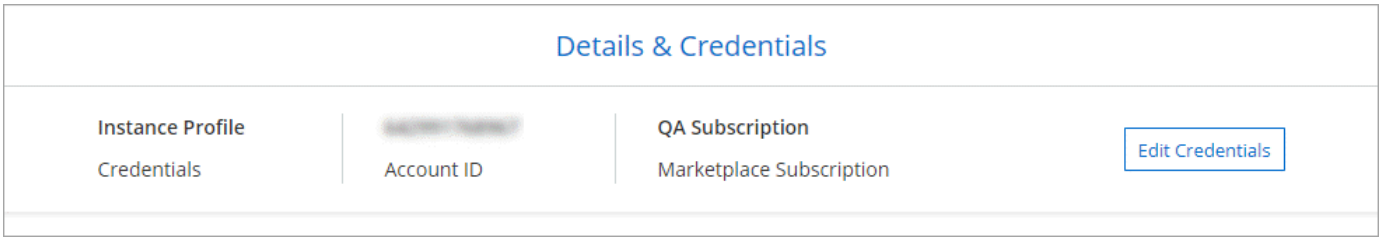
BlueXPからコネクタを展開する場合は、IAMロールのARNまたはIAMユーザのアクセスキーを指定する必要があります。使用する認証方式に、 Connector インスタンスを AWS に導入するための必要な権限がある必要があります。必要な権限は、に表示されます "AWS 用のコネクタ導入ポリシー"。

BlueXPがAWSでコネクタインスタンスを起動すると、インスタンスのIAMロールとインスタンスプロファイ

ルが作成されます。また、ポリシーを適用して、指定した AWS アカウント内のリソースやプロセスを管理する権限を Connector に提供します。 "BlueXPがどのように権限を使用しているかを確認します"。



Cloud Volumes ONTAPの新しい作業環境を作成すると、BlueXPでは次のAWSクレデンシャルがデフォルトで選択されます。



ページの[Switch Account]オプションを示すスクリーンショット。"]

すべての Cloud Volumes ONTAP システムは、初期の AWS クレデンシャルを使用して導入することも、クレデンシャルを追加することもできます。

追加の **AWS** クレデンシャル

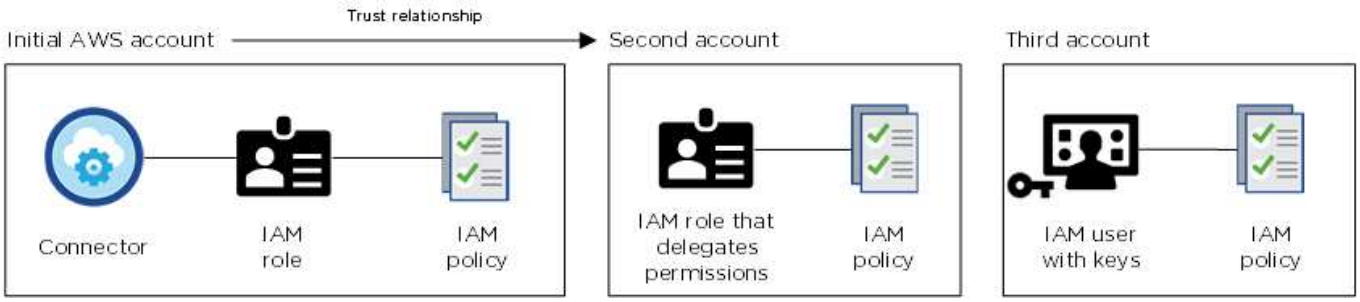
AWSクレデンシャルを追加するには、次の2つの方法があります。

- 既存のコネクタにAWSクレデンシャルを追加できます
- AWSクレデンシャルはBlueXPに直接追加できます

詳細については、以下のセクションを参照してください。

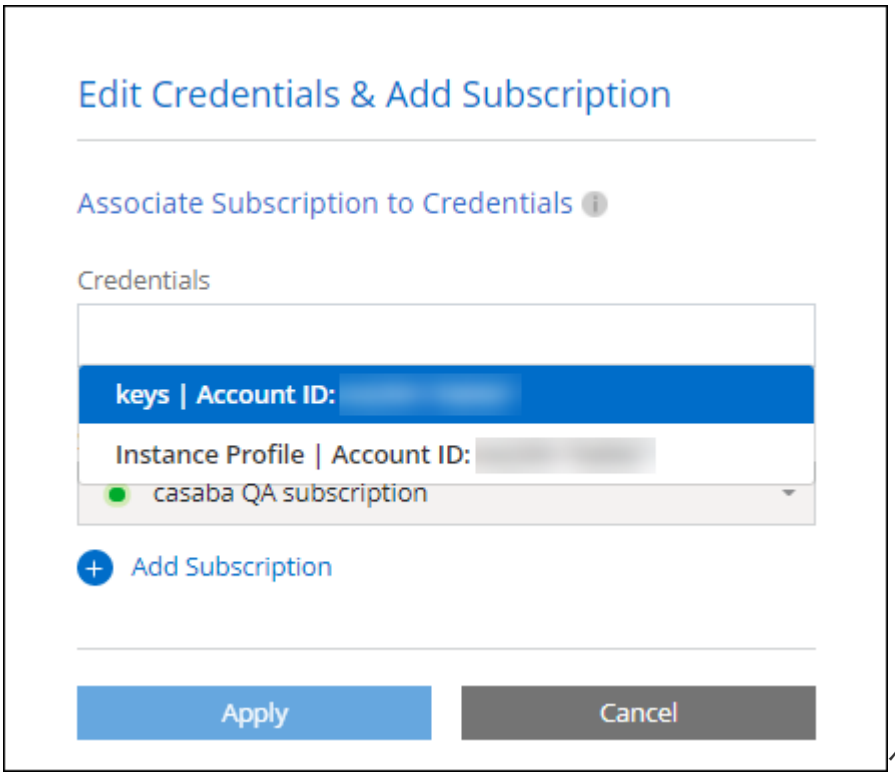
AWS クレデンシャルを既存のコネクタに追加する

BlueXPを追加のAWSアカウントで使用する場合は、IAMユーザのAWSキー、または信頼されたアカウントのロールのARNを指定できます。次の図は、 2 つの追加アカウントを示しています。 1 つは、信頼されたアカウントの IAM ロールを介してアクセス許可を提供し、もう 1 つは IAM ユーザの AWS キーを使用してアクセス許可を提供します。



その後、IAMロールのAmazon Resource Name（ARN）またはIAMユーザのAWSキーを指定して、アカウントクレデンシャルをBlueXPに追加します。

たとえば、新しいCloud Volumes ONTAP 作業環境を作成するときにクレデンシャルを切り替えることができます。



ページで[Switch Account]を選択した後、クラウドプロバイダアカウントを選択するスクリーンショット。"]

"既存のコネクタにAWSクレデンシャルを追加する方法を説明します。"

AWSクレデンシャルを**BlueXP**に直接追加します

BlueXPに新しいAWS資格情報を追加すると'FSX for ONTAP 作業環境の作成と管理'またはコネクタの作成に必要な権限が提供されます

- "BlueXP for Amazon FSx for ONTAP にAWSクレデンシャルを追加する方法をご紹介します"
- "コネクタを作成するためにAWSクレデンシャルをBlueXPに追加する方法について説明します"

クレデンシャルとマーケットプレイスのサブスクリプション

Cloud Volumes ONTAPの料金を時間単位（PAYGO）または年間契約で支払い、その他のBlueXPサービスを

使用できるようにするには、Connectorに追加するクレデンシャルをAWS Marketplaceサブスクリプションに関連付ける必要があります。

"AWSサブスクリプションを関連付ける方法について説明します"。

AWSクレデンシャルとマーケットプレイスサブスクリプションについては、次の点に注意してください。

- 1つのAWSクレデンシャルに関連付けることができるAWS Marketplaceサブスクリプションは1つだけです。
- 既存のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えることが可能

よく寄せられる質問

次の質問は、クレデンシャルとサブスクリプションに関するものです。

AWS クレデンシャルを安全にローテーションするにはどうすればよいですか。

前述のセクションで説明したように、BlueXPではいくつかの方法でAWSクレデンシャルを指定できます。コネクタインスタンスに関連付けられたIAMロール、信頼されたアカウントでIAMロールを想定するか、AWSアクセスキーを指定します。

最初の2つのオプションでは、BlueXPはAWS Security Token Serviceを使用して、絶えず回転する一時的な資格情報を取得します。このプロセスはベストプラクティスであり、自動的に実行され、セキュリティが確保されています。

BlueXPにAWSアクセスキーを提供する場合は、BlueXPで定期的にキーを更新して、キーを回転させる必要があります。これは完全に手動で行います。

AWS Marketplaceの**Cloud Volumes ONTAP**作業環境向けサブスクリプションを変更できますか。

はい、できます。一連のクレデンシャルに関連付けられているAWS Marketplaceサブスクリプションを変更すると、既存および新規のすべてのCloud Volumes ONTAP作業環境に新しいサブスクリプション料金が請求されます。

"AWSサブスクリプションを関連付ける方法について説明します"。

マーケットプレイスのサブスクリプションごとに、複数の**AWS**クレデンシャルを追加できますか。

同じAWSアカウントに属するすべてのAWSクレデンシャルは、同じAWS Marketplaceサブスクリプションに関連付けられます。

異なるAWSアカウントに属する複数のAWSクレデンシャルがある場合は、それらのクレデンシャルを同じAWS Marketplaceサブスクリプションまたは異なるサブスクリプションに関連付けることができます。

既存の**Cloud Volumes ONTAP**作業環境を別の**AWS**アカウントに移動できますか。

いいえ、Cloud Volumes ONTAP作業環境に関連付けられているAWSリソースを別のAWSアカウントに移動することはできません。

マーケットプレイスの導入とオンプレミスの導入でクレデンシャルはどのように機能しますか？

上記の項では、BlueXPのコネクタの推奨される展開方法について説明します。AWS MarketplaceからAWSに

コネクタを導入したり、独自のLinuxホストにコネクタソフトウェアを手動でインストールしたりすることもできます。

Marketplace を使用する場合も、アクセス許可は同じ方法で提供されます。IAM ロールを手動で作成して設定し、追加のアカウントに権限を付与するだけで済みます。

オンプレミス環境の場合、BlueXPシステム用のIAMロールを設定することはできませんが、AWSアクセスキーを使用して権限を指定することはできます。

権限の設定方法については、次のページを参照してください。

- 標準モード
  - "AWS Marketplace環境の権限を設定する"
  - "オンプレミス環境の権限を設定する"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

BlueXPの**AWS**クレデンシャルとマーケットプレイスサブスクリプションを管理

AWSクレデンシャルを追加および管理して、BlueXPがAWSアカウントでクラウドリソースを導入および管理するために必要な権限を持つようにします。複数のAWS Marketplaceサブスクリプションを管理している場合は、[Credentials]ページで各サブスクリプションを異なるAWSクレデンシャルに割り当てることができます。

概要

AWSクレデンシャルを既存のコネクタに追加するか、またはBlueXPに直接追加できます。

- 既存のコネクタにAWSクレデンシャルを追加する

  AWSクレデンシャルを既存のコネクタに追加すると、パブリッククラウド環境内のリソースとプロセスの管理に必要な権限が付与されます。 AWS クレデンシャルをコネクタに追加する方法について説明します。

- BlueXPに、コネクタを作成するためのAWSクレデンシャルを追加します

  新しいAWSクレデンシャルをBlueXPに追加すると、コネクタの作成に必要な権限がBlueXPに付与されます。 AWSクレデンシャルをBlueXPに追加する方法について説明します。

- BlueXP for FSX for ONTAP にAWSクレデンシャルを追加します

  BlueXPに新しいAWS資格情報を追加すると'BlueXPにONTAP 用FSXの作成と管理に必要な権限が与えられます "FSX for ONTAP のアクセス許可を設定する方法について説明します"

クレデンシャルのローテーション方法

BlueXPでは、いくつかの方法でAWSクレデンシャルを提供できます。コネクタインスタンスに関連付けられたIAMロールで、信頼されたアカウントでIAMロールを割り当てるか、AWSアクセスキーを指定します。 "AWS のクレデンシャルと権限に関する詳細情報"。

最初の2つのオプションでは、BlueXPはAWS Security Token Serviceを使用して、絶えず回転する一時的な資格情報を取得します。このプロセスは自動でセキュアであるため、ベストプラクティスです。

BlueXPにAWSアクセスキーを提供する場合は、BlueXPで定期的にキーを更新して、キーを回転させる必要があります。これは完全に手動で行います。

コネクタにクレデンシャルを追加してください

AWSクレデンシャルをコネクタに追加して、パブリッククラウド環境内のリソースとプロセスの管理に必要な権限をコネクタに付与します。別のアカウントの IAM ロールの ARN を指定するか、 AWS アクセスキーを指定できます。

BlueXPを使い始めたばかりの方は、 "BlueXPでのAWSのクレデンシャルと権限の使用方法をご紹介します"。

権限を付与します

ConnectorにAWSクレデンシャルを追加する前に、必要な権限を指定する必要があります。この権限を持つBlueXPは、そのAWSアカウント内のリソースとプロセスを管理できるようになります。アクセス許可の指定方法は、BlueXPに信頼されたアカウントまたはAWSキーの役割のARNを提供するかどうかによって異なります。

> BlueXPからコネクタを導入した場合'BlueXPはコネクタを導入したアカウントのAWS資格情報を自動的に追加しましたこの初期アカウントは、AWS MarketplaceからConnectorを導入した場合や、Connectorソフトウェアを既存のシステムに手動でインストールした場合は追加されません。 "AWS のクレデンシャルと権限について説明します"。

- 選択肢 *
- 別のアカウントで IAM ロールを想定して権限を付与します
- AWS キーを指定して権限を付与します

別のアカウントで **IAM** ロールを想定して権限を付与します

IAM ロールを使用して、コネクタインスタンスを導入したソース AWS アカウントと他の AWS アカウントの間に信頼関係を設定できます。次に、信頼できるアカウントのIAMロールのARNをBlueXPに提供します。

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、この認証方法は使用できません。AWSキーを使用する必要があります。

手順

1. コネクタに権限を付与するターゲットアカウントのIAMコンソールに移動します。
2. [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。

   必ず次の手順を実行してください。

   - 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。
   - 別の AWS アカウント * を選択し、コネクタインスタンスが存在するアカウントの ID を入力します。
   - の内容をコピーして貼り付けることで、必要なポリシーを作成します "コネクタのIAMポリシー"。
3. 後でBlueXPに貼り付けることができるように、IAMロールの役割ARNをコピーします。

結果

これで、アカウントに必要な権限が付与されました。 これで、クレデンシャルをコネクタに追加できるようになりました。

AWS キーを指定して権限を付与します

IAMユーザにAWSキーを提供する場合は、そのユーザに必要な権限を付与する必要があります。BlueXP IAMポリシーでは、BlueXPで使用できるAWSのアクションとリソースを定義しています。

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. IAMコンソールで、の内容をコピーして貼り付けることでポリシーを作成する "コネクタのIAMポリシー"。

   "AWS のドキュメント：「 Creating IAM Policies"

2. IAMロールまたはIAMユーザにポリシーを関連付けます。
   - "AWS のドキュメント：「 Creating IAM Roles"
   - "AWS のドキュメント：「 Adding and Removing IAM Policies"

結果

これで、アカウントに必要な権限が付与されました。 これで、クレデンシャルをコネクタに追加できるようになりました。

クレデンシャルを追加します

必要な権限を AWS アカウントに付与したら、そのアカウントのクレデンシャルを既存のコネクタに追加できます。これにより、同じコネクタを使用してアカウントの Cloud Volumes ONTAP システムを起動できます。

作業を開始する前に

作成したクレデンシャルをクラウドプロバイダで使用できるよう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. ページで[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. * クレデンシャルの定義 * ：信頼された IAM ロールの ARN （ Amazon リソース名）を指定するか、AWS アクセスキーとシークレットキーを入力します。

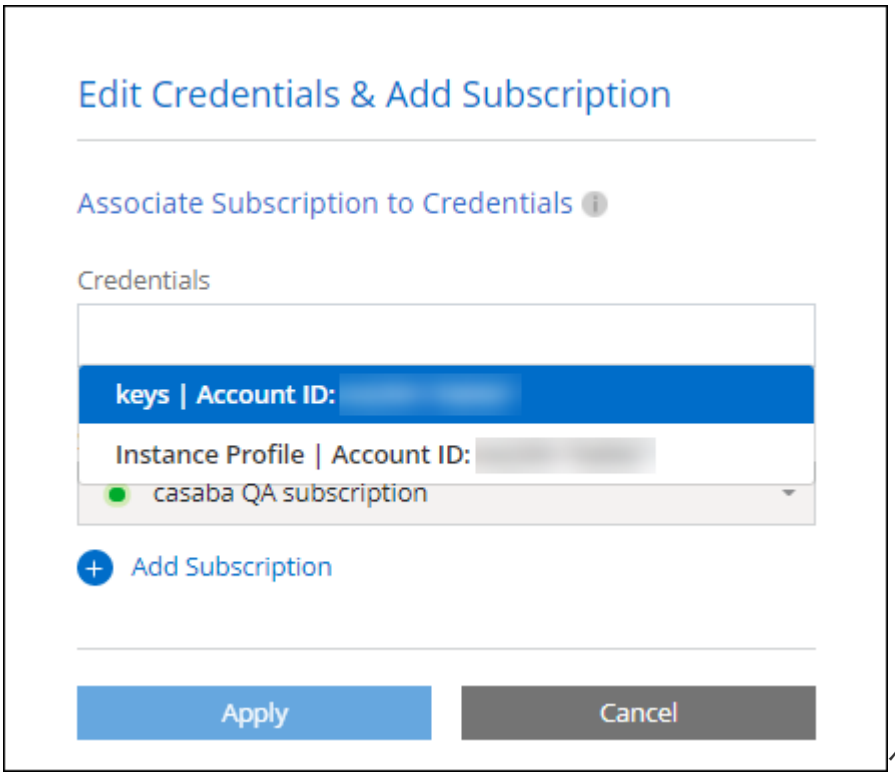
c. * Marketplace サブスクリプション *: 今すぐ登録するか、既存のサブスクリプションを選択して、Marketplace サブスクリプションをこれらの資格情報に関連付けます。

   BlueXPサービスの料金を時間単位（PAYGO）または年間契約で支払うには、AWSクレデンシャルをAWS Marketplaceサブスクリプションに関連付ける必要があります。

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

新しい作業環境を作成するときに、 [詳細と資格情報] ページから別の資格情報セットに切り替えることができるようになりました。



ページで[Switch Account]を選択した後、クラウドプロバイダアカウントを選択するスクリーンショット。"]

コネクタを作成するために、**BlueXP**に資格情報を追加します

BlueXPに、Connectorの作成に必要な権限をBlueXPに与えるIAMロールのARNを提供して、AWSクレデンシャルをBlueXPに追加します。これらのクレデンシャルは、新しいコネクタを作成するときに選択できます。

IAM ロールを設定します

BlueXP SaaSレイヤからロールを引き継ぐためのIAMロールを設定します。

手順

1. ターゲットアカウントの IAM コンソールに移動します。
2. [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。

   必ず次の手順を実行してください。

   - 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。

- 別のAWSアカウント*を選択して、BlueXP SaaSのID 952013314444を入力します
- コネクタの作成に必要な権限を含むポリシーを作成します。
  - "ONTAP の FSX に必要な権限を表示します"
  - "Connector展開ポリシーを表示します"

3. 次の手順で、IAMロールのロールARNをコピーしてBlueXPに貼り付けることができます。

結果

IAM ロールに必要な権限が割り当てられます。 これで、BlueXPに追加できます。

クレデンシャルを追加します

IAMロールに必要な権限を付与したら、BlueXPにARNロールを追加します。

作業を開始する前に

IAM ロールを作成したばかりの場合は、使用できるようになるまで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. ページで[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 > BlueXP *」を選択します。
   b. * クレデンシャルの定義 * ： IAM ロールの ARN （ Amazon リソース名）を指定します。
   c. 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

新しいコネクタを作成するときにクレデンシャルを使用できるようになりました。

BlueXP for Amazon FSx for ONTAP にクレデンシャルを追加

詳細については、を参照してください "Amazon FSx for ONTAP 向けBlueXPドキュメント"

AWS サブスクリプションを関連付ける

AWSのクレデンシャルをBlueXPに追加したら、AWS Marketplaceサブスクリプションをそれらのクレデンシャルに関連付けることができます。このサブスクリプションでは、Cloud Volumes ONTAP の料金を時間単位（PAYGO）または年単位の契約で支払い、その他のBlueXPサービスを利用できます。

BlueXPに資格情報を追加した後、AWS Marketplaceサブスクリプションを関連付けるシナリオは2つあります。

- BlueXPに最初に資格情報を追加したときに、サブスクリプションを関連付けませんでした。

- AWSクレデンシャルに関連付けられているAWS Marketplaceサブスクリプションを変更する。

  現行のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAP作業環境とすべての新規作業環境のMarketplaceサブスクリプションが変更されます。

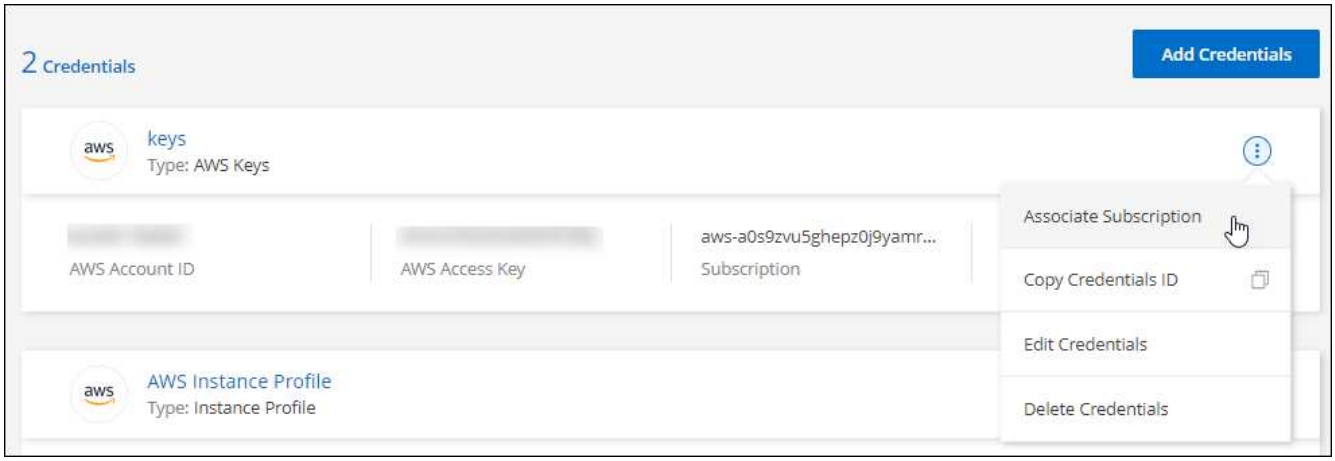
作業を開始する前に

BlueXP設定を変更する前にコネクタを作成する必要があります。 "コネクタの作成方法を説明します"。

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。

   コネクタに関連付けられているクレデンシャルを選択する必要があります。BlueXPに関連付けられているクレデンシャルにMarketplaceサブスクリプションを関連付けることはできません。



3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからサブスクリプションを選択し、*[関連付け]*を選択します。
4. クレデンシャルを新しいサブスクリプションに関連付けるには、*[Add Subscription]>[Continue]*を選択し、AWS Marketplaceで次の手順を実行します。

   a. [購入オプションの表示]*を選択します。
   b. [サブスクライブ]*を選択します。
   c. [アカウントを設定する]*を選択します。

      BlueXPのWebサイトにリダイレクトされます

   d. [サブスクリプションの割り当て*]ページで、次の操作を行います。

      - このサブスクリプションを関連付けるBlueXPアカウントを選択します。
      - [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

