



# クレデンシャルを管理する

## Cloud Manager

NetApp  
June 07, 2021

# 目次

クレデンシャルを管理する .....	1
AWS .....	1
Azure .....	7
GCP .....	19
Cloud Manager へのネットアップサポートサイトのアカウントの追加 .....	25

# クレデンシャルを管理する

## AWS

### 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ときは、権限を持つ AWS アカウントを使用して Connector インスタンスを起動する必要があります。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、Cloud Manager にその 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付与するポリシーも適用されます。 ["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 クレデンシャルにはデフォルトで次のものがあります。

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

### 追加の AWS クレデンシャル

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 ユーザーまたは 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 ユーザーの 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。

### Edit Account & Add Subscription

Credentials

Keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

QA Subscription

#### Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

+ Add Subscription

Apply Cancel

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 用の AWS 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 AWS のクレデンシャルとサブスクリプションを選択する必要があります。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。

Cloud Manager に AWS クレデンシャルを追加する前に、そのアカウントに必要な権限を付与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 AWS キーを提供するか、信頼されたアカウントのロールの ARN を提供する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 \*
- [\[Granting permissions by providing AWS keys\]](#)
- [\[Granting permissions by assuming IAM roles in other accounts\]](#)

## 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。

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。このプロセスはベストプラクティスであり、自動的に実行され、安全です。

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。

### 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、[Cloud Manager](#) に追加できます。

### 他のアカウントで IAM ロールを想定して権限を付与する

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に移動し、\* 別の AWS アカウント \* を選択して IAM ロールを作成します。

必ず次の手順を実行してください。

- 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 ポリシーを関連付けます "[Cloud Manager Policies ページ](#)"。

