



# Cloud Manager の管理

## Set up and administration

NetApp  
July 13, 2022

# 目次

Cloud Manager の管理 .....	1
ネットアップアカウント .....	1
コネクタ .....	17
AWS クレデンシャル .....	45
Azure のクレデンシャル .....	53
Google Cloud のクレデンシャル .....	65
Cloud Manager でネットアップサポートサイトのアカウントを追加および管理します .....	73

# Cloud Manager の管理

## ネットアップアカウント

### ネットアップアカウントの管理

"初期セットアップを実行したあと"では、後でユーザー、サービスアカウント、ワークスペース、コネクタ、およびサブスクリプションを管理することで、アカウント設定を管理できます。

"ネットアップアカウントの仕組みをご覧ください"。

テナンシー **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 の作業環境の作成と管理に使用する Cloud Manager 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"

### ユーザの作成と管理

アカウント内のユーザーは、アカウントのワークスペース内のリソースを管理するためにアクセスできます。

### ユーザを追加する

Cloud Central ユーザをネットアップアカウントに関連付けて、これらのユーザが Cloud Manager で作業環境を作成および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 Cloud Central" 登録してください。
2. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックします。



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 \* ] をクリックします。



4. メンバータブで、\* ユーザーを関連付け \* をクリックします。
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。
  - \* アカウント管理者 \* : Cloud Manager で任意の操作を実行できます。
  - \* 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 \* : クラウドデータセンスのコンプライアンス情報のみを表示し、アクセス権限のあるワークスペースのレポートを生成できます。
  - \* SnapCenter Admin\* : SnapCenter サービスを使用して、アプリケーションと整合性のあるバックアップを作成し、それらのバックアップを使用してデータをリストアできます。\_ このサービスは現在ベータ版です。 \_
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。



The image shows a web interface for associating a user. At the top is a user icon and the title "Associate User". Below this is a light blue box with instructions: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below the instructions are three input fields: "User's Email" with the value "test@netapp.com", "Role" with the value "Workspace Admin", and "Associate User to Workspaces" with the value "Workspace-1". At the bottom are two buttons: "Cancel" and "Associate User".



## Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. [ 関連付け（Associate） ] をクリックします。

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

#### ユーザの削除

ユーザが割り当てを解除すると、ネットアップ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. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。



2. メンバー (Members) タブで 'ユーザー' に対応する行のアクションメニューをクリックします

5 Members

Type	Name	Email	Role	Workspace	
	Ben		☆ Account Admin	All Workspaces	...
	Tom		☆ Account Admin	All Workspaces	...
	Ben		Workspace Admin	Newone	

3. [ ユーザーの関連付けを解除 ( Disassociate User ) ] をクリックし、[ 関連付けを解除 ( Disassociate ) ] をクリックして

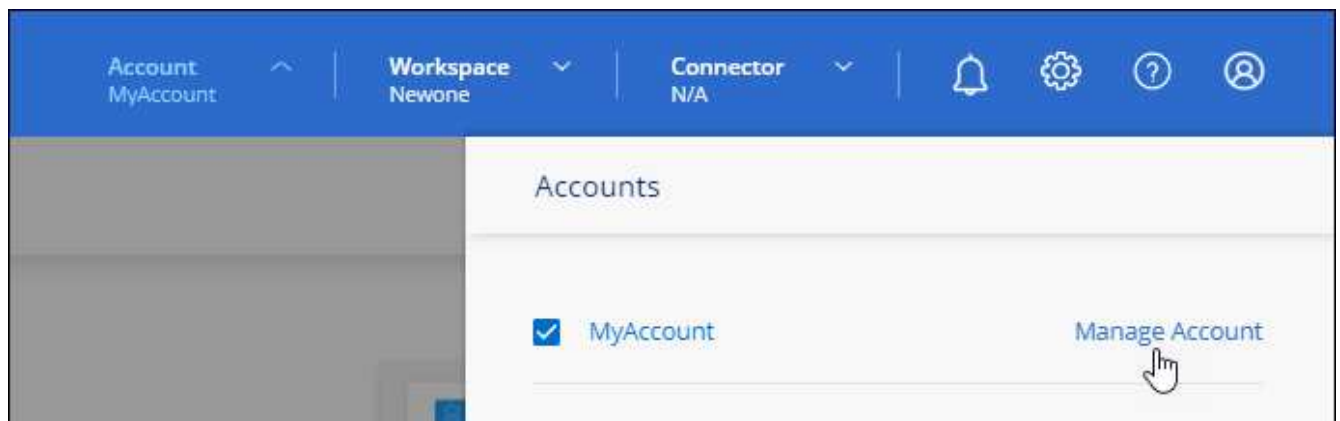
ユーザはこのネットアップアカウントのリソースにアクセスできなくなります。

ワークスペース管理者のワークスペースの管理

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。ユーザーに関連付けると、ワークスペース内の作業環境を作成して表示できます。

手順

1. Cloud Manager の上部で、 \* Account \* ドロップダウンをクリックし、 \* Manage Account \* をクリックします。



- メンバー (Members) タブで 'ユーザー' に対応する行のアクションメニューをクリックします



Type	Name	Email	Role	Workspace	
👤	Ben		☆ Account Admin	All Workspaces	⋮
👤	Tom		☆ Account Admin	All Workspaces	⋮
👤	Ben		Workspace Admin	Newone	⋮

- \* ワークスペースの管理 \* をクリックします。
- ユーザーに関連付けるワークスペースを選択し、\* 適用 \* をクリックします。

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 Cloud Manager 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の作成と管理

サービスアカウントは「ユーザ」の役割を果たし、Cloud Manager に対して自動化のための許可された API 呼び出しを実行できます。これにより、自動化スクリプトを作成する必要がなくなります。自動化スクリプトは、会社を離れることができる実際のユーザアカウントに基づいて作成する必要がなくなります。フェデレーションを使用している場合は、クラウドから更新トークンを生成することなくトークンを作成できます。

サービスアカウントには、他の Cloud Manager ユーザと同様にロールを割り当てることで権限を付与します。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、Cloud Manager で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、Cloud Manager との認証に使用されます。

### サービスアカウントの作成

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

- Cloud Manager の上部で、\* Account \* ドロップダウンをクリックします。



- 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 \* ] をクリックします。



3. メンバータブで、\* サービスアカウントの作成 \* をクリックします。
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. [ 作成 ( Create ) ] をクリックします。
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、Cloud Manager では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 \*] をクリックします。

