



# コネクタをセットアップします

## Set up and administration

NetApp  
April 13, 2022

# 目次

|   |    |
|---|----|
| コネクタをセットアップします .....                            | 1  |
| コネクタについて説明します .....                             | 1  |
| コネクタのネットワークを設定します .....                         | 5  |
| Cloud Manager から AWS にコネクタを作成します .....          | 12 |
| Cloud Manager から Azure にコネクタを作成します .....        | 15 |
| Cloud Manager から Google Cloud でコネクタを作成します ..... | 26 |

# コネクタをセットアップします

## コネクタについて説明します

ほとんどの場合、アカウント管理者は \_コネクタ\_ をクラウドまたはオンプレミスネットワークに導入する必要があります。Connector は、Cloud Manager を日常的に使用するための重要なコンポーネントです。Connector を使用すると、Cloud Manager で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できます。

### コネクタが必要な場合

Cloud Manager の多くの機能やサービスを使用するには、コネクタが必要です。

#### サービス

- ONTAP 管理機能用の Amazon FSX
- Amazon S3 バケットの検出
- クラウドバックアップ
- クラウドデータの意味
- クラウド階層化
- Cloud Volumes ONTAP
- グローバルファイルキャッシュ
- Kubernetes クラスタ
- 監視
- オンプレミスの ONTAP クラスタ

次のサービスには、コネクタが \*\_ ではありません \_\*。

- Active IQ デジタルアドバイザー
- 作業環境の作成にはコネクタは必要ありませんが、ONTAP FSX for ONTAP を作成して管理し、データをレプリケートし、データセンスや Cloud Sync などのクラウドサービスと FSX for を統合する必要があります。
- Azure NetApp Files の特長

Azure NetApp Files のセットアップと管理にコネクタは必要ありませんが、Azure NetApp Files データのスキャンにクラウドデータセンスを使用する場合はコネクタが必要です。

- Cloud Volumes Service for Google Cloud
- Cloud Sync

#### デジタルウォレット

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

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

## サポートされている場所

コネクタは次の場所でサポートされています。

- Amazon Web Services の
- Microsoft Azure
- Google Cloud
- オンプレミス
- インターネットに接続できない、オンプレミス

### Azure の導入についての注意

Azure でコネクタを導入する場合は、コネクタを管理する Cloud Volumes ONTAP システムと同じ Azure リージョンまたはに導入する必要があります ["Azure リージョンペア"](#) Cloud Volumes ONTAP システム用。この要件により、Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間で Azure Private Link 接続が使用されるようになります。 ["Cloud Volumes ONTAP での Azure プライベートリンクの使用方法をご確認ください"](#)。

### Google Cloud の導入についての注意

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。

## 共有 Linux ホストはサポートされません

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

## サードパーティのエージェントと内線番号

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

## コネクタは動作したままにしてください

コネクタは常時稼働している必要があります。有効にするサービスの継続的な健全性と運用性にとって重要です。

たとえば、Cloud Volumes ONTAP PAYGO システムの正常性と運用においては、コネクタが重要な要素です。コネクタの電源がオフの場合、Cloud Volumes ONTAP PAYGO システムは、コネクタとの通信を 14 日以上失った後にシャットダウンします。

## コネクタを作成する方法

Workspace 管理者が Cloud Volumes ONTAP 作業環境を作成し、上記の他の機能を使用するには、アカウント管理者がコネクタを作成する必要があります。

アカウント管理者は、さまざまな方法でコネクタを作成できます。

- Cloud Manager から直接（推奨）
  - ["AWS で作成します"](#)
  - ["Azure で作成します"](#)
  - ["GCP で作成します"](#)
- ソフトウェアを手動で独自の Linux ホストにインストールする
  - ["インターネットにアクセスできるホスト"](#)
  - ["インターネットにアクセスできないオンプレミスのホスト"](#)
- クラウドプロバイダのマーケットプレイスから
  - ["AWS Marketplace"](#)
  - ["Azure Marketplace で入手できます"](#)

操作を完了するためにコネクタが必要な場合は、Cloud Manager からコネクタの作成を求められます。

## 権限

コネクタを作成するには特定の権限が必要であり、コネクタインスタンス自体に別の権限セットが必要です。

### コネクタを作成する権限

Cloud Manager からコネクタを作成するユーザには、任意のクラウドプロバイダにインスタンスを導入するための特定の権限が必要です。Connector を作成するときは、Cloud Manager に権限の要件が通知されます。

["各クラウドプロバイダのポリシーを表示します"](#)。

### コネクタインスタンスの権限

Connector で処理を実行するには、特定のクラウドプロバイダの権限が必要です。たとえば、Cloud Volumes ONTAP を導入して管理するには、のように指定します。

Cloud Manager から直接コネクタを作成すると、必要な権限を持つコネクタが Cloud Manager によって作成されます。必要なことは何もありません。

コネクタを AWS Marketplace、Azure Marketplace、またはソフトウェアを手動でインストールして作成する場合は、適切な権限が設定されていることを確認する必要があります。

["各クラウドプロバイダのポリシーを表示します"](#)

## コネクタごとの作業環境数

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

大規模な導入の場合は、ネットアップの担当者にご相談のうえ、環境のサイジングを行ってください。途中で

問題が発生した場合は、製品内のチャットでお問い合わせください。

## 複数のコネクタを使用する場合

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

次にいくつかの例を示します。

- マルチクラウド環境（AWS と Azure）を使用しているため、AWS と Azure のコネクタが 1 つずつ必要です。各で、それらの環境で実行される Cloud Volumes ONTAP システムを管理します。
- サービスプロバイダは、1 つのネットアップアカウントを使用してお客様にサービスを提供しながら、別のアカウントを使用してお客様のビジネスユニット 1 つにディザスタリカバリを提供することができます。アカウントごとに個別のコネクタがあります。

## 同じ作業環境で複数のコネクタを使用する

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

この構成をセットアップするには：

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

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

## コネクタを切り替えるタイミング

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

["コネクタを切り替える方法について説明します"](#)。

## ローカルユーザインターフェイス

ではほぼすべてのタスクを実行する必要がありますが ["SaaS ユーザインターフェイス"](#)では、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えます。このインターフェイスは、インターネットにアクセスできない環境に Connector をインストールする場合や、SaaS インターフェイスではなく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の場合に必要になります。

- ["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）

"ローカル UI へのアクセス方法について説明します"。

## コネクタのアップグレード

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。

## コネクタのネットワークを設定します

コネクタがパブリッククラウド環境内のリソースやプロセスを管理できるように、ネットワークを設定します。最も重要なステップは、さまざまなエンドポイントへのアウトバウンドインターネットアクセスを確保することです。

