NetApp Encryptionの管理

ONTAP 9

NetApp
January 23, 2026

目次

NetApp Encryptionの管理

ONTAPでボリュームデータの暗号化を解除する

`volume move start`コマンドを使用して、ボリュームデータを移動し、暗号化を解除できます。

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. 既存の暗号化されたボリュームを移動し、ボリュームのデータの暗号化を解除します。

   `volume move start -vserver *SVM_name* -volume volume_name -destination-aggregate *aggregate_name* -encrypt-destination false`

   `volume move start`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-move-start.html["ONTAPコマンド リファレンス"^]を参照してください。

   次のコマンドは、`vol1`という名前の既存のボリュームを宛先アグリゲート`aggr3`に移動し、ボリューム上のデータを暗号化解除します：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   ボリュームの暗号化キーが削除されます。ボリュームのデータの暗号化が解除されます。

2. ボリュームで暗号化が無効になっていることを確認します。

   `volume show -encryption`

   `volume show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

   次のコマンドは、`cluster1`上のボリュームが暗号化されているかどうかを表示します：

```
cluster1::> volume show -encryption

Vserver  Volume   Aggregate   State    Encryption State
-------  ------   ---------   -----    ----------------
vs1      vol1     aggr1       online   none
```

ONTAPで暗号化されたボリュームを移動する

`volume move start`コマンドを使用して、暗号化されたボリュームを移動できます。移動したボリュームは、同じアグリゲートまたは別のアグリゲートに配置できます。

タスク概要

デスティネーション ノードまたはデスティネーション ボリュームでボリューム暗号化がサポートされていない場合、移動は失敗します。

`-encrypt-destination`オプションは、 `volume move start`暗号化されたボリュームの場合、デフォルトで`true`に設定されます。宛先ボリュームを暗号化しないことを指定する必要があるのは、ボリューム上のデータが誤って暗号化解除されないようにするためです。

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. 既存の暗号化されたボリュームを移動し、ボリュームのデータを暗号化されたままにします。

   volume move start -vserver *SVM_name* -volume *volume_name* -destination-aggregate *aggregate_name*

   `volume move start`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-move-start.html["ONTAPコマンド リファレンス"^]を参照してください。

   次のコマンドは、 `vol1`という名前の既存のボリュームを宛先アグリゲート `aggr3`に移動し、ボリューム上のデータを暗号化されたままにします（：）

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

`volume show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

次のコマンドは、`cluster1`の暗号化されたボリュームを表示します：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

ONTAPのvolume encryption rekey startコマンドを使用してボリュームの暗号化キーを変更する

ボリュームの暗号化キーを定期的に変更することは、セキュリティ上のベストプラクティスです。ONTAP 9.3以降では、`volume encryption rekey start`コマンドを使用して暗号化キーを変更できます。

タスク概要

キー再生成操作を開始すると、必ず完了する必要があります。以前のキーに戻すことはできません。操作中にパフォーマンスの問題が発生した場合は、`volume encryption rekey pause`コマンドを実行して操作を一時停止し、`volume encryption rekey resume`コマンドを実行して操作を再開することができます。

キー更新操作が完了するまで、ボリュームには2つのキーが存在します。新しい書き込みとそれに対応する読み取りには新しいキーが使用されます。それ以外の場合、読み取りには古いキーが使用されます。

`volume encryption rekey start`を使用してSnapLockボリュームのキーを再設定することはできません。

手順

1. 暗号化キーを変更します。

   ```
   volume encryption rekey start -vserver SVM_name -volume volume_name
   ```

   次のコマンドは、SVM`vs1`上の`vol1`の暗号化キーを変更します：

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. キー変更処理のステータスを確認します。

```
volume encryption rekey show
```

`volume encryption rekey show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-encryption-rekey-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

次のコマンドは、キー再生成操作のステータスを表示します：

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ----------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. キー変更処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

`volume show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

次のコマンドは、`cluster1`の暗号化されたボリュームを表示します：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

ONTAP volume move startコマンドを使用してボリュームの暗号化キーを変更します

セキュリティ上のベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することをお勧めします。`volume move start`コマンドを使用して暗号化キーを変更できます。移動したボリュームは、同じアグリゲート上にあっても、別のアグリゲート上にあっても構いません。

タスク概要

`volume move start`を使用してSnapLockまたはFlexGroupボリュームのキーを再設定することはできません。

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. 既存のボリュームを移動し、暗号化キーを変更します。

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true`

   `volume move start`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-move-start.html["ONTAPコマンド リファレンス"^]を参照してください。

   次のコマンドは、`**vol1**`という名前の既存のボリュームを宛先アグリゲート`**aggr2**`に移動し、暗号化キーを変更します：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr2 -generate-destination-key true
   ```

   ボリュームの新しい暗号化キーが作成されます。ボリュームのデータは暗号化されたままです。

2. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   `volume show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

   次のコマンドは、`cluster1`の暗号化されたボリュームを表示します：

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  ---------  ----
   vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
   ```

ONTAP NetApp Storage Encryptionの認証キーをローテーションする

NetApp Storage Encryption（NSE）を使用する場合、認証キーをローテーションすることができます。

タスク概要

外部キー管理ツール（KMIP）を使用している場合、NSE環境での認証キーのローテーションがサポートされます。

> オンボード キー マネージャ（OKM）では、NSE環境での認証キーのローテーションはサポートされません。

手順

1. `security key-manager create-key`コマンドを使用して新しい認証キーを生成します。

   認証キーを変更する前に、新しい認証キーを生成しておく必要があります。

2. `storage encryption disk modify -disk * -data-key-id`コマンドを使用して認証キーを変更します。

関連情報

- "ストレージ暗号化ディスクの変更"