サービスアカウントのベアラートークンを取得する

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。

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' \
--header 'Content-Type: application/json' \
--data-raw '{
  "grant_type": "client_credentials",
  "client_secret": "<client secret>",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "<client id>"
}'
```

クライアント ID をコピーしています

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クリックします。





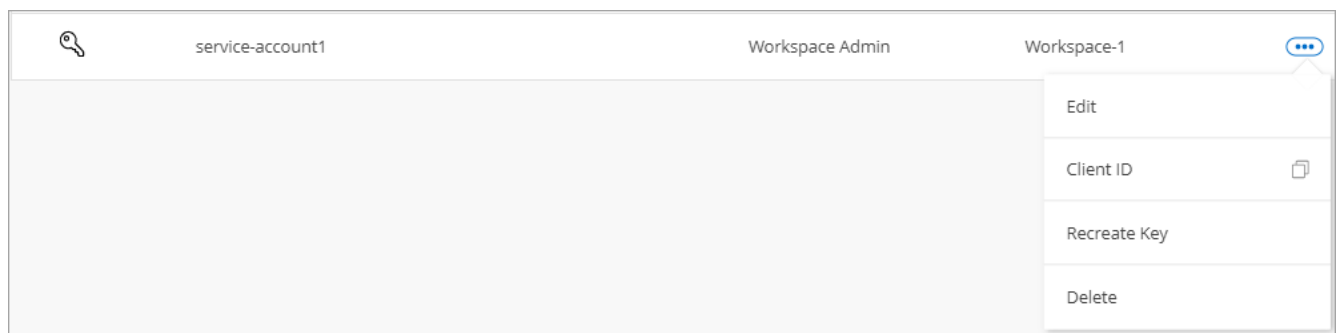
2. [クライアント ID] をクリックします。
3. ID がクリップボードにコピーされます。

キーの再作成中です

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。前のキーを使用することはできません。

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クリックします。



2. [キーの再作成 \*] をクリックします。
3. 再作成 \* をクリックして確定します。
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、Cloud Manager では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 \*] をクリックします。

サービスアカウントを削除する

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クリックします。



2. [ 削除（Delete） ] をクリックします。
3. 再度 \* Delete \* をクリックして確定します。

## ワークスペースの管理

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. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
2. [\* ワークスペース \*] をクリックします。
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を作成するには、\* 新しいワークスペースを追加 \* をクリックします。
  - \* 名前変更 \* をクリックして、ワークスペースの名前を変更します。
  - ワークスペースを削除するには、\* 削除 \* をクリックします。

## コネクタのワークスペースを管理する

ワークスペース管理者が Cloud Manager 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、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。

["ユーザー、ワークスペース、コネクタの詳細をご覧ください"](#)。

### 手順

1. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
2. コネクタ（\* Connector）をクリックします。
3. 関連付けるコネクタの \* ワークスペースの管理 \* をクリックします。
4. コネクタに関連付けるワークスペースを選択し、\* 適用 \* をクリックします。

## サブスクリプションの管理

クラウドプロバイダのマーケットプレイスからサブスクライブすると、各サブスクリプションはアカウント設定ウィジェットから利用できます。サブスクリプションの名前を変更したり、1つまたは複数のアカウントからサブスクリプションの関連付けを解除したりすることができます。

たとえば、2つのアカウントがあり、それぞれが別々のサブスクリプションで課金されるとします。いずれかのアカウントとサブスクリプションの関連付けを解除することで、Cloud Volume ONTAP 作業環境の作成時にそのアカウントのユーザが誤って誤ったサブスクリプションを選択しないようにすることができます。

"サブスクリプションの詳細については、こちらをご覧ください"。

### 手順

1. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
2. [サブスクリプション] をクリックします。

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。

3. 管理するサブスクリプションに対応する行のアクションメニューをクリックします。



Name	Service	Cloud Provider	Status
QA Subscription	test-service	aws	Unsubscribed
metering service subscription QA !!!!	cloud-volumes-ontap	aws	Subscribed

4. サブスクリプションの名前を変更するか、サブスクリプションに関連付けられているアカウントを管理するかを選択します。

### アカウント名を変更する

アカウント名はいつでも変更して、わかりやすい名前に変更してください。

### 手順

1. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
2. 「\* 概要 \*」タブで、アカウント名の横にある編集アイコンをクリックします。
3. 新しいアカウント名を入力し、\* 保存 \* をクリックします。

### 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有効にすると、Cloud Manager でプレビュー版として提供される新しい NetApp クラウドサービスにアクセスできるようになります。

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. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
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。

#### サードパーティサービスを許可しています

アカウント内のサードパーティサービスが、Cloud Manager で使用可能なサードパーティサービスにアクセスできるようにします。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. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
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。

#### SaaS プラットフォームを無効にする

会社のセキュリティポリシーに準拠するために必要な場合を除き、SaaS プラットフォームを無効にすることはお勧めしません。SaaS プラットフォームを無効にすると、ネットアップの統合クラウドサービスを使用できなくなります。

SaaS プラットフォームを無効にすると、Cloud Manager から次のサービスを使用できなくなります。

- クラウドデータの意味
- Kubernetes
- クラウド階層化
- グローバルファイルキャッシュ

SaaS プラットフォームを無効にする場合は、からすべてのタスクを実行する必要があります ["コネクタで使用する可能なローカルユーザインターフェイス"](#)。



これは元に戻すことができない操作であり、Cloud Manager SaaS プラットフォームを使用できなくなります。ローカルコネクタからアクションを実行する必要があります。ネットアップの統合クラウドサービスの多くを利用することはできません。また、SaaS プラットフォームを再度有効にするには、ネットアップのサポートが必要になります。

#### 手順

1. Cloud Manager の上部で、\* Account \* ドロップダウンをクリックし、\* Manage Account \* をクリックします。
2. [概要] タブで、SaaS プラットフォームの使用を無効にするオプションを切り替えます。

#### アカウントでの操作の監視

Cloud Manager で実行されている処理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。

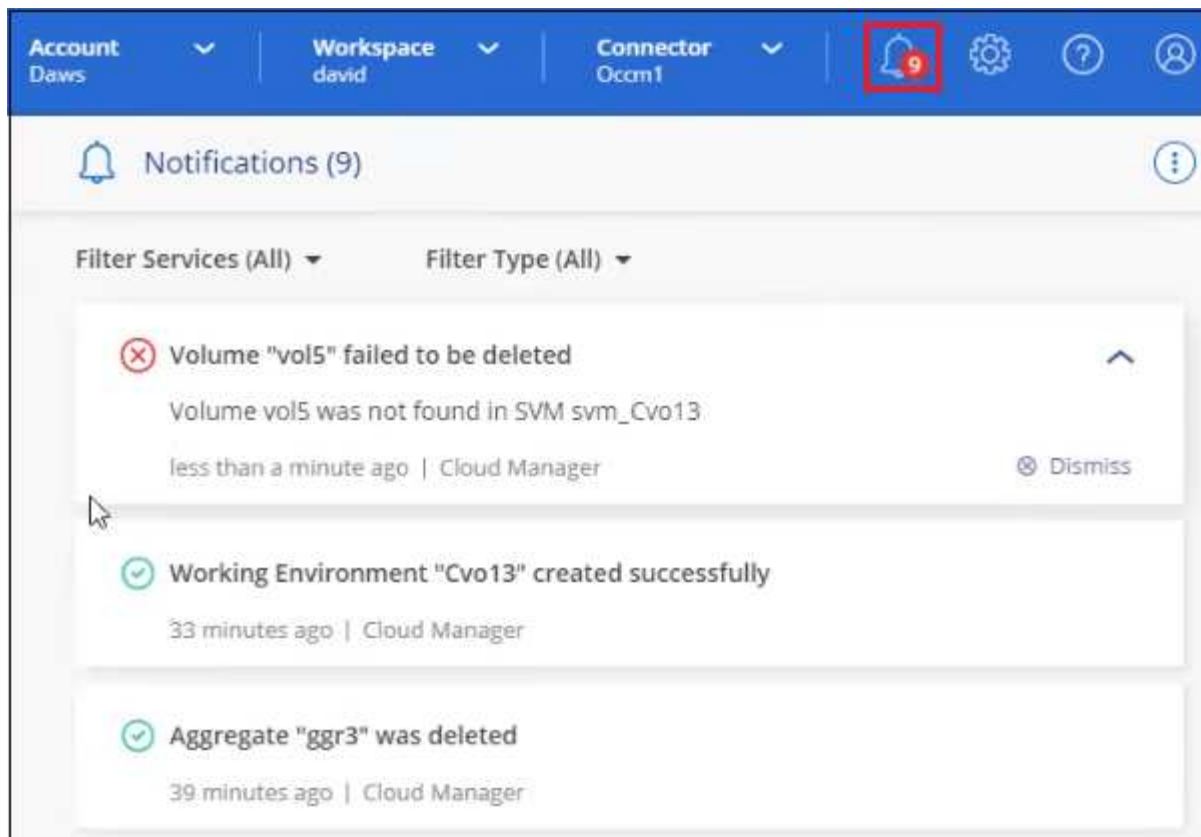
次の表は、通知センターとタイムラインの比較を示しています。これにより、それぞれの機能を理解することができます。

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。ログオフすると、通知センターに情報が表示されなくなります	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
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たアクティビティの監視

通知には、Cloud Managerで開始した処理の進捗状況が追跡されるため、処理が成功したかどうかを確認できます。現在のログインセッションで開始した多くのCloud Manager処理のステータスを表示できます。現時点では、すべての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。

通知を表示するには、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、Cloud ManagerからEメールで通知を送信するように設定することで、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、NetApp Cloud Accountの一部であるCloud Centralユーザ、または特定のタイプのシステムアクティビティを認識する必要のあるその他の受信者に送信できます。を参照してください [Eメール通知を設定しています](#) 下。

#### 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。

#### 通知のフィルタリング

デフォルトでは、すべての通知が表示されます。通知センターに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。Cloud Manager の「サービス」および通知の「タイプ」でフィルタできます。

The image shows a user interface for filtering notifications in Cloud Manager. It consists of two side-by-side panels, each with a title and a list of items with checkboxes, and buttons at the bottom.

**Filter Services (All) ▲**

- ☒ Digital Wallet (3)
- ☒ Active IQ (2)
- ☐ AppTemplate (1)

Buttons: Clear, Apply

**Filter Type (All) ▲**

- ☐ Information (0)
- ☐ Success (1)
- ☒ Warning (2)
- ☒ Error (1)
- ☒ Critical (0)
- ☐ Recommendation (0)

Buttons: Clear, Apply

たとえば、Cloud Manager の処理に対する「エラー」通知と「警告」通知のみを表示する場合は、それらのエントリを選択します。表示される通知のタイプはでのみです。

#### Eメール通知を設定しています

特定のタイプの通知をEメールで送信することで、Cloud Manager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、ネットアップアカウントの一部であるユーザや、特定のタイプのシステムアクティビティについて認識しておく必要のあるその他の受信者に送信することができます。

注意：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、電子メール通知の送信はサポートされていません。

デフォルトでは、アカウント管理者はすべての「重大」通知と「推奨事項」通知のEメールを受信します。他のすべてのユーザと受信者は、通知メールを受信しないようにデフォルトで設定されています。

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。

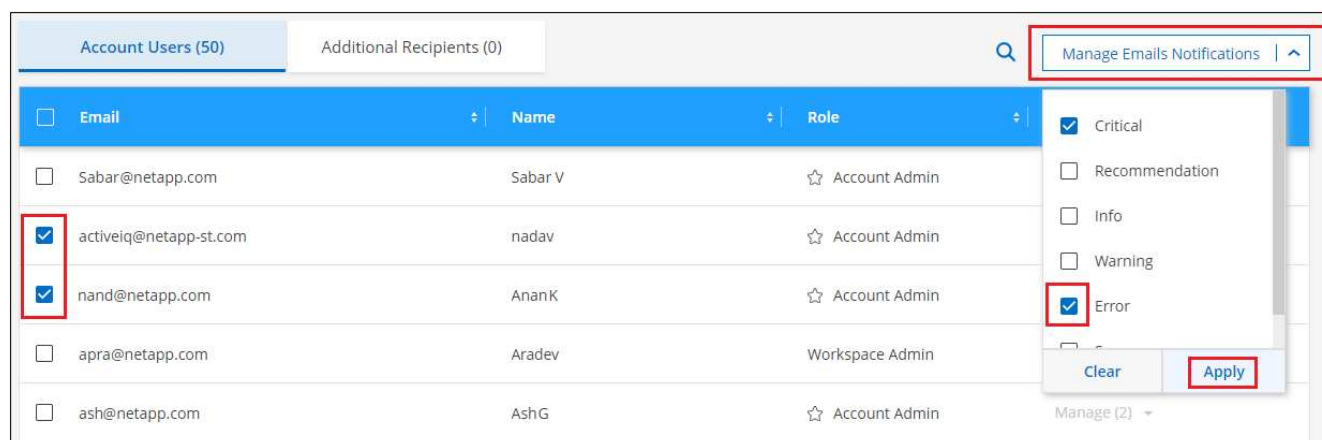
#### 手順

1. Cloud Managerのメニューバーで、\* Settings > Alerts and Notifications Settings \*の順にクリックします。



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人のユーザーに変更を加えるには、そのユーザーの通知列のメニューをクリックし、送信する通知の種類を確認して、\*適用\*をクリックします。
- 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、\*電子メール通知の管理\*をクリックして、送信する通知の種類を選択し、\*適用\*をクリックします。



Eメール受信者を追加しています

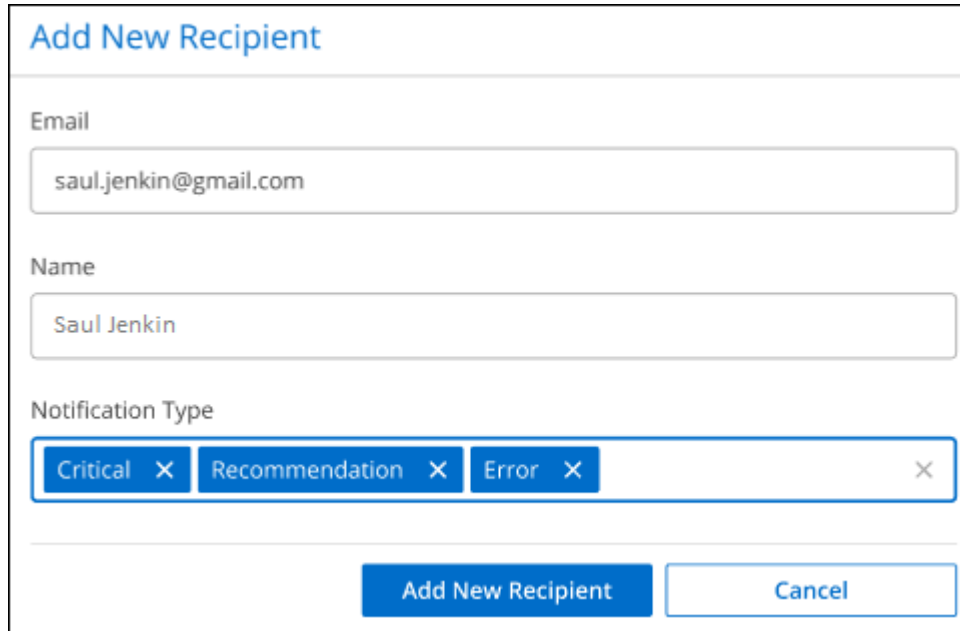
\_Account Users\_ タブに表示されるユーザには、ネットアップアカウントのユーザの情報が自動的に入力されます（から） " [\[アカウントの管理\] ページ](#) )。Cloud Managerにアクセスできないものの、特定の種類のアラートと通知に関する通知を受け取る必要がある他のユーザまたはグループの場合は、\_Additional



Recipients\_tabにEメールアドレスを追加できます。

手順

1. [Alerts and Notifications Settings]ページで、[Add New Recipients]をクリックします。

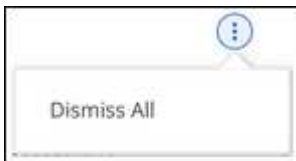


2. 名前、電子メールアドレスを入力し、受信者が受け取る通知の種類を選択して、\*新しい受信者の追加\*をクリックします。

通知が欠落します

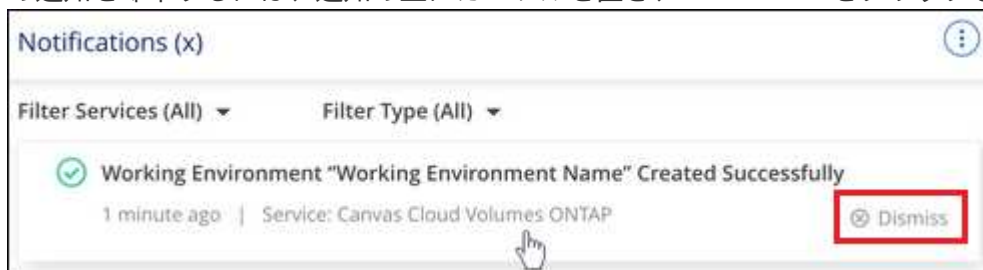
通知が不要になった場合は、ページから削除できます。すべての通知を一度に却下することも、個々の通知を却下することもできます。

すべての通知を却下するには、通知センターでをクリックします。をクリックして、[すべてを却下]を選択



します。

個々の通知を却下するには、通知の上にカーソルを置き、\*Dismiss\*をクリックしま



す。

アカウント内のユーザアクティビティを監査する

Cloud Manager のタイムラインには、アカウントの管理用にユーザが完了した操作が表示されます。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. Cloud Managerのメニューバーで、\* Settings > Timeline \*をクリックします。
2. [フィルタ]で、[サービス\*]、[テナント\*]の順にクリックし、[適用\*]をクリックします。

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。

#### 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。

Compliance Viewer ロールは、読み取り専用の Cloud Data Sense 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
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
データセンススキャンの結果を表示します	はい。	はい。	はい。	いいえ
作業環境を削除します	はい。	いいえ	いいえ	いいえ
Kubernetes クラスタを作業環境に接続	はい。	いいえ	いいえ	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
ネットアップアカウントを管理	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
Cloud Manager の設定を変更	はい。	いいえ	いいえ	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
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
Cloud Manager から作業環境を削除します	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
SnapCenter サービスを使用します	はい。	はい。	いいえ	はい。

#### 関連リンク

- ["ネットアップアカウントでワークスペースとユーザをセットアップ"](#)
- ["ネットアップ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

### 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

- EC2 インスタンス用の IAM ポリシーとロールを作成します。
  - 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"](#)
  - 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。
  - 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。
- 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 ユーザがサブスクライブとサブスクライブ解除を行うには、AWS Marketplace の権限が必要です。
- [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](#)

Continue to Subscribe

Save to List

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す "[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-V3.9.19.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-V3.9.19.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。

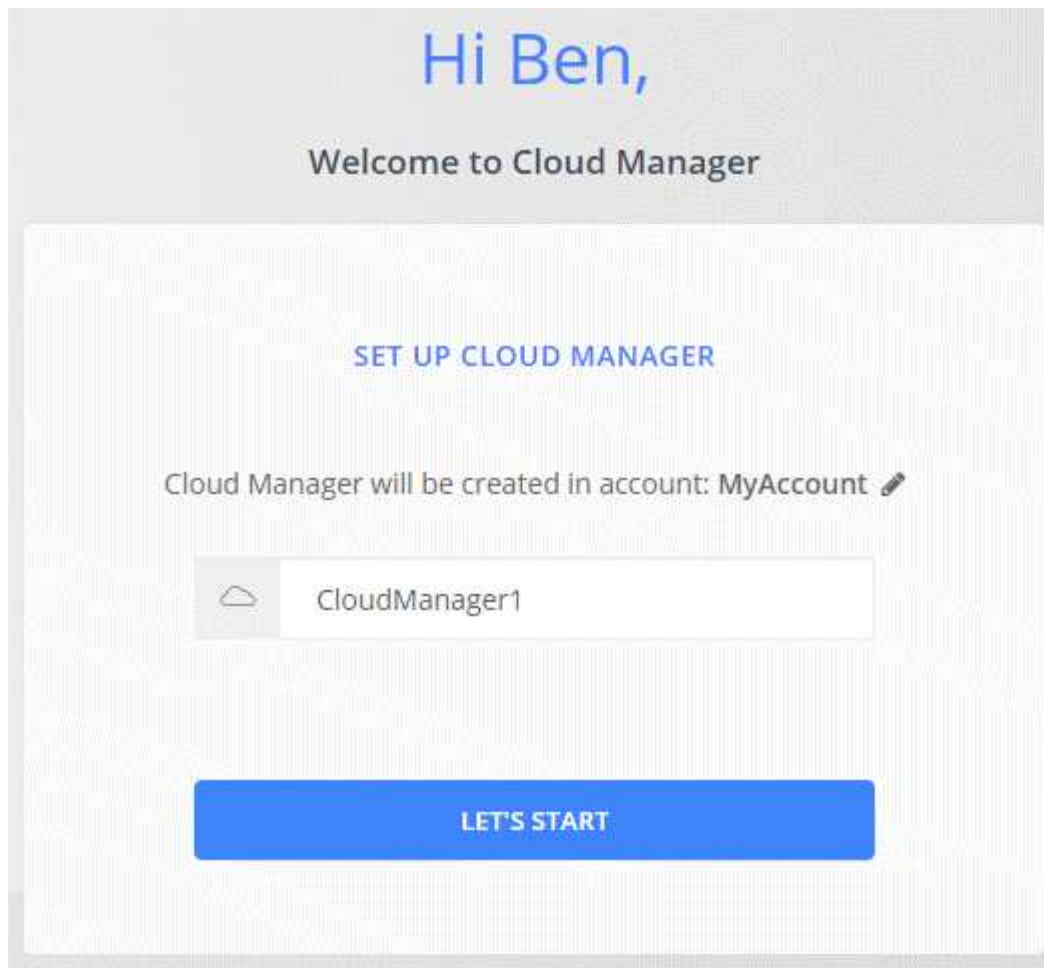
Cloud Manager がインストールされました。プロキシサーバを指定した場合、インストールの最後に Cloud Manager Service (OCCM) が 2 回再起動します。

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、Cloud Backupを使用してボリュームをバックアップし、Cloud Data Senseでスキャンできます。

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-v3.9.19
```

5. インストールスクリプトを実行します。

```
sudo /path/cloud-manager-connector-offline-v3.9.19
```

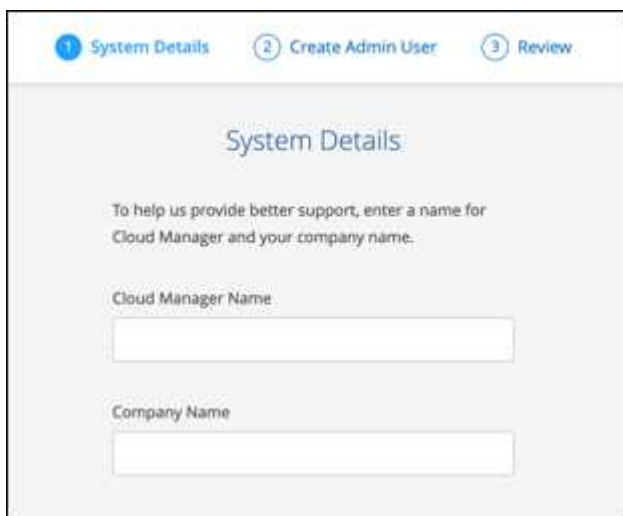
6. Web ブラウザを開き、と入力します `https://ipaddress[]` ここで、`ipaddress` は Linux ホストの IP アドレスです。