このページの情報は、コネクタがアウトバウンドインターネットアクセスを持つ一般的な配置用です。



ネットワーク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している場合は、[設定] ページでプロキシサーバを指定できます。を参照してください ["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"](#)。

## ターゲットネットワークへの接続

コネクタには、作成する作業環境の種類と、有効にする予定のサービスへのネットワーク接続が必要です。

たとえば、企業ネットワークにコネクタを設置する場合は、Cloud Volumes ONTAP を起動する VPC または VNet への VPN 接続を設定する必要があります。

## 172 の範囲の IP アドレスと競合する可能性があります

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

これらの範囲のいずれかでネットワークのサブネットが設定されている場合、Cloud Manager から接続エラーが発生することがあります。たとえば、Cloud Manager でオンプレミスの ONTAP クラスタを検出すると失敗することがあります。

回避策は、コネクタのインターフェイスの IP アドレスを変更します。ネットアップサポートにお問い合わせください。

## アウトバウンドインターネットアクセス

コネクタからのアウトバウンドインターネットアクセスが必要です。

### パブリッククラウド環境内のリソースを管理するためのエンドポイント

Connector では、パブリッククラウド環境内のリソースとプロセスを管理するためにアウトバウンドインターネットアクセスが必要です。

| エンドポイント  | 目的  |
|--|---|
| \ <a href="https://support.netapp.com">https://support.netapp.com</a>  | ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。 |
| \ <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>  | Cloud Manager 内で SaaS の機能やサービスを提供できます。            |
| ¥ <a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> ¥<br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> | をクリックして、Connector と Docker コンポーネントをアップグレードします。    |

## Linux ホストにコネクタをインストールするエンドポイント

Connector ソフトウェアは、手動でインストールすることもできます。その場合、Connector のインストーラは、インストールプロセス中に次の URL にアクセスする必要があります。

- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- ¥ [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) または ¥ <https://hub.docker.com>

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

## ポートおよびセキュリティグループ

コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます "ローカル UI"は、まれな状況で使われます。SSH が必要になるのは、トラブルシューティングのためにホストに接続する必要がある場合のみです。

### AWS のコネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

#### インバウンドルール

| プロトコル | ポート  | 目的  |
|-------|------|---|
| SSH   | 22   | コネクタホストへの SSH アクセスを提供します  |
| HTTP  | 80   | クライアント Web ブラウザからローカルユーザインターフェイスへの HTTP アクセス、および Cloud Data Sense からの接続を提供します |
| HTTPS | 443  | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス                          |
| TCP   | 3128 | AWS ネットワークで NAT やプロキシを使用していない場合に、Cloud Data Sense インスタンスにインターネットアクセスを提供します    |
| TCP   | 9060 | Cloud Data Sense を有効にして使用できる（GovCloud 環境の場合のみ必要）                              |

#### アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンド



ルールを使用します。

## 基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

| プロトコル    | ポート | 目的           |
|----------|-----|--------------|
| すべての TCP | すべて | すべての発信トラフィック |
| すべての UDP | すべて | すべての発信トラフィック |

## 高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス             | プロトコル | ポート | 宛先                     | 目的  |
|------------------|-------|-----|------------------------|---|
| Active Directory | TCP   | 88  | Active Directory フォレスト | Kerberos V 認証   |
|                  | TCP   | 139 | Active Directory フォレスト | NetBIOS サービスセッション                                     |
|                  | TCP   | 389 | Active Directory フォレスト | LDAP  |
|                  | TCP   | 445 | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP            |
|                  | TCP   | 464 | Active Directory フォレスト | Kerberos V パスワードの変更と設定 (SET_CHANGE)                   |
|                  | TCP   | 749 | Active Directory フォレスト | Active Directory Kerberos v の変更とパスワードの設定 (RPCSEC_GSS) |
|                  | UDP   | 137 | Active Directory フォレスト | NetBIOS ネームサービス                                       |
|                  | UDP   | 138 | Active Directory フォレスト | NetBIOS データグラムサービス                                    |
|                  | UDP   | 464 | Active Directory フォレスト | Kerberos キー管理   |

| サービス                 | プロトコル | ポート  | 宛先                                 | 目的  |
|----------------------|-------|------|------------------------------------|---|
| API コールと AutoSupport | HTTPS | 443  | アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF | AWS および ONTAP への API コール、および ネットアップ への AutoSupport メッセージの送信 |
| API コール              | TCP   | 3000 | ONTAP HA メディエーター                   | ONTAP HA メディエーターとの通信  |
|                      | TCP   | 8088 | S3 へのバックアップ                        | S3 へのバックアップを API で呼び出します                                    |
| DNS                  | UDP   | 53   | DNS                                | Cloud Manager による DNS 解決に使用されます                             |
| クラウドデータの意味           | HTTP  | 80   | Cloud Data Sense インスタンス            | Cloud Volumes ONTAP に最適なクラウドデータ                             |

## Azure のコネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

### インバウンドルール

| ポート | プロトコル | 目的   |
|-----|-------|--|
| 22  | SSH   | コネクタホストへの SSH アクセスを提供します                             |
| 80  | HTTP  | クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス  |
| 443 | HTTPS | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス |

### アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

### 基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

| ポート | プロトコル    | 目的           |
|-----|----------|--------------|
| すべて | すべての TCP | すべての発信トラフィック |

| ポート | プロトコル    | 目的           |
|-----|----------|--------------|
| すべて | すべての UDP | すべての発信トラフィック |

## 高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス                 | ポート | プロトコル | 宛先                                 | 目的  |
|----------------------|-----|-------|------------------------------------|---|
| Active Directory     | 88  | TCP   | Active Directory フォレスト             | Kerberos V 認証   |
|                      | 139 | TCP   | Active Directory フォレスト             | NetBIOS サービスセッション   |
|                      | 389 | TCP   | Active Directory フォレスト             | LDAP  |
|                      | 445 | TCP   | Active Directory フォレスト             | NetBIOS フレーム同期を使用した Microsoft SMB over TCP                |
|                      | 464 | TCP   | Active Directory フォレスト             | Kerberos V パスワードの変更と設定 (SET_CHANGE)                       |
|                      | 749 | TCP   | Active Directory フォレスト             | Active Directory Kerberos v の変更とパスワードの設定 (RPCSEC_GSS)     |
|                      | 137 | UDP   | Active Directory フォレスト             | NetBIOS ネームサービス   |
|                      | 138 | UDP   | Active Directory フォレスト             | NetBIOS データグラムサービス  |
|                      | 464 | UDP   | Active Directory フォレスト             | Kerberos キー管理   |
| API コールと AutoSupport | 443 | HTTPS | アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF | AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信 |
| DNS                  | 53  | UDP   | DNS                                | Cloud Manager による DNS 解決に使用されます                           |