ONTAPで暗号化されたボリュームを削除する

`volume delete`コマンドを使用して暗号化されたボリュームを削除できます。

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。
- ボリュームはオフラインである必要があります。

手順

1. 暗号化されたボリュームを削除します。

   `volume delete -vserver SVM_name -volume volume_name`

   > `volume delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

   次のコマンドは、`vol1`という名前の暗号化されたボリュームを削除します：

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

削除の確認を求められたら `yes`を入力します。

24時間後にボリュームの暗号化キーが削除されます。

`volume delete`と `-force true`オプションを使用して、ボリュームを削除し、対応する暗号化キーを直ちに破棄します。このコマンドには高度な権限が必要です。 `volume delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-delete.html["ONTAPコマンド リファレンス"^]を参照してください。

終了後の操作

`volume delete`コマンドを発行した後、保持期間中に `volume recovery-queue`コマンドを使用して削除されたボリュームを回復できます：

```
volume recovery-queue SVM_name -volume volume_name
```

"ボリュームリカバリ機能の使い方"

暗号化されたボリュームでのデータのセキュア パージ

暗号化された**ONTAP**ボリュームからデータを安全に消去する方法について説明します。

ONTAP 9.4以降では、セキュアパージを使用して、NVE対応ボリューム上のデータを無停止でスクラブできます。暗号化されたボリューム上のデータをスクラブすることで、例えばブロックの上書き時にデータの痕跡が残ってしまう「スピレッジ」が発生した場合や、退去するテナントのデータを安全に削除する場合など、物理メディアからのデータの復元を不可能にすることができます。

セキュア パージの対象となるのは、NVE対応ボリューム上で以前に削除されたファイルだけです。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボード キー マネージャではなく、KMIPサーバを使用する必要があります。

セキュア パージを使用する場合の考慮事項

- NetApp Aggregate Encryption（NAE）が有効になっているアグリゲートに作成されたボリュームでは、セキュア パージがサポートされません。
- セキュア パージの対象となるのは、NVE対応ボリューム上で以前に削除されたファイルだけです。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボード キー マネージャではなく、KMIPサーバを使用する必要があります。

セキュア パージの動作は、ONTAPのバージョンによって異なります。

ONTAP 9.8以降

- セキュア パージはMetroClusterとFlexGroupでサポートされます。
- パージするボリュームがSnapMirror関係のソースである場合、セキュア パージを実行するためにSnapMirror関係を解除する必要はありません。
- 再暗号化の方法は、SnapMirrorデータ保護（DP）を使用するボリュームと使用しないボリューム、またはSnapMirror拡張データ保護を使用するボリュームとで異なります。
  - SnapMirrorデータ保護（DP）モードを使用するボリュームでは、デフォルトでボリューム移動方式を使用してデータが再暗号化されます。
  - SnapMirrorデータ保護を使用しないボリュームまたはSnapMirror拡張データ保護（XDP）モードを使用するボリュームでは、インプレース再暗号化方式がデフォルトで使用されます。
  - これらのデフォルトは `secure purge re-encryption-method [volume-move|in-place-rekey]`コマンドを使用して変更できます。
- デフォルトでは、FlexVolボリューム内のすべてのスナップショットは、セキュアパージ操作中に自動的に削除されます。デフォルトでは、FlexGroupボリューム内のスナップショットおよびSnapMirrorデータ保護を使用しているボリューム内のスナップショットは、セキュアパージ操作中に自動的に削除されません。これらのデフォルトは、 `secure purge delete-all-snapshots [true|false]`コマンドを使用して変更できます。

ONTAP 9.7以前

- 次の機能ではセキュア パージがサポートされません。
  - FlexClone
  - SnapVault
  - FabricPool
- パージするボリュームがSnapMirror関係のソースである場合、ボリュームをパージする前にSnapMirror関係を解除する必要があります。

  ボリューム内に使用中のスナップショットがある場合は、ボリュームをパージする前にスナップショットを解放する必要があります。たとえば、FlexCloneボリュームを親ボリュームから分割する必要がある場合などです。

- セキュア パージ機能を呼び出すと、ボリューム移動がトリガーされ、パージされない残りのデータが新しいキーで再度暗号化されます。

  移動されたボリュームは現在のアグリゲートに残ります。パージされたデータをストレージ メディアからリカバリできないように、古いキーは自動的に破棄されます。

暗号化された**ONTAP**ボリュームから**SnapMirror**関係なしでデータを消去する

ONTAP 9.4 以降では、 secure-purge を使用して、 NVE 対応ボリューム上のデータを中断せずに「スクラブ」することができます。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して、操作のステータスを表示できます。 `volume

encryption secure-purge abort`コマンドを使用して、操作を終了できます。

> SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

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。
- このタスクを実行するにはadvanced権限が必要です。

手順

1. セキュア パージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュア パージを実行するファイルを削除します。
   - SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。
2. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

3. セキュア パージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 削除したファイルのセキュア パージを実行します。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   次のコマンドは、SVM`vs1`上の `vol1`で削除されたファイルを安全に消去します：

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. セキュア パージ処理のステータスを確認します。

   ```
   volume encryption secure-purge show
   ```

SnapMirror非同期関係を持つ暗号化された ONTAP ボリュームからデータをスクラブする

ONTAP 9.8 以降では、セキュア パージを使用して、SnapMirror 非同期関係にある NVE 対応ボリューム上のデータを中断することなく「スクラブ」することができます。

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。

- このタスクを実行するにはadvanced権限が必要です。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して、操作のステータスを表示できます。 `volume encryption secure-purge abort`コマンドを使用して、操作を終了できます。

> SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュア パージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュア パージを実行するファイルを削除します。
   - SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。
3. 非同期関係のデスティネーション ボリュームでセキュア パージを準備します。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

4. セキュア パージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. セキュア パージを実行するファイルがベースSnapshotに含まれている場合は、次の手順を実行します。
   a. SnapMirror非同期関係の宛先ボリュームにSnapshotを作成します：

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. SnapMirrorを更新してベーススナップショットを前進させる：

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   a. 手順（a）と（b）を、ベースSnapshotの数に1を加えた回数だけ繰り返します。

