



## コネクタ Set up and administration

NetApp  
May 03, 2022

# 目次

コネクタ .....	1
高度な導入 .....	1
コネクタのシステム ID の確認 .....	14
既存のコネクタの管理 .....	15
セキュアなアクセスのための HTTPS 証明書の管理 .....	23
HTTP プロキシサーバを使用するためのコネクタの設定 .....	25
コネクタのデフォルト設定 .....	27

# コネクタ

## 高度な導入

### AWS Marketplace からコネクタを作成します

Cloud Manager からコネクタを直接作成することを推奨します。AWS アクセスキーを指定しない場合は、AWS Marketplace からコネクタを起動できます。Connector の作成とセットアップが完了すると、新しい作業環境を作成するときに、Cloud Manager によって自動的に Connector が使用されます。

#### 手順

1. EC2 インスタンス用の IAM ポリシーとロールを作成します。
  - a. 次のサイトから Cloud Manager IAM ポリシーをダウンロードします。  
  
"NetApp Cloud Manager : AWS 、 Azure 、 GCP ポリシー"
  - b. IAM コンソールから、Cloud Manager IAM ポリシーからテキストをコピーアンドペーストして、独自のポリシーを作成します。
  - c. ロールタイプが Amazon EC2 の IAM ロールを作成し、前の手順で作成したポリシーをロールに付加します。
2. 次に、に進みます "AWS Marketplace の Cloud Manager のページ" AMI から Cloud Manager を導入  
  
IAM ユーザがサブスクリプションとサブスクリプション解除を行うには、AWS Marketplace の権限が必要です。
3. [Marketplace] ページで [\* Continue to Subscribe\* ] をクリックし、 [\* Continue to Configuration\* ] をクリックします。

**a**

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

Typical Total Price  
**\$0.226/hr**  
Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Review

### Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

### Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

**b**

Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

[< Product Detail](#) [Subscribe](#)

### Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

### Terms and Conditions

#### NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

- デフォルトのオプションを変更し、[\* Continue to Launch] をクリックします。
- [アクションの選択] で [EC2 で起動] を選択し、[\* 起動 \*] をクリックします。

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

- プロンプトに従って、インスタンスを設定および導入します。
  - \* インスタンスタイプを選択 \* : リージョンの可用性に応じて、サポートされているインスタンスタイプ (t3.xlarge を推奨) のいずれかを選択します。

"インスタンスの要件を確認します"。

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

<b>Number of instances</b> ⓘ	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group ⓘ</a>
<b>Purchasing option</b> ⓘ	<input type="checkbox"/> Request Spot instances	
<b>Network</b> ⓘ	<input type="text" value="vpc-a76d91c2   VPC4QA (default)"/>	<a href="#">Create new VPC</a>
<b>Subnet</b> ⓘ	<input type="text" value="subnet-39536c13   QASubnet1   us-east-1b"/> 155 IP Addresses available	<a href="#">Create new subnet</a>
<b>Auto-assign Public IP</b> ⓘ	<input type="text" value="Enable"/>	
<b>Placement group</b> ⓘ	<input type="checkbox"/> Add instance to placement group	
<b>Capacity Reservation</b> ⓘ	<input type="text" value="Open"/>	<a href="#">Create new Capacity Reservation</a>
<b>IAM role</b> ⓘ	<input type="text" value="Cloud_Manager"/>	<a href="#">Create new IAM role</a>
<b>CPU options</b> ⓘ	<input type="checkbox"/> Specify CPU options	
<b>Shutdown behavior</b> ⓘ	<input type="text" value="Stop"/>	
<b>Enable termination protection</b> ⓘ	<input checked="" type="checkbox"/> Protect against accidental termination	
<b>Monitoring</b> ⓘ	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

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

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

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

`http://ipaddress:80[]`

8. ログイン後、コネクタを設定します。
  - a. コネクタに関連付けるネットアップアカウントを指定します。  
["ネットアップアカウントについて"](#)。
  - b. システムの名前を入力します。



これで、Connector のインストールとセットアップが完了しました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。ただし、コネクタが複数ある場合は、が必要です ["スイッチを切り替えます"](#)。

## Azure Marketplace からコネクタを作成します

Cloud Manager からコネクタを直接作成することを推奨しますが、必要に応じて Azure Marketplace からコネクタを起動できます。Connector の作成とセットアップが完了すると、新しい作業環境を作成するときに、Cloud Manager によって自動的に Connector が使用されます。

### Azure でコネクタを作成する

Azure Marketplace のイメージを使用して Azure に Connector を導入し、コネクタにログインしてネットアップアカウントを指定します。

#### 手順

1. Azure MarketplaceのNetApp Connector VMのページに移動します。
  - ["Azure Marketplaceの一般企業向けページ"](#)
  - ["Azure GovernmentリージョンのAzure Marketplaceのページ"](#)
2. [\* Get it Now\* ( 今すぐ取得 )] をクリックし、[\* Continue \* ( 続行 )] をクリックします。

3. Azure ポータルで、\* Create \* をクリックし、手順に従って仮想マシンを設定します。

VM を設定する際には、次の点に注意してください。

- Cloud Manager は、HDD または SSD ディスクのいずれかで最適なパフォーマンスを実現できます。
- CPU と RAM の要件を満たす VM サイズを選択します。DS3 v2 を推奨します。