## GCP のコネクタのルール

コネクタのファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。

### インバウンドルール

| プロトコル | ポート | 目的   |
|-------|-----|--|
| SSH   | 22  | コネクタホストへの SSH アクセスを提供します                             |
| HTTP  | 80  | クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス  |
| HTTPS | 443 | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス |

### アウトバウンドルール

コネクタの定義済みファイアウォールルールによって、すべてのアウトバウンドトラフィックが開かれます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

### 基本的なアウトバウンドルール

コネクタの定義済みファイアウォールルールには、次のアウトバウンドルールが含まれています。

| プロトコル    | ポート | 目的           |
|----------|-----|--------------|
| すべての TCP | すべて | すべての発信トラフィック |
| すべての UDP | すべて | すべての発信トラフィック |

### 高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス                    | プロトコル | ポート | 宛先                                    | 目的   |
|-------------------------|-------|-----|---------------------------------------|--|
| Active Directory        | TCP   | 88  | Active Directory フォレスト                | Kerberos V 認証  |
|                         | TCP   | 139 | Active Directory フォレスト                | NetBIOS サービスセッション  |
|                         | TCP   | 389 | Active Directory フォレスト                | LDAP   |
|                         | TCP   | 445 | Active Directory フォレスト                | NetBIOS フレーム同期を使用した<br>Microsoft SMB over TCP                    |
|                         | TCP   | 464 | Active Directory フォレスト                | Kerberos V パスワードの変更と設定（<br>SET_CHANGE）                           |
|                         | TCP   | 749 | Active Directory フォレスト                | Active Directory Kerberos v の変更と<br>パスワードの設定（<br>RPCSEC_GSS）     |
|                         | UDP   | 137 | Active Directory フォレスト                | NetBIOS ネームサービス  |
|                         | UDP   | 138 | Active Directory フォレスト                | NetBIOS データグラムサービス   |
|                         | UDP   | 464 | Active Directory フォレスト                | Kerberos キー管理  |
| API コールと<br>AutoSupport | HTTPS | 443 | アウトバウンドインターネットおよび<br>ONTAP クラスタ管理 LIF | GCP および ONTAP への API コール、<br>およびネットアップへの<br>AutoSupport メッセージの送信 |
| DNS                     | UDP   | 53  | DNS                                   | Cloud Manager による<br>DNS 解決に使用<br>されます                           |

## オンプレミスコネクタ用のポート

コネクタは、オンプレミスの Linux ホストに手動でインストールする場合、下記の \_ インバウンド \_ ポートを使用します。

これらのインバウンドルールは、オンプレミスコネクタの両方の配置モデルに適用されます。つまり、インターネットアクセスがインストールされているか、インターネットアクセスがないかです。

| プロトコル | ポート | 目的   |
|-------|-----|--|
| HTTP  | 80  | クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザーインターフェイス |

| プロトコル | ポート | 目的   |
|-------|-----|--|
| HTTPS | 443 | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス |

## Cloud Manager から AWS にコネクタを作成します

Cloud Manager のほとんどの機能を使用するには、Account Admin が \_ Connector を導入する必要があります。"コネクタが必要になるタイミングを学習します"。Connector を使用すると、Cloud Manager で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できます。

このページでは、Cloud Manager から AWS でコネクタを直接作成する方法について説明します。"コネクタを配置するその他の方法について説明します"。

これらの手順は、Account Admin ロールを持つユーザが実行する必要があります。ワークスペース管理者はコネクタを作成できません。



最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、Cloud Manager からコネクタの作成を求められます。

### AWS 認証をセットアップする

Cloud Manager で VPC にコネクタインスタンスを導入するには、AWS で認証する必要があります。次のいずれかの認証方式を選択できます。

- Cloud Manager に IAM ロールを割り当てます
- IAM ユーザの AWS アクセスキーとシークレットキーを指定します

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。

#### IAM ロールを設定する

Cloud Manager で Connector を AWS に導入するために想定できる IAM ロールを設定します。

##### 手順

1. からコネクタ IAM ポリシーをダウンロードします "Cloud Manager Policies ページ"。

このポリシーには、AWS でコネクタを作成するために必要な権限が含まれています。Cloud Manager は、作成時にコネクタインスタンスに新しい権限セットを適用します。

2. ターゲットアカウントの AWS IAM コンソールに移動します。
3. [ アクセス管理 ] で、[ 役割 ]、[ 役割の作成 \* ] の順にクリックし、手順に従って役割を作成します。

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、Cloud Manager SaaS アカウントの ID として「952013314444」を入力してください
  - 以前にダウンロードしたコネクタ IAM ポリシーに表示されている権限を含むポリシーを作成します。
4. IAM ロールのロール ARN をコピーして、コネクタの作成時に Cloud Manager に貼り付けることができるようにします。

IAM ロールに必要な権限が割り当てられます。

## **IAM ユーザの権限を設定します**

コネクタを作成するときに、Connector インスタンスの導入に必要な権限を持つ IAM ユーザに AWS アクセスキーとシークレットキーを指定できます。

### 手順

1. から Connector 展開ポリシーをダウンロードします "[Cloud Manager Policies ページ](#)".

この IAM ポリシーには、AWS でコネクタを作成するために必要な権限が含まれています。Cloud Manager は、作成時にコネクタインスタンスに新しい権限セットを適用します。

2. AWS IAM コンソールで、コネクタ IAM ポリシーからコピーしたテキストを貼り付けて独自のポリシーを作成します。
3. 前の手順で作成したポリシーを、Cloud Manager からコネクタを作成する IAM ユーザに関連付けます。
4. IAM ユーザのアクセスキーとシークレットキーにアクセスできることを確認します。

AWS ユーザに、Cloud Manager からコネクタを作成するために必要な権限が付与されました。Cloud Manager からプロンプトが表示されたら、このユーザの AWS アクセスキーを指定する必要があります。

## コネクタを作成します

Cloud Manager では、ユーザインターフェイスから AWS に直接コネクタを作成できます。

### 必要なもの

- AWS 認証方式：Cloud Manager が権限を持つ IAM ロールの ARN、または IAM ユーザの AWS アクセスキーとシークレットキーのいずれかです。
- 選択した AWS リージョン内の VPC、サブネット、キーペア。
- Cloud Manager でコネクタ用の IAM ロールが自動的に作成されないようにするには、専用のを作成する必要があります "[使用するポリシー](#)".