      たとえば、ベースSnapshotが2つある場合は手順（a）と（b）を3回繰り返します。

b. ベーススナップショットが存在することを確認します：+ `snapshot show -vserver *SVM_name* -volume *volume_name*`

c. ベーススナップショットを削除します：+ `snapshot delete -vserver *svm_name* -volume *volume_name* -snapshot snapshot`

6. 削除したファイルのセキュア パージを実行します。

   `volume encryption secure-purge start -vserver *svm_name* -volume *volume_name*`

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは、SVM “vs1” 上の “vol1” 上の削除されたファイルを安全に消去します：

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. セキュア パージ処理のステータスを確認します。

   `volume encryption secure-purge show`

関連情報

- "snapmirror update"

SnapMirror同期関係を持つ暗号化された ONTAP ボリュームからデータをスクラブする

ONTAP 9.8以降では、セキュア パージを使用して、SnapMirror同期関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、完了までに数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して操作のステータスを確認できます。 `volume encryption secure-purge abort`コマンドを使用して操作を終了できます。

> SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

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。
- このタスクを実行するにはadvanced権限が必要です。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   `set -privilege advanced`

2. セキュア パージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュア パージを実行するファイルを削除します。
   - SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。
3. 非同期関係のデスティネーション ボリュームでセキュア パージを準備します。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   SnapMirror同期関係のもう一方のボリュームに対してこの手順を繰り返します。
4. セキュア パージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```
5. 対象ファイルがベースSnapshotまたは共通Snapshotに含まれている場合は、SnapMirrorを更新して共通Snapshotを最新の状態にします。

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   共通Snapshotは2つあるため、このコマンドは2回実行する必要があります。
6. セキュア パージ ファイルがアプリケーション整合性スナップショット内にある場合は、SnapMirror 同期関係にある両方のボリューム上のスナップショットを削除します：

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   この手順は両方のボリュームで実行します。
7. 削除したファイルのセキュア パージを実行します。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   SnapMirror同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは、SVM "`vs1`"上の"`vol1`"上の削除されたファイルを安全に消去します。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```
8. セキュア パージ処理のステータスを確認します。

   ```
   volume encryption secure-purge show
   ```

関連情報

- "snapmirror update"

ONTAPオンボードキー管理パスフレーズを変更する

NetAppでは、オンボードキー管理パスフレーズを定期的に変更することを推奨しています。新しいパスフレーズは、ストレージシステム外の安全な場所に保管する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。
- MetroCluster環境では、ローカル クラスタでパスフレーズを更新した後、パートナー クラスタでパスフレーズの更新を同期します。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. オンボードキー管理パスフレーズを変更します。使用するコマンドは、実行している ONTAP のバージョンによって異なります。

   ONTAP 9.6以降

   ```
   security key-manager onboard update-passphrase
   ```

   ONTAP 9.5以前

   ```
   security key-manager update-passphrase
   ```

3. 32文字から256文字までのパスフレーズを入力します。"`cc-mode`"の場合は64文字から256文字までのパスフレーズを入力します。

   指定された「`cc-mode`」パスフレーズが64文字未満の場合、キー マネージャーのセットアップ操作でパスフレーズ プロンプトが再度表示されるまでに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. MetroCluster構成の場合は、パートナー クラスタで更新されたパスフレーズを同期します。
   a. ONTAPバージョンに適したコマンドを選択して、パートナー クラスタのパスフレーズを同期します：

ONTAP 9.6以降

```
security key-manager onboard sync
```

ONTAP 9.5以前

- ONTAP 9.5 では、次のコマンドを実行します。

  ```
  security key-manager setup -sync-metrocluster-config
  ```

- ONTAP 9.4 以前では、ローカル クラスタでパスフレーズを更新した後、20 秒待ってから、パートナー クラスタで次のコマンドを実行します：

  ```
  security key-manager setup
  ```

b. プロンプトが表示されたら、新しいパスフレーズを入力します。

   両方のクラスターで同じパスフレーズを使用する必要があります。

終了後の操作

将来使用するために、オンボード キー管理パスフレーズをストレージ システム外部の安全な場所にコピーします。

オンボードキー管理パスフレーズを変更するたびに、キー管理情報を手動でバックアップします。

関連情報

- "オンボード キー管理情報の手動バックアップ"
- "セキュリティキー・マネージャーオンボードのパスフレーズ更新"

ONTAPオンボードキー管理情報を手動でバックアップする

オンボード キー マネージャのパスフレーズを設定するときは必ず、オンボード キー管理情報をストレージ システム外部の安全な場所にコピーする必要があります。

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。
- このタスクを実行するにはadvanced権限が必要です。

タスク概要

すべてのキー管理情報は、クラスターの複製データベース（RDB）に自動的にバックアップされます。災害発生時に備えて、キー管理情報を手動でバックアップすることも必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスターのキー管理バックアップ情報を表示します：

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard show-backup`
ONTAP 9.5以前	`security key-manager backup show`

次の 9.6 コマンドは、 `cluster1`のキー管理バックアップ情報を表示します：

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

3. 災害発生時に使用するために、バックアップ情報をストレージ システム外部の安全な場所にコピーします。

関連情報

- "security key-manager onboard show-backup"
- "security key-manager backup show"

ONTAPでオンボードキー管理暗号化キーをリストアする

場合によっては、オンボードキー管理暗号化キーを復元する必要があります。キーの復元が必要であることを確認したら、オンボードキーマネージャを設定してキーを復元できます。オンボードキー管理暗号化キーの復元手順は、ONTAPのバージョンによって異なります。

開始する前に

- NSEを外部KMIPサーバーと併用する場合は、外部キーマネージャーデータベースを削除してください。詳細については、"外部キー管理からONTAPオンボードキー管理への移行"を参照してください。
- 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。

Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEでは、Flash Cacheモジュール上のデータは暗号化されません。

ONTAP 9.6以降

ONTAP 9.8以降を実行していて、ルートボリュームが暗号化されている場合は、[ontap-9-8]の手順に従ってください。

1. キーを復元する必要があることを確認します：+ `security key-manager key query -node node`

   `security key-manager key query`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-query.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. キーを復元する：+ `security key-manager onboard sync`