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"
- "クラウドバックアップを使用して、オンプレミスのONTAP ボリュームのデータをStorageGRID にバックアップします"
- "クラウドデータセンズを使用してオンプレミスのONTAP ボリュームデータをスキャン"

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

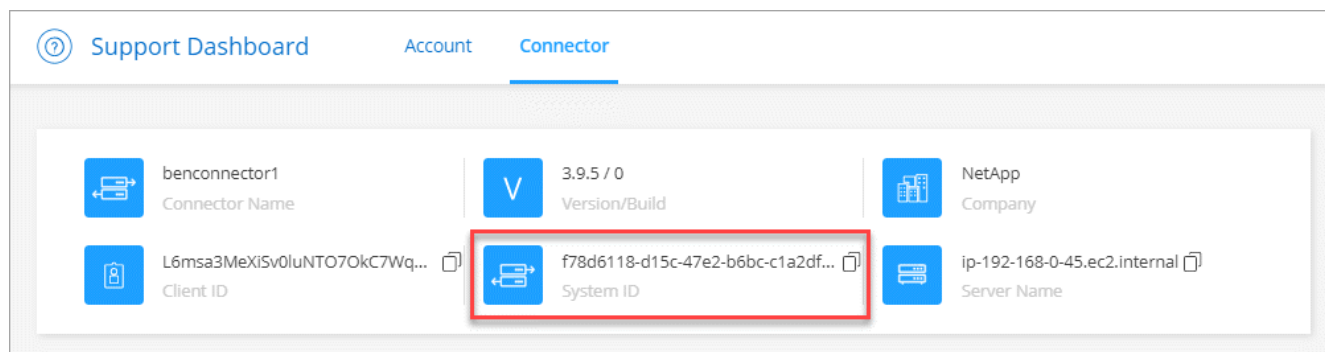
1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックします。



## 2. [ サポート ( Support ) ] > [ コネクタ ( 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 ユーザー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、ローカルユーザーインターフェイスは引き続きコネクタで使用できます。政府機関のリージョンまたはアウトバウンドのインターネットアクセスがないサイトからCloud Managerにアクセスする場合は、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イスを使用する必要があります。

### 手順

1. Web ブラウザを開き、次の URL を入力します。

`https://ipaddress[]`

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

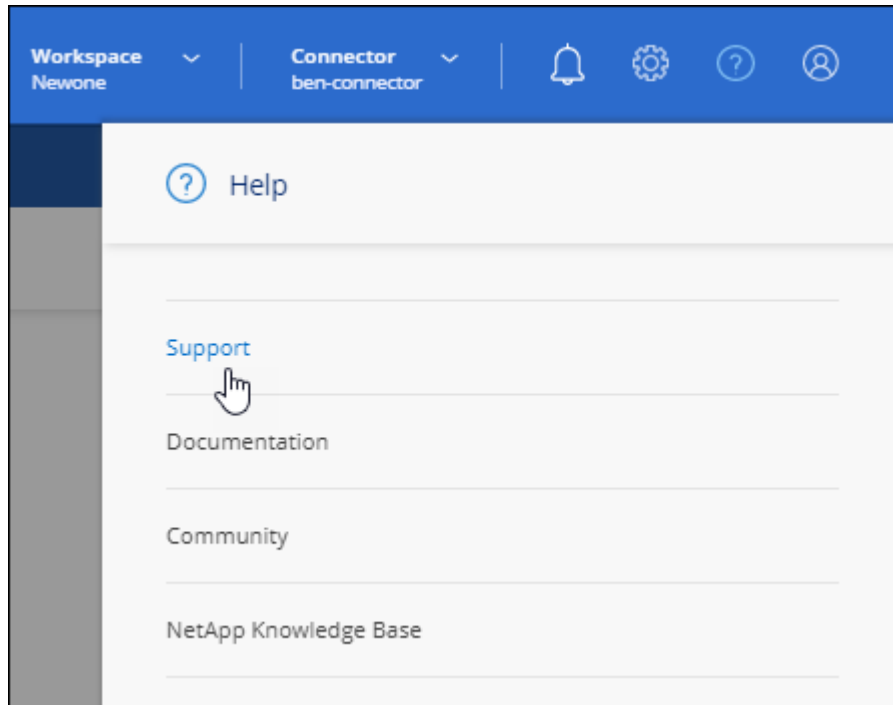
2. ログインするためのユーザ名とパスワードを入力します。

### 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

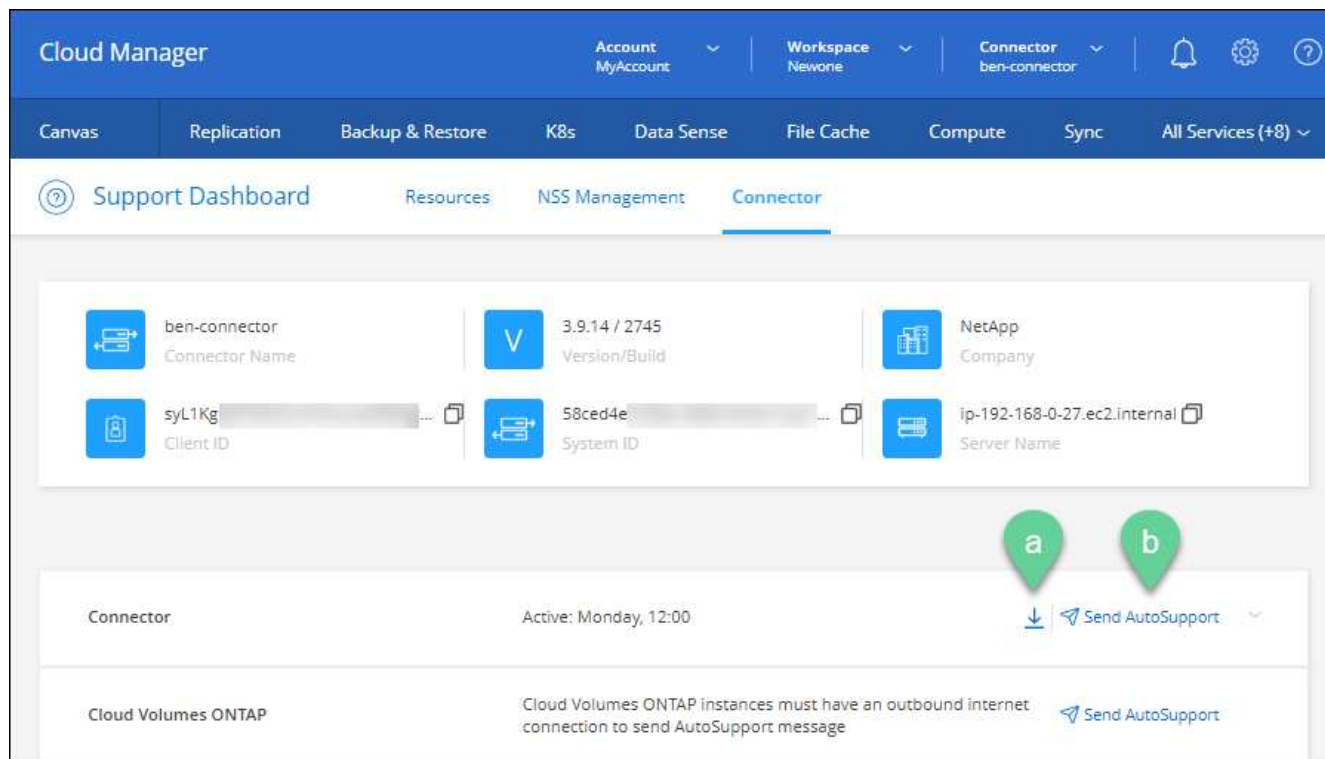
1. 上のセクションの説明に従って、コネクタローカル UI に接続します。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、\* Support \* を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

3. コネクター（\* 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。
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。
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。
  - 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削除します。

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

- b. Cloud Manager に移動して、作業環境を開きます。
- c. メニューをクリックして、\* Advanced > Configuration Backups \* を選択します。
- d. [\* 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

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. [\* コネクターの管理 \*] をクリックします。
3. 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。
4. 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

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"](#)。

### 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

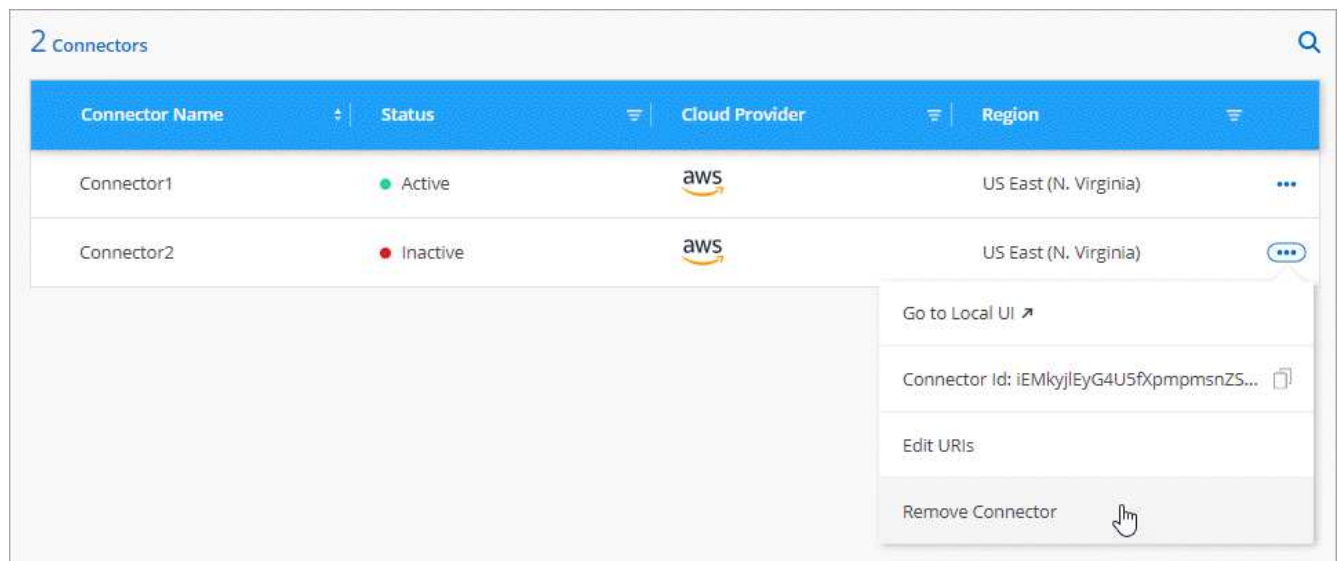
非アクティブなコネクタは、Cloud Manager のコネクタのリストから削除できます。この処理は、Connector 仮想マシンを削除した場合や Connector ソフトウェアをアンインストールした場合に実行できます。

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. [\* コネクターの管理 \*] をクリックします。
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。

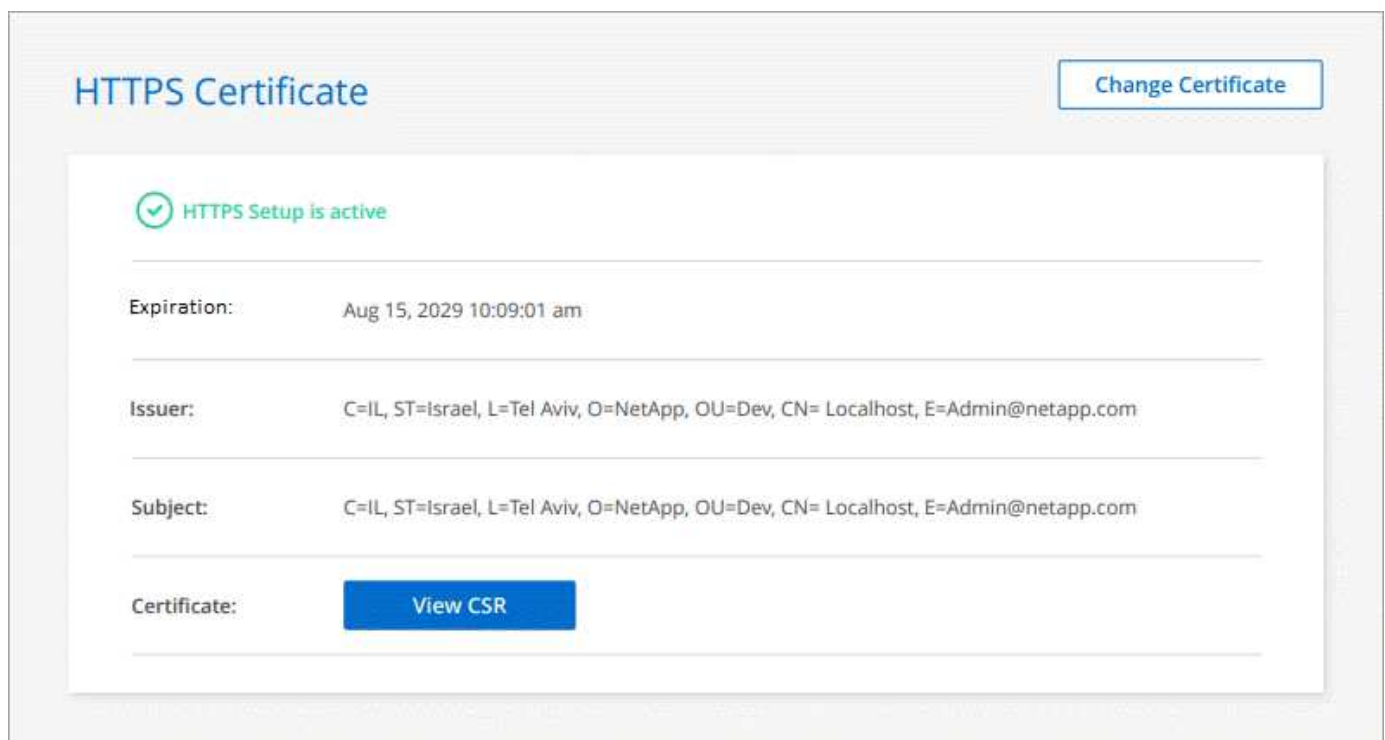




2. [HTTPS Setup] ページで、証明書署名要求（CSR）を生成するか、独自の CA 署名付き証明書をインストールして、証明書をインストールします。

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>
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

