コネクタ

Setup and administration

NetApp
April 26, 2024

目次

コネクタ

コネクタのシステム ID を確認します

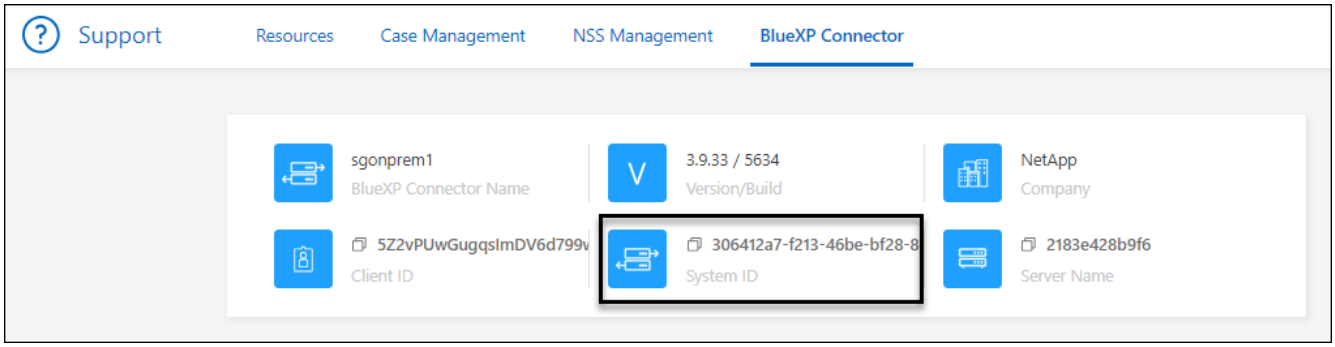
使用を開始するにあたり、ネットアップの担当者からコネクタのシステムIDを尋ねられることがあります。この ID は通常、ライセンスの取得やトラブルシューティングの目的で使用されます。