   `security key-manager onboard sync`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-onboard-sync.html["ONTAPコマンド リファレンス
   "^]を参照してください。

3. パスフレーズのプロンプトで、クラスタのオンボード キー管理のパスフレーズを入力します。

ONTAP 9.8以降でルート ボリュームが暗号化されている場合

ONTAP 9.8以降を実行していてルート ボリュームが暗号化されている場合は、ブート メニューを使用してオンボード キー管理のリカバリ パスフレーズを設定する必要があります。ブート メディアを交換する場合に

も、このプロセスが必要です。

1. ノードをブートメニューにブートし、オプション `(10) Set onboard key management recovery secrets`を選択します。
2. このオプションを使用するには `y`を入力してください。
3. プロンプトで、クラスタのオンボード キー管理のパスフレーズを入力します。
4. プロンプトで、バックアップ キーのデータを入力します。

   バックアップキーデータを入力すると、ノードはブートメニューに戻ります。

5. ブートメニューからオプション `(1) Normal Boot`を選択します。

ONTAP 9.5以前

1. キーを復元する必要があることを確認します：+ `security key-manager key show`
2. キーを復元する：+ `security key-manager setup -node` *node*

   `security key-manager setup`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli-9161/security-key-manager-setup.html["ONTAPコマンド リファレンス"^]を参照してください。

3. パスフレーズのプロンプトで、クラスタのオンボード キー管理のパスフレーズを入力します。

ONTAP外部キー管理暗号化キーを復元する

外部キー管理の暗号化キーを手動でリストアし、別のノードにプッシュすることができます。この処理は、クラスタのキーの作成時に一時的に停止していたノードを再起動する場合に実行します。

タスク概要

ONTAP 9.6 以降では、 `security key-manager key query -node node_name`コマンドを使用して、キーを復元する必要があるかどうかを確認できます。

ONTAP 9.5 以前では、 `security key-manager key show`コマンドを使用して、暗号化キーを復元する必要があるかどうかを確認できます。

Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEでは、Flash Cacheモジュール上のデータは暗号化されません。

`security key-manager key query`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-query.html["ONTAPコマンド リファレンス"^]をご覧ください。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. ONTAP 9.8以降を実行していてルート ボリュームが暗号化されている場合は、次の手順を実行します。

   ONTAP 9.7以前を実行している場合、またはONTAP 9.8以降を実行していてルート ボリュームが暗号化されていない場合は、この手順を省略してください。

   a. ブート引数を設定します：+
   ```
   setenv kmip.init.ipaddr <ip-address>
   setenv kmip.init.netmask <netmask>
   setenv kmip.init.gateway <gateway>
   setenv kmip.init.interface e0M
   boot_ontap
   ```

   b. ノードをブートメニューにブートし、オプション `(11) Configure node for external key management` を選択します。

   c. プロンプトに従って管理証明書を入力します。

      管理証明書の情報をすべて入力すると、システムがブート メニューに戻ります。

   d. ブートメニューからオプション `(1) Normal Boot`を選択します。

2. キーをリストアします。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5以前

   `node`デフォルトではすべてのノードが対象になります。

   このコマンドは、オンボード キー管理が有効な場合はサポートされません。

   次のONTAP 9.6コマンドは、外部キー管理認証キーを `cluster1`のすべてのノードに復元します：

```
clusterl::> security key-manager external restore
```

関連情報

- "セキュリティキー・マネージャ外部リストア"

ONTAPクラスタ上のKMIP SSL証明書を置き換える

すべてのSSL証明書には有効期限があります。認証キーへのアクセスが失われないように、証明書の有効期限が切れる前に証明書を更新する必要があります。

開始する前に

- クラスタに対して新しいパブリック証明書（KMIPクライアント証明書）と秘密鍵を入手しておく必要があります。
- KMIPサーバに対して新しいパブリック証明書（KMIPサーバCA証明書）を入手しておく必要があります。
- このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。
- MetroCluster環境でKMIP SSL証明書を交換する場合は、同じ交換用KMIP SSL証明書を両方のクラスタにインストールする必要があります。

KMIPサーバへの交換用のクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

手順

1. 新しいKMIPサーバCA証明書をインストールします。

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. 新しいKMIPクライアント証明書をインストールします。

   ```
   security certificate install -type client -vserver <>
   ```

3. 新しくインストールした証明書を使用するようにキー管理ツールの設定を更新します。

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   MetroCluster環境でONTAP 9.6以降を実行している場合に管理SVMのキー管理ツールの設定を変更するには、構成内の両方のクラスタでコマンドを実行する必要があります。

新しくインストールされた証明書を使用するようにキーマネージャーの設定を更新すると、新しいクライアント証明書の公開鍵/秘密鍵が以前にインストールされた鍵と異なる場合、エラーが返されます。このエラーを回避する方法については、"NetAppナレッジベース：新しいクライアント証明書の公開鍵または秘密鍵が既存のクライアント証明書と異なります"をご覧ください。

関連情報

- "security certificate install"
- "セキュリティキー・マネージャ外部変更"

ONTAPでFIPSドライブまたはSEDを交換する

FIPSドライブとSEDは、通常のディスクと同じ方法で交換できます。交換用ドライブに新しいデータ認証キーを割り当ててください。FIPSドライブの場合は、新しいFIPS 140-2認証キーを割り当てることもできます。

HAペアで"SASまたはNVMeドライブの暗号化（SED、NSE、FIPS）"を使用している場合は、システムを初期化する前に（ブートオプション4または9）、HAペア内のすべてのドライブについて、"FIPSドライブまたはSEDを非保護モードに戻す"トピックの指示に従う必要があります。これを行わないと、将来ドライブを再利用した場合にデータが失われる可能性があります。

開始する前に

- ドライブで使用される認証キーのキーIDを確認しておく必要があります。
- 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. ディスクが障害状態とマークされていることを確認します。

