NetApp暗号化の管理

ONTAP 9

NetApp
December 20, 2024

目次

NetApp暗号化の管理

ボリュームデータの暗号化解除

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

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

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`

   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。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに `aggr3`移動し `vol1`、ボリュームのデータの暗号化を解除します。

   ```
   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`

   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。

   次のコマンドは、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`。

   ```
   cluster1::> volume show -encryption

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

暗号化されたボリュームを移動する

コマンドを使用すると、暗号化されたボリュームを移動できます `volume move start`。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

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。

のオプション `volume move start`は `-encrypt-destination`、暗号化されたボリュームに対してはデフォルトでtrueになります。デスティネーションボリュームを暗号化しないように指定すると、ボリューム上のデータの暗号化が誤って解除されることがなくなります。

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

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`*

   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。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに `aggr3`移動し `vol1`、ボリュームのデータを暗号化したままにします。

   ```
   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`

   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。

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

volume moveコマンドの実行権限を委譲する

コマンドを使用して、既存のボリュームの暗号化、暗号化されたボリュームの移動、またはボリュームの暗号化解除を行うことができます `volume move`。クラスタ管理者は、コマンドを自分で実行することも、コマンドの実行権限をSVM管理者に委譲することもできます `volume move`。

タスクの内容

デフォルトでは、SVM管理者にはロールが割り当て `vsadmin`られます。このロールには、ボリュームを移動する権限は含まれていません。SVM管理者がコマンドを実行できるようにするには、ロールをSVM管理者に `volume move`割り当てる必要があります `vsadmin-volume`。

ステップ

1. コマンドの実行権限を委譲し `volume move`ます。

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role vsadmin-
   volume
   ```

