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 Manager

Ben Cammett, Aksel Davis
February 14, 2021

目次

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は、 Azure のクレデンシャルと Marketplace サブスクリプションを選択して、そのシステムで使用する必要があります。複数の Azure Marketplace 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、クレデンシャルページから別々の Azure クレデンシャルに割り当てることができます。

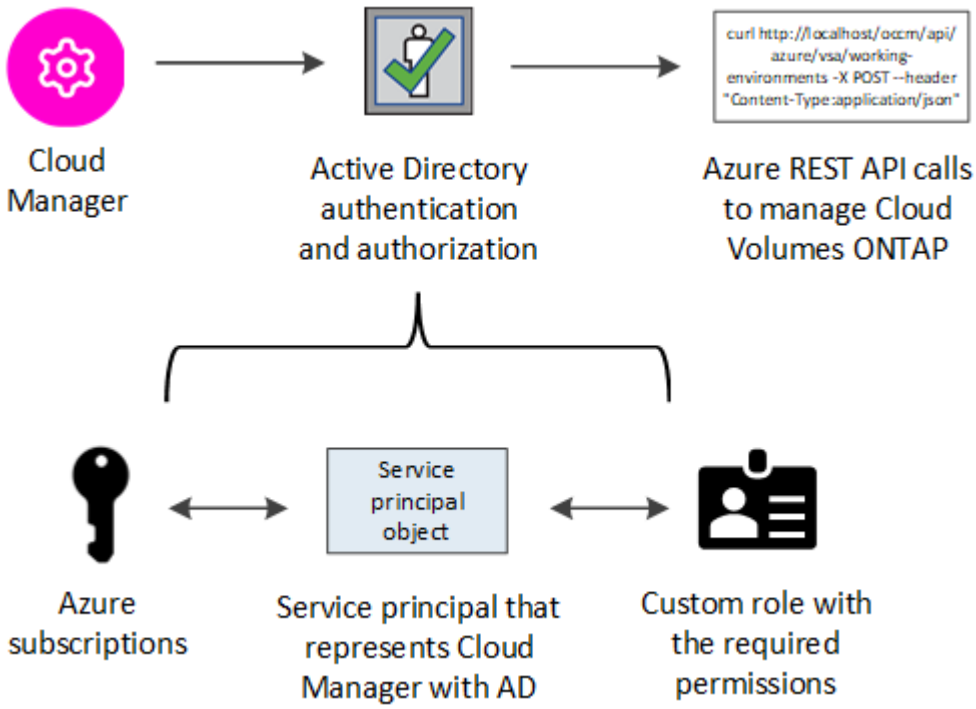
Cloud Manager で Azure クレデンシャルを管理するには、 2 つの方法があります。まず、別の Azure アカウントに Cloud Volumes ONTAP を導入する場合は、必要な権限を指定し、そのクレデンシャルを Cloud Manager に追加する必要があります。もう 1 つは、追加のサブスクリプションを Azure マネージド ID に関連付ける方法です。

Cloud Manager からコネクタを導入すると、コネクタを導入した Azure アカウントが Cloud Manager によって自動的に追加されます。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、初期アカウントは追加されません。 "Azure のアカウントと権限について説明します"。