   ```
   storage disk show -broken
   ```

   `storage disk show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                    Usable
   Physical
       Disk   Outage Reason HA Shelf Bay Chan   Pool   Type    RPM     Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
   -------
       0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
   133.9GB
       0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
   134.2GB
   [...]
   ```

2. ディスク シェルフ モデルのハードウェア ガイドの指示に従い、障害ディスクを取り外して、新しいFIPSドライブまたはSEDに交換します。
3. 交換した新しいディスクの所有権を割り当てます。

   ```
   storage disk assign -disk disk_name -owner node
   ```

   `storage disk assign`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-disk-assign.html["ONTAPコマンド リファレンス"^]を参照してください。

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 新しいディスクが割り当てられていることを確認します。

   `storage encryption disk show`

   `storage encryption disk show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   "FIPSドライブまたはSEDへのデータ認証キーの割り当て（外部キー管理）"

6. 必要に応じて、FIPS 140-2認証キーをFIPSドライブに割り当てます。

   "FIPSドライブへのFIPS 140-2認証キーの割り当て"

関連情報

- "storage disk assign"
- "storage disk show"
- "storage disk show | more"

FIPSドライブまたはSEDのデータにアクセスできない状態にする方法

FIPSドライブまたはSED上のONTAPデータをアクセス不能にする方法について学習します

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブの未使用スペースは新しいデータに使用できるようにしておく場合は、ディスクを完全消去で

きます。データに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、ディスクを破棄できます。

- ディスク完全消去

  自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID（SAS;メーカーのセキュアID）0x0（SASドライブ）またはnull（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去されたディスクは、初期化されていないスペア ディスクとして再利用できます。

- ディスクの破棄

  FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ディスクが完全にロックされます。これにより、ディスクが永続的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。

完全消去と破棄は、個々の自己暗号化ドライブまたはノードのすべての自己暗号化ドライブに対して実行できます。

ONTAPでFIPSドライブまたはSEDを完全消去する

FIPS ドライブまたは SED 上のデータを永続的にアクセス不能にし、そのドライブを新しいデータ用に使用する場合は、 `storage encryption disk sanitize` コマンドを使用してドライブをサニタイズできます。

タスク概要

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オン ロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID（SAS;メーカーのセキュアID）0x0（SASドライブ）またはnull（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去されたディスクは、初期化されていないスペア ディスクとして再利用できます。

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. 保持しておく必要があるデータを別のディスクのアグリゲートにすべて移行します。
2. 完全消去するFIPSドライブまたはSEDのアグリゲートを削除します。

   `storage aggregate delete -aggregate` *`aggregate_name`*

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

`storage aggregate delete`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

3. 完全消去するFIPSドライブまたはSEDのディスクIDを確認します。

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

`storage encryption disk show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

`security key-manager query`コマンドを使用してキー ID を表示できます。

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. ドライブを完全消去します。

```
storage encryption disk sanitize -disk disk_id
```

このコマンドは、ホットスペアディスクまたは破損ディスクのみをサニタイズするために使用できます。ディスクの種類に関係なくすべてのディスクをサニタイズするには、 `-force-all-state`オプションを使用してください。 `storage encryption disk sanitize`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

続行する前に、ONTAPから確認フレーズの入力を求められます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. サニタイズされたディスクをアンフェイルします： `storage disk unfail -spare true -disk disk_id`
7. ディスクに所有者がいるかどうかを確認します： `storage disk show -disk disk_id`ディスクに所有者がいない場合は、所有者を割り当てます。 `storage disk assign -owner node -disk disk_id`
8. 完全消去するディスクを所有するノードのノードシェルに切り替えます。

   `system node run -node node_name`

   `disk sanitize release`コマンドを実行します。

9. ノードシェルを終了します。ディスクの障害を再度解除します： `storage disk unfail -spare true -disk disk_id`
10. ディスクがスペアになり、アグリゲート内で再利用できる状態になっていることを確認します： `storage disk show -disk disk_id`

関連情報

- "storage disk assign"
- "storage disk show"
- "ストレージディスクのアンフェイル"
- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスク完全消去"
- "storage encryption disk show-status"

ONTAPでFIPSドライブまたはSEDを破棄する

FIPS ドライブまたは SED 上のデータを永続的にアクセス不能にし、ドライブを再利用する必要がない場合は、 `storage encryption disk destroy`コマンドを使用してディスクを破棄できます。

タスク概要

FIPSドライブまたはSEDを破壊すると、システムはディスク暗号化キーを未知のランダム値に設定し、ドライブを不可逆的にロックします。これにより、ディスクは事実上使用できなくなり、ディスク上のデータにも永久にアクセスできなくなります。ただし、ディスクのラベルに記載されている物理セキュアID（PSID）を使用して、ディスクを工場出荷時の設定にリセットすることができます。詳細については、"認証キーが失われた場合にFIPSドライブまたはSEDを使用可能な状態に戻す"をご覧ください。

（故障）ディスク返却不要サービス（NRD Plus）を契約している場合を除き、FIPSドライブまたはSEDは破棄しないでください。ディスクを破棄すると保証が無効になります。

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. 保持しておく必要があるデータを別のディスクのアグリゲートにすべて移行します。
2. 破棄する FIPS ドライブまたは SED 上のアグリゲートを削除します：

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   ```
   `storage aggregate delete`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。
   ```

3. 破棄する FIPS ドライブまたは SED のディスク ID を特定します：

   ```
   storage encryption disk show
   ```

   ```
   `storage encryption disk show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。
   ```

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. ディスクを破壊します：

```
storage encryption disk destroy -disk disk_id
```

`storage encryption disk destroy`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-destroy.html["ONTAPコマンド リファレンス"^]をご覧ください。

処理を続行する前に確認のフレーズを入力するように求められます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

関連情報

- "ストレージ暗号化ディスク破壊"
- "storage disk show | more"
- "storage encryption disk show-status"

ONTAPのFIPSドライブまたはSEDで緊急データ消去を実行

セキュリティに関する緊急事態が発生した場合は、ストレージ システムまたはKMIPサーバへの給電が遮断されていても、FIPSドライブまたはSEDへのアクセスをただちに禁止できます。