"VM の要件を確認します"。

- ネットワークセキュリティグループの場合、コネクタには、SSH、HTTP、および HTTPS を使用したインバウンド接続が必要です。

"コネクタのセキュリティグループルールの詳細については、こちらを参照してください"。

- [\* 管理 (\* Management) ] で、[\* オン \* (\* on \*) ] を選択して、コネクタに割り当てられた管理 ID \* を有効にします。

管理対象の ID を使用すると、Connector 仮想マシンはクレデンシャルを指定せずに自身を Azure Active Directory に識別できるため、この設定は重要です。"Azure リソース用の管理対象 ID の詳細については、こちらをご覧ください"。

4. [\* Review + create \* (レビュー + 作成) ] ページで選択内容を確認し、[\* Create \* (作成) ] をクリックして展開を開始します。

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

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

`http://ipaddress:80[]`

6. ログイン後、コネクタを設定します。

- a. コネクタに関連付けるネットアップアカウントを指定します。

"ネットアップアカウントについて"。

- b. システムの名前を入力します。



これでコネクタがインストールされ、セットアップされました。Cloud Volumes ONTAP を Azure に導入するには、Azure の権限を付与する必要があります。

#### Azure 権限を付与しています

Azure にコネクタを導入したら、を有効にしておく必要があります ["システムによって割り当てられた管理 ID"](#)。カスタムロールを作成し、そのロールを Connector 仮想マシンに割り当てて、1 つ以上のサブスクリプションに必要な Azure 権限を付与する必要があります。

#### 手順

1. Cloud Manager ポリシーを使用してカスタムロールを作成します。
  - a. をダウンロードします ["Cloud Manager Azure ポリシー"](#)。
  - 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 \*

「譲渡対象」：「 / 契約 / D333AF45-0D07-4154-943D-C25FBZZZZ 」、「 / 契約 / 契約 / 54B91999-B3E6-4599-908E-416E0ZZZZ 」、「 / 契約 / E471C-3B42-4AE7-9B59-CE5BBZZZZ 」\*\*



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。

次の例は、Azure CLI 2.0 を使用してカスタムロールを作成する方法を示しています。

「AZ role definition create — role-definition C : \Policy\_for \_cloud\_Manager\_azure\_3.9.8.json

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

2. 1 つ以上のサブスクリプションのロールを Connector 仮想マシンに割り当てます。

- a. [サブスクリプション] サービスを開き、Cloud Volumes ONTAP システムを展開するサブスクリプションを選択します。
- b. \* アクセス制御 (IAM) \* > \* 追加 \* > \* 役割の割り当ての追加 \* をクリックします。
- c. [\* 役割] タブで、\* Cloud Manager Operator \* 役割を選択し、\* Next \* をクリックします。



Cloud Manager Operator は、で指定されたデフォルトの名前で **"Cloud Manager ポリシー"**。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。

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

- \* 管理対象 ID \* へのアクセス権を割り当てます。
- [\* メンバーの選択 \*] をクリックし、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、[\* 仮想マシン \*] を選択してから、Connector 仮想マシンを選択します。
- [\* 選択 \*] をクリックします。
- 「\* 次へ \*」 をクリックします。

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

f. 追加のサブスクリプションから Cloud Volumes ONTAP を導入する場合は、そのサブスクリプションに切り替えてから、これらの手順を繰り返します。

Connector には、パブリッククラウド環境内のリソースとプロセスを管理するために必要な権限が付与されました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。ただし、コネクタが複数ある場合は、が必要です **"スイッチを切り替えます"**。

インターネットにアクセスできる既存の **Linux** ホストにコネクタをインストールします

コネクタを作成する最も一般的な方法は、Cloud Manager から直接、またはクラウドプロバイダのマーケットプレイスから直接行う方法です。ただし、ネットワークまたはクラウドにある既存の Linux ホストに Connector ソフトウェアをダウンロードしてインストールすることもできます。以下の手順は、インターネットにアクセスできるホストに固有の手順です。

**"コネクタを配置するその他の方法について説明します"**。



Google Cloud で Cloud Volumes ONTAP システムを作成する場合は、Google Cloud でも実行されているコネクタが必要です。AWS、Azure、オンプレミスで実行されているコネクタは使用できません。

ホストの要件を確認

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

専用のホストが必要です

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

## CPU

4 コアまたは 4 個の vCPU

## RAM

16 GB

## AWS EC2 インスタンスタイプ

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

## Azure VM サイズ

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

## GCP マシンタイプ

上記の CPU と RAM の要件を満たすインスタンスタイプ。n1-standard-4を推奨します。

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

サポートされているオペレーティングシステム

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux システムは、Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、Connector のインストール中に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。

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

## ハイパーバイザー

認定済みのベアメタルハイパーバイザーまたはホスト型ハイパーバイザー CentOS または Red Hat Enterprise Linux を実行します<https://access.redhat.com/certified-hypervisors>["Red Hat ソリューション : 「 Which hypervisors are certified to run Red Hat Enterprise Linux ? 」 "^]

## /opt のディスクスペース

100GiB のスペースが使用可能である必要があります

## /var のディスク領域

20GiB のスペースが必要です

## アウトバウンドインターネットアクセス

コネクタをインストールし、パブリッククラウド環境内でリソースとプロセスを管理するには、アウトバウンドインターネットアクセスが必要です。エンドポイントのリストについては、を参照してください "[コネクタのネットワーク要件](#)".

