BlueXPを管理します

Setup and administration

NetApp
April 22, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-setup-admin/concept-federation.html on April 22, 2024. Always check docs.netapp.com for the latest.

目次

BlueXPを管理します 1
BlueXPでアイデンティティフェデレーションを使用 1
BlueXPのアカウント 6
コネクタ 21
クレデンシャルとサブスクリプション 41

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。

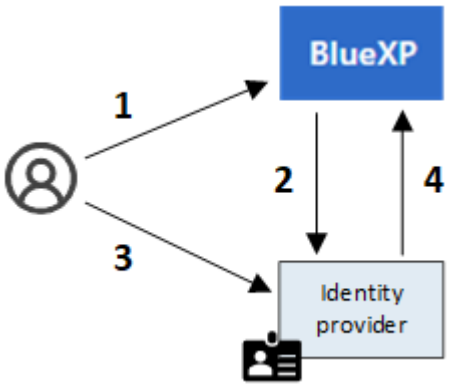
- をダウンロードして実行します "ネットアップフェデレーションリクエストフォーム"
- フォームに指定されたメールアドレスにフォームを送信します

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

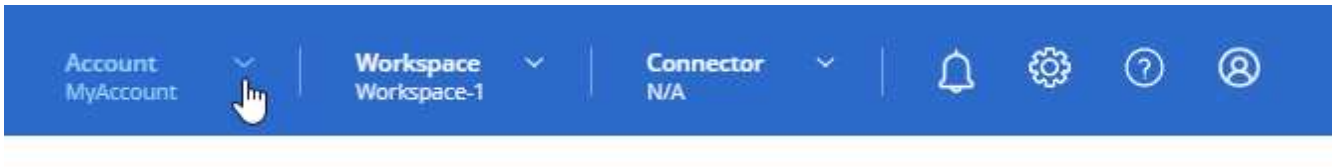
アカウントのユーザーは、特定のワークスペースのリソースにアクセスして管理できます。

ユーザを追加します

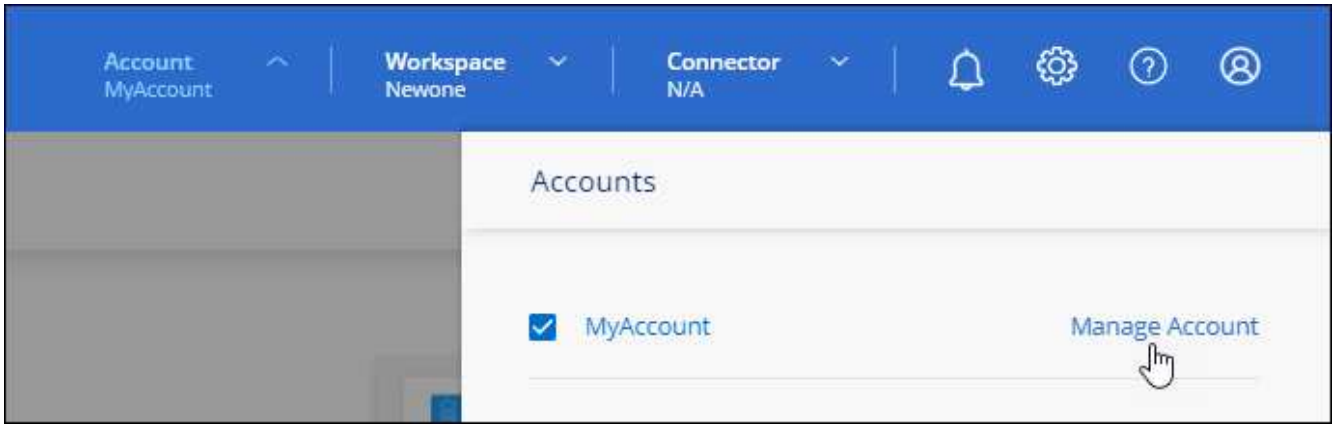
ユーザをBlueXPアカウントに関連付けて、BlueXPで作業環境を作成、管理できるようにします。

手順

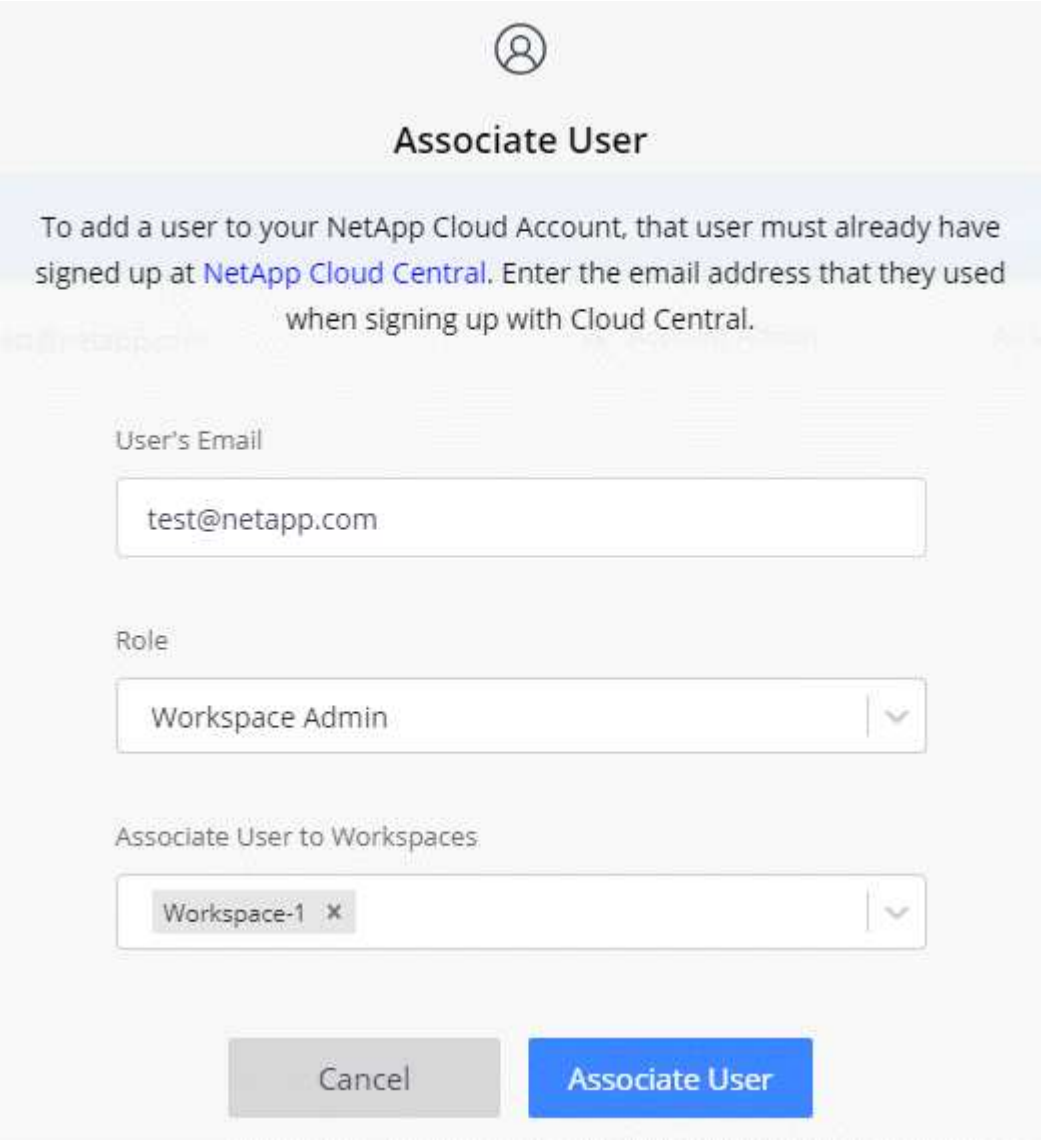
1. ユーザーがまだ行っていない場合は、にアクセスするようにユーザーに依頼します "NetApp BlueXP のWebサイト" 登録してください。
2. BlueXPの上部で、*[Account]*ドロップダウンを選択します。



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

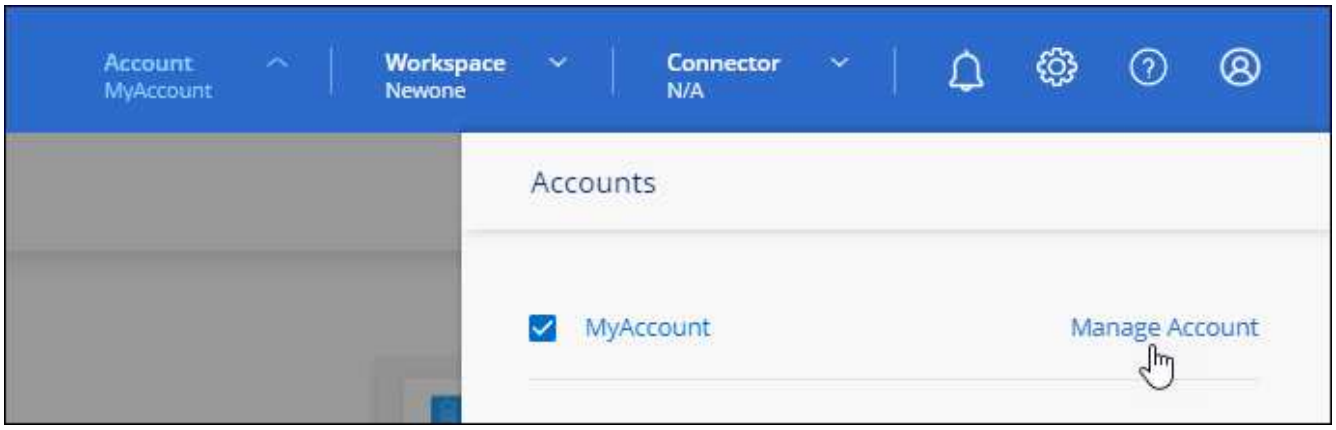
ユーザには、NetApp BlueXPの「Account Association」というタイトルのEメールが送信されます。 このメールには、BlueXPにアクセスするために必要な情報が記載されています。

ユーザを削除します

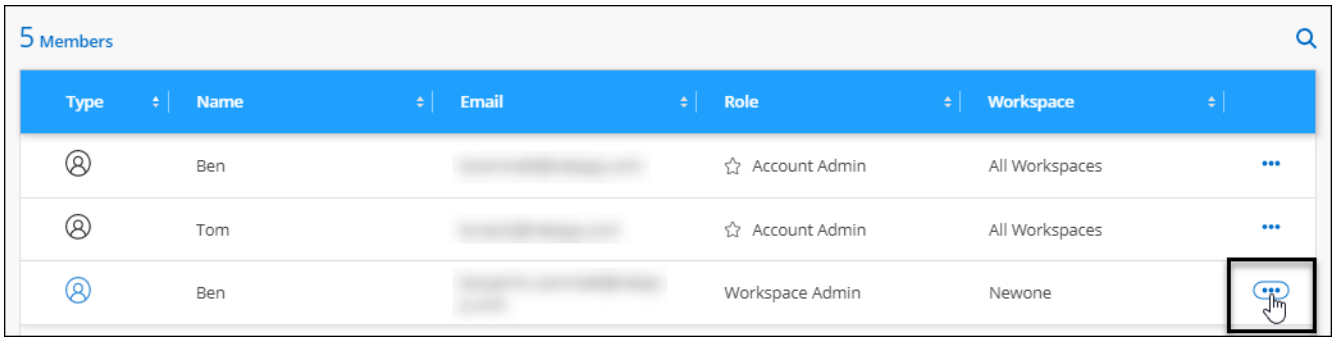
関連付けを解除すると、ユーザはBlueXPアカウントのリソースにアクセスできなくなります。

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。

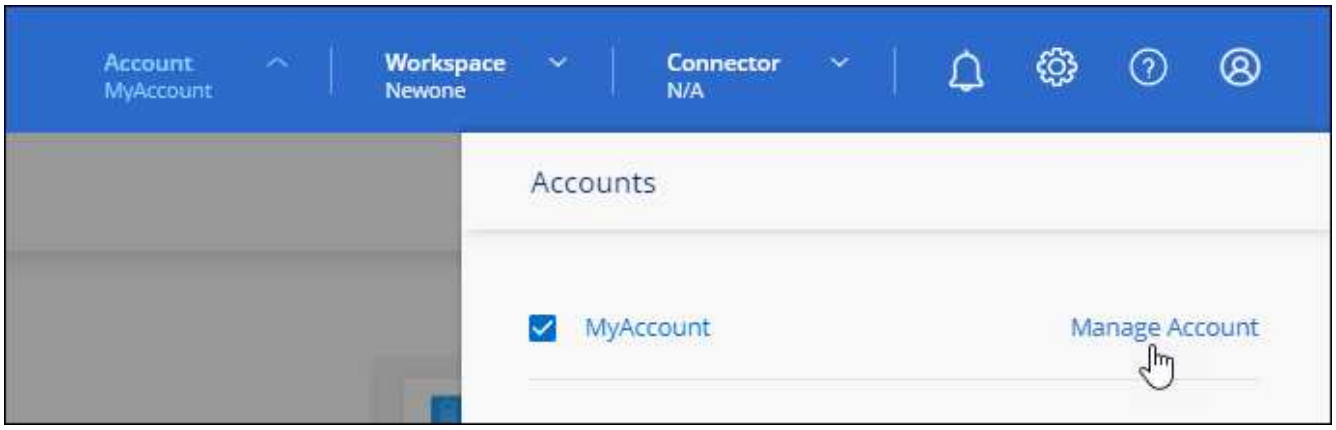
ワークスペース管理者のワークスペースを管理します

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。

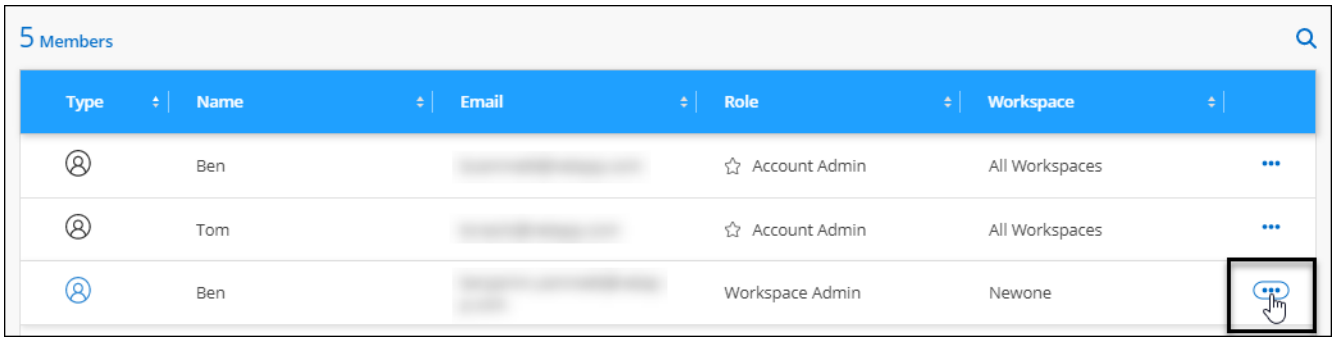
> ワークスペース管理者がBlueXPからこれらのワークスペースにアクセスできるように、コネクタをワークスペースに関連付ける必要もあります。 "コネクターのワークスペースを管理する方法について説明します。"。

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。

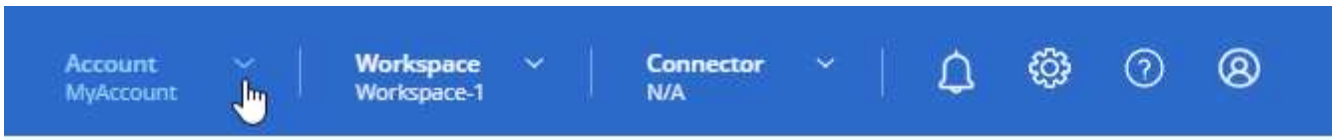
サービスアカウントを使用する場合、API処理に更新トークンは必要ありません。 "リフレッシュトークンの詳細"

サービスアカウントを作成します

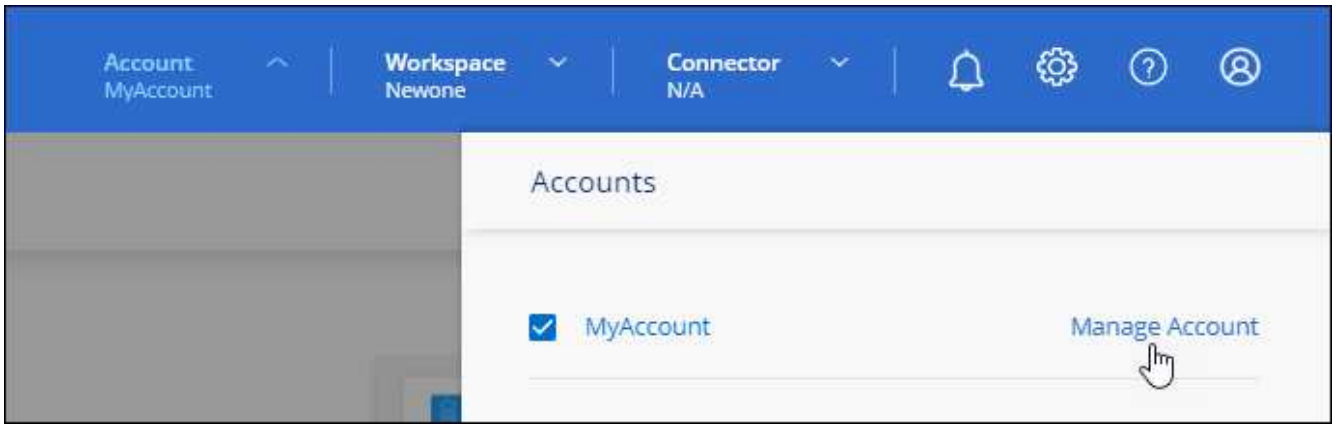
作業環境でリソースを管理するために必要な数のサービスアカウントを作成します。

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。

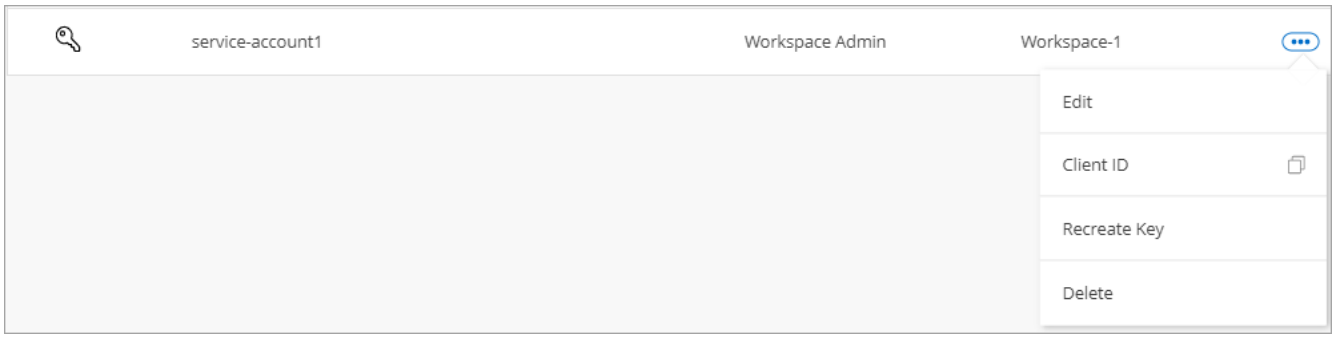
"サービスアカウントトークンの作成方法について説明します"