   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。

   次のコマンドは、SVM管理者にコマンドの実行権限を付与し `volume move`ます。

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   SVM-admin -application ssh -authmethod domain -role vsadmin-volume
   ```

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

セキュリティ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が重要です。ONTAP 9 .3以降では、コマンドを使用して暗号化キーを変更できます `volume encryption rekey start`。

タスクの内容

キー変更処理を開始したら、最後まで完了する必要があります。古いキーに戻ることはできません。処理中にパフォーマンスの問題が発生した場合は、コマンドを実行して処理を一時停止し、 `volume encryption rekey resume`コマンドを実行して処理を再開できます `volume encryption rekey pause`。

キー変更処理が完了するまで、ボリュームには 2 つのキーが存在することになります。新しい書き込みとそれに対応する読み取りでは、新しいキーが使用されます。それ以外の読み取りでは、古いキーが使用されます。

SnapLockボリュームのキー変更にはを使用できません `volume encryption rekey start`。

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ののvs1暗号化キーを変更し `vol1`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`

   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。

   次のコマンドは、キー変更処理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`

   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。

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

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する

セキュリティ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が重要です。暗号化キーは、コマンドを使用して変更できます `volume move start`。ONTAP 9 .2以前ではを使用する必要があります `volume move start`。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいま

せん。

タスクの内容

SnapLockボリュームまたはFlexGroupボリュームのキーの変更にはを使用できません `volume move start`。

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

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`

   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。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに **aggr2**`移動し`**vol1**、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`

   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。

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

NetAppストレージ暗号化の認証キーのローテーション

NetAppストレージ暗号化（NSE）を使用する場合、認証キーをローテーションできます。

タスクの内容

外部キーマネージャ（KMIP）を使用している場合は、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ていません。

手順

1. コマンドを使用し `security key-manager create-key`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する必要があります。

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

暗号化されたボリュームを削除する

コマンドを使用すると、暗号化されたボリュームを削除できます `volume delete`。

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume move コマンドの実行権限を委譲する"。
- ボリュームはオフラインである必要があります。

ステップ

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`*

   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。

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

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

   削除の確認を求められたら、と入力し `yes`ます。

   ボリュームの暗号化キーは24時間後に削除されます。

   オプションとともに `-force true`使用して、 `volume delete`ボリュームを削除し、対応する暗号化キーをただちに破棄します。このコマンドには高度なPrivilegesが必要です。詳細については、のマニュアルページを参照してください。

終了後

コマンドの実行後、コマンドを使用して、削除したボリュームを保持期間内にリカバリ `volume delete`できます `volume recovery-queue`。

`volume recovery-queue SVM_name -volume volume_name`

"ボリュームリカバリ機能の使用方法"

暗号化されたボリューム上のデータのセキュアパージ

暗号化されたボリューム上のデータのセキュアパージの概要

ONTAP 9 4以降では、セキュアパージを使用して、NVE対応ボリュームのデータを無停止でスクラビングできます。暗号化されたボリュームのデータをスクラビングすることで、「柱」、「ブロックが上書きされたときにデータトレースが残されている」などの物理メディアからデータをリカバリすることができなくなります。また、解約するテナントのデータを安全に削除することもできます。

セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。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で作成したボリュームでは、セキュアパージはサポートされません。
- セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。
- 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でサポートされています。
- パージするボリュームがSnapMirror関係のソースである場合は、SnapMirror関係を解除してセキュアパージを実行する必要はありません。
- 再暗号化の方法は、SnapMirrorデータ保護を使用するボリュームとSnapMirrorデータ保護（DP）を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再暗号化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 XDP（拡張データ保護）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値は、コマンドを使用して変更でき `secure purge re-encryption-method [volume-move|in-place-rekey]`ます。
- デフォルトでは、セキュアパージ処理の実行中に、FlexVolボリューム内のすべてのSnapshotコピーが自動的に削除されます。デフォルトでは、FlexGroupおよびSnapMirrorデータ保護を使用するボリューム内のSnapshotは、セキュアパージ処理で自動的に削除されません。これらのデフォルト値は、コマンドを使用して変更でき `secure purge delete-all-snapshots [true|false]`ます。

ONTAP 9 .7以前：

- セキュアパージでは、次の項目は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は、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Snapshotコピーがある場合は、ボリュームをパージする前にSnapshotコピーを解放する必要があります。たとえば、FlexCloneボリュームを親からスプリットする必要がある場合があります。

- 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、パージされていない残りのデータが新しいキーで再暗号化されます。

  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。古いキーは自動的に破棄されるため、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ません。

SnapMirror関係のない暗号化されたボリューム上のデータのセキュアパージ

ONTAP 9.4 以降では、 NVE 対応ボリューム上で、システムを停止することなく「 crub 」データにセキュアパージを使用できます。

タスクの内容

削除されたファイル内のデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、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。
- このタスクには高度なPrivileges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上vs1で削除したファイルのセキュアパージを実行し `vol1`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非同期関係にある暗号化されたボリューム上のデータのセキュアパージ

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対応ボリュームで無停止でデータを「スクラビング」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。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

削除されたファイル内のデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、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をセキュアパージする準備をします。

   ```
   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コピーに含まれている場合は、Snapshotコピーを削除します。

   ```
   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コピーに含まれている場合は、次の手順を実行します。

   a. SnapMirror非同期関係のデスティネーションボリュームにSnapshotコピーを作成します。

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

   b. SnapMirrorを更新してベースのSnapshotコピーを転送します。

      ```
      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コピーの数に1を足した数だけ繰り返します。

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

   b. ベースのSnapshotコピーが存在することを確認します。+ `snapshot show -vserver SVM_name`

`-volume volume_name`

c. ベースのSnapshotコピーを削除します。+ `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 」にある削除済みファイルを安全にパージします。

   ```
   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`

SnapMirror同期関係にある暗号化されたボリュームのデータをスクラビングする

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。

タスクの内容

セキュアパージは、削除されたファイル内のデータ量によっては、完了までに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、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。
- このタスクには高度なPrivileges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をセキュアパージする準備をします。