これらは、Connector がパブリッククラウド環境内のリソースを管理するために必要な権限です。これは、コネクタインスタンスの作成時に指定したアクセス許可とは異なります。

### 手順

1. 最初の作業環境を作成する場合は、\* 作業環境の追加 \* をクリックし、プロンプトに従います。それ以外の場合は、[connector] ドロップダウンをクリックし、[Add connector] を選択します。



2. クラウドプロバイダとして「\* Amazon Web Services \*」を選択し、「\* Continue \*」をクリックします。

Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があります。ことに注意してください。

["Connector のネットワーク要件の詳細については、こちらをご覧ください"](#)。

3. ウィザードの手順に従って、コネクタを作成します。
  - \* 準備をしてください \* : 必要なものを確認してください。
  - \* AWS クレデンシャル \* : AWS リージョンを指定してから認証方式を選択します。認証方式は、Cloud Manager が引き受けることができる IAM ロールか、AWS のアクセスキーとシークレットキーのどちらかです。



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

- \* 詳細 \* : コネクタの詳細を入力します。
  - インスタンスの名前を入力します。
  - カスタムタグ（メタデータ）をインスタンスに追加します。
  - 必要な権限を含む新しいロールを Cloud Manager で作成するか、またはを使用して設定した既存のロールを選択するかを選択します ["必要な権限"](#)。
  - コネクタの EBS ディスクを暗号化するかどうかを選択します。デフォルトの暗号化キーを使用することも、カスタムキーを使用することもできます。
- \* ネットワーク \* : インスタンスに VPC、サブネット、キーペアを指定し、パブリック IP アドレスを有効にするかどうかを選択し、必要に応じてプロキシ設定を指定します。
- \* セキュリティグループ \* : 新しいセキュリティグループを作成するか、インバウンド HTTP、HTTPS、SSH アクセスを許可する既存のセキュリティグループを選択するかを選択します。





コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます "[ローカル UI](#)"は、まれな状況で使用します。SSH が必要になるのは、トラブルシューティングのためにホストに接続する必要がある場合のみです。

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

4. [ 追加 (Add) ] をクリックします。

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

ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、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、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。 "[詳細はこちら](#)。"

## Cloud Manager から Azure にコネクタを作成します

Cloud Manager のほとんどの機能を使用するには、Account Admin が \_Connector を導入する必要があります。Connector を使用すると、Cloud Manager で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できます。 "[コネクタが必要になるタイミングを学習します](#)"。

このページでは、Cloud Manager から直接 Azure でコネクタを作成する方法について説明します。 "[コネクタを配置するその他の方法について説明します](#)"。

これらの手順は、Account Admin ロールを持つユーザが実行する必要があります。ワークスペース管理者はコネクタを作成できません。



最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、Cloud Manager からコネクタの作成を求められます。

### 概要

Connector を導入するには、Azure で Connector VM を作成するために必要な権限を持つログインを Cloud Manager に付与する必要があります。

次の 2 つのオプションがあります。

1. プロンプトが表示されたら、Microsoft アカウントでサインインします。このアカウントには Azure 固有の権限が必要です。これがデフォルトのオプションです。

[次の手順に従って、作業を開始してください。](#)

2. Azure AD サービスプリンシパルの詳細を指定します。このサービスプリンシパルには、特定の権限も必要です。

[次の手順に従って、作業を開始してください。](#)

## Azure のリージョンに関する注意

コネクタは、管理対象の Cloud Volumes ONTAP システムまたはにある Azure リージョンと同じ Azure リージョンに導入する必要があります ["Azure リージョンペア"](#) Cloud Volumes ONTAP システム用。この要件により、Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間で Azure Private Link 接続が使用されるようになります。 ["Cloud Volumes ONTAP での Azure プライベートリンクの使用方法をご確認ください"](#)。

## Azure アカウントを使用してコネクタを作成します

Azure でコネクタを作成するデフォルトの方法は、プロンプトが表示されたら Azure アカウントでログインすることです。ログインフォームは、Microsoft が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

### Azure アカウントの権限を設定します

Cloud Manager からコネクタを導入する前に、Azure アカウントが正しい権限を持っていることを確認する必要があります。

#### 手順

1. をダウンロードします ["コネクタの Azure ポリシー"](#)。



リンクを右クリックし、[名前を付けてリンクを保存 ...] をクリックしてファイルをダウンロードする。

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

。例 \*

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

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

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

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



c. Azure CLI で次のコマンドを入力します。

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

これで、\_Azure SetupAsService\_という カスタムロールが作成されました。

4. Cloud Manager からコネクタを導入するユーザにロールを割り当てます。
  - a. [サブスクリプション] サービスを開き、ユーザーのサブスクリプションを選択します。
  - b. 「\* アクセスコントロール (IAM) \*」をクリックします。
  - c. [\* 追加 > 役割の割り当ての追加 \*] をクリックして、権限を追加します。
    - Azure SetupAsService \* ロールを選択し、\* 次へ \* をクリックします。



Azure SetupAsService は、で指定されているデフォルトの名前で ["Azure の Connector 導入ポリシー"](#)。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。

- [\* 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 \*] をクリックし、ユーザーアカウントを選択して、[\* 選択 \*] をクリックします。
- 「\* 次へ \*」をクリックします。
- [レビュー + 割り当て (Review + Assign)] をクリックします。