## Create role

1

2

3

4

### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
  - ☐ Require MFA 

2. コネクタインスタンスが存在するソースアカウントに移動し、インスタンスに関連付けられている IAM ロールを選択します。

a. [\* ポリシーの適用 \*] をクリックし、[ ポリシーの作成 \*] をクリックします。

b. 「STS : AssumeRole」アクションと、ターゲットアカウントで作成したロールの ARN を含むポリシーを作成します。

▪ 例 \*

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
  }
}
```

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、Cloud Manager に追加できます。

### Cloud Manager に AWS クレデンシャルを追加しています

必要な権限を持つ AWS アカウントを入力したら、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。

#### 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、\* AWS \* を選択します。
3. 信頼できる IAM ロールの AWS キーまたは ARN を指定します。
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. 資格情報に関連付ける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。

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。

6. [追加（Add）] 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。

## Edit Account & Add Subscription

Credentials

Keys | Account ID: [REDACTED]

Instance Profile | Account ID: [REDACTED]

QA Subscription

### Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

+ Add Subscription

Apply

Cancel

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 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 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。

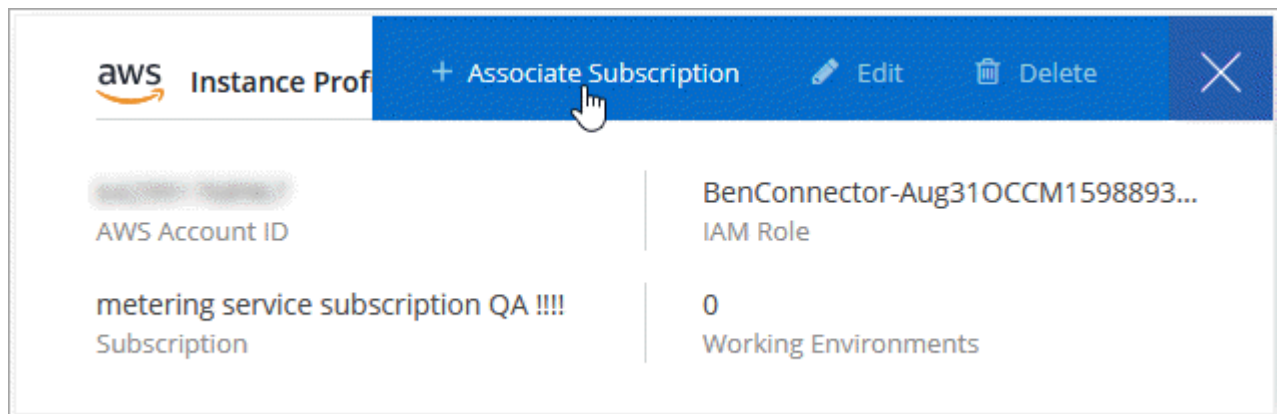
Cloud Manager にクレデンシャルを追加したあとに、AWS Marketplace サブスクリプションに関連付けるシナリオは 2 つあります。

- 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。"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。

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

## Azure

### Azure 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 Azure 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 Azure 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。

## Azure の初期クレデンシャル

Cloud Manager から Connector を導入する場合は、Connector 仮想マシンの導入権限を持つ Azure アカウント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 での権限の使用方法を確認します。"](#)。

### Cloud Manager



### Azure account



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。

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

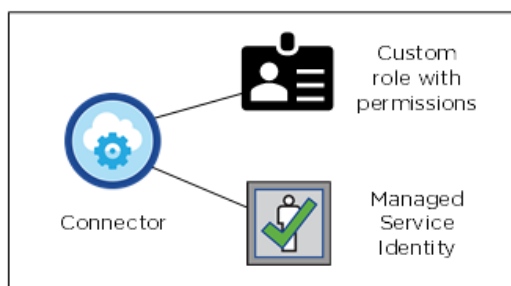
マネージド ID 向けの **Azure** サブスクリプションが追加されました

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"](#)。

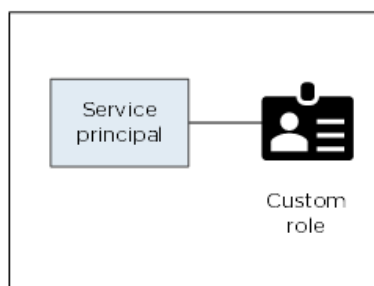
## Azure の追加クレデンシャル

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。

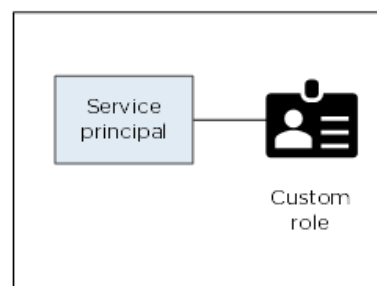
Initial Azure account



Second account



Third account



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。

The screenshot shows the 'Edit Account & Add Subscription' page. Under the 'Credentials' section, there is a text input field with a dropdown menu. The dropdown menu is open, showing 'cloud-manager-app | Application ID: 57c42424-88a0-480a...' and 'Managed Service Identity' (highlighted in blue). Below it, 'OCCM QA1 (Default)' is visible.

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。

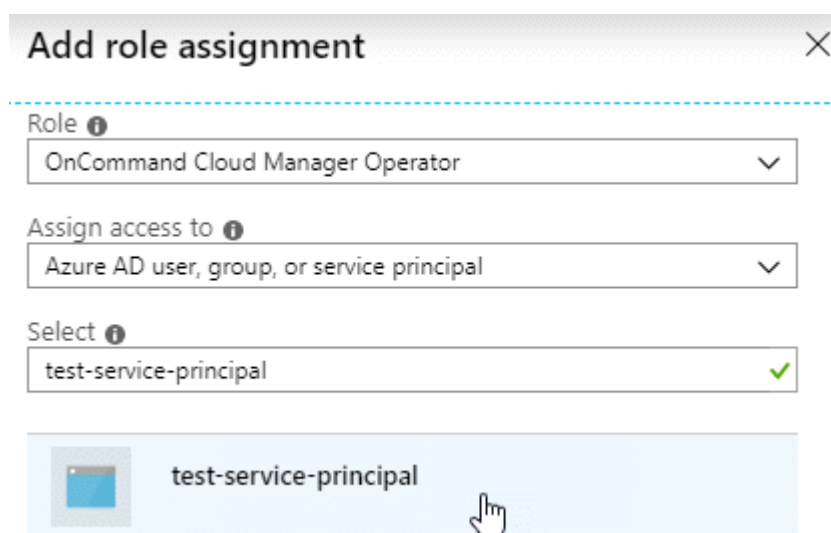
「 az role definition create — role-definition C : \Policy\_for \_cloud\_Manager\_azure\_3.8.7.json 」 という名前で作成します

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。

- Azure ポータルで、 \* Subscriptions \* サービスを開きます。
- サブスクリプションを選択します。