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。



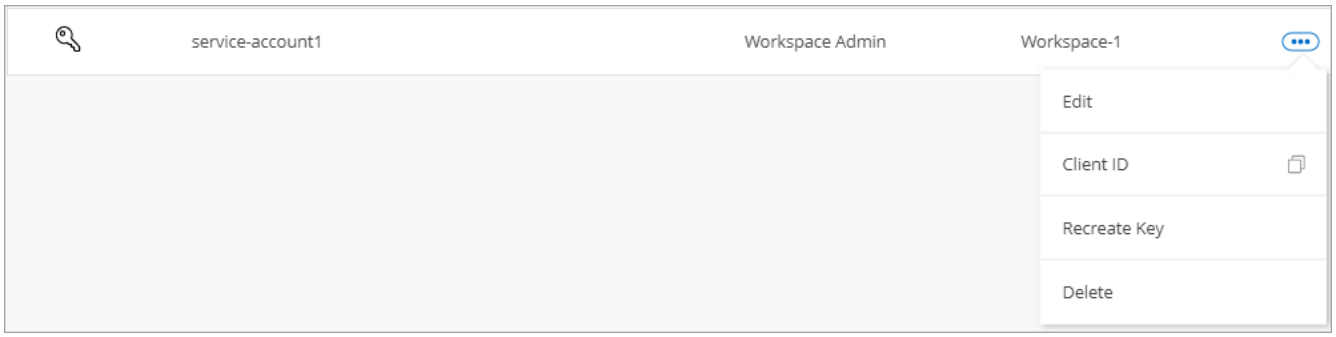
2. [Client ID]*を選択します。
3. ID がクリップボードにコピーされます。

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。

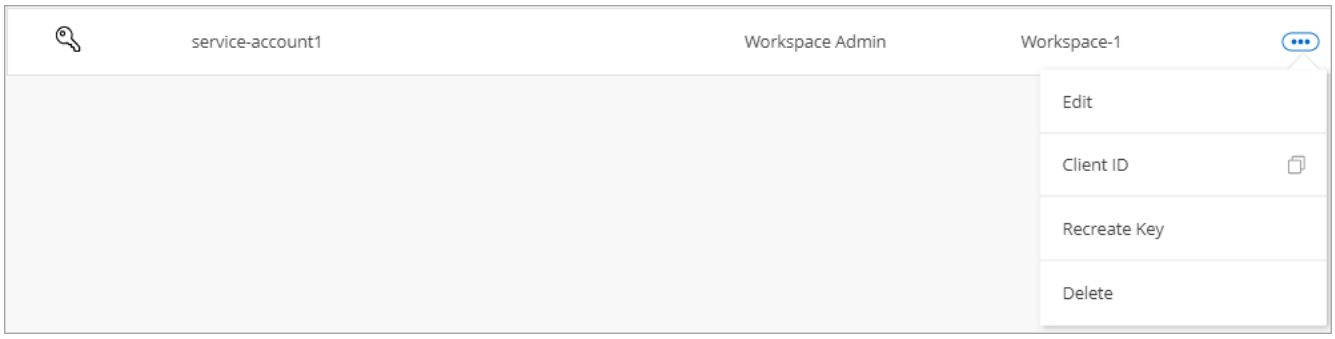
5. [閉じる（ Close ）] を選択します。

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。

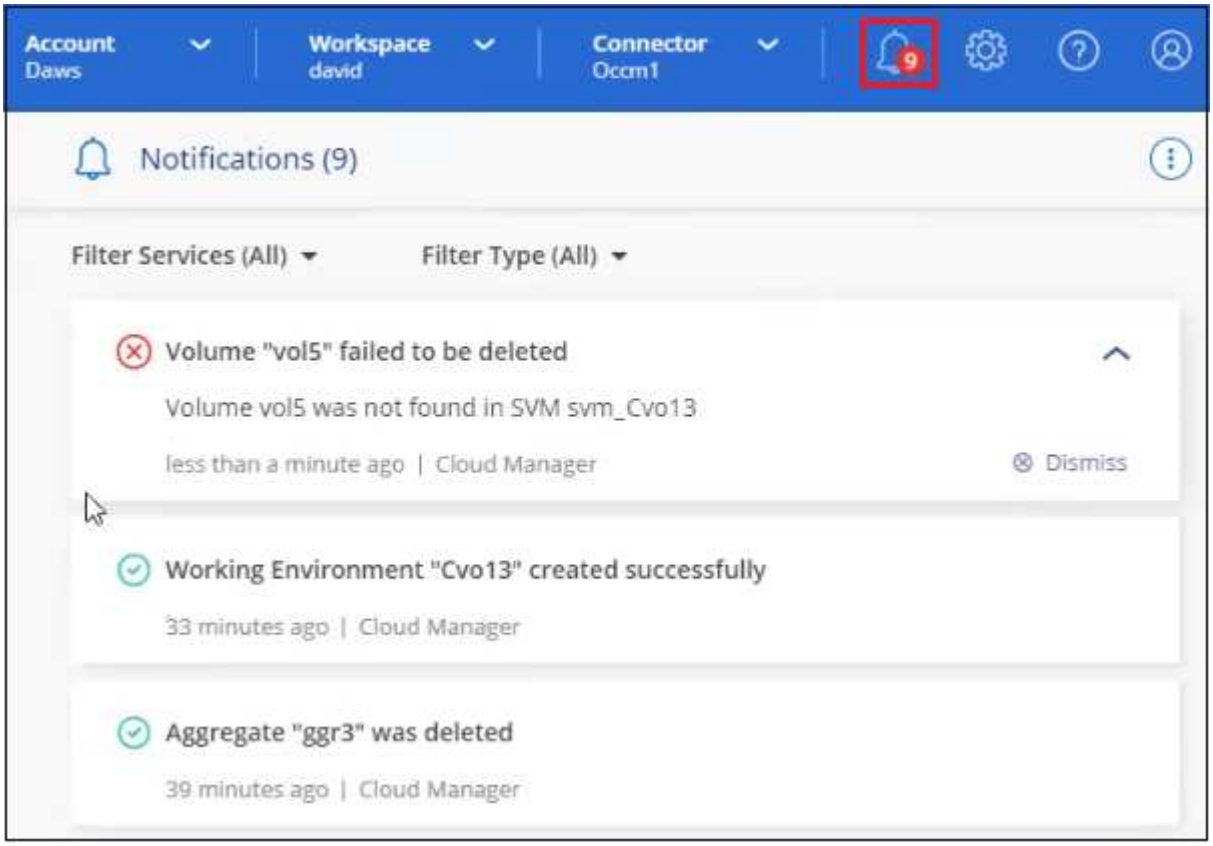
通知センター	タイムライン
イベントとアクションのステータスの概要が表示されます	各イベントまたはアクションの詳細を表示し、詳細な調査を行います
現在のログインセッションのステータスを表示します（ログオフ後、この情報は通知センターに表示されません）。	過去1カ月間のステータスを保持します
ユーザインターフェイスで開始されたアクションのみを表示します	UI または API からのすべての操作が表示されます

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。

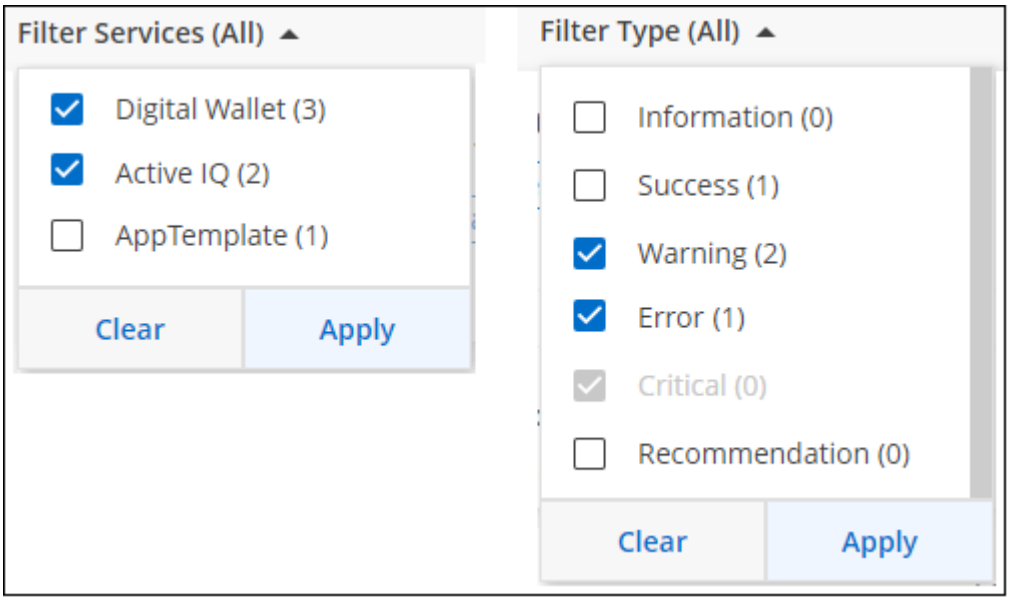
通知タイプ

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。



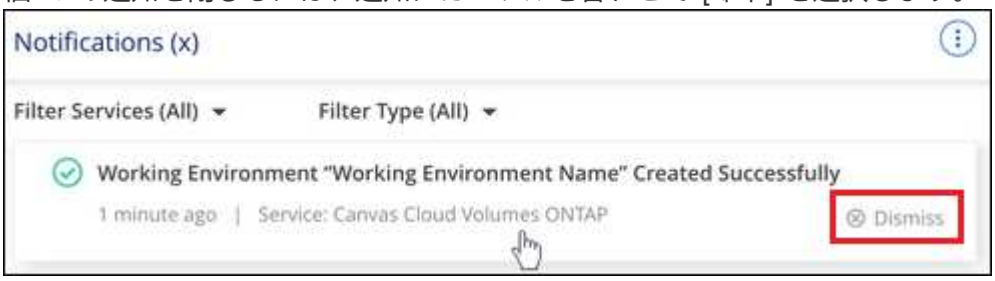
たとえば、BlueXP操作の「エラー」および「警告」通知のみを表示する場合は、これらのエントリを選択すると、これらの通知タイプのみが表示されます。

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。

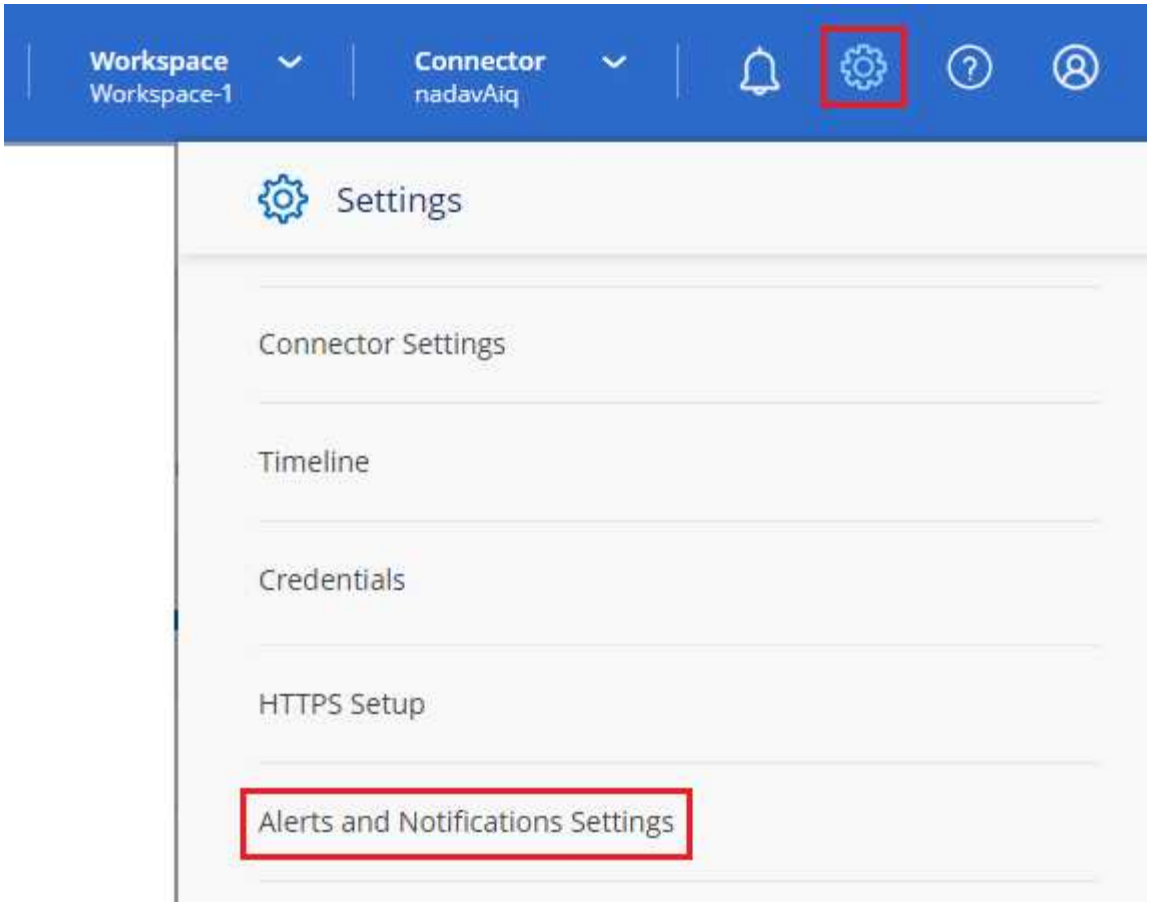
通知センターで設定したフィルタは、電子メールで受信する通知の種類を決定するものではありません。既定では、BlueXPアカウント管理者はすべての「重要」および「推奨」通知の電子メールを受信します。これらの通知はすべてのサービスに適用されます。コネクタやBlueXPのバックアップとリカバリなど、特定のサービスについてのみ通知を受け取ることはできません。

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。

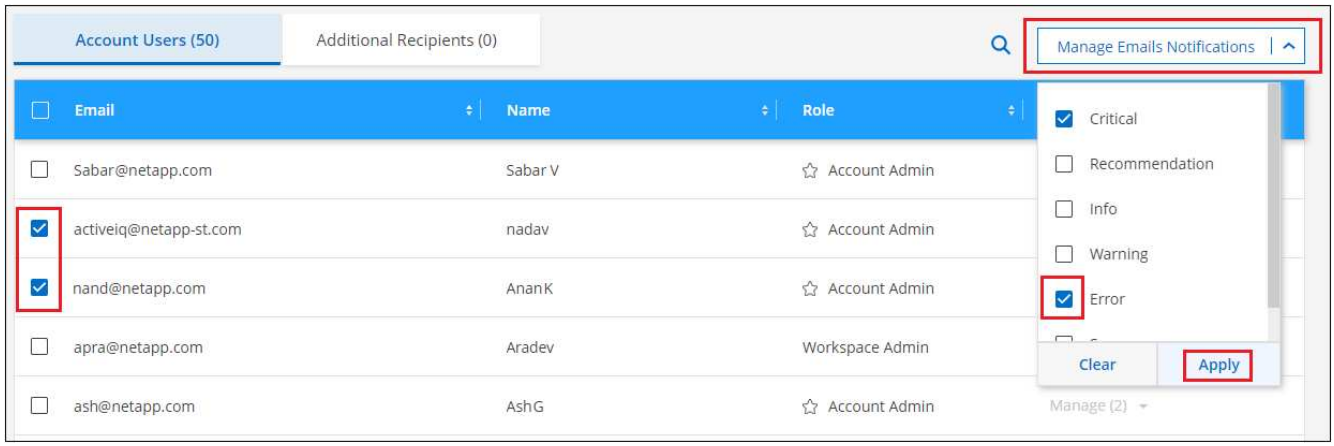
手順

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。



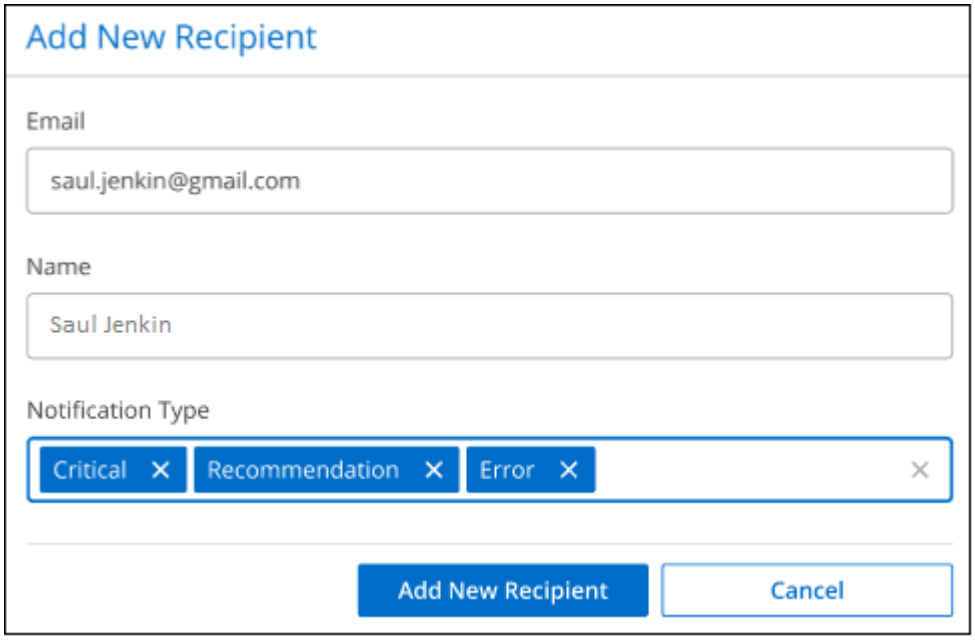
Eメール受信者を追加します

[_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

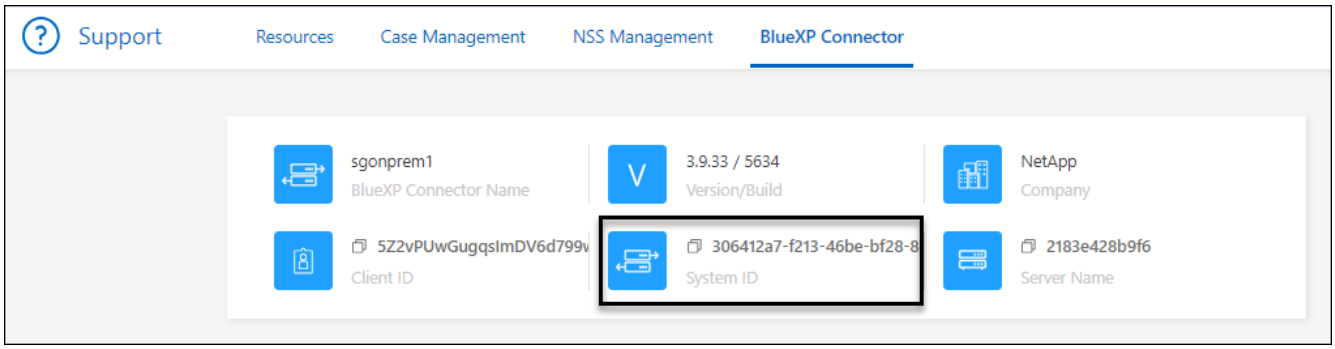
使用を開始するにあたり、ネットアップの担当者からコネクタのシステムIDを尋ねられることがあります。この ID は通常、ライセンスの取得やトラブルシューティングの目的で使用されます。

