



AWS のクレデンシャルと権限 Cloud Manager

Ben Cammett, Aksel Davis
April 08, 2021

目次

| | |
|---|---|
| AWS のクレデンシャルと権限 | 1 |
| AWS の初期クレデンシャル | 1 |
| 追加の AWS クレデンシャル | 1 |
| 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。 | 3 |
| 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。 | 3 |

AWS のクレデンシアルと権限

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

AWS の初期クレデンシアル

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

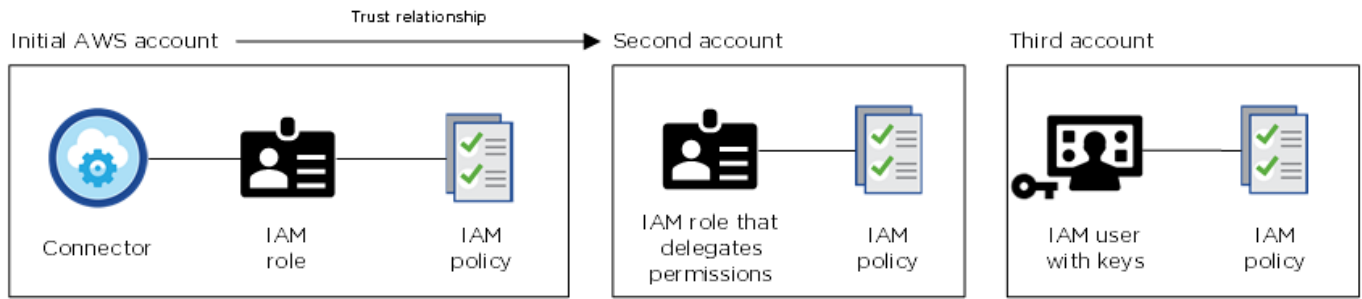


Cloud Volumes ONTAP の新しい作業環境を作成すると、Cloud Manager で選択される AWS クレデンシアルにはデフォルトで次のものがあります。

| Details & Credentials | | | |
|-----------------------|------------|--------------------------|----------------------------------|
| Instance Profile | Account ID | QA Subscription | Edit Credentials |
| Credentials | | Marketplace Subscription | |

追加の AWS クレデンシアル

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。

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.