Azure ユーザに、Cloud Manager から Connector を導入するために必要な権限が付与されるようになりました。

**Azure** アカウントでログインしてコネクタを作成します

Cloud Manager では、ユーザインターフェイスから直接 Azure にコネクタを作成できます。

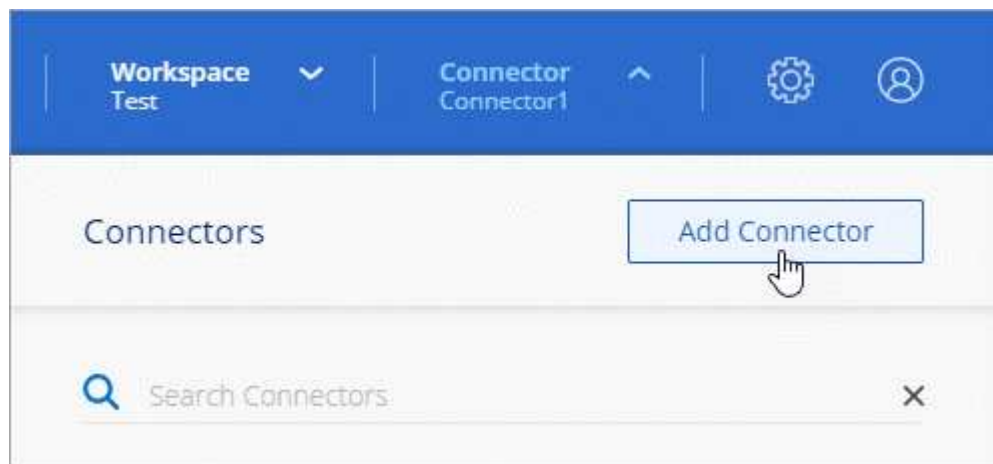
## 必要なもの

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet およびサブネット
- Cloud Manager で Connector 用の Azure ロールが自動的に作成されないようにするには、独自のを作成する必要があります ["使用するポリシー"](#)。

これらの権限はコネクタインスタンス自体に適用されます。これは、以前にコネクタを展開するように設定したアクセス権とは異なります。

## 手順

1. 最初の作業環境を作成する場合は、\* 作業環境の追加 \* をクリックし、プロンプトに従います。それ以外の場合は、[connector] ドロップダウンをクリックし、[Add connector] を選択します。



2. クラウドプロバイダとして「\* Microsoft Azure \*」を選択します。

Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があることに注意してください。

["Connector のネットワーク要件の詳細については、こちらをご覧ください"](#)。

3. ウィザードの手順に従って、コネクタを作成します。

- \* 準備完了 \* : 必要なものを確認して、\* 次へ \* をクリックしてください。
- プロンプトが表示されたら、Microsoft アカウントにログインします。このアカウントには、仮想マシンの作成に必要な権限が付与されている必要があります。

このフォームは、Microsoft が所有およびホストしています。クレデンシャルがネットアップに提供されていません。



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

- \* VM 認証 \* : Azure サブスクリプション、場所、新しいリソースグループ、または既存のリソースグループを選択し、認証方法を選択します。

- \* 詳細 \* : インスタンスの名前を入力し、タグを指定し、必要な権限を持つ新しいロールを Cloud Manager で作成するか、で設定した既存のロールを選択するかを選択します ["必要な権限"](#)。

このロールに関連付けられているサブスクリプションを選択できます。選択した各サブスクリプションには、Cloud Volumes ONTAP をこれらのサブスクリプションに導入するための権限が Connector に付与されます。

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



コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます ["ローカル UI"](#)は、まれな状況で使用します。SSH が必要になるのは、トラブルシューティングのためにホストに接続する必要がある場合のみです。

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

4. [ 追加 (Add) ] をクリックします。

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

ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、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、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。 ["詳細はこちら"](#)。

## サービスプリンシパルを使用してコネクタを作成します

Azure アカウントでログインする代わりに、必要な権限がある Azure サービスプリンシパルのクレデンシャルを Cloud Manager に入力することもできます。

### サービスプリンシパルを使用した **Azure** 権限の付与

Azure Active Directory でサービスプリンシパルを作成およびセットアップし、Cloud Manager で必要な Azure クレデンシャルを取得して、Azure に Connector を導入するために必要な権限を付与します。

#### 手順

1. [\[Create an Azure Active Directory application\]](#)。
2. [\[Assign the application to a role\]](#)。
3. [\[Add Windows Azure Service Management API permissions\]](#)。
4. [\[Get the application ID and directory ID\]](#)。
5. [\[Create a client secret\]](#)。

### **Azure Active Directory** アプリケーションを作成します

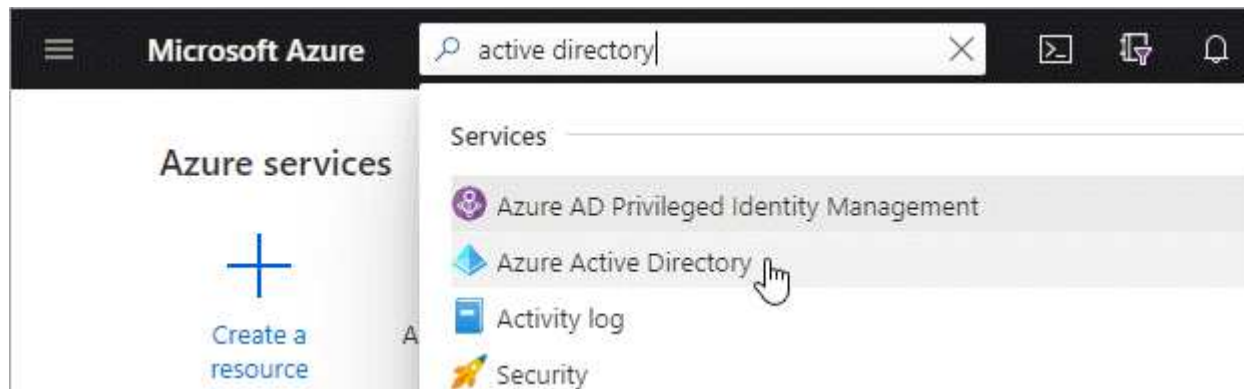
Cloud Manager でコネクタの導入に使用する Azure Active Directory (AD) アプリケーションとサービスプ

リンシパルを作成します。

Azure で Active Directory アプリケーションを作成してロールに割り当てるための適切な権限が必要です。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](#)」。

#### 手順

1. Azure ポータルで、 \* Azure Active Directory \* サービスを開きます。



2. メニューで、 \* アプリ登録 \* をクリックします。
3. [ 新規登録 ] をクリックします。
4. 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。
  - \* アカウントタイプ \* : アカウントタイプを選択します（ Cloud Manager で使用できます）。
  - \* 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。
5. [\*Register] をクリックします。

AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

コネクタを導入する Azure サブスクリプションにサービスプリンシパルをバインドし、カスタムの「Azure SetupAsService」ロールを割り当てる必要があります。