## コネクタを取り付ける

サポートされている Linux ホストがあることを確認したら、コネクタソフトウェアを取得してインストールできます。

コネクタをインストールするには root 権限が必要です。

## このタスクについて

- インストールを実行すると、ネットアップサポートからのリカバリ手順用に AWS コマンドラインツール（awscli）がインストールされます。

AWSCLI のインストールに失敗したというメッセージが表示された場合は、このメッセージを無視しても問題ありません。コネクタは、工具なしで正常に作動する。

- ネットアップサポートサイトで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後、新しいバージョンが利用可能になると、コネクタは自動的に更新されます。

## 手順

- から Cloud Manager ソフトウェアをダウンロードします "[ネットアップサポートサイト](#)" をクリックし、Linux ホストにコピーします。

AWS の EC2 インスタンスに接続してファイルをコピーする方法については、を参照してください "[AWS ドキュメント：「Connecting to Your Linux Instance Using SSH」](#)".

- スクリプトを実行する権限を割り当てます。

```
chmod +x OnCommandCloudManager-V3.9.16.sh
```

- インストールスクリプトを実行します。

プロキシサーバを使用している場合は、次のようにコマンドパラメータを入力する必要があります。プロキシに関する情報の入力を求めるプロンプトは表示されません。

```
./OnCommandCloudManager-V3.9.16.sh [silent] [proxy=ipaddress]  
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

*silent* 情報の入力を求めずにインストールを実行します。

プロキシサーバの背後にホストがある場合は、`_proxy_is` が必要です。

`proxyport_` は、プロキシサーバのポートです。

`proxyUser` は、ベーシック認証が必要な場合に、プロキシサーバのユーザ名です。

`_proxypwd_` は、指定したユーザー名のパスワードです。

4. `silent` パラメータを指定しなかった場合は、「\*Y\*」と入力してインストールを続行します。

Cloud Manager がインストールされました。プロキシサーバを指定した場合、インストールの最後に Cloud Manager Service (OCCM) が 2 回再起動します。

5. Web ブラウザを開き、次の URL を入力します。

`https://ipaddress[]`

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

6. NetApp Cloud Central に登録するか、ログインします。
7. Connector を Google Cloud にインストールした場合は、Cloud Manager がプロジェクトで Cloud Volumes ONTAP システムを作成および管理するために必要な権限を持つサービスアカウントをセットアップします。
  - a. ["GCP で役割を作成します"](#) で定義した権限を含むポリシーを作成します ["GCP 向け Cloud Manager ポリシー"](#)。
  - b. ["GCP サービスアカウントを作成し、カスタムロールを適用します を作成しました"](#)。
  - c. ["このサービスアカウントを Connector VM に関連付けます"](#)。
  - d. Cloud Volumes ONTAP を他のプロジェクトに導入する場合は、["クラウドでサービスアカウントを追加してアクセスを許可します そのプロジェクトに対するマネージャの役割"](#)。プロジェクトごとにこの手順を繰り返す必要があります。
8. ログインしたら、Cloud Manager をセットアップします。
  - a. コネクタに関連付けるネットアップアカウントを指定します。  
["ネットアップアカウントについて"](#)。
  - b. システムの名前を入力します。



これで、Connector のインストールとセットアップが完了しました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。

Cloud Manager がパブリッククラウド環境内のリソースやプロセスを管理できるように、権限を設定します。

- AWS "[AWS アカウントをセットアップして、に追加します Cloud Manager の略](#)"
- Azure "[Azure アカウントをセットアップして、に追加します Cloud Manager の略](#)"
- Google Cloud : 上記の手順 7 を参照してください

インターネットにアクセスせずにオンプレミスにコネクタをインストールします

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インストールできます。オンプレミスの ONTAP クラスタを検出し、クラスタ間でデータをレプリケートして、クラウドデータを検出してデータをスキャンできます。

ここで説明するインストール手順は、前述の使用事例を対象としています。"[コネクタを配置するその他の方法について説明します](#)"。

ホストの要件を確認

コネクタソフトウェアは、特定のオペレーティングシステム要件、RAM 要件、ポート要件などを満たすホス

トで実行する必要があります。

専用のホストが必要です

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

## CPU

4 コアまたは 4 個の vCPU

## RAM

16 GB

サポートされているオペレーティングシステム

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux システムは、Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、Connector のインストール中に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。

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

ハイパーバイザー

認定済みのベアメタルハイパーバイザーまたはホスト型ハイパーバイザー CentOS または Red Hat Enterprise Linux を実行します<https://access.redhat.com/certified-hypervisors>["Red Hat ソリューション : 「 Which hypervisors are certified to run Red Hat Enterprise Linux ? 」 "^]

ディスクタイプ

SSD が必要です

/opt のディスクスペース

100GiB のスペースが使用可能である必要があります

/var のディスク領域

20GiB のスペースが必要です

**Docker Engine** の略

Connector をインストールする前に、ホストに Docker Engine バージョン 19 以降が必要です。"[インストール手順を確認します](#)"。

## コネクタを取り付ける

サポートされている Linux ホストがあることを確認したら、コネクタソフトウェアを取得してインストールできます。

コネクタをインストールするには root 権限が必要です。

### 手順

1. Docker が有効で実行されていることを確認します。

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

2. から Cloud Manager ソフトウェアをダウンロードします "ネットアップサポートサイト".
3. インストーラを Linux ホストにコピーします。
4. スクリプトを実行する権限を割り当てます。

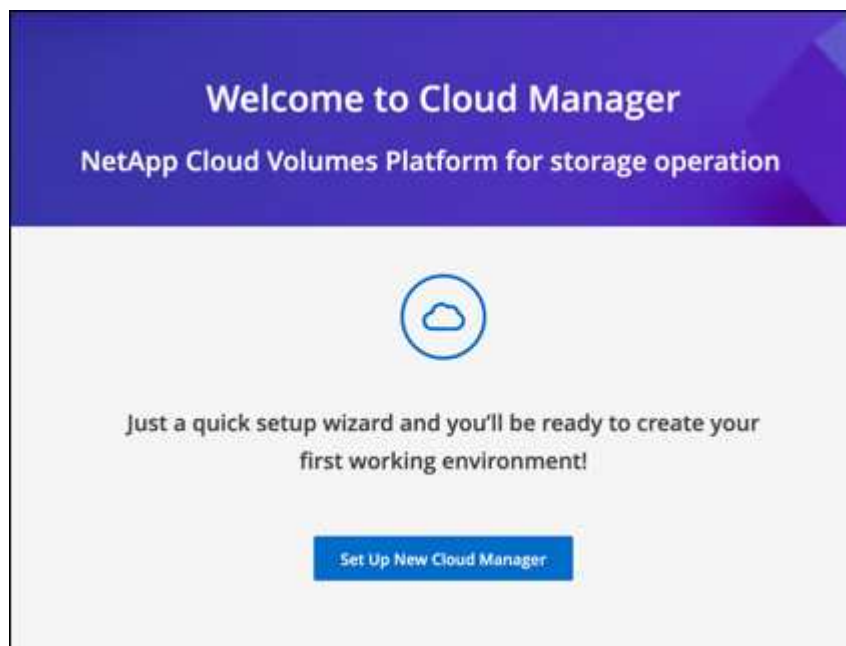
```
chmod +x /path/cloud-manager-connector-offline-v3.9.16
```

5. インストールスクリプトを実行します。