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"。

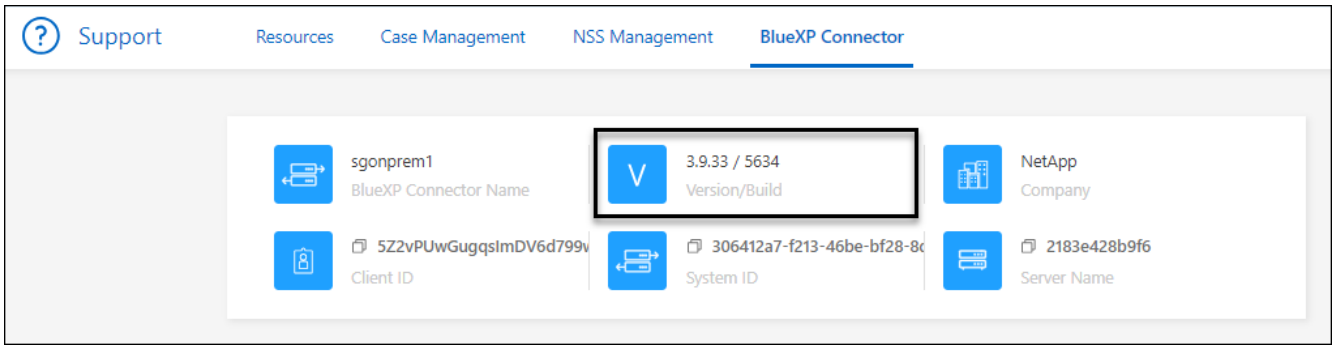
コネクタのバージョンの表示

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。



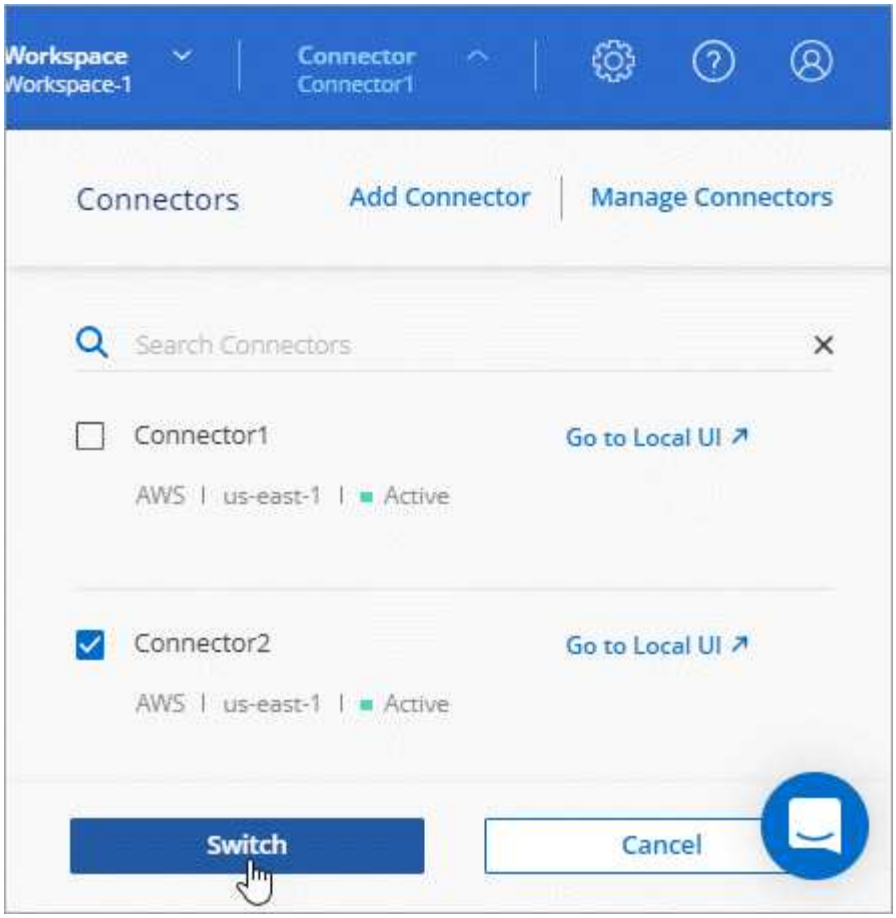
コネクタを切り替えます

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

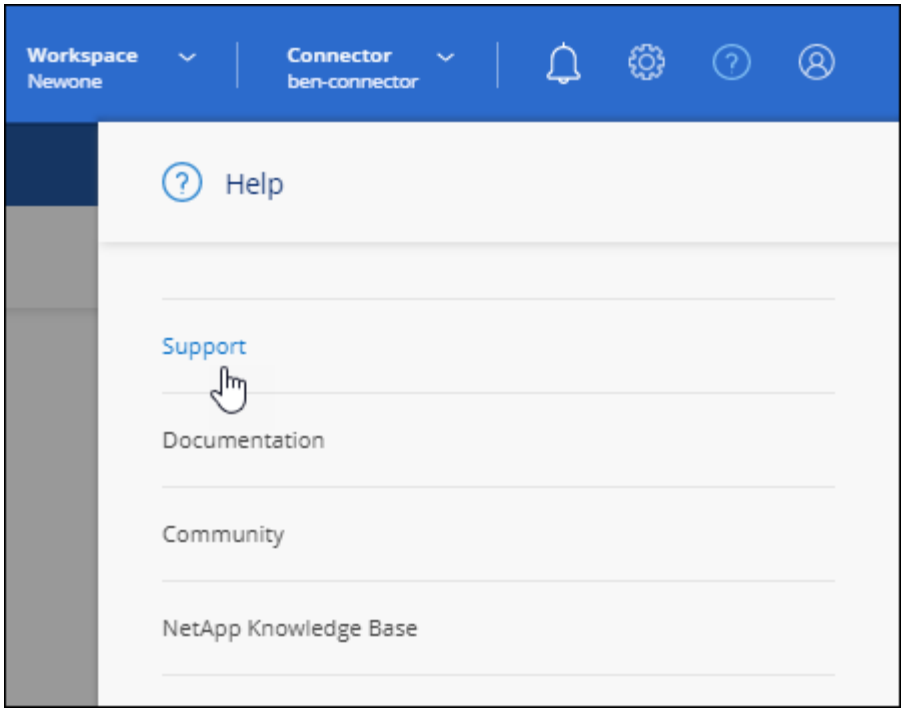
BlueXPが更新され'選択したコネクタに関連付けられている作業環境が表示されます

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。

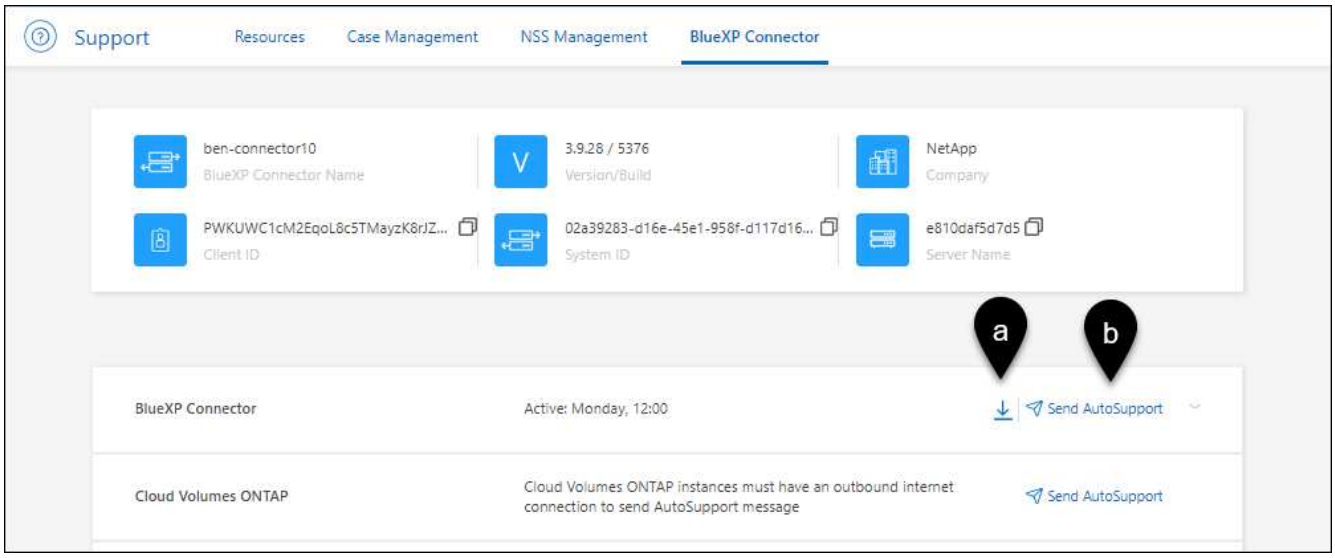
手順

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

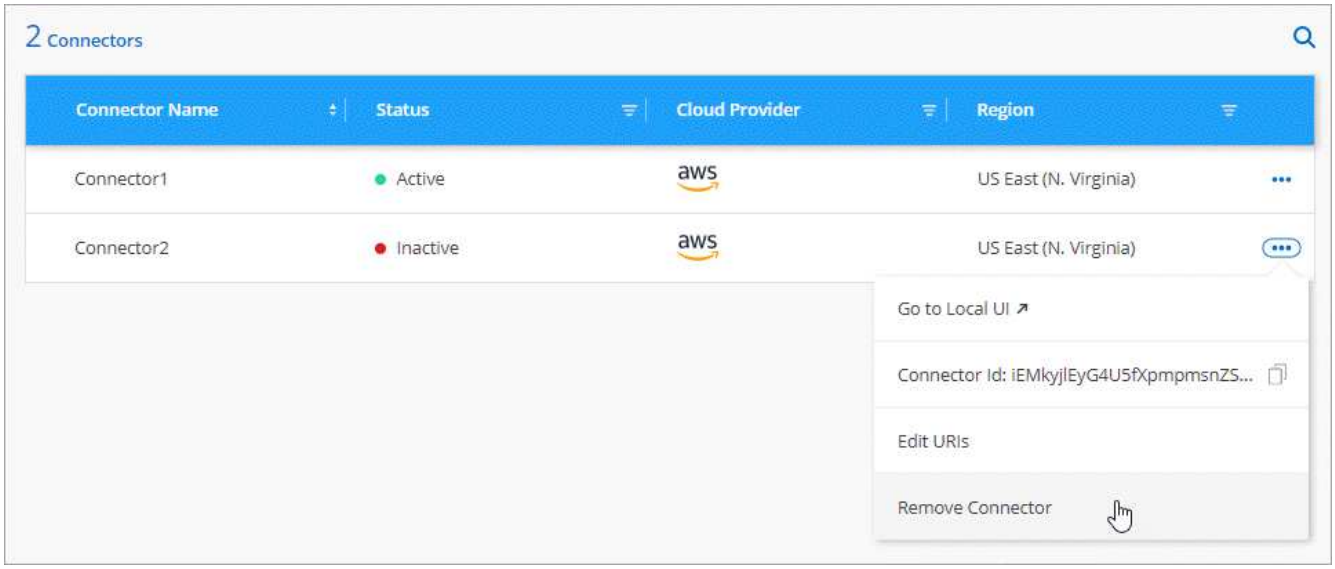
コネクタがアクティブでない場合は、BlueXPのコネクタのリストから削除できます。この処理は、Connector 仮想マシンを削除した場合や Connector ソフトウェアをアンインストールした場合に実行できます。

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

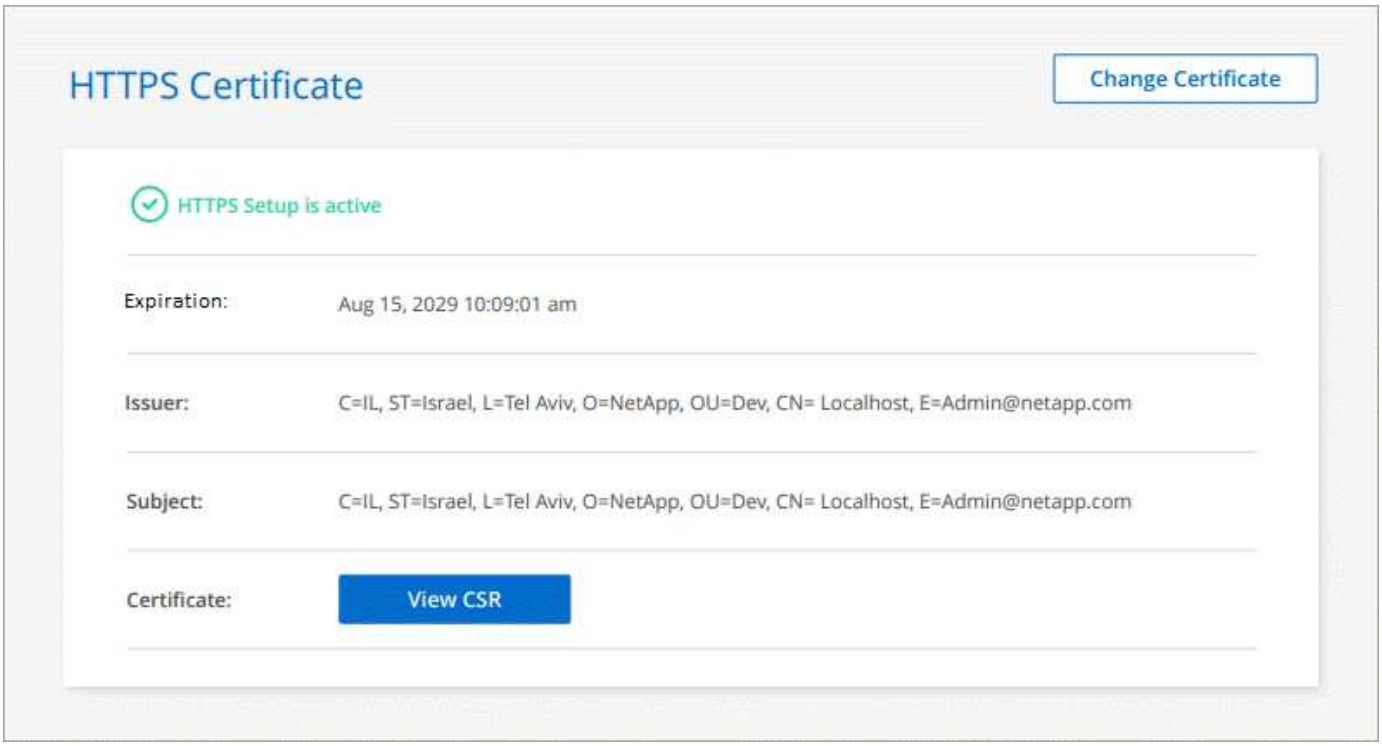
1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[HTTPSセットアップ]*を選択します。

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

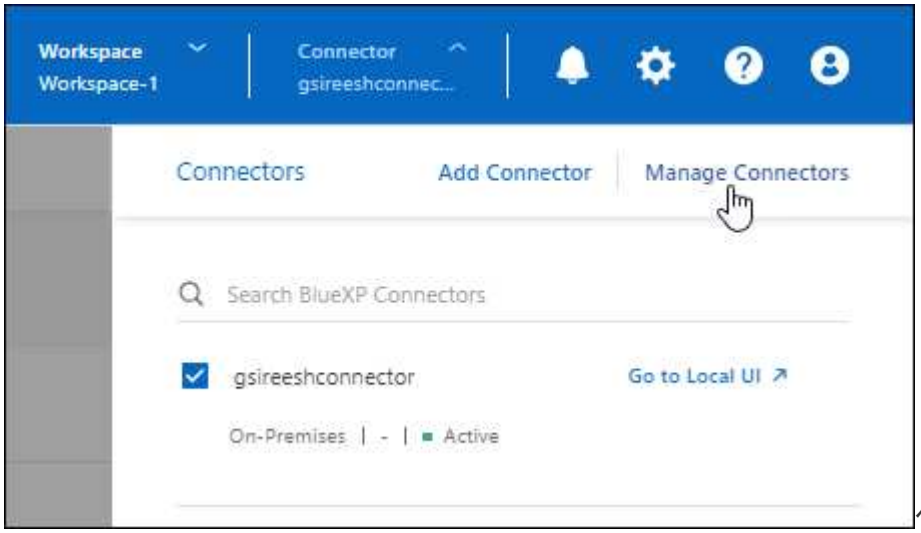
1. [BlueXPコネクタの編集]*ページに移動します。

   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

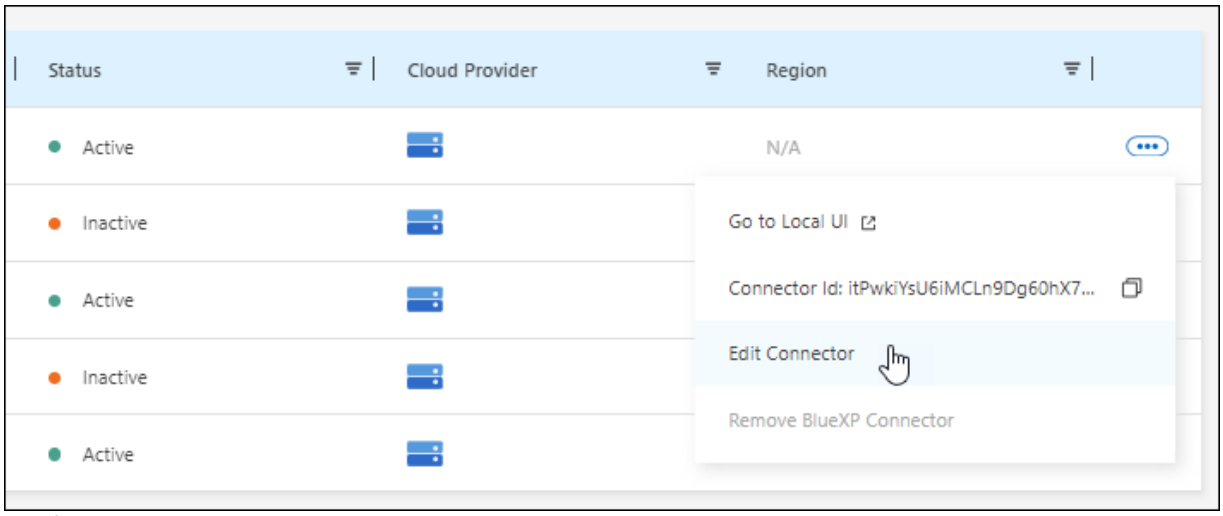
a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