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。

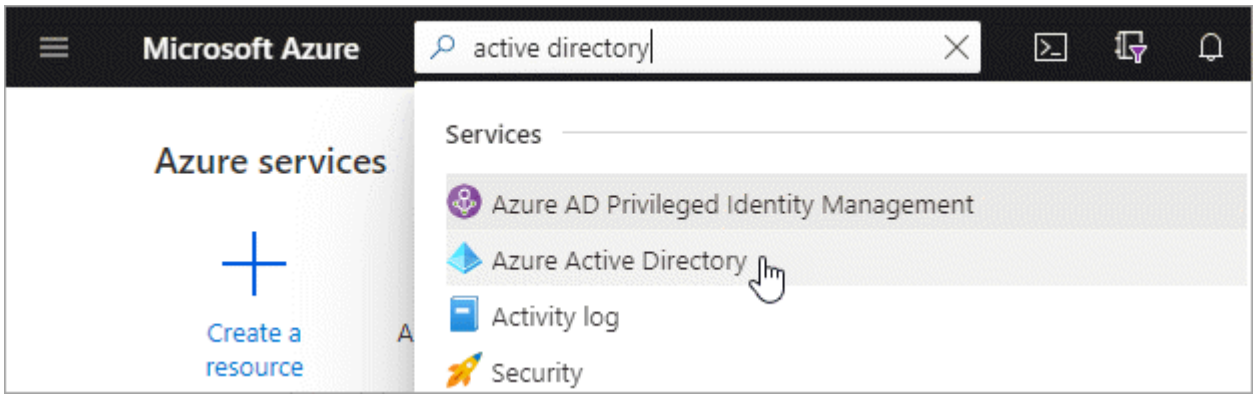
Azure Active Directory アプリケーションの作成

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. 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 *

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

   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_3.8.7.json 」という名前で作成します

   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。

2. 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。

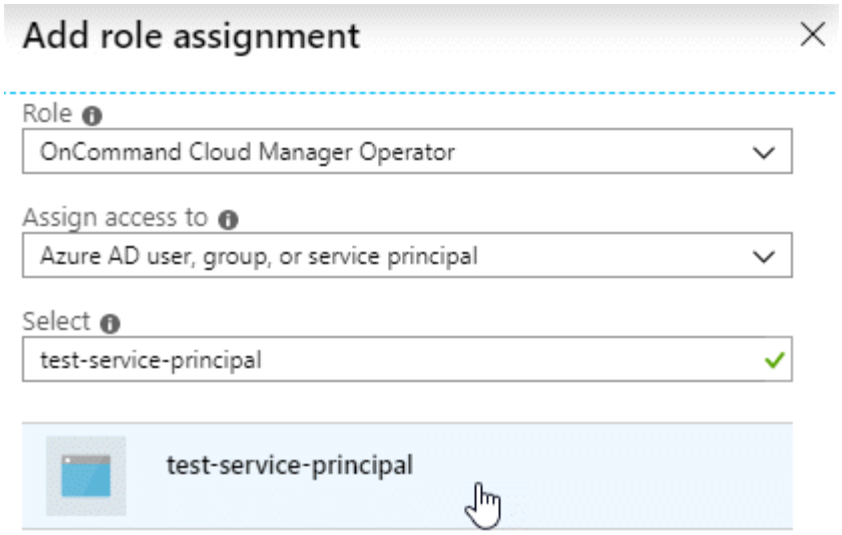
   c. [* アクセス制御 (IAM)] 、 [追加] 、 [役割の割り当ての追加 *] の順にクリックします。