- [保存（ Save ）] を選択します。

  次のビデオは、AWS Marketplaceからサブスクライブする手順を示しています。

AWS MarketplaceでBlueXPにサブスクライブ

既存のサブスクリプションをアカウントに関連付ける

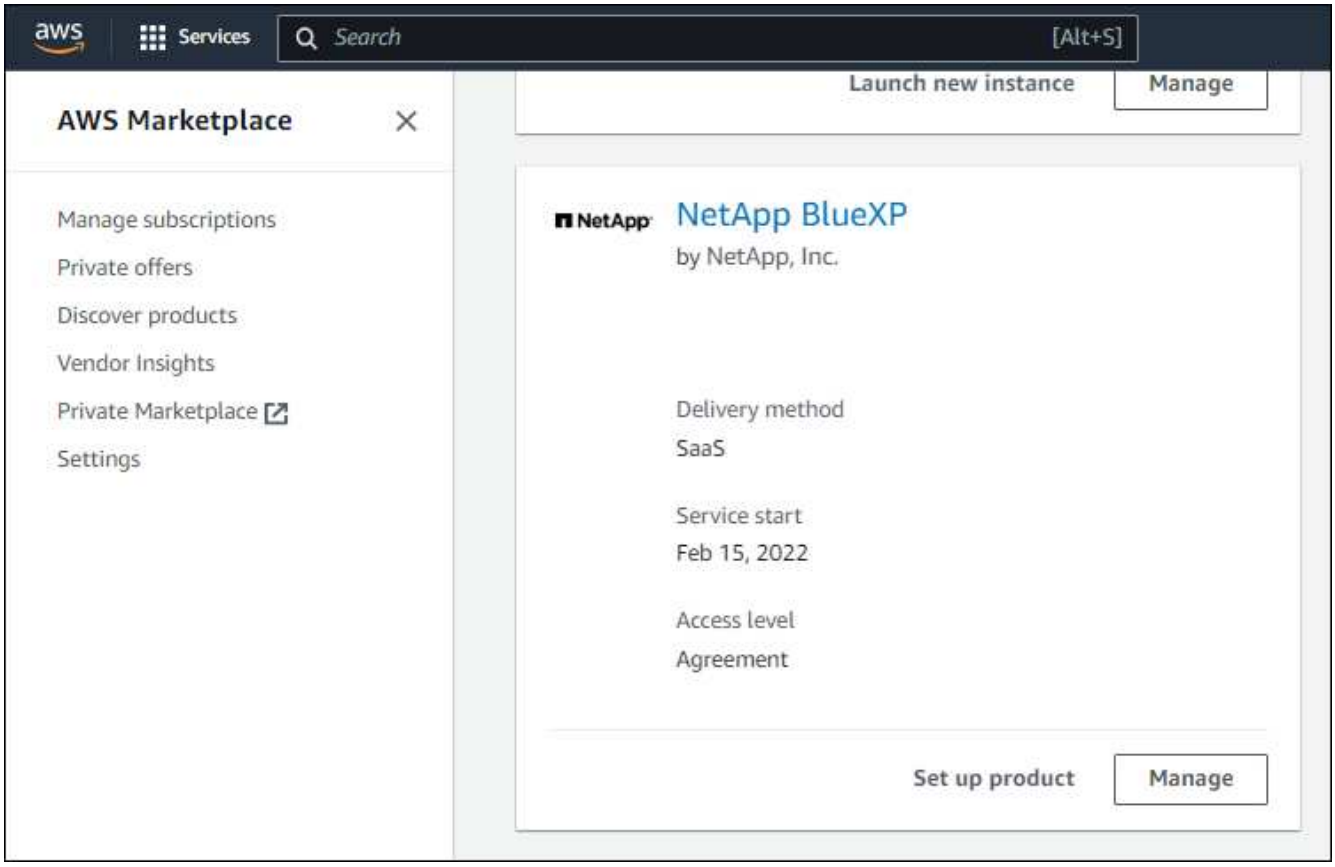
AWS MarketplaceからBlueXPにサブスクライブする際の最後の手順は、BlueXP WebサイトからBlueXPアカウントにサブスクリプションを関連付けることです。この手順を完了していない場合は、BlueXPアカウントでサブスクリプションを使用することはできません。

AWS MarketplaceからBlueXPのサブスクリプションを登録していて、アカウントにサブスクリプションを関連付ける手順をまだ間に合わなかった場合は、次の手順を実行してください。

手順

1. BlueXPのデジタルウォレットにアクセスして、サブスクリプションとBlueXPアカウントが関連付けられていないことを確認します。
   a. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
   b. [サブスクリプション]を選択します。
   c. BlueXPサブスクリプションが表示されないことを確認します。

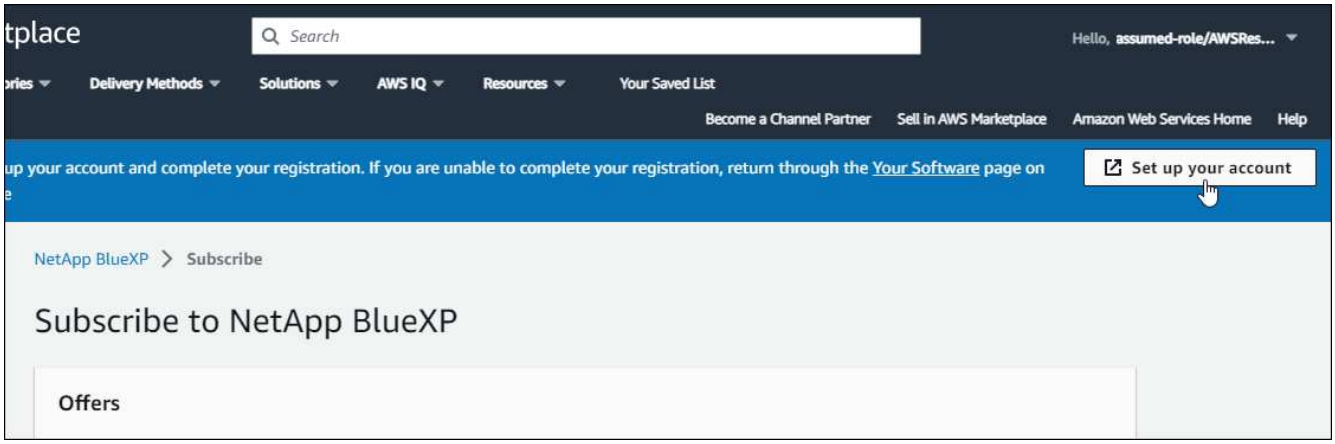
      現在表示しているアカウントに関連付けられている月額プランのみが表示されます。サブスクリプションが表示されない場合は、次の手順に進みます。
2. AWSコンソールにログインし、*[AWS Marketplace Subscriptions]*に移動します。
3. NetApp BlueXPサブスクリプションを見つけましょう。



4. [製品の設定]*を選択します。

   サブスクリプションオファーページが新しいブラウザタブまたはウィンドウにロードされます。

5. [アカウントを設定する]*を選択します。



オプションを示しています。"]

   netapp.comの* Subscription Assignment *ページが新しいブラウザタブまたはウィンドウにロードされます。

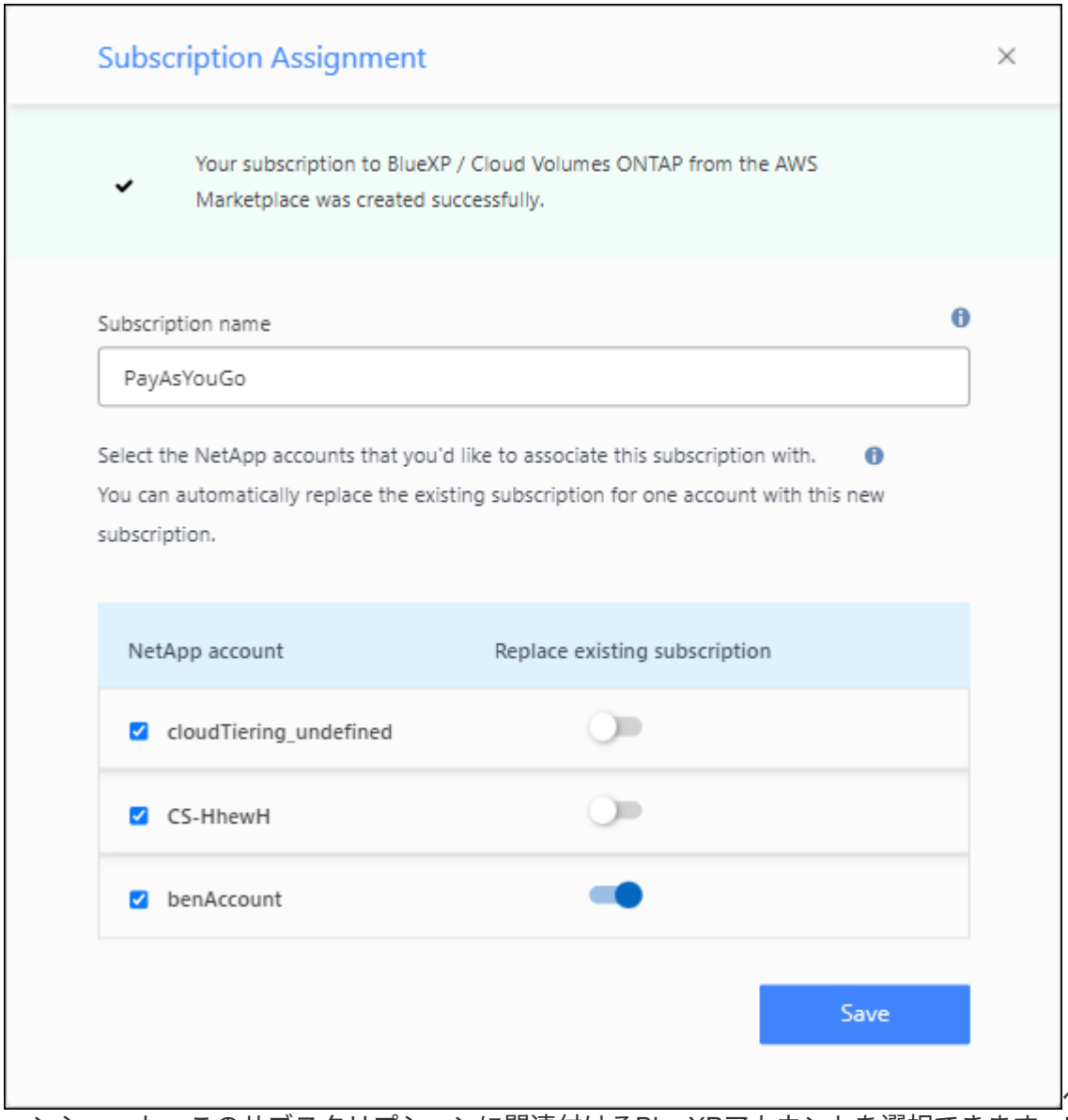
   最初にBlueXPにログインするように求められる場合があります。

6. [サブスクリプションの割り当て*]ページで、次の操作を行います。

- このサブスクリプションを関連付けるBlueXPアカウントを選択します。
- [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

  他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。



ページのスクリーンショット。このサブスクリプションに関連付けるBlueXPアカウントを選択できます。"]

7. BlueXPのデジタルウォレットに移動して、サブスクリプションがBlueXPアカウントに関連付けられていることを確認します。
   a. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
   b. [サブスクリプション]を選択します。

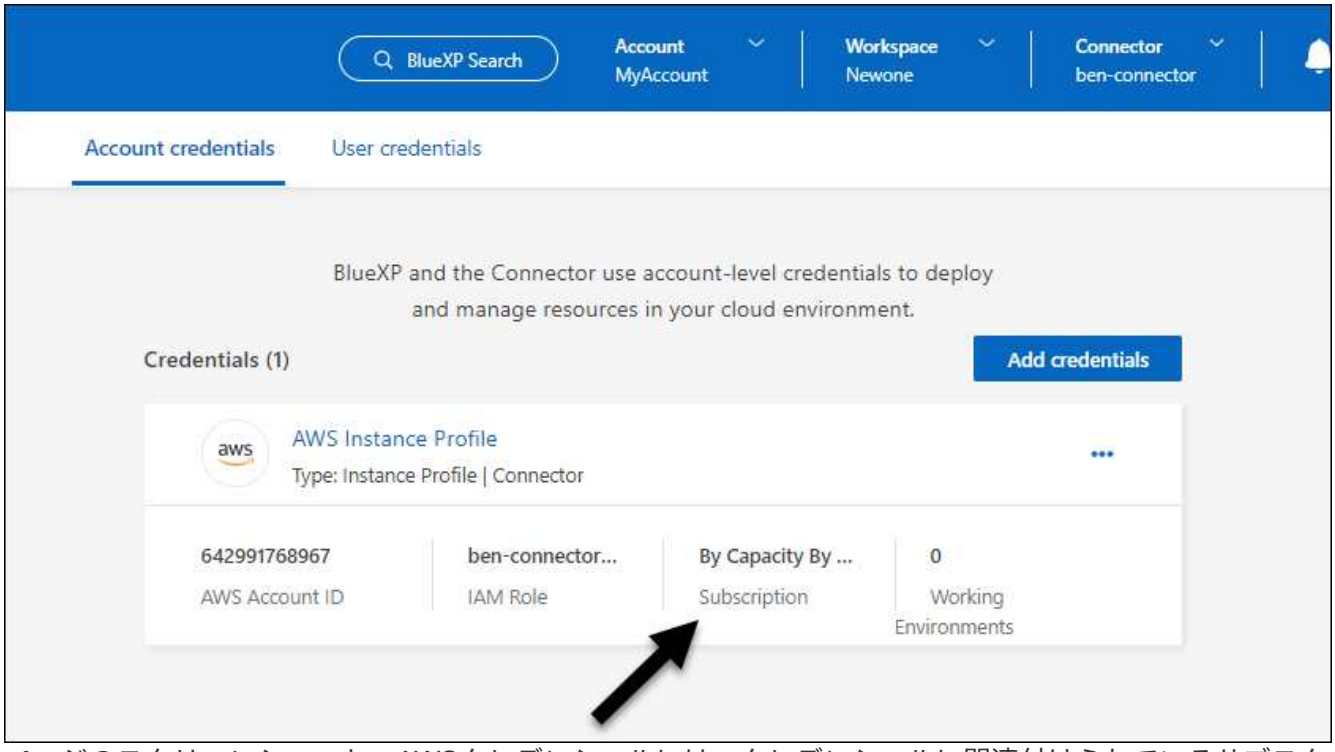
c. BlueXPサブスクリプションが表示されることを確認します。

8. サブスクリプションがAWSクレデンシャルに関連付けられていることを確認します。

   a. 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。

   b. [Account credentials]*ページで、サブスクリプションがAWSクレデンシャルに関連付けられていることを確認します。

      次に例を示します。



ページのスクリーンショット。AWSクレデンシャルには、クレデンシャルに関連付けられているサブスクリプションの名前を示すサブスクリプションフィールドが含まれています。"]

クレデンシャルを編集する

BlueXPでAWSクレデンシャルを編集するには、アカウントタイプ（AWSキーまたは権限）を変更するか、名前を編集するか、クレデンシャル自体（キーまたはロールARN）を更新します。

> コネクタインスタンスに関連付けられているインスタンスプロファイルのクレデンシャルは編集できません。

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. ページで、一連のクレデンシャルの操作メニューを選択し、[クレデンシャルの編集]*を選択します。
3. 必要な変更を行い、*適用*を選択します。

クレデンシャルを削除

一連の資格情報が不要になった場合は、BlueXPから削除できます。削除できるのは、作業環境に関連付けら

れていないクレデンシャルのみです。

> コネクタインスタンスに関連付けられているインスタンスプロファイルのクレデンシャルは削除できません。

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. ページで、一連のクレデンシャルの操作メニューを選択し、[クレデンシャルの削除]*を選択します。
3. [削除]*を選択して確定します。

Azure

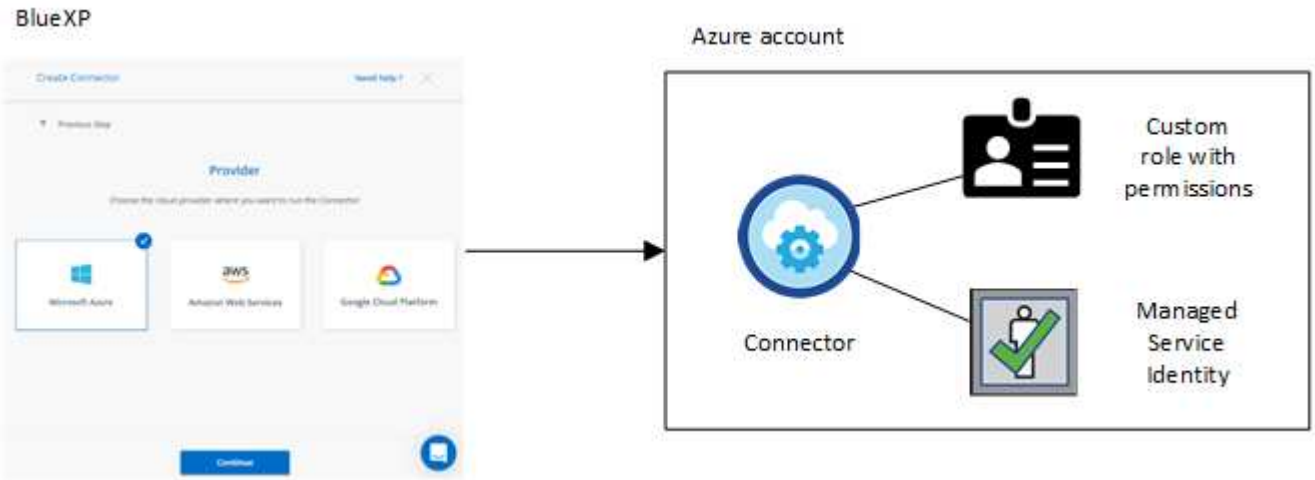
Azure のクレデンシャルと権限について説明します

BlueXPがAzureクレデンシャルを使用してユーザに代わってアクションを実行する方法と、それらのクレデンシャルがマーケットプレイスのサブスクリプションにどのように関連付けられているかをご確認くださいこれらの詳細を理解しておくと、1つ以上のAzureサブスクリプションのクレデンシャルを管理する際に役立ちます。たとえば、AzureクレデンシャルをBlueXPに追加するタイミングを確認できます。

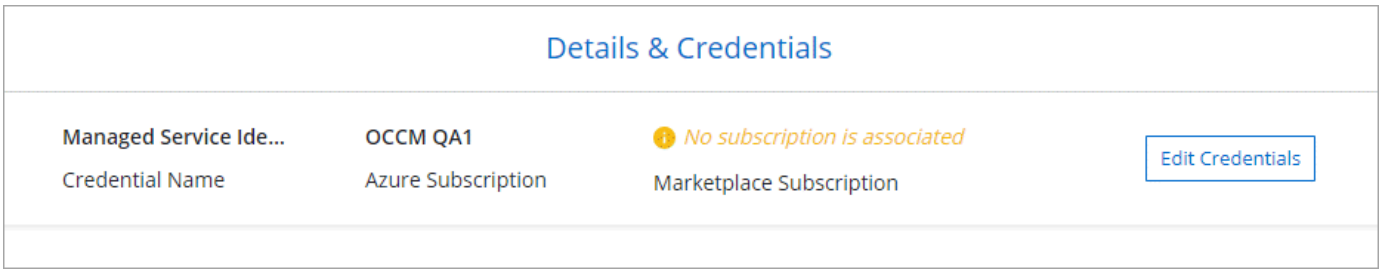
Azure の初期クレデンシャル

BlueXPからConnectorを導入する場合は、Connector仮想マシンを導入する権限を持つAzureアカウントまたはサービスプリンシパルを使用する必要があります。必要な権限は、に表示されます "Azure の Connector 導入ポリシー"。

BlueXPがAzureにConnector仮想マシンを導入すると、が有効になります "システムによって割り当てられた管理 ID" 仮想マシンで、カスタムロールを作成して仮想マシンに割り当てます。このロールは、そのAzureサブスクリプション内でリソースとプロセスを管理するために必要な権限をBlueXPに提供します。 "BlueXPがどのように権限を使用しているかを確認します"。



Cloud Volumes ONTAPの新しい作業環境を作成すると、BlueXPでは次のAzureクレデンシャルがデフォルトで選択されます。



ページの[Switch Account]オプションを示すスクリーンショット。"]

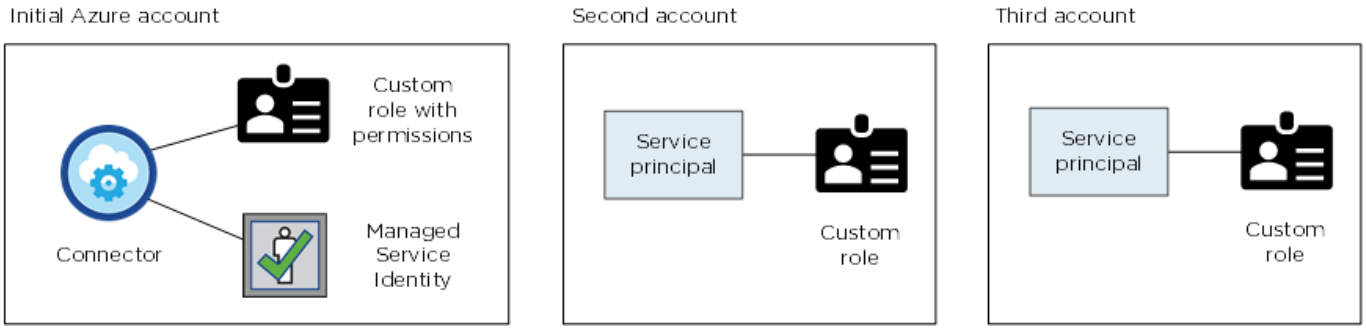
すべての Cloud Volumes ONTAP システムは、初期の Azure クレデンシャルを使用して導入することも、クレデンシャルを追加することもできます。

マネージド **ID** 向けの **Azure** サブスクリプションが追加されました

コネクタVMに割り当てられたシステム割り当ての管理IDは、コネクタを起動したサブスクリプションに関連付けられています。別の Azure サブスクリプションを選択する場合は、が必要です "管理対象 ID をこれらのサブスクリプションに関連付けます"。

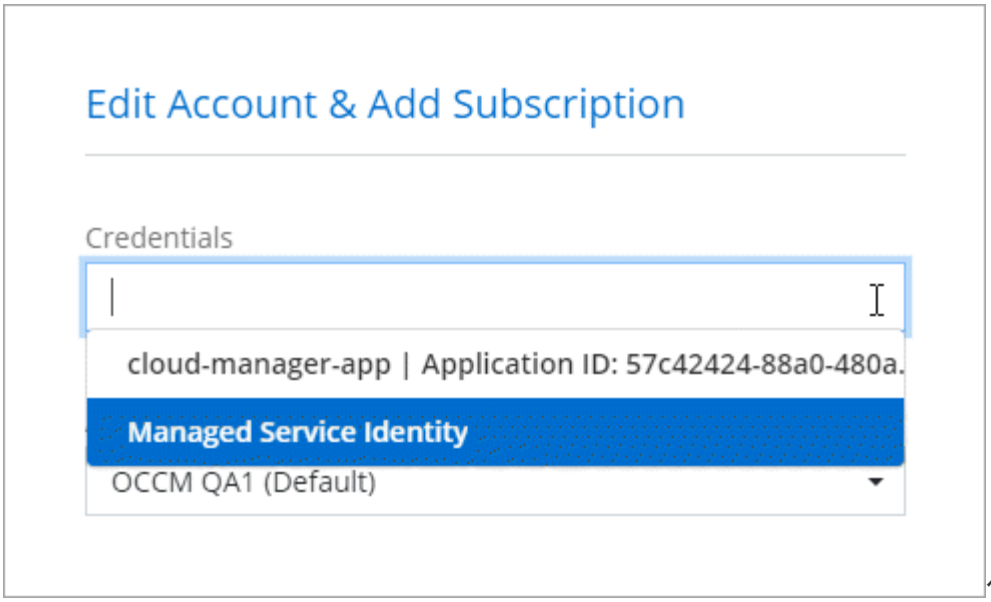
Azure の追加クレデンシャル

BlueXPで別のAzureクレデンシャルを使用する場合は、で必要な権限を付与する必要があります "Microsoft Entra IDでのサービスプリンシパルの作成と設定" を Azure アカウントごとに用意します。次の図は、 2 つの追加アカウントを示しています。各アカウントには、権限を提供するサービスプリンシパルとカスタムロールが設定されています。



そのあとで "アカウントの資格情報をBlueXPに追加します" AD サービスプリンシパルの詳細を指定します。

たとえば、新しいCloud Volumes ONTAP 作業環境を作成するときにクレデンシャルを切り替えることができます。



ページで[Switch Account]を選択した後、クラウドプロバイダアカウントを選択するスクリーンショット。"]

クレデンシャルとマーケットプレイスのサブスクリプション

Cloud Volumes ONTAPの料金を時間単位（PAYGO）または年間契約で支払い、その他のBlueXPサービスを使用できるようにするには、Connectorに追加するクレデンシャルをAzure Marketplaceサブスクリプションに関連付ける必要があります。

"Azureサブスクリプションを関連付ける方法について説明します"。

Azureクレデンシャルとマーケットプレイスサブスクリプションについては、次の点に注意してください。

- 一連のAzureクレデンシャルに関連付けることができるAzure Marketplaceサブスクリプションは1つだけです。
- 既存のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えることが可能

よく寄せられる質問

次の質問は、クレデンシャルとサブスクリプションに関するものです。

Azure MarketplaceのCloud Volumes ONTAP作業環境向けサブスクリプションを変更できますか。

はい、できます。一連のAzureクレデンシャルに関連付けられているAzure Marketplaceサブスクリプションを変更すると、既存および新規のすべてのCloud Volumes ONTAP作業環境が新しいサブスクリプションに対して課金されます。

"Azureサブスクリプションを関連付ける方法について説明します"。

マーケットプレイスのサブスクリプションが異なる複数の**Azure**クレデンシャルを追加できますか。

同じAzureサブスクリプションに属するすべてのAzureクレデンシャルは、同じAzure Marketplaceサブスクリプションに関連付けられます。

異なるAzureサブスクリプションに属する複数のAzureクレデンシャルがある場合、それらのクレデンシャルを同じAzure Marketplaceサブスクリプションまたは異なるマーケットプレイスサブスクリプションに関連付