開始する前に

- 使用しているKMIPサーバに給電されていない場合は、KMIPサーバに簡単に破棄できる認証アイテム（スマート カードやUSBドライブなど）が設定されている必要があります。
- 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のデータの緊急時のシュレッディングを実行します。

状况	操作

ストレージ システムに給電されており、ストレージ システムを適切な手順でオフラインにする時間がある	a. ストレージ システムがHAペアとして設定されている場合は、テイクオーバーを無効にします。 b. すべてのアグリゲートをオフラインにしてから削除します。 c. 権限レベルを詳細に設定します：+ `set -privilege advanced` d. ドライブが FIPS 準拠モードの場合は、ノードの FIPS 認証キー ID をデフォルトの MSID に戻します：+ `storage encryption disk modify -disk * -fips-key-id 0x0` e. ストレージ システムを停止します。 f. メンテナンス モードでブートします。 g. ディスクを完全消去するか破棄します。 ◦ ディスク上のデータにアクセスできないようにしながらもディスクを再利用できるようにするには、ディスクをサニタイズします：+ `disk encrypt sanitize -all` ◦ ディスク上のデータにアクセスできないようにし、ディスクを保存する必要がない場合は、ディスクを破棄します： `disk encrypt destroy disk_id1 disk_id2 …`	ストレージ システムに給電されており、データをただちにシュレッディングする必要がある

a. ディスク上のデータにアクセスできないようにしながらもディスクを再利用できるようにするには、ディスクをサニタイズします：
b. ストレージ システムがHAペアとして設定されている場合は、テイクオーバーを無効にします。
c. 権限レベルをadvancedに設定します。
`set -privilege advanced`
d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. ディスクをサニタイズします：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. ディスク上のデータにアクセスできないようにし、ディスクを保存する必要がない場合は、ディスクを破壊します：
	b. ストレージ システムがHAペアとして設定されている場合は、テイクオーバーを無効にします。
	c. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	d. ディスクを破壊します：
	`storage encryption disk destroy -disk * -force-all-states true`
		ストレージ システムがパニック状態になります。これで、ストレージ システムは永続的に無効な状態になり、すべてのデータが消去されます。システムを再度使用するには、再設定する必要があります。

KMIPサーバに給電されているが、ストレージ システムには給電されていない	a. KMIPサーバにログインします。 b. アクセスを禁止するデータを含むFIPSドライブまたはSEDに関連付けられているすべてのキーを破棄します。これにより、ストレージ システムからディスク暗号化キーにアクセスできなくなります。	KMIPサーバまたはストレージ システムに給電されていない

関連情報

- "ストレージ暗号化ディスク破壊"
- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスク完全消去"

ONTAPで認証キーが失われた場合にFIPSドライブまたはSEDをサービスに戻す

FIPSドライブまたはSEDの認証キーが永久に失われ、KMIPサーバから取得できない場合、FIPSドライブまたはSEDは破損しているとみなされます。ディスクのデータにアクセスしたりリカバリしたりすることはできませんが、SEDの未使用スペースをデータに再び使用できるようにすることができます。

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。

タスク概要

このプロセスは、FIPSドライブまたはSEDの認証キーが永久に失われてリカバリできないことが確実である場合にのみ使用してください。

ディスクがパーティショニングされている場合は、このプロセスを開始する前にパーティショニングを解除する必要があります。

> ディスクのパーティションを解除するコマンドは、diagレベルでのみ使用可能であり、NetAppサポートの監督下でのみ実行する必要があります。続行する前に**NetApp**サポートに連絡することを強くお勧めします。"NetAppナレッジベース：ONTAPでスペアドライブのパーティション化を解除する方法"を参照することもできます。

手順

1. FIPSドライブまたはSEDを使用可能な状態に戻します。

SEDS が…	次の手順を使用します…

FIPS準拠モードでない、またはFIPS準拠モードでFIPSキーを使用できる	a. 権限レベルをadvancedに設定します：
	`set -privilege advanced`
	b. FIPS キーをデフォルトの製造元セキュア ID 0x0 にリセットします：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 操作が成功したことを確認します：
	`storage encryption disk show-status`操作が失敗した場合は、このトピックの PSID プロセスを使用します。
	d. 壊れたディスクをサニタイズする：
	`storage encryption disk sanitize -disk disk_id`次の手順に進む前に、コマンド `storage encryption disk show-status`で操作が成功したことを確認します。
	e. サニタイズされたディスクをアンフェイルします：
	`storage disk unfail -spare true -disk disk_id`
	f. ディスクに所有者がいるかどうかを確認します：
	`storage disk show -disk disk_id`ディスクに所有者がいない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk disk_id`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node node_name`
	`disk sanitize release`コマンドを実行します。
	g. ノードシェルを終了します。ディスクの障害を再度解除します：
	`storage disk unfail -spare true -disk disk_id`
	h. ディスクがスペアになり、アグリゲート内で再利用できる状態になっていることを確認します：
	`storage disk show -disk disk_id`

FIPS準拠モードであるがFIPSキーは使用できず、SEDのPSIDがラベルに印刷されている	a. ディスクのPSIDをディスク ラベルで確認します。
	b. 権限レベルをadvancedに設定します：
	`set -privilege advanced`
	c. ディスクを工場出荷時の設定にリセットします：
	`storage encryption disk revert-to-original-state -disk *disk_id* -psid *disk_physical_secure_id*`次の手順に進む前に、コマンド`storage encryption disk show-status`で操作が成功したことを確認します。
	d. ONTAP 9.8P5以前を実行している場合は、次の手順に進んでください。ONTAP 9.8P6以降を実行している場合は、サニタイズされたディスクの障害を解除してください。
	`storage disk unfail -disk *disk_id*`
	e. ディスクに所有者がいるかどうかを確認します：
	`storage disk show -disk *disk_id*`ディスクに所有者がいない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk *disk_id*`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node *node_name*`
	`disk sanitize release`コマンドを実行します。
	f. ノードシェルを終了します。ディスクの障害を再度解除します：
	`storage disk unfail -spare true -disk *disk_id*`
	g. ディスクがスペアになり、アグリゲート内で再利用できる状態になっていることを確認します：
	`storage disk show -disk *disk_id*`