   ```
   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コピーに含まれている場合は、Snapshotコピーを削除します。

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

5. ベースのSnapshotコピーまたは共通のSnapshotコピーにセキュアパージファイルが含まれている場合は、SnapMirrorを更新して共通のSnapshotコピーを転送します。

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

   共通のSnapshotコピーは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と整合性のあるSnapshotコピーに含まれている場合は、SnapMirror同期関係の両方のボリュームでSnapshotコピーを削除します。

   ```
   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パージします

   ```
   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
   ```

オンボードキー管理のパスフレーズの変更

セキュリティのベストプラクティスとして、オンボードキー管理のパスフレーズを定期的に変更することが推奨されます。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オンボードキー管理の新しいパスフレーズをコピーしておく必要があ

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管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。

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のパスフレーズを変更します。

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

   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ONTAP 9 .6コマンドでは、のオンボードキー管理のパスフレーズを変更でき `cluster1`ます。

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. オンボードキー管理のパスフレーズを変更するかどうかを確認するプロンプトでと入力し `y`ます。
4. 現在のパスフレーズのプロンプトで現在のパスフレーズを入力します。
5. 新しい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。

6. 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。

終了後

MetroCluster環境では、パートナークラスタでパスフレーズを更新する必要があります。

- ONTAP 9 .5以前では、パートナークラスタで同じパスフレーズを使用してを実行する必要があります `security key-manager update-passphrase`。
- ONTAP 9 .6以降では、パートナークラスタで同じパスフレーズを使用してを実行するように求められます

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

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オンボードキー管理のパスフレーズをコピーしておく必要があります。

オンボードキー管理のパスフレーズを変更するときは、キー管理情報を手動でバックアップする必要があります。

"オンボードキー管理情報の手動バックアップ"

オンボードキー管理情報の手動でのバックアップ

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、ストレージシステムの外部の安全な場所にオンボードキー管理の情報をコピーしておく必要があります。

必要なもの

- 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。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

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、キー管理情報を手動でもバックアップしておく必要があります。

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`

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

+

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. 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バックアップ情報をコピーします。

オンボードキー管理暗号化キーのリストア

オンボードキー管理の暗号化キーをリストアする手順は、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。詳細については、を参照してください。 "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。

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、の手順を実行します [ontap-9-8]。

1. キーをリストアする必要があることを確認します。+ `security key-manager key query -node node`
2. キーをリストアします。+ `security key-manager onboard sync`

   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ONTAP 9 .6コマンドは、オンボードキー階層のキーを同期します。

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

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

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。

ルートボリュームを暗号化したONTAP 9.8以降

ONTAP 9 .8以降を実行しており、ルートボリュームが暗号化されている場合は、ブートメニューで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。このプロセスは、ブートメディアを交換する場合にも必要です。

1. ノードをブートメニューでブートし、オプションを選択します `(10) Set onboard key management recovery secrets`。
2. と入力して、 `y`このオプションを使用します。
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。

   ノードが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を選択します `(1) Normal Boot`。

ONTAP 9.5以前

1. キーをリストアする必要があることを確認します。+ `security key-manager key show`
2. 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 .6または9.7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、この手順をスキップします。

3. キーをリストアします。+ `security key-manager setup -node node`

   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。

4. 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。

外部キー管理の暗号化キーのリストア

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。

タスクの内容

ONTAP 9 .6以降では、コマンドを使用してキーのリストアが必要かどうかを確認できます `security key-manager key query -node node_name`。

ONTAP 9 .5以前では、コマンドを使用してキーのリストアが必要かどうかを確認できます `security key-manager key show`。

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。

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、この手順を省略します。

   a. bootarg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でブートし、オプションを選択します `(11) Configure node for external key management`。

   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を選択します `(1) Normal Boot`。

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`デフォルトはすべてのノードです。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。このコマンドは、オンボードキー管理が有効になっている場合はサポートされません。

次のONTAP 9 .6コマンドは、外部キー管理の認証キーをのすべてのノードにリストアします `cluster1`。

```
cluster1::> security key-manager external restore
```