- [ \* 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。
- Cloud Manager Operator \* ロールを選択します。
- 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。
- 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。





**Add role assignment** ✕

Role ⓘ  
OnCommand Cloud Manager Operator ▼

Assign access to ⓘ  
Azure AD user, group, or service principal ▼

Select ⓘ  
test-service-principal ✓

 test-service-principal 

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。


## 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.





**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud


**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets


**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions


**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios


**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server


**Azure Import/Export**  
Programmatic control of import/export jobs


**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**  
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**  
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。

[Delete](#) [Endpoints](#)

**i** Welcome to the new and improved App registrations. Looking to learn

**Display name** : test-service-principal

**Application (client) ID** : 73de25f9-99be-4ae0-8b24-538ca787a6b3

**Directory (tenant) ID** : 4b0911a0-929b-4715-944b-c03745165b3a

**Object ID** : b37489a9-379f-49c2-b27c-e630514106a5

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。

### 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.

+ New client secret			
DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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に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に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/ja-jp/occm//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/ja-jp/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。管理対象に別の Azure サブスクリプションを選択しない限り、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。



**Edit Account & Add Subscription**

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

*No subscription is associated with this account*

## GCP

### 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 と同じプロジェクトまたは異なるプロジェクトに Cloud Volumes ONTAP システムを導入して管理する権限が Cloud Manager に付与されます。

#### 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（手順 2 を参照）。"](#)
- ["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"](#)。

データの階層化を考慮してください



Cloud Manager には Cloud Volumes ONTAP 9.6 用の GCP アカウントが必要ですが、9.7 以降の GCP アカウントは必要ありません。Cloud Volumes ONTAP 9.7 以降でデータ階層化を使用する場合は、の [手順 4](#) を実行します ["Google Cloud Platform での Cloud Volumes ONTAP の使用を開始する"](#)。

Cloud Volumes ONTAP 9.6 システムでデータの階層化を有効にするには、Cloud Manager に Google Cloud アカウントを追加する必要があります。データ階層化により、コールドデータを低コストのオブジェクトストレージに自動的に階層化し、プライマリストレージのスペースを再利用してセカンダリストレージを縮小できます。

アカウントを追加するときは、Storage Admin の権限を持つサービスアカウントのストレージアクセスキーを Cloud Manager に提供する必要があります。Cloud Manager は、アクセスキーを使用して Cloud Storage バケットをセットアップおよび管理し、データを階層化します。

Google Cloud アカウントを追加したら、作成、変更、または複製するときに、個々のボリュームでデータ階層化を有効にできます。

- ["GCP アカウントの設定方法と追加方法について説明します Cloud Manager の略"](#)。
- ["アクセス頻度の低いデータを低コストのオブジェクトストレージに階層化する方法について説明します"](#)。

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

