



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
March 10, 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	1
サービスプリンシパルを使用した Azure 権限の付与	1
Cloud Manager に Azure クレデンシャルを追加しています	7
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	8
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	9

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。

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"/> user_impersonation 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

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
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 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/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 に関連付けられない限り、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*

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.