管理NetApp加密

ONTAP 9

NetApp
February 12, 2026

目錄

管理NetApp加密

取消 ONTAP 中的 Volume 資料加密

您可以使用 `volume move start` 用於移動和取消加密 Volume 資料的命令。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有的加密磁碟區、並取消加密磁碟區上的資料：

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

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume `vol1` 至目的地 Aggregate `aggr3` 並取消加密磁碟區上的資料：

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

   系統會刪除磁碟區的加密金鑰。磁碟區上的資料未加密。

2. 確認磁碟區已停用加密：

   `volume show -encryption`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示磁碟區是否開啟 `cluster1` 已加密：

   ```
   cluster1::> volume show -encryption

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

在 ONTAP 中移動加密磁碟區

您可以使用 `volume move start` 用於移動加密磁碟區的命令。移動的磁碟區可以位於相同的集合體或不同的集合體上。

關於這項工作

如果目的地節點或目的地Volume不支援Volume加密、則移動將會失敗。

。 `-encrypt-destination` 的選項 `volume move start` 加密磁碟區的預設值為 true 。指定您不希望目的地 Volume 加密的要求、可確保您不會不小心將磁碟區上的資料解密。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有的加密磁碟區、並將磁碟區上的資料保持加密狀態：

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

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume `vol1` 至目的地 Aggregate `aggr3` 並將磁碟區上的資料加密：

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

2. 確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster1`：

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

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

使用 ONTAP 中的 Volume Encryption rekey start 命令變更磁碟區的加密金鑰

定期變更磁碟區的加密金鑰是安全性最佳做法。從功能介紹9.3開始ONTAP 、您可以使用 `volume encryption rekey start` 變更加密金鑰的命令。

關於這項工作

重新輸入作業一旦開始、就必須完成。不會返回舊金鑰。如果您在作業期間遇到效能問題、可以執行 `volume encryption rekey pause` 暫停作業的命令、以及 `volume encryption rekey resume` 命令以恢復作業。

在重新輸入作業完成之前、磁碟區會有兩個按鍵。新的寫入及其對應的讀取將使用新的金鑰。否則、讀取將使用舊的金鑰。

您無法使用 `volume encryption rekey start` 重新輸入 SnapLock Volume 。

步驟

1. 變更加密金鑰：

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

   下列命令會變更的加密金鑰 `vol1` 在 SVM 上`vs1`：

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

2. 確認重新輸入作業的狀態：

   `volume encryption rekey show`

   如"指令參考資料ONTAP"需詳細 `volume encryption rekey show`資訊，請參閱。

   下列命令會顯示重新輸入作業的狀態：

   ```
   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. 重新輸入作業完成後、請確認磁碟區已啟用加密功能：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster1`：

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

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

使用ONTAP磁碟區移動啟動指令變更磁碟區的加密金鑰

定期變更磁碟區的加密金鑰是安全性最佳做法。您可以使用 `volume move start`命令來變更加密金鑰。移動的磁碟區可以位於相同的集合體或不同的集合體上。

關於這項工作

您無法使用 `volume move start` 重新輸入 SnapLock 或 FlexGroup 磁碟區。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有磁碟區並變更加密金鑰：

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

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume **`vol1`** 至目的地 Aggregate **`aggr2`** 並變更加密金鑰：

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

   系統會為磁碟區建立新的加密金鑰。磁碟區上的資料仍保持加密狀態。

2. 確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster1`：

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

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

輪換ONTAP NetApp儲存加密的驗證金鑰

使用NetApp儲存加密（NSE）時、您可以旋轉驗證金鑰。

關於這項工作

如果您使用外部金鑰管理程式（KMIP）、則可支援NSE環境中的旋轉驗證金鑰。

Onboard Key Manager（OKM）不支援NSE環境中的旋轉驗證金鑰。

步驟

1. 使用 `security key-manager create-key` 產生新驗證金鑰的命令。

   您必須先產生新的驗證金鑰、才能變更驗證金鑰。

2. 使用 `storage encryption disk modify -disk * -data-key-id` 變更驗證金鑰的命令。

相關資訊

- "儲存加密磁碟修改"