Cloud Manager から管理できる Google Cloud Platform のクレデンシャルには、Cloud Volumes ONTAP 9.6 システムで使用される Connector VM インスタンスとストレージアクセスキーに関連付けられたクレデンシャルの 2 種類があります ["データの階層化"](#)。

### 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. 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 Google Cloud プロジェクトと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。





Google Cloud Project

OCCM-Dev ▼

Subscription

● GCP subscription for staging ▼

+ Add Subscription

5. [ 関連付け（Associate） ] をクリックします。

#### でのデータ階層化のための **GCP** アカウントの設定と追加 **Cloud Volumes ONTAP 9.6**

Cloud Volumes ONTAP 9.6 を有効にする場合は のシステム "[データの階層化](#)"、Storage Admin の権限があるサービスアカウントのストレージアクセスキーを Cloud Manager に提供する必要があります。Cloud Manager は、アクセスキーを使用して Cloud Storage バケットをセットアップおよび管理し、データを階層化します。



Cloud Volumes ONTAP 9.7 以降でデータ階層化を使用する場合は、の手順 4 を実行します "[Google Cloud Platform での Cloud Volumes ONTAP の使用を開始する](#)"。

#### **Google** のサービスアカウントとアクセスキーを設定する クラウドストレージ

サービスアカウントを使用すると、Cloud Manager でデータの階層化に使用する Cloud Storage バケットを認証してアクセスできます。キーは、Google Cloud Storage がリクエストを発行しているユーザーを認識できるようにするために必要です。

#### 手順

1. GCP IAM コンソールを開き、を開きます "[Storage Admin ロールを持つサービスアカウントを作成します](#)"。





2. に進みます "GCP Storage Settings ( GCP ストレージ設定) "。
3. プロンプトが表示されたら、プロジェクトを選択します。
4. [\*Interoperability \*] タブをクリックします。
5. まだ有効にしていない場合は、 \* 相互運用アクセスを有効にする \* をクリックします。
6. [ サービスアカウントのアクセスキー \*] で、 [ サービスアカウントのキーの作成 \*] をクリックします。
7. 手順 1 で作成したサービスアカウントを選択します。

## Select a service account

Email	Name	Keys
<input checked="" type="radio"/> data-tiering-for-netapp@top-monitor-250116.iam.gserviceaccount.com	data tiering for netapp	—

[CANCEL](#) [CREATE KEY](#) | [CREATE NEW ACCOUNT](#)

8. [ キーの作成 \*] をクリックします。

9. アクセスキーとシークレットをコピーします。

データ階層化用の GCP アカウントを追加する場合は、Cloud Manager でこの情報を入力する必要があります。

### Cloud Manager に GCP アカウントを追加する

サービスアカウントのアクセスキーが作成されたら、そのアクセスキーを Cloud Manager に追加できます。

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、[\* Google Cloud \*] を選択します。

3. サービスアカウントのアクセスキーとシークレットを入力します。

これらのキーを使用して、Cloud Manager でデータ階層化用の Cloud Storage バケットを設定できます。

4. ポリシーの要件が満たされていることを確認し、\* アカウントの作成 \* をクリックします。

Cloud Volumes ONTAP 9.6 システムでは、ボリュームを作成、変更、またはレプリケートするときに、個々のボリュームでデータ階層化を有効にできるようになりました。詳細については、[を参照してください](#) ["使用頻度の低いデータを低コストのオブジェクトストレージに階層化"](#)。

ただし、事前に、Cloud Volumes ONTAP が存在するサブネットがプライベート Google アクセス用に構成されていることを確認してください。手順については、[を参照してください](#) ["Google Cloud のドキュメント：「Configuring Private Google Access」"](#)。

# Cloud Manager へのネットアップサポートサイトのアカウントの追加

BYOL システムを導入するには、NetApp Support Site のアカウントを Cloud Manager に追加する必要があります。また、従量課金制システムの登録や ONTAP ソフトウェアのアップグレードも必要です。

次のビデオを視聴して、ネットアップサポートサイトのアカウントを Cloud Manager に追加する方法をご確認ください。または、下にスクロールして手順を確認します。



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. 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、\* NetApp Support Site \* を選択します。
4. アカウントの名前を指定し、ユーザ名とパスワードを入力します。
  - 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）。
  - 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。

5. [ アカウントの作成 ] をクリックします。 \*

新しい Cloud Volumes ONTAP システムの作成時や既存のシステムの登録時に、ユーザが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"](#)
- ["従量課金制システムの登録"](#)
- ["Cloud Manager によるライセンスファイルの管理方法について説明します"](#)

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

## Trademark Information

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