けることができます。

既存の**Cloud Volumes ONTAP**作業環境を別の**Azure**サブスクリプションに移行できますか。

いいえ、Cloud Volumes ONTAP作業環境に関連付けられているAzureリソースを別のAzureサブスクリプションに移動することはできません。

マーケットプレイスの導入とオンプレミスの導入でクレデンシャルはどのように機能しますか？

上記の項では、BlueXPのコネクタの推奨される展開方法について説明します。Azure MarketplaceからAzureにコネクタを導入したり、独自のLinuxホストにコネクタソフトウェアをインストールしたりすることもできます。

Marketplaceを使用する場合は、コネクタVMとシステムによって割り当てられた管理IDにカスタムロールを割り当てることで権限を付与することも、Microsoft Entraサービスプリンシパルを使用することもできます。

オンプレミス展開の場合、コネクタの管理IDを設定することはできませんが、サービスプリンシパルを使用して権限を提供することはできます。

権限の設定方法については、次のページを参照してください。

- 標準モード
  - "Azure Marketplace環境の権限を設定する"
  - "オンプレミス環境の権限を設定する"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

BlueXPの**Azure**クレデンシャルとマーケットプレイスサブスクリプションを管理

Azureクレデンシャルを追加および管理して、Azureサブスクリプションのクラウドリソースの導入と管理に必要な権限をBlueXPに付与する。複数の Azure Marketplace サブスクリプションを管理する場合は、それぞれのサブスクリプションを、クレデンシャルページから別々の Azure クレデンシャルに割り当てることができます。

複数の Azure クレデンシャルを使用する場合や、複数の Azure Marketplace サブスクリプションを Cloud Volumes ONTAP に使用する場合は、このページの手順に従います。

概要

Azureサブスクリプションと資格情報をBlueXPに追加するには、2つの方法があります。

1. 追加の Azure サブスクリプションを Azure 管理 ID に関連付けます。
2. 別のAzureクレデンシャルを使用してCloud Volumes ONTAP を導入する場合は、サービスプリンシパルを使用してAzure権限を付与し、そのクレデンシャルをBlueXPに追加します。

追加の**Azure**サブスクリプションを管理対象**ID**に関連付けます

BlueXPを使用すると、Cloud Volumes ONTAP を導入するAzureクレデンシャルとAzureサブスクリプションを選択できます。管理対象に別の Azure サブスクリプションを選択することはできません を関連付けない限

り、アイデンティティプロファイルを作成します "管理された ID" それらの登録と。

このタスクについて

管理対象 ID はです "最初の Azure アカウント" BlueXPからコネクタを展開すると、コネクタを展開すると、BlueXPはBlueXP Operatorロールを作成し、Connector仮想マシンに割り当てました。

手順

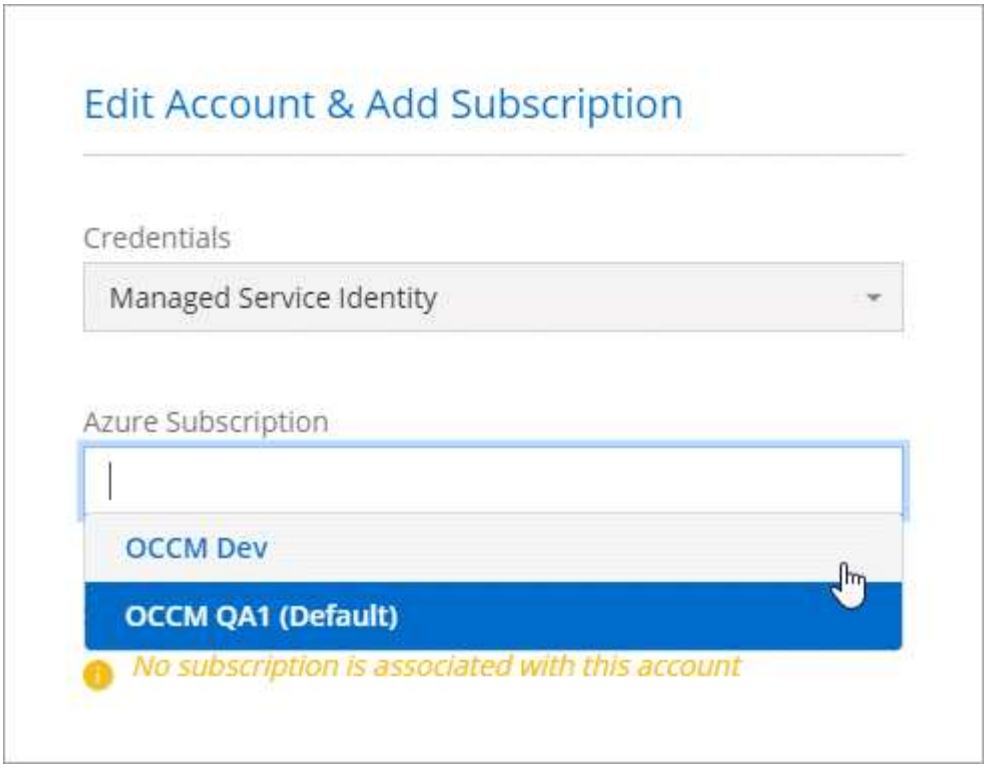
1. Azure ポータルにログインします。
2. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP を展開するサブスクリプションを選択します。
3. [Access control（IAM）]*を選択します。
   a. >[ロール割り当ての追加]*を選択し、権限を追加します。
      - BlueXP Operator *ロールを選択します。

        BlueXP Operatorは、コネクタ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。

      - 仮想マシン * へのアクセスを割り当てます。
      - Connector 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。
      - Connector 仮想マシンを選択します。
      - [保存（ Save ）] を選択します。
4. 追加のサブスクリプションについても、この手順を繰り返します。

結果

新しい作業環境を作成するときに、管理対象 ID プロファイルに対して複数の Azure サブスクリプションから選択できるようになりました。



Azureクレデンシャルを**BlueXP**に追加します

BlueXPからConnectorを展開すると、BlueXPでは、必要な権限を持つシステム割り当ての管理対象IDを仮想マシンで使用できるようになります。Cloud Volumes ONTAP 用の新しい作業環境を作成すると、デフォルトでAzureクレデンシャルが選択されます。

> 既存のシステムに Connector ソフトウェアを手動でインストールした場合、初期クレデンシャルは追加されません。 "Azure のクレデンシャルと権限について説明します"。

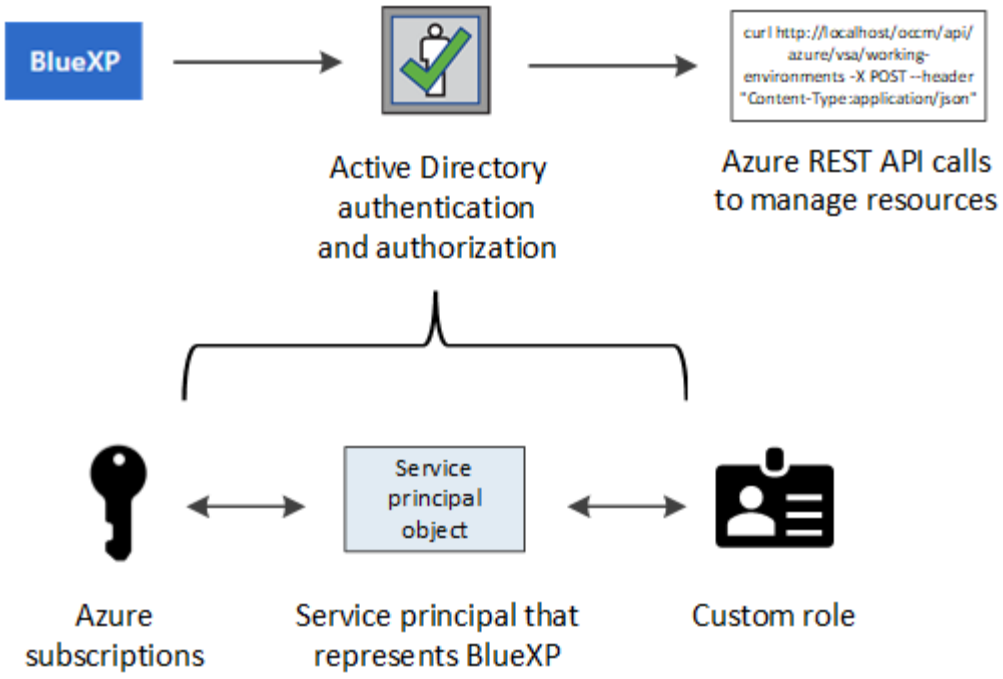
_different_azureクレデンシャルを使用してCloud Volumes ONTAPを導入する場合は、各AzureアカウントのMicrosoft Entra IDでサービスプリンシパルを作成して設定し、必要な権限を付与する必要があります。その後、新しい資格情報をBlueXPに追加できます。

サービスプリンシパルを使用して**Azure**権限を付与します

BlueXPには、Azureで処理を実行するための権限が必要です。Azureアカウントに必要な権限を付与するには、Microsoft Entra IDでサービスプリンシパルを作成して設定し、BlueXPに必要なAzureクレデンシャルを取得します。

このタスクについて

次の図は、Azureで処理を実行するための権限をBlueXPが取得する方法を示しています。1つ以上のAzureサブスクリプションに関連付けられたサービスプリンシパルオブジェクトは、Microsoft Entra IDではBlueXPを表し、必要な権限を許可するカスタムロールに割り当てられます。



手順

1. Microsoft Entraアプリケーションの作成。
2. [アプリケーションをロールに割り当てます]。
3. Windows Azure Service Management API 権限を追加します。
4. アプリケーション ID とディレクトリ ID を取得します。
5. [クライアントシークレットを作成します]。

Microsoft Entraアプリケーションの作成

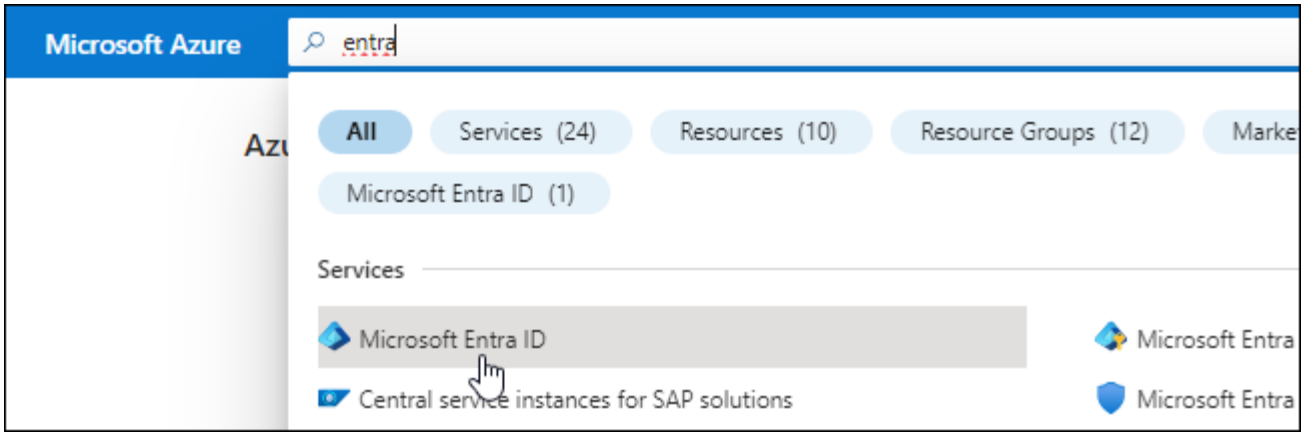
BlueXPでロールベースアクセス制御に使用できるMicrosoft Entraアプリケーションとサービスプリンシパルを作成します。

手順

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。

結果

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

Azureで権限を持つように、サービスプリンシパルを1つ以上のAzureサブスクリプションにバインドし、カスタムの「BlueXP Operator」ロールを割り当てる必要があります。