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。

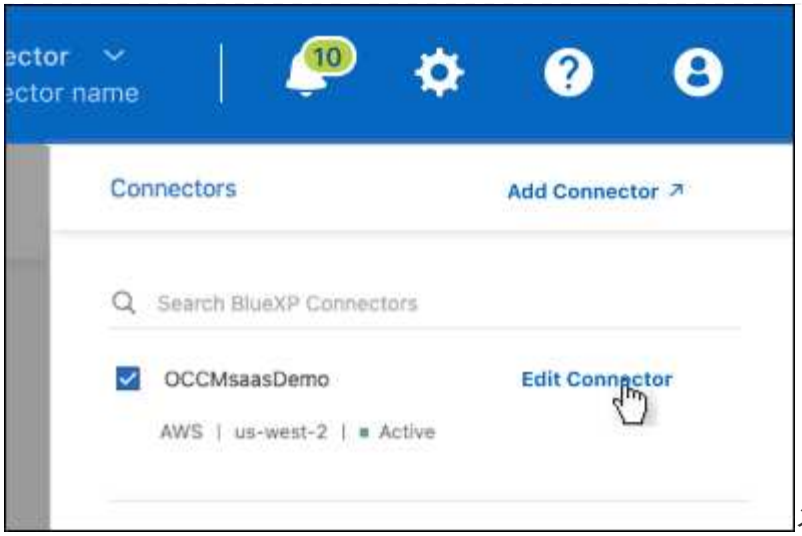


オプションを示すスクリーンショット。"]

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

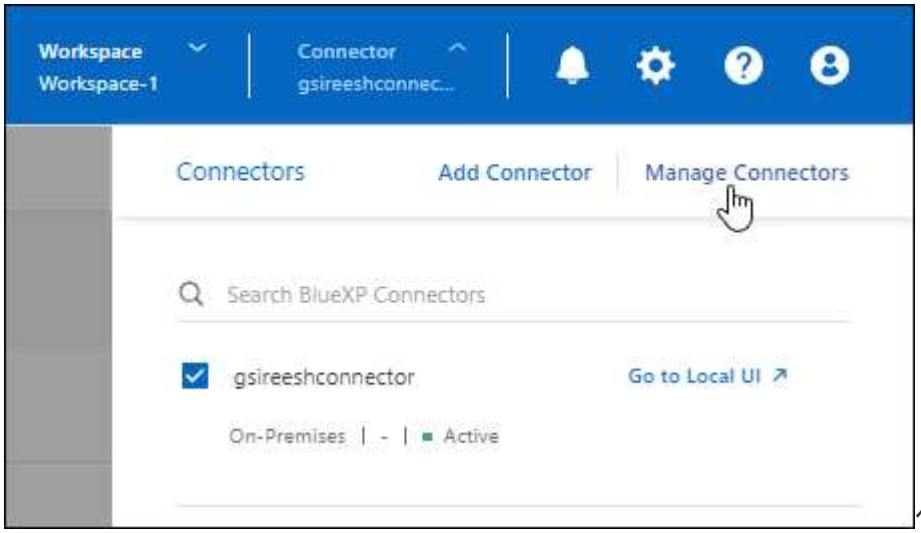
1. [BlueXPコネクタの編集]*ページに移動します。

   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

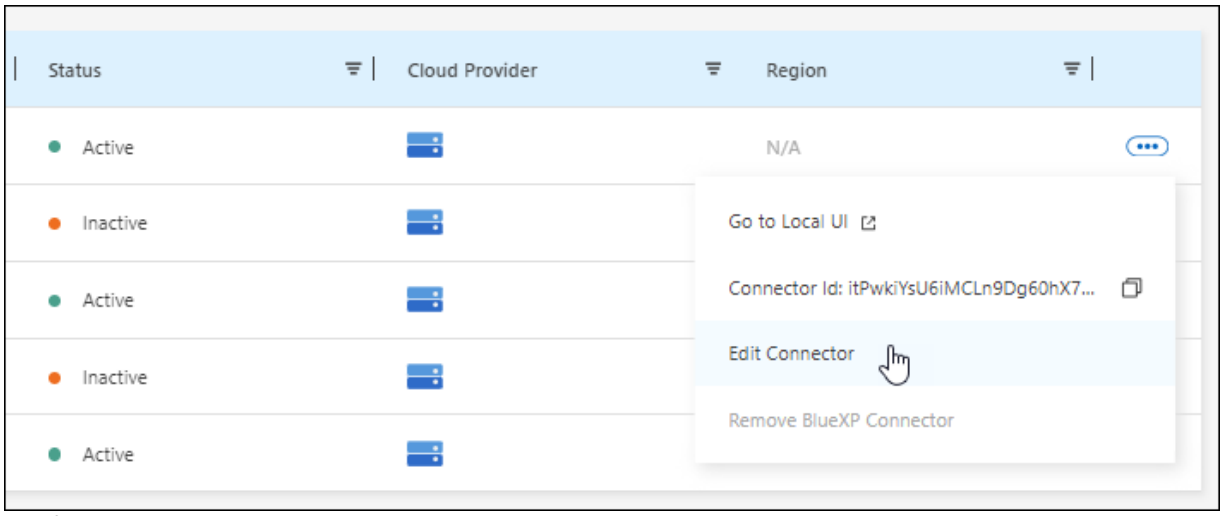
a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

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。

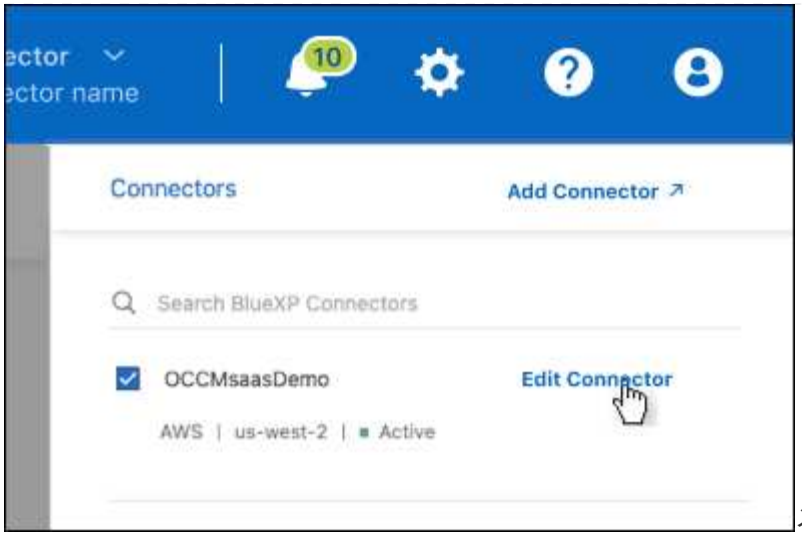


オプションを示すスクリーンショット。"]

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

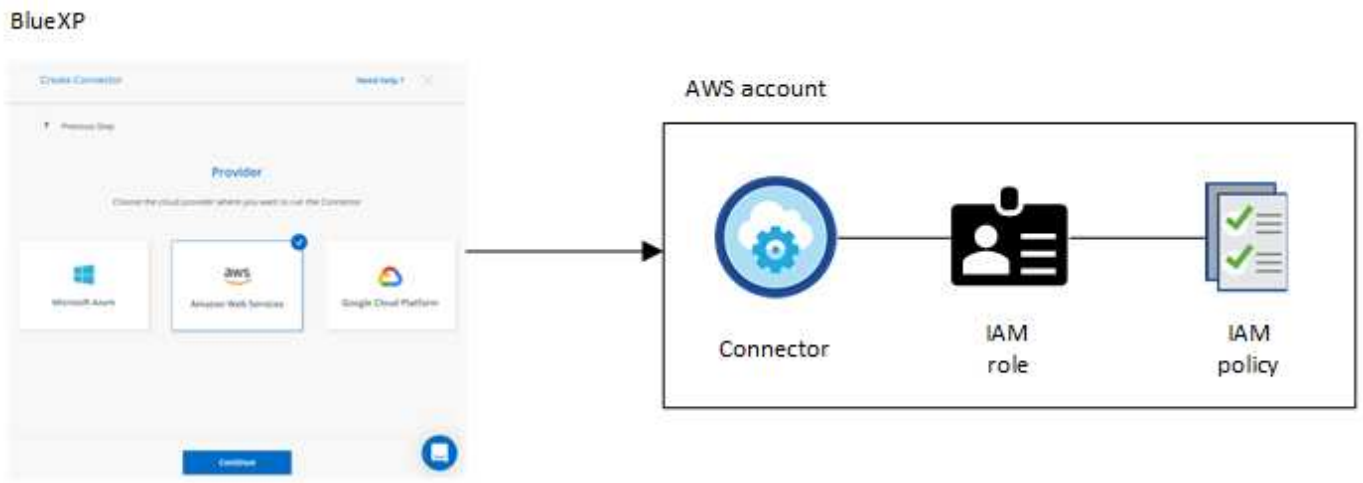
BlueXPがAWSクレデンシャルを使用してユーザに代わって操作を実行する方法と、それらのクレデンシャルがマーケットプレイスのサブスクリプションにどのように関連付けられているかをご確認くださいこれらの詳細を理解しておくと、BlueXPで1つ以上のAWSアカウントのクレデンシャルを管理する際に役立ちます。たとえば、AWSクレデンシャルをBlueXPに追加するタイミングを把握できます。

AWS の初期クレデンシャル

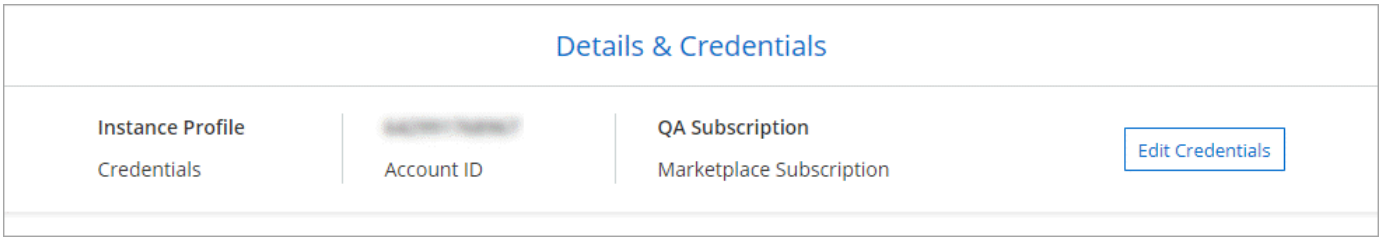
BlueXPからコネクタを展開する場合は、IAMロールのARNまたはIAMユーザのアクセスキーを指定する必要があります。使用する認証方式に、 Connector インスタンスを AWS に導入するための必要な権限がある必要があります。必要な権限は、に表示されます "AWS 用のコネクタ導入ポリシー"。

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

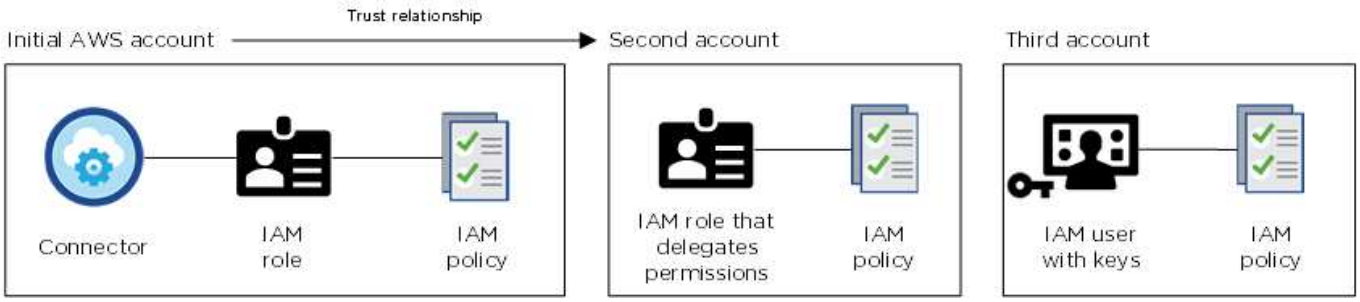
AWSクレデンシャルを追加するには、次の2つの方法があります。

- 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。

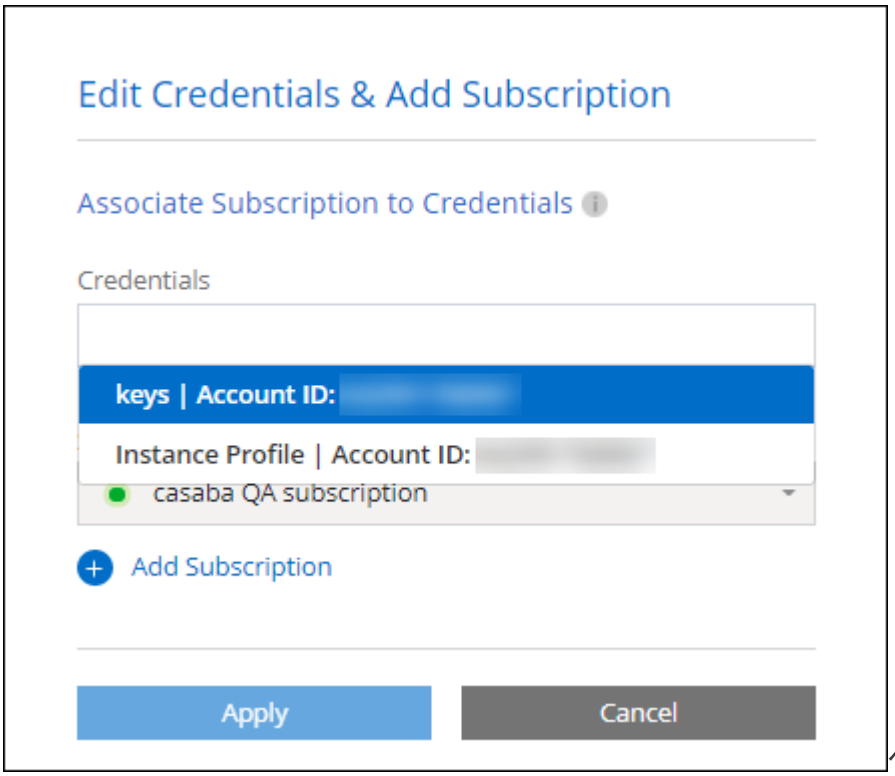
AWS クレデンシャルを既存のコネクタに追加する

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。

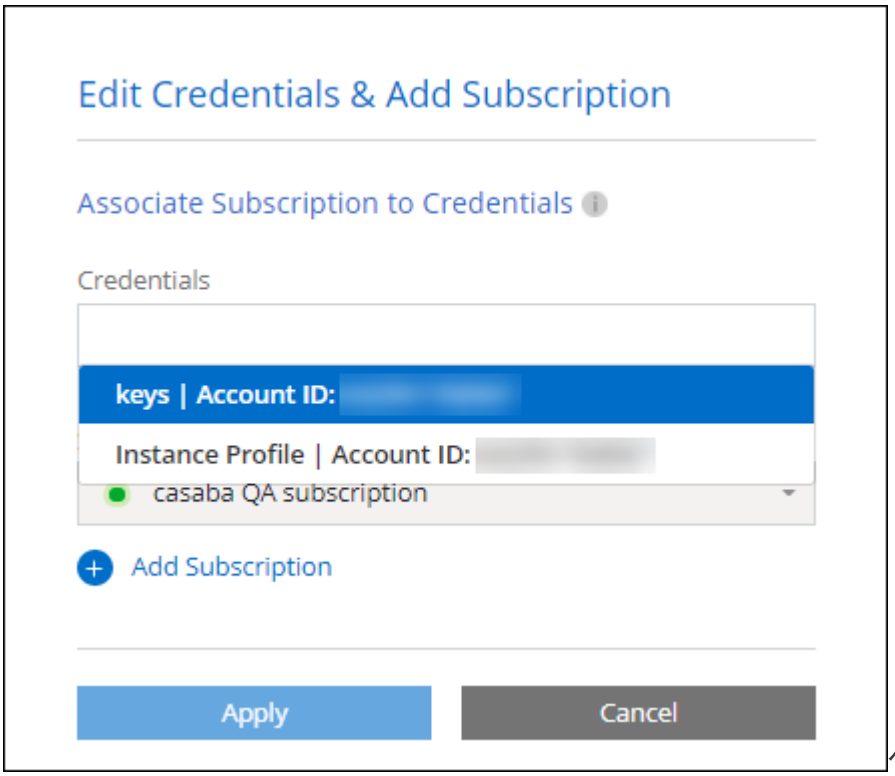
c. * Marketplace サブスクリプション *: 今すぐ登録するか、既存のサブスクリプションを選択して、Marketplace サブスクリプションをこれらの資格情報に関連付けます。