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"。

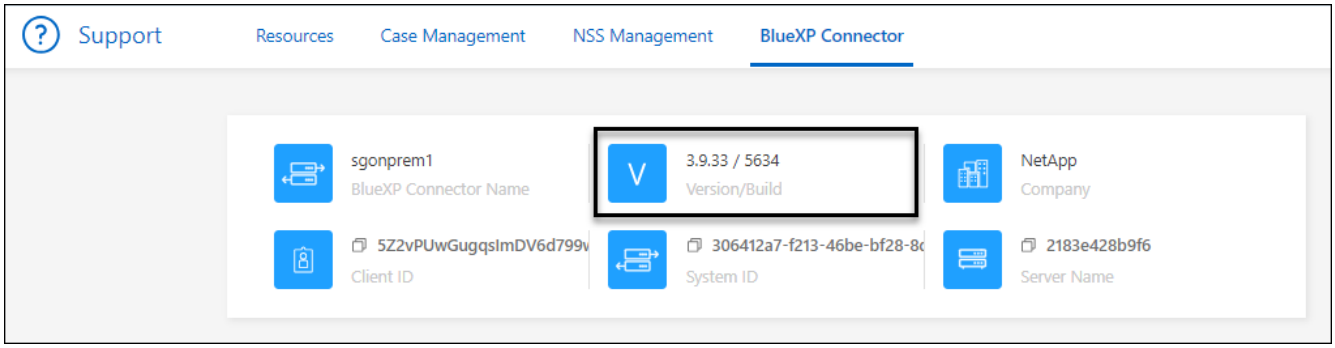
コネクタのバージョンの表示

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。



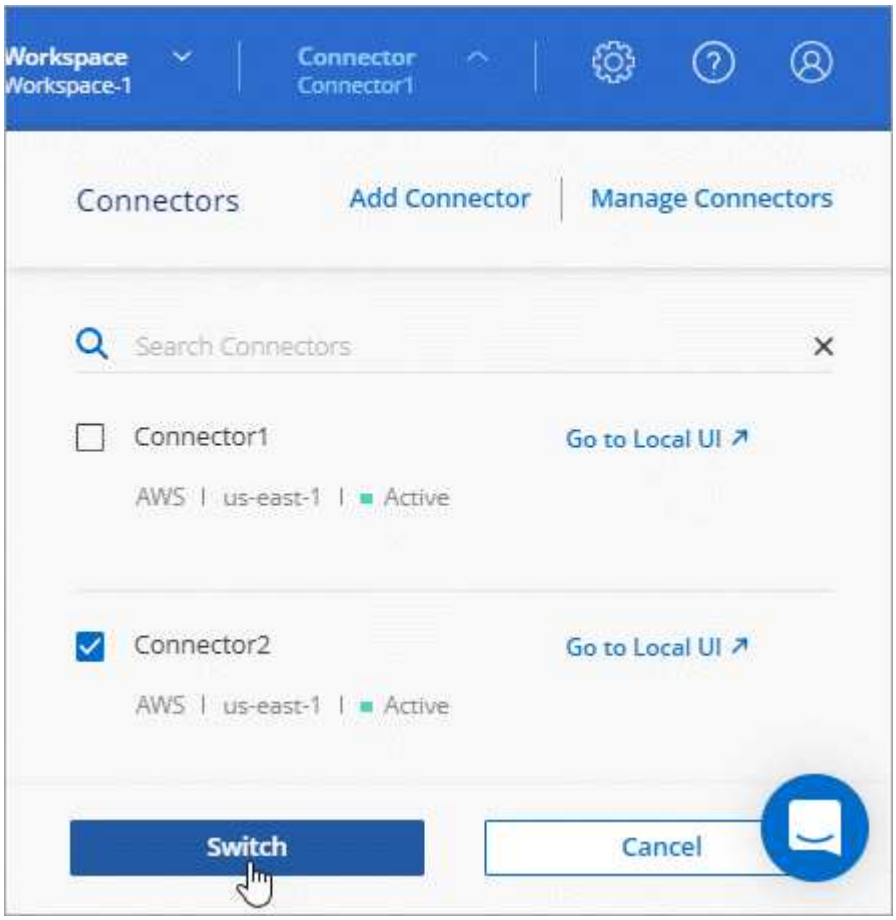
コネクタを切り替えます

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

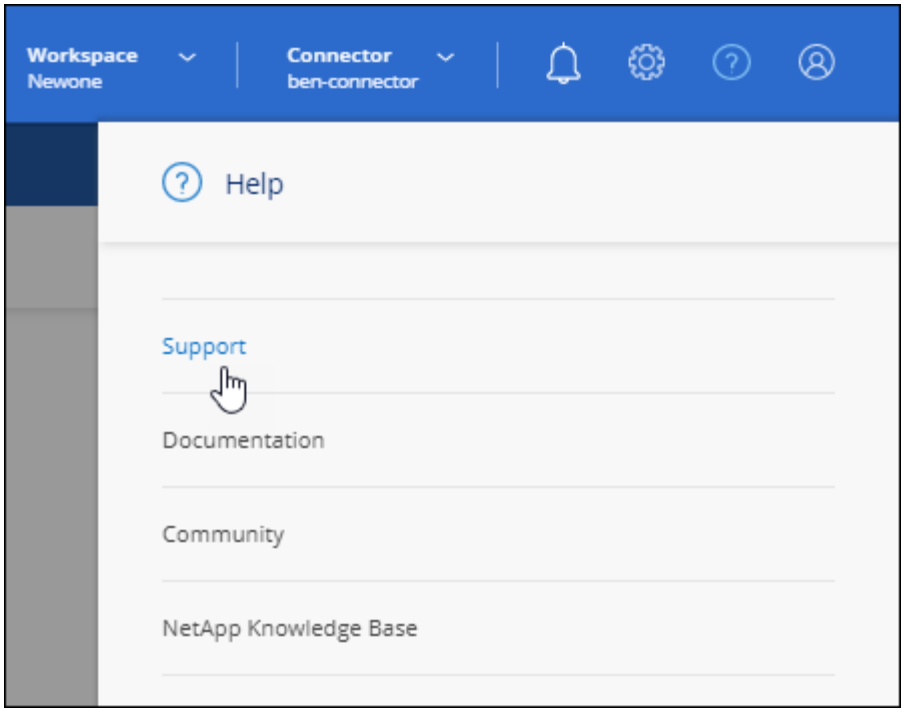
BlueXPが更新され'選択したコネクタに関連付けられている作業環境が表示されます