```
sudo /path/cloud-manager-connector-offline-v3.9.16
```

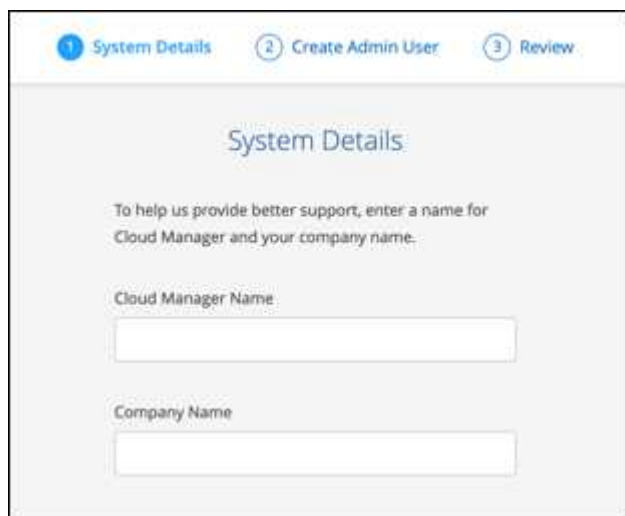
6. Web ブラウザを開き、と入力します `https://ipaddress[]` ここで、`ipaddress` は Linux ホストの IP アドレスです。

次の画面が表示されます。



7. Set Up New Cloud Manager \* をクリックし、プロンプトに従ってシステムをセットアップします。

- \* System Details \* : Cloud Manager システムの名前と会社名を入力します。



- \* 管理者ユーザーの作成 \* : システムの管理者ユーザーを作成します。

このユーザアカウントはシステム上でローカルに実行されます。NetApp Cloud Central への接続はありません。

- \* 復習 \* : 詳細を確認し、ライセンス契約に同意して、\* セットアップ \* をクリックします。

8. 作成した管理者ユーザを使用して Cloud Manager にログインします。

これでコネクタがインストールされ、ダークサイト環境で利用できる Cloud Manager の機能の使用を開始できるようになります。

次の内容

- ["オンプレミスの ONTAP クラスタを検出"](#)
- ["オンプレミスの ONTAP クラスタ間でデータをレプリケート"](#)
- ["Cloud Data Sense を使用してボリュームデータをスキャンする"](#)

新しいバージョンの Connector ソフトウェアが利用可能になると、ソフトウェアはネットアップサポートサイトにアップロードされます。 ["コネクタをアップグレードする方法について説明します"](#)。

## コネクタのシステム ID の確認

作業を開始する際に、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。

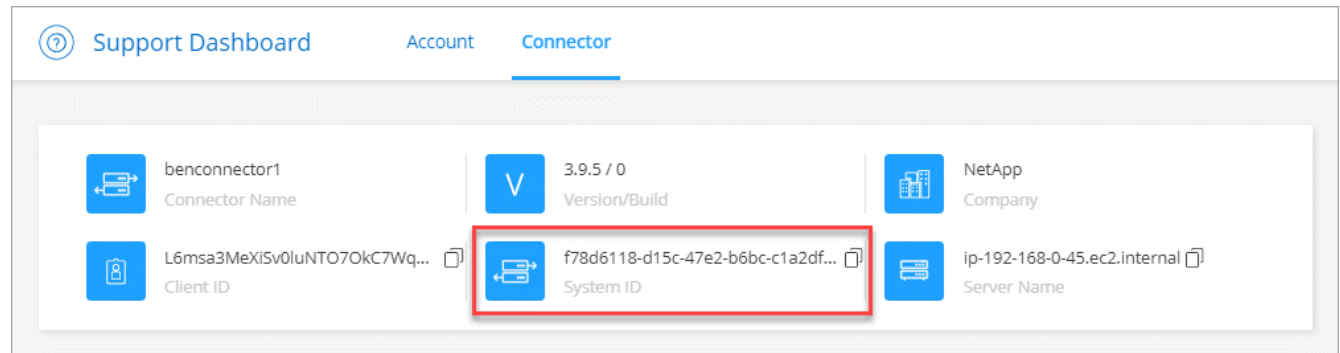
手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックします。
2. [ サポート ( Support ) ] > [ コネクター ( Connector ) ] をクリック



システム ID が一番上に表示されます。

。例 \*



## 既存のコネクタの管理

1 つ以上のコネクタを作成した後、コネクタを切り替えたり、コネクタで実行されているローカルユーザーインターフェースに接続したりすることで、コネクタを管理できます。

### 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. [\* コネクタ] ドロップダウンをクリックし、別のコネクタを選択して、[スイッチ \*] をクリックします。



Cloud Manager 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。

## ローカル UI にアクセスします

SaaS ユーザインターフェイスからほとんどのタスクを実行する必要がありますが、ローカルユーザインターフェイスは引き続きコネクタで使用できます。このインターフェイスは、コネクタ自体から実行する必要があるいくつかのタスクに必要です。

- "プロキシサーバを設定しています"
- パッチをインストールしています（通常はネットアップの担当者と協力してパッチをインストールします）
- AutoSupport メッセージをダウンロードしています（通常は問題が発生したときにネットアップの担当者が指示）

### 手順

1. "Cloud Manager SaaS インターフェイスにログインします" コネクタインスタンスへのネットワーク接続を持つマシンから。

コネクタにパブリック IP アドレスがない場合は、VPN 接続が必要です。そうでない場合は、コネクタと同じネットワークにあるジャンプホストから接続する必要があります。

2. [\* Connector\*（コネクタ\*）] ドロップダウンをクリックし、[\* ローカル UI へ移動\*（Go to Local UI\*）] をクリックします。



コネクタで実行されている Cloud Manager インターフェイスが新しいブラウザタブに表示されます。

## 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

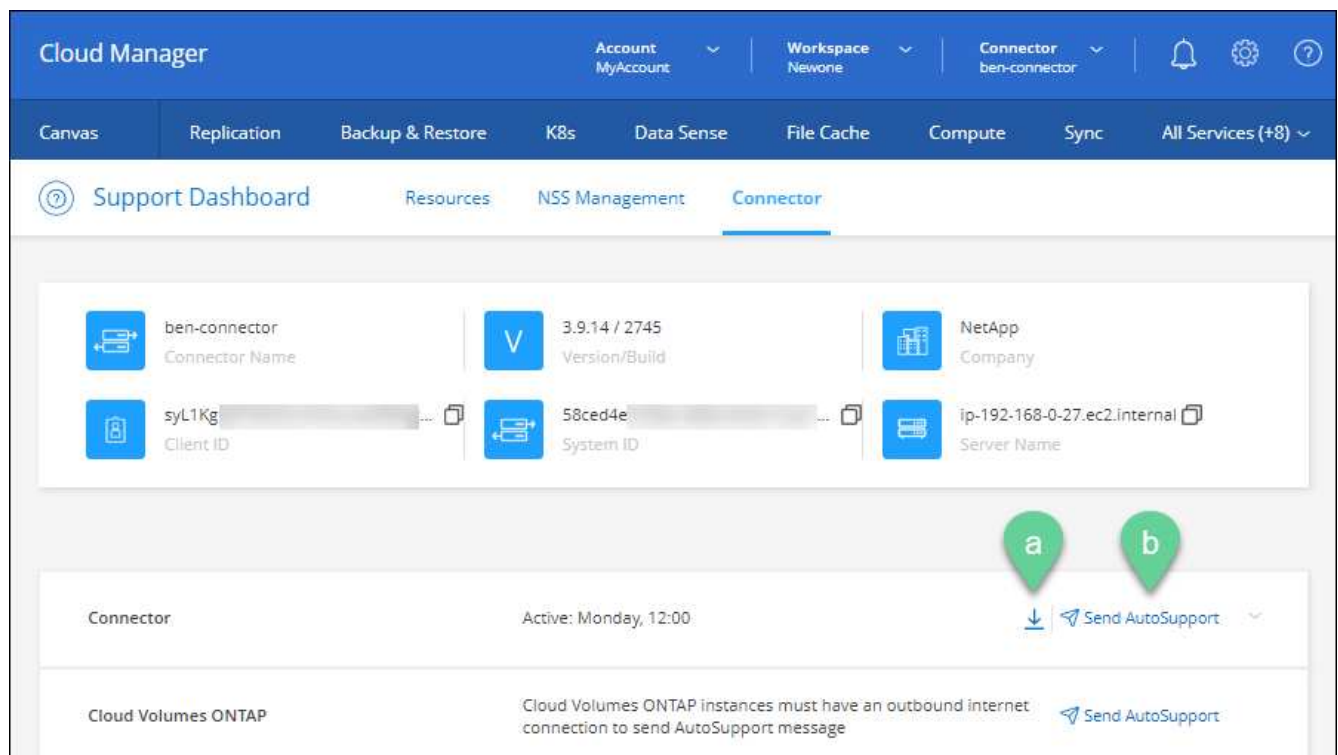
1. 上のセクションの説明に従って、コネクタローカル UI に接続します。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、\* Support \* を選択します。



メニューのスクリーンショット

ト。サポートは最初に表示されるオプションです"]

3. コネクタ（\* Connector）をクリックします。
4. 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. 「\* Send AutoSupport \*」をクリックして、メッセージをネットアップサポートに直接送信します。



## 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。

["AWS Docs : Linux インスタンスに接続します"](#)

### Azure

Azure で Connector VM を作成する際に、パスワードまたは SSH 公開鍵を使用して認証するように選択します。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"](#)

## セキュリティ更新プログラムを適用する

コネクタのオペレーティングシステムをアップデートして、最新のセキュリティアップデートでパッチが適用されていることを確認します。

### 手順

1. コネクタホストの CLI シェルにアクセスします。
2. 管理者権限で次のコマンドを実行します。

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

## 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。

- 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ります。新しい IP アドレスを Cloud Manager に登録するには、コネクタインスタンスを再起動してください。
- 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。
  - 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削除します。