刪除 ONTAP 中的加密磁碟區

您可以使用 `volume delete` 刪除加密磁碟區的命令。

開始之前

- 您必須是叢集管理員才能執行此工作。
- Volume必須離線。

步驟

1. 刪除加密磁碟區：

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   如"指令參考資料ONTAP"需詳細 `volume delete`資訊，請參閱。

   下列命令會刪除名為的加密磁碟區 `vol1`：

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

   輸入 `yes` 當系統提示您確認刪除時。

   系統會在24小時後刪除磁碟區的加密金鑰。

   與選項搭配 `-force true`使用 `volume delete`，可立即刪除磁碟區並銷毀對應的加密金鑰。此命令需要進階權限。如"指令參考資料ONTAP"需詳細 `volume delete`資訊，請參閱。

完成後

您可以使用 `volume recovery-queue` 發出後在保留期間內恢復已刪除磁碟區的命令 `volume delete` 命令：

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

"如何使用Volume Recovery功能"

安全地清除加密磁碟區上的資料

了解如何安全地從加密**ONTAP**磁碟區中清除數據

從支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的情況下清除資料。ONTAP加密磁碟區上的資料清理功能可確保資料無法從實體媒體中恢復、例如在「資源回收」的情況下、資料追蹤可能會在區塊遭到覆寫時留下、或是安全地刪除租戶的資料。

安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。您無法清理未加密的Volume。您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

使用安全清除的考量事項

- 在啟用NetApp Aggregate Encryption（NAE）的Aggregate中建立的磁碟區不支援安全清除。
- 安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。
- 您無法清理未加密的Volume。
- 您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

視ONTAP 您的版本而定、安全清除功能會有所不同。

更新版本**ONTAP**

- 支援安全清除MetroCluster 功能的不受支援。FlexGroup
- 如果要清除的磁碟區是SnapMirror關係的來源、您就不需要中斷SnapMirror關係、就能執行安全的清除。
- 對於使用SnapMirror資料保護的磁碟區而言、重新加密方法不同於未使用SnapMirror資料保護（DP）或使用SnapMirror延伸資料保護的磁碟區。
  - 根據預設、使用SnapMirror資料保護（DP）模式的磁碟區會使用Volume Move Re-Encryption方法重新加密資料。
  - 根據預設、未使用SnapMirror資料保護的磁碟區或使用SnapMirror延伸資料保護（XDP）模式的磁碟區、會使用就地重新加密方法。
  - 您可以使用變更這些預設值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令。
- 根據預設， FlexVol 磁碟區中的所有快照都會在安全清除作業期間自動刪除。根據預設、FlexGroup 在安全清除作業期間、不會自動刪除使用SnapMirror資料保護的所有SnapMirror Volume和Snapshot快照。您可以使用命令變更這些預設值 `secure purge delete-all-snapshots [true|false]`。

更新版本：**ONTAP**

- 安全清除不支援下列項目：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的磁碟區是SnapMirror關係的來源、您必須先中斷SnapMirror關係、才能清除該磁碟區。

  如果磁碟區中有忙碌的快照，您必須先釋放快照，才能清除磁碟區。例如、您可能需要從其父磁碟區分割FlexClone磁碟區。

- 成功叫用安全清除功能會觸發磁碟區移動、以新金鑰重新加密其餘未清除的資料。

  移動的磁碟區會保留在目前的Aggregate上。舊金鑰會自動銷毀、確保清除的資料無法從儲存媒體中恢復。

從沒有**SnapMirror**關係的加密**ONTAP**磁碟區中清理數據

從使用支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的「crub」資料中進行安全清除。ONTAP

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
2. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

3. 如果您要安全清除的檔案位於快照中、請刪除快照：

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

4. 安全地清除刪除的檔案：

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

   下列命令可安全地清除上刪除的檔案 `vol1` 在 SVM 上`vs1`：

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

5. 驗證安全清除作業的狀態：

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

從具有SnapMirror非同步關係的加密ONTAP磁碟區中清理數據

從 ONTAP 9 8 開始、您可以在具有 SnapMirror 非同步關係且啟用 NVE 的磁碟區上、使用安全清除功能、以不中斷營運的「 crub 」資料。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命

令以終止作業。

> 若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

步驟

1. 在儲存系統上、切換至進階權限層級：

   ```
   set -privilege advanced
   ```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