手順

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。

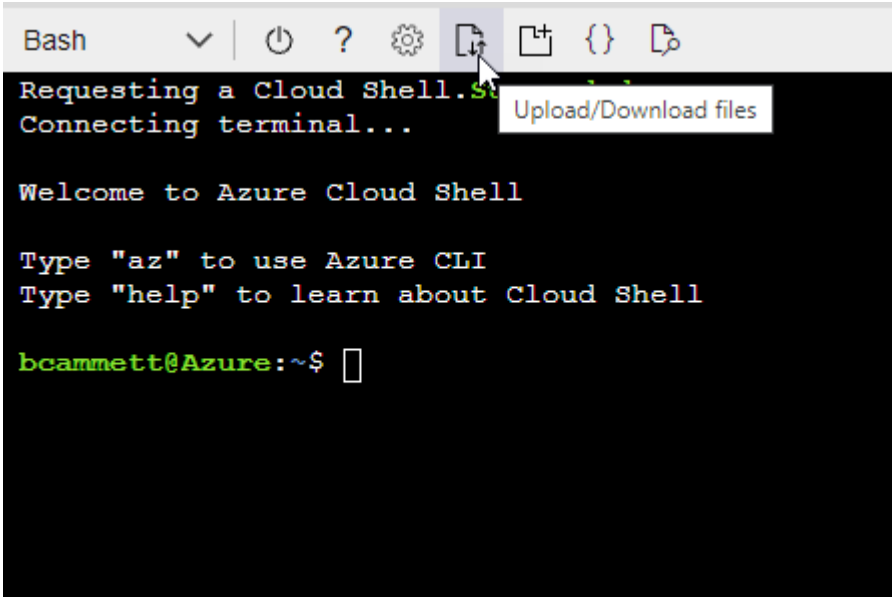
      - 例 *

```
"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。

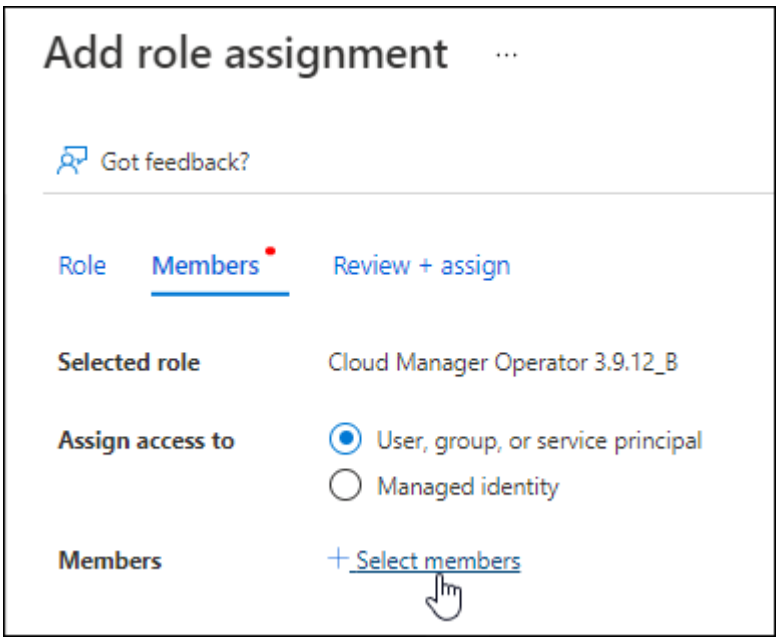
c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。

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。

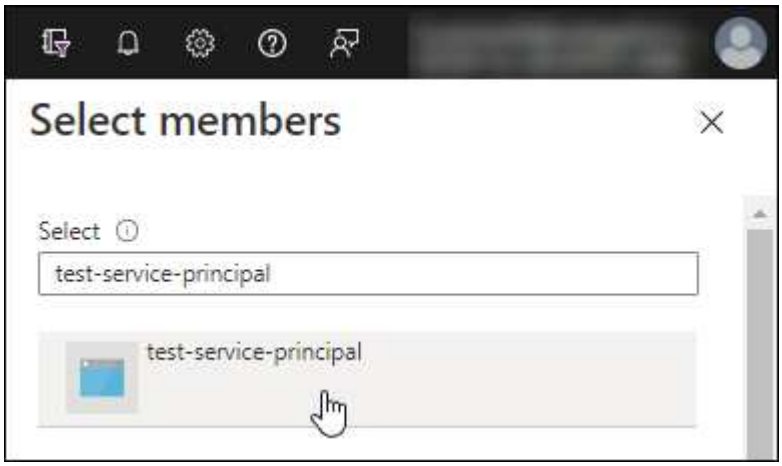
- [* ユーザー、グループ、またはサービスプリンシパル *] を選択したままにします。

- [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。

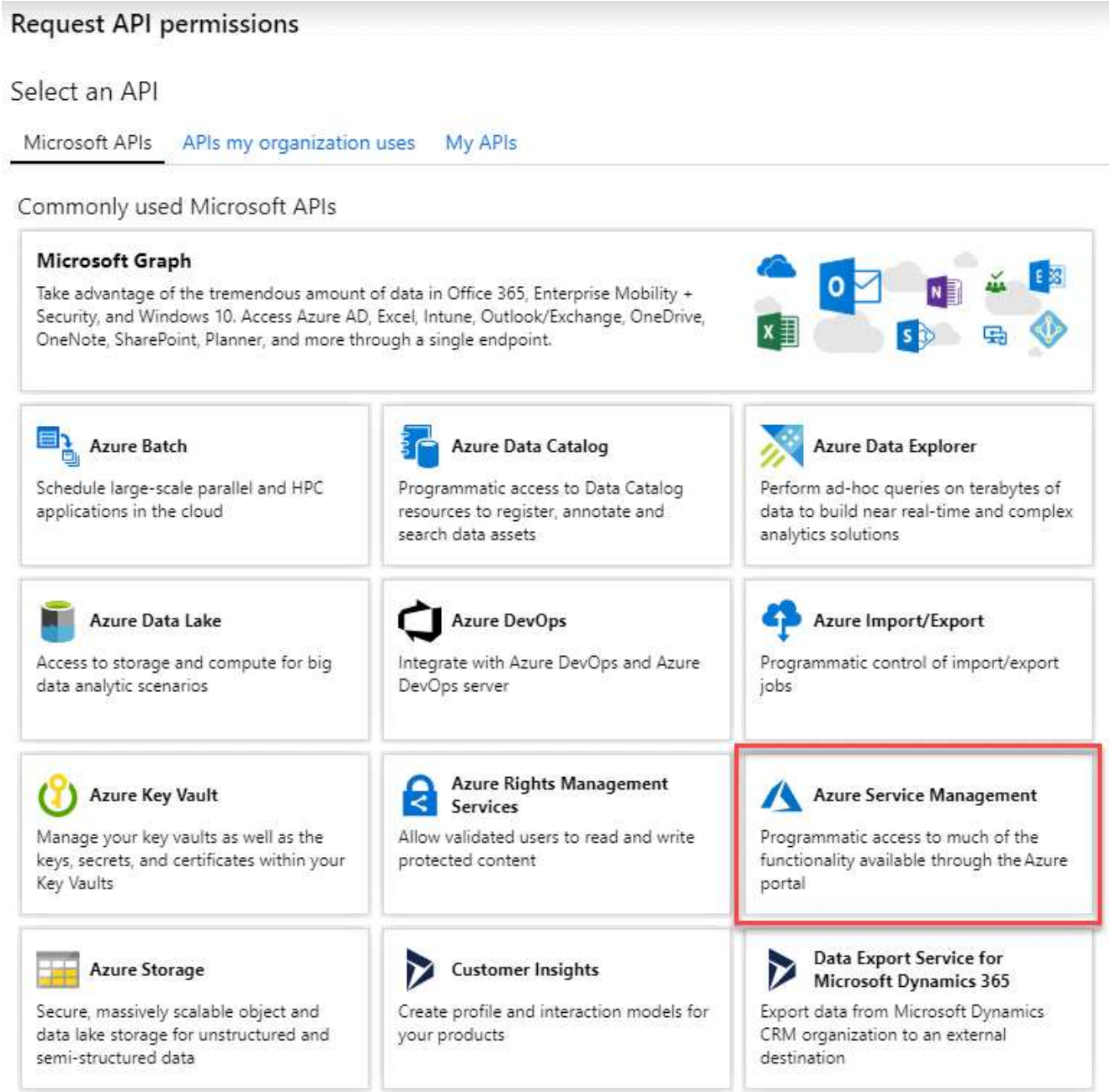
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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

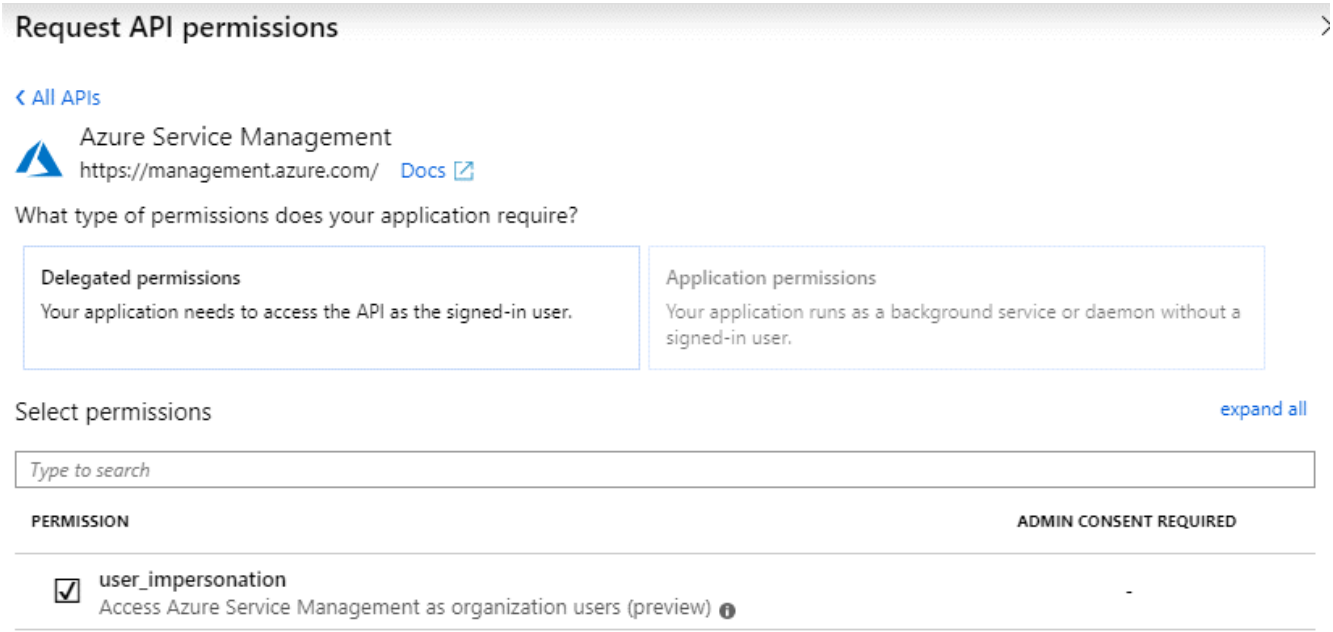
サービスプリンシパルに「 Windows Azure Service Management API 」の権限が必要です。

手順

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。

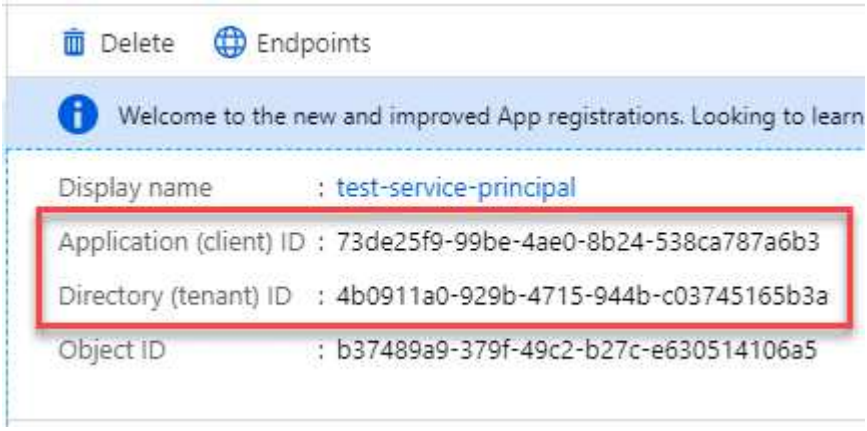


アプリケーション **ID** とディレクトリ **ID** を取得します

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。

手順

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

クライアントシークレットを作成し、そのシークレットの値をBlueXPに提供して、BlueXPがMicrosoft Entra IDで認証できるようにする必要があります。

手順

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。

BlueXPにクレデンシャルを追加します

必要な権限を持つAzureアカウントを入力したら、そのアカウントのクレデンシャルをBlueXPに追加できます。この手順を完了すると、複数の Azure クレデンシャルを使用して Cloud Volumes ONTAP を起動できます。

作業を開始する前に

作成したクレデンシャルをクラウドプロバイダで使用できるよう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。

作業を開始する前に

BlueXP設定を変更する前にコネクタを作成する必要があります。 "コネクタの作成方法を説明します"。

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。

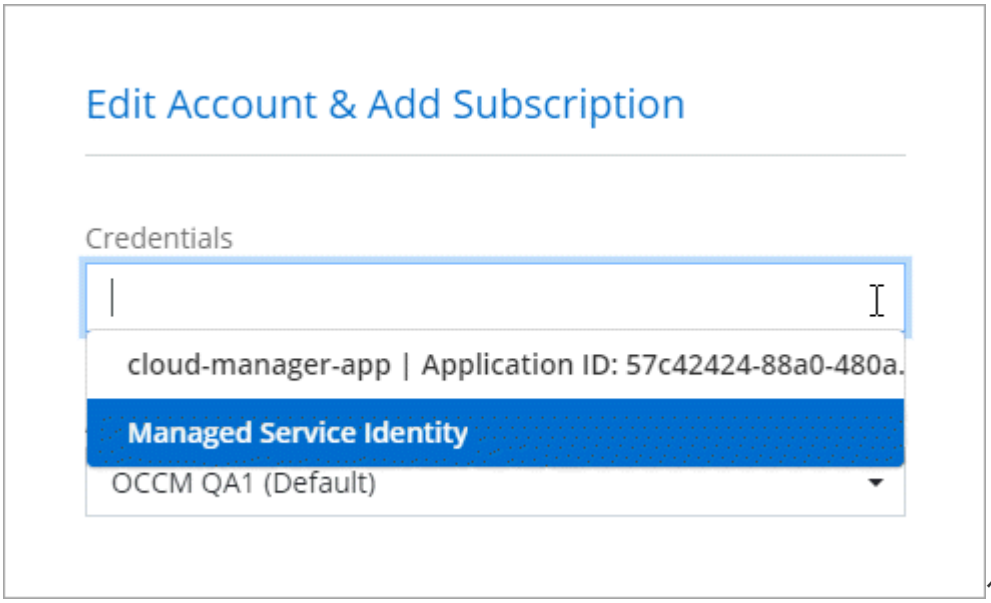
- アプリケーション（クライアント）ID
- ディレクトリ（テナント）ID
- クライアントシークレット

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

これで、から別のクレデンシャルセットに切り替えることができます [詳細と資格情報] ページ "新しい作業環境を作成する場合"



ページで[資格情報の編集]を選択した後の資格情報の選択を示すスクリーンショット。"]

既存のクレデンシャルを管理する

Marketplaceサブスクリプションを関連付け、クレデンシャルを編集し、削除することで、BlueXPに追加済みのAzureクレデンシャルを管理します。

Azure Marketplaceサブスクリプションをクレデンシャルに関連付けます

AzureのクレデンシャルをBlueXPに追加したら、Azure Marketplaceサブスクリプションをそれらのクレデンシャルに関連付けることができます。このサブスクリプションでは、従量課金制のCloud Volumes ONTAP システムを作成したり、他のBlueXPサービスを使用したりできます。

資格情報をBlueXPに追加した後、Azure Marketplaceサブスクリプションを関連付けるシナリオは2つあります。

- BlueXPに最初に資格情報を追加したときに、サブスクリプションを関連付けませんでした。
- Azureクレデンシャルに関連付けられているAzure Marketplaceサブスクリプションを変更する。

  現行のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAP作業環境とすべての新規作業環境のMarketplaceサブスクリプションが変更されます。

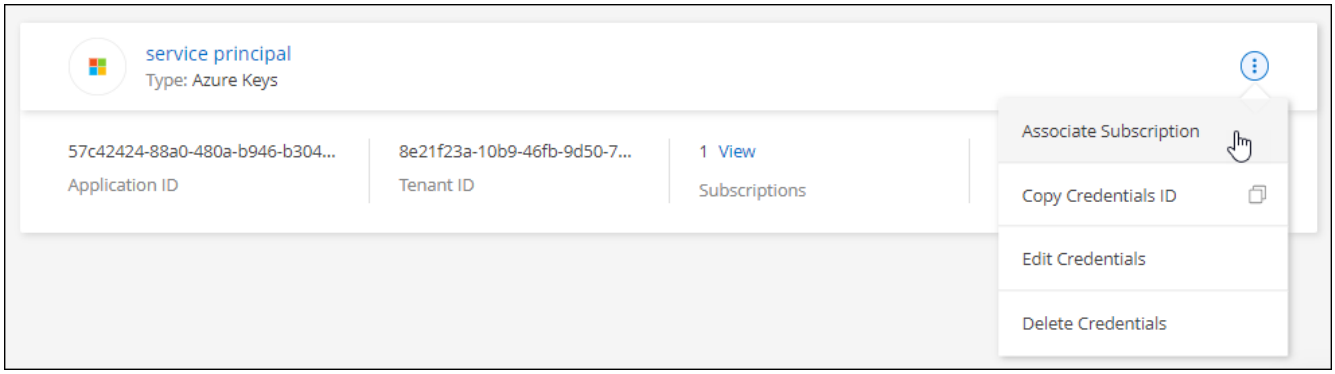
作業を開始する前に

BlueXP設定を変更する前にコネクタを作成する必要があります。 "詳細をご確認ください"。

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。

   コネクタに関連付けられているクレデンシャルを選択する必要があります。BlueXPに関連付けられているクレデンシャルにMarketplaceサブスクリプションを関連付けることはできません。



3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからサブスクリプションを選択し、*[関連付け]*を選択します。
4. クレデンシャルを新しいサブスクリプションに関連付けるには、*[サブスクリプションの追加]>[続行]*を選択し、Azure Marketplaceで次の手順を実行します。

   a. プロンプトが表示されたら、Azureアカウントにログインします。
   b. [サブスクライブ]*を選択します。
   c. フォームに必要事項を入力し、* Subscribe *を選択します。
   d. サブスクリプションプロセスが完了したら、*[今すぐアカウントを設定する]*を選択します。

      BlueXPのWebサイトにリダイレクトされます

   e. [サブスクリプションの割り当て*]ページで、次の操作を行います。

      - このサブスクリプションを関連付けるBlueXPアカウントを選択します。
      - [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

      他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

      - [保存（ Save ）] を選択します。

        次のビデオでは、Azure Marketplaceでのサブスクライブ手順を紹介しています。

Azure MarketplaceでBlueXPにサブスクライブ

クレデンシャルを編集する

Azureサービスクレデンシャルの詳細を変更して、BlueXPでAzureクレデンシャルを編集します。たとえば、サービスプリンシパルアプリケーション用に新しいシークレットが作成された場合は、クライアントシークレットの更新が必要になることがあります。

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. ページで、一連のクレデンシャルの操作メニューを選択し、[クレデンシャルの編集]*を選択します。
3. 必要な変更を行い、*適用*を選択します。

クレデンシャルを削除

一連の資格情報が不要になった場合は、BlueXPから削除できます。削除できるのは、作業環境に関連付けられていないクレデンシャルのみです。

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. ページで、一連のクレデンシャルの操作メニューを選択し、[クレデンシャルの削除]*を選択します。
3. [削除]*を選択して確定します。

Google Cloud

Google Cloudのプロジェクトと権限の詳細

BlueXPでGoogle Cloudのクレデンシャルを使用してユーザに代わって操作を実行する方法と、それらのクレデンシャルがマーケットプレイスのサブスクリプションにどのように関連付けられているかをご確認くださいこれらの詳細を理解しておくと、1つ以上のGoogle Cloudプロジェクトのクレデンシャルを管理する際に役立ちます。たとえば、コネクタVMに関連付けられているサービスアカウントの詳細を確認できます。

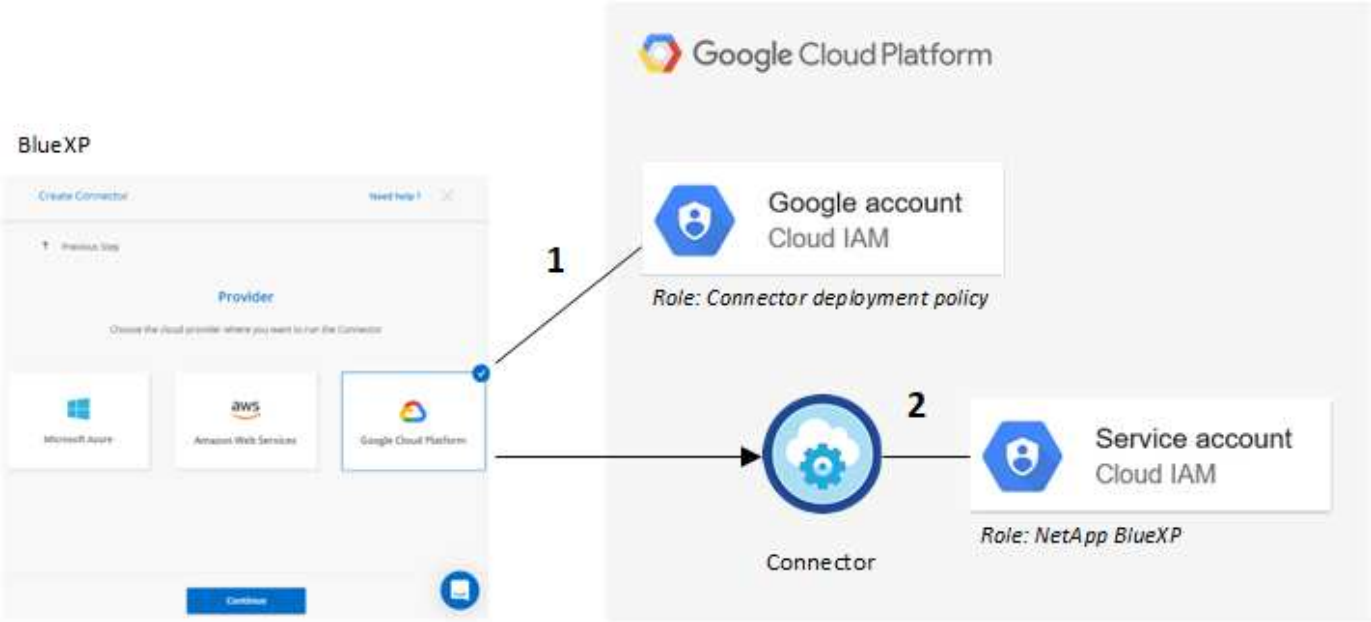
BlueXPのプロジェクトと権限

BlueXPを使用してGoogle Cloudプロジェクトのリソースを管理するには、まずコネクタを導入する必要があります。Connector は、オンプレミスでも別のクラウドプロバイダでも実行できません。

BlueXPからコネクタを直接展開するには、次の2セットの権限が必要です。

1. BlueXPからConnector VMインスタンスを起動する権限を持つGoogleアカウントを使用してConnectorを導入する必要があります。
2. コネクタを配置するときに、を選択するよう求められます "サービスアカウント" VM インスタンスの場合です。BlueXPは、サービスアカウントから、Cloud Volumes ONTAPシステムの作成と管理、BlueXPのバックアップとリカバリを使用したバックアップの管理などの権限を取得します。権限は、サービスアカウントにカスタムロールを割り当てることによって提供されます。

次の図は、上記の番号 1 と 2 で説明した権限の要件を示しています。



権限の設定方法については、次のページを参照してください。

- "標準モードのGoogle Cloud権限を設定します"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

クレデンシャルとマーケットプレイスのサブスクリプション

Google Cloudにコネクタを導入すると、BlueXPによって、コネクタが配置されているプロジェクト内のGoogle Cloudサービスアカウント用のデフォルトクレデンシャルのセットが作成されます。Cloud Volumes ONTAPの料金を時間単位（PAYGO）で支払い、他のBlueXPサービスを使用できるように、これらのクレデンシャルをGoogle Cloud Marketplaceのサブスクリプションに関連付ける必要があります。

"Google Cloud Marketplaceのサブスクリプションを関連付ける方法を確認する"。

Google Cloudクレデンシャルとマーケットプレイスのサブスクリプションについては、次の点に注意してください。

- コネクタに関連付けることができるGoogle Cloudクレデンシャルのセットは1つだけです
- クレデンシャルに関連付けることができるGoogle Cloud Marketplaceサブスクリプションは1つだけです。
- 既存のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えることが可能

Project for Cloud Volumes ONTAP の略

Cloud Volumes ONTAP は、コネクタと同じプロジェクトに存在することも、別のプロジェクトに存在することもできます。Cloud Volumes ONTAP を別のプロジェクトに配置するには、まずコネクタサービスアカウントとその役割をそのプロジェクトに追加する必要があります。

- "サービスアカウントの設定方法について説明します"

- "Google CloudにCloud Volumes ONTAP を導入する方法とプロジェクトを選択する方法について説明します"

BlueXPの**Google Cloud**クレデンシャルとサブスクリプションを管理します

Connector VMインスタンスに関連付けられているGoogle Cloudクレデンシャルを管理するには、Marketplaceサブスクリプションを関連付け、サブスクリプションプロセスをトラブルシューティングします。どちらのタスクも、Marketplaceのサブスクリプションを使用してBlueXPサービスの料金を支払うことができます。

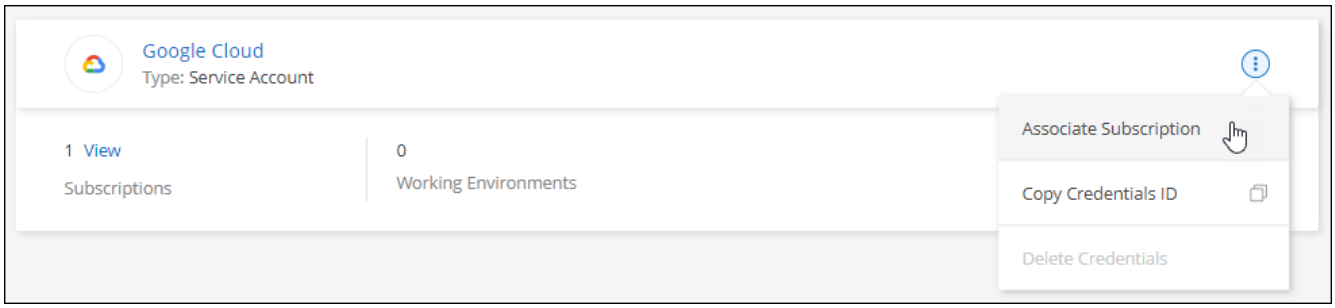
Marketplaceサブスクリプションを**Google Cloud**のクレデンシャルに関連付ける

Google CloudでConnectorを導入すると、Connector VMインスタンスに関連付けられたデフォルトのクレデンシャルセットがBlueXPによって作成されます。これらのクレデンシャルに関連付けられているGoogle Cloud Marketplaceサブスクリプションは、いつでも変更できます。このサブスクリプションでは、従量課金制のCloud Volumes ONTAP システムを作成したり、他のBlueXPサービスを使用したりできます。

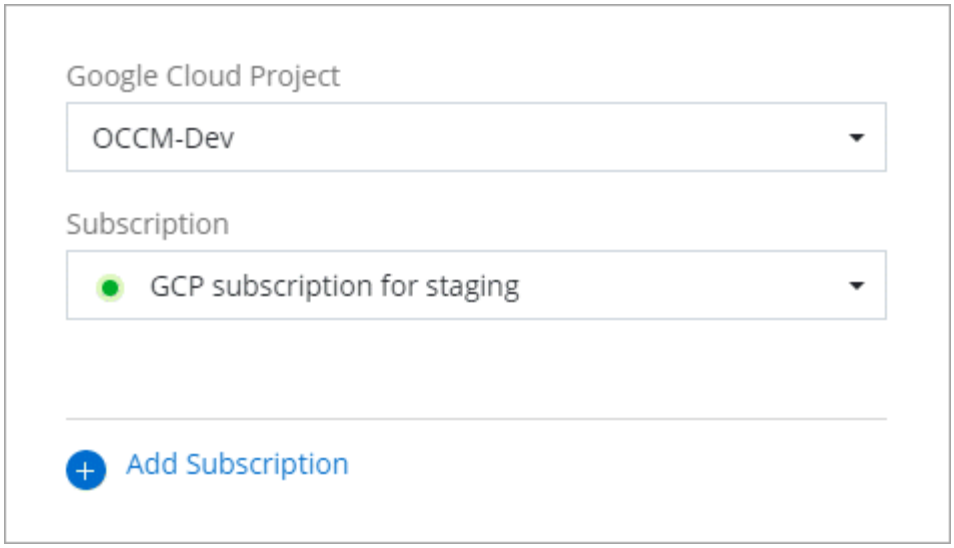
現行のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAP作業環境とすべての新規作業環境のMarketplaceサブスクリプションが変更されます。

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. 一連の資格情報のアクションメニューを選択し、*サブスクリプションの関連付け*を選択します。



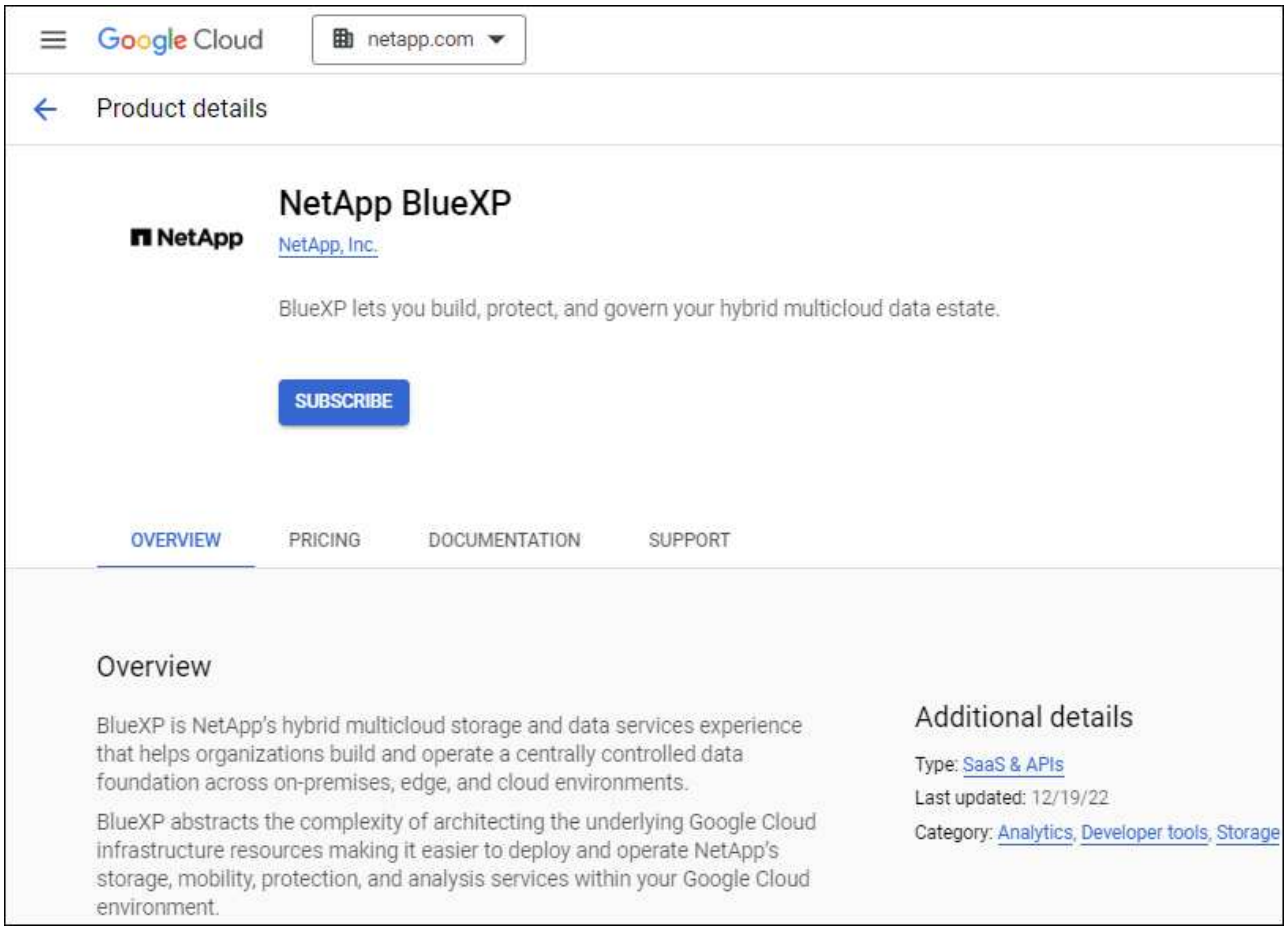
3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからGoogle Cloudプロジェクトとサブスクリプションを選択し、*[関連付け]*を選択します。



4. サブスクリプションをまだお持ちでない場合は、*[サブスクリプションの追加]>[続行]*を選択し、Google Cloud Marketplaceの手順に従います。

> 次の手順を実行する前に、Google CloudアカウントとBlueXPログインの両方に課金管理者権限があることを確認してください。

a. にリダイレクトされたら "Google Cloud MarketplaceのNetApp BlueXPページ"をクリックし、上部のナビゲーションメニューで正しいプロジェクトが選択されていることを確認します。



b. [サブスクライブ]*を選択します。

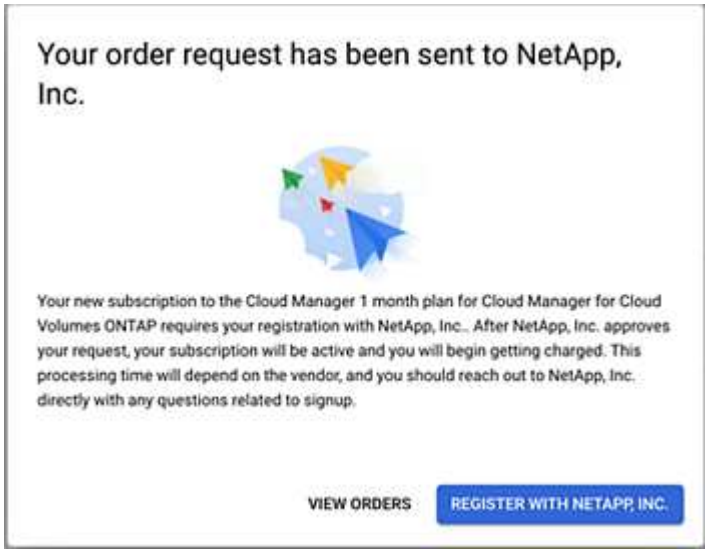
c. 適切な請求先アカウントを選択し、条件に同意します。

d. [サブスクライブ]*を選択します。

転送要求がネットアップに送信されます。

e. ポップアップダイアログボックスで、* NetApp、Inc.への登録*を選択します

Google CloudサブスクリプションをBlueXPアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされてBlueXPにサインインするまで、サブスクリプションをリンクするプロセスは完了していません。



f. [サブスクリプションの割り当て*]ページで次の手順を実行します。

> 組織の誰かが請求アカウントからNetApp BlueXPサブスクリプションにすでに登録している場合は、にリダイレクトされます "BlueXP WebサイトのCloud Volumes ONTAP ページ" 代わりに、予想外の場合は、ネットアップの営業チームにお問い合わせください。Google では、 1 つの Google 請求アカウントにつき 1 つのサブスクリプションのみが有効です。

- このサブスクリプションを関連付けるBlueXPアカウントを選択します。
- [既存のサブスクリプションを置き換える*]フィールドで、1つのアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  BlueXPは、アカウントのすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。一連の資格情報がサブスクリプションに関連付けられていない場合、この新しいサブスクリプションはこれらの資格情報に関連付けられません。

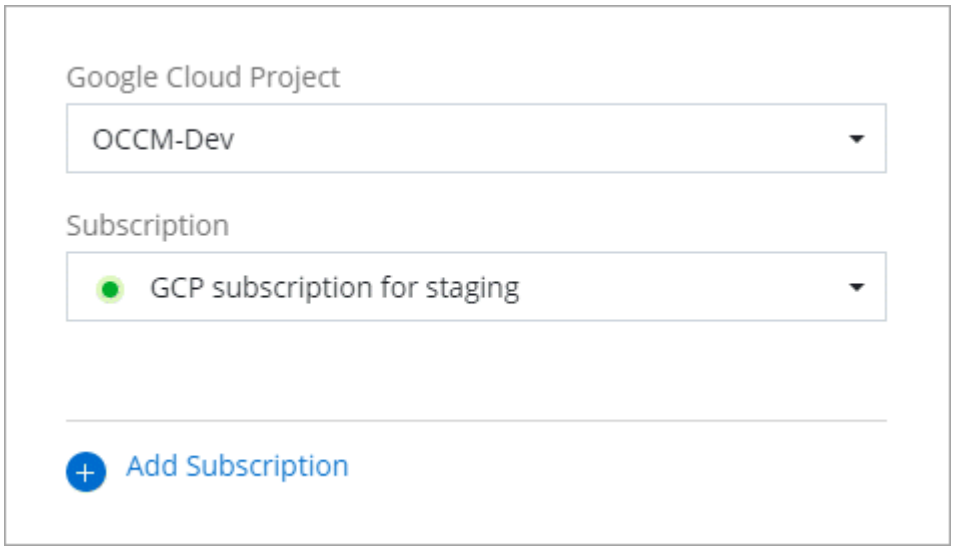
他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

- [保存（ Save ）] を選択します。

  次のビデオでは、Google Cloud Marketplaceから登録する手順を紹介しています。

Google Cloud MarketplaceからBlueXPにサブスクライブ

a. このプロセスが完了したら、BlueXPの[資格情報]ページに戻り、この新しいサブスクリプションを選択します。

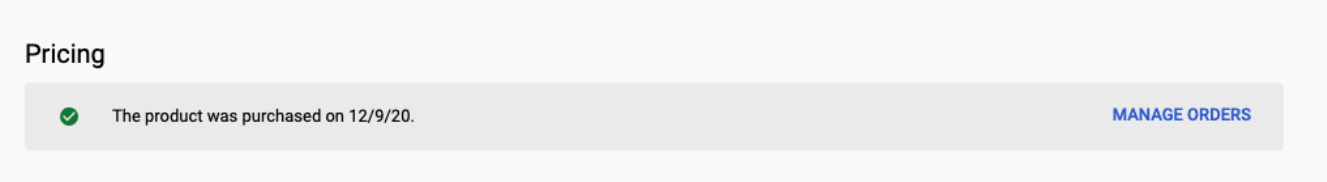


Marketplaceのサブスクリプションプロセスのトラブルシューティング

Google Cloud MarketplaceからBlueXPにサブスクライブすると、権限が正しくない場合やBlueXP Webサイトへのリダイレクトを誤って実行しなかった場合に、断片化されることがあります。この場合は、次の手順に従ってサブスクリプションプロセスを完了してください。

手順

1. に移動します "Google Cloud MarketplaceのNetApp BlueXPページ" 注文の状態を確認します。ページに「プロバイダで管理」と表示されている場合は、下にスクロールして「注文の管理」を選択します。



   - 注文に緑のチェックマークが表示されていて、これが予期しない場合は、同じ請求アカウントを使用している組織の他の人がすでに登録されている可能性があります。想定外のサポートやサブスクリプションの詳細が必要な場合は、ネットアップの営業チームにお問い合わせください。

   - 注文に時計と * 保留中 * のステータスが表示されている場合は、マーケットプレイスのページに戻り、 * プロバイダで管理 * を選択して、上記の手順を完了します。

Filter Enter property name or value

Status	Order number	Plan	Discount	Start date	Plan duration	End date	Payment Schedule	Auto-renew	Next plan
	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A

BlueXPアカウントに関連付けられているNSSクレデンシャルを管理します

NetApp Support SiteアカウントをBlueXPアカウントに関連付けて、Cloud Volumes ONTAPの主要なワークフローを有効にします。これらのNSSクレデンシャルはBlueXPアカウント全体に関連付けられます。

> BlueXPでは、BlueXPユーザごとに1つのNSSアカウントを関連付けることもできます。 "ユーザレベルのクレデンシャルを管理する方法について説明します"。

概要

BlueXPで次のタスクを有効にするには、NetApp Support Site クレデンシャルを特定のBlueXPアカウントIDに関連付ける必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

  ライセンスキーをBlueXPでアップロードし、購入した契約期間のサブスクリプションを有効にするには、NSSアカウントを提供する必要があります。これには、期間の更新の自動更新も含まれます。

- 従量課金制のCloud Volumes ONTAP システムを登録しています

  お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、 NSS アカウントを用意する必要があります。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

これらのクレデンシャルは、特定のBlueXPアカウントIDに関連付けられます。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

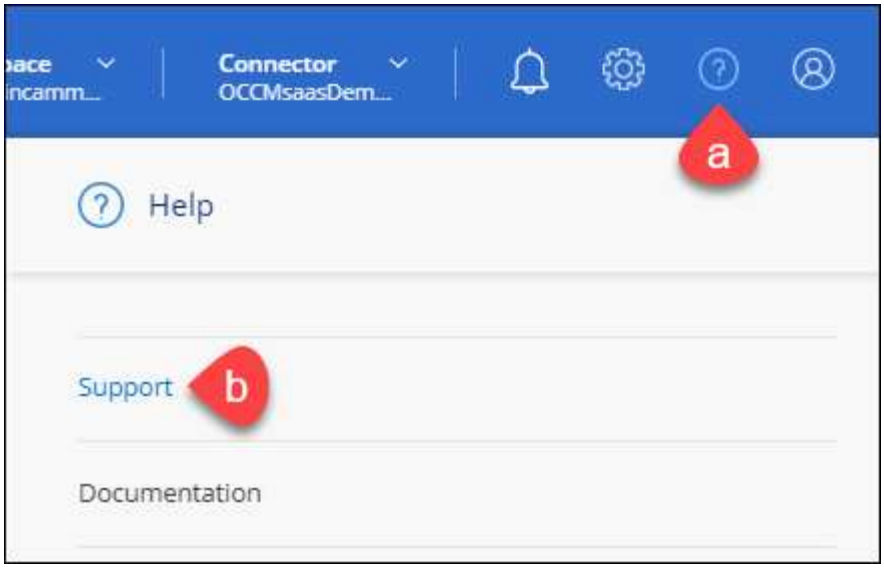
NSS アカウントを追加します

サポートダッシュボードでは、BlueXPで使用するNetApp Support Site アカウントをBlueXPアカウントレベルで追加および管理できます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*を選択します。
3. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

   NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、NetApp Support Siteの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   これらのアクションにより、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

   次の点に注意してください。

   - NSSアカウントは、お客様レベルのアカウントである必要があります（ゲストアカウントや一時アカウントではありません）。複数のお客様レベルのNSSアカウントを設定できます。
   - NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、パートナーレベルのアカウントが存在する場合は、次のエラーメッセージが表示されます。

     「別のタイプのNSSユーザーがすでに存在するため、このアカウントではNSS顧客タイプは許可されていません。」

   既存のお客様レベルのNSSアカウントがあり、パートナーレベルのアカウントを追加しようとする場合も同様です。

   - ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

     これはシステムによって生成されたIDで、電子メールにマッピングされます。[**NSS Management**]ページで、から電子メールを表示できます ••• メニュー。

   - ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます ••• メニュー。

このオプションを使用すると、再度ログインするように求められます。これらのアカウントのトークンは90日後に期限切れになります。このことを通知する通知が投稿されます。

次の手順

新しいCloud Volumes ONTAPシステムの作成時や既存のCloud Volumes ONTAPシステムの登録時にアカウントを選択できるようになりました。

- "AWS での Cloud Volumes ONTAP の起動"
- "Azure で Cloud Volumes ONTAP を起動します"
- "Google Cloud で Cloud Volumes ONTAP を起動しています"
- "従量課金制システムの登録"

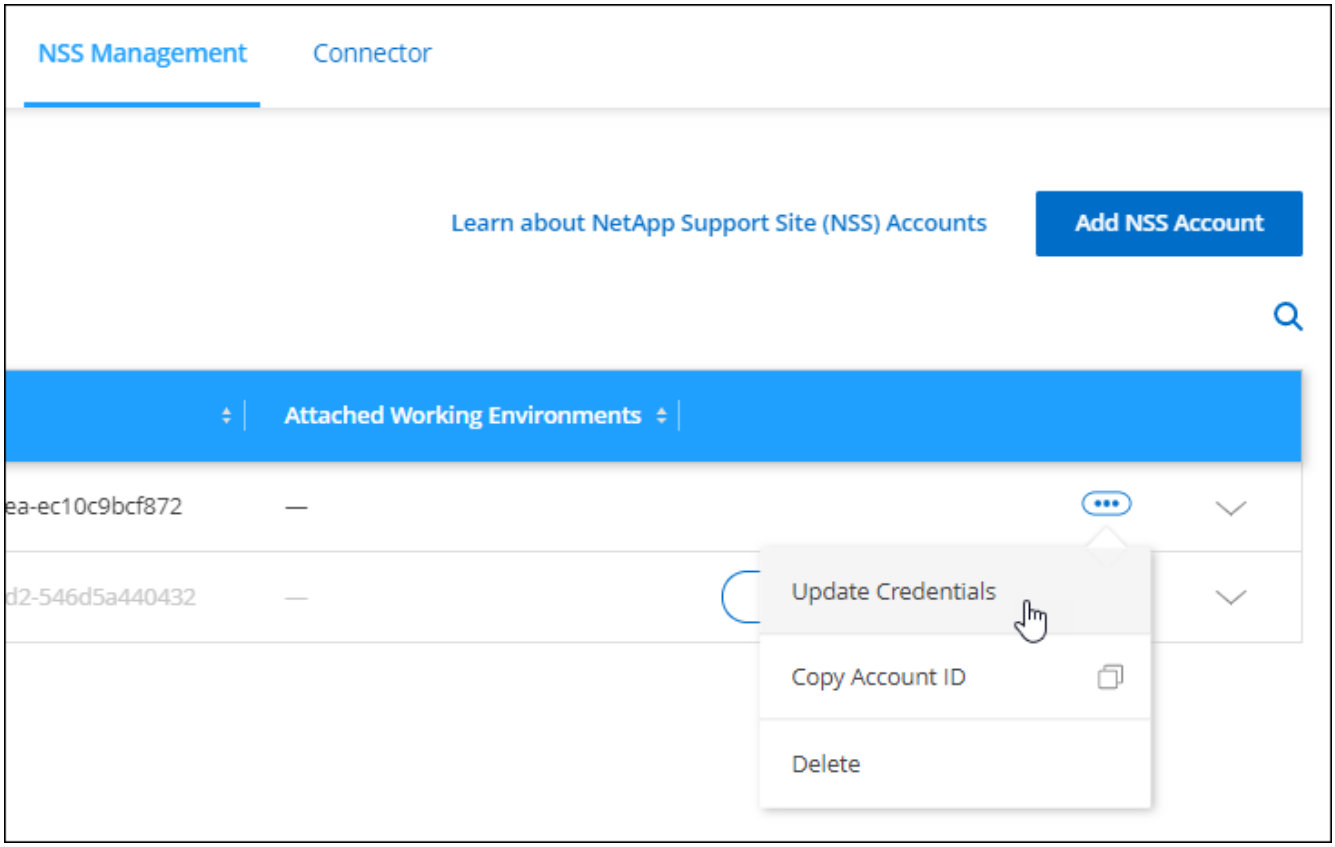
NSS クレデンシャルを更新します

次のいずれかの場合は、BlueXPでNSSアカウントの資格情報を更新する必要があります。

- このアカウントのクレデンシャルを変更した場合
- アカウントに関連付けられた更新トークンの有効期限は3カ月です

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。
2. [NSS Management]*を選択します。
3. 更新するNSSアカウントのを選択します ••• 次に、 [資格情報の更新] を選択します。



4. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

   NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

5. ログインページで、NetApp Support Siteの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

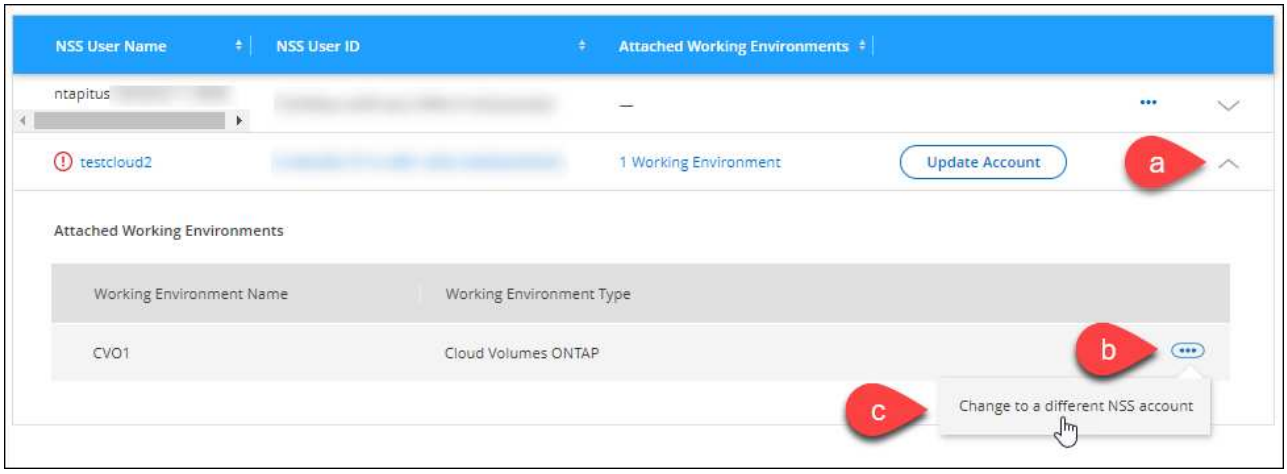
作業環境を別の **NSS** アカウントに接続します

組織に複数のNetApp Support Siteのアカウントがある場合、 Cloud Volumes ONTAP システムに関連付けられているアカウントを変更することができます。

この機能は、ID管理にNetAppが採用したMicrosoftエントラIDを使用するように設定されたNSSアカウントでのみサポートされます。この機能を使用する前に、* NSSアカウントの追加*または*アカウントの更新*を選択する必要があります。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。
2. [NSS Management]*を選択します。
3. NSS アカウントを変更するには、次の手順を実行します。
   a. 作業環境が現在関連付けられているNetApp Support Siteのアカウントの行を展開します。
   b. 関連付けを変更する作業環境で、を選択します ⋯
   c. 別の NSS アカウントに変更 * を選択します。



   d. アカウントを選択し、*[保存]*を選択します。

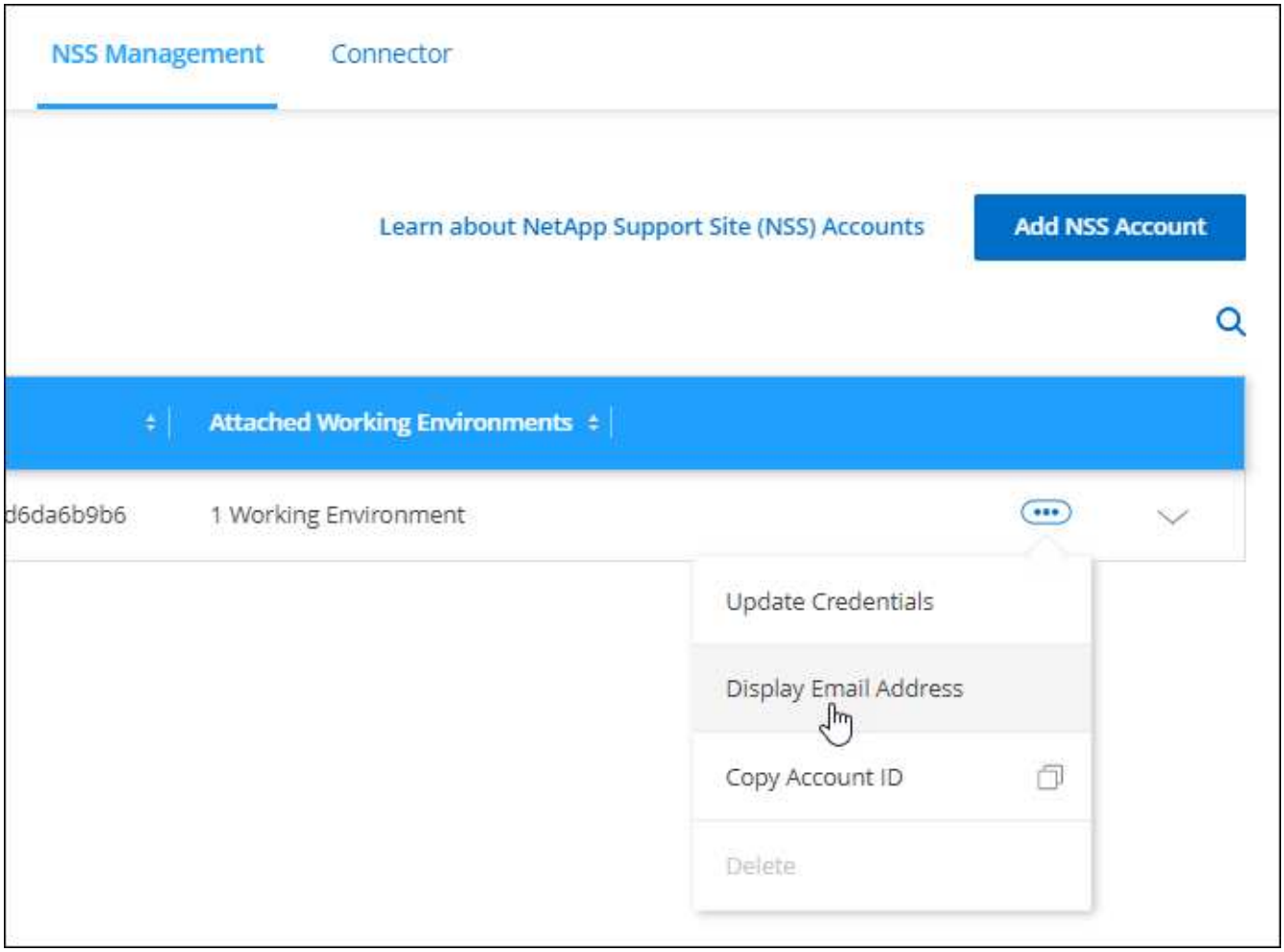
NSS アカウントの **E** メールアドレスを表示します

NetApp Support Siteアカウントで認証サービスにMicrosoft Entra IDが使用されるようになったため、BlueXPに表示されるNSSユーザ名は通常、Microsoft Entraによって生成された識別子です。そのため、そのアカウントに関連付けられている E メールアドレスがすぐにわからない場合があります。しかし、BlueXPには、関連するメールアドレスを表示するオプションがあります。

NSS管理ページに移動すると、表の各アカウントのトークンがBlueXPによって生成されます。このトークンには、関連付けられた E メールアドレスに関する情報が含まれます。その後、ページから移動するとトークンが削除されます。この情報はキャッシュされないため、プライバシーを保護できます。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。
2. [NSS Management]*を選択します。
3. 更新するNSSアカウントのを選択します ••• 次に、 [電子メールアドレスの表示 *] を選択します。



結果

NetApp Support Site ユーザー名と関連するメールアドレスが表示されます。コピーボタンを使用して、電子メールアドレスをコピーできます。

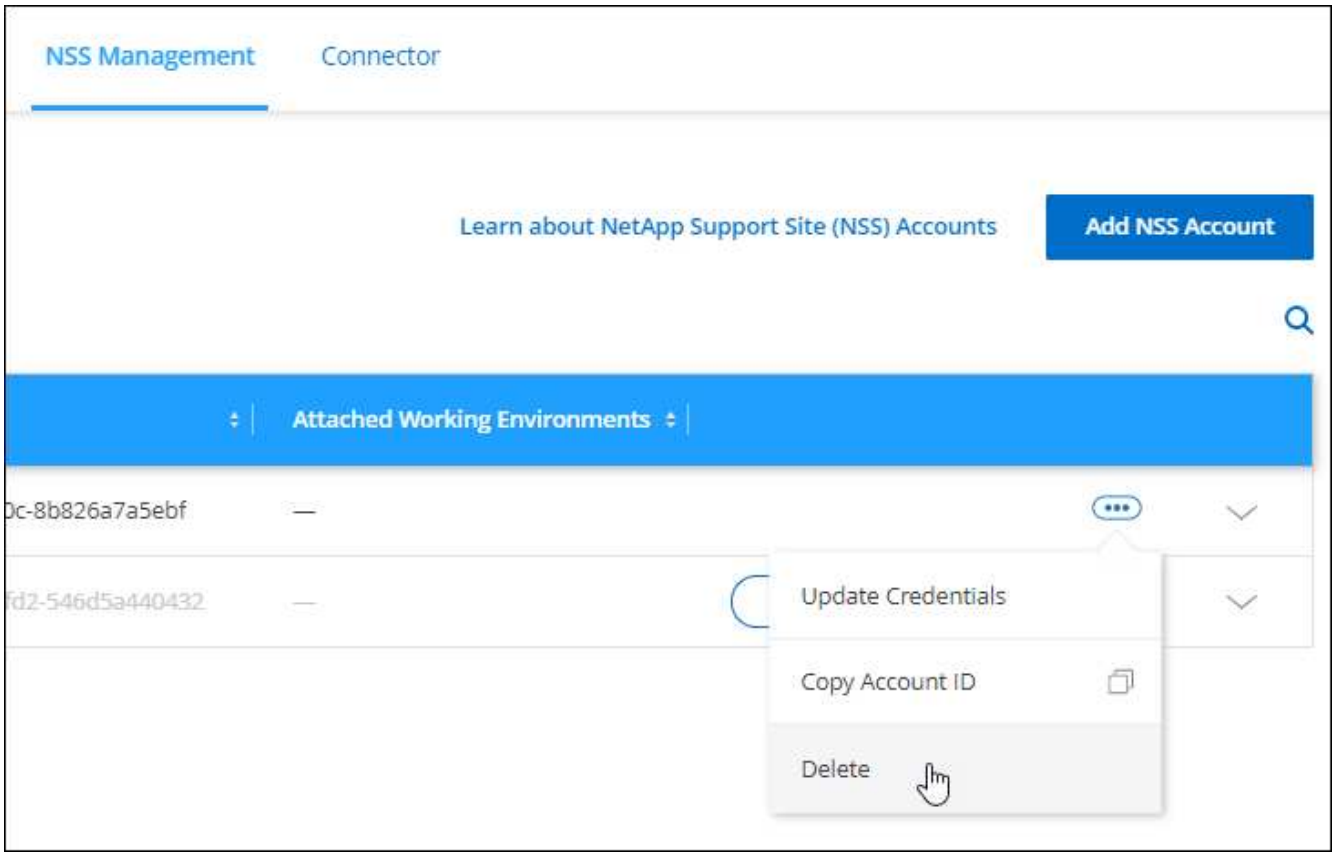
NSS アカウントを削除します

BlueXPで使用しないNSSアカウントをすべて削除します。

Cloud Volumes ONTAP 作業環境に現在関連付けられているアカウントは削除できません。最初にが必要です[それらの作業環境を別の NSS アカウントに接続します](#)。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。
2. [NSS Management]*を選択します。
3. 削除するNSSアカウントのを選択します ••• 次に、 * Delete * を選択します。



4. [削除]*を選択して確定します。

BlueXPログインに関連付けられているクレデンシャルを管理します

BlueXPで実行した操作によっては、ONTAP クレデンシャルとNetApp Support Site（NSS）クレデンシャルがBlueXPユーザログインに関連付けられている場合があります。関連付けたクレデンシャルは、BlueXPで表示および管理できます。たとえば、これらのクレデンシャルのパスワードを変更した場合は、BlueXPでパスワードを更新する必要があります。

ONTAP クレデンシャル

コネクタを使用せずにオンプレミスのONTAP クラスタを直接検出すると、クラスタのONTAP クレデンシャルを入力するように求められます。これらのクレデンシャルはユーザレベルで管理されます。つまり、ログインした他のユーザはこれらのクレデンシャルを表示できません。

NSSクレデンシャル

BlueXPログインに関連付けられたNSSクレデンシャルにより、サポート登録、ケース管理、Digital Advisorへのアクセスが可能になります。

- [サポート]>[リソース]*にアクセスしてサポートに登録すると、NSSクレデンシャルをBlueXPログインに関連付けるように求められます。

  この操作により、BlueXPアカウントがサポート用に登録され、サポート使用権がアクティブ化されます。サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウント内の1人のユーザだけがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。これが完了すると、*リソース*ページにアカウントがサポートに登録されたことが表示されます。

  "サポートに登録する方法について説明します"

- [サポート]>[ケース管理]*にアクセスすると、NSSクレデンシャルを入力するように求められます（まだ入力していない場合）。このページでは、NSSアカウントと会社に関連付けられたサポートケースを作成および管理できます。
- BlueXPでDigital Advisorにアクセスすると、NSS資格情報を入力してDigital Advisorにログインするように求められます。

BlueXPログインに関連付けられているNSSアカウントについては、次の点に注意してください。

- アカウントはユーザレベルで管理されるため、他のユーザがログインしても表示できません。
- Digital Advisorとサポートケース管理に関連付けることができるNSSアカウントは、ユーザごとに1つだけです。
- NetApp Support SiteアカウントをCloud Volumes ONTAP作業環境に関連付ける場合は、メンバーであるBlueXPアカウントに追加されたNSSアカウントからのみ選択できます。

  NSSアカウントレベルのクレデンシャルは、BlueXPログインに関連付けられたNSSアカウントとは異なります。NSSアカウントレベルのクレデンシャルを使用して、お客様所有のライセンスを使用（BYOL）した場合、PAYGOシステムを登録した場合、Cloud Volumes ONTAPソフトウェアをアップグレードした場合にCloud Volumes ONTAPを導入できます。

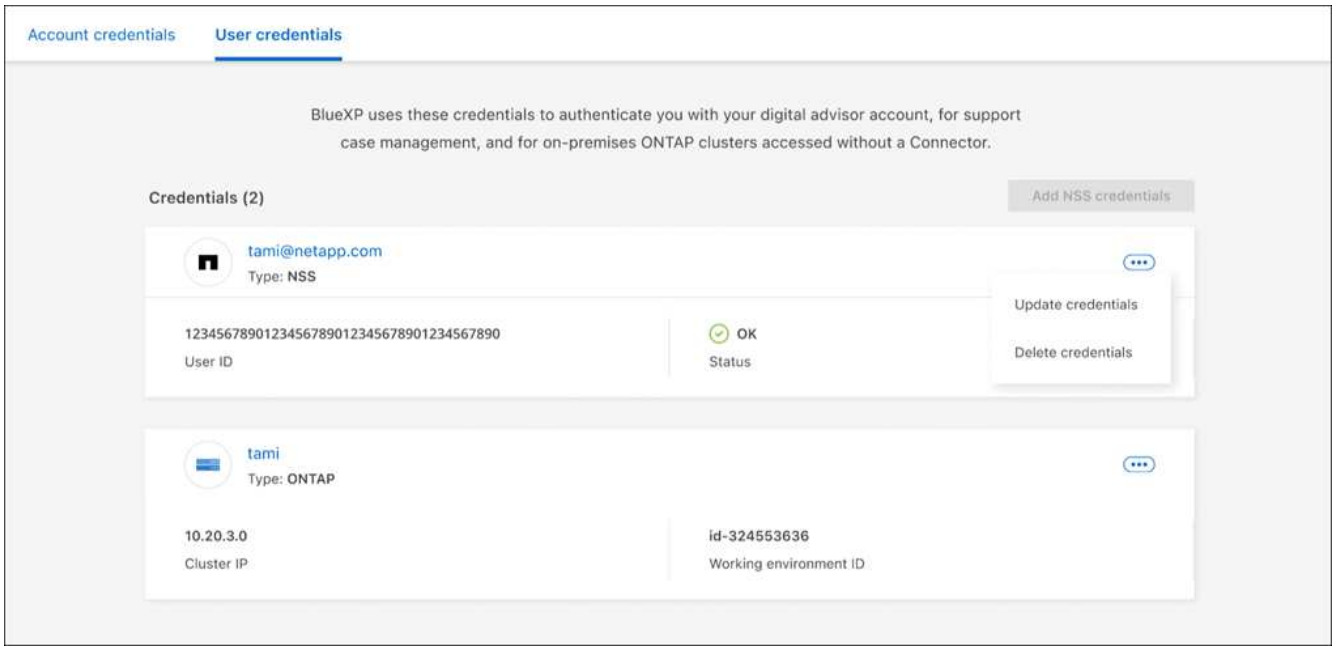
  "BlueXPアカウントでNSSクレデンシャルを使用する方法の詳細については、こちらをご覧ください"。

ユーザクレデンシャルを管理します

ユーザ名とパスワードを更新するか、クレデンシャルを削除して、ユーザクレデンシャルを管理します。

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. [ユーザクレデンシャル]*を選択します。
3. まだユーザクレデンシャルがない場合は、*[NSSクレデンシャルの追加]*を選択してNetApp Support Siteアカウントを追加できます。
4. 次のオプションを選択して既存のクレデンシャルを管理します。
   - 資格情報の更新：アカウントのユーザー名とパスワードを更新します。
   - クレデンシャルを削除：BlueXPユーザアカウントに関連付けられているアカウントを削除します。



と[Delete credentials]を選択する機能を示すスクリーンショット"]

結果

クレデンシャルが更新されます。変更は、ONTAP クラスタ、デジタルアドバイザ、または[ケース管理]ページにアクセスすると反映されます。

参照

権限

BlueXPの権限の概要

BlueXPの機能やサービスを使用するには、権限を指定してBlueXPがクラウド環境で処理を実行できるようにする必要があります。このページのリンクを使用して、目的に応じて必要な権限にすばやくアクセスできます。

AWS権限

BlueXPでは、コネクタと個 々 のサービスにAWS権限が必要です。

コネクタ

目標	説明	リンク
BlueXPからコネクタを導入	BlueXPからConnectorを作成するユーザには、AWSにインスタンスを導入するための特別な権限が必要です。	"AWS権限を設定"
コネクタの権限を指定します	BlueXPがConnectorを起動すると、AWSアカウントのリソースとプロセスの管理に必要な権限を提供するポリシーがインスタンスに関連付けられます。 AWS Marketplaceからコネクタを起動した場合、コネクタを手動でインストールした場合、または "AWSクレデンシャルをコネクタに追加します"。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"Connector の AWS 権限"

バックアップとリカバリ

目標	説明	リンク
オンプレミスのONTAPクラスタをAmazon S3にバックアップ	ONTAPボリュームでバックアップをアクティブ化すると、特定の権限を持つIAMユーザのアクセスキーとシークレットを入力するように求められます。	"バックアップのS3権限を設定"

Cloud Volumes ONTAP

目標	説明	リンク
Cloud Volumes ONTAPノードの権限を付与する	AWSの各Cloud Volumes ONTAP ノードにIAMロールを関連付ける必要があります。HAメディエーターについても同様です。デフォルトではBlueXPにIAMロールが作成されますが、作業環境の作成時に独自のロールを使用することもできます。	"IAMロールを自分で設定する方法について説明します"

コピーと同期

目標	説明	リンク
データブローカーをAWSに導入	データブローカーの導入に使用するAWSユーザアカウントには、特定の権限が必要です。	"AWS にデータブローカーを展開するために必要な権限"
データブローカーの権限を指定	BlueXPのコピーと同期でデータブローカーを導入すると、データブローカーインスタンス用のIAMロールが作成されます。必要に応じて、独自の IAM ロールを使用してデータブローカーを展開できます。	"AWS データブローカーで独自の IAM ロールを使用するための要件"
手動でインストールしたデータブローカーに対してAWSへのアクセスを有効にする	データブローカーをS3バケットを含む同期関係で使用する場合は、AWSにアクセスできるLinuxホストを準備する必要があります。データブローカーをインストールするときは、プログラムによるアクセスと特定の権限を持つIAMユーザにAWSキーを指定する必要があります。	"AWS へのアクセスを有効化"

FSX for ONTAP の略

目標	説明	リンク
FSx for ONTAPの作成と管理	Amazon FSx for NetApp ONTAP作業環境を作成または管理するには、作業環境の作成に必要な権限をBlueXPに付与するIAMロールのARNを指定して、AWSクレデンシャルをBlueXPに追加する必要があります。	"FSx用のAWSクレデンシャルの設定方法をご確認ください"

階層化

目標	説明	リンク
オンプレミスのONTAPクラスタをAmazon S3に階層化	AWSへのBlueXPの階層化を有効にすると、アクセスキーとシークレットキーを入力するように求められます。これらのクレデンシャルは、ONTAP がS3バケットにデータを階層化できるようにONTAP クラスタに渡されます。	"階層化のためのS3権限を設定する"

Azure権限

BlueXPでは、コネクタと個 々 のサービスにAzure権限が必要です。

コネクタ

目標	説明	リンク
BlueXPからコネクタを導入	BlueXPからConnectorを導入する場合は、AzureにConnector VMを導入する権限を持つAzureアカウントまたはサービスプリンシパルを使用する必要があります。	"Azure権限を設定する"

目標	説明	リンク
コネクタの権限を指定します	BlueXPがConnector VMをAzureに導入すると、そのAzureサブスクリプション内でリソースとプロセスを管理するために必要な権限を提供するカスタムロールが作成されます。 Marketplaceからコネクタを起動する場合、コネクタを手動でインストールする場合、またはカスタムロールを自分で設定する必要があります。 "Azureクレデンシャルをコネクタに追加します"。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"Connector の Azure 権限"

コピーと同期

目標	説明	リンク
Azureにデータブローカーを導入	データブローカーの導入に使用するAzureユーザアカウントに、必要な権限が付与されている必要があります。	"Azureにデータブローカーを導入するための権限が必要です"

Google Cloud権限

BlueXPでは、コネクタと個 々 のサービスにGoogle Cloudの権限が必要です。

コネクタ

目標	説明	リンク
BlueXPからコネクタを導入	BlueXPからConnectorを導入するGoogle Cloudユーザーには、Google CloudにConnectorを導入するための特定の権限が必要です。	"コネクタを作成するための権限を設定する"
コネクタの権限を指定します	Connector VMインスタンスのサービスアカウントには、日常処理に対する特定の権限が必要です。導入時にサービスアカウントをコネクタに関連付ける必要があります。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"コネクタの権限を設定します"

バックアップとリカバリ

目標	説明	リンク
Cloud Volumes ONTAP を Google Cloud にバックアップ	BlueXPのバックアップとリカバリを使用してCloud Volumes ONTAPをバックアップする場合は、次のシナリオでコネクタに権限を追加する必要があります。 • 「検索と復元」機能を使用する場合 • 顧客管理の暗号化キー（CMEK）を使用する場合	• "検索と復元機能の権限" • "CMEKの権限"
オンプレミスのONTAPクラスタをGoogle Cloudにバックアップ	BlueXPのバックアップとリカバリを使用してオンプレミスのONTAPクラスタをバックアップする場合は、「検索とリストア」機能を使用するためにコネクタに権限を追加する必要があります。	"検索と復元機能の権限"

Cloud Volumes Service for Google Cloud

目標	説明	リンク
Cloud Volumes Service for Google Cloudの詳細	BlueXPでは、Google Cloudサービスアカウントを使用してCloud Volumes Service APIにアクセスし、適切な権限を付与する必要があります。	"サービスアカウントを設定します"

コピーと同期

目標	説明	リンク
Google Cloudにデータブローカーを導入	データブローカーを導入するGoogle Cloudユーザに必要な権限が割り当てられていることを確認します。	"Google Cloud にデータブローカーを導入するための権限が必要です"
手動でインストールしたデータブローカーに対してGoogle Cloudへのアクセスを有効にする	Google Cloud Storage バケットを含む同期関係でデータブローカーを使用する場合は、 Google Cloud アクセス用の Linux ホストを準備しておく必要があります。データブローカーをインストールする場合、特定の権限を持つサービスアカウントにキーを提供する必要があります。	"Google Cloud へのアクセスを有効にします"

StorageGRIDケンケン

BlueXPでは、2つのサービスに対してStorageGRID権限が必要です。

バックアップとリカバリ

目標	説明	リンク
オンプレミスのONTAPクラスタをStorageGRIDにバックアップ	StorageGRIDをONTAPクラスタのバックアップターゲットとして準備する際、特定の権限を持つIAMユーザのアクセスキーとシークレットを入力するように求められます。	"バックアップターゲットとしてStorageGRIDを準備します"

階層化

目標	説明	リンク
オンプレミスのONTAPクラスタをStorageGRIDに階層化	StorageGRIDへのBlueXPの階層化をセットアップするときは、S3のアクセスキーとシークレットキーを使用してBlueXPの階層化を提供する必要があります。BlueXPの階層化サービスでは、このキーを使用してバケットにアクセスします。	"StorageGRIDへの階層化を準備"

Connector の AWS 権限

BlueXPがAWSでConnectorインスタンスを起動すると、そのAWSアカウント内のリソースとプロセスを管理するための権限をConnectorに提供するポリシーがインスタンスにアタッチされます。Connectorでは、権限を使用してAPI呼び出しを実行することで、EC2、S3、CloudFormation、IAM、 Key Management Service（KMS；キー管理サービス）など。

IAMポリシー

以下のIAMポリシーは、ConnectorがAWSリージョンに基づいてパブリッククラウド環境内のリソースとプロセスを管理するために必要な権限を提供します。

次の点に注意してください。

- BlueXPから直接、標準のAWSリージョンでコネクタを作成すると、BlueXPによって自動的にそのコネクタにポリシーが適用されます。この場合、何も行う必要はありません。
- AWS Marketplaceからコネクタを導入する場合、Linuxホストにコネクタを手動でインストールする場合、またはBlueXPにAWSクレデンシャルを追加する場合は、ポリシーを自分で設定する必要があります。
- また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。
- 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"
- これらのポリシーの使用手順については、次のページを参照してください。
  - "AWS Marketplace環境の権限を設定する"
  - "オンプレミス環境の権限を設定する"
  - "制限モードの権限を設定します"
  - "プライベートモードの権限を設定します"

必要なポリシーを表示する地域を選択します。

標準領域

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。

1つ目のポリシーでは、次のサービスに対する権限を付与します。

- Amazon S3 バケットの検出
- バックアップとリカバリ
- 分類
- Cloud Volumes ONTAP
- FSX for ONTAP の略
- 階層化

2つ目のポリシーは、次のサービスに対する権限を提供します。

- エッジキャッシュ
- Kubernetes

ポリシー1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
```

```
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
```

```
                "s3:GetObject",
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
```

```
                "glue:BatchDeletePartition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::netapp-backup-*"
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
```

```
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
```

```
    ]
}
```