導入前にコネクタの詳細を確認したり、問題のトラブルシューティングが必要な場合に利用できます。

### インターネットアクセスを使用するデフォルト設定

以下の構成の詳細は、Cloud Manager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

Cloud Manager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ている場合は、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Red Hat Enterprise Linux 7.6 (HVM) 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ec2-userです。
- デフォルトのシステムディスクは50GiBのgp2ディスクです。

#### Azureの詳細

Cloud Manager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ている場合は、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CentOS 7.6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

Cloud Manager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ている場合は、次の点に注意してください。

- VMインスタンスはn1-standard-4です。
- イメージのオペレーティングシステムはCentOS 7.9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

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。

#### コネクタサービス

- 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。

#### パッケージ

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

## 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
- 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/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

# AWS クレデンシアル

## AWS のクレデンシアルと権限

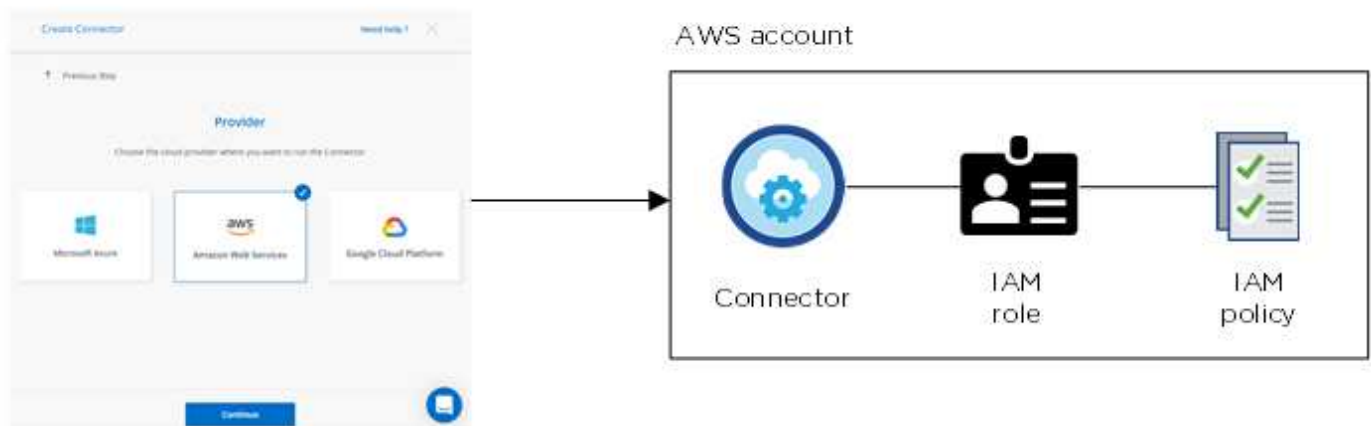
Cloud Manager では、Cloud Volumes ONTAP の導入時に使用する AWS クレデンシアルを選択できます。すべての Cloud Volumes ONTAP システムは、初期の AWS クレデンシアルを使用して導入することも、クレデンシアルを追加することもできます。

### AWS の初期クレデンシアル

Cloud Manager からコネクタを導入する場合は、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"](#)。

Cloud Manager が AWS でコネクタインスタンスを起動すると、インスタンス用の 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。 ["Cloud Manager での権限の使用方法を確認します。"](#)。

#### Cloud Manager



Cloud Volumes ONTAP の新しい作業環境を作成すると、Cloud Manager で選択される AWS クレデンシアルにはデフォルトで次のものがあります。

Details & Credentials			
Instance Profile		QA Subscription	<a href="#">Edit Credentials</a>
Credentials	Account ID	Marketplace Subscription	

### 追加の AWS クレデンシアル

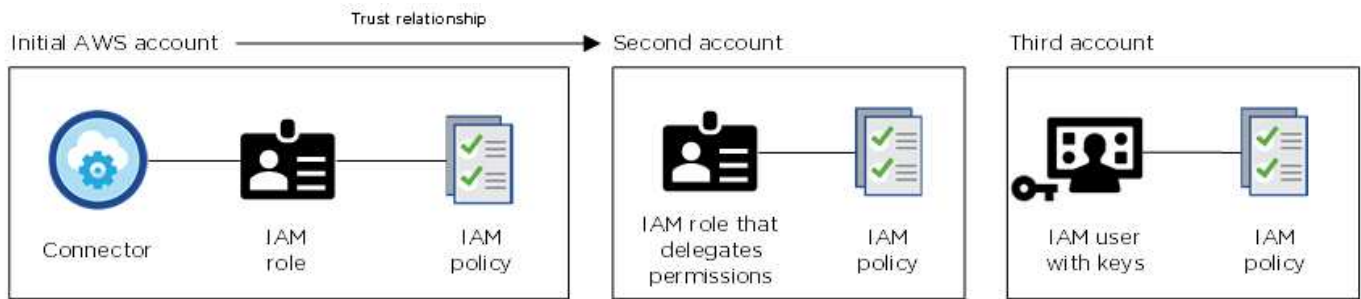
AWS クレデンシアルを追加する方法は 2 種類あります。

#### AWS クレデンシアルを既存のコネクタに追加する

別々の AWS アカウントで Cloud Volumes ONTAP を起動する場合は、どちらかを実行します ["IAM ユーザま](#)



たは ARN に AWS キーを指定します 信頼できるアカウントのロール”。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。



そのあとで "Cloud Manager にアカウントのクレデンシャルを追加します" IAM ロールの Amazon リソース名 (ARN)、または IAM ユーザの AWS キーを指定します。

クレデンシャルを追加したら、新しい作業環境を作成するときにクレデンシャルに切り替えることができます。

The screenshot shows the "Edit Credentials & Add Subscription" interface. Under the "Associate Subscription to Credentials" section, there is a list of credentials. The first entry is "keys | Account ID:". Below this, there is a section for "Instance Profile | Account ID:" and a dropdown menu showing "casaba QA subscription". At the bottom, there are "Apply" and "Cancel" buttons.

ページで [ アカウントの切り替え ] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

#### AWS クレデンシャルを Cloud Manager に直接追加

Cloud Manager に新しい AWS クレデンシャルを追加すると、ONTAP 作業環境の FSX の作成と管理、またはコネクタの作成に必要な権限が Cloud Manager に付与されます。

市場への導入とオンプレミスの導入についてはどうでしょうか。

上記の各セクションでは、Cloud Manager のコネクタで推奨される導入方法について説明します。から AWS に Connector を導入することもできます "AWS Marketplace" また、次のことも可能です "コネクタをオンプレミスにインストールします"。



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。

オンプレミス環境では、Cloud Manager システム用の IAM ロールを設定することはできませんが、追加の AWS アカウントの場合と同様に権限を付与することはできます。

**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。

前述したように、Cloud Manager 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。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することで、コネクタインスタンスに関連付けられた IAM ロールを指定できます。

最初の 2 つのオプションでは、Cloud Manager は AWS Security Token Service を使用して、継続的にローテーションする一時的なクレデンシャルを取得します。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。

Cloud Manager に AWS アクセスキーを指定する場合は、Cloud Manager でキーを一定の間隔で更新して、キーをローテーションする必要があります。これは完全に手動で行います。

## Cloud Manager の AWS クレデンシャルとサブスクリプションを管理します

AWS クレデンシャルを追加および管理して、Cloud Manager 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付与されるようにします。複数の AWS 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のクレデンシャルページから別々の AWS クレデンシャルに割り当てることができます。

### 概要

AWS クレデンシャルは、既存のコネクタに追加するか、Cloud Manager 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

既存のコネクタに新しい AWS クレデンシャルを追加すると、同じコネクタを使用して別の AWS アカウントに Cloud Volumes ONTAP を導入できるようになります。 [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](#)。

- Cloud ManagerにAWSクレデンシャルを追加してコネクタを作成します

Cloud Managerに新しいAWSクレデンシャルを追加すると、Connectorの作成に必要な権限がCloud Managerに付与されます。 [Cloud Manager に AWS クレデンシャルを追加する方法について説明します](#)。

- Cloud Manager for FSX for ONTAP にAWSクレデンシャルを追加します

Cloud Managerに新しいAWSクレデンシャルを追加すると、ONTAP 用のFSXの作成と管理に必要な権限がCloud Managerに付与されます。 ["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

Cloud Manager 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。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することで、コネクタインスタンスに関連付けられた IAM ロールを指定します。 ["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、Cloud Manager は AWS Security Token Service を使用して、継続的にローテーションする一時的なクレデンシャルを取得します。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。

Cloud Manager に AWS アクセスキーを指定する場合は、Cloud Manager でキーを一定の間隔で更新して、キーをローテーションする必要があります。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

他の AWS アカウントで Cloud Volumes ONTAP を導入して管理できるように、AWS クレデンシャルをコネクタに追加します。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。

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。この権限を付与することで、Cloud Manager からその AWS アカウント内のリソースやプロセスを管理できるようになります。権限の指定方法は、Cloud Manager に信頼されたアカウントまたは AWS キーのロールの ARN を提供するかどうかによって異なります。



Cloud Manager からコネクタを導入すると、Cloud Manager はコネクタを導入したアカウントの AWS クレデンシャルを自動的に追加しました。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、この初期アカウントは追加されません。"[AWS のクレデンシャルと権限について説明します](#)"。

- 選択肢 \*
- [\[Grant permissions by assuming an IAM role in another account\]](#)
- [\[Grant permissions by providing AWS keys\]](#)

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。その後、Cloud Manager に信頼されたアカウントの IAM ロールの ARN を提供します。

手順

1. Cloud Volumes ONTAP を導入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. [ 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、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。
- から入手できる Cloud Manager IAM ポリシーを使用してポリシーを作成します "[Cloud Manager Policies ページ](#)"。

3. 後日 Cloud Manager に貼り付けることができるように、IAM ロールの ARN をコピーします。

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

Cloud Manager に IAM ユーザの AWS キーを提供する場合は、必要な権限をそのユーザに付与する必要があります。Cloud Manager IAM ポリシーは、Cloud Manager が使用できる AWS アクションとリソースを定義します。

### 手順

1. から Cloud Manager IAM ポリシーをダウンロードします "[Cloud Manager Policies ページ](#)"。
2. 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。

"AWS のドキュメント：「[Creating IAM Policies](#)」

3. 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](#)」

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。

作成したクレデンシャルをクラウドプロバイダで使えるようになるまでに数分かかることがあります。Cloud Manager にクレデンシャルを追加するまで数分待ってから、

### 手順

1. Cloud Manager 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. 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、\* クレデンシャル \* を選択します。

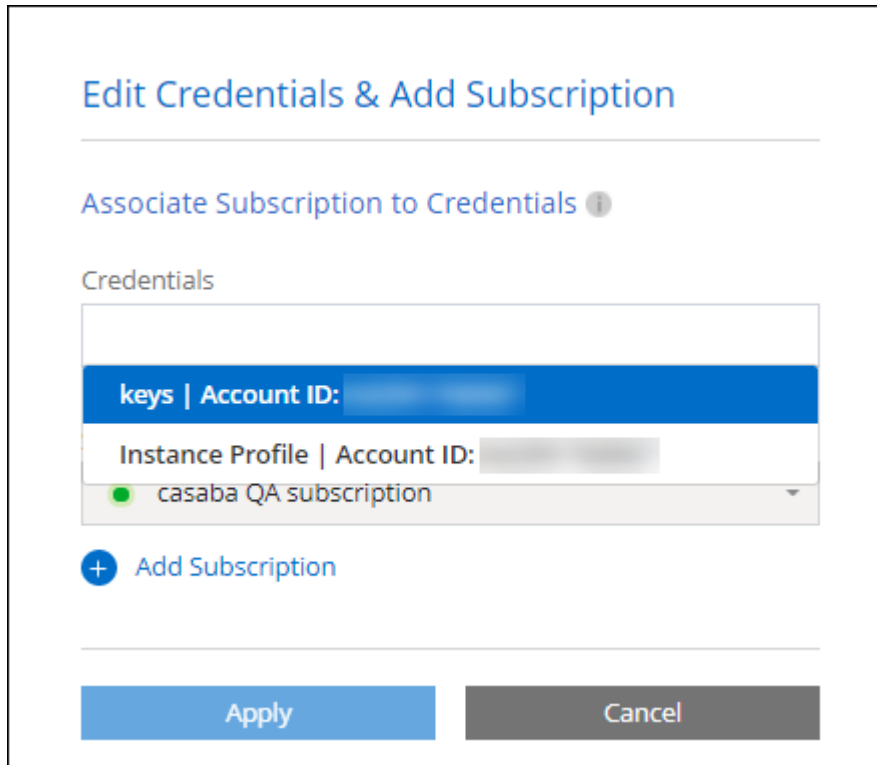


3. [Add Credentials] をクリックし、ウィザードの手順に従います。
  - a. \* 資格情報の場所 \* : 「\* Amazon Web Services > Connector \*」を選択します。
  - b. \* クレデンシャルの定義 \* : 信頼された IAM ロールの ARN (Amazon リソース名) を指定するか、AWS アクセスキーとシークレットキーを入力します。
  - c. \* Marketplace サブスクリプション \*: 今すぐ登録するか、既存のサブスクリプションを選択して、Marketplace サブスクリプションをこれらの資格情報に関連付けます。

Cloud Volumes ONTAP の料金を 1 時間単位で支払う (PAYGO) 場合や 1 年単位で支払う場合は、AWS のクレデンシャルを AWS Marketplace から Cloud Volumes ONTAP への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 \* をクリックします。

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 [ アカウントの切り替え ] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

### Cloud Managerにクレデンシャルを追加してコネクタを作成します

Cloud ManagerにAWSクレデンシャルを追加するには、Cloud Managerにコネクタの作成に必要な権限を付与するIAMロールのARNを指定します。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

Cloud Manager SaaS で役割を引き受けることを可能にする 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. [ 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 の ID として 952013314444 を入力してください
- 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。

から Connector 展開ポリシーを表示します "[Cloud Manager Policies ページ](#)"

3. IAM ロールのロール ARN をコピーして、次の手順で Cloud Manager に貼り付けることができます。

IAM ロールに必要な権限が割り当てられます。これで、Cloud Manager 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、Cloud Manager に ARN ロールを追加します。

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。Cloud Manager にクレデンシャルを追加するまで数分待ってから、

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、\* クレデンシャル \* を選択します。



2. [Add Credentials] をクリックし、ウィザードの手順に従います。
  - a. \* クレデンシャルの場所 \* : 「\* Amazon Web Services > Cloud Manager \*」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 \* をクリックします。

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。

### AWS サブスクリプションを関連付ける

Cloud Manager に AWS のクレデンシャルを追加したら、AWS Marketplace の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。サブスクリプションを使用すると、Cloud Volumes ONTAP の料金を時間単位で支払う (PAYGO) と年単位の契約を使用する、および他の NetApp クラウドサービスを使用することができます。