SSL証明書の交換

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

- クラスタの交換用のパブリック証明書と秘密鍵（KMIPクライアント証明書）を入手しておく必要があります。
- KMIPサーバの交換用のパブリック証明書（KMIP server-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実行できます。

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以降を実行していて、管理SVMのキー管理ツールの設定を変更する場合は、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した鍵と異なる場合、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するとエラーが返されます。このエラーを無効にする方法については、ナレッジベースの記事を参照してください"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"。

FIPSドライブまたはSEDの交換

FIPSドライブまたは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ペアでを使用している場合は"SAS ドライブまたは NVMe ドライブの暗号化（ SED 、 NSE 、 FIPS ）"、システムを初期化する前に、HAペア内のすべてのドライブに対応するトピックの手順に従う必要があります"FIPSドライブまたはSEDを非保護モードに戻す"（ブートオプション4または9）。これを行わないと、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

- 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してマークされていることを確認します。

   ```
   storage disk show -broken
   ```

   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 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手順に従って、障害ディスクを取り外し、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`

   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 disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. 新しいディスク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
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.0  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   1.10.1  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   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"

FIPSドライブまたはSEDのデータにアクセスできないようにする

FIPSドライブまたはSEDのデータにアクセスできない概要

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

用スペースを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 0x0（SASドライブ）またはnullキー（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。完全消去したディスクは、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。

FIPSドライブまたはSEDの完全消去

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、そのドライブを新しいデータに使用する場合は、コマンドを使用してドライブを完全消去できます `storage encryption disk sanitize`。

タスクの内容

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 0x0（SASドライブ）またはnullキー（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。完全消去したディスクは、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. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
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`*

   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 aggregate delete -aggregate aggr1
   ```

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
```

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
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

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
```

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

```
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
```

このコマンドを使用して完全消去できるのは、ホットスペアディスクまたは破損ディスクのみです。タイプに関係なくすべてのディスクを完全消去するには、オプションを使用し `-force-all-state`ます。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。

続行する前に、確認フレーズの入力を求めるプロンプトがONTAPに表示されます。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. 完全消去したディスクの障害状態を解除します。 `storage disk unfail -spare true -disk disk_id`
7. ディスクに所有者があ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`

   コマンドを実行します `disk sanitize release`。
9. ノードシェルを終了します。ディスクの障害状態を再度解除します。 `storage disk unfail -spare true -disk disk_id`
10. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。 `storage disk show -disk disk_id`

FIPSドライブまたはSEDの破棄

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、ドライブを再利用する必要もない場合は、コマンドを使用してディスクを破棄できます `storage encryption disk destroy`。

タスクの内容

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、ドライブが完全にロックされます。これにより、ディスクが実質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。ただし、ディスクのラベルに印刷されているPhysical Secure ID（PSID；物理的なセキュアID）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、を参照してください "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"。

> 障害ディスク返却不要サービス（NRD Plus）を利用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. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 破棄する 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`

   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 aggregate delete -aggregate aggr1
   ```

3. 破棄する 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`

   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
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. ディスクを破棄します。