ポリシー#2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

GovCloud（US）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "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:CreateSnapshot",
```

```
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
```

```
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
```

```
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

シークレットリージョン

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Top Secret領域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

AWS権限の使用方法

以降のセクションでは、各BlueXPサービスでの権限の使用方法について説明します。この情報は、企業のポリシーによって、必要な場合にのみアクセス許可が指定されるように指定されている場合に役立ちます。

ONTAP 対応の Amazon FSX

コネクタは、Amazon FSx for ONTAP を管理するための次のAPI要求を行います。

- EC2: DescribeInstances
- EC2: DescribeInstanceStatus
- EC2: DescribeInstanceAttributeのこと
- EC2: DescribeRouteTables
- EC2: DescribeImages
- ec2：CreateTags
- EC2: DescribeVolumesの場合
- EC2: DescribeSecurityGroups
- EC2: DescribeNetworkInterfaces

- EC2: DescribeSubnets
- EC2: DescribeVpcs
- EC2: DescribeDhcpOptions
- ec2: DescribeSnapshots
- EC2：DescribeKeyPairs
- EC2: DescribeRegions (説明領域
- EC2: DescribeTags (説明タグ)
- EC2: DescribeIamInstanceProfileAssociations
- EC2: DescribeReservedInstancesOfferings
- EC2: DescribeVpcEndpoints
- EC2: DescribeVpcs
- EC2: DescribeVolumesModifications (EC2 : DescribeVolumesMod
- EC2: DescribePlacementGroups
- KMS：リスト*
- KMS：説明*
- KMS：CreateGrant
- KMS：エイリアスを確認する
- FSx：説明*
- FSx：リスト*

Amazon S3 バケットの検出

コネクタは、Amazon S3バケットを検出するために次のAPI要求を実行します。

S3 ： GetEncryptionConfiguration

バックアップとリカバリ

Connectorは、Amazon S3でバックアップを管理するために次のAPI要求を実行します。

- S3 ： GetBucketLocation
- S3 ： ListAllMyBuckets
- S3 ： ListBucket
- S3 ： CreateBucket を指定します
- S3 ： GetLifecycleConfiguration
- S3 ： PutLifecycleConfiguration
- S3 ： PutBucketTagging
- S3 ： ListBucketVersions
- S3 ： GetBucketAcl

- S3：PutBucketPublicAccessBlock
- KMS：リスト*
- KMS：説明*
- S3 ： GetObject
- EC2: DescribeVpcEndpoints
- KMS：エイリアスを確認する
- S3 ： PutEncryptionConfiguration

コネクタは、Search & Restoreメソッドを使用してボリュームとファイルをリストアする場合に次のAPI要求を実行します。

- S3 ： CreateBucket を指定します
- S3 ： DeleteObject
- S3 ： DeleteObjectVersion
- S3 ： GetBucketAcl
- S3 ： ListBucket
- S3 ： ListBucketVersions
- S3 ： ListBucketMultipartUploads
- S3 ： PutObject
- S3：PutBucketAcl
- S3 ： PutLifecycleConfiguration
- S3：PutBucketPublicAccessBlock
- S3 ： AbortMultipartUpload
- S3 ： ListMultipartUploadParts
- Athena：StartQueryExecution
- Athena: GetQueryResults.
- Athena: GetQueryExecution
- Athena：StopQueryExecution
- グルー：データベースを作成します
- グルー: CreateTable
- グルー: BatchDeletePartition

このコネクタは、データロックとランサムウェア保護を使用してボリュームのバックアップを行う際に次のAPI要求を実行します。

- S3 ： GetObjectVersionTagging
- S3 ： GetBucketObjectLockConfiguration
- S3：GetObjectVersionAcl

- S3 ： PutObjectTagging
- S3 ： DeleteObject
- S3 ： DeleteObjectTagging
- S3 ： GetObjectRetention
- S3 ： DeleteObjectVersionTagging
- S3 ： PutObject
- S3 ： GetObject
- S3 ： PutBucketObjectLockConfiguration
- S3 ： GetLifecycleConfiguration
- S3：ListBucketByTags
- S3 ： GetBucketTagging
- S3 ： DeleteObjectVersion
- S3 ： ListBucketVersions
- S3 ： ListBucket
- S3 ： PutBucketTagging
- S3 ： GetObjectTagging
- S3 ： PutBucketVersioning
- S3 ： PutObjectVersionTagging
- S3 ： GetBucketVersioning
- S3 ： GetBucketAcl
- S3：Bypassガバナー 保持
- S3 ： PutObjectRetention
- S3 ： GetBucketLocation
- S3 ： GetObjectVersion

Cloud Volumes ONTAP バックアップにソースボリュームとは異なるAWSアカウントを使用する場合、Connectorは次のAPI要求を実行します。

- S3 ： PutBucketPolicy
- S3：PutBucketOwnershipControls

分類

コネクタは、BlueXP分類インスタンスを導入するために次のAPI要求を行います。

- EC2: DescribeInstances
- EC2: DescribeInstanceStatus
- EC2：RunInstances

- EC2：TerminateInstances
- ec2：CreateTags
- EC2：CreateVolume
- EC2：AttachVolume
- EC2：CreateSecurityGroup
- EC2: DeleteSecurityGroup
- EC2: DescribeSecurityGroups
- EC2：CreateNetworkInterface
- EC2: DescribeNetworkInterfaces
- EC2：DeleteNetworkInterface
- EC2: DescribeSubnets
- EC2: DescribeVpcs
- EC2: CreateSnapshotの作成
- EC2: DescribeRegions (説明領域
- CloudFormation：CreateStack
- CloudFormation：DeleteStack
- CloudFormation：DescribeStack
- CloudFormation：DescribeStackEvents
- IAM：AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: DescribeIamInstanceProfileAssociations

BlueXP分類を使用する場合、コネクタはS3バケットをスキャンするために次のAPI要求を行います。

- IAM：AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: DescribeIamInstanceProfileAssociations
- S3 ： GetBucketTagging
- S3 ： GetBucketLocation
- S3 ： ListAllMyBuckets
- S3 ： ListBucket
- S3：GetBucketPolicyStatus
- S3 ： GetBucketPolicy
- S3 ： GetBucketAcl
- S3 ： GetObject
- IAM：GetRole

- S3 ： DeleteObject
- S3 ： DeleteObjectVersion
- S3 ： PutObject
- STS: AssumeRole

Cloud Volumes ONTAP

Connectorは、AWSでのCloud Volumes ONTAP の導入と管理に対して次のAPI要求を実行します。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP インスタンスのIAMロールとインスタンスプロファイルを作成および管理します	IAM ：ListInstanceProfiles	はい。	はい。	いいえ
	IAM ：CREATEROLE	はい。	いいえ	いいえ
	IAM：DeleteRole	いいえ	はい。	はい。
	IAM：PutRolePolicy	はい。	いいえ	いいえ
	IAM ：CreateInstanceProfile	はい。	いいえ	いいえ
	IAM ：DeleteRolePolicy	いいえ	はい。	はい。
	IAM ：AddRoleToInstanceProfile	はい。	いいえ	いいえ
	IAM ：RemoveRoleFromInstanceProfile	いいえ	はい。	はい。
	IAM ：DeleteInstanceProfile	いいえ	はい。	はい。
	IAM：PassRole	はい。	いいえ	いいえ
	EC2: AssociateIamInstanceProfile	はい。	はい。	いいえ
	EC2: DescribeIamInstanceProfileAssociations	はい。	はい。	いいえ
	EC2: DisassociateIamInstanceProfile	いいえ	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
読み取り許可ステータスメッセージ	STS: DecodeAuthorizationMessage	はい。	はい。	いいえ
アカウントで使用可能な指定イメージ（AMIS）について説明します	EC2: DescribeImages	はい。	はい。	いいえ
VPC内のルーティングテーブルの説明（HAペアの場合のみ必要）	EC2: DescribeRouteTables	はい。	いいえ	いいえ
インスタンスの停止、開始、監視	EC2：StartInstances（EC2：開始インスタンス	はい。	はい。	いいえ
	EC2：StopInstances	はい。	はい。	いいえ
	EC2: DescribeInstances	はい。	はい。	いいえ
	EC2: DescribeInstanceStatus	はい。	はい。	いいえ
	EC2：RunInstances	はい。	いいえ	いいえ
	EC2：TerminateInstances	いいえ	いいえ	はい。
	EC2：ModifyInstanceAttribute	いいえ	はい。	いいえ
サポートされるインスタンスタイプに対して拡張ネットワークが有効になっていることを確認します	EC2: DescribeInstanceAttributeのこと	いいえ	はい。	いいえ
メンテナンスとコストの割り当てに使用する「WorkingEnvironment」タグと「WorkingEnvironmentId」タグを使用してリソースにタグを付けます	ec2：CreateTags	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP がバックエンドストレージとして使用するEBSボリュームを管理します	EC2：CreateVolume	はい。	はい。	いいえ
	EC2: DescribeVolumesの場合	はい。	はい。	はい。
	EC2 ：ModifyVolumeAttributeのことです	いいえ	はい。	はい。
	EC2：AttachVolume	はい。	はい。	いいえ
	EC2：DeleteVolume	いいえ	はい。	はい。
	EC2 ：DetachVolumeの場合	いいえ	はい。	はい。
Cloud Volumes ONTAP のセキュリティグループを作成および管理します	EC2 ：CreateSecurityGroup	はい。	いいえ	いいえ
	EC2: DeleteSecurityGroup	いいえ	はい。	はい。
	EC2: DescribeSecurityGroups	はい。	はい。	はい。
	EC2: RevokeSecurityGroupEgress	はい。	いいえ	いいえ
	ec2 ：AuthorizeSecurityGroupEgress	はい。	いいえ	いいえ
	ec2 ：AuthorizeSecurityGroupIngress	はい。	いいえ	いいえ
	EC2: RevokeSecurityGroupIngress	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
ターゲットサブネットのCloud Volumes ONTAP のネットワークインターフェイスを作成および管理します	EC2：CreateNetworkInterface	はい。	いいえ	いいえ
	EC2: DescribeNetworkInterfaces	はい。	はい。	いいえ
	EC2：DeleteNetworkInterface	いいえ	はい。	はい。
	EC2:ModifyNetworkInterfaceAttributeのいずれかです	いいえ	はい。	いいえ
デスティネーションのサブネットとセキュリティグループの一覧を取得します	EC2: DescribeSubnets	はい。	はい。	いいえ
	EC2: DescribeVpcs	はい。	はい。	いいえ
Cloud Volumes ONTAP インスタンスのDNSサーバおよびデフォルトのドメイン名を取得します	EC2: DescribeDhcpOptions	はい。	いいえ	いいえ
Cloud Volumes ONTAP 用のEBSボリュームのSnapshotを作成します	EC2: CreateSnapshotの作成	はい。	はい。	いいえ
	EC2：DeleteSnapshot	いいえ	はい。	はい。
	ec2: DescribeSnapshots	いいえ	はい。	いいえ
AutoSupport メッセージに添付されているCloud Volumes ONTAP コンソールをキャプチャします	EC2: GetConsoleOutput	はい。	はい。	いいえ
使用可能なキーペアのリストを取得します	EC2：DescribeKeyPairs	はい。	いいえ	いいえ
使用可能なAWSリージョンのリストを取得します	EC2: DescribeRegions (説明領域	はい。	はい。	いいえ
Cloud Volumes ONTAP インスタンスに関連付けられたリソースのタグを管理します	EC2:タグを削除します	いいえ	はい。	はい。
	EC2: DescribeTags (説明タグ)	いいえ	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
AWS CloudFormationテンプレートのスタックの作成と管理	CloudFormation：CreateStack	はい。	いいえ	いいえ
	CloudFormation：DeleteStack	はい。	いいえ	いいえ
	CloudFormation：DescribeStack	はい。	はい。	いいえ
	CloudFormation：DescribeStackEvents	はい。	いいえ	いいえ
	CloudFormation：ValidateTemplate	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP システムでデータ階層として使用するS3バケットを作成および管理します	S3 ： CreateBucket を指定します	はい。	はい。	いいえ
	S3 ： DeleteBucket	いいえ	はい。	はい。
	S3 ： GetLifecycleConfiguration	いいえ	はい。	いいえ
	S3 ： PutLifecycleConfiguration	いいえ	はい。	いいえ
	S3 ： PutBucketTagging	いいえ	はい。	いいえ
	S3 ： ListBucketVersions	いいえ	はい。	いいえ
	S3 ：GetBucketPolicyStatus	いいえ	はい。	いいえ
	S3 ：GetBucketPublicAccessBlock	いいえ	はい。	いいえ
	S3 ： GetBucketAcl	いいえ	はい。	いいえ
	S3 ： GetBucketPolicy	いいえ	はい。	いいえ
	S3 ：PutBucketPublicAccessBlock	いいえ	はい。	いいえ
	S3 ： GetBucketTagging	いいえ	はい。	いいえ
	S3 ： GetBucketLocation	いいえ	はい。	いいえ
	S3 ： ListAllMyBuckets	いいえ	いいえ	いいえ
	S3 ： ListBucket	いいえ	はい。	いいえ
AWS Key Management Service（KMS；キー管理サービス）を使用してCloud Volumes ONTAP のデータ暗号化を有効にする	KMS：リスト*	はい。	はい。	いいえ
	KMS：再暗号化*	はい。	いいえ	いいえ
	KMS：説明*	はい。	はい。	いいえ
	KMS：CreateGrant	はい。	はい。	いいえ
	KMS ：GenerateDataKeyWithoutPlaintext	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
2つのHAノードとメディエーター用のAWS分散配置グループを1つのAWSアベイラビリティゾーンに作成して管理します	EC2：CreatePlacementGroup	はい。	いいえ	いいえ
	EC2: DeletePlacementGroup	いいえ	はい。	はい。
レポートを作成します	FSx：説明*	いいえ	はい。	いいえ
	FSx：リスト*	いいえ	はい。	いいえ
Amazon EBS Elastic Volumes機能をサポートするアグリゲートを作成して管理します	EC2: DescribeVolumesModifications (EC2 : DescribeVolumesMod	いいえ	はい。	いいえ
	EC2：ModifyVolume	いいえ	はい。	いいえ