関連情報

- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスクの元の状態へのリバート"
- "ストレージ暗号化ディスク完全消去"
- "storage encryption disk show-status"

ONTAP で FIPS ドライブまたは SED を非保護モードに戻す

FIPSドライブまたはSEDは、ノードの認証キー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。`storage encryption disk modify`コマンドを使用してキーIDをデフォルトに設定することで、FIPSドライブまたはSEDを非保護モードに戻すことができます。非保護モードのFIPSドライブまたはSEDはデフォルトの暗号化キーを使用し、保護モードのFIPSドライブまたはSEDは提供された秘密の暗号化キーを使用します。ドライブ上に暗号化されたデータが存在する場合、ドライブを非保

護モードにリセットしても、データは暗号化されたままであり、漏洩することはありません。

> FIPSドライブまたはSEDが非保護モードに戻った後、暗号化されたデータにアクセスできないようにするには、以下の手順に従ってください。FIPSとデータキーIDがリセットされると、元のキーを復元しない限り、既存のデータは復号化できなくなり、アクセスできなくなります。

HAペアでSASドライブまたはNVMeドライブ（SED、NSE、FIPS）の暗号化を使用している場合は、システムを初期化（ブート オプション4または9）する前に、HAペア内のすべてのドライブに対してこのプロセスを実行しておく必要があります。この手順を実行しないと、将来ドライブを転用した場合にデータが失われる可能性があります。

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. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   `security key-manager query`コマンドを使用してキー ID を表示できます。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

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

   次のコマンドを使用して、処理が成功したことを確認します。

   ```
   storage encryption disk show-status
   ```

   「Disks Begun」と「Disks Done」の数字が同じになるまで、show-statusコマンドを繰り返します。

```
cluster1:: storage encryption disk show-status

            FIPS    Latest   Start               Execution   Disks
Disks Disks
Node        Support Request  Timestamp           Time (sec)  Begun
Done  Successful
-------     ------- -------- ------------------  ---------- ------
------  ----------
cluster1    true    modify   1/18/2022 15:29:38    3           14     5
5
1 entry was displayed.
```

3. ノードのデータ認証キーIDをデフォルトのMSIDである0x0に戻します。

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   SAS ドライブまたは NVMe ドライブを非保護モードに戻す場合は、 `-data-key-id`の値を 0x0 に設定する必要があります。

   `security key-manager query`コマンドを使用してキー ID を表示できます。

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

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

   次のコマンドを使用して、処理が成功したことを確認します。

   `storage encryption disk show-status`

   数値が同じになるまで、show-statusコマンドを繰り返します。「disks begun」と「disks done」の数値が同じになったら、操作は完了です。

メンテナンスモード

ONTAP 9.7以降では、FIPSドライブのキー変更をメンテナンス モードから行うことができます。メンテナンス モードは、前のセクションに記載したONTAP CLIの手順を実行できない場合にのみ使用してください。

手順

1. ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   `disk encrypt rekey_fips 0x0 disklist`

2. ノードのデータ認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   disk encrypt rekey 0x0 disklist
   ```

3. FIPS認証キーが正常に変更されたことを確認します。

   ```
   disk encrypt show_fips
   ```

4. 次のコマンドを使用して、データ認証キーが正常に変更されたことを確認します。

   ```
   disk encrypt show
   ```

   出力には、デフォルトのMSID 0x0キーID、またはキーサーバーが保持する64文字の値が表示される可能性があります。 `Locked?`フィールドはデータロックを示します。

```
Disk       FIPS Key ID                  Locked?
---------- ---------------------------- -------
0a.01.0    0x0                           Yes
```

関連情報

- "ストレージ暗号化ディスクの変更"
- "storage encryption disk show-status"

ONTAPで外部キーマネージャ接続を削除する

KMIPサーバが不要になったときはノードから切断できます。たとえば、ボリューム暗号化に移行する場合はKMIPサーバを切断できます。

タスク概要

HAペアのいずれかのノードからKMIPサーバを切断すると、自動的にすべてのクラスタ ノードからサーバが切断されます。

KMIPサーバを切断したあとも外部キー管理を引き続き使用する場合は、別のKMIPサーバから認証キーを提供できることを確認してください。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。

手順

1. 現在のノードからKMIPサーバを切断します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external remove-servers -vserver SVM -key-servers host_name

IP_address:port,…`	ONTAP 9.5以前

MetroCluster環境では、これらのコマンドを管理SVMの両方のクラスタで実行する必要があります。

次のONTAP 9.6コマンドは、 `cluster1`の2つの外部キー管理サーバへの接続を無効にします。最初のサーバは `ks1`という名前で、デフォルトポート5696でリッスンしており、2番目のサーバはIPアドレス10.0.0.20で、ポート24482でリッスンしています：

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

`security key-manager external remove-servers`および `security key-manager delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+key-manager["ONTAPコマンド リファレンス "^]をご覧ください。

ONTAP外部キー管理サーバーのプロパティを変更する

ONTAP 9.6 以降では、 `security key-manager external modify-server`コマンドを使用して外部キー管理サーバの I/O タイムアウトとユーザ名を変更できます。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。
- MetroCluster環境では、この手順を管理SVMの両方のクラスタで実行する必要があります。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスタの外部キー管理サーバのプロパティを変更します。

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   タイムアウト値は秒単位で指定します。ユーザー名を変更すると、新しいパスワードの入力を求められます。クラスタログインプロンプトでコマンドを実行すると、 `*admin_SVM*`デフォルトで現在のクラスタの管理SVMが使用されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者である必要があります。

次のコマンドは、デフォルトポート5696でリッスンしている `cluster1`外部キー管理サーバーのタイムアウト値を45秒に変更します：

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. SVMの外部キー管理サーバのプロパティを変更します（NVEのみ）。

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > タイムアウト値は秒単位で指定します。ユーザー名を変更すると、新しいパスワードの入力を求められます。SVMログインプロンプトでコマンドを実行すると、 `*SVM*`デフォルトで現在のSVMに設定されます。外部キーマネージャサーバのプロパティを変更するには、クラスタまたはSVM管理者である必要があります。

   次のコマンドは、デフォルトポート5696でリッスンしている `svm1`外部キー管理サーバーのユーザー名とパスワードを変更します：

   ```
   svm1::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. 最後の手順をその他のSVMに対して繰り返します。

