



AWS

Cloud Manager

NetApp
June 08, 2021

目次

AWS	1
AWS のクレデンシャルと権限	1
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	3

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	[Redacted]	QA Subscription	Edit Credentials
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。

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

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation 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。

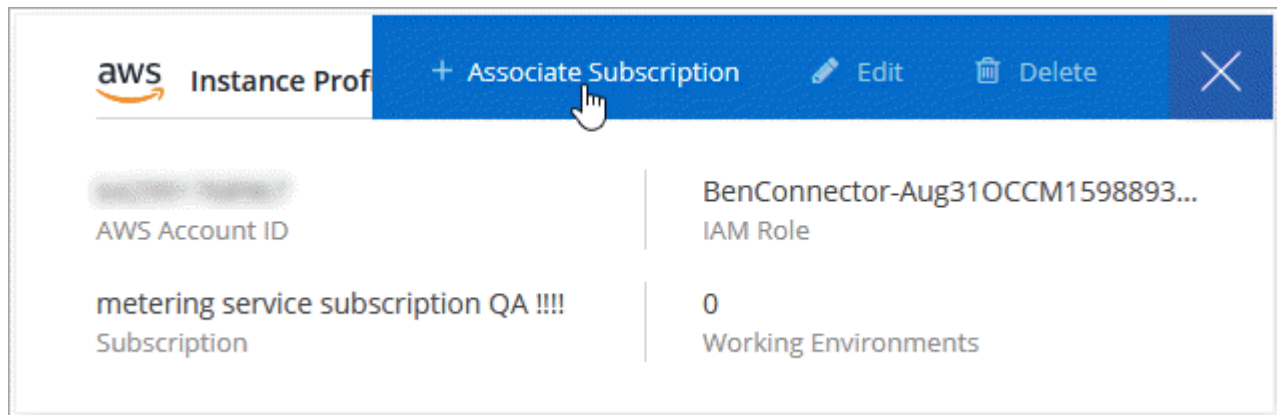
Cloud Manager にクレデンシャルを追加したあとに、AWS Marketplace サブスクリプションを関連付けるシナリオは 2 つあります。

- 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。"[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 (video)

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.