エッジキャッシュ

コネクタは、導入時にBlueXPエッジキャッシュインスタンスを導入するために次のAPI要求を行います。

- CloudFormation：DescribeStack
- CloudWatch：GetMetricStatistics
- CloudFormation：リストスタック

Kubernetes

コネクタは、次のAPI要求を実行してAmazon EKSクラスタを検出および管理します。

- EC2: DescribeRegions (説明領域
- EKS：リストクラスタ
- EKS：DescribeCluster
- IAM：GetInstanceProfile

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2024年3月8日

次の権限がコネクタポリシーに含まれるようになりました。

EC2：説明AvailabilityZones

この権限は、今後のリリースで必要になります。リリースノートの詳細については、リリースノートを更新し

ます。

2023年6月6日

Cloud Volumes ONTAPには次の権限が必要です。

KMS：GenerateDataKeyWithoutPlaintext

2023年2月14日

BlueXPの階層化には次の権限が必要です。

EC2: DescribeVpcEndpoints

Connector の Azure 権限

BlueXPがAzureでConnector VMを起動すると、そのAzureサブスクリプション内のリソースとプロセスを管理するための権限をConnectorに提供するカスタムロールがVMに割り当てられます。Connectorは、権限を使用して複数のAzureサービスに対してAPI呼び出しを実行します。

カスタムロールの権限

以下のカスタムロールには、Azureネットワーク内のリソースとプロセスを管理するためにConnectorで必要となる権限が含まれています。

BlueXPからコネクタを直接作成すると、BlueXPは自動的にこのカスタムロールをコネクタに適用します。

Azure MarketplaceからConnectorを導入する場合、またはLinuxホストにConnectorを手動でインストールする場合は、カスタムロールを自分で設定する必要があります。

これらのポリシーの使用手順については、次のページを参照してください。

- "Azure Marketplace環境の権限を設定する"
- "オンプレミス環境の権限を設定する"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

