# AWS クレデンシャル

Set up and administration

NetApp
April 13, 2022

# 目次

# AWS クレデンシャル

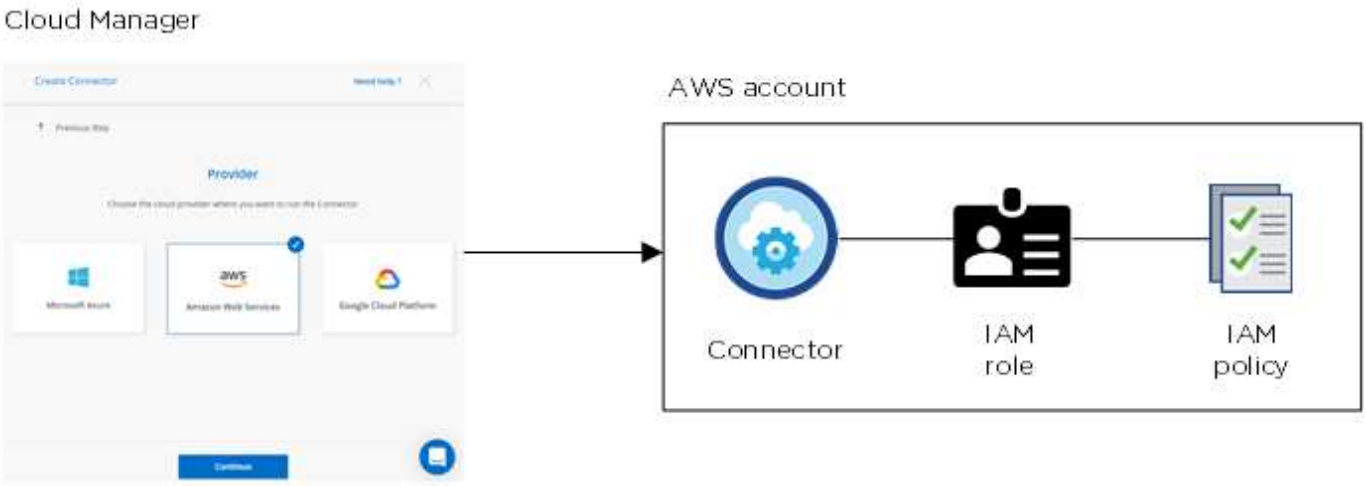
## AWS のクレデンシャルと権限

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

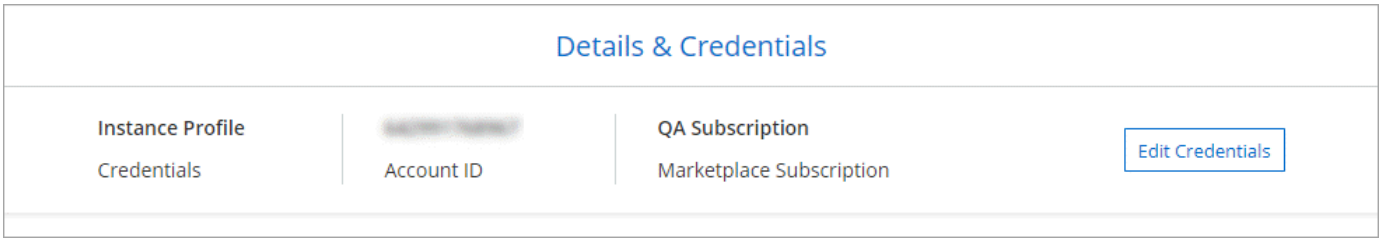
### AWS の初期クレデンシャル

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 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 クレデンシャルにはデフォルトで次のものがあります。