   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。

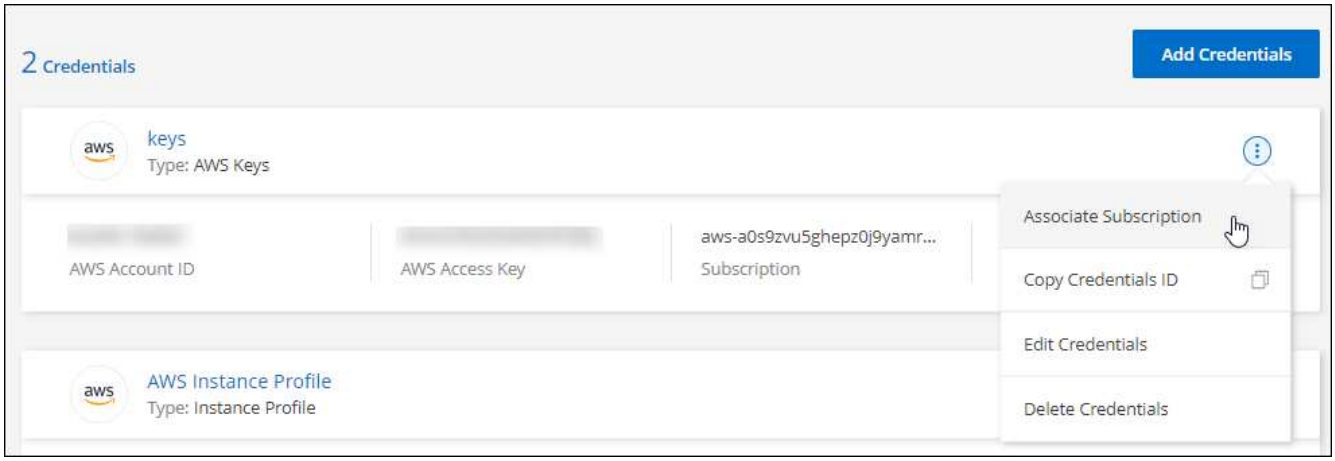
作業を開始する前に

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

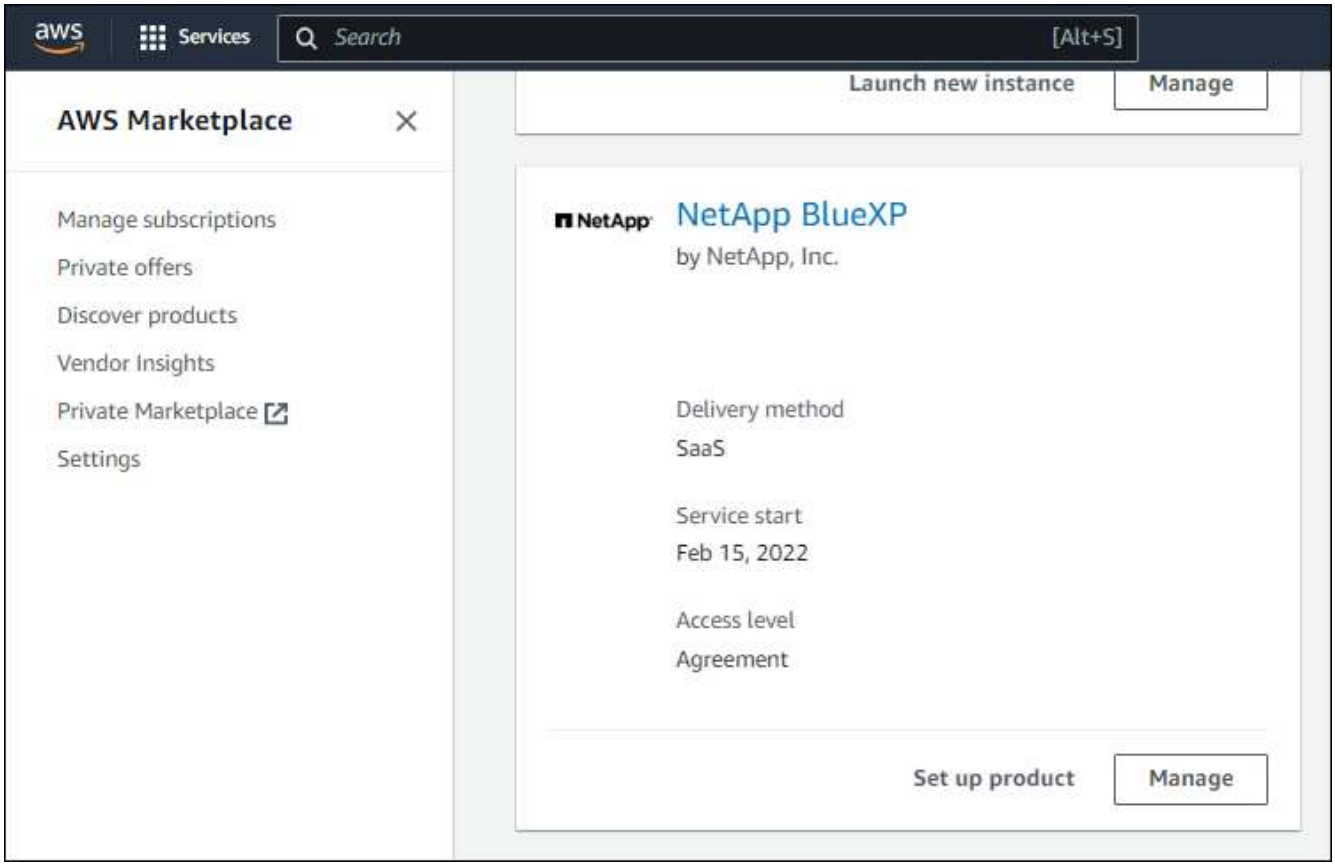
AWS MarketplaceからBlueXPにサブスクライブする際の最後の手順は、BlueXP WebサイトからBlueXPアカウントにサブスクリプションを関連付けることです。この手順を完了していない場合は、BlueXPアカウントでサブスクリプションを使用することはできません。

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。

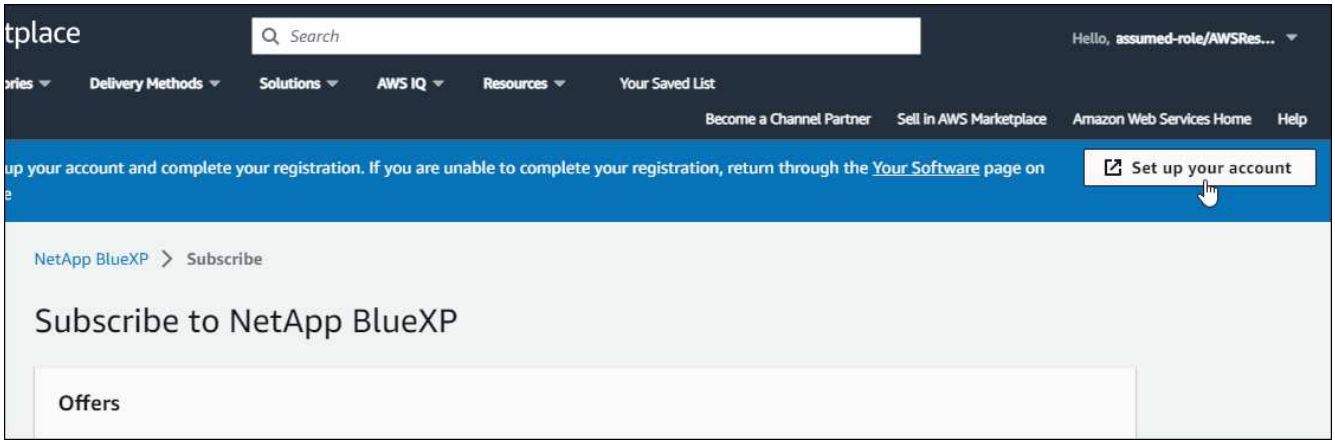
      現在表示しているアカウントに関連付けられている月額プランのみが表示されます。サブスクリプションが表示されない場合は、次の手順に進みます。
2. AWSコンソールにログインし、*[AWS Marketplace Subscriptions]*に移動します。
3. NetApp BlueXPサブスクリプションを見つけましょう。



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。

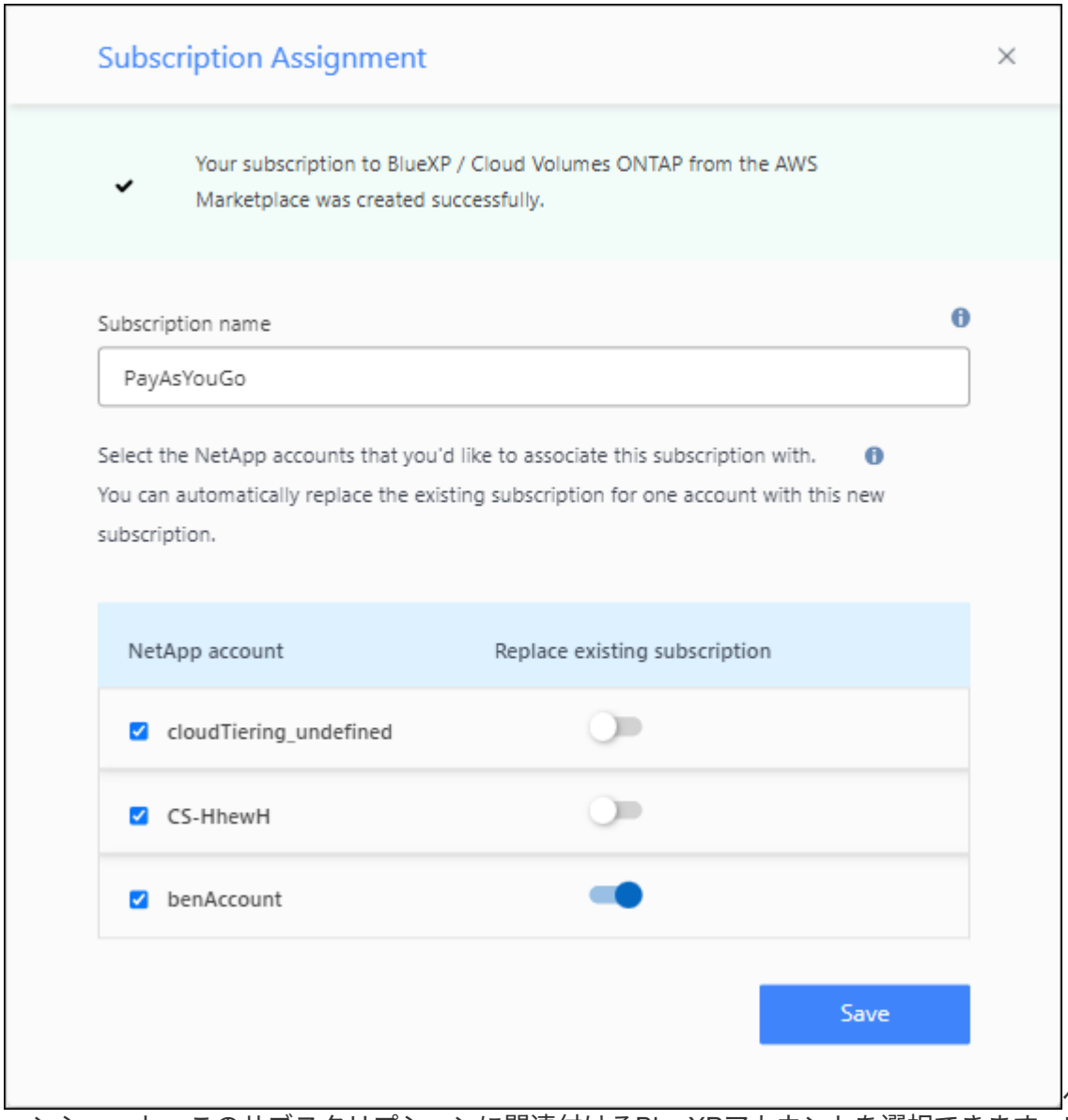
   最初にBlueXPにログインするように求められる場合があります。

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。

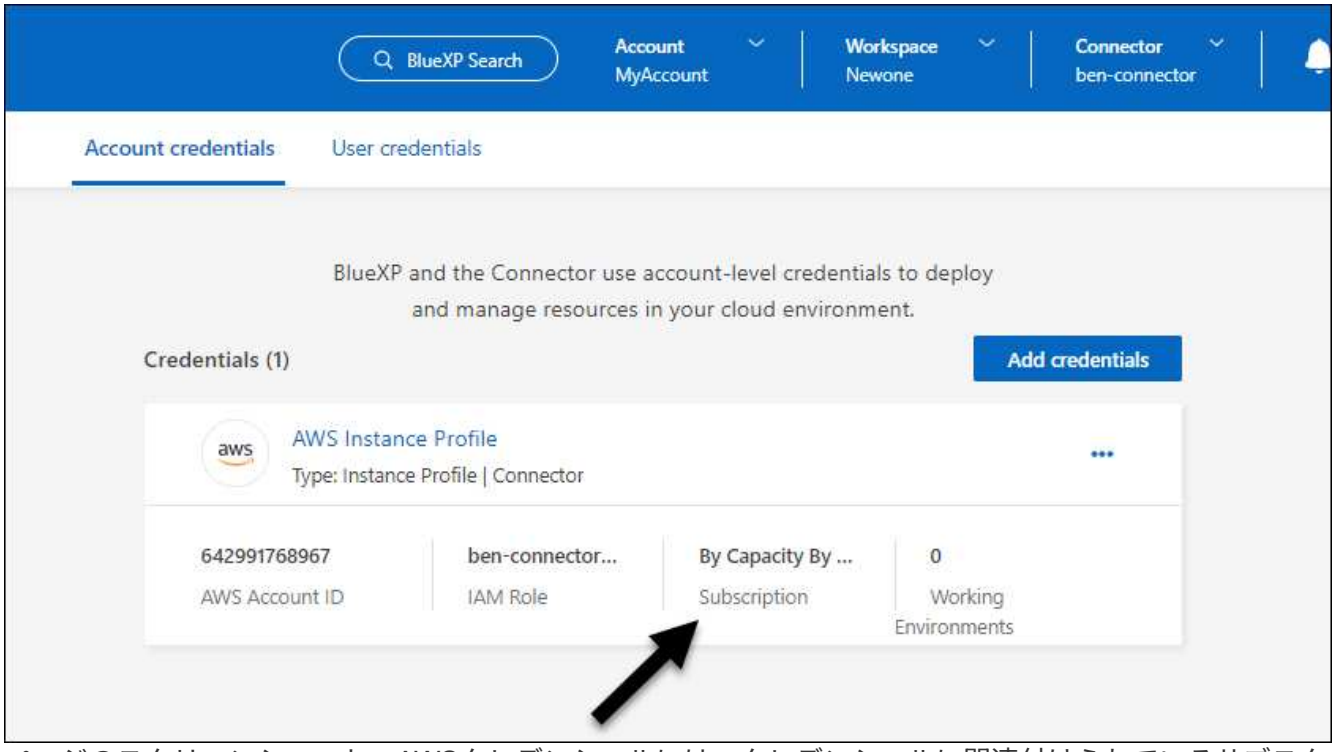
c. BlueXPサブスクリプションが表示されることを確認します。

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

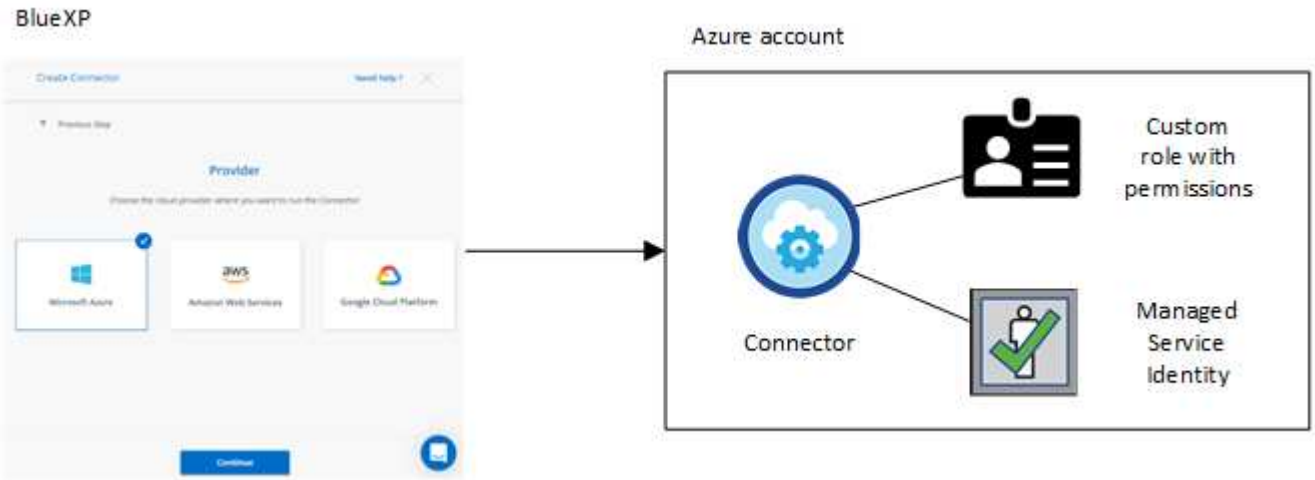
Azure のクレデンシャルと権限について説明します

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。

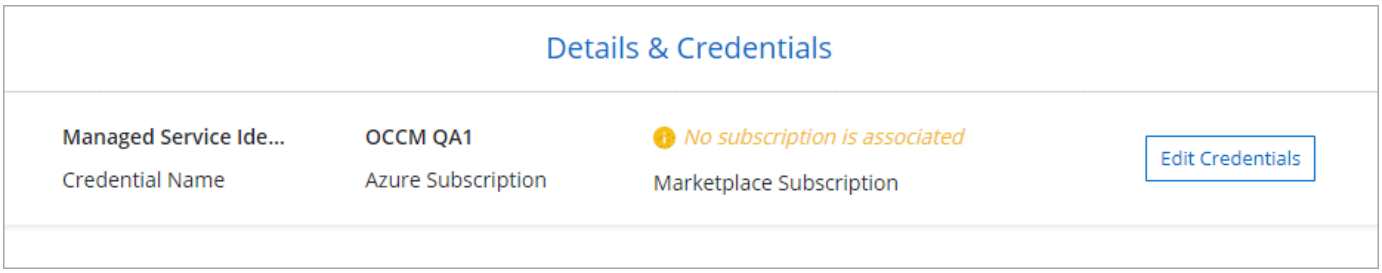
Azure の初期クレデンシャル

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。"]

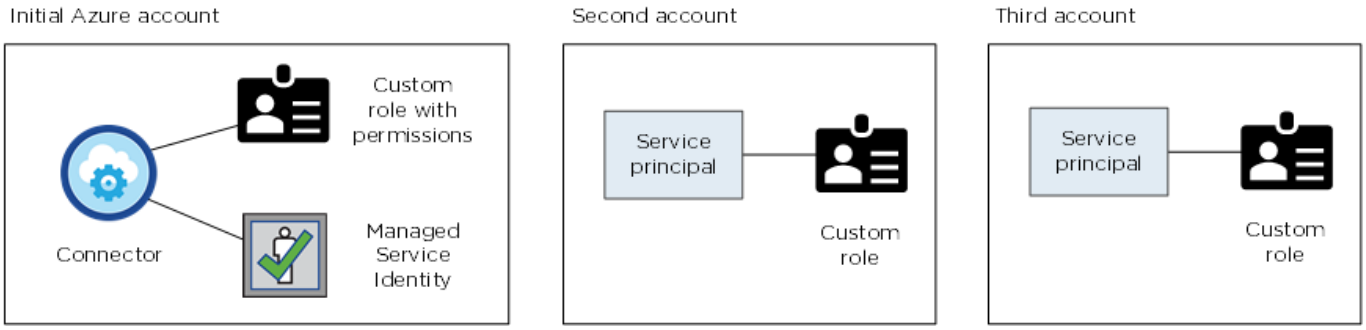
すべての Cloud Volumes ONTAP システムは、初期の Azure クレデンシャルを使用して導入することも、クレデンシャルを追加することもできます。