Cloud Manager にクレデンシャルを追加したあとに、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。

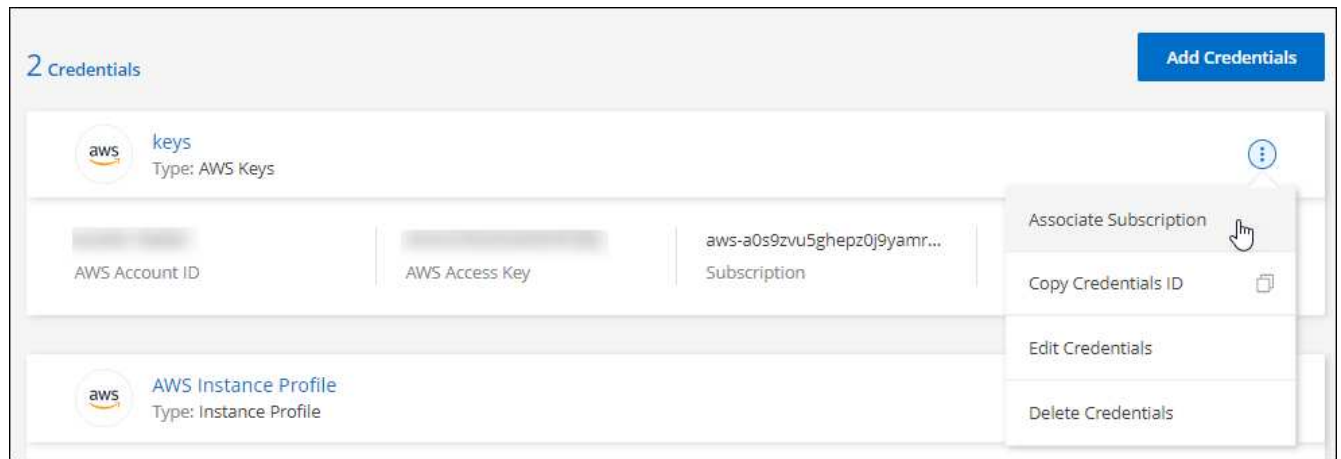
- Cloud Manager にクレデンシャルを最初に追加したときに、サブスクリプションを関連付けていません。
- 既存の AWS Marketplace サブスクリプションを新しいサブスクリプションに置き換える場合。

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。"[コネクタの作成方法を説明します](#)"。

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、\* 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クリックし、\* 契約の関連付け \* を選択します。





3. ダウンリストから既存のサブスクリプションを選択するか、\* サブスクリプションの追加 \* をクリックして、新しいサブスクリプションを作成する手順を実行します。

▶ [https://docs.netapp.com/ja-jp/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/ja-jp/cloud-manager-setup-admin//media/video_subscribing_aws.mp4) (video)

## クレデンシャルを編集する

Cloud Manager 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 キーまたは想定ロール）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. 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、\* 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クリックし、\* 資格情報の編集 \* を選択します。
3. 必要な変更を行い、\* 適用 \* をクリックします。

## クレデンシャルを削除し

クレデンシャルが不要になった場合は、Cloud Manager 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. 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、\* 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クリックし、\* 資格情報の削除 \* を選択します。
3. 削除を確定するには、\* 削除 \* をクリックします。

# Azure のクレデンシアル

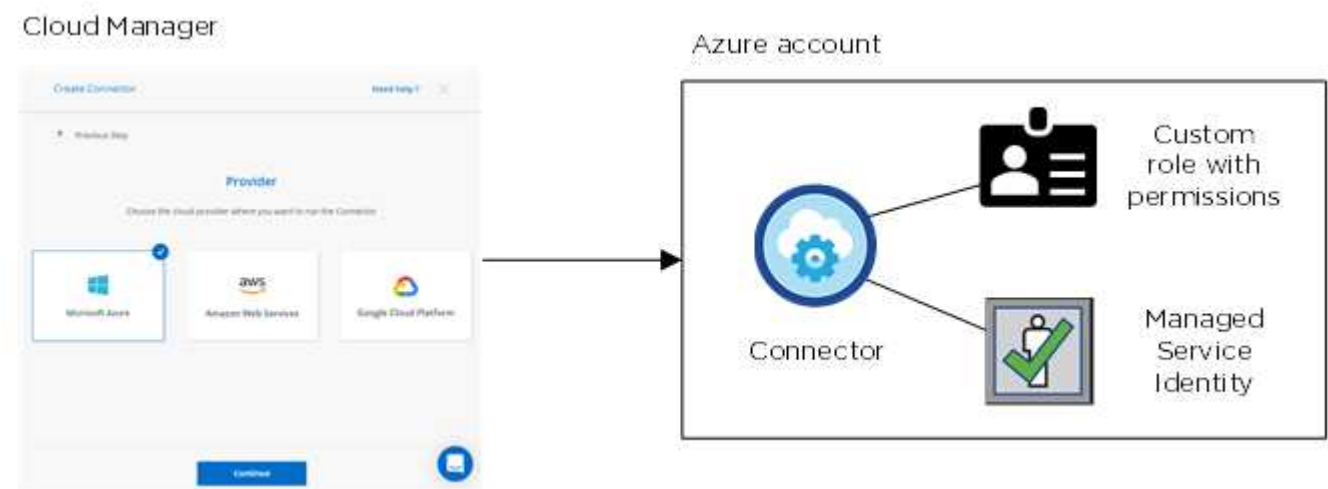
## Azure のクレデンシアルと権限

Cloud Manager では、Cloud Volumes ONTAP の導入時に使用する Azure クレデンシアルを選択できます。すべての Cloud Volumes ONTAP システムは、初期の Azure クレデンシアルを使用して導入することも、クレデンシアルを追加することもできます。

### Azure の初期クレデンシアル

Cloud Manager 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"](#)。

Cloud Manager 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。Cloud Manager に、その Azure サブスクリプション内のリソースとプロセスを管理する権限が付与されます。 ["Cloud Manager での権限の使用法を確認します。"](#)



Cloud Volumes ONTAP 用の新しい作業環境を作成すると、Cloud Manager でデフォルトで次の Azure クレデンシアルが選択されます。

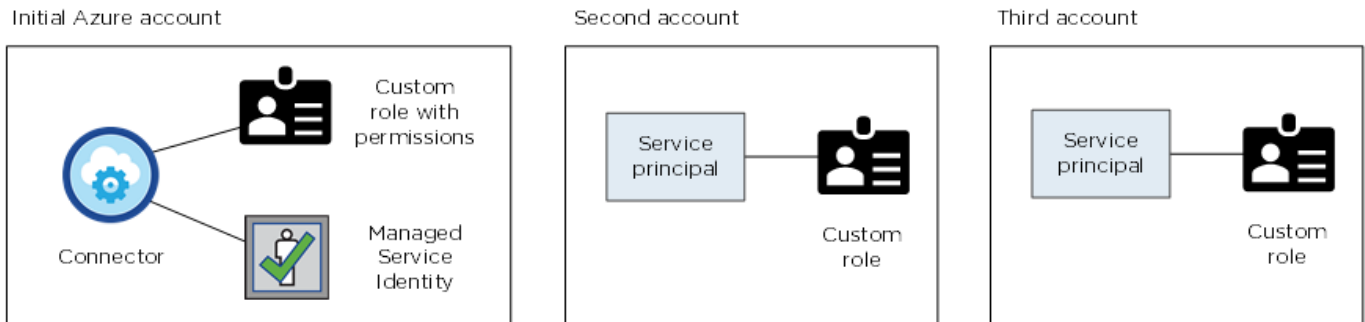
Details & Credentials			
Managed Service Ide...	OCCM QA1	No subscription is associated	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	

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

管理対象 ID は、Connector を起動したサブスクリプションに関連付けられます。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"](#)。

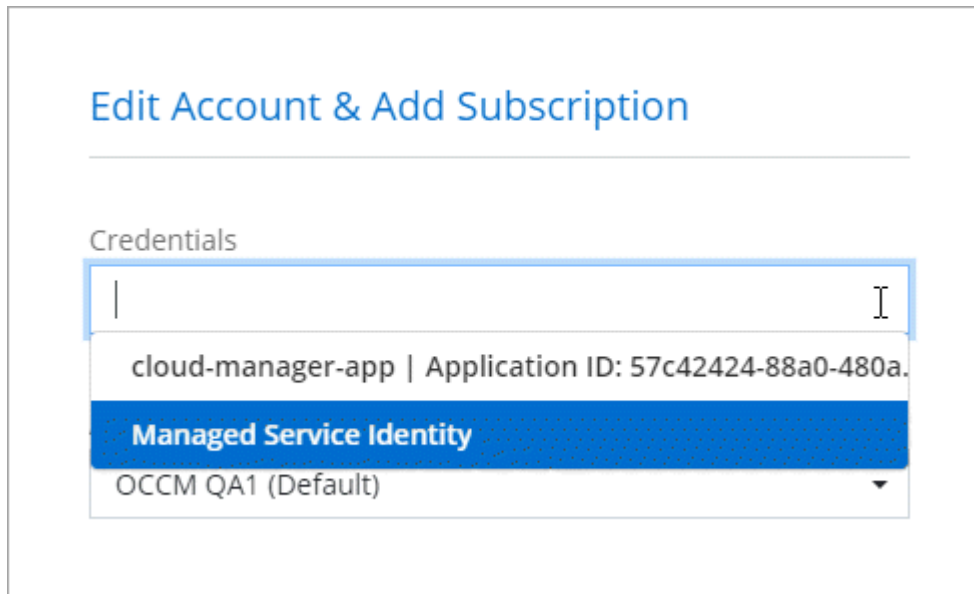
## Azure の追加クレデンシャル

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、必要な権限をに付与する必要があります ["Azure Active でサービスプリンシパルを作成およびセットアップする ディレクトリ"](#) 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 ["Cloud Manager にアカウントのクレデンシャルを追加します"](#) AD サービスプリンシパルの詳細を指定します。

クレデンシャルを追加したら、新しい作業環境を作成するときにクレデンシャルに切り替えることができます。



ページで [ アカウントの切り替え ] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]



## 市場への導入とオンプレミスの導入についてはどうでしょうか。

上記のセクションでは、NetApp Cloud Central のコネクタで推奨される導入方法について説明します。から Azure に Connector を導入することもできます ["Azure Marketplace で入手できます"](#)を使用できます ["コネクタをオンプレミスにインストールします"](#)。

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。コネクタの管理 ID を手動で作成してセットアップし、追加のアカウントに権限を付与するだけで済みます。

オンプレミス環境では、Connector の管理対象 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追加のアカウントの場合と同様に権限を設定できます。

## Cloud Manager の Azure クレデンシャルとサブスクリプションの管理

Cloud Volumes ONTAP システムを作成するときに、そのシステムで使用する Azure クレデンシャルを選択する必要があります。従量課金制のライセンスを使用している場合は、Marketplace サブスクリプションも選択する必要があります。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。

Cloud Manager で Azure サブスクリプションとクレデンシャルを追加するには、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 Cloud Manager 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 に関連付ける

Cloud Manager では、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。に関連付けられない、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。

管理対象 ID はです ["最初の Azure アカウント"](#) Cloud Manager からコネクタを導入する場合。コネクタを導入すると、Cloud Manager Operator ロールが作成され、Connector 仮想マシンに割り当てられます。

### 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. 「\* アクセスコントロール (IAM) \*」をクリックします。
  - a. [\* 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。
    - Cloud Manager Operator \* ロールを選択します。



Cloud Manager Operator は、で指定されたデフォルトの名前です ["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。

- 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 ) ] をクリックします。

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。

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。

### Cloud Manager に Azure クレデンシャルを追加しておきます

Cloud Manager からコネクタを導入すると、必要な権限が割り当てられた仮想マシンで、Cloud Manager によってシステムによって割り当てられた管理対象 ID を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、Cloud Manager でデフォルトで次の Azure クレデンシャルが選択されます。



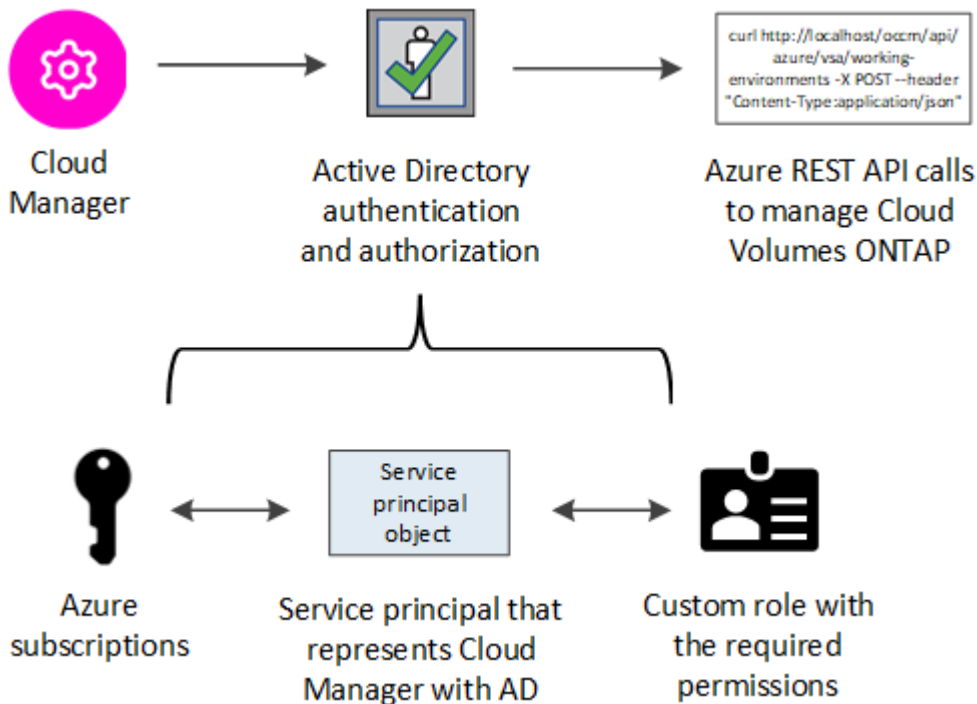
既存のシステムに Connector ソフトウェアを手動でインストールした場合、初期クレデンシャルは追加されません。 ["Azure のクレデンシャルと権限について説明します"](#)。

異なる Azure クレデンシャルを使用して Cloud Volumes ONTAP を導入する場合は、Azure Active Directory 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、Cloud Manager に新しいクレデンシャルを追加できます。

### サービスプリンシパルを使用した Azure 権限の付与

Cloud Manager には、Azure でアクション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、Azure Active Directory でサービスプリンシパルを作成して設定し、Cloud Manager で必要な Azure クレデンシャルを取得します。