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

   在 SnapMirror 非同步關係中的每個磁碟區上重複此步驟。

4. 如果您要安全清除的檔案位於快照中、請刪除快照：

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

5. 如果您要安全清除的檔案位於基礎快照中，請執行下列步驟：

   a. 在 SnapMirror 非同步關係中的目的地磁碟區上建立快照：

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

   b. 更新 SnapMirror 以向前移動基礎快照：

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

   對 SnapMirror 非同步關係中的每個 Volume 重複此步驟。

   a. 重複步驟（a）和（b），等於基礎快照的數量加上 1 。

      例如，如果您有兩個基礎快照，則應重複步驟（a）和（b）三次。

   b. 確認基礎快照存在：
      `snapshot show -vserver SVM_name -volume volume_name`
   c. 刪除基礎快照：
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`
6. 安全地清除刪除的檔案：

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

在 SnapMirror 非同步關係中的每個磁碟區上重複此步驟。

下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案：

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

7. 確認安全清除作業的狀態：

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

相關資訊

- "SnapMirror 更新"

從具有SnapMirror同步關係的加密ONTAP磁碟區中清理數據

從 ONTAP 9 8 開始、您可以使用安全清除功能、在具有 SnapMirror 同步關係的 NVE 磁碟區上、不中斷地「清理」資料。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 在儲存系統上、變更為進階權限層級：

```
set -privilege advanced
```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

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

針對 SnapMirror 同步關係中的其他磁碟區重複此步驟。

4. 如果您要安全清除的檔案位於快照中、請刪除快照：

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

5. 如果安全清除檔案位於基礎快照或一般快照中，請更新 SnapMirror 以將一般快照向前移：

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

   共有兩個常用快照，因此必須發出兩次此命令。

6. 如果安全清除檔案位於應用程式一致的快照中，請刪除 SnapMirror 同步關係中兩個磁碟區上的快照：

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

   在兩個磁碟區上執行此步驟。

7. 安全地清除刪除的檔案：

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

   在 SnapMirror 同步關係中的每個磁碟區上重複此步驟。

   下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案。

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

8. 確認安全清除作業的狀態：

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

相關資訊

- "SnapMirror 更新"

更改ONTAP板載密鑰管理密碼

NetApp建議您定期變更板載金鑰管理密碼。您必須將新密碼短語儲存在儲存系統之外的安全位置。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 此工作需要進階權限。
- 在MetroCluster環境中，在本地叢集上更新密碼短語後，同步夥伴叢集上的密碼短語更新。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 更改機載密鑰管理密碼。您使用的命令取決於您執行的ONTAP版本。

   更新版本**ONTAP**

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

   不含更新版本**ONTAP**

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

3. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“cc-mode”，輸入一個介於 64 到 256 個字元之間的密碼。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。

5. 如果您使用的是MetroCluster配置，請在夥伴叢集上同步更新後的密碼短語。

   a. 透過選擇適合您ONTAP版本的正確指令，在夥伴叢集上同步密碼短語：

      更新版本**ONTAP**

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

      不含更新版本**ONTAP**

      - 在ONTAP 9.5 中，運行：

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

      - 在ONTAP 9.4 及更早版本中，更新本機叢集上的密碼短語後，等待 20 秒，然後在夥伴叢集上執行以下命令：

        ```
        security key-manager setup
        ```

   b. 出現提示時，請輸入新的密碼短語。

      兩個群集必須使用相同的密碼短語。

完成後

將板載金鑰管理密碼短語複製到儲存系統外部的安全位置，以備將來使用。

每次變更機載金鑰管理密碼時，請手動備份金鑰管理資訊。

相關資訊

- "手動備份內建金鑰管理資訊"
- "安全金鑰管理程式內建更新密碼"

手動備份ONTAP板載金鑰管理訊息

設定Onboard Key Manager複雜密碼時、您應該將內建金鑰管理資訊複製到儲存系統外部的安全位置。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

所有的金鑰管理資訊都會自動備份到叢集的複寫資料庫（RDB）。您也應該手動備份金鑰管理資訊、以便在發生災難時使用。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 顯示叢集的金鑰管理備份資訊：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager onboard show-backup`
不含更新版本ONTAP	`security key-manager backup show`