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。

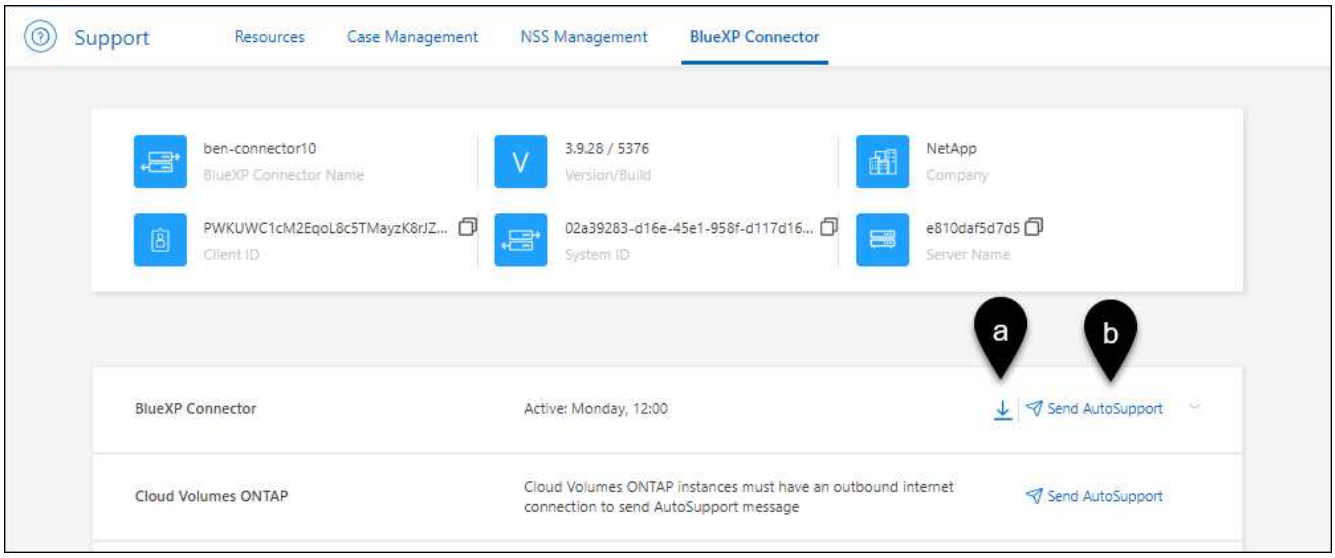
手順

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

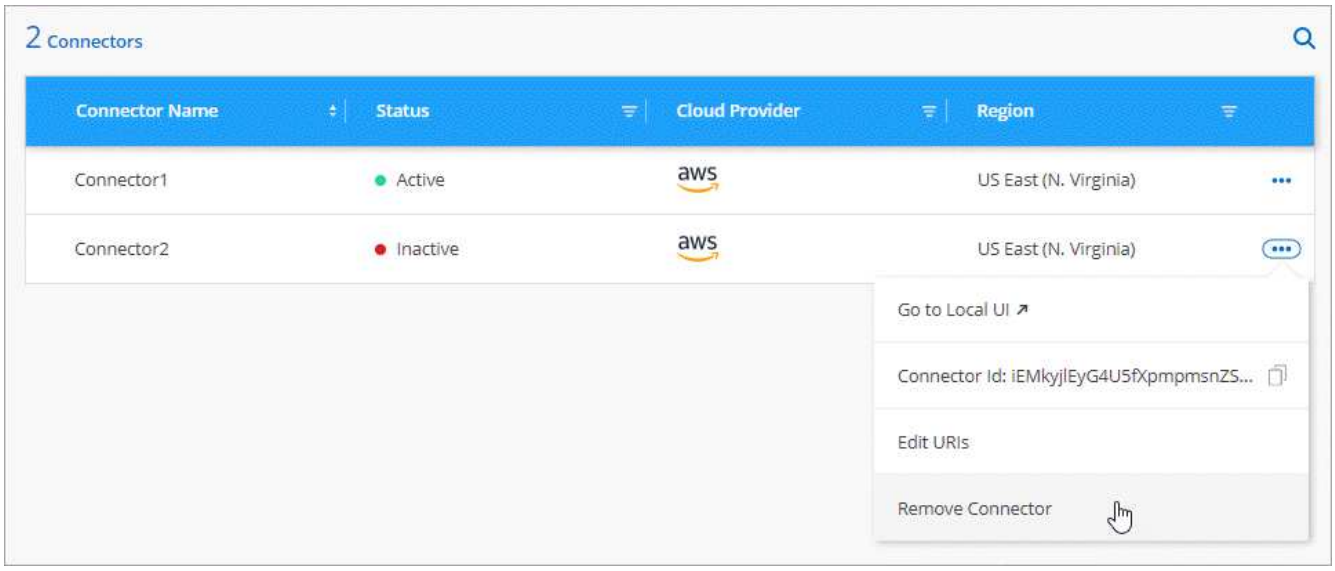
コネクタがアクティブでない場合は、BlueXPのコネクタのリストから削除できます。