```
system configuration backup settings modify -destination ""
```

- Cloud Manager に移動して、作業環境を開きます。
- メニューをクリックして、**\* Advanced > Configuration Backups \*** を選択します。
- [ **\* バックアップターゲットの設定 \*** ] をクリックします。

## コネクタの URI を編集します

コネクタの URI を追加および削除します。

### 手順

- Cloud Manager ヘッダーの **\* Connector \*** ドロップダウンをクリックします。
- [ **\* コネクターの管理 \*** ] をクリックします。
- コネクターのアクションメニューをクリックし、**\* URI を編集 \*** をクリックする。
- URI を追加して削除し、**\* 適用 \*** をクリックします。

## 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、Cloud Manager API を使用して実行する必要があります。

### ステップ

- 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"](#)。

## インターネットにアクセスせずにオンプレミスのコネクタをアップグレードします

あなたの場合 ["インターネットにアクセスできないオンプレミスホストにコネクタをインストール"](#)では、ネットアップサポートサイトで新しいバージョンを利用できる場合にコネクタをアップグレードできます。

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るため、アップグレード中はユーザインターフェイスを使用できなくなります。

### 手順

1. から Cloud Manager ソフトウェアをダウンロードします ["ネットアップサポートサイト"](#)。
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/cloud-manager-connector-offline-v3.9.14
```