#### 手順

1. をダウンロードします "[Azure の Connector 導入ポリシー](#)"。



リンクを右クリックし、[名前を付けてリンクを保存 ...] をクリックしてファイルをダウンロードする。

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

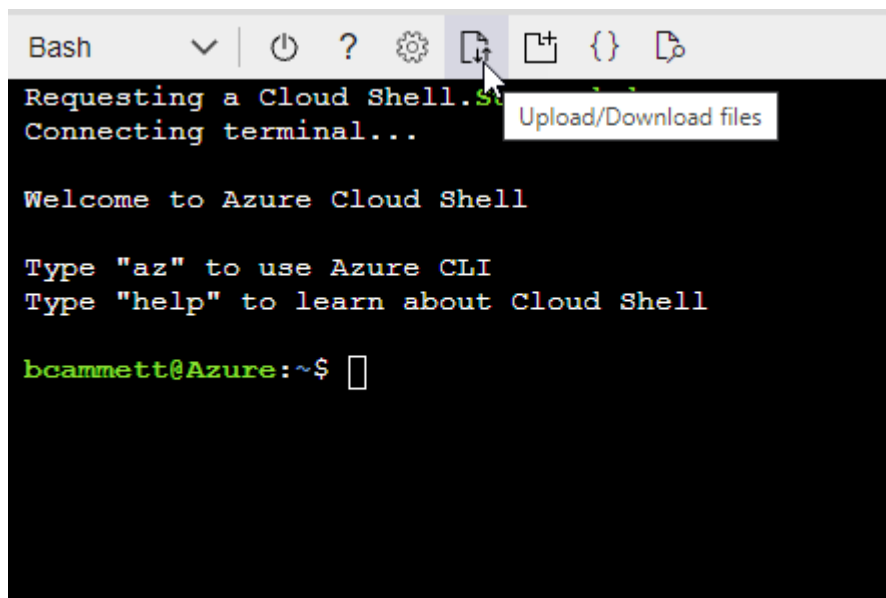
◦ 例 \*

```
"AssignableScopes": [  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzzz"
```

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

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

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



- c. Azure CLI で次のコマンドを入力します。

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

これで、\_Azure SetupAsService\_という カスタムロールが作成されました。

### 4. 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 ]、[ 役割の割り当ての追加 \*] の順にクリックします。
- d. [\* 役割 ( \* Role ) ] タブで、\* Azure SetupAsService \* 役割を選択し、\* 次へ \* をクリックします。
- 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 ] をクリックします。

**Add role assignment** ...

[Got feedback?](#)

**Role**   **Members**   [Review + assign](#)

**Selected role**   Cloud Manager Operator 3.9.12\_B

**Assign access to**   ☒ User, group, or service principal  
☐ Managed identity

**Members**   [+ Select members](#)

- ・ 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。

**Select members** ×

Select ⓘ

test-service-principal

test-service-principal

- アプリケーションを選択し、\* Select \* をクリックします。
- 「\* 次へ \*」 をクリックします。
- a. [ レビュー + 割り当て ( Review + Assign ) ] をクリックします。

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

#### 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. Azure Active Directory \* サービスで、\* アプリ登録 \* をクリックしてアプリケーションを選択します。
2. [API アクセス許可]、[アクセス許可の追加] の順にクリックします。




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













## Request API permissions

### Select an API

Microsoft APIs APIs my organization uses My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

|   |   |  |
|---|---|--|
|  <b>Azure Batch</b><br>Schedule large-scale parallel and HPC applications in the cloud                                       |  <b>Azure Data Catalog</b><br>Programmatic access to Data Catalog resources to register, annotate and search data assets |  <b>Azure Data Explorer</b><br>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions          |
|  <b>Azure Data Lake</b><br>Access to storage and compute for big data analytic scenarios                                     |  <b>Azure DevOps</b><br>Integrate with Azure DevOps and Azure DevOps server  |  <b>Azure Import/Export</b><br>Programmatic control of import/export jobs   |
|  <b>Azure Key Vault</b><br>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults    |  <b>Azure Rights Management Services</b><br>Allow validated users to read and write protected content                  |  <b>Azure Service Management</b><br>Programmatic access to much of the functionality available through the Azure portal                   |
|  <b>Azure Storage</b><br>Secure, massively scalable object and data lake storage for unstructured and semi-structured data |  <b>Customer Insights</b><br>Create profile and interaction models for your products                                   |  <b>Data Export Service for Microsoft Dynamics 365</b><br>Export data from Microsoft Dynamics CRM organization to an external destination |

4. [\* 組織ユーザーとして Azure サービス管理にアクセスする \*] をクリックし、[\* 権限の追加 \*] をクリックします。

## Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

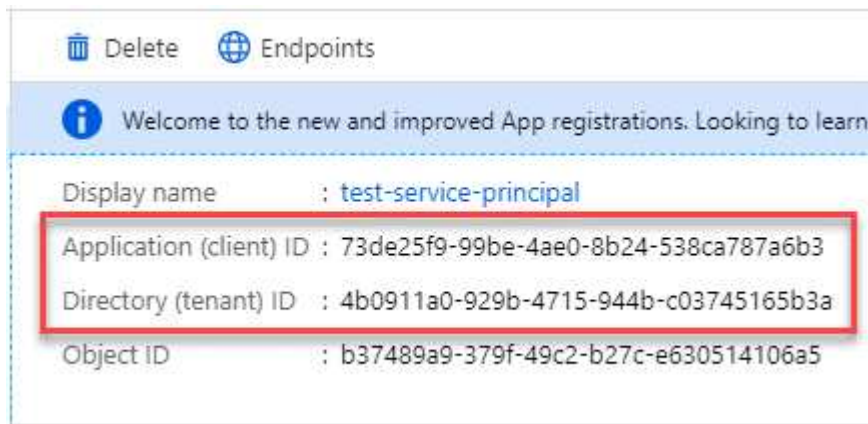
| Type to search   |                        |
|--|------------------------|
| PERMISSION   | ADMIN CONSENT REQUIRED |
| <input checked="" type="checkbox"/> <b>user_impersonation</b><br>Access Azure Service Management as organization users (preview) ⓘ | -                      |

アプリケーション ID とディレクトリ ID を取得します

Cloud Manager でコネクタを作成するときは、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。Cloud Manager は、この ID を使用してプログラムによってサインインします。

手順

1. Azure Active Directory \* サービスで、\* アプリ登録 \* をクリックして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。



クライアントシークレットを作成します

Cloud Manager がクライアントシークレットを使用して Azure AD で認証できるようにするには、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 Cloud Manager に指定する必要があります。