   以下 9.6 指令顯示金鑰管理備份訊息 `cluster1` ：

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

3. 將備份資訊複製到儲存系統以外的安全位置、以便在發生災難時使用。

相關資訊

* "安全金鑰管理程式內建show Backup"
* "安全金鑰管理程式的備份展示"

在 ONTAP 中還原內建金鑰管理加密金鑰

有時，您可能需要恢復板載金鑰管理加密金鑰。確認需要恢復密鑰後，您可以設定板載密鑰管理器來恢復密鑰。恢復板載金鑰管理加密金鑰所遵循的步驟因ONTAP版本的不同而不同。

開始之前

- 如果您將 NSE 與外部 KMIP 伺服器一起使用，請刪除外部金鑰管理員資料庫。有關詳細信息，請參閱"從外部金鑰管理過渡到ONTAP板載金鑰管理"。
- 您必須是叢集管理員才能執行此工作。

如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

更新版本ONTAP

如果您執行的是 ONTAP 9.8 或更新版本、而且根磁碟區已加密、請遵循的程序 [ontap-9-8]。

1. 確認金鑰需要還原：
   `security key-manager key query -node node`

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

2. 還原金鑰：
   `security key-manager onboard sync`

   如"指令參考資料ONTAP"需詳細 `security key-manager onboard sync`資訊，請參閱。

3. 在通關密碼提示字元下、輸入叢集的內建金鑰管理通關密碼。

ONTAP 9.8 或更新版本、含加密的根磁碟區

如果您執行ONTAP 的是更新版本的版本、而且根磁碟區已加密、則必須使用開機功能表設定內建金鑰管理還原密碼。如果您要更換開機媒體、也必須執行此程序。

1. 將節點開機至開機功能表、然後選取選項 `(10) Set onboard key management recovery secrets`。
2. 輸入 `y` 以使用此選項。
3. 出現提示時、輸入叢集的內建金鑰管理通關密碼。
4. 出現提示時、輸入備份金鑰資料。

   輸入備份金鑰資料後，節點返回啟動選單。

5. 從開機功能表中、選取選項 `(1) Normal Boot`。

不含更新版本ONTAP

1. 確認金鑰需要還原：
   `security key-manager key show`
2. 還原金鑰：
   `security key-manager setup -node node`

   詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

3. 在通關密碼提示字元下、輸入叢集的內建金鑰管理通關密碼。

恢復ONTAP外部金鑰管理加密金鑰

您可以手動還原外部金鑰管理加密金鑰、並將其推送到不同的節點。如果您重新啟動的節點在建立叢集的金鑰時暫時停機、您可能會想要這麼做。

關於這項工作

在 ONTAP 9.6 及更新版本中、您可以使用 `security key-manager key query -node node_name` 命令以驗證金鑰是否需要還原。

在 ONTAP 9.5 或更早版本中、您可以使用 `security key-manager key show` 命令以驗證金鑰是否需要還原。

> 如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 如果您執行ONTAP 的是更新版本的版本、且根磁碟區已加密、請執行下列步驟：

   如果您執行ONTAP 的是更新版本的版本、或是執行ONTAP 的是版本不加密的版本、請跳過此步驟。

   a. 設定 bootargs ：
      ```
      setenv kmip.init.ipaddr <ip-address>
      setenv kmip.init.netmask <netmask>
      setenv kmip.init.gateway <gateway>
      setenv kmip.init.interface e0M
      boot_ontap
      ```
   b. 將節點開機至開機功能表、然後選取選項 `(11) Configure node for external key management`。
   c. 依照提示輸入管理憑證。

      輸入所有管理憑證資訊後、系統會返回開機功能表。

   d. 從開機功能表中、選取選項 `(1) Normal Boot`。
2. 還原金鑰：

此版本… ONTAP	使用此命令…
更新版本ONTAP	`security key-manager external restore -vserver SVM -node node -key-server host_name

IP_address:port -key-id key_id -key -tag key_tag`	不含更新版本ONTAP

`node`預設為所有節點。

啟用內建金鑰管理時、不支援此命令。

下列 ONTAP 9.6 命令可將外部金鑰管理驗證金鑰還原至中的所有節點 `cluster1`：

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

相關資訊

- "安全金鑰管理程式外部還原"