この処理は、Connector 仮想マシンを削除した場合や Connector ソフトウェアをアンインストールした場合に実行できます。

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

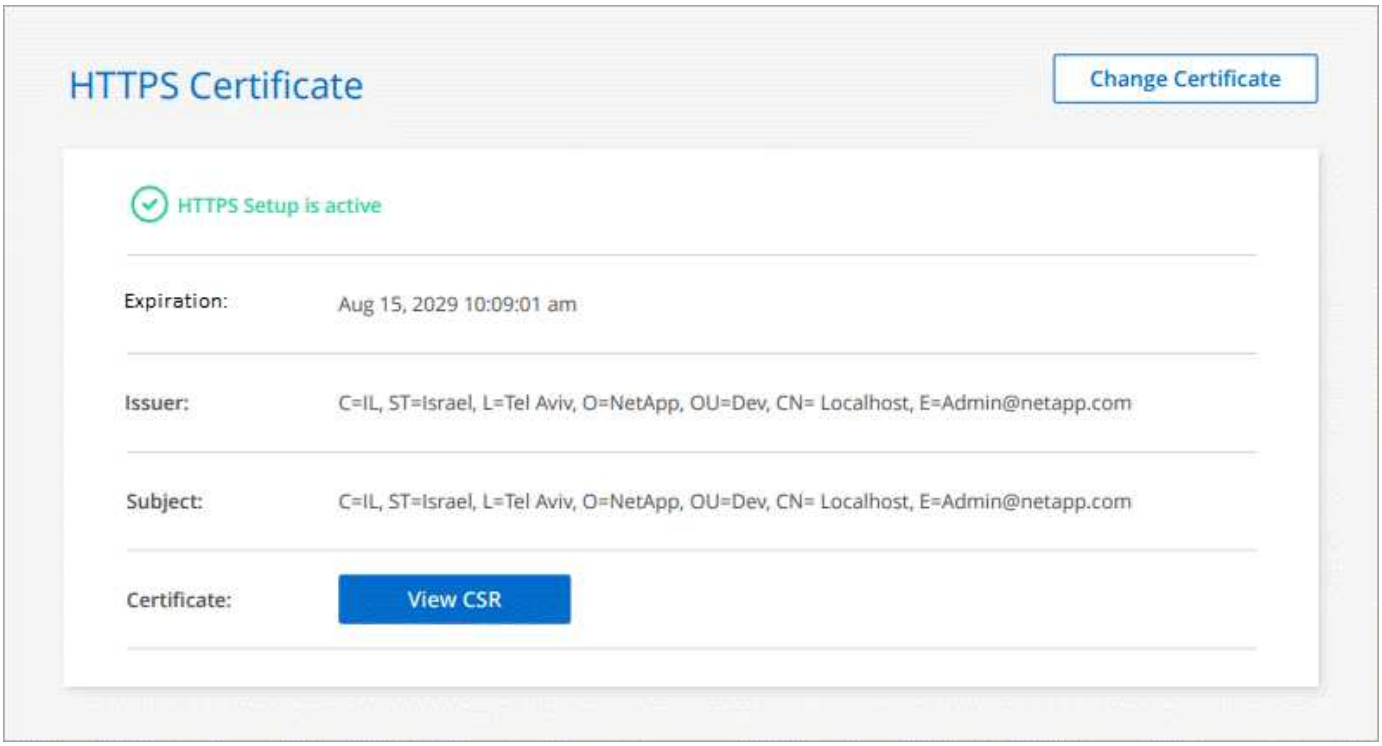
1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[HTTPSセットアップ]*を選択します。