関連情報

- "セキュリティキー・マネージャ外部サーバー修正"

ONTAPでのオンボードキー管理から外部キー管理への移行

オンボード キー管理から外部キー管理に切り替える場合は、外部キー管理を有効にする前にオンボード キー管理の設定を削除する必要があります。

開始する前に

- ハードウェアベースの暗号化の場合は、すべてのFIPSドライブまたはSEDのデータ キーをデフォルト値にリセットする必要があります。

  "FIPSドライブまたはSEDを非保護モードに戻す"

- ソフトウェアベースの暗号化では、すべてのボリュームの暗号化を解除する必要があります。

  "ボリューム データの暗号化の解除"

- 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. クラスタのオンボード キー管理の設定を削除します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5以前	`security key-manager delete-key-database`

`security key-manager onboard disable`および `security key-manager delete-key-database`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+key-manager["ONTAPコマンドリファレンス"^]を参照してください。

外部キー管理からONTAPオンボードキー管理に切り替える

オンボードキー管理に切り替えるには、オンボードキー管理を有効にする前に、外部キー管理構成を削除します。

開始する前に

- ハードウェアベースの暗号化の場合は、すべてのFIPSドライブまたはSEDのデータ キーをデフォルト値にリセットする必要があります。

  "FIPSドライブまたはSEDを非保護モードに戻す"

- すべての外部キー管理ツールの接続を削除しておく必要があります。

  "外部キー管理ツールの接続の削除"

- 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

キー管理を移行する手順は、使用しているONTAPのバージョンによって異なります。

ONTAP 9.6以降

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを使用します。

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   MetroCluster環境では、このコマンドを管理SVMの両方のクラスタで実行する必要があります。

`security key-manager external disable`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-disable.html["ONTAPコマンドリファレンス"^]を参照してください。

ONTAP 9.5以前

次のコマンドを使用します：
`security key-manager delete-kmip-config`

`security key-manager delete-kmip-config`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli-9161/security-key-manager-delete-kmip-config.html["ONTAPコマンドリファレンス"^]をご覧ください。

関連情報

- "セキュリティキー・マネージャ外部無効化"

ONTAPブートプロセス中にキー管理サーバにアクセスできない場合の動作

ONTAP は、NSE 用に設定されたストレージ システムがブート プロセス中に指定されたキー管理サーバのいずれにもアクセスできない場合に、望ましくない動作を回避するために特定の予防措置を講じます。

ストレージシステムがNSE用に設定され、SEDのキーが再設定されてロックされ、SEDの電源がオンになっている場合、ストレージシステムは、データにアクセスする前に、キー管理サーバーから必要な認証キーを取得して、SEDに対して認証を行う必要があります。

ストレージシステムは、指定されたキー管理サーバへの接続を最大3時間試行します。その時間が経過してもいずれのサーバにも接続できない場合、ブートプロセスは停止し、ストレージシステムは停止します。

ストレージシステムが指定されたキー管理サーバへの接続に成功した場合、最大15分間SSL接続の確立を試行します。ストレージシステムが指定されたキー管理サーバとのSSL接続を確立できない場合、ブートプロセスは停止し、ストレージシステムは停止します。

ストレージシステムがキー管理サーバへの接続を試行している間、失敗した接続試行に関する詳細情報がCLIに表示されます。Ctrl+Cキーを押すことで、いつでも接続試行を中断できます。

セキュリティ対策として、SEDへの無許可のアクセス試行回数には上限があり、試行回数が上限に達すると既存データへのアクセスは無効になります。指定されたどのキー管理サーバにもアクセスできず、適切な認証キーを取得できない場合、ストレージ システムはデフォルト キーでの認証のみ試行できますが、その場合、認証が失敗してパニック状態になります。パニック状態になった場合に自動的にリブートするように構成されている場合、ストレージ システムはブート ループに入り、SEDでの認証は繰り返し失敗します。

このようなシナリオでストレージ システムが停止するのは、ストレージ システムがブート ループに入ることを回避し、上限を超えて連続して認証に失敗したためにSEDが永続的にロックされて意図しないデータ損失が発生することを回避するための設計です。ロックアウト保護の上限とタイプは、SEDの仕様とタイプによって異なります。

SEDタイプ	ロックアウトにつながる認証の連続失敗回数	安全限界に達したときのロックアウト保護タイプ
HDD	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。
X440_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョン NA00 または NA01）	5	一時的。ロックアウトはディスクの電源を入れ直すまでのみ有効です。
X577_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョン NA00 または NA01）	5	一時的。ロックアウトはディスクの電源を入れ直すまでのみ有効です。
X440_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョンが高いもの）	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。
X577_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョンが高いもの）	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。
その他すべてのSSDモデル	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。

すべての SED タイプでは、認証が成功すると試行回数がゼロにリセットされます。

指定されたキー管理サーバーに到達できないためにストレージ システムが停止するというシナリオに遭遇した場合は、ストレージ システムの起動を続行する前に、まず通信障害の原因を特定して修正する必要があります。

ONTAPの暗号化をデフォルトで無効にする

ONTAP 9.7以降では、Volume Encryption（VE）ライセンスがあり、オンボード / 外部キー マネージャを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。必要に応じて、クラスタ全体に対してデフォルトで暗号化が無効になるようにすることができます。

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か、クラスタ管理者から権限を委譲されたSVM管理者である必要があります。

手順

1. ONTAP 9.7以降でクラスタ全体に対して暗号化をデフォルトで無効にするには、次のコマンドを実行します。

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```