4. インストールスクリプトを実行します。

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

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。

## インターネットにアクセスできるホスト上のソフトウェアアップグレードについて はどうでしょうか。

Connector は、ソフトウェアが最新バージョンである限り、自動的にソフトウェアを更新します ["アウトバウンドインターネットアクセス"](#) をクリックしてソフトウェアアップデートを入手します。

## Cloud Manager からコネクタを削除します

非アクティブなコネクタは、Cloud Manager 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。

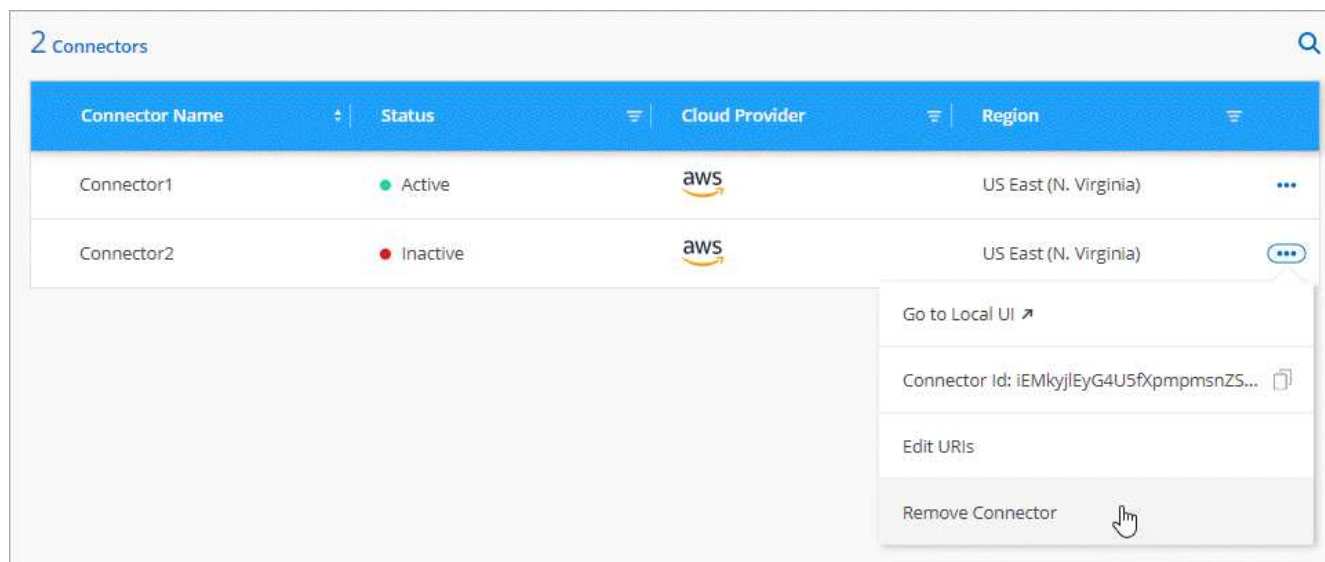
コネクタの取り外しについては、次の点に注意してください。

- この操作で仮想マシンが削除されることはありません。
- この操作は元に戻せません — Cloud Manager からコネクタを削除すると、再度 Cloud Manager に追加することはできません。