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

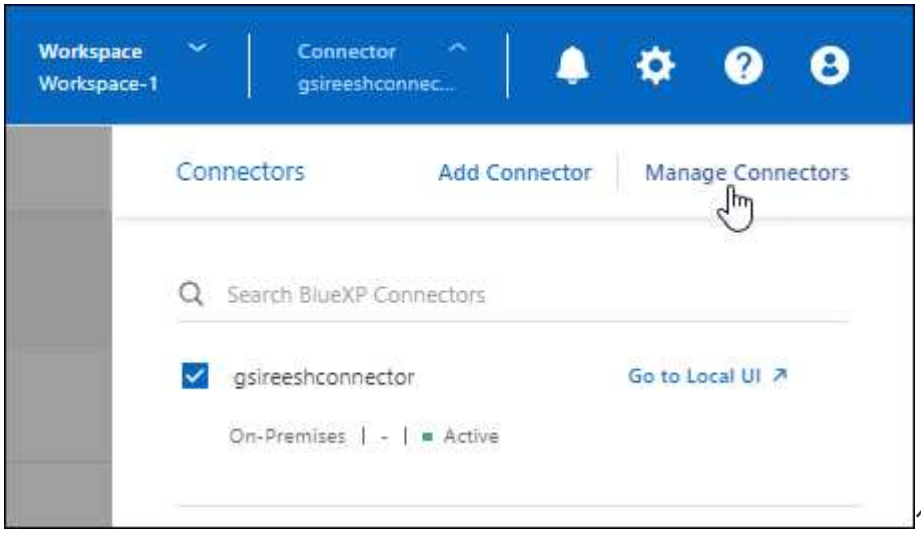
1. [BlueXPコネクタの編集]*ページに移動します。

   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

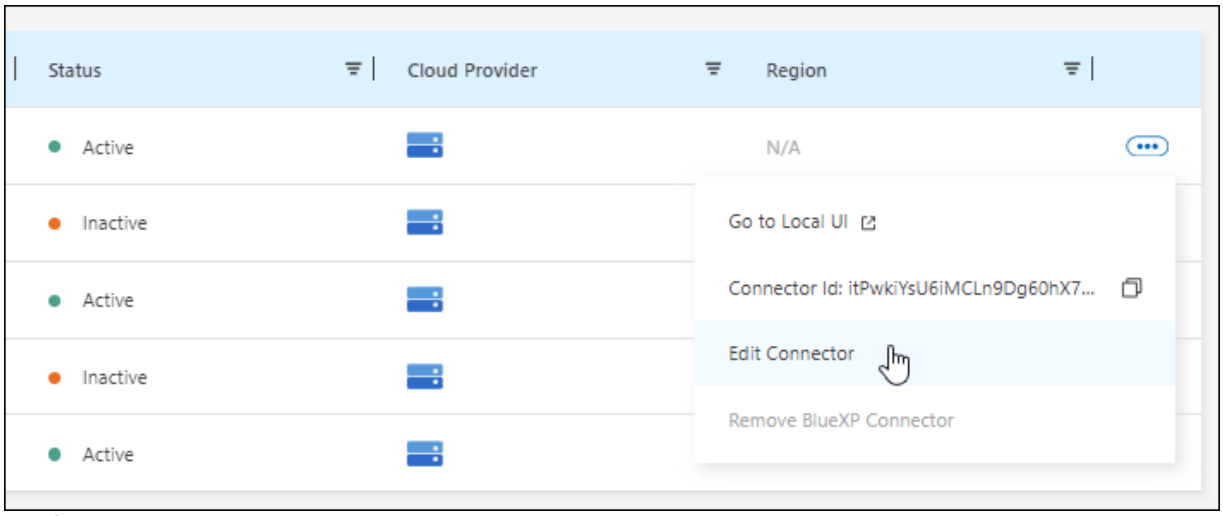
a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