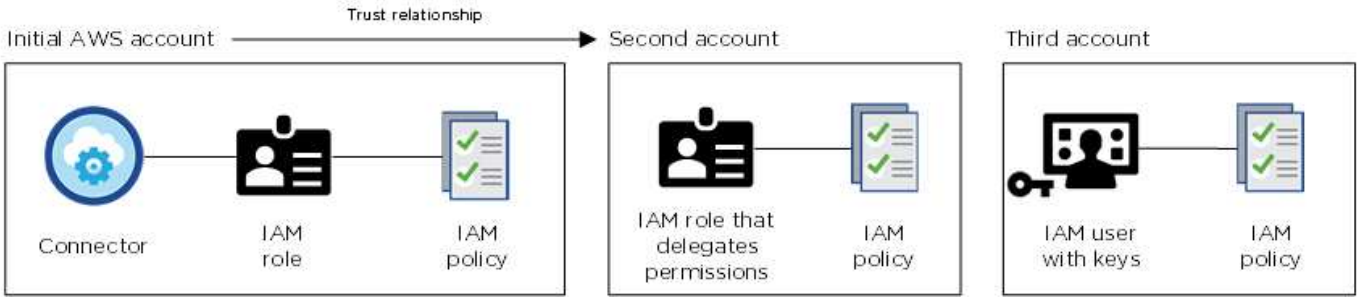



### 追加の AWS クレデンシャル

AWS クレデンシャルを追加する方法は 2 種類あります。

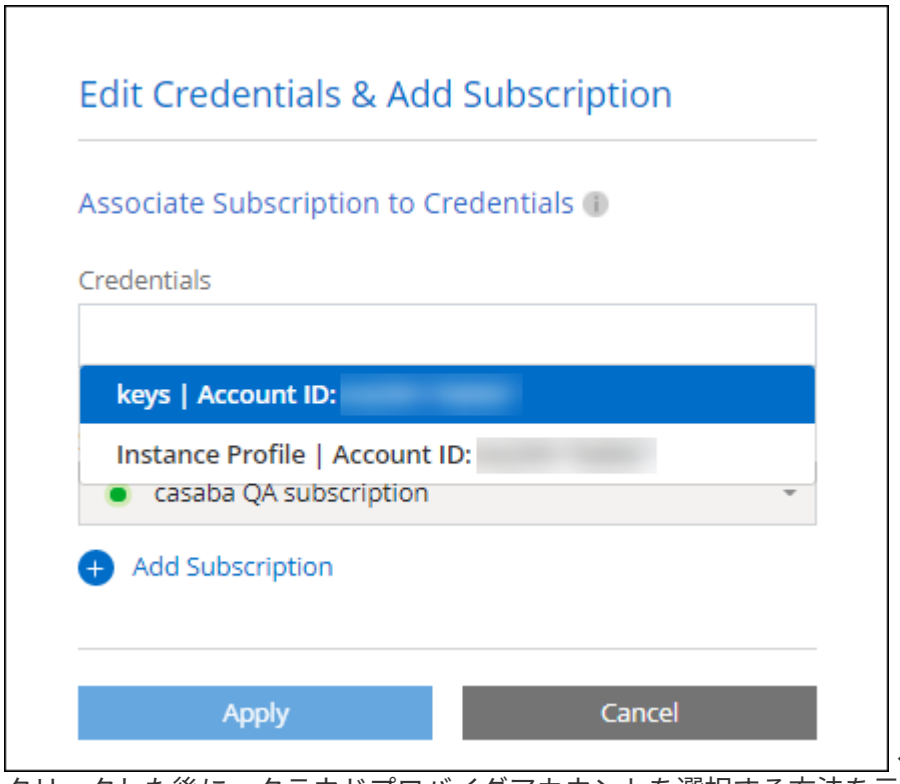
### AWS クレデンシャルを既存のコネクタに追加する

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。




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。

- AWS クレデンシャルを既存のコネクタに追加する

  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。

- 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。 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。

## 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ます

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用でき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。