   d. Cloud Manager Operator * ロールを選択します。

   e. Azure AD のユーザ、グループ、サービスプリンシパル * は選択したままにします。

   f. アプリケーションの名前を検索します（リストをスクロールして探すことはできません）。

      次に例を示します。



g. アプリケーションを選択し、 * 保存 * をクリックします。

Cloud Manager のサービスプリンシパルに、そのサブスクリプションに必要な Azure の権限が付与されるようになりました。

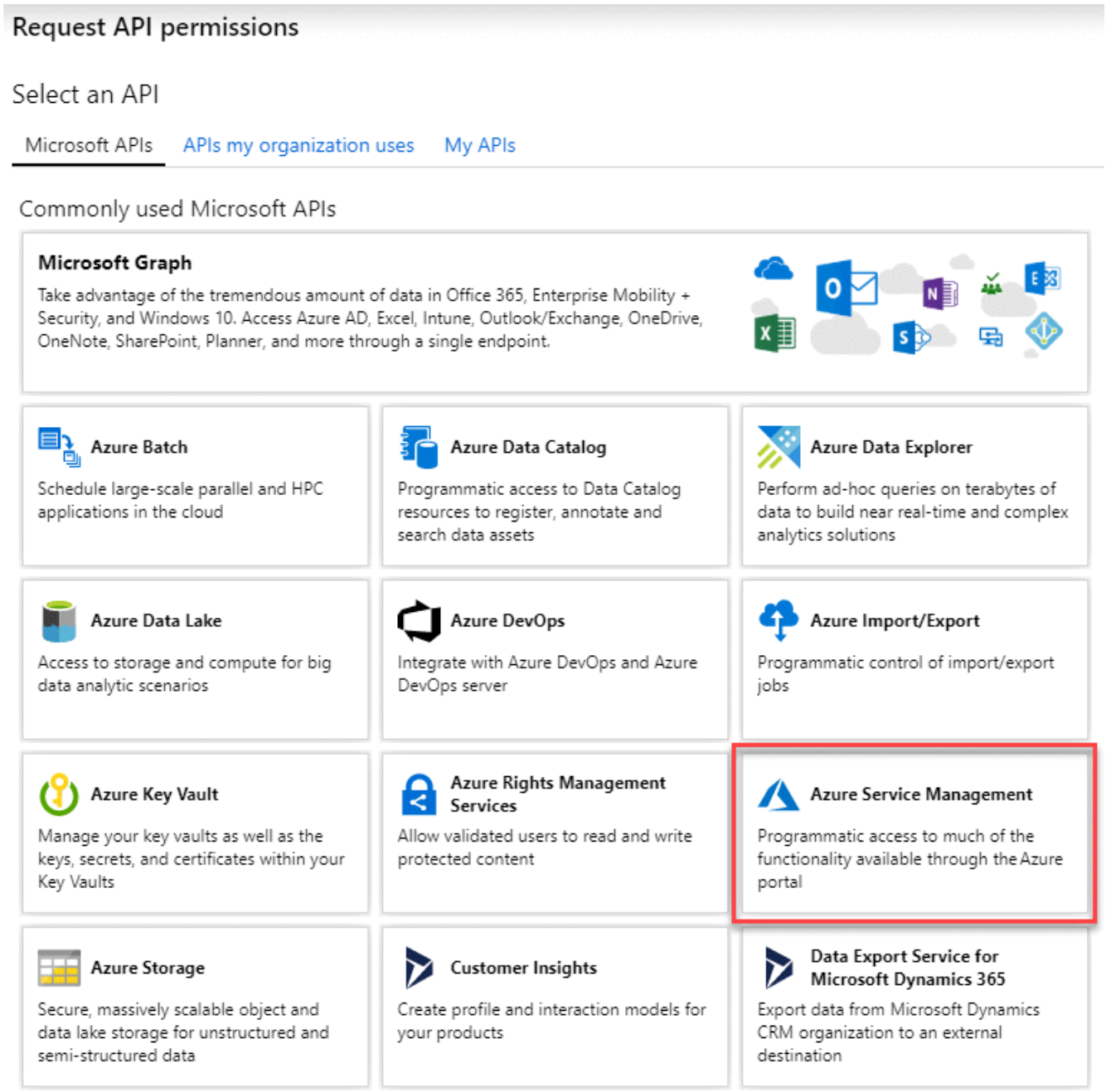
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。Cloud Manager では、 Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