替換ONTAP叢集上的 KMIP SSL 憑證

所有SSL憑證都有到期日。您必須在憑證過期之前更新憑證、以避免喪失驗證金鑰的存取權。

開始之前

- 您必須已取得叢集的替代公開憑證和私密金鑰（KMIP用戶端憑證）。
- 您必須已取得KMIP伺服器（KMIP伺服器- CA憑證）的替代公共憑證。
- 您必須是叢集或SVM管理員、才能執行此工作。
- 如果您要在 MetroCluster 環境中更換 KMIP SSL 憑證、則必須在兩個叢集上安裝相同的置換 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝替換用戶端和伺服器憑證。

步驟

1. 安裝新的KMIP伺服器CA憑證：

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

2. 安裝新的KMIP用戶端憑證：

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

3. 更新金鑰管理程式組態以使用新安裝的憑證：

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

   如果您在ONTAP 支援支援功能的環境中執行的是支援支援功能的版本9.6或更新版本MetroCluster 、而您想要修改管理SVM上的金鑰管理程式組態、則必須在組態中的兩個叢集上執行命令。

如果新用戶端憑證的公鑰/私鑰與先前安裝的金鑰不同，則更新金鑰管理器設定以使用新安裝的憑證將傳回錯誤。查看"NetApp知識庫：新的用戶端憑證公鑰或私鑰與現有用戶端憑證不同"有關如何覆寫此錯誤的說明。

相關資訊

- "安全性憑證安裝"
- "安全金鑰管理程式外部修改"

更換 ONTAP 中的 FIPS 磁碟機或 SED

更換FIPS磁碟機或SED的方式與更換一般磁碟相同。請務必將新的資料驗證金鑰指派給更換的磁碟機。對於FIPS磁碟機、您可能也想指派新的FIPS 140-2驗證金鑰。

如果HA配對正在使用 "加密SAS或NVMe磁碟機（SED、NSE、FIPS）"、您必須遵循主題中的指示 "將FIPS磁碟機或SED恢復為無保護模式" 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

開始之前

- 您必須知道磁碟機使用的驗證金鑰金鑰ID。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 確定磁碟已標示為故障：

   ```
   storage disk show -broken
   ```

   如"指令參考資料ONTAP"需詳細 `storage disk show`資訊，請參閱。

   ```
   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. 請依照磁碟櫃模型硬體指南中的指示、移除故障磁碟、並以新的FIPS磁碟機或SED進行更換。

3. 指派新更換磁碟的擁有權：

   `storage disk assign -disk disk_name -owner node`

   如"指令參考資料ONTAP"需詳細 `storage disk assign`資訊，請參閱。

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

4. 確認已指派新磁碟：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   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. 將資料驗證金鑰指派給FIPS磁碟機或SED。

   "指派資料驗證金鑰給FIPS磁碟機或SED（外部金鑰管理）"

6. 如有必要、請指派FIPS 140-2驗證金鑰給FIPS磁碟機。

   "將FIPS 140-2驗證金鑰指派給FIPS磁碟機"

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"
- "儲存加密磁碟顯示"

使FIPS磁碟機或SED上的資料無法存取

了解如何使 FIPS 驅動器或 SED 上的ONTAP資料無法存取

如果您想要使FIPS磁碟機或SED上的資料永久無法存取、但要保留磁碟機未使用的空間以供新資料使用、您可以清理磁碟。如果您想要永久無法存取資料、而且不需要重複使用磁

碟機、可以將其銷毀。

- 磁碟資料抹除

  當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0（SAS磁碟機）或null金鑰（NVMe磁碟機）。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

- 磁碟銷毀

  當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟。這樣做會使磁碟永遠無法使用、且上的資料永遠無法存取。

您可以清除或銷毀個別自我加密磁碟機、或是節點的所有自我加密磁碟機。

在 ONTAP 中清理 FIPS 磁碟機或 SED

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、並將磁碟機用於新資料、您可以使用 `storage encryption disk sanitize` 用於清理磁碟機的命令。

關於這項工作

當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0（SAS磁碟機）或null金鑰（NVMe磁碟機）。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將任何需要保留的資料移轉到另一個磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要消毒的Aggregate：

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

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

   如"指令參考資料ONTAP"需詳細 `storage aggregate delete`資訊，請參閱。

3. 識別要消毒的FIPS磁碟機或SED的磁碟ID：

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

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
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. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

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

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

