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。

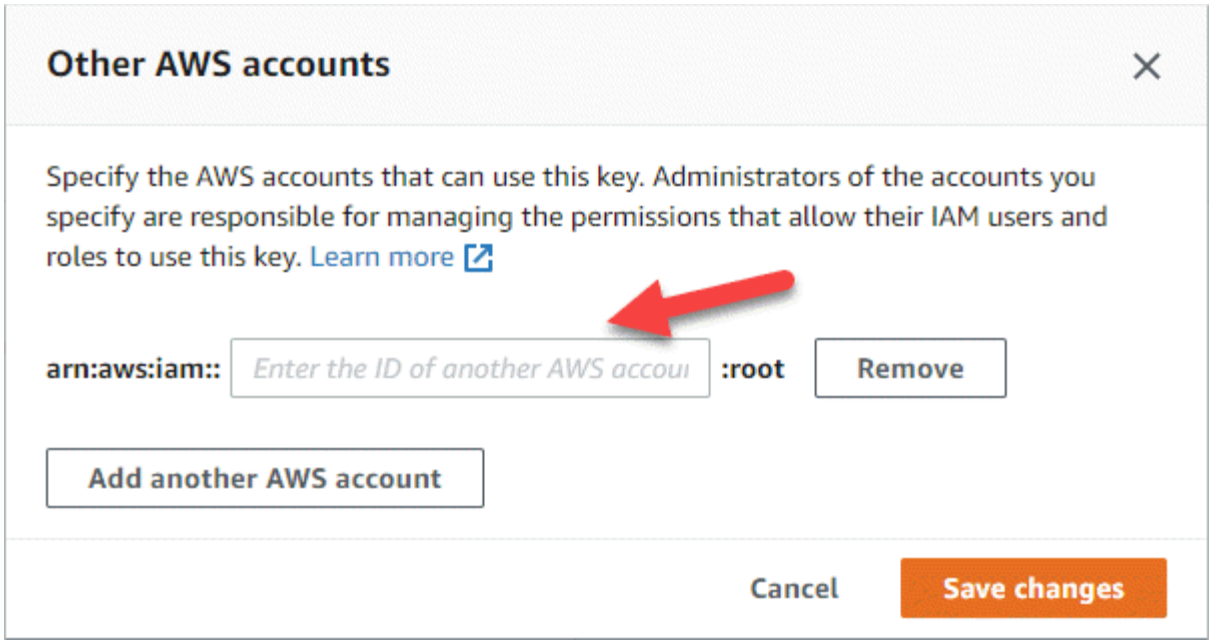
   b. キーを選択します。

   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。



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"