手順

1. Azure Active Directory \* サービスを開きます。
2. [\* アプリ登録 \*] をクリックして、アプリケーションを選択します。

3. [ \* 証明書とシークレット > 新しいクライアントシークレット \* ] をクリックします。
4. シークレットと期間の説明を入力します。
5. [ 追加 (Add) ] をクリックします。
6. クライアントシークレットの値をコピーします。

### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| <a href="#">+ New client secret</a> |           |                                  |
|-------------------------------------|-----------|----------------------------------|
| DESCRIPTION                         | EXPIRES   | VALUE                            |
| test secret                         | 8/16/2020 | *sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA |

Copy to clipboard

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。この情報は、コネクタを作成するときに Cloud Manager で入力する必要があります。

サービスプリンシパルでログインしてコネクタを作成します

Cloud Manager では、ユーザインターフェイスから直接 Azure にコネクタを作成できます。

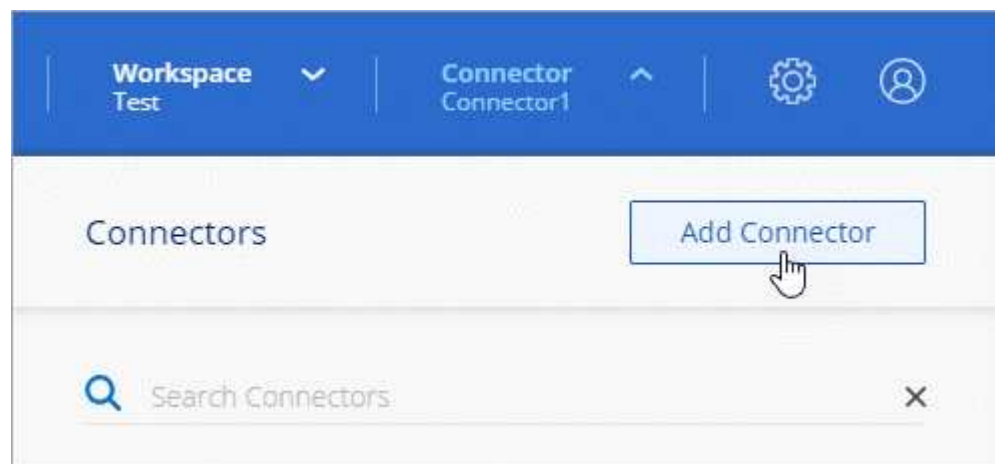
必要なもの

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet およびサブネット
- Cloud Manager で Connector 用の Azure ロールが自動的に作成されないようにするには、独自のを作成する必要があります ["使用するポリシー"](#)。

これらの権限はコネクタインスタンス自体に適用されます。これは、以前にコネクタを展開するように設定したアクセス権とは異なります。

手順

1. 最初の作業環境を作成する場合は、\* 作業環境の追加 \* をクリックし、プロンプトに従います。それ以外の場合は、[connector] ドロップダウンをクリックし、[Add connector] を選択します。



## 2. クラウドプロバイダとして「\* Microsoft Azure \*」を選択します。

Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があります。ことに注意してください。

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

## 3. ウィザードの手順に従って、コネクタを作成します。

- \* Get Ready \* : \* Azure AD サービスプリンシパル \* をクリックし、必要な権限を付与する Azure Active Directory 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 : を参照してください [\[Get the application ID and directory ID\]](#)。
- ディレクトリ（テナント） ID : を参照してください [\[Get the application ID and directory ID\]](#)。
- クライアントシークレット : を参照してください [\[Create a client secret\]](#)。
- \* VM 認証 \* : Azure サブスクリプション、場所、新しいリソースグループ、または既存のリソースグループを選択し、認証方法を選択します。
- \* 詳細 \* : インスタンスの名前を入力し、タグを指定し、必要な権限を持つ新しいロールを Cloud Manager で作成するか、で設定した既存のロールを選択するかを選択します **"必要な権限"**。

このロールに関連付けられているサブスクリプションを選択できます。選択した各サブスクリプションには、Cloud Volumes ONTAP をこれらのサブスクリプションに導入するための権限が Connector に付与されます。

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



コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます **"ローカル UI"**は、まれな状況で使用します。SSH が必要になるのは、トラブルシューティングのためにホストに接続する必要がある場合のみです。

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

## 4. [ 追加（Add） ] をクリックします。

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

ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、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、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。 **"詳細はこちら"**。

# Cloud Manager から Google Cloud でコネクタを作成します

Cloud Manager のほとんどの機能を使用するには、Account Admin が \_Connector を導

入する必要があります。 ["コネクタが必要になるタイミングを学習します"](#)。Connector を使用すると、Cloud Manager で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できます。

このページでは、Cloud Manager から GCP でコネクタを直接作成する方法について説明します。 ["コネクタを配置するその他の方法について説明します"](#)。

これらの手順は、Account Admin ロールを持つユーザが実行する必要があります。ワークスペース管理者はコネクタを作成できません。



最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、Cloud Manager からコネクタの作成を求められます。

## 権限を設定しています

Connector を展開する前に、GCP アカウントに正しい権限があること、および Connector VM のサービスアカウントが設定されていることを確認する必要があります。

### 手順

1. コネクタを展開する GCP ユーザーが、で権限を持っていることを確認します ["GCP の Connector 展開ポリシー"](#)。

["YAML ファイルを使用してカスタムロールを作成できます"](#) ユーザーに添付します。gcloud コマンドラインを使用して、ロールを作成する必要があります。

2. 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 Cloud Manager 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。

このサービスアカウントは、作成時に Connector VM に関連付けます。

- 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"](#)。ここでも gcloud コマンドラインを使用する必要があります。

この YAML ファイルに含まれる権限は、手順 1 の権限とは異なります。

- 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. 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。