次の図は、Cloud Manager が Azure で操作を実行するための権限を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、Azure Active Directory の Cloud Manager 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. [Azure Active Directory アプリケーション](#)を作成します。
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。

#### Azure Active Directory アプリケーションの作成

Cloud Manager でロールベースアクセス制御に使用できる 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

Azure で Cloud Manager に権限を付与するには、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「 OnCommand Cloud Manager Operator 」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 "Cloud Manager 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. 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。

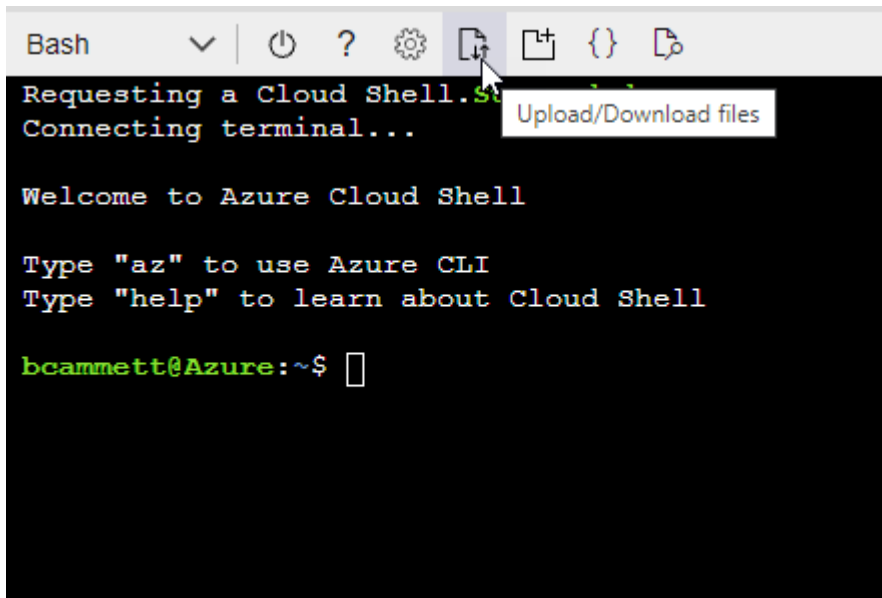
◦ 例 \*

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

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。

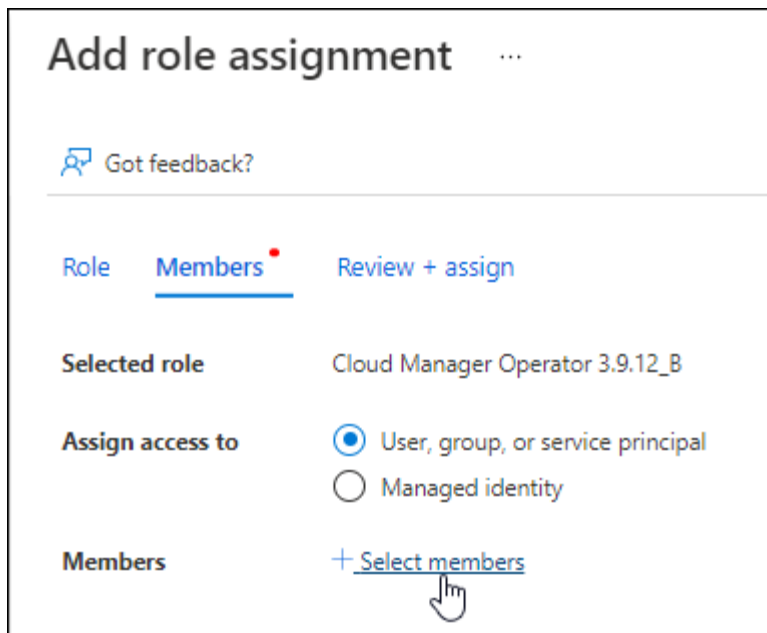


- c. Azure CLI で次のコマンドを入力します。

```
az role definition create --role-definition  
Policy_for_cloud_Manager_Azure_3.9.8.json
```

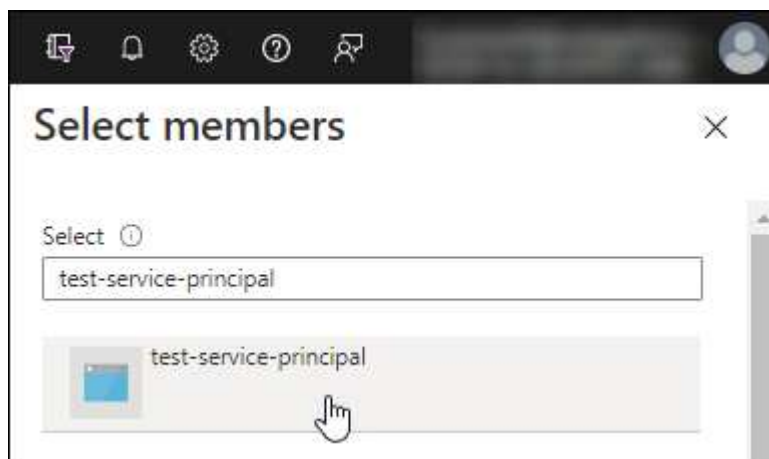
これで、\_Cloud Manager Operator\_ という名前のカスタムロールが作成されます。

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] タブで、\* Cloud Manager Operator \* 役割を選択し、\* Next \* 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。



- 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、\* Select \* をクリックします。
  - 「\* 次へ \*」をクリックします。
- f. [ 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。

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。Cloud Manager では、Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

## Windows Azure Service Management API 権限を追加しています

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

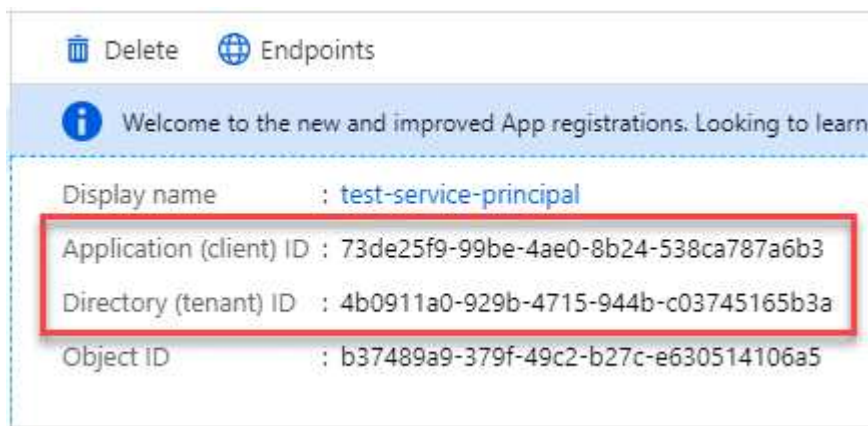
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

アプリケーション ID とディレクトリ ID を取得しています

Cloud Manager に Azure アカウントを追加するときは、アプリケーション（クライアント）の 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の作成

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、Cloud Manager で Azure アカウントを追加するときに入力する必要があります。

**Cloud Manager** にクレデンシャルを追加してください

必要な権限を Azure 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 Cloud Manager 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。

作成したクレデンシャルをクラウドプロバイダで使えるようになるまでに数分かかることがあります。Cloud Manager にクレデンシャルを追加するまで数分待つてから、

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](#)"。

### 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、\* クレデンシャル \* を選択します。



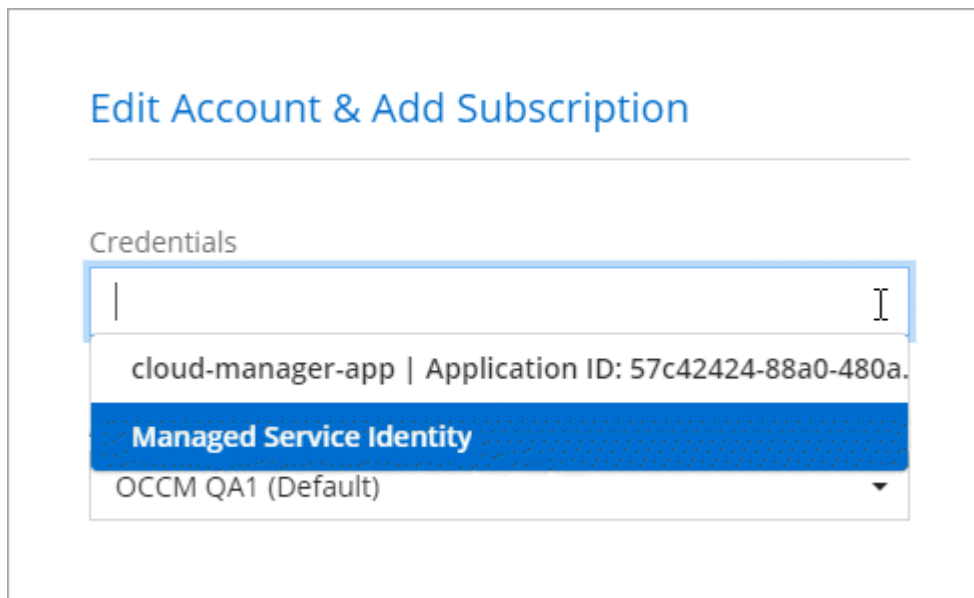
2. [Add Credentials] をクリックし、ウィザードの手順に従います。
  - a. \* 資格情報の場所 \* : Microsoft Azure > Connector \* を選択します。
  - b. \* クレデンシャルの定義 \* : 必要な権限を付与する Azure Active Directory サービスプリンシパルに関する情報を入力します。
    - アプリケーション（クライアント）ID : を参照してください [\[Getting the application ID and directory ID\]](#)。
    - ディレクトリ（テナント）ID : を参照してください [\[Getting the application ID and directory ID\]](#)。
    - クライアントシークレット : を参照してください [\[Creating a client secret\]](#)。

- 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。

Cloud Volumes ONTAP の料金を時間単位で支払う（PAYGO）には、Azure のクレデンシャルが Azure Marketplace からのサブスクリプションに関連付けられている必要があります。

- d. \* 確認 \*: 新しいクレデンシャルの詳細を確認し、\* 追加 \* をクリックします。

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 ] をクリックした後で資格情報を選択する方法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

Cloud Manager にすでに追加した Azure クレデンシャルの管理では、Marketplace でのサブスクリプションの関連付け、クレデンシャルの編集、および削除を行います。

#### Azure Marketplace サブスクリプションをクレデンシャルに関連付ける

Cloud Manager に Azure のクレデンシャルを追加したら、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。サブスクリプションを使用すると、従量課金制の Cloud Volumes ONTAP システムを作成し、他のネットアップクラウドサービスを使用できます。

Cloud Manager にクレデンシャルを追加したあとに、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。

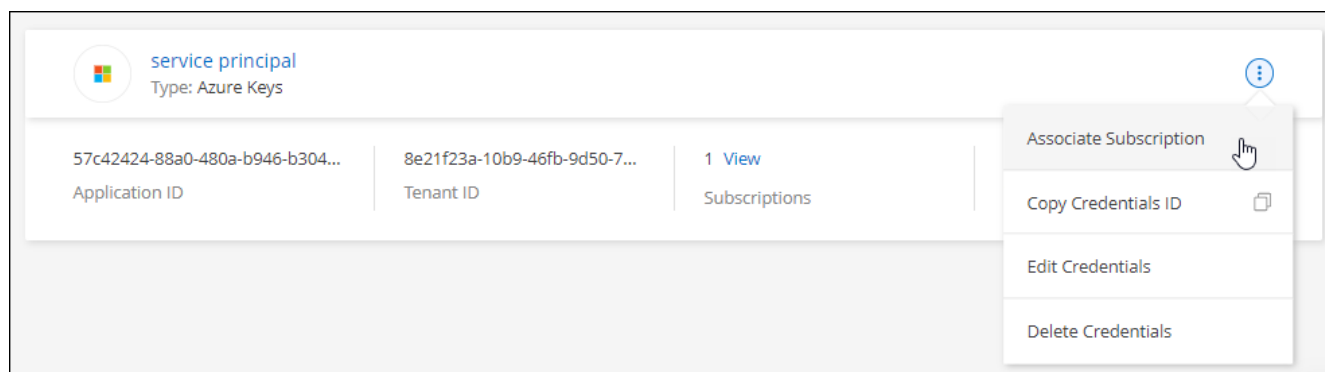
- Cloud Manager にクレデンシャルを最初に追加したときに、サブスクリプションを関連付けていません。
- 既存の Azure Marketplace サブスクリプションを新しいサブスクリプションに置き換える場合。

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"](#)。

### 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、\* クレデンシャル \* を選択します。

- 一連の資格情報のアクションメニューをクリックし、\* 契約の関連付け \* を選択します。



- ダウリストからサブスクリプションを選択するか、\* サブスクリプションの追加 \* をクリックして、手順に従って新しいサブスクリプションを作成します。

次のビデオは、作業環境ウィザードのコンテキストから開始しますが、[サブスクリプションの追加]をクリックした後も同じワークフローが表示されます。

▶ [https://docs.netapp.com/ja-jp/cloud-manager-setup-admin//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/ja-jp/cloud-manager-setup-admin//media/video_subscribing_azure.mp4) (video)

#### クレデンシャルの編集

Azure サービスクレデンシャルの詳細を変更して、Cloud Manager 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

- 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、\* クレデンシャル \* を選択します。
- 一連の資格情報のアクションメニューをクリックし、\* 資格情報の編集 \* を選択します。
- 必要な変更を行い、\* 適用 \* をクリックします。

#### クレデンシャルを削除し

クレデンシャルが不要になった場合は、Cloud Manager 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

- 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、\* クレデンシャル \* を選択します。
- 一連の資格情報のアクションメニューをクリックし、\* 資格情報の削除 \* を選択します。
- 削除を確定するには、\* 削除 \* をクリックします。

## Google Cloud のクレデンシャル

### Google Cloud のプロジェクト、権限、アカウント

サービスアカウントを使用すると、Cloud Manager に対し、Connector と同じプロジェクトまたは異なるプロジェクトにある Cloud Volumes ONTAP システムを導入および管