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"。

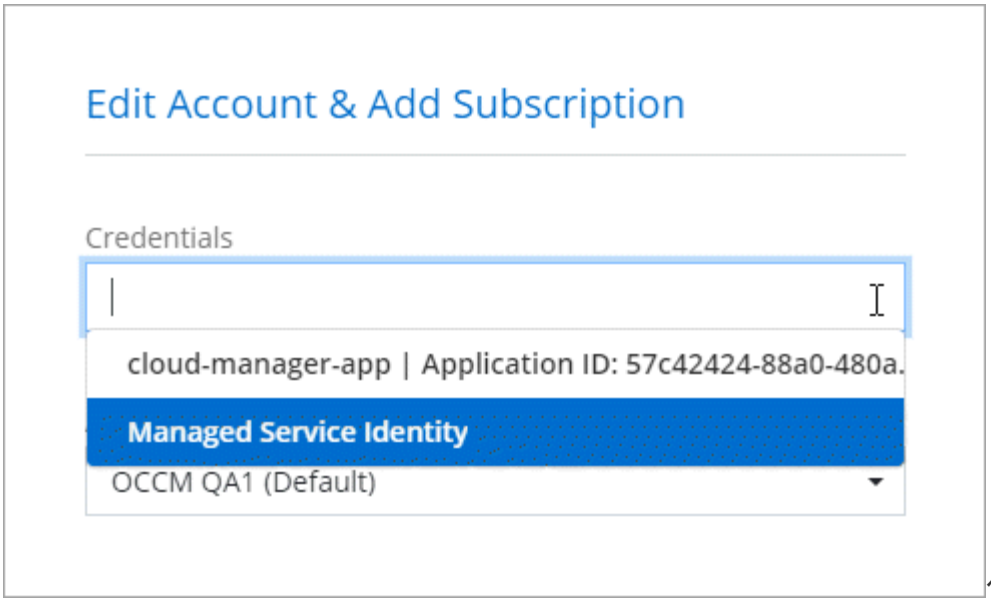
Azure の追加クレデンシャル

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

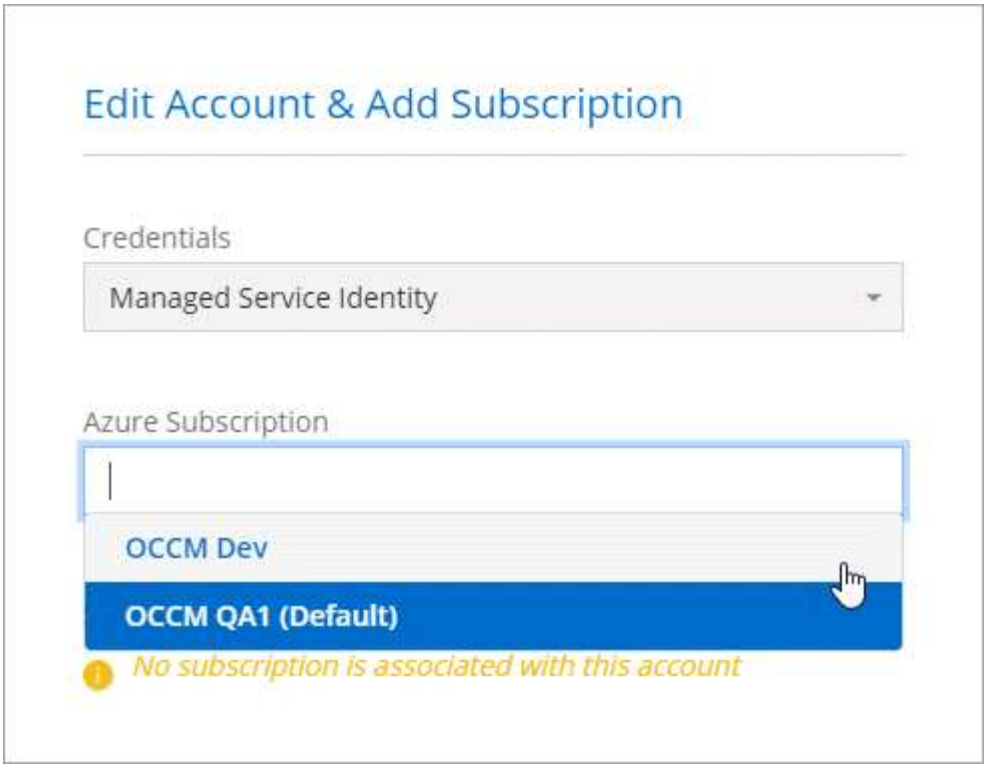
1. Azure ポータルにログインします。
2. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP を展開するサブスクリプションを選択します。
3. [Access control（IAM）]*を選択します。
   a. >[ロール割り当ての追加]*を選択し、権限を追加します。
      - BlueXP Operator *ロールを選択します。

        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"。

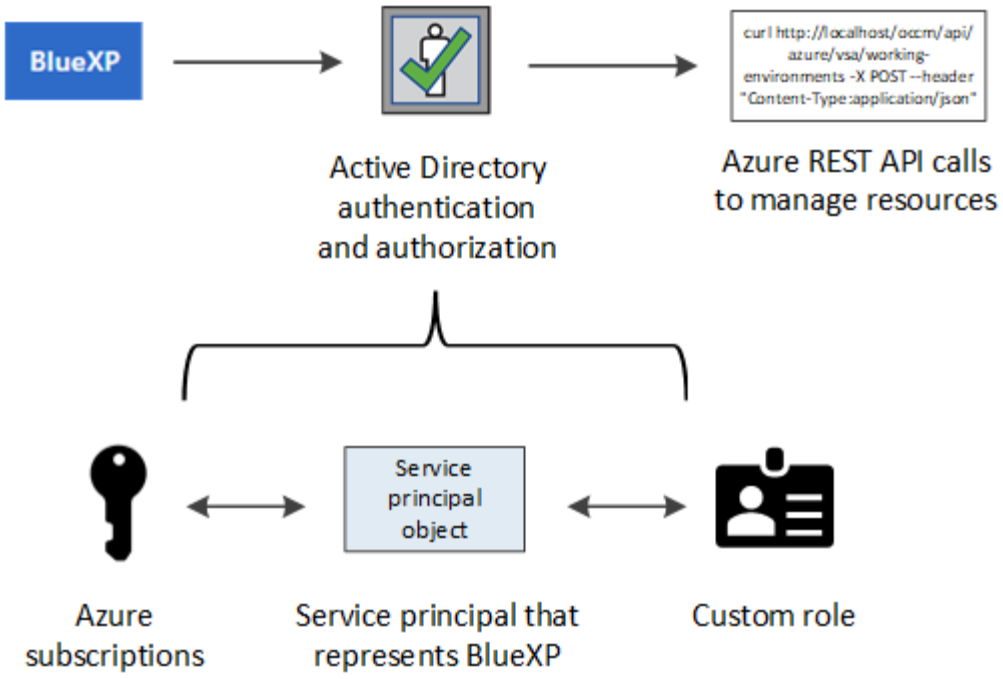
_different_azureクレデンシャルを使用してCloud Volumes ONTAPを導入する場合は、各AzureアカウントのMicrosoft Entra IDでサービスプリンシパルを作成して設定し、必要な権限を付与する必要があります。その後、新しい資格情報をBlueXPに追加できます。

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

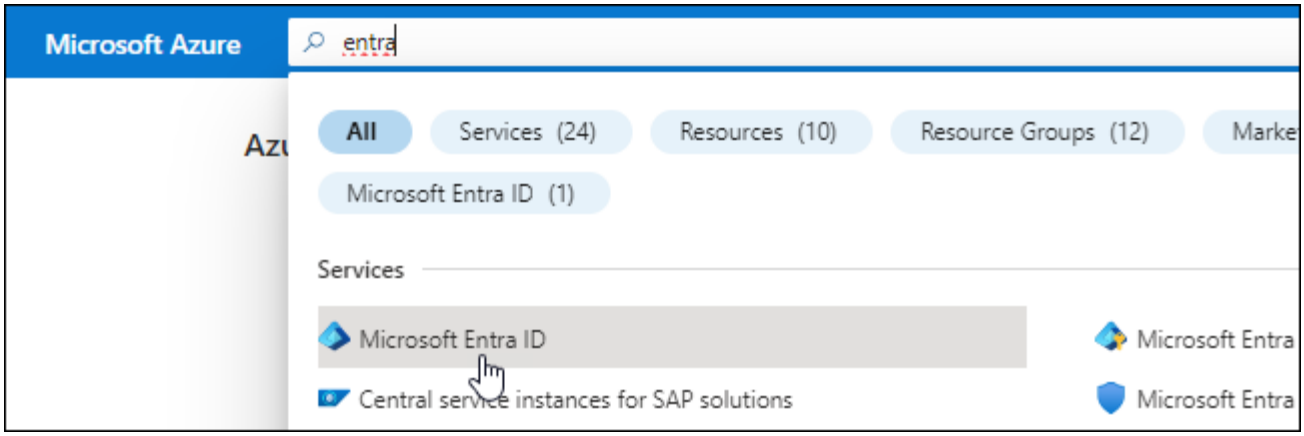
BlueXPでロールベースアクセス制御に使用できるMicrosoft Entraアプリケーションとサービスプリンシパルを作成します。