### 手順

1. Cloud Manager ヘッダーの \* Connector \* ドロップダウンをクリックします。

2. [ \* コネクタの管理 \* ] をクリックします。
3. 非アクティブなコネクタのアクションメニューをクリックし、 \* コネクタを除去 \* をクリックする。



4. 確認するコネクタの名前を入力し、[ 削除 ] をクリックします。

Cloud Manager によってレコードからコネクタが削除されます。

## 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。使用する必要がある手順は、インターネットにアクセスできるホストにコネクタを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制限されたネットワーク内のホストにインストールしたかによって異なります。

インターネットにアクセスできるホストからをアンインストールします

Online Connector には、ソフトウェアのアンインストールに使用できるアンインストールスクリプトが含まれています。

### ステップ

1. 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/cloudmanager/bin/uninstall.sh [ サイレント ] *`

`silent_` 確認を求めずにスクリプトを実行します。

インターネットにアクセスできないホストからをアンインストールします

ネットアップサポートサイトからコネクタソフトウェアをダウンロードし、インターネットにアクセスできない制限されたネットワークにインストールした場合は、ここに示すコマンドを使用します。

### ステップ

1. Linux ホストから、次のコマンドを実行します。



```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

## セキュアなアクセスのための HTTPS 証明書の管理

デフォルトでは、Cloud Manager 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。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優れたセキュリティ保護が提供されます。

### 始める前に

Cloud Manager の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 証明書のインストール

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. Cloud Manager コンソールの右上にある設定アイコンをクリックし、\* HTTPS セットアップ \* を選択します。

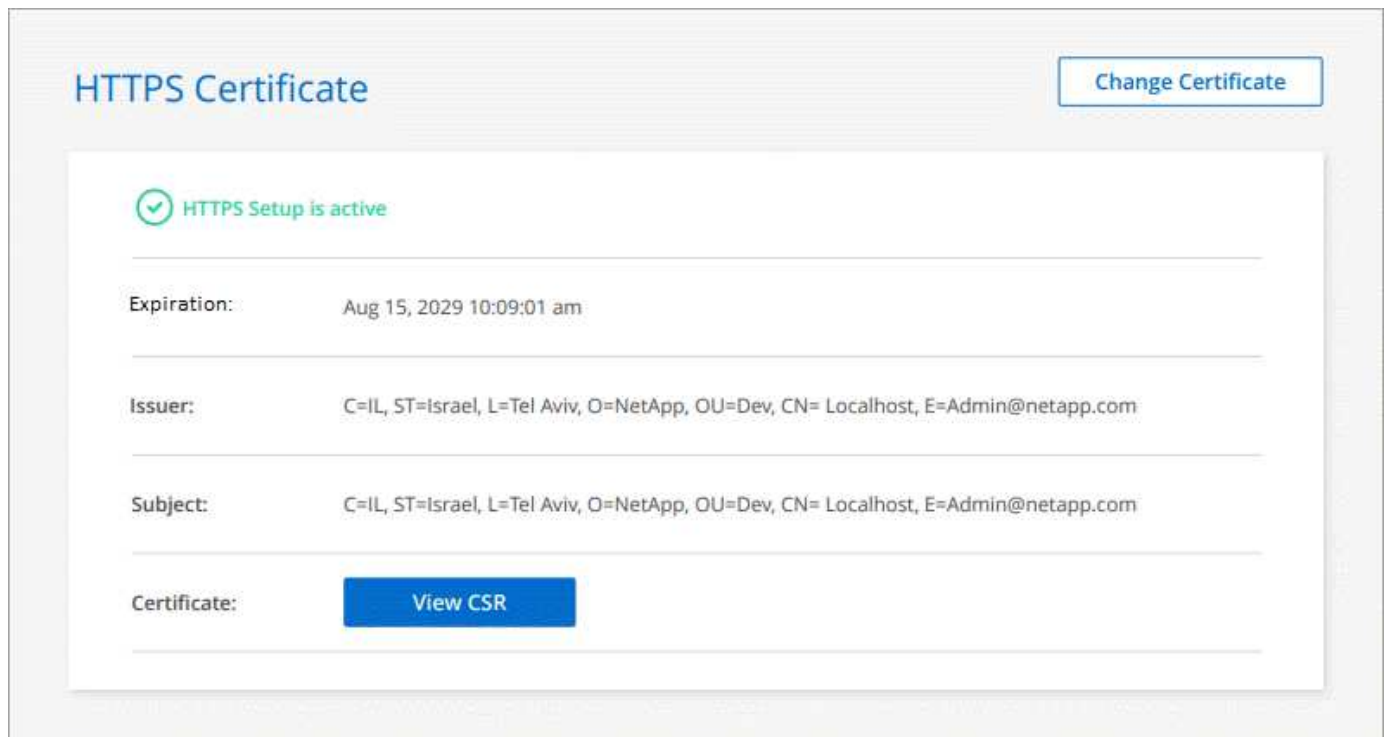


2. [HTTPS Setup] ページで、証明書署名要求（CSR）を生成するか、独自の CA 署名付き証明書をインストールして、証明書をインストールします。

オプション	説明
CSR を生成します	<p>a. コネクターホストのホスト名または DNS（共通名）を入力し、* CSR の生成 * をクリックします。</p> <p>証明書署名要求が表示されます。</p> <p>b. CSR を使用して、SSL 証明書要求を CA に送信します。</p> <p>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。</p> <p>c. 証明書ファイルをアップロードし、* Install * をクリックします。</p>

オプション	説明
独自の CA 署名付き証明書をインストールします	<p>a. 「CA 署名証明書のインストール」を選択します。</p> <p>b. 証明書ファイルと秘密鍵の両方をロードし、* Install * をクリックします。</p> <p>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。</p>

Cloud Manager は、CA 署名付き証明書を使用して、セキュアな HTTPS アクセスを提供するようになりました。次の図は、セキュアアクセス用に設定された Cloud Manager システムを示しています。



## Cloud Manager の HTTPS 証明書を更新します

Cloud Manager Web コンソールへの安全なアクセスを確保するために、Cloud Manager HTTPS 証明書は有効期限が切れる前に更新する必要があります。証明書の有効期限が切れる前に証明書を更新しないと、ユーザーが 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. Cloud Manager コンソールの右上にある設定アイコンをクリックし、\* HTTPS セットアップ \* を選択します。

Cloud Manager 証明書の詳細が表示されます。有効期限も表示されます。

2. [ 証明書の変更 ] をクリックし、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。

Cloud Manager は新しい CA 署名付き証明書を使用して、セキュアな HTTPS アクセスを提供します。

# HTTP プロキシサーバを使用するためのコネクタの設定

社内ポリシーで、インターネットへのすべての HTTP 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 HTTP 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。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。