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。

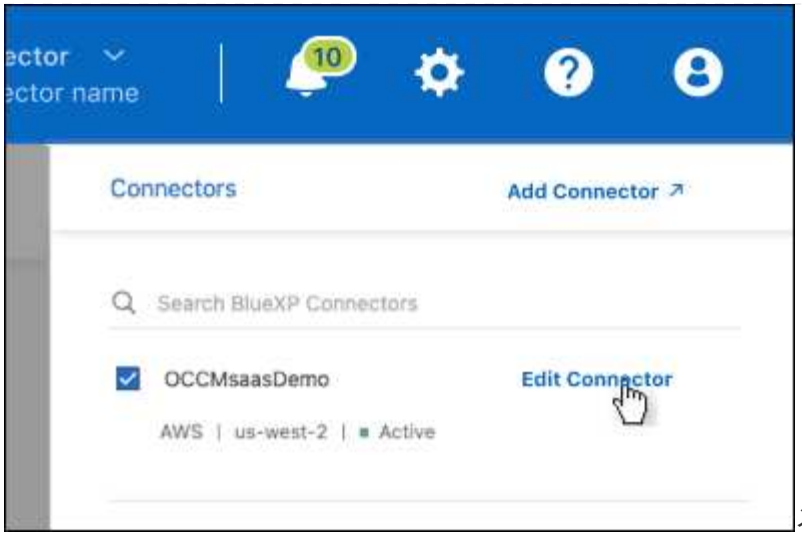


オプションを示すスクリーンショット。"]