これで、GCP ユーザーはコネクタの作成に必要な権限を持ち、Connector VM のサービスアカウントが設定されました。

### 共有 VPC の権限

共有 VPC を使用してリソースをサービスプロジェクトに導入する場合は、次の権限が必要です。IAM の設定が完了したら、この表を参考にして権限の表を環境に反映させる必要があります。

| サービスアカウント                              | 作成者  | でホストされています | サービスプロジェクトの権限   | ホストプロジェクトの権限  | 目的  |
|--|------|------------|---|---|---|
| Cloud Manager サービスアカウント                | カスタム | サービスプロジェクト | <ul style="list-style-type: none"> <li>• "この <a href="#">.yaml ファイルで見つかった権限</a>"</li> </ul>   | <ul style="list-style-type: none"> <li>• compute.networkUser</li> <li>• deploymentmanager.editor</li> </ul> | サービスプロジェクトへの Cloud Volumes ONTAP とサービスの導入と保守                                |
| Cloud Volumes ONTAP サービスアカウント          | カスタム | サービスプロジェクト | <ul style="list-style-type: none"> <li>• storagec.admin</li> <li>• メンバー：Cloud Manager サービスアカウント。<br/>serviceAccount.user</li> </ul> | 該当なし  | (オプション) データ階層化と Cloud Backup に使用できます  |
| Google API サービスエージェント                  | GCP  | サービスプロジェクト | <ul style="list-style-type: none"> <li>• (デフォルト) Editor</li> </ul>  | <ul style="list-style-type: none"> <li>• compute.networkUser</li> </ul>                                     | 導入に代わって GCP API とやり取りします。Cloud Manager で共有ネットワークを使用できるようにします。               |
| Google Compute Engine のデフォルトのサービスアカウント | GCP  | サービスプロジェクト | <ul style="list-style-type: none"> <li>• (デフォルト) Editor</li> </ul>  | <ul style="list-style-type: none"> <li>• compute.networkUser</li> </ul>                                     | 導入に代わって GCP インスタンスとコンピューティングインフラを導入します。Cloud Manager で共有ネットワークを使用できるようにします。 |

注：

1. deploymentmanager.editor は、ファイアウォールルールを導入環境に渡しておらず、Cloud Manager に作成を許可することを選択している場合にのみホストプロジェクトで必要です。ルールを指定しない場合、Cloud Manager はホストプロジェクトに導入を作成し、VPC0 ファイアウォールルールを適用します。
2. Firewall.create および firewall.delete が必要となるのは、ファイアウォールルールを導入環境に渡しず、Cloud Manager で作成することを選択している場合だけです。これらの権限は、Cloud Manager サービスアカウントの .yaml ファイルに格納されています。共有 VPC を使用して HA ペアを導入する場合は、これらの権限を使用して VPC1、2、および 3 のファイアウォールルールが作成されます。他のすべての展開では、これらの権限は VPC0 のルールの作成にも使用されます。
3. データ階層化の場合、階層化サービスアカウントは、プロジェクトレベルだけでなく、サービスアカウントに対して serviceAccount.user ロールを持つ必要があります。現在、プロジェクトレベルで serviceAccount.user を割り当てている場合、getIAMPolicy でサービスアカウントを照会しても権限は表示されません。

## Google Cloud API の有効化

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



## ステップ

### 1. "プロジェクトで次の Google Cloud API を有効にします"。

- Cloud Deployment Manager V2 API
- クラウドロギング API
- Cloud Resource Manager API の略
- Compute Engine API
- ID およびアクセス管理（IAM）API

## GCP でコネクタを作成する

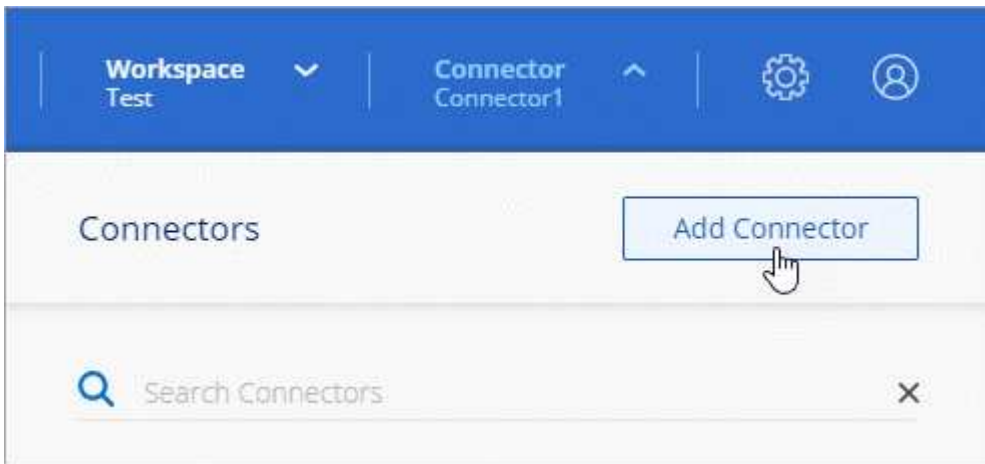
Cloud Manager ユーザインターフェイスから直接、または gcloud を使用して、Google Cloud でコネクタを作成する。

### 必要なもの

- "必要な権限" Google Cloud アカウントの場合は、このページの最初のセクションで説明します。
- Google Cloud プロジェクト。
- このページの最初のセクションで説明するように、Cloud Volumes ONTAP の作成と管理に必要な権限を持つサービスアカウント。
- Google Cloud リージョン内の VPC とサブネット。

## クラウドマネージャ

1. 最初の作業環境を作成する場合は、\* 作業環境の追加 \* をクリックし、プロンプトに従います。それ以外の場合は、[connector] ドロップダウンをクリックし、[Add connector] を選択します。



2. クラウドプロバイダとして \* Google Cloud Platform \* を選択します。

Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があることに注意してください。

["Connector のネットワーク要件の詳細については、こちらをご覧ください"](#)。

3. ウィザードの手順に従って、コネクタを作成します。

- \* 準備をしてください \* : 必要なものを確認してください。
- プロンプトが表示されたら、Google アカウントにログインします。このアカウントには、仮想マシンインスタンスを作成するために必要な権限が付与されている必要があります。

このフォームは Google が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

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



コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます。"ローカル UI"は、まれな状況で使用します。SSH が必要になるのは、トラブルシューティングのためにホストに接続する必要がある場合のみです。



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

4. [ 追加 ( Add ) ] をクリックします。

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

## gcloud

1. ご希望の方法で gcloud SDK にログインします。

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

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

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

```
gcloud auth list
```

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

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

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

```
gcloud compute instances create <instance-name>
  --machine-type=n1-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

### インスタンス名

VM インスタンスに必要なインスタンス名。

### プロジェクト

(オプション) VM を導入するプロジェクト。

### service-account のことです

手順 2 の出力で指定したサービスアカウント。

### ゾーン

VM を導入するゾーン

### no-address

(オプション) 外部 IP アドレスは使用されません (パブリックインターネットにトラフィックをルーティングするには、クラウド NAT またはプロキシが必要です)。

### ネットワークタグ

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

### network-path

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

### subnet-path」を指定します

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

### kms -key-path

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

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

ト"。

+

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

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

`http://ipaddress:80[]`

2. ログイン後、コネクタを設定します。
  - a. コネクタに関連付ける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"](#)。

## 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.