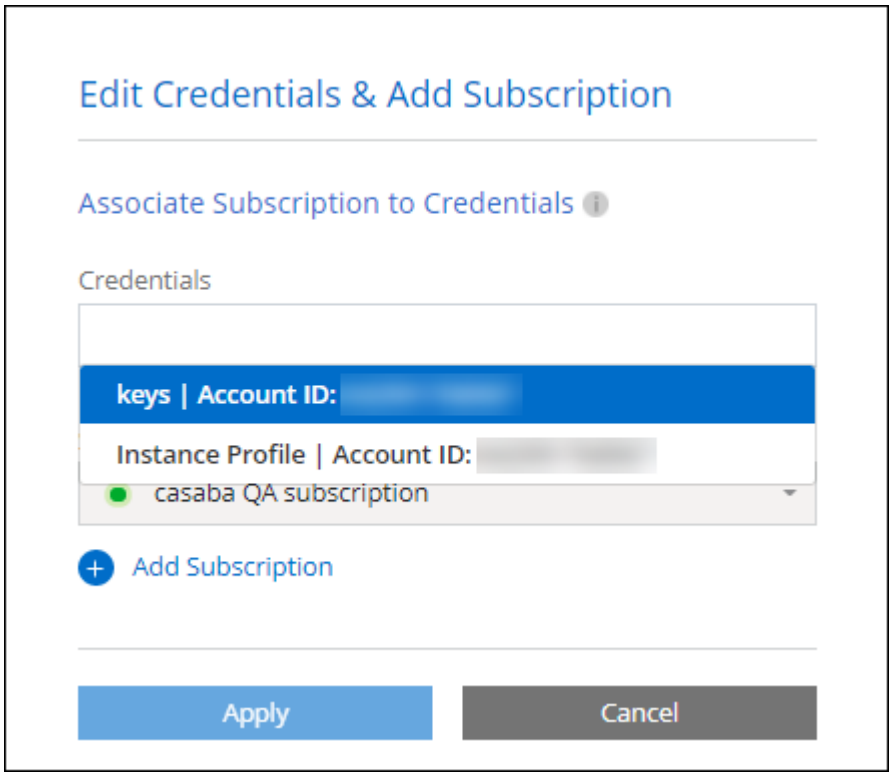

3. [Add Credentials] をクリックし、ウィザードの手順に従います。
   a. * 資格情報の場所 * ：「 * Amazon Web Services > Connector * 」を選択します。
   b. * クレデンシャルの定義 * ：信頼された IAM ロールの ARN （ Amazon リソース名）を指定するか、 AWS アクセスキーとシークレットキーを入力します。

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ます

Cloud Manager に AWS クレデンシャルを追加するには、 IAM ロールの ARN を指定します。このロールにより、 ONTAP 作業環境で FSX を作成したり、コネクタを作成したりするために必要な権限が Cloud Manager に付与されます。

ONTAP 作業環境で FSX を作成する場合、または新しいコネクタを作成する場合に、資格情報を使用できます。

### 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
- ONTAP 作業環境の FSX を作成するため、またはコネクタを作成するために必要な権限を含むポリシーを作成します。
  - "ONTAP の FSX に必要な権限を表示します"
  - 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。

FSX for ONTAP 作業環境を作成するとき、または新しいコネクタを作成するときに、資格情報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。

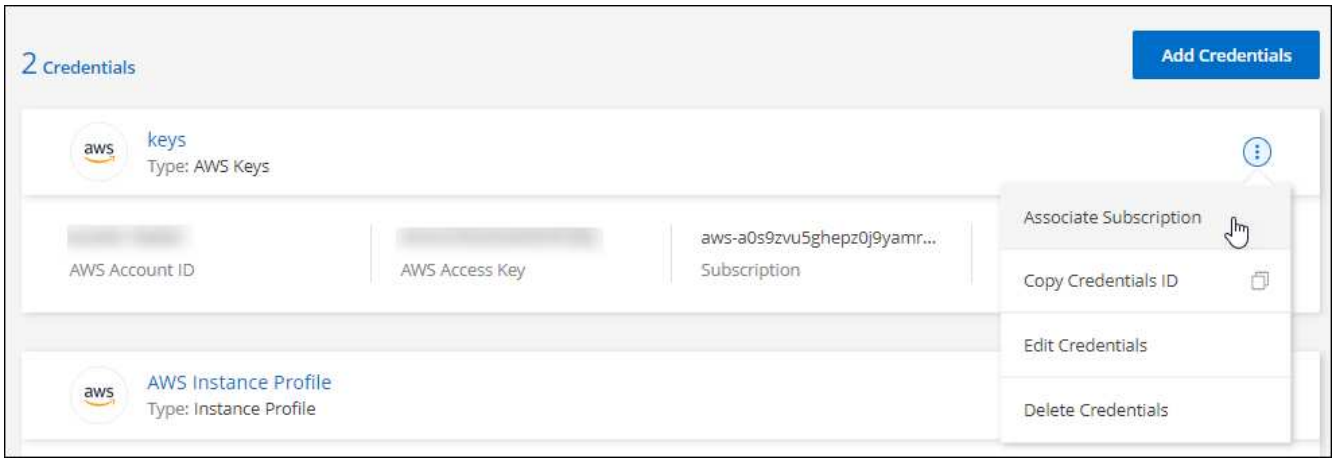
- Cloud Manager にクレデンシャルを最初に追加したときに、サブスクリプションを関連付けていません。

- 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 *(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。