理する権限が付与されます。

## Cloud Manager のプロジェクトと権限

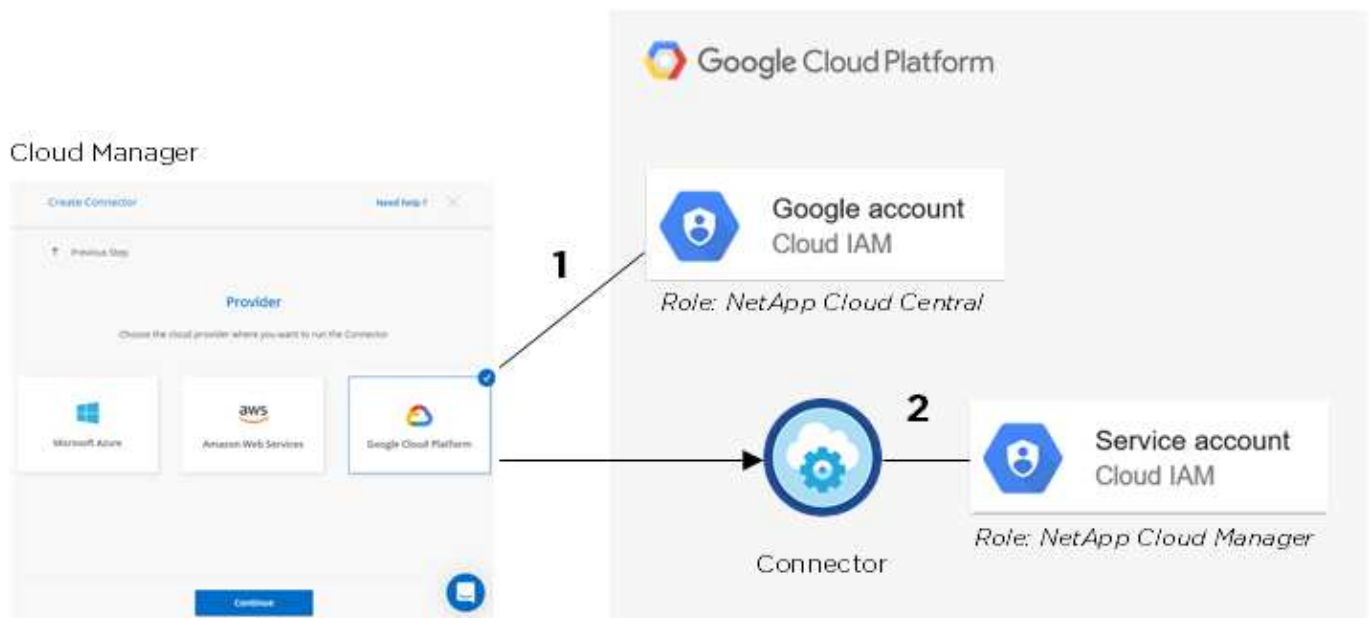
Google Cloud に Cloud Volumes ONTAP を導入する前に、まず Google Cloud プロジェクトに Connector を導入する必要があります。Connector は、オンプレミスでも別のクラウドプロバイダでも実行できません。

Cloud Manager からコネクタを直接導入するには、次の 2 組の権限が必要です。

1. Cloud Manager から Connector VM インスタンスを起動する権限がある 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。Cloud Manager は、サービスアカウントから権限を取得して、Cloud Volumes ONTAP システムを代わりに作成および管理します。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。

ユーザとサービスアカウントに必要な権限を含む YAML ファイルを 2 つ設定しました。 ["YAML ファイルを使用して設定する方法を学習します 権限"](#)。

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。



## 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"](#)
- ["GCP とで Cloud Volumes ONTAP を導入する方法について説明します プロジェクトを選択します"](#)

## Cloud Manager の GCP クレデンシャルとサブスクリプションの管理

Connector VM インスタンスに関連付けられているクレデンシャルを管理できます。

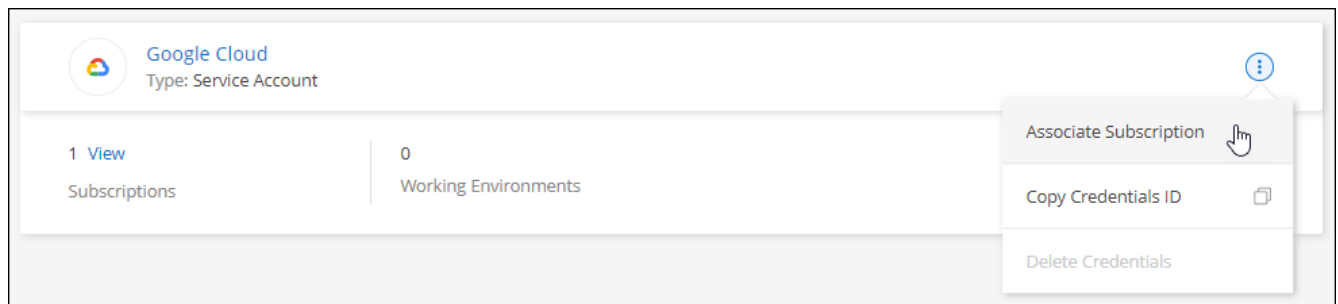
### Marketplace サブスクリプションと GCP クレデンシャルの関連付け

GCP に Connector を導入すると、Cloud Manager は 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を作成します。Cloud Manager で Cloud Volumes ONTAP の導入に使用するクレデンシャルを指定します。

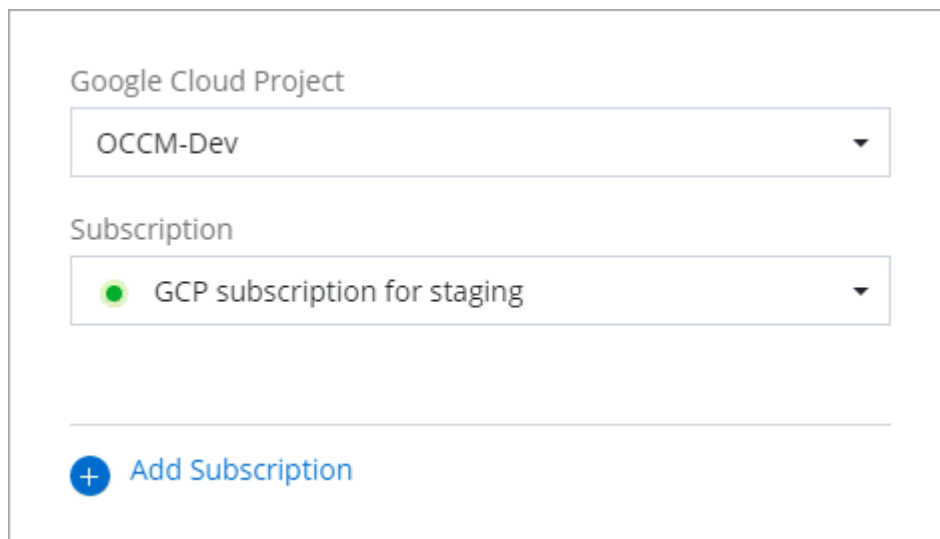
これらの資格情報に関連付けられている Marketplace サブスクリプションは、いつでも変更できます。サブスクリプションを使用すると、従量課金制の Cloud Volumes ONTAP システムを作成し、他のネットアップクラウドサービスを使用できます。

#### 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、\* 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クリックし、\* 契約の関連付け \* を選択します。



3. 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ます。



4. [ 関連付け (Associate) ] をクリックします。
5. 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 ] をクリックし、以下の手順に従って新しいサブスクリプションを作成します。



次の手順を実行する前に、Google Cloud アカウントと NetApp Cloud Central への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。

6. サブスクリプションの手順をもう一度表示し、[\* Continue (続行) ] をクリックします。

## Add Subscription

**Subscription Steps:**

- 1 Cloud Manager**  
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
- 2 Google Cloud Marketplace**  
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
- 3 Cloud Central**  
Save your subscription.
- 4 Cloud Manager**  
Associate the Marketplace subscription with your Google Cloud project.

View video instructions

ContinueCancel

7. にリダイレクトされたら "[Google Cloud Marketplace の NetApp Cloud Manager のページ](#)"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。

 Google Cloud Platform 





## Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

[SUBSCRIBE](#)

[OVERVIEW](#) [PRICING](#) [SUPPORT](#)

### Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

### Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. **[Subscribe]** をクリックします
9. 適切な請求先アカウントを選択し、条件に同意します。



## 2. Purchase details

Select a billing account \*

Secondary\_Billing\_Account

## 3. Terms

### Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

### Additional terms

- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. [Subscribe] をクリックします

転送要求がネットアップに送信されます。

11. ポップアップダイアログボックスで、NetApp Cloud Central にリダイレクトされる \* Register with NetApp、Inc. \* をクリックします。





GCP サブスクリプションをネットアップ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 NetApp Cloud Central 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。

12. Cloud Central にリダイレクトされたら、NetApp Cloud Central にログインするか、サインアップして \* Done \* をクリックして続行します。

GCP サブスクリプションは、ユーザログインが関連付けられているすべてのネットアップアカウントにリンクされます。



組織のユーザが請求用アカウントから NetApp Cloud Manager 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 ["NetApp Cloud Central 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。

13. このプロセスが完了したら、Cloud Manager のクレデンシャルページに戻り、この新しいサブスクリプションを選択します。

Google Cloud Project

OCCM-Dev
▼

Subscription

● GCP subscription for staging
▼

---

+ Add Subscription

## Marketplace 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 Cloud Volumes ONTAP にサブスクライブすると、権限が正しくないために断片化されたり、NetApp Cloud Central へのリダイレクトに誤って追従したりしない場合があります。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 Cloud Manager のページ"](#) 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 \*」をクリックします。

Pricing

✓ The product was purchased on 12/9/20.

MANAGE ORDERS

- a. 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。

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
<span style="color: green;">✓</span>	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- b. 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	⋮

# Cloud Manager でネットアップサポートサイトのアカウントを追加および管理します

ネットアップサポートサイト（NSS）アカウントのクレデンシャルを入力して、Cloud Volumes ONTAP の主要なワークフローを有効にし、Active IQ による予測分析とプロアクティブなサポートを有効にします。

## 概要

次のタスクを実行するには、Cloud Manager にネットアップサポートサイトのアカウントを追加する必要があります。

- お客様所有のライセンスを使用（BYOL）した場合に Cloud Volumes ONTAP を導入するには

Cloud Manager でライセンスキーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを指定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 システムを登録できます

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。

- をクリックして、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ます
- から Active IQ デジタルアドバイザーを使用します

## NSS アカウントを追加します

サポートダッシュボードを使用すると、すべてのネットアップサポートサイトのアカウントを 1 箇所から追加および管理できます。

### 手順

1. ネットアップサポートサイトのアカウントがない場合は、**"1 名で登録します"**。
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. **[NSS Management] > [Add NSS Account]** をクリックします。
4. メッセージが表示されたら、[\* Continue (続行)] をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 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。

Cloud Manager で NSS アカウントを使用することができます。

アカウントに関する次の要件に注意してください。

- お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。
- ノードベースの BYOL システムを導入する場合は、次の点に注意してください。
  - BYOL システムのシリアル番号にアクセスする権限がアカウントに必要です。
  - セキュアな BYOL サブスクリプションを購入した場合は、セキュアな NSS アカウントが必要です。

新しい Cloud Volumes ONTAP システムの作成時、既存の Cloud Volumes ONTAP システムの登録時、および Active IQ でデータを表示するときに、アカウントを選択できるようになりました。

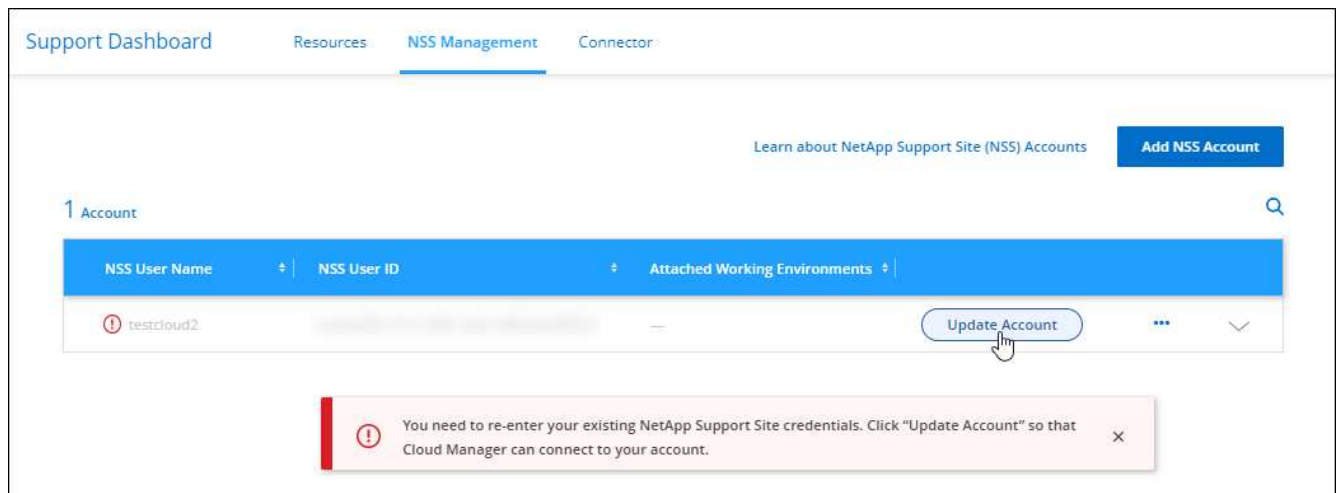
- ["AWS での Cloud Volumes ONTAP の起動"](#)
- ["Azure で Cloud Volumes ONTAP を起動します"](#)
- ["GCP での Cloud Volumes ONTAP の起動"](#)
- ["従量課金制システムの登録"](#)

## NSS アカウントを更新して新しい認証方法を適用します

2021 年 11 月以降、ネットアップはサポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用します。この更新によって、Cloud Manager は、以前に追加した既存のアカウントのクレデンシャルの更新を求めます。

### 手順

1. まだ行っていない場合は、"[現在のネットアップアカウントにリンクする Microsoft Azure Active Directory B2C アカウントを作成します](#)"。
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。
3. [\*NSS 管理 \*] をクリックします。
4. アップデートする NSS アカウントの場合は、\* アカウントの更新 \* をクリックします。



5. メッセージが表示されたら、[\* Continue (続行) ] をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

6. ログインページで、ネットアップサポートサイトの登録 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。

処理が完了したら、更新したアカウントが表に `_new_account` として表示されるようになります。古いバージョンのアカウントは ' 既存の作業環境の関連付けとともにテーブルに表示されます

7. 既存の Cloud Volumes ONTAP 作業環境が古いバージョンのアカウントに接続されている場合は、次の手順に従ってください [それらの作業環境を別の NSS アカウントに接続します](#)。
8. 古いバージョンの NSS アカウントに移動し、をクリックします ... 次に、\* Delete \* を選択します。

