オンボードキー管理の設定
ONTAP 9

NetApp
December 20, 2024

目次

オンボードキー管理の設定

ONTAP 9 .6以降でオンボードキー管理を有効にする

オンボードキーマネージャを使用して、クラスタノードをFIPSドライブまたはSEDに対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャはFIPS-140-2レベル1に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager onboard enable`ます。`MetroCluster`構成では、同じパスフレーズを使用してまずローカルクラスタでを実行し、次にリモートクラスタでを実行する `security key-manager onboard sync`必要があります `security key-manager onboard enable`。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。MetroClusterの場合を除き、オプションを使用すると、リブート後にユーザにパスフレーズの入力を求めることができます `cc-mode-enabled=yes`。

オンボードキーマネージャがCCモードで有効になっ(`cc-mode-enabled=yes`ている場合）、システムの動作が次のように変更されます。

- システムは、情報セキュリティ国際評価基準モードで動作しているときに、クラスタパスフレーズの連続した失敗を監視します。

  NetAppストレージ暗号化（NSE）が有効になっている場合にブート時に正しいクラスタパスフレーズを入力しないと、システムはドライブを認証できず、自動的にリブートします。これを修正するには、ブートプロンプトで正しいクラスタパスフレーズを入力する必要があります。ブート後、クラスタパスフレーズをパラメータとして必要とするコマンドについては、24時間以内に最大5回連続してクラスタパスフレーズを正しく入力できます。制限に達した場合（クラスタパスフレーズを5回連続で正しく入力しなかった場合など）は、24時間のタイムアウト時間が経過するまで待つか、ノードをリブートして制限をリセットする必要があります。

- システムイメージの更新では、通常のNetApp RSA-2048コード署名証明書とSHA-256コード署名ダイジェストの代わりに、NetApp RSA-3072コード署名証明書とSHA-384コード署名ダイジェストを使用してイメージの整合性をチェックします。

  upgradeコマンドでは、さまざまなデジタル署名をチェックして、イメージの内容が変更または破損していないことを確認します。検証が成功すると、イメージの更新プロセスは次のステップに進みます。それ以外の場合、イメージの更新は失敗します。システムの更新については ' cluster image マニュアル・ページを参照してください

オンボードキーマネージャは、キーを揮発性メモリに格納します。揮発性メモリの内容は、システムを再起動または停止するとクリアされます。通常の動作状態では、システムが停止すると、揮発性メモリの内容は30秒以内に消去されます。

開始する前に

- NSEで外部キー管理（KMIP）サーバを使用する場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

  "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster環境を設定する必要があります。

手順

1. キー管理ツールのsetupコマンドを開始します。

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるように設定し `cc-mode-enabled=yes`ます。この `- cc-mode-enabled`オプションはMetroCluster構成ではサポートされません。 `security key-manager onboard enable`コマンドは、コマンドに置き換わるもの `security key-manager setup`です。

   次の例は、リブートのたびにパスフレーズの入力を要求せずに、cluster1でkey manager setupコマンドを開始します。

   ```
   cluster1::> security key-manager onboard enable

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

   ```
   security key-manager key query -node node
   ```

`security key-manager key query`コマンドは、コマンドに置き換わるもの `security key-manager query key`です。コマンド構文全体については、マニュアルページを参照してください。

次の例では、の認証キーが作成されたことを確認し `cluster1`ます。

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000020000000000001006f4e2513353a674305872a4c9f3bf797000000000000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000020000000000001006f4e2513353a674305872a4c9f3bf797000000000000000
```

終了後

あとで使用できるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーします。

キー管理情報はすべて、クラスタのReplicated Database（RDB；複製データベース）に自動的にバックアップされます。災害時に備えて、情報を手動でもバックアップしておく必要があります。

ONTAP 9 .5以前でオンボードキー管理を有効にする

オンボードキーマネージャを使用して、クラスタノードをFIPSドライブまたはSEDに対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャはFIPS-140-2レベル1に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスするためにクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager setup`ます。

MetroCluster構成の場合は、次のガイドラインを確認してください。

- ONTAP 9 .5では、同じパスフレーズを使用してローカルクラスタと `security key-manager setup -sync-metrocluster-config yes`リモートクラスタでを実行する必要があります `security key-manager setup`。
- ONTAP 9を実行する前に、同じパスフレーズを使用してローカルクラスタでを実行し、20秒ほど待ってからリモートクラスタでを実行する `security key-manager setup`必要があります `security key-manager setup`。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができ `-enable-cc-mode yes`ます。

NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。で `volume create`は、を指定する必要はありません `-encrypt true`。で `volume move start`は、を指定する必要はありません `-encrypt-destination true`。

パスフレーズの入力に失敗した場合は、ノードを再起動する必要があります。

開始する前に

- NSEで外部キー管理（KMIP）サーバを使用する場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

  "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster環境を設定する必要があります。

手順

1. キー管理ツールのセットアップを開始します。

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

ONTAP 9 .4以降では、オプションを使用して、リブート後にユーザにキー管理ツールのパスフレーズの入力を求めることができます `-enable-cc-mode yes`。NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。

次の例では、リブートのたびにパスフレーズの入力を要求せずに、cluster1でキー管理ツールのセットアップを開始します。

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. オンボードキー管理を設定するかどうかを確認するプロンプトでと入力し `yes`ます。
3. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

4. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
5. すべてのノードにキーが設定されていることを確認します。

   ```
   security key-manager key show
   ```

   完全なコマンド構文については、マニュアルページを参照してください。

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

終了後

キー管理情報はすべて、クラスタのReplicated Database（RDB；複製データベース）に自動的にバックアップされます。

オンボードキーマネージャのパスフレーズを設定する場合は、災害時に備えて、ストレージシステムの外部の安全な場所に情報を手動でバックアップする必要があります。を参照して "オンボードキー管理情報の手動でのバックアップ"

FIPSドライブまたはSEDへのデータ認証キーの割り当て（オンボードキー管理）

コマンドを使用して、FIPSドライブまたはSEDにデータ認証キーを割り当てることができます `storage encryption disk modify`。このキーは、クラスタノードでドライブ上のデータにアクセスするときに使用します。

タスクの内容

自己暗号化ドライブは、認証キーIDがデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。SASドライブの標準のデフォルト値は、キーIDが0x0のManufacturer Secure ID（MSID；メーカーのセキュアID）です。NVMeドライブの場合、標準のデフォルト値はnullキーで、空のキーIDで表されます。このキーIDを自己暗号化ドライブに割り当てると、認証キーIDがデフォルト以外の値に変更されます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

`storage encryption disk modify -disk *disk_ID* -data-key-id *key_ID*`

完全なコマンド構文については、コマンドのマニュアルページを参照してください。

> キーIDは、コマンドを使用して表示できます `security key-manager key query -key-type NSE-AK`。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 認証キーが割り当てられたことを確認します。

`storage encryption disk show`

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

著作権に関する情報

商標に関する情報