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

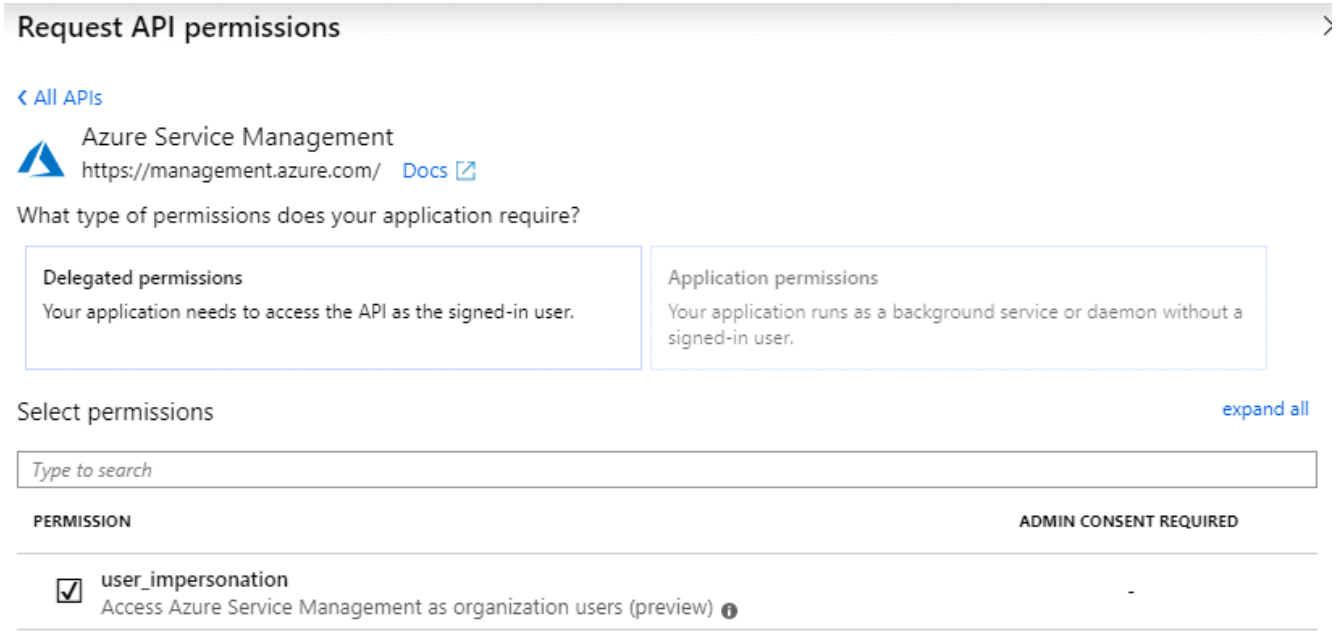
サービスプリンシパルに「 Windows Azure Service Management API 」の権限が必要です。

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。



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。

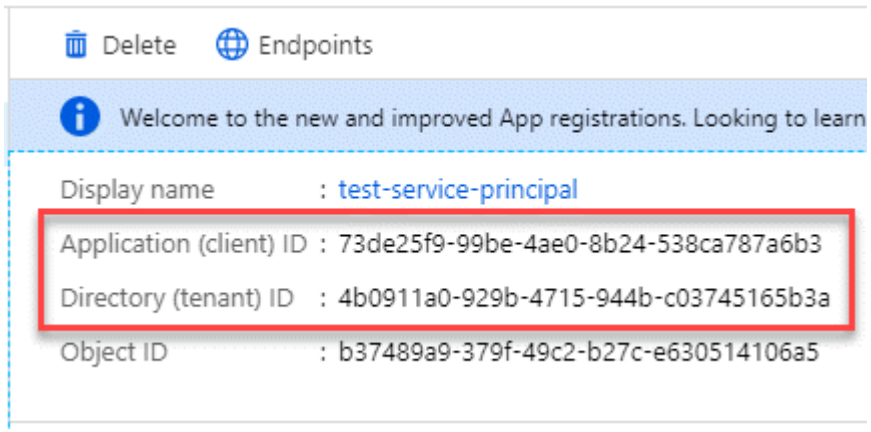


アプリケーション ID とディレクトリ ID を取得しています

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。

Cloud Manager にアカウントを追加すると、 Cloud Manager はクライアントシークレットをアプリケーションキーとして参照します。

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。

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 Azure クレデンシャルを追加しています

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。これにより、そのアカウントで Cloud Volumes ONTAP システムを起動できます。