Cloud Manager では、コネクタでの HTTPS プロキシの使用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. ["Cloud Manager SaaS インターフェイスにログインします"](#) コネクターインスタンスへのネットワーク接続を持つマシンから。

コネクタにパブリック IP アドレスがない場合は、VPN 接続が必要です。そうでない場合は、コネクタと同じネットワークにあるジャンプホストから接続する必要があります。

2. [\* コネクタ \*（Connector \*）] ドロップダウンをクリックし、特定のコネクターの [ローカル UI へ移動（\* Go to local UI \*）] をクリックする。



コネクタで実行されている Cloud Manager インターフェイスが新しいブラウザタブに表示されます。

3. Cloud Manager コンソールの右上にある設定アイコンをクリックし、\* コネクタ設定 \* を選択します。



4. [General] で、[\*HTTP Proxy Configuration] をクリックします。
5. プロキシを設定します。
  - a. [プロキシを有効にする \*] をクリックします
  - b. 構文を使用してサーバを指定します `http://address:port[]`
  - c. ベーシック認証の場合は、ユーザ名とパスワードを指定します サーバに必要です
  - d. [保存 (Save)] をクリックします。



Cloud Manager では、@ 文字を含むパスワードはサポートされていません。

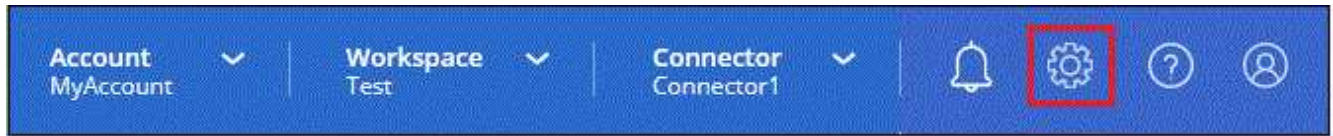
プロキシサーバを指定すると、AutoSupport メッセージの送信時にプロキシサーバを使用するように、新しい Cloud Volumes ONTAP システムが自動的に設定されます。ユーザが Cloud Volumes ONTAP システムを作成する前にプロキシサーバを指定しなかった場合は、System Manager を使用して、各システムの AutoSupport オプションでプロキシサーバを手動で設定する必要があります。

## API の直接トラフィックを有効にします

プロキシサーバを設定している場合は、プロキシを経由せずに Cloud Manager に API 呼び出しを直接送信できます。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。

### 手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、\* コネクタ設定 \* を選択します。



2. [General] で、[ Support Direct API traffic\* ] をクリックします。
3. チェックボックスをクリックしてオプションを有効にし、\* 保存 \* をクリックします。

## コネクタのデフォルト設定

コネクタのトラブルシューティングが必要な場合は、コネクタの設定を理解すると役立つことがあります。

### インターネットアクセスを使用するデフォルト設定

- Cloud Manager から（またはクラウドプロバイダのマーケットプレイスから直接）Connector を導入した場合は、次の点に注意してください。

- AWS では、EC2 Linux インスタンスのユーザ名は EC2-user です。
- イメージのオペレーティングシステムは次のとおりです。
  - AWS : Red Hat Enterprise Linux 7.6 (HVM)
  - Azure : CentOS 7.6
  - GCP : CentOS 7.9

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。

- Cloud Manager から導入した場合、デフォルトのシステムディスクは次のようになります。

- AWS : 50GiB の gp2 ディスクです
- Azure : 100GiB の Premium SSD ディスク
- Google Cloud : 100GiB の SSD 永続ディスク

- 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

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。

- /opt/application/NetApp/cloudmanager/docx\_occm/data/log

このフォルダには、コネクタで実行されているクラウドサービスと Cloud Manager サービスの詳細が記録されます。

- Cloud Manager 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。

- 次のパッケージがまだインストールされていない場合は、Cloud Manager によって Linux ホストにインストールされます。
  - 7 郵便番号
  - AWSCLI
  - Docker です
  - Java
  - Kubectl のように入力する
  - MySQL
  - Tridentctl
  - プル
  - 取得
- 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
  - 3306 (Cloud Manager データベース用)
  - クラウドマネージャ API プロキシの場合は 8080
  - Service Manager API の場合は 8666
  - 8777 (Health-Checker コンテナサービス API の場合)

## 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/app/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

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.