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

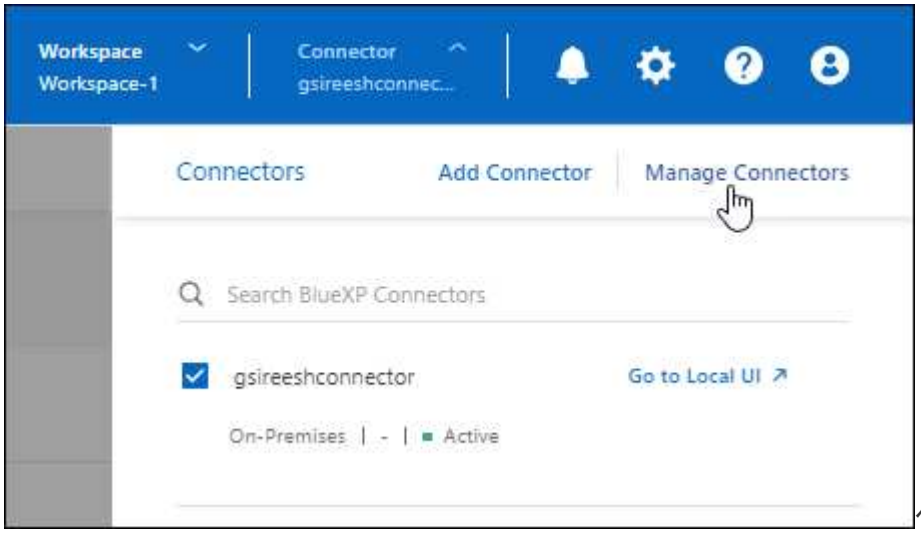
1. [BlueXPコネクタの編集]*ページに移動します。

   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

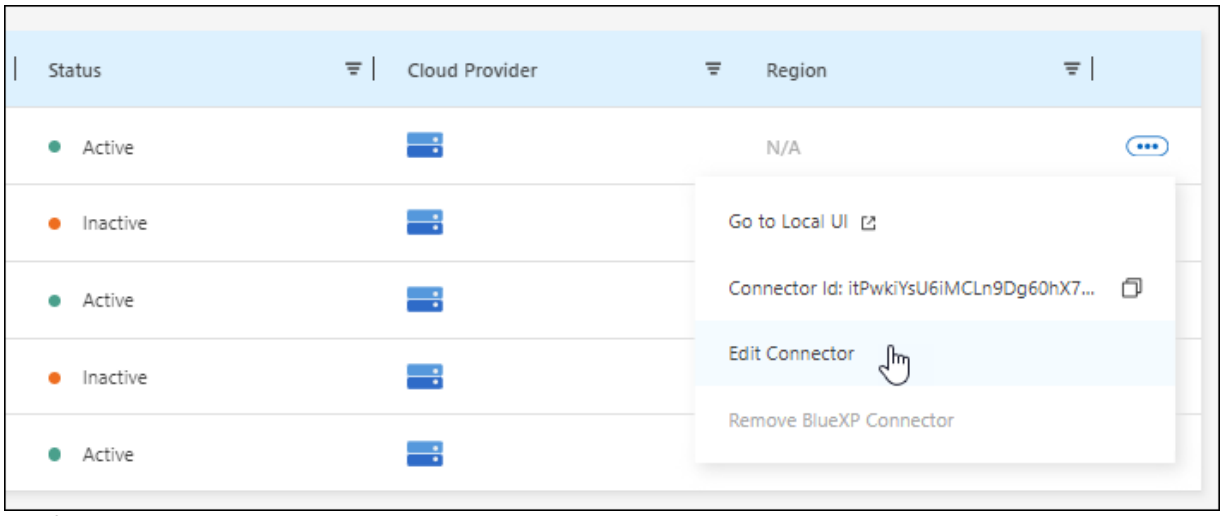
a. BlueXPヘッダーの* Connector *ドロップダウンを選択します。

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。

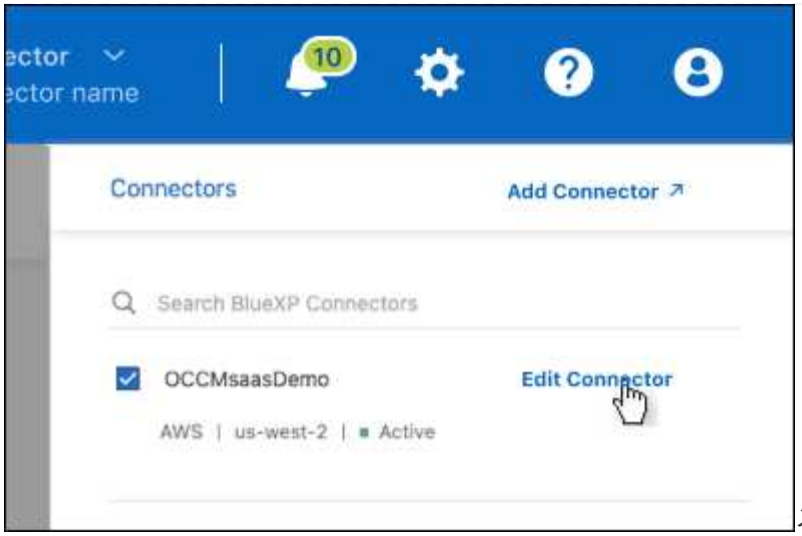


オプションを示すスクリーンショット。"]

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