



AWS KMS のセットアップ Cloud Manager

Ben Cammett
March 24, 2021

目次

AWS KMS のセットアップ	1
-----------------------	---

AWS KMS のセットアップ

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、AWS Key Management Service (KMS) を設定する必要があります。

手順

1. アクティブな Customer Master Key (CMK) が存在することを確認します。

CMK は、AWS 管理の CMK または顧客管理の CMK にすることができます。Cloud Manager および Cloud Volumes ONTAP と同じ AWS アカウントにすることも、別の AWS アカウントにすることもできます。

"AWS ドキュメント：「[Customer Master Keys \(CMK ; カスタマーマスターキー \)](#)」"

2. 各 CMK のキーポリシーを変更します。変更するには、Cloud Manager に a_key user_権限 を付与する IAM ロールを追加します。

IAM ロールをキーユーザとして追加すると、Cloud Volumes ONTAP で CMK を使用する権限が Cloud Manager に付与されます。

"AWS のドキュメント：「[キーの編集](#)」"

3. CMK が別の AWS アカウントにある場合は、次の手順を実行します。

- a. CMK が存在するアカウントから KMS コンソールにアクセスします。
- b. キーを選択します。
- c. General configuration * ペインで、キーの ARN をコピーします。

Cloud Volumes ONTAP システムの作成時には、Cloud Manager の ARN の指定が必要になります。

- d. その他の AWS アカウント * ペインで、Cloud Manager に権限を付与する AWS アカウントを追加します。

ほとんどの場合、Cloud Manager が配置されているアカウントです。Cloud Manager が AWS にインストールされていない場合、Cloud Manager に AWS アクセスキーを指定したアカウントになります。



Other AWS accounts

×

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam::

Enter the ID of another AWS accoui

:

root

Remove

Add another AWS account

Cancel

Save changes

- e. 次に、Cloud Manager に権限を付与する AWS アカウントに切り替えて、IAM コンソールを開きます。
- f. 以下の権限を含む IAM ポリシーを作成します。
- g. Cloud Manager に権限を付与する IAM ロールまたは IAM ユーザにポリシーを関連付けます。

次のポリシーは、Cloud Manager が外部 AWS アカウントから CMK を使用するために必要な権限を提供します。「リソース」セクションで、リージョンとアカウント ID を必ず変更してください。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

このプロセスの詳細については、を参照してください ["AWS ドキュメント：「外部 AWS アカウントによる CMK へのアクセスの許可」](#)。

4. お客様が管理する CMK を使用している場合は、Cloud Volumes ONTAP IAM ロールを a_key user_権限として追加して、CMK のキーポリシーを変更します。

この手順は、Cloud Volumes ONTAP でデータの階層化を有効にし、S3 バケットに格納されているデータを暗号化する場合に必要です。

作業環境の作成時に IAM ロールが作成されるため、このステップの _ 導入後 _ Cloud Volumes ONTAP を実行する必要があります。（もちろん、既存の Cloud Volumes ONTAP IAM ロールを使用することもできるため、この手順を前に実行することもできます）。

["AWS のドキュメント：「キーの編集」"](#)

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.