また、新しい権限が以降のリリースで追加されるときに、ロールが最新の状態であることを確認する必要があります。

```
{
    "Name": "BlueXP Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
```

```
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "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.Storage/checknameavailability/read",
```

```
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
```

```
"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

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

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential/acti
on",
                    "Microsoft.ContainerService/managedClusters/read",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Azure権限の使用方法

以降のセクションでは、各BlueXPサービスでの権限の使用方法について説明します。この情報は、企業のポリシーによって、必要な場合にのみアクセス許可が指定されるように指定されている場合に役立ちます。

Azure NetApp Files の特長

BlueXP分類を使用してAzure NetApp Filesデータをスキャンする場合、コネクタは次のAPI要求を行います。

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

バックアップとリカバリ

コネクタは、BlueXPのバックアップとリカバリ用に次のAPI要求を行います。

- microsoft.Storage/storageAccounts/listkeys/action
- microsoft.Storage/storageAccounts/read
- microsoft.Storage/storageAccounts/write
- microsoft.Storage/storageAccounts/blobServices/container/read
- microsoft.Storage/storageAccountSas/action
- microsoft.KeyVault/vaults/read
- Microsoft。KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- microsoft.Resources/Subscriptions /locations /read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- microsoft.Resources/Subscriptions /resourceGroups/read
- microsoft.resources/Subscriptions /resourcegroups/resources/read
- microsoft.Resources/Subscriptions /resourceGroups/write
- Microsoft 。許可/ロック/
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- microsoft.Resources/Deployments/delete
- microsoft.ManagedIdentity/userAssignedIdentities/assign/action

検索とリストア機能を使用すると、コネクタは次のAPI要求を実行します。

- Microsoft .Synapse/workspaces /書き込み
- Microsoft . Synapse/workspaces / read
- Microsoft .Synapse/workspaces /削除
- Microsoft .Synapse/register/action
- microsoft.Synapse/checkNameAvailability/action
- Microsoft .Synapse/workspaces /operationStatuses /read
- Microsoft . Synapse/workspaces / firewallRules/read
- Microsoft .Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft .Synapse/workspaces /操作結果/読み取り

- Microsoft .Synapse/workspaces /privateEndpointConnectionsApproval / action

分類

BlueXP分類を使用する場合、コネクタは次のAPI要求を行います。

アクション	セットアップに使用？	日々の業務に使用されるか？
Microsoft.Compute/locations/operations/read	はい。	はい。
Microsoft.Compute/locations/vmSizes/read	はい。	はい。
Microsoft.Compute/operations/read	はい。	はい。
Microsoft.Compute/virtualMachines/instanceView/read	はい。	はい。
Microsoft.Compute/virtualMachines/powerOff/action	はい。	いいえ
Microsoft.Compute/virtualMachines/read	はい。	はい。
Microsoft.Compute/virtualMachines/restart/action	はい。	いいえ
Microsoft.Compute/virtualMachines/start/action	はい。	いいえ
Microsoft.Compute/virtualMachines/vmSizes/read	いいえ	はい。
Microsoft.Compute/virtualMachines/write	はい。	いいえ
Microsoft.Compute/images/read	はい。	はい。
Microsoft.Compute/disks/delete	はい。	いいえ
Microsoft.Compute/disks/read	はい。	はい。
Microsoft.Compute/disks/write	はい。	いいえ
Microsoft.Storage/checknameavailability/read	はい。	はい。
Microsoft。ストレージ/運用/読み取り	はい。	はい。
microsoft.Storage/storageAccounts/listkeys/action	はい。	いいえ
microsoft.Storage/storageAccounts/read	はい。	はい。
microsoft.Storage/storageAccounts/write	はい。	いいえ
microsoft.Storage/storageAccounts/blobServices/container/read	はい。	はい。

アクション	セットアップに使用？	日々の業務に使用されるか？
Microsoft.Network/networkInterfaces/read	はい。	はい。
Microsoft.Network/networkInterfaces/write	はい。	いいえ
Microsoft.Network/networkInterfaces/join/action	はい。	いいえ
Microsoft.Network/networkSecurityGroups/read	はい。	はい。
Microsoft.Network/networkSecurityGroups/write	はい。	いいえ
microsoft.Resources/Subscriptions/locations /read	はい。	はい。
Microsoft.Network/locations/operationResults/read	はい。	はい。
Microsoft.Network/locations/operations/read	はい。	はい。
Microsoft.Network/virtualNetworks/read	はい。	はい。
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	はい。	はい。
Microsoft.Network/virtualNetworks/subnets/read	はい。	はい。
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	はい。	はい。
Microsoft.Network/virtualNetworks/virtualMachines/read	はい。	はい。
Microsoft.Network/virtualNetworks/subnets/join/action	はい。	いいえ
Microsoft.Network/virtualNetworks/subnets/write	はい。	いいえ
Microsoft.Network/routeTables/join/action	はい。	いいえ
microsoft.Resources/Deployments/operations/read	はい。	はい。
Microsoft .Resources/Deployments/read	はい。	はい。
Microsoft .Resources/Deployments/write	はい。	いいえ
microsoft.resources/resources/read	はい。	はい。

アクション	セットアップに使用？	日々の業務に使用されるか？
microsoft.Resources/Subscriptions/operationresults/read	はい。	はい。
microsoft.Resources/Subscriptions/resourceGroups/delete	はい。	いいえ
microsoft.Resources/Subscriptions/resourceGroups/read	はい。	はい。
microsoft.resources/Subscriptions/resourcegroups/resources/read	はい。	はい。
microsoft.Resources/Subscriptions/resourceGroups/write	はい。	いいえ

Cloud Volumes ONTAP

Connectorは、AzureでCloud Volumes ONTAP の導入と管理を行うために次のAPI要求を実行します。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
VMの作成と管理	Microsoft.Compute/locations/operations/read	はい。	はい。	いいえ
	Microsoft.Compute/locations/vmSizes/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/locations /read	はい。	いいえ	いいえ
	Microsoft.Compute/operations/read	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/instanceView/read	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/powerOff/action	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/read	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/restart/action	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/start/action	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/deallocate/action	いいえ	はい。	はい。
	Microsoft.Compute/virtualMachines/vmSizes/read	いいえ	はい。	いいえ
	Microsoft.Compute/virtualMachines/write	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/delete	はい。	はい。	はい。
	microsoft.Resources/Deployments/delete	はい。	いいえ	いいえ
VHDからの導入を有効にします	Microsoft.Compute/images/read	はい。	いいえ	いいえ
	Microsoft.Compute/images/write	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
ターゲットサブネットのネットワークインターフェイスを作成および管理します	Microsoft.Network/networkInterfaces/read	はい。	はい。	いいえ
	Microsoft.Network/networkInterfaces/write	はい。	はい。	いいえ
	Microsoft.Network/networkInterfaces/join/action	はい。	はい。	いいえ
	Microsoft.Network/networkInterfaces/delete	はい。	はい。	いいえ
ネットワークセキュリティグループを作成および管理します	Microsoft.Network/networkSecurityGroups/read	はい。	はい。	いいえ
	Microsoft.Network/networkSecurityGroups/write	はい。	はい。	いいえ
	Microsoft.Network/networkSecurityGroups/join/action	はい。	いいえ	いいえ
	Microsoft.Network/networkSecurityGroups/delete	いいえ	はい。	はい。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
リージョンおよびターゲットのVNetとサブネットのネットワーク情報を取得し、VMをVNetに追加します	Microsoft.Network/locations/operationResults/read	はい。	はい。	いいえ
	Microsoft.Network/locations/operations/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/read	はい。	いいえ	いいえ
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	はい。	いいえ	いいえ
	Microsoft.Network/virtualNetworks/subnets/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/virtualMachines/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/subnets/join/action	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
リソースグループを作成および管理する	microsoft.Resources/Deployments/operations/read	はい。	はい。	いいえ
	Microsoft.Resources/Deployments/read	はい。	はい。	いいえ
	Microsoft.Resources/Deployments/write	はい。	はい。	いいえ
	microsoft.resources/resources/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/operationresults/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/resourceGroups/delete	はい。	はい。	はい。
	microsoft.Resources/Subscriptions/resourceGroups/read	いいえ	はい。	いいえ
	microsoft.resources/Subscriptions/resourcegroups/resources/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/resourceGroups/write	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Azureストレージアカウントおよびディスクを管理する	Microsoft.Compute/disks/read	はい。	はい。	はい。
	Microsoft.Compute/disks/write	はい。	はい。	いいえ
	Microsoft.Compute/disks/delete	はい。	はい。	はい。
	Microsoft.Storage/checknameavailability/read	はい。	はい。	いいえ
	Microsoft。ストレージ/運用/読み取り	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/listkeys/action	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/read	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/delete	いいえ	はい。	はい。
	microsoft.Storage/storageAccounts/write	はい。	はい。	いいえ
	Microsoft.Storage/uses/read：ストレージ/使用状況/読み取り	いいえ	はい。	いいえ
ストレージアカウントのBLOBストレージへのバックアップと暗号化を有効にします	microsoft.Storage/storageAccounts/blobServices/container/read	はい。	はい。	いいえ
	microsoft.KeyVault/vaults/read	はい。	はい。	いいえ
	Microsoft。KeyVault/vaults/accessPolicies/write	はい。	はい。	いいえ
データ階層化のためのVNetサービスエンドポイントを有効にします	Microsoft.Network/virtualNetworks/subnets/write	はい。	はい。	いいえ
	Microsoft.Network/routeTables/join/action	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Azureで管理されるSnapshotを作成および管理します	Microsoft.Compute/snapshots/write	はい。	はい。	いいえ
	Microsoft.Compute/snapshots/read	はい。	はい。	いいえ
	Microsoft.Compute/snapshots/delete	いいえ	はい。	はい。
	Microsoft.Compute/disks/beginGetAccess/action	いいえ	はい。	いいえ
アベイラビリティセットを作成および管理します	Microsoft.Compute/availabilitySets/write	はい。	いいえ	いいえ
	Microsoft.Compute/availabilitySets/read	はい。	いいえ	いいえ
市場からのプログラムによる導入を可能にします	"Microsoft.MarketplaceOrdering/offerTypes/publisher/offers/plans/agrees/read	はい。	いいえ	いいえ
	"Microsoft.MarketplaceOrdering/offerTypes/publisher/offers/plans/agrees/write	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
HAペアのロードバランサを管理します	Microsoft.Network/loadBalancers/read	はい。	はい。	いいえ
	Microsoft.Network/loadBalancers/write	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/delete	いいえ	はい。	はい。
	Microsoft.Network/loadBalancers/backendAddressPools/read	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	はい。	はい。	いいえ
	Microsoft.Network/loadBalancers/loadBalancingRules/read	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/probes/read	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/probes/join/action	はい。	いいえ	いいえ
Azureディスク上のロックの管理を有効にします	Microsoft 。許可/ロック/	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
サブネット外に接続がない場合は、HAペアのプライベートエンドポイントを有効にします	Microsoft.Network/privateEndpoints/write	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval / action	はい。	いいえ	いいえ
	microsoft.Storage/storageAccounts/privateEndpointConnections/ read	はい。	はい。	はい。
	Microsoft.Network/privateEndpoints/read	はい。	はい。	はい。
	Microsoft.Network/privateDnsZones/write	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/join/action	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/A/write	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/read	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	はい。	はい。	いいえ
基盤となる物理ハードウェアに応じて、一部のVM環境で必要です	microsoft.Resources/Deployments/operationStatuses /read	はい。	はい。	いいえ
導入に失敗した場合やリソースを削除した場合は、リソースグループからリソースを削除します	Microsoft.Network/privateEndpoints/delete	はい。	はい。	いいえ
	Microsoft.Compute/availabilitySets/delete	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
APIを使用する際に、お客様が管理する暗号化キーの使用を有効にします	Microsoft.Compute/diskEncryptionSets/read	はい。	はい。	はい。
	Microsoft.Compute/diskEncryptionSets/write	はい。	はい。	いいえ
	microsoft.KeyVault/vaults/deploy/action	はい。	いいえ	いいえ
	Microsoft.Compute/diskEncryptionSets/delete	はい。	はい。	はい。
HAペアのアプリケーションセキュリティグループを設定して、HAインターコネクトのNICとクラスタネットワークのNICを分離します	Microsoft.Network/applicationSecurityGroups/write	いいえ	はい。	いいえ
	Microsoft.Network/applicationSecurityGroups/read	いいえ	はい。	いいえ
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	いいえ	はい。	いいえ
	Microsoft.Network/networkSecurityGroups/securityRules/write	はい。	はい。	いいえ
	Microsoft.Network/applicationSecurityGroups/delete	いいえ	はい。	はい。
	Microsoft.Network/networkSecurityGroups/securityRules/delete	いいえ	はい。	はい。
Cloud Volumes ONTAP リソースに関連付けられたタグの読み取り、書き込み、および削除	microsoft.Resources/tags/read	いいえ	はい。	いいえ
	microsoft.Resources/tags/write	はい。	はい。	いいえ
	microsoft.Resources/tags/delete	はい。	いいえ	いいえ
作成時にストレージアカウントを暗号化	microsoft.ManagedIdentity/userAssignedIdentities/assign/action	はい。	はい。	いいえ

エッジキャッシュ

BlueXPエッジキャッシングを使用する場合、コネクタは次のAPI要求を行います。

- Microsoft .Insights / Metrics / Read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- microsoft.Resources/Deployments/delete

Kubernetes

Connectorは、Azure Kubernetes Service（AKS）で実行されているクラスタを検出し管理するために次のAPI要求を実行します。

- Microsoft.Compute/virtualMachines/read
- microsoft.Resources/Subscriptions /locations /read
- microsoft.Resources/Subscriptions /operationresults/read
- microsoft.Resources/Subscriptions /resourceGroups/read
- microsoft.resources/Subscriptions /resourcegroups/resources/read
- Microsoft .ContainerService/managedClusters/read
- Microsoft .ContainerService/managedClusters/listClusterUserCredential/action

階層化

BlueXP階層化のセットアップ時に、コネクタは次のAPI要求を行います。

- microsoft.Storage/storageAccounts/listkeys/action
- microsoft.Resources/Subscriptions /resourceGroups/read
- microsoft.Resources/Subscriptions /locations /read

このコネクタは、次のAPI要求を日々の処理に送信します。

- microsoft.Storage/storageAccounts/blobServices/container/read
- Microsoft。Storage/storageAccounts/managementPolicies/read
- microsoft.StorageAccounts/managementPolicies/write
- microsoft.Storage/storageAccounts/read

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2023年12月5日

Azure BLOBストレージにボリュームデータをバックアップする場合、BlueXPのバックアップとリカバリに次の権限は不要になりました。

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

これらの権限は他のBlueXPストレージサービスに必要なため、他のストレージサービスを使用している場合はコネクタのカスタムロールが引き続き使用されます。

2023年5月12日

次の権限はCloud Volumes ONTAP の管理に必要なため、JSONポリシーに追加されました。

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

JSONポリシーから次の権限が削除されました。これらの権限は不要になりました。

- microsoft.Storage/storageAccounts/blobServices/container/write
- Microsoft.Network/publicIPAddresses/delete

2023年3月23日

BlueXPの分類に「Microsoft.Storage/storageAccounts/delete」権限は不要になりました。

この権限はCloud Volumes ONTAP では引き続き必要です。

2023年1月5日

JSONポリシーに次の権限が追加されました。

- microsoft.Storage/storageAccountSas/action
- Microsoft .Synapse/workspaces /privateEndpointConnectionsApproval / action

  これらの権限はBlueXPのバックアップとリカバリに必要です。

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  この権限はCloud Volumes ONTAP の導入に必要です。

Connector の Google Cloud 権限

BlueXPには、Google Cloudでアクションを実行するための権限が必要です。これらの権限は、ネットアップが提供するカスタムロールに含まれています。これらの権限

でBlueXPが何を実行するのかを理解しておくとよいでしょう。

サービスアカウントの権限

次のカスタムロールは、ConnectorがGoogle Cloudネットワーク内のリソースとプロセスを管理するために必要な権限を提供します。

このカスタムロールは、Connector VMに関連付けられているサービスアカウントに適用する必要があります。

- "標準モードのGoogle Cloud権限を設定します"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

また、新しい権限が以降のリリースで追加されるときに、ロールが最新の状態であることを確認する必要があります。

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- 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.addAccessConfig
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- 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
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Google Cloud権限の使用方法

アクション	目的
- compute.disks.create - compute.disks.createsnapshot - compute.disks.delete -コンピューティング、ディスク、取得 - compute.disksリスト - compute.disks.setLabels - compute.disks.us	Cloud Volumes ONTAP 用のディスクを作成および管理します。
- compute.firewalls.create - compute.firewalls.delete -コンピューティング、ファイアウォール、取得 - compute.firewalls.list	Cloud Volumes ONTAP のファイアウォールルールを作成します。
-computer.globalOperationsGet	処理のステータスを確認できます。

アクション	目的
-計算画像取得 - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	VM インスタンスのイメージを取得します。
- compute.instances.attachDisk - compute.instances.detachDisk	ディスクを Cloud Volumes ONTAP に接続して接続解除します。
- compute.instances.create - compute.instances.delete	Cloud Volumes ONTAP VM インスタンスを作成および削除します。
- compute.instances.get	VM インスタンスを一覧表示します。
- compute.instances.getSerialPortOutput	をクリックしてコンソールログを取得してください
- compute.instances.list	ゾーン内のインスタンスのリストを取得します。
- compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。
- compute.instances.setLabels	ラベルを追加します。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Cloud Volumes ONTAP のマシンタイプを変更します。
- compute.instances.setMetadata	をクリックしてください。
- compute.instances.setTags	ファイアウォールルールのタグを追加します。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP を開始および停止します。
-computesCompute .machineTypes.get	コア数を取得して qoutas をチェックしてください。
- compute.projects.get	複数のプロジェクトをサポートするため。
- compute.snapshots.create - compute.snapshots.delete -コンピュートスナップショット取得 - compute.snapshots.list - compute.snapshots.setLabels	永続ディスクスナップショットを作成および管理するには、次の手順に従います。
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get -コンピュートゾーン取得 - compute.zones.list	新しい Cloud Volumes ONTAP 仮想マシンインスタンスの作成に必要なネットワーク情報を取得するため。

アクション	目的
- 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	Google Cloud Deployment Manager を使用して Cloud Volumes ONTAP 仮想マシンインスタンスを導入します。
-logging.logEntries.list -logging.privateLogEntries.list	スタックログドライブを取得する方法
- resourcemanager.projects.get	複数のプロジェクトをサポートするため。
-storage.buckets.create - storage.buckets.delete -ストレージ、バケツ、取得します -storage.buckets.list -storage.buckets.update	Google Cloud Storage バケットを作成して管理し、データを階層化します。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyrings.list	Cloud Volumes ONTAP でクラウドキー管理サービスからお客様が管理する暗号化キーを使用するため。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list -storage.objects.get -storage.objects.list	Cloud Volumes ONTAP インスタンスにサービスアカウントを設定します。このサービスアカウントは、Google Cloud Storage バケットへのデータ階層化の権限を提供します。
-compute-addresslist	HAペアを導入する際にリージョン内のアドレスを取得する。
-compute.backendServices.create -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list	HAペアでトラフィックを分散するためのバックエンドサービスを設定するには、次の手順を実行します。
- compute.networks.updatePolicy	HAペアのVPCおよびサブネットにファイアウォールルールを適用する。
- compute.subnetworks.us - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	してBlueXPの分類を有効にします。

アクション	目的
-container.clusters.get -container.clusters.list	Google Kubernetes Engine で実行されている Kubernetes クラスタを検出する。
- compute.instanceGroups.get -計算アドレス取得 - compute.instances.updateNetworkInterface	Cloud Volumes ONTAP HAペアでStorage VMを作成および管理する方法。
- monitoring.timeseries.list -storage.buckets.getIamPolicy	をクリックして、Google Cloud Storageバケットに関する情報を確認してください。
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkmsキーリング取得 - cloudkms.keyrings.getIamPolicy - cloudkms.keyrings.list - cloudkms.keyRings.setIamPolicy	Googleが管理するデフォルトの暗号化キーを使用する代わりに、BlueXPのバックアップとリカバリのアクティブ化ウィザードでお客様が管理する独自のキーを選択します。

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2023年2月6日

このポリシーには次の権限が追加されています：

- compute.instances.updateNetworkInterface

この権限はCloud Volumes ONTAP に必要です。

2023年1月27日

ポリシーに追加された権限は次のとおりです。

- Cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.keyrings.get
- cloudks.keyrings.getIamPolicyを参照してください
- cloudkms.keyRings.setIamPolicy

これらの権限はBlueXPのバックアップとリカバリに必要です。

ポート

AWSでのコネクタセキュリティグループのルール

コネクタのAWSセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。BlueXPでコネクタを作成すると、BlueXPでこのセキュリティグルー

プが自動的に作成されます。他のすべてのインストールオプションには、このセキュリティグループを設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22.	コネクタホストへの SSH アクセスを提供します
HTTP	8時80分	• クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	クライアントWebブラウザからローカルユーザインターフェイスへのHTTPSアクセス、およびBlueXP分類インスタンスからの接続を提供します
TCP	3128だ	Cloud Volumes ONTAP からネットアップサポートにAutoSupport メッセージを送信するためのインターネットアクセスを提供します。導入後にこのポートを手動で開く必要があります。 "コネクタがAutoSupport メッセージのプロキシとしてどのように使用されるかについて説明します"
TCP	9060、9061	政府機関の地域でBlueXPの分類とBlueXPのバックアップとリカバリを有効にして使用できるようになります。

アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべてのUDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。

送信元 IP アドレスは、コネクタホストです。

サービス	プロトコル	ポート	宛先	目的
API コールと AutoSupport	HTTPS	443年	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	AWS、ONTAP、BlueXPへのAPI呼び出し、NetAppへのAutoSupportメッセージの送信
API コール	TCP	3000	ONTAP HA メディエーター	ONTAP HA メディエーターとの通信
	TCP	8080 です	BlueXPの分類	導入時にBlueXP分類インスタンスを確認します
DNS	UDP	53.	DNS	BlueXPによるDNS解決に使用されます

Azureでのコネクタセキュリティグループのルール

コネクタのAzureセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。BlueXPでコネクタを作成すると、BlueXPでこのセキュリティグループが自動的に作成されます。他のすべてのインストールオプションには、このセキュリティグループを設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22.	コネクタホストへの SSH アクセスを提供します
HTTP	8時80分	• クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	クライアントWebブラウザからローカルユーザインターフェイスへのHTTPSアクセス、およびBlueXP分類インスタンスからの接続を提供します

プロトコル	ポート	目的
TCP	3128だ	Cloud Volumes ONTAP からネットアップサポートにAutoSupport メッセージを送信するためのインターネットアクセスを提供します。導入後にこのポートを手動で開く必要があります。 "コネクタがAutoSupport メッセージのプロキシとしてどのように使用されるかについて説明します"
TCP	9060、9061	政府機関の地域でBlueXPの分類とBlueXPのバックアップとリカバリを有効にして使用できるようになります。

アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべてのUDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。

送信元 IP アドレスは、コネクタホストです。

サービス	プロトコル	ポート	宛先	目的
API コールと AutoSupport	HTTPS	443年	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	Azure、ONTAP、BlueXPへのAPI呼び出し、NetAppへのAutoSupportメッセージの送信
API コール	TCP	8080 です	BlueXPの分類	導入時にBlueXP分類インスタンスを確認します
DNS	UDP	53.	DNS	BlueXPによるDNS解決に使用されます

Google Cloudのコネクタファイアウォールルール

ConnectorのGoogle Cloudファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。BlueXPでコネクタを作成すると、BlueXPでこのセキュリティグループが自動的に作成されます。他のすべてのインストールオプションには、このセキュリティグループを設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22.	コネクタホストへの SSH アクセスを提供します
HTTP	8時80分	• クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	クライアントWebブラウザからローカルユーザインターフェイスへのHTTPSアクセスを提供します
TCP	3128だ	Cloud Volumes ONTAP からネットアップサポートにAutoSupport メッセージを送信するためのインターネットアクセスを提供します。導入後にこのポートを手動で開く必要があります。 "コネクタがAutoSupport メッセージのプロキシとしてどのように使用されるかについて説明します"

アウトバウンドルール

コネクタの定義済みファイアウォールルールによって、すべてのアウトバウンドトラフィックが開かれます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの定義済みファイアウォールルールには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべてのUDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。

送信元 IP アドレスは、コネクタホストです。

サービス	プロトコル	ポート	宛先	目的
API コールと AutoSupport	HTTPS	443年	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	Google Cloud 、ONTAP、BlueXP へのAPI呼び出し、NetAppへのAutoSupportメッセージの送信
API コール	TCP	8080 です	BlueXPの分類	導入時にBlueXP分類インスタンスを確認します
DNS	UDP	53.	DNS	BlueXPによるDNS解決に使用されます

オンプレミスコネクタ用のポート

コネクタは、オンプレミスのLinuxホストに手動でインストールした場合、_inbound_portsを使用します。計画のためにこれらのポートを参照しなければならない場合があります。

これらのインバウンドルールは、すべてのBlueXP導入モデルに適用されます。

プロトコル	ポート	目的
HTTP	8時80分	• クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス • Cloud Volumes ONTAPのアップグレードプロセスで使用
HTTPS	443年	クライアントWebブラウザからローカルユーザインターフェイスへのHTTPSアクセスを提供します

知識とサポート

サポートに登録します

BlueXPとそのストレージソリューションおよびサービスに固有のテクニカルサポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウドプロバイダのファイルサービスでNetAppのサポートは有効になりません。クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

サポート登録の概要

サポート資格を有効にする登録には、次の2つの形式があります。

- BlueXPアカウントIDサポートサブスクリプションの登録(BlueXPの[サポートリソース]ページにある20桁の960xxxxxxxxxシリアル番号)。

  これは、BlueXP内のすべてのサービスのシングルサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポート契約が登録されている必要があります。

- クラウドプロバイダのマーケットプレイスでのサブスクリプションに関連付けられているCloud Volumes ONTAP のシリアル番号を登録している（909201xxxxxxxxのシリアル番号）。

  これらのシリアル番号は、通常PAY_GOシリアル番号と呼ばれ、Cloud Volumes ONTAP の導入時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録することで、サポートチケットのオープンやケースの自動生成などの機能を利用できます。登録を完了するには、以下の手順でNetApp Support Site（NSS）アカウントをBlueXPに追加してください。

NetAppサポートに**BlueXP**アカウントを登録します

サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウントの1人のユーザがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。ネットアップサポートへの登録方法は、NetApp Support Site （NSS）アカウントがあるかどうかによって異なります。

NSSアカウントをお持ちの既存のお客様

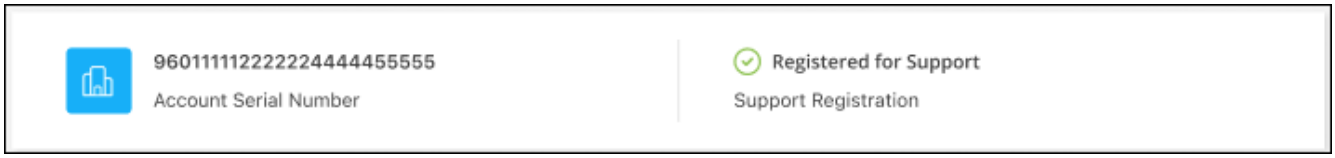
NSSアカウントをお持ちのネットアップのお客様は、BlueXPからサポートに登録するだけで済みます。

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. [ユーザクレデンシャル]*を選択します。
3. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site（NSS）認証プロンプトに従います。
4. 登録プロセスが正常に完了したことを確認するには、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。

   [リソース]ページに、アカウントがサポートに登録されていることが表示されます。

   他のBlueXPユーザにNetApp Support Siteアカウントが関連付けられていない場合、このサポート登録ステータスは表示されません。ただし、BlueXPアカウントがサポートに登録されていないわけではありません。アカウント内の1人のユーザーがこれらの手順を実行している限り、アカウントは登録されています。

NSSアカウントを持たない既存のお客様

NetAppの既存のお客様で、ライセンスとシリアル番号は_NO_NSSアカウントしかお持ちでない場合は、NSSアカウントを作成してBlueXPログインに関連付ける必要があります。

手順

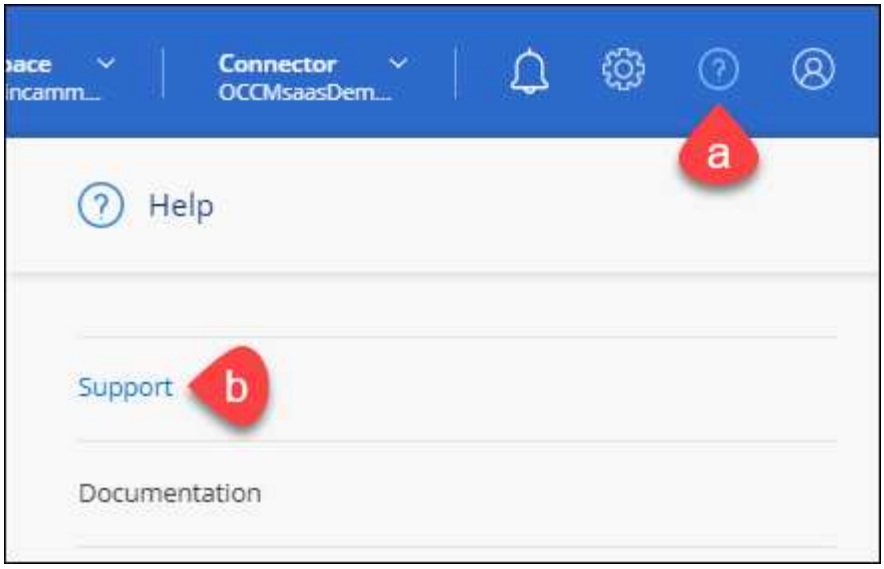
1. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. 必ず、上記のシリアル番号フィールドに使用されているBlueXPアカウントのシリアル番号(960xxxx)をコピーしてください。これにより、アカウント処理が高速化されます。
2. の手順を実行して、新しいNSSアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

ネットアップのソリューションを初めて導入する場合は

ネットアップ製品を初めてご利用になり、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

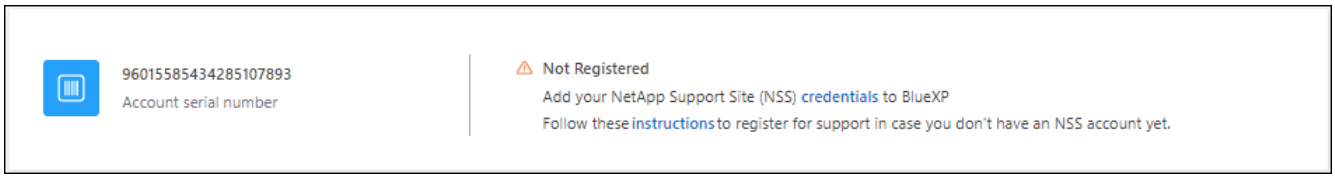
手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

2. サポート登録ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. に移動します "ネットアップサポート登録サイト" 「ネットアップ登録のお客様ではありません」を選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line ）]フィールドで、[Cloud Manager *]を選択し、該当する課金プロバイダーを選択します。
6. 上記の手順2からアカウントのシリアル番号をコピーし、セキュリティチェックを完了して、ネットアップのグローバルデータプライバシーポリシーを確認します。

   この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

   確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が高速化されます。

完了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetApp Support Siteアカウントを作成したら、の手順を実行してアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

Cloud Volumes ONTAPサポートのためにNSSクレデンシャルを関連付けます

NetApp Support Siteで次の主要なワークフローを有効にするには、BlueXPアカウントにクレデンシャルを関連付ける必要がCloud Volumes ONTAPあります。

- 従量課金制のCloud Volumes ONTAPシステムのサポートを登録しています

  お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、 NSS アカウントを用意する必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

  ライセンスキーをBlueXPでアップロードし、購入した契約期間のサブスクリプションを有効にするには、NSSアカウントを提供する必要があります。これには、期間の更新の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

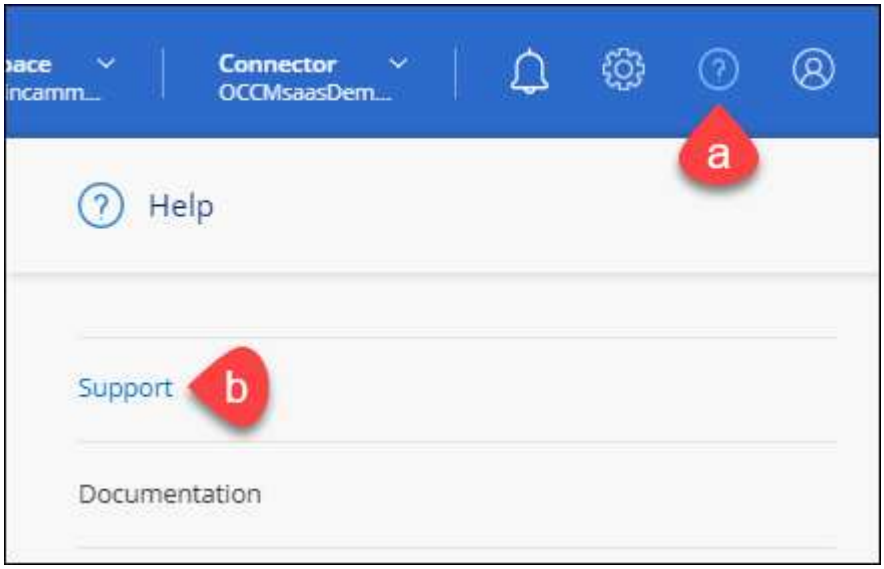
NSSクレデンシャルをBlueXPアカウントに関連付ける方法は、BlueXPユーザログインに関連付けられたNSSアカウントとは異なります。

これらのNSSクレデンシャルは、特定のBlueXPアカウントIDに関連付けられています。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*を選択します。
3. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

   NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、NetApp Support Siteの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   これらのアクションにより、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

   次の点に注意してください。

   - NSSアカウントは、お客様レベルのアカウントである必要があります（ゲストアカウントや一時アカウントではありません）。複数のお客様レベルのNSSアカウントを設定できます。
   - NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、パートナーレベルのアカウントが存在する場合は、次のエラーメッセージが表示されます。

     「別のタイプのNSSユーザーがすでに存在するため、このアカウントではNSS顧客タイプは許可されていません。」

   既存のお客様レベルのNSSアカウントがあり、パートナーレベルのアカウントを追加しようとする場合も同様です。

   - ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

     これはシステムによって生成されたIDで、電子メールにマッピングされます。[**NSS Management**]ページで、から電子メールを表示できます ••• メニュー。

   - ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます ••• メニュー。

     このオプションを使用すると、再度ログインするように求められます。これらのアカウントのトークンは90日後に期限切れになります。このことを通知する通知が投稿されます。

ヘルプを表示します

ネットアップでは、BlueXPとその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（ KB ）記事やコミュニティフォーラムなど、 24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

クラウドプロバイダのファイルサービスのサポート

クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、以下に記載されているサポートオプションを使用してください。

セルフサポートオプションを使用します

次のオプションは、 1 日 24 時間、週 7 日間無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPのマニュアル。

- "ナレッジベース"

  BlueXPナレッジベースで問題のトラブルシューティングに役立つ記事を検索します。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

- [ケースの作成]*機能を使用するには、最初にNetApp Support SiteクレデンシャルをBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられているクレデンシャルの管理方法について説明します"。
- シリアル番号のあるONTAPシステムのケースをオープンする場合は、そのシステムのシリアル番号にNSSアカウントを関連付ける必要があります。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [**Resources**]ページで、[Technical Support]で次のいずれかのオプションを選択します。

   a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。

   b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。

      - **Service**:問題 が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能を備えたテクニカルサポート問題 に固有のBlueXPなどです。
      - 作業環境：ストレージに該当する場合は、* Cloud Volumes ONTAP *または*オンプレミス*を選択し、関連する作業環境を選択します。

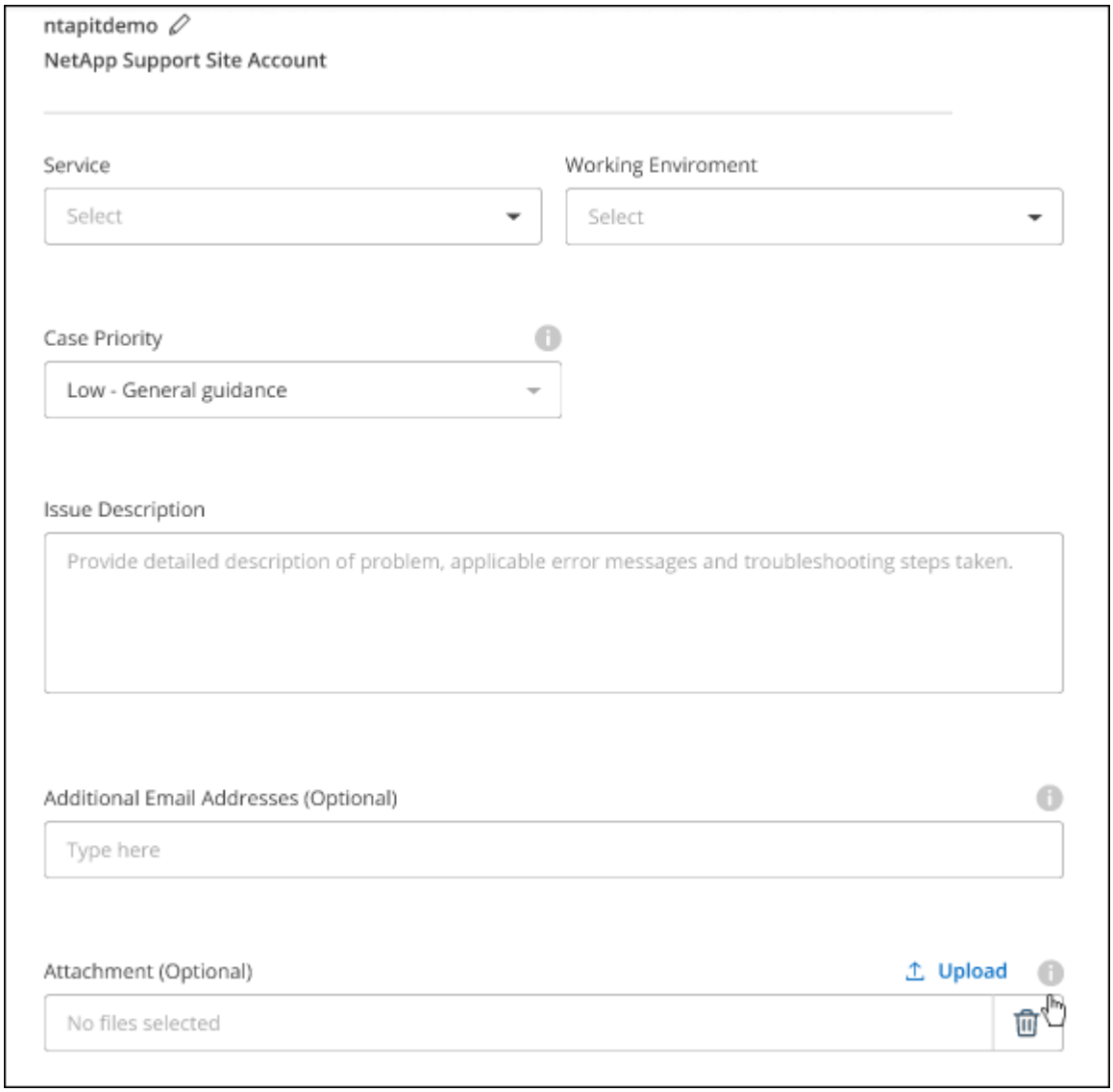
作業環境のリストは、サービスの上部バナーで選択したBlueXPアカウント、ワークスペース、コネクタの範囲内にあります。

- ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

  これらの優先度の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスポインタを合わせます。

- *事象の説明 *：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要 を入力します。
- その他のメールアドレス：この問題 を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
- 添付ファイル（オプション）：一度に1つずつ、最大5つの添付ファイルをアップロードできます。

  添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。



完了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[設定]>[タイムライン]*を選択し、「サポートケースの作成」というアクションを検索します。 右端のボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラーメッセージが表示される場合があります。

"選択したサービスに対してケースを作成する権限がありません"

このエラーは、NSSアカウントとそれに関連付けられているレコードの会社が、BlueXPアカウントのシリアル番号(例960xxxx）または動作環境のシリアル番号。次のいずれかのオプションを使用して、サポートを受けることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースをに送信します https://mysupport.netapp.com/site/help

サポートケースの管理（プレビュー）

アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の2つのビューがあります。
  - 左側のビューには、指定したユーザNSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
  - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

  テーブルの結果には、選択したビューに関連するケースが反映されます。
- 目的の列を追加または削除したり、[優先度]や[ステータス]などの列の内容をフィルタリングしたりできます。他の列には、並べ替え機能だけがあります。

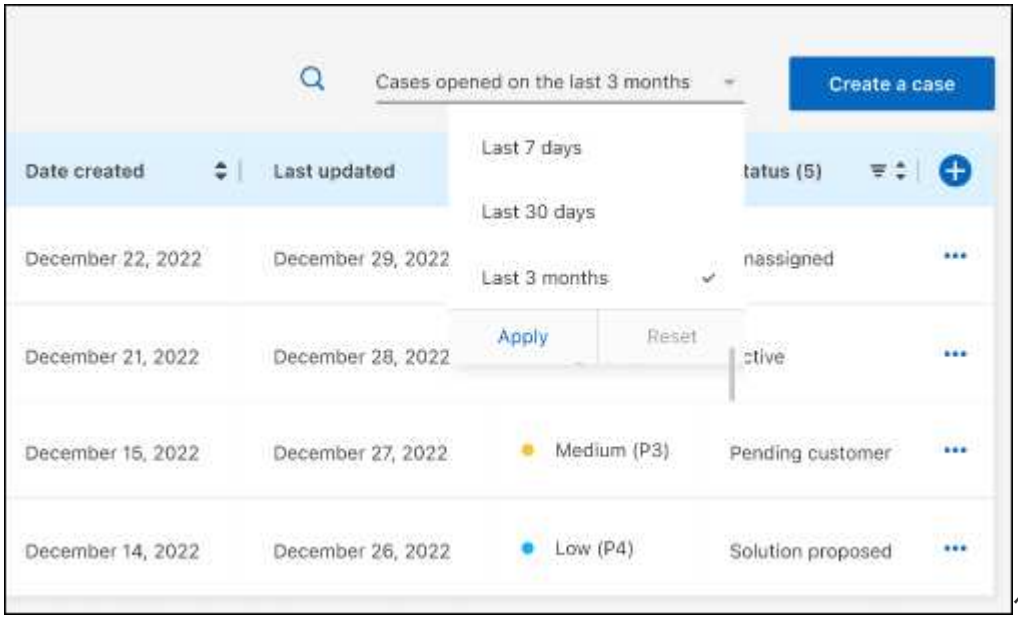
  詳細については、以下の手順を参照してください。
- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [ケース管理]*を選択し、プロンプトが表示されたらNSSアカウントをBlueXPに追加します。

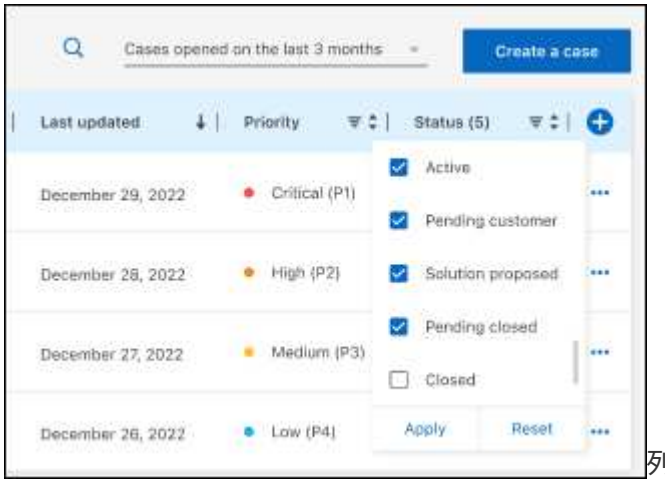
   ケース管理*ページには、BlueXPユーザアカウントに関連付けられたNSSアカウントに関連するオープンケースが表示されます。これは、* NSS管理*ページの上部に表示されるNSSアカウントと同じです。

3. 必要に応じて、テーブルに表示される情報を変更します。
    - [Organization’s Cases]*で[View]*を選択すると、会社に関連付けられているすべてのケースが表示されます。
    - 正確な日付範囲を選択するか、別の期間を選択して、日付範囲を変更します。



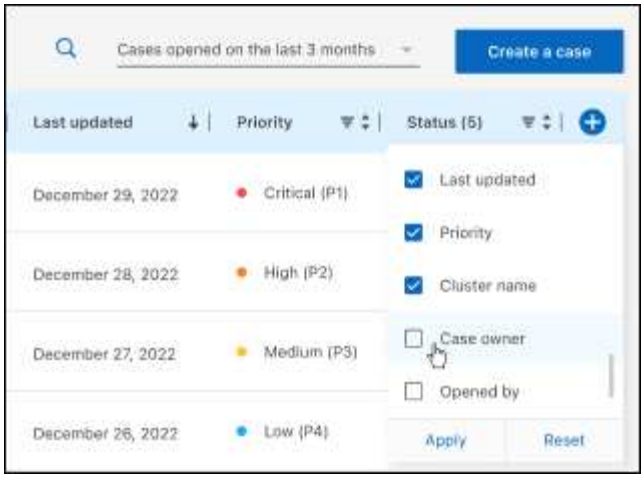
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

    - 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

    - テーブルに表示される列を変更するには、 次に、表示する列を選択します。

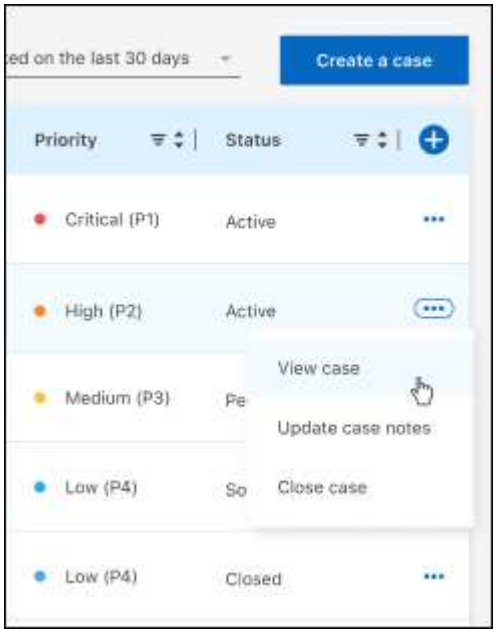


4. 既存のケースを管理するには、 ••• 使用可能なオプションのいずれかを選択します。

   - ケースの表示:特定のケースの詳細を表示します。
   - ケースノートの更新：問題の詳細を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付します。

     添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。

   - ケースをクローズ：ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

"BlueXPに関する注意事項"