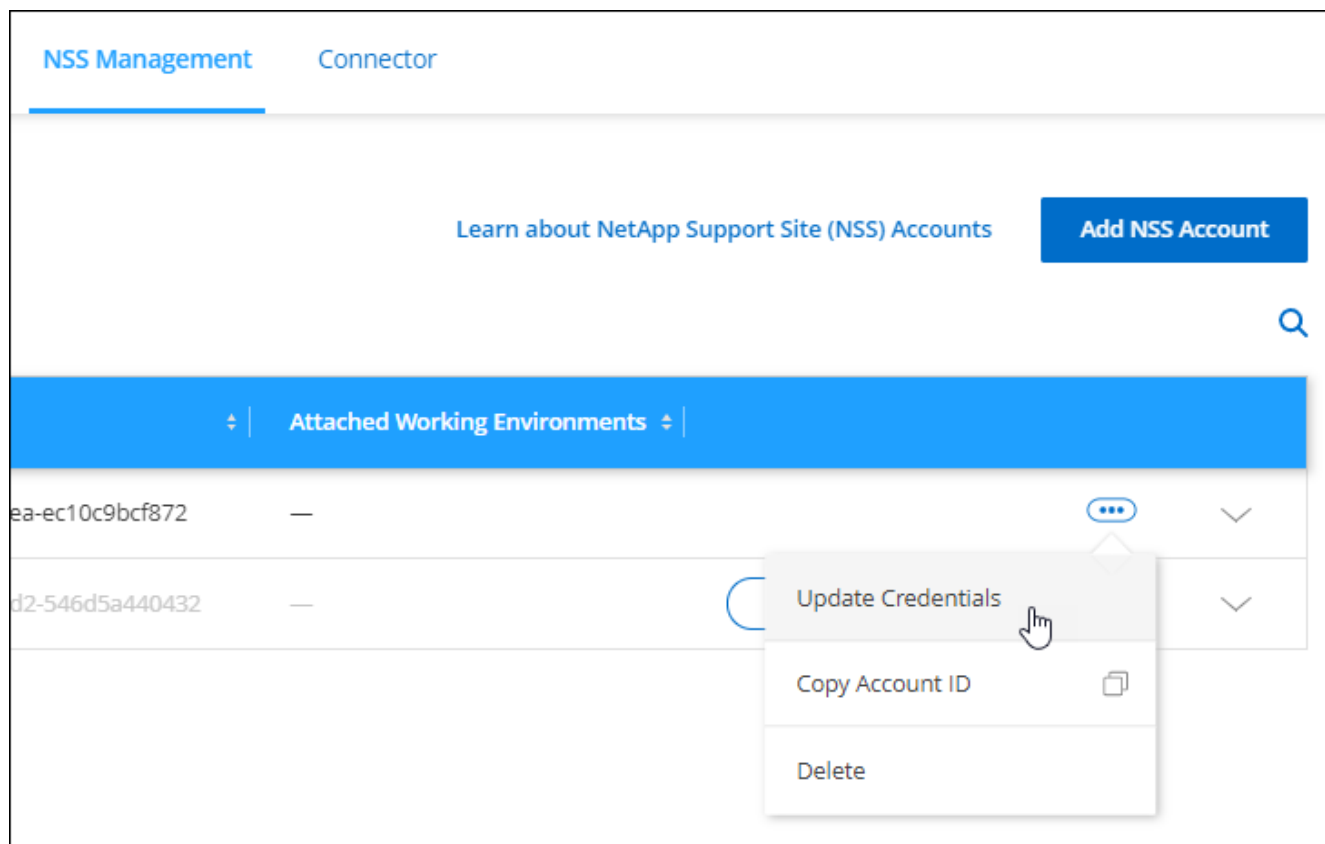
## NSS クレデンシャルを更新します

NSS アカウントのクレデンシャルを変更するたびに、Cloud Manager で更新する必要があります。

### 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、\* Support \* を選択します。

2. [\*NSS 管理 \*] をクリックします。
3. アップデートする NSS アカウントのをクリックします ... 次に、[ 資格情報の更新 ] を選択します。



4. メッセージが表示されたら、[\* Continue (続行) ] をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 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

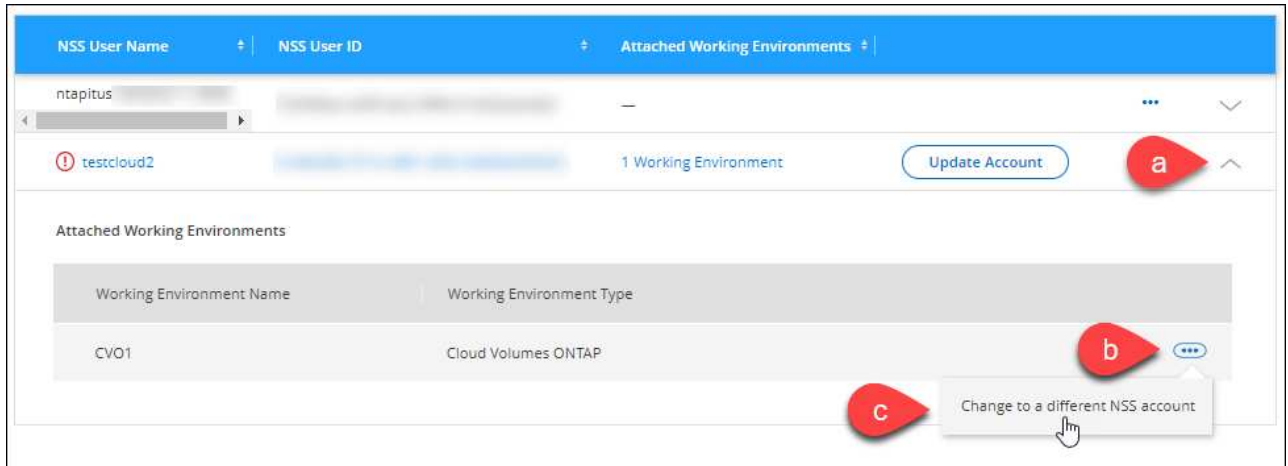
組織に複数のネットアップサポートサイトのアカウントがある場合、Cloud Volumes ONTAP システムに関連付けられているアカウントを変更することができます。

この機能は、ネットアップがアイデンティティ管理に導入した Microsoft Azure AD 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 アカウントを追加 \*」または「\* アカウントを更新 \*」をクリックする必要があります。

### 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、\* Support \* を選択します。
2. [\*NSS 管理 \*] をクリックします。
3. NSS アカウントを変更するには、次の手順を実行します。

- 作業環境が現在関連付けられているネットアップサポートサイトのアカウントの行を展開します。
- 関連付けを変更する作業環境で、をクリックします ...
- 別の NSS アカウントに変更 \* を選択します。



- アカウントを選択し、\* 保存 \* をクリックします。

## NSS アカウントの E メールアドレスを表示します

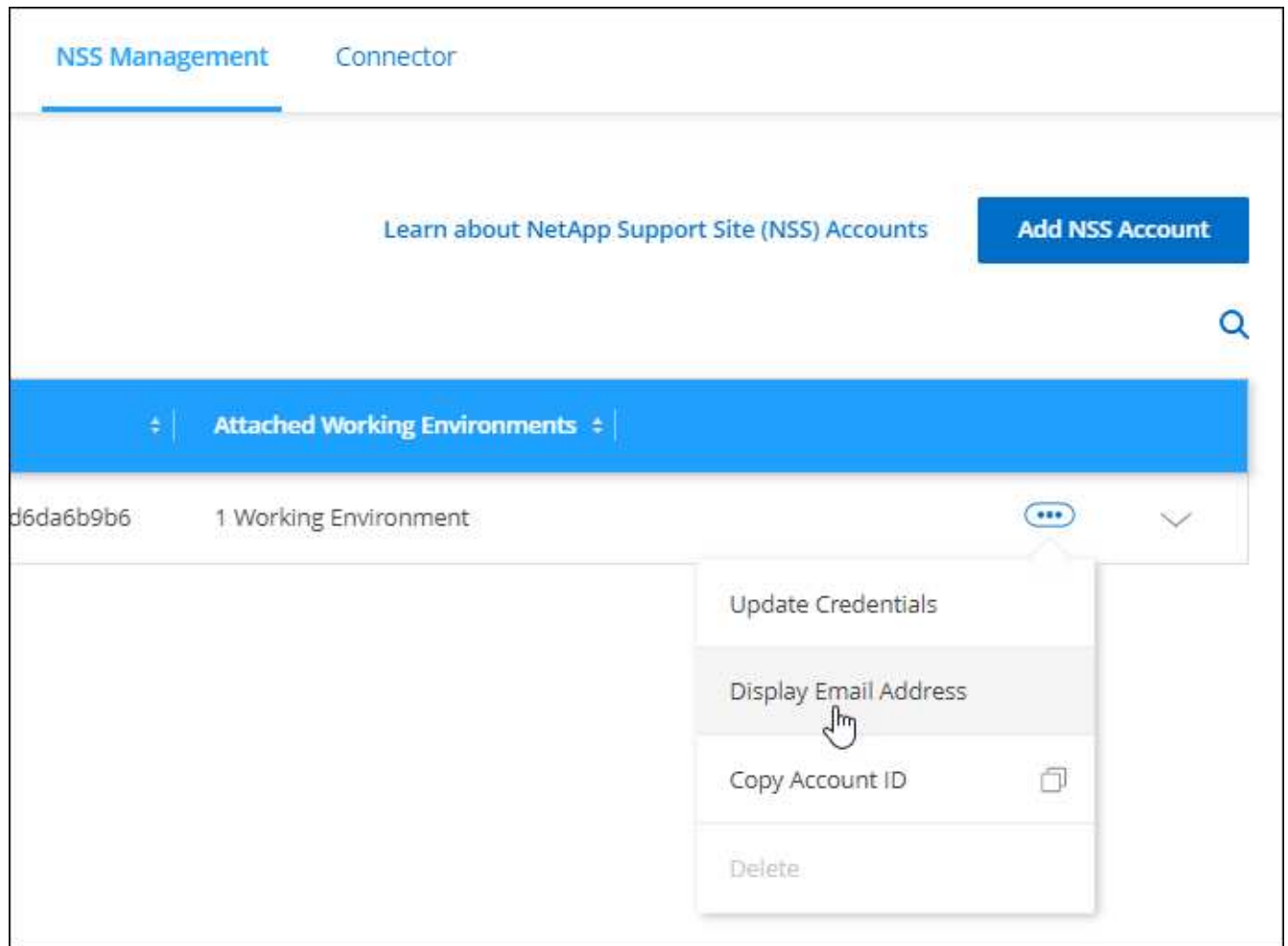
ネットアップサポートサイトのアカウントで認証サービスに Microsoft Azure Active Directory が使用されているため、Cloud Manager に表示される NSS ユーザ名は通常、Azure AD で生成された識別子です。そのため、そのアカウントに関連付けられている E メールアドレスがすぐにわからない場合があります。Cloud Manager には、関連付けられている E メールアドレスを表示するオプションがあります。



NSS の管理ページに移動すると、Cloud Manager のテーブル内のアカウントごとにトークンが生成されます。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

- 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。
- [\*NSS 管理\*] をクリックします。
- アップデートする NSS アカウントのをクリックします ... 次に、[電子メールアドレスの表示\*] を選択します。



Cloud Manager に、ネットアップサポートサイトのユーザ名と関連付けられている E 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

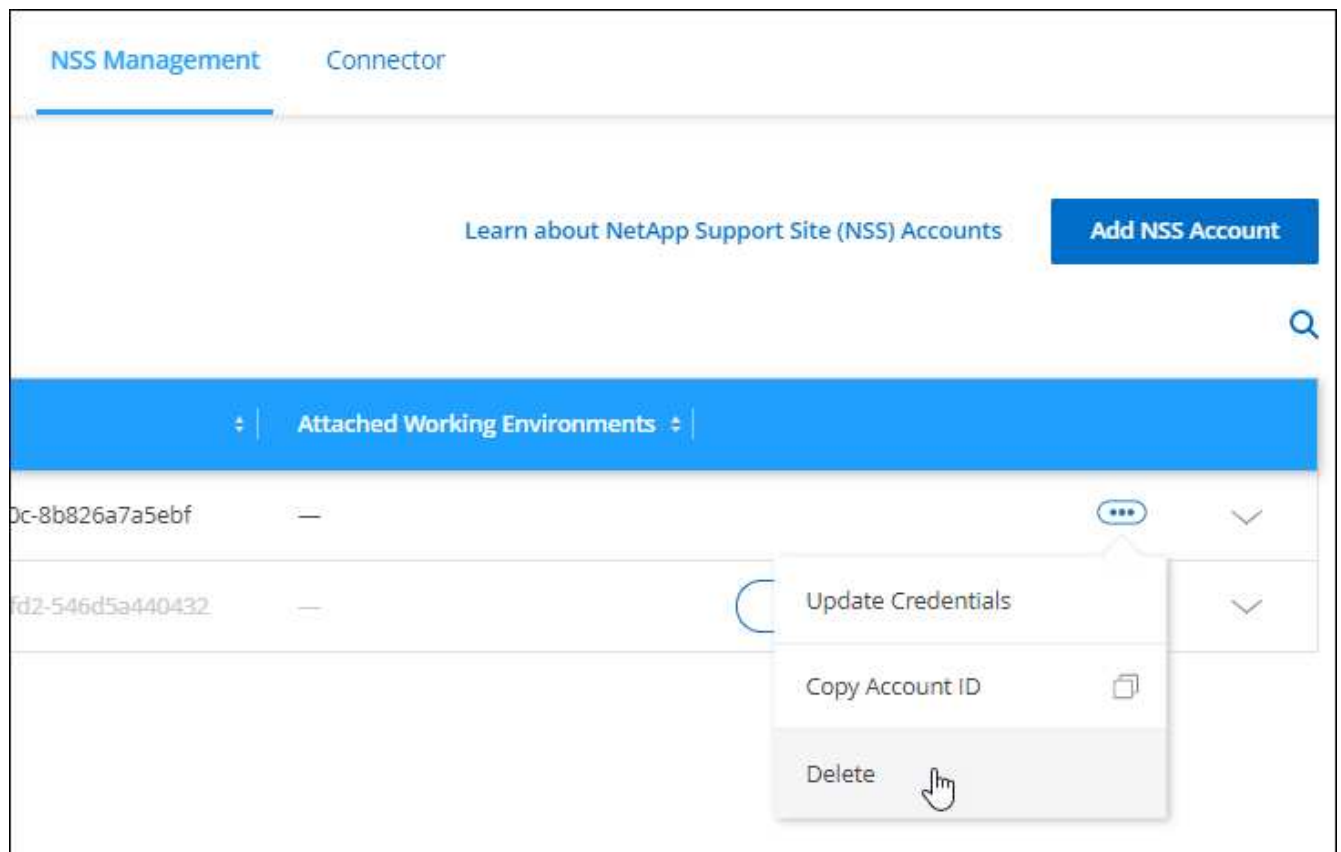
Cloud Manager で使用しない NSS アカウントを削除します。

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。最初に必要なです [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. 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。
2. [\*NSS 管理\*] をクリックします。
3. 削除する NSS アカウントのをクリックします ... 次に、\* Delete \* を選択します。





4. 削除を確定するには、\* 削除 \* をクリックします。

## 著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

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、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、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

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、またはその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り特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

## 商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> 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。