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。

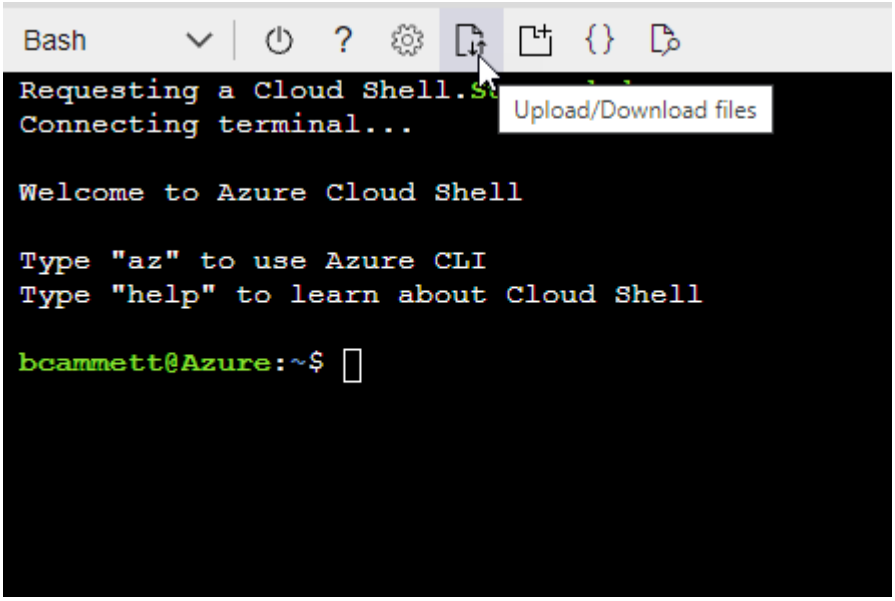
      - 例 *

```
"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。

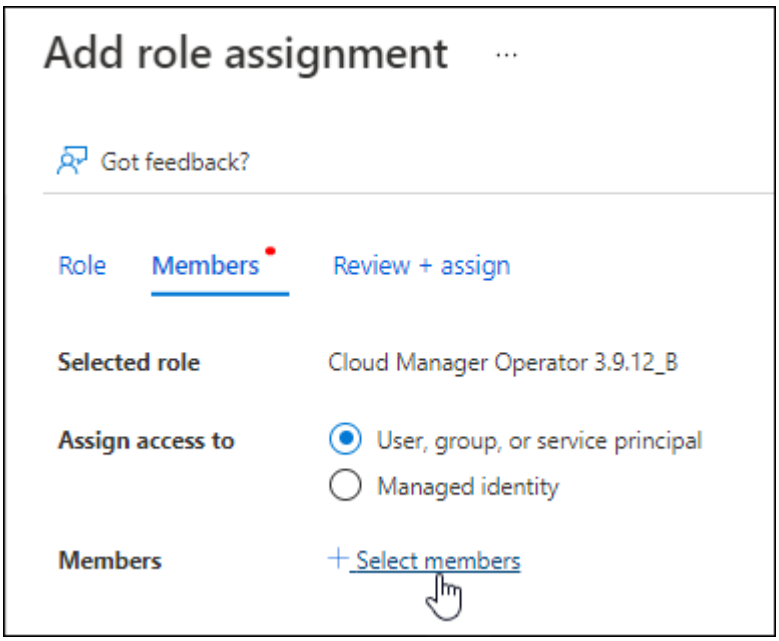
c. [アクセス制御（IAM）]>[追加]>[ロール割り当ての追加]*を選択します。

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。

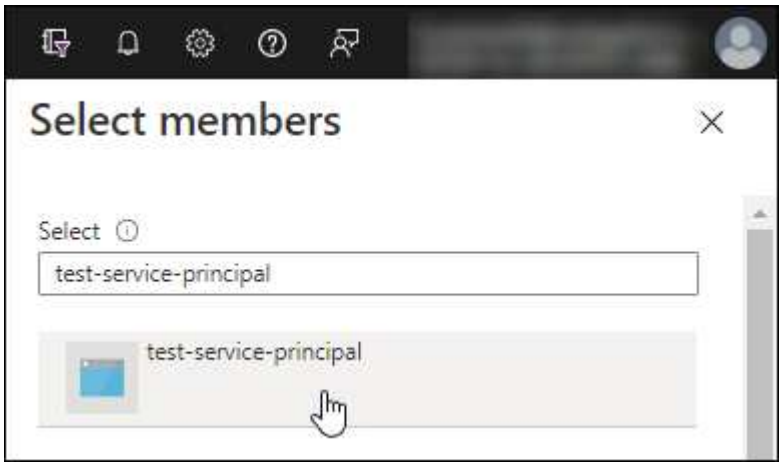
- [* ユーザー、グループ、またはサービスプリンシパル *] を選択したままにします。

- [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。

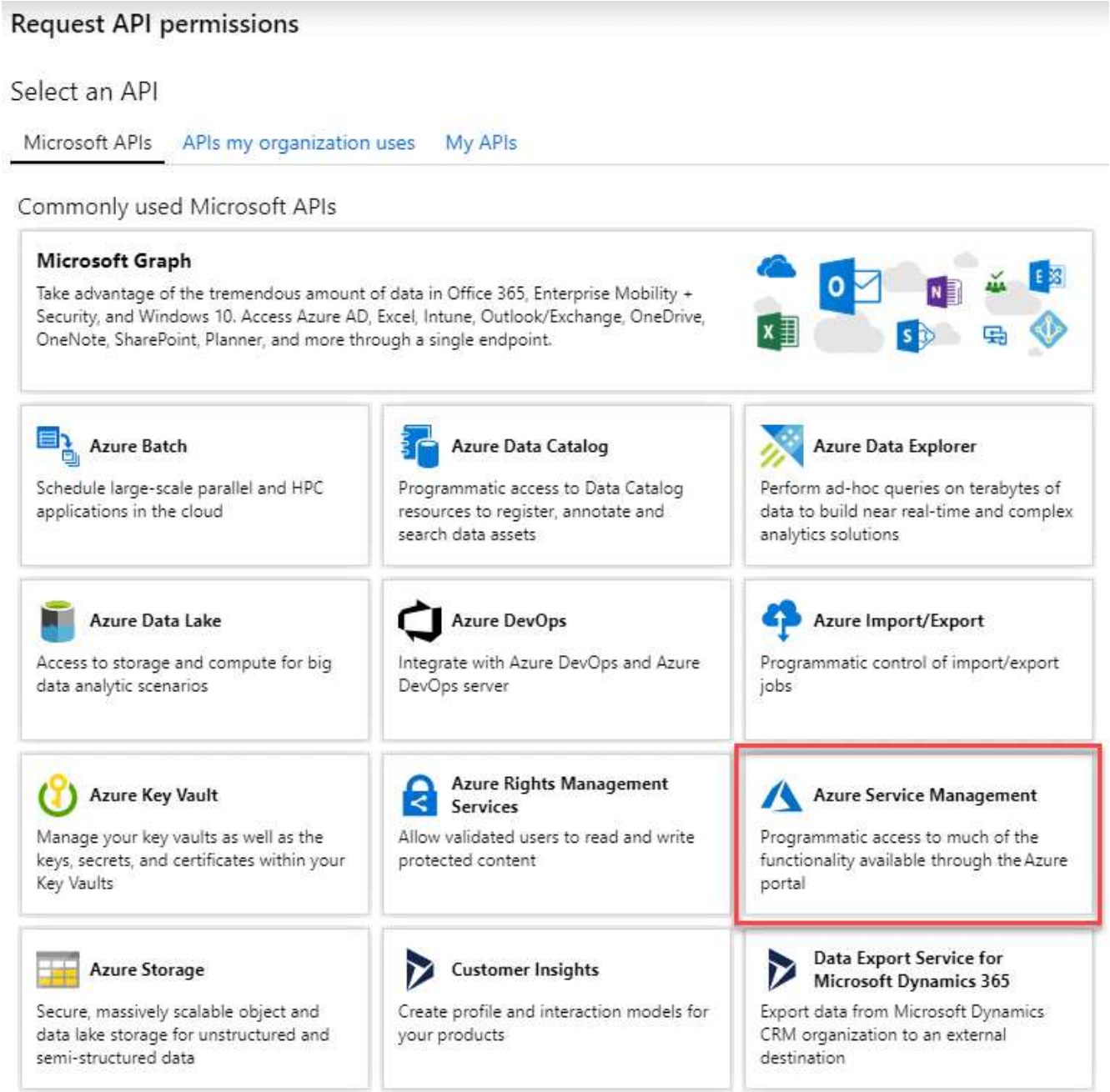
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。BlueXPを使用すると、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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

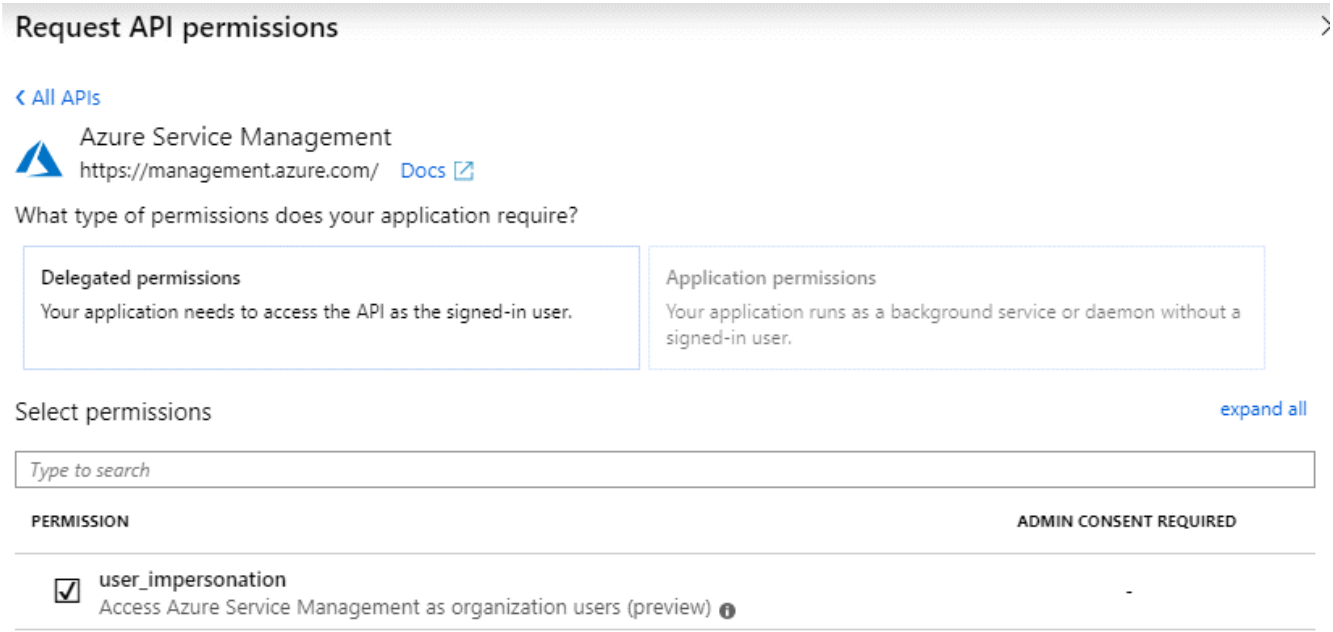
サービスプリンシパルに「 Windows Azure Service Management API 」の権限が必要です。

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。

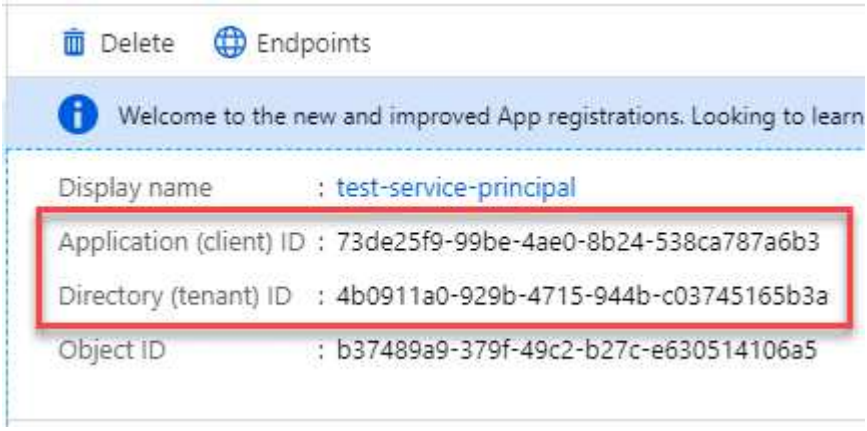


アプリケーション **ID** とディレクトリ **ID** を取得します

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。

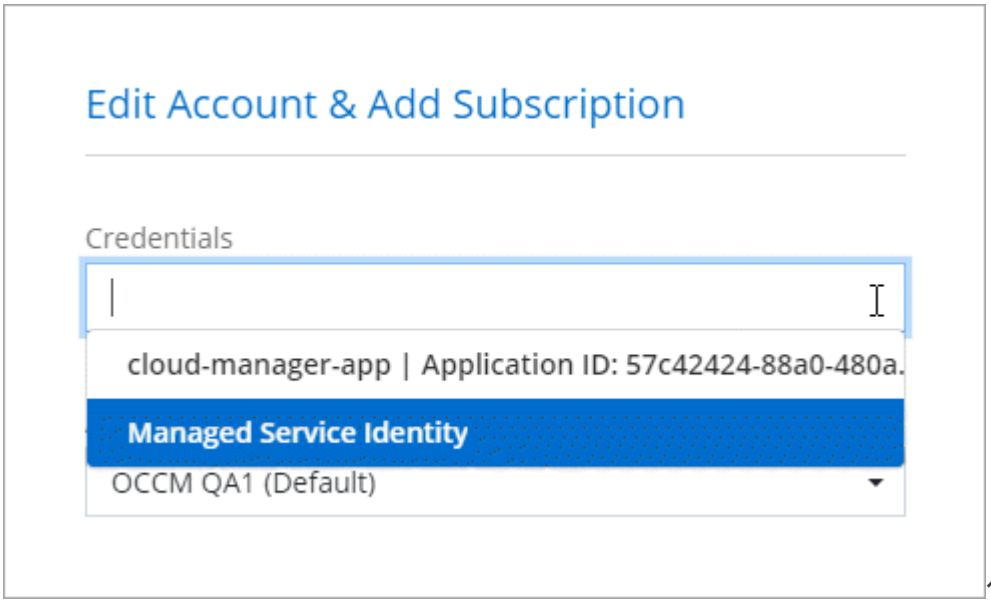
- アプリケーション（クライアント）ID
- ディレクトリ（テナント）ID
- クライアントシークレット

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。

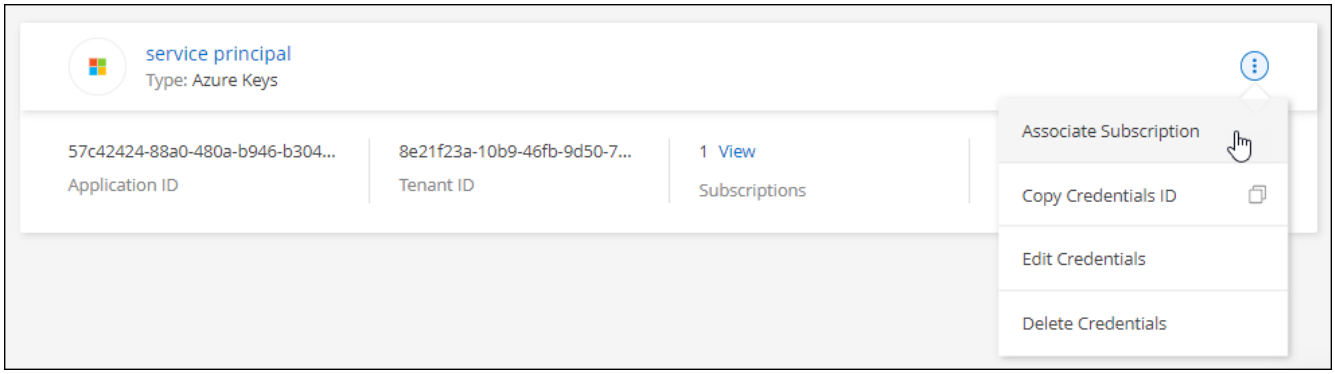
作業を開始する前に

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。

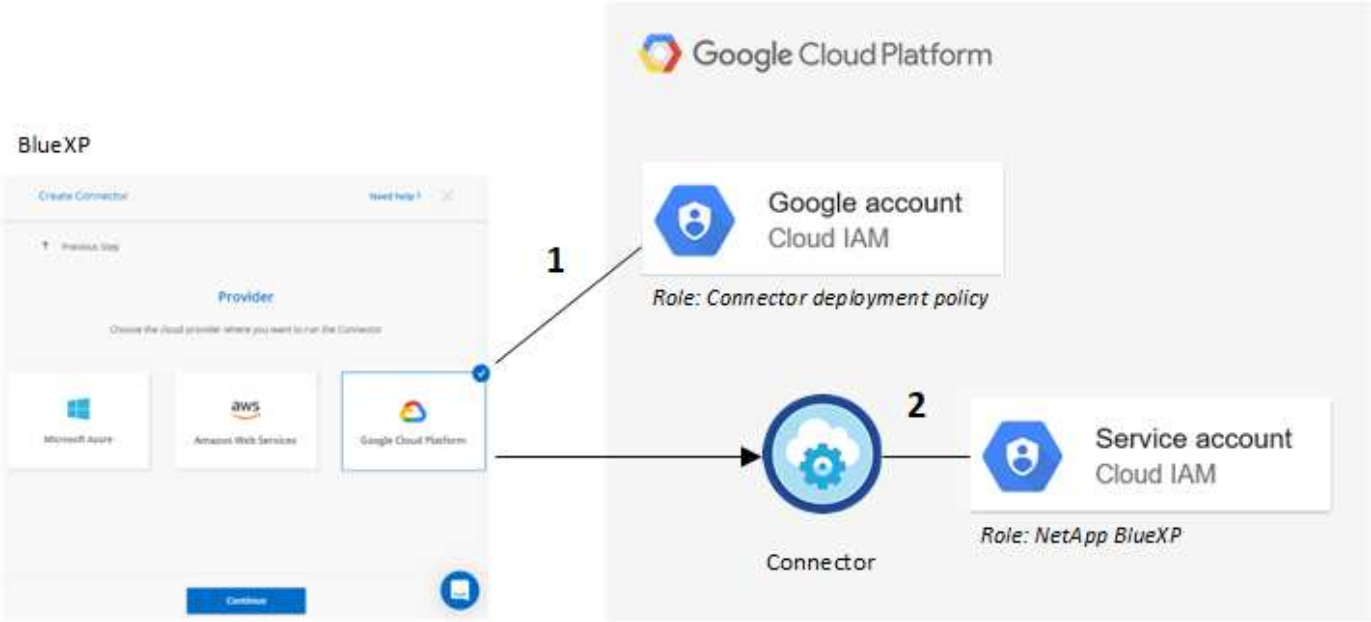
BlueXPのプロジェクトと権限

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。

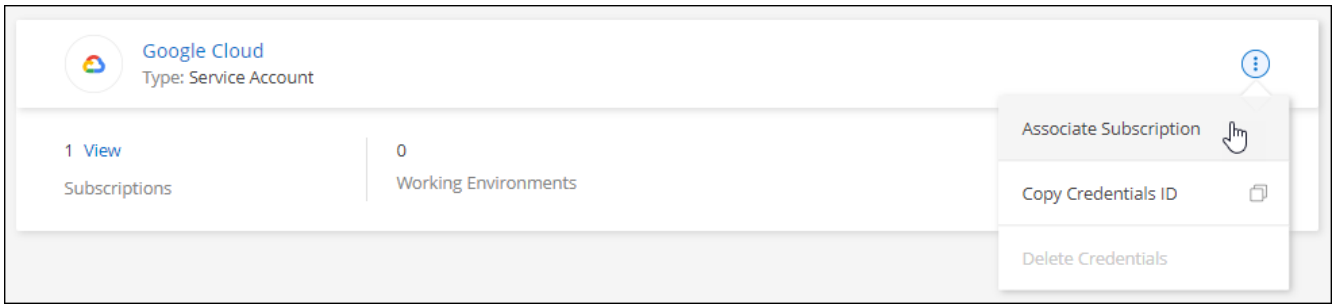
Marketplaceサブスクリプションを**Google Cloud**のクレデンシャルに関連付ける

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。

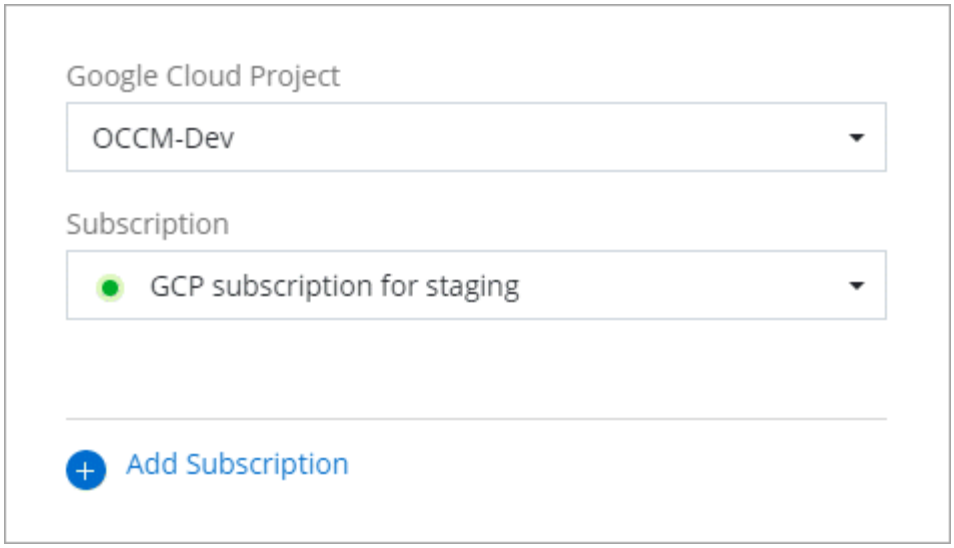