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。

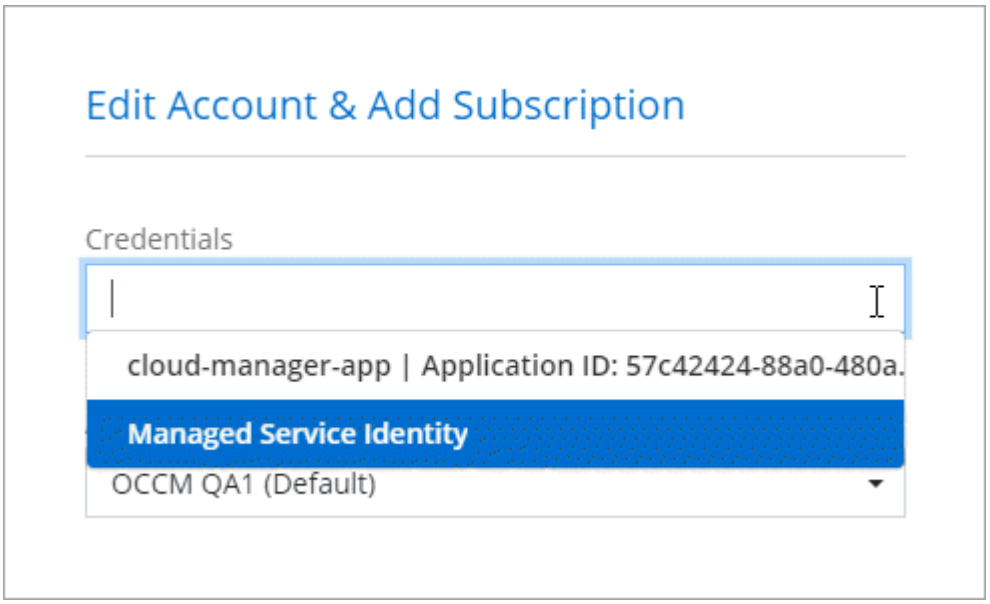
2. 資格情報の追加 * をクリックし、 * Microsoft Azure * を選択します。
3. 必要な権限を付与する Azure Active Directory サービスプリンシパルに関する情報を入力します。
   - アプリケーション（クライアント） ID ：を参照してください [Getting the application ID and directory ID]。
   - ディレクトリ（テナント） ID ：を参照してください [Getting the application ID and directory ID]。
   - クライアントシークレット：を参照してください [Creating a client secret]。
4. ポリシーの要件が満たされていることを確認し、 [* Continue （続行）] をクリックします。
5. クレデンシャルに関連付ける従量課金制サブスクリプションを選択するか、まだサブスクリプションを追

加していない場合は「 * 」をクリックします。

従量課金制の Cloud Volumes ONTAP システムを作成するには、 Azure クレデンシャルが Azure Marketplace からの Cloud Volumes ONTAP へ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。

6. [追加（ Add ）] 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"]

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。

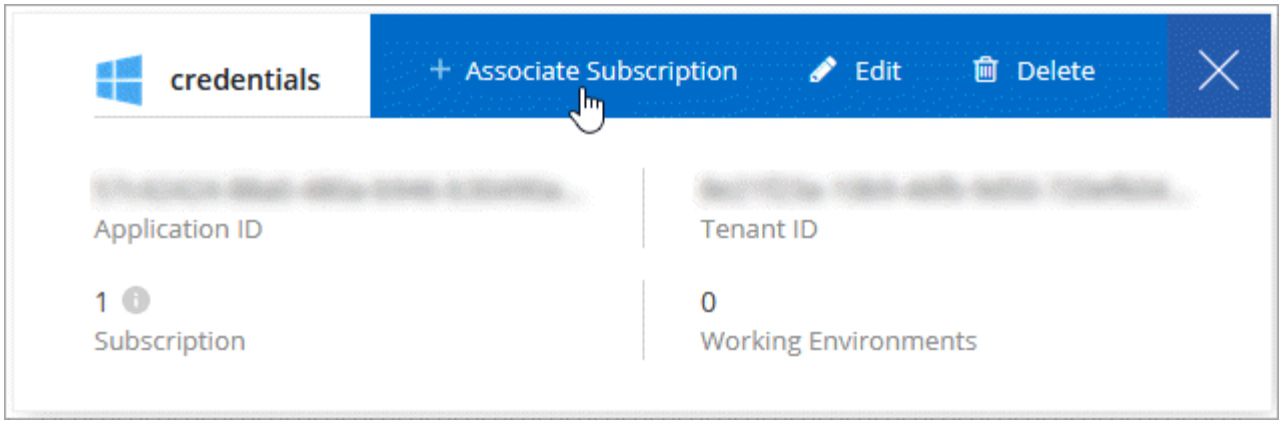
Cloud Manager にクレデンシャルを追加したあとに、 Azure Marketplace サブスクリプションを関連付けるシナリオは 2 つあります。

- 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。
2. 資格情報のセットにカーソルを合わせ、アクションメニューをクリックします。
3. メニューから、 * サブスクリプションを関連付ける * をクリックします。



4. ダウン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/us-en/occm/media/video_subscribing_azure.mp4 *(video)*

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 を関連付けない限り、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。