   `storage encryption disk destroy -disk disk_id`

   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。

   > 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.
```

FIPSドライブまたはSEDの緊急時のシュレッドデータ

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へのアクセスを即座に禁止できます。

開始する前に

- 使用可能な電力が供給されていないKMIPサーバを使用している場合は、破棄しやすい認証アイテム（スマートカードやUSBドライブなど）を使用してKMIPサーバを設定する必要があります。
- 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。

ステップ

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。

状況	そしたら…。

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正常に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ペアとして構成されている場合は、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. 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。 ◦ ディスクのデータにアクセスできない状態にしてディスクを再利用する場合は、ディスクを完全消去します。+ `disk encrypt sanitize -all` ◦ ディスクのデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、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状態にし、ディスクを再利用する場合は、ディスクを完全消去します。 *
b. ストレージシステムがHAペアとして構成されている場合は、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. ディスクを完全消去します。
`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状態にし、ディスクを保存する必要もない場合は、ディスクを破棄してください： *
	b. ストレージシステムがHAペアとして構成されている場合は、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. ディスクを破棄します。
	`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、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

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。

認証キーが失われた場合に**ONTAP**を使用して**FIPS**ドライブまたは**SED**を使用可能な状態に戻す

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。ディスク上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。

タスクの内容

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ニングを解除するコマンドはdiagレベルでのみ使用でき、NetAppサポートから指示があった場合にのみ実行してください。続行する前に、ネットアップサポートにお問い合わせください。ナレッジベースの記事も参照できます"ONTAP でスペアドライブのパーティショニングを解除する方法"。

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。

SED の状況	実行する手順

FIPS準拠モードではない、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メーカーセキュアIDである0x0にリセットします。
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 処理が成功したことを確認します。
	`storage encryption disk show-status`処理に失敗した場合は、このトピックのPSIDプロセスを使用してください。
	d. 破損ディスクを完全消去します。次の手順に進む前に、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`。
	`storage encryption disk sanitize -disk disk_id`
	e. 完全消去したディスクの障害状態を解除します。
	`storage disk unfail -spare true -disk disk_id`
	f. ディスクに所有者があ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`
	コマンドを実行します `disk sanitize release`。
	g. ノードシェルを終了します。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk disk_id`
	h. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk disk_id`

FIPS準拠モードでFIPSキーを使用できず、SEDのPSIDがラベルに印刷されている	a. ディスクラベルからディスクのPSIDを確認します。
	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。次の手順に進む前に、コマンドを使用して処理が成功したことを確認し `storage encryption disk show-status`ます。
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`
	d. ONTAP 9.8P5以前を実行している場合は、次の手順に進みます。ONTAP 9 .8P6以降を実行している場合は、完全消去したディスクの障害状態を解除します。
	`storage disk unfail -disk disk_id`
	e. ディスクに所有者があ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`
	コマンドを実行します `disk sanitize release`。
	f. ノードシェルを終了します。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk disk_id`
	g. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk disk_id`

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

FIPSドライブまたはSEDを非保護モードに戻します。

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。FIPSドライブまたはSEDを非保護モードに戻すには、コマンドを使用して `storage encryption disk modify`キーIDをデフォルトに設定します。

HAペアで暗号化SASドライブまたはNVMeドライブ（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、HAペア内のすべてのドライブでこのプロセスを実行する必要があります（ブートオプション4または9）。これを行わないと、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
   ```

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

   ```
   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.
   ```

   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 Begin」と「Disks Done」の数値が同じになるまで、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ドライブとNVMeドライブのどちらを非保護モードに戻すかに関係なく、の値は `-data-key-id`0x0に設定する必要があります。

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

```
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.
```

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
```

番号が同じになるまで、show-statusコマンドを繰り返します。処理が完了するのは、「ディスクの開始」と「ディスクの終了」の番号が同じ場合です。

メンテナンスモオト

ONTAP 9 .7以降では、保守モードからFIPSドライブのキーを変更できます。保守モードは、前述のONTAP CLIの手順を使用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認証キーのキーが正常に変更されたことを確認します。

   ```
   disk encrypt show_fips
   ```

4. データ認証キーのキーが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参照します。

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

外部キー管理ツールの接続を削除する

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

化に移行するときにKMIPサーバを切断できます。

タスクの内容

HAペアの一方のノードからKMIPサーバを切断すると、すべてのクラスタノードから自動的に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サーバで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管理者である必要があります。

ステップ

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環境の場合は、管理SVMの両方のクラスタでこれらのコマンドを繰り返す必要があります。

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ONTAP 9 .6コマンドは、2つの外部キー管理サーバへの接続を無効にします。1つ目はデフォルトポート5696をリスンするという名前のサーバ、 `ks1`もう1つはポート24482をリスンするIPアドレス10.0.0.20のサーバ `cluster1`です。

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

外部キー管理サーバのプロパティを変更します。

ONTAP 9 .6以降では、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 `security key-manager external modify-server`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管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。
- MetroCluster環境の場合は、管理SVMの両方のクラスタで上記の手順を繰り返す必要があります。

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表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。このコマンドをクラスタのログインプロンプトで実行すると、が`*admin_SVM*`デフォルトで現在のクラスタの管理SVMに設定されます。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をリスンしている外部キー管理サーバのタイムアウト値を45秒に変更します `cluster1`。