現行のMarketplaceサブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAP作業環境とすべての新規作業環境のMarketplaceサブスクリプションが変更されます。

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。



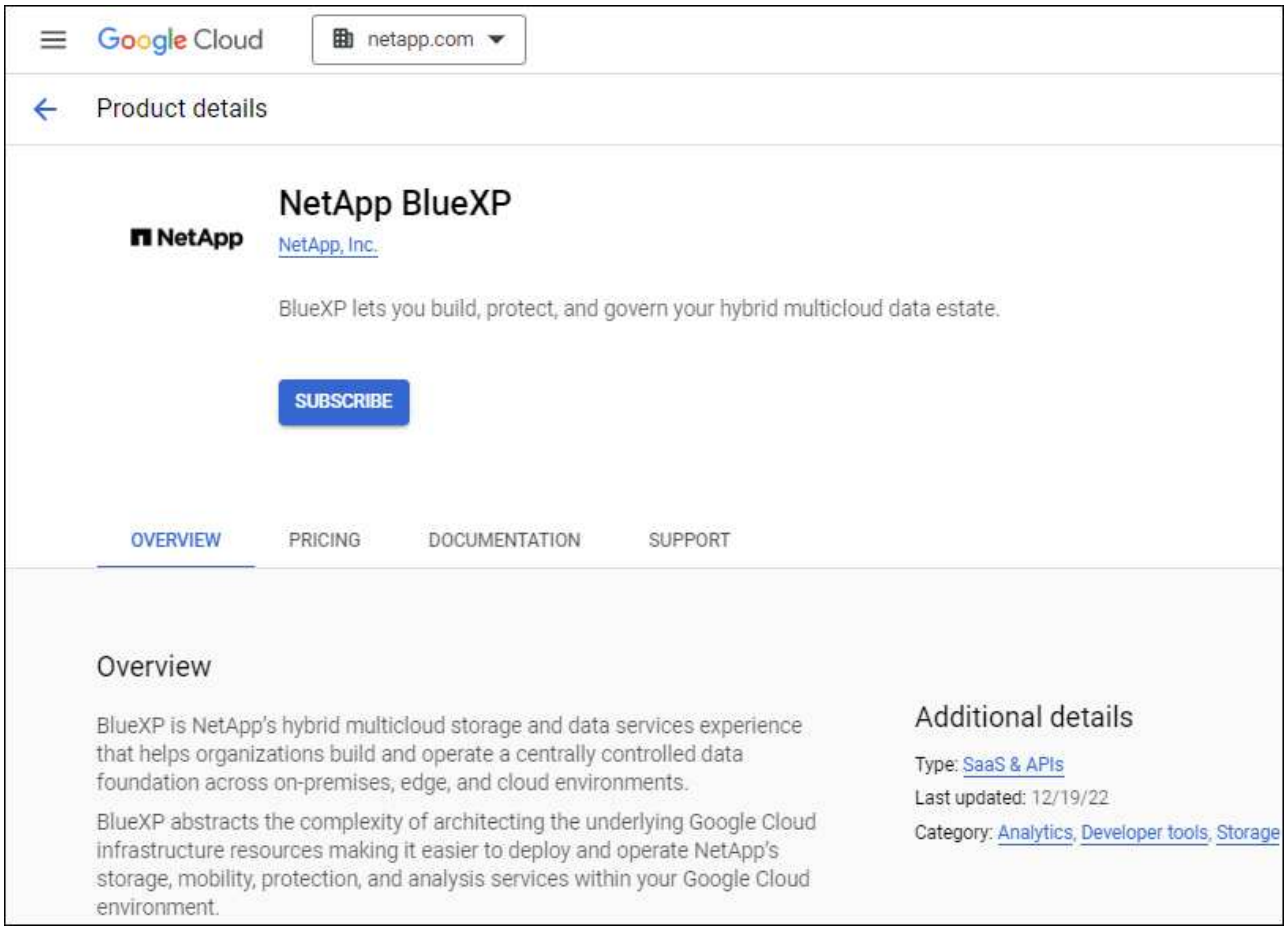
3. クレデンシャルを既存のサブスクリプションに関連付けるには、ダウンリストからGoogle Cloudプロジェクトとサブスクリプションを選択し、*[関連付け]*を選択します。



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。

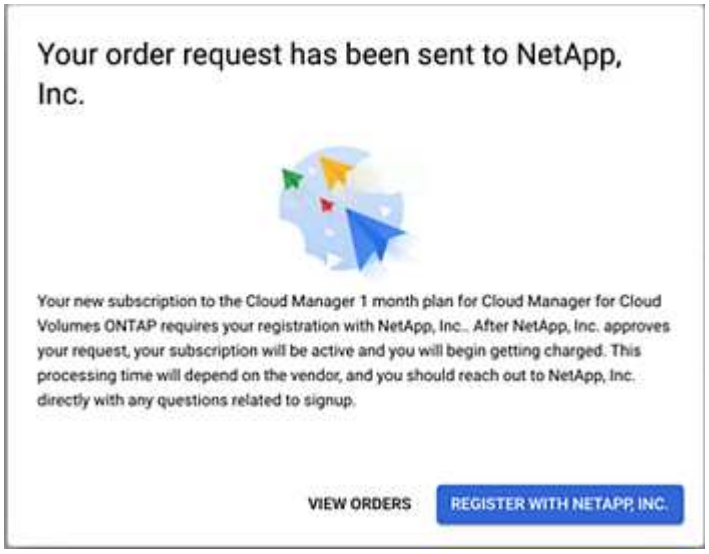
c. 適切な請求先アカウントを選択し、条件に同意します。

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。

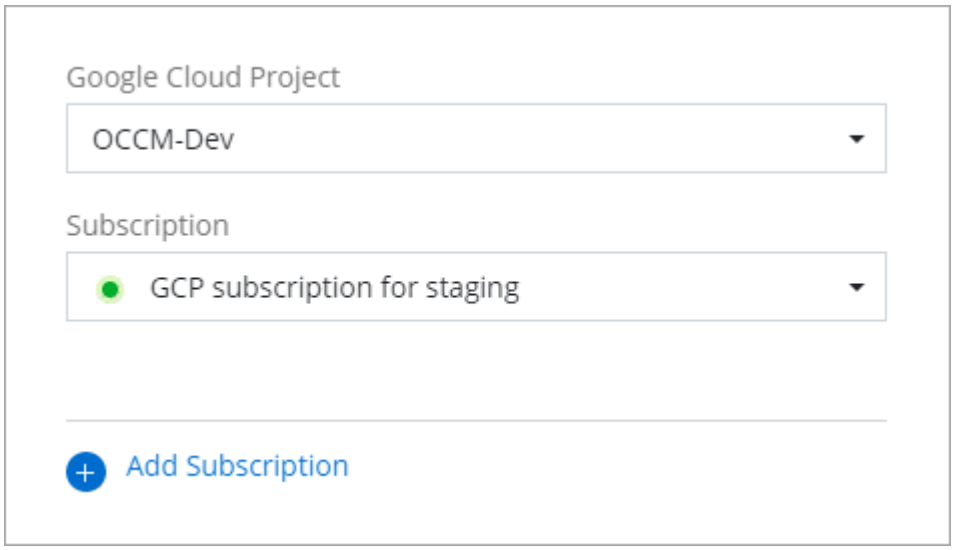
他のすべてのアカウントについては、以下の手順を繰り返して、手動で契約を関連付ける必要があります。

- [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。

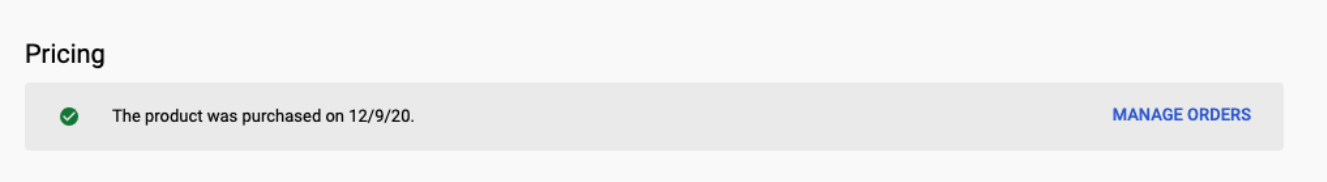


Marketplaceのサブスクリプションプロセスのトラブルシューティング

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。

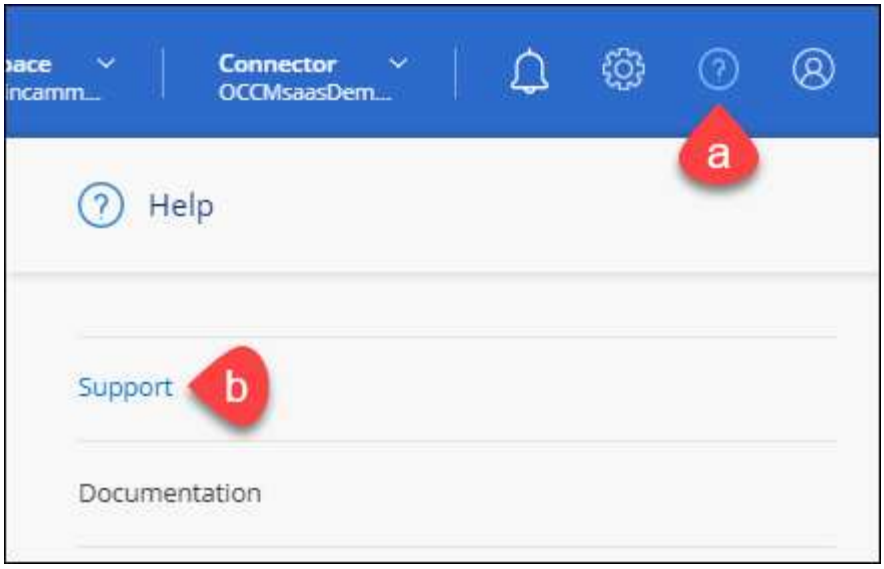
NSS アカウントを追加します

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"

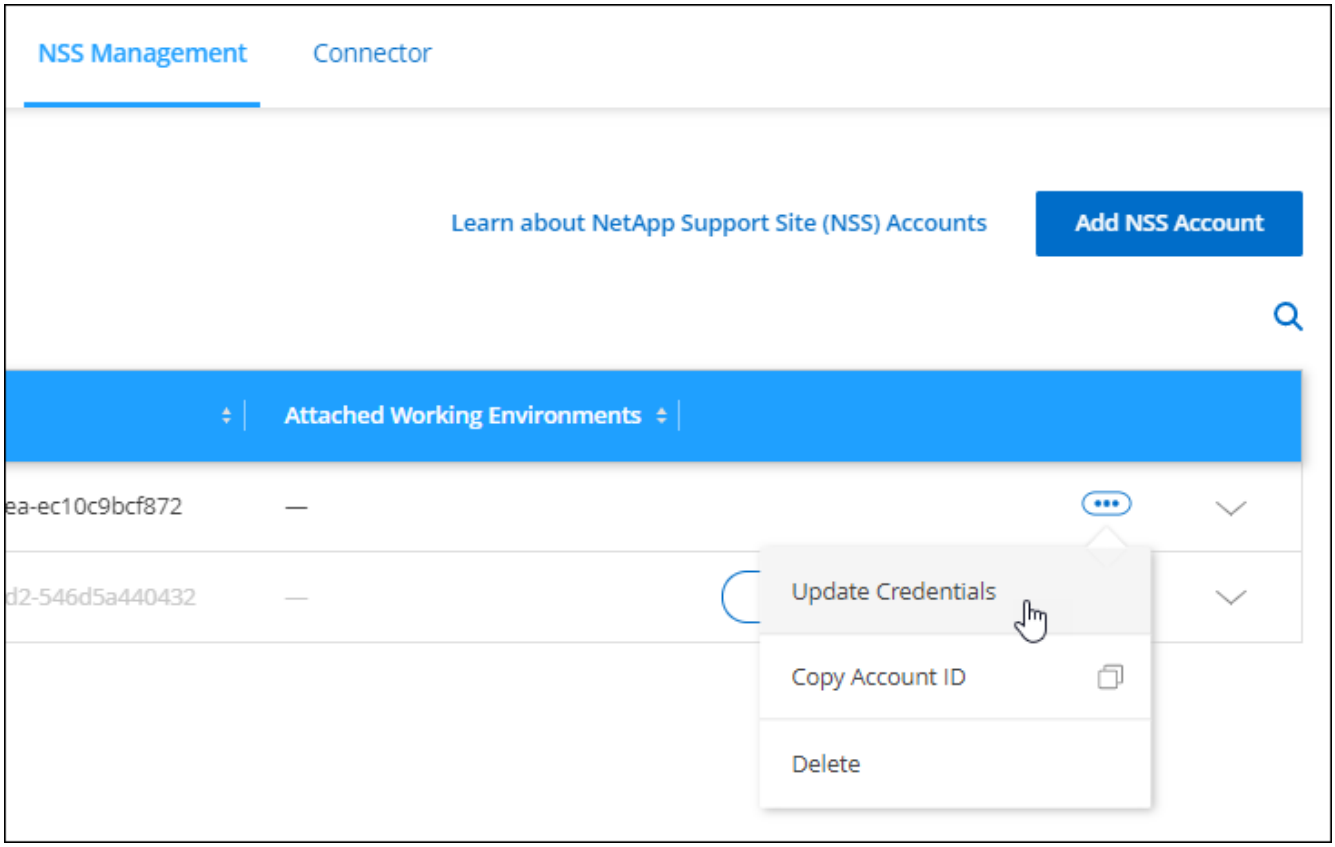
NSS クレデンシャルを更新します

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。

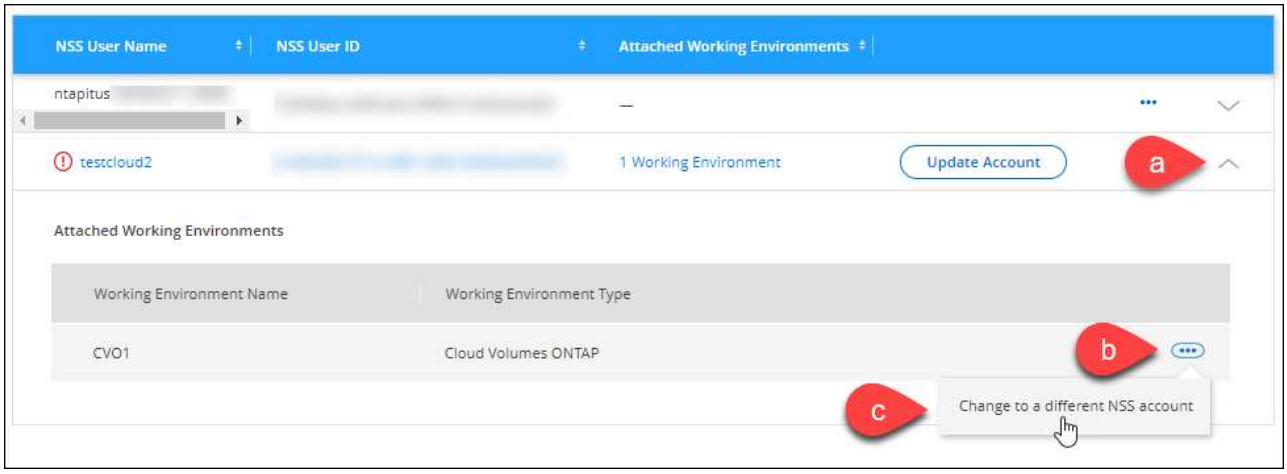
作業環境を別の **NSS** アカウントに接続します

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。

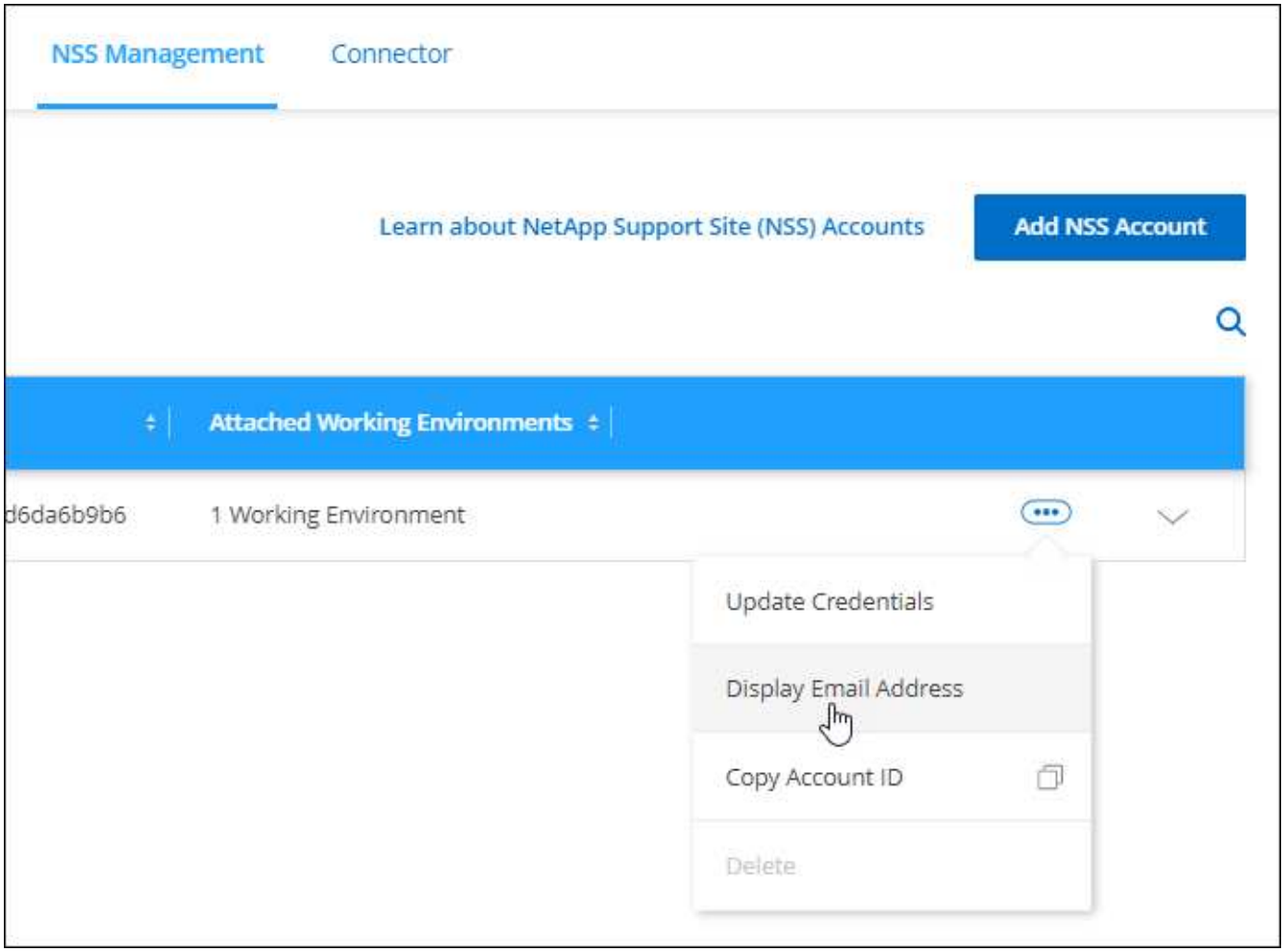
NSS アカウントの **E** メールアドレスを表示します

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。

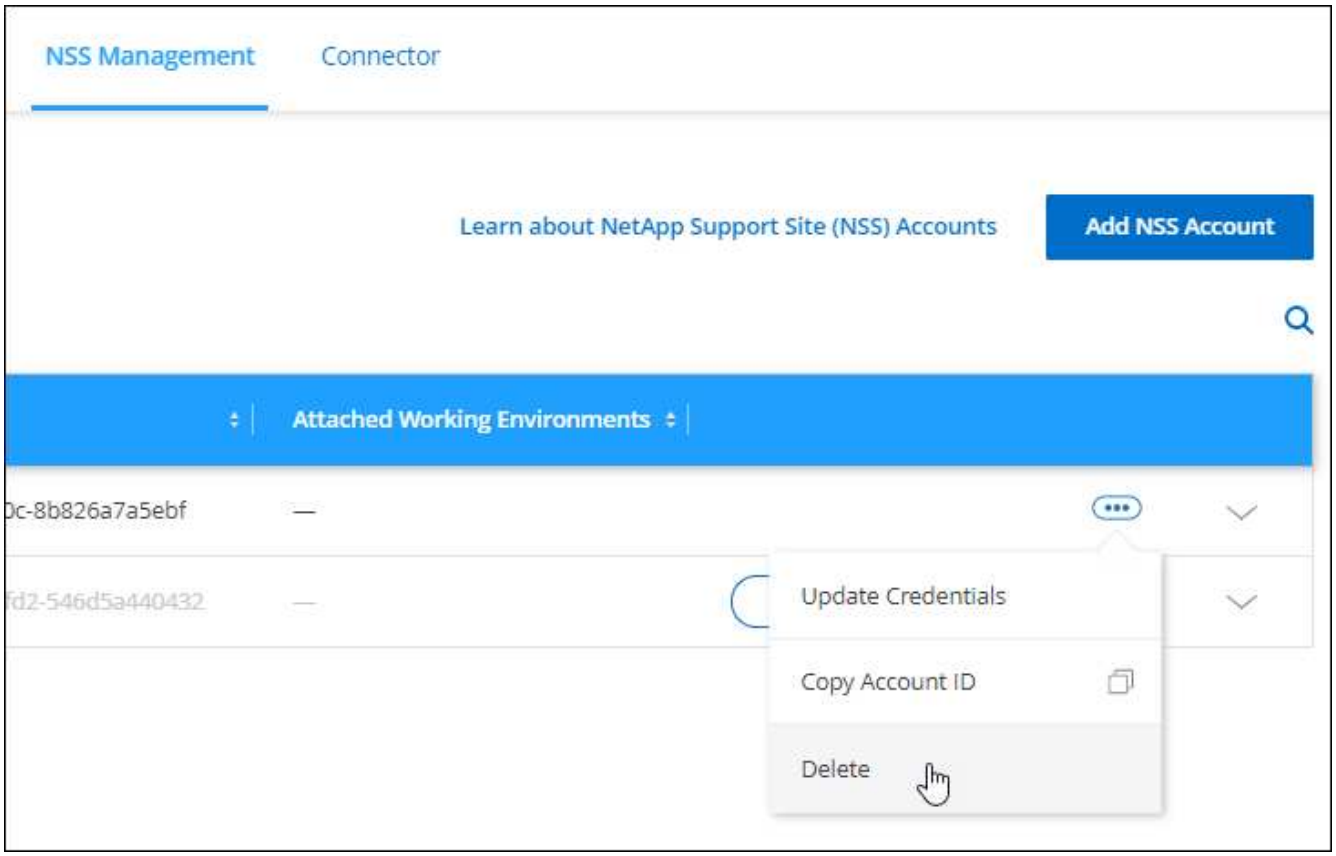
NSS アカウントを削除します

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。

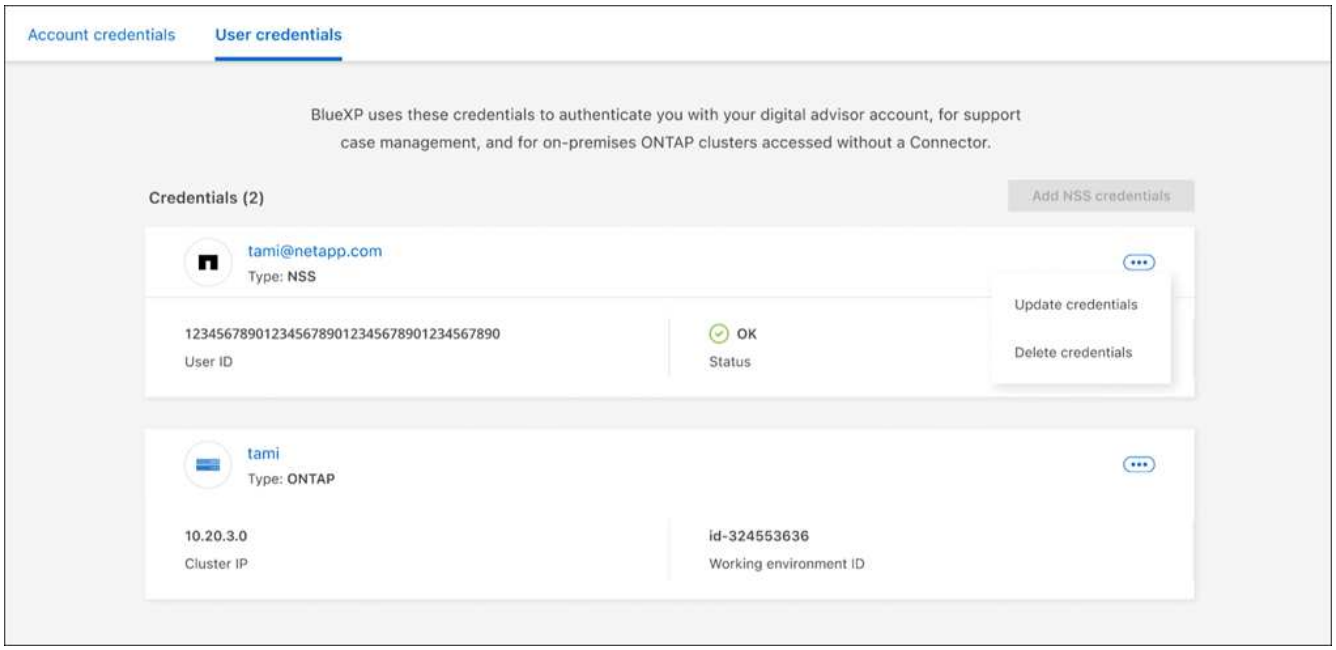
  "BlueXPアカウントでNSSクレデンシャルを使用する方法の詳細については、こちらをご覧ください"。

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。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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