



# 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 .....	1
ONTAP 9 .6以降でオンボードキー管理を有効にする .....	1
ONTAP 9 .5以前でオンボードキー管理を有効にする .....	4
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） .....	6

# 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ます `security key-manager onboard enable`。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実行し、次にリモートクラスタで実行する `security key-manager onboard sync` する必要があります `security key-manager onboard enable`。

デフォルトでは、ノードのリポ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、リポ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た (`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:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

      Vserver: cluster1
      Key Manager: onboard
      Node: node2

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

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、クラスターの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ます `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実行し、20秒ほど待ってからリモートクラスタで実行する `security key-manager setup` 必要があります `security key-manager setup`。

デフォルトでは、ノードのリポ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、リポ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
-----
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF 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
0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
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
0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1    data
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。