```
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表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。このコマンドをSVMのログインプロンプトで実行すると、が`*SVM*`デフォルトで現在のSVMに設定されます。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をリスンする外部キー管理サーバのユーザ名とパスワードを変更し`svm1`ます。

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

4. SVMを追加する場合は、最後の手順を繰り返します。

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。

ステップ

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`

コマンド構文全体については、を参照してください "ONTAPコマンド リファレンス"。

外部キー管理からオンボードキー管理への移行

外部キー管理からオンボードキー管理に切り替える場合は、オンボードキー管理を有効にする前に外部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"

- 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

キー管理の移行手順は、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環境の場合は、管理SVMに対して両方のクラスタでこのコマンドを繰り返す必要があります。

ONTAP 9.5以前

次のコマンドを使用します。

```
security key-manager delete-kmip-config
```

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

ブートプロセス時に NSE 用に構成されたストレージシステムが指定されたどのキー管理サーバにもアクセスできない場合、 ONTAP ではストレージシステムの望ましくない動作を回避するために、特定の予防措置を取ります。

ストレージシステムが NSE 用に設定されている場合、 SED のキーが変更されてロックされ、 SED の電源がオンになっているときは、ストレージシステムは、キー管理サーバから必要な認証キーを取得して SED に対して自身を認証し、データにアクセスできるようにする必要があります。

ストレージシステムは、指定されたキー管理サーバへのアクセスを最大 3 時間試行します。その時間が経過してもストレージシステムがどのキー管理サーバにもアクセスできない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムは、指定されたいずれかのキー管理サーバに正常にアクセスできた場合、SSL接続の確立を最大15分間試行します。ストレージシステムが指定されたどのキー管理サーバとも SSL 接続を確立できない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムがキー管理サーバへのアクセスと接続を試行している間、失敗したアクセス試行に関する詳細情報がCLIに表示されます。アクセスの試行は、 Ctrl+C キーを押すことによっていつでも中断できます

セキュリティ対策として、SEDでは許可される不正アクセスの試行回数が制限され、試行回数が制限されたあとは既存データへのアクセスが無効になります。ストレージシステムが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、デフォルトのキーでの認証しか試行できないため、試行が失敗してパニック状態になります。パニック状態が発生した場合に自動的にリブートするように設定されているストレージシステムはブートループに入り、SEDでの認証が連続して失敗します。

設計上、このような状況でストレージシステムを停止するのは、認証の連続失敗回数の上限を超えたためにSEDが永続的にロックされた場合に、ストレージシステムがブートループに入ったり、意図しないデータ損失が発生したりするのを防ぐためです。ロックアウト保護の制限とタイプは、SEDの製造仕様とタイプによって異なります。

SEDタイプ	ロックアウトされるまでの認証の連続失敗回数	安全制限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使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンがNA00またはNA01のX440_PHM2800MCTO 800GB NSE SSD	5	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンがNA00またはNA01のX577_PHM2800MCTO 800GB NSE SSD	5	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンが上位のX440_PHM2800MCTO 800GB NSE SSD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンが上位のX577_PHM2800MCTO 800GB NSE SSD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
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使用可能になった場合でも、データをリカバリできません。

すべての SED タイプでは、認証が成功すると試行回数が 0 にリセットされます。

ストレージシステムが指定されたどのキー管理サーバにもアクセスできないために停止した場合は、引き続きストレージシステムのブートを試行する前に、通信エラーの原因を特定して修正しておく必要があります。

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、オンボードまたは外部のキー管理ツール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、暗号化をデフォルトでクラスタ全体で無効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。

ステップ

1. ONTAP 9 .7以降でクラスタ全体の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
```

著作権に関する情報

商標に関する情報