```
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. 為磁碟機消毒：

   `storage encryption disk sanitize -disk *disk_id*`

   您只能使用此命令來清除熱備援磁碟或中斷的磁碟。若要清理所有磁碟，無論其類型為何，請使用 `-force-all-state`選項。如"指令參考資料ONTAP"需詳細 `storage encryption disk sanitize`資訊，請參閱。

   ONTAP 會提示您輸入確認片語、然後再繼續。輸入完全如畫面所示的詞彙。

```
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. 解除清理磁碟故障：`storage disk unfail -spare true -disk *disk_id*`
7. 檢查磁碟是否擁有擁有者：`storage disk show -disk *disk_id*`
   如果磁碟沒有擁有者、請指派一個擁有者。`storage disk assign -owner node -disk *disk_id*`

8. 輸入要清理磁碟的節點節點節點的節點節點節點：

   `system node run -node node_name`

   執行 `disk sanitize release` 命令。

9. 離開 nodesdroand 。再次解除磁碟故障： `storage disk unfail -spare true -disk disk_id`
10. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用： `storage disk show -disk disk_id`

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"
- "儲存磁碟未故障"
- "儲存加密磁碟修改"
- "儲存加密磁碟清理"
- "儲存加密磁碟顯示狀態"

在 ONTAP 中銷毀 FIPS 磁碟機或 SED

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、而且不需要重複使用磁碟機、您可以使用 `storage encryption disk destroy` 破壞磁碟的命令。

關於這項工作

當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟機。這樣做會使磁碟幾乎無法使用、且上的資料永遠無法存取。不過、您可以使用印在磁碟標籤上的實體安全ID（PSID）、將磁碟重設為原廠設定的設定。如需詳細資訊、請參閱 "當驗證金鑰遺失時、將FIPS磁碟機或SED恢復服務"。

> ⓘ 除非您擁有不可傳的Disk Plus服務（NRD Plus）、否則請勿銷毀FIPS磁碟機或SED。銷毀磁碟會使其保固失效。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將任何需要保留的資料移轉到另一個不同磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要銷毀的Aggregate：

   `storage aggregate delete -aggregate aggregate_name`

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

   如"指令參考資料ONTAP"需詳細 `storage aggregate delete`資訊，請參閱。

3. 識別要銷毀的FIPS磁碟機或SED的磁碟ID：

   ```
   storage encryption disk show
   ```

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   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. 銷毀磁碟：

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

   如"指令參考資料ONTAP"需詳細 `storage encryption disk destroy`資訊，請參閱。

   系統會提示您輸入確認短句、然後再繼續。輸入完全如畫面所示的詞彙。

   ```
   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.
   ```

相關資訊

- "儲存加密磁碟銷毀"
- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

ONTAP 中的 FIPS 磁碟機或 SED 上的緊急資料會被粉碎

發生安全性緊急情況時、即使儲存系統或KMIP伺服器無法使用電源、您仍可立即防止存取FIPS磁碟機或SED。

開始之前

- 如果您使用的KMIP伺服器沒有可用的電源、則KMIP伺服器必須設定容易銷毀的驗證項目（例如智慧卡或USB磁碟機）。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 緊急銷毀FIPS磁碟機或SED上的資料：

如果…	然後…

儲存系統可提供電力、您也有時間讓儲存系統正常離線	a. 如果儲存系統設定為HA配對、請停用接管功能。 b. 使所有集合體離線並加以刪除。 c. 將權限層級設為進階：`set -privilege advanced` d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：`storage encryption disk modify -disk * -fips-key-id 0x0` e. 停止儲存系統。 f. 開機進入維護模式。 g. 清理或銷毀磁碟： ◦ 如果您想讓磁碟上的資料無法存取、但仍能重複使用磁碟、請清理磁碟：`disk encrypt sanitize -all` ◦ 如果您想讓磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：`disk encrypt destroy disk_id1 disk_id2 …` ◦ `disk encrypt sanitize` 和 `disk encrypt destroy` 命令僅保留用於維護模式。這些命令必須在每個HA節點上執行、而且無法用於中斷的磁碟。 h. 針對合作夥伴節點重複這些步驟。 如此一來、儲存系統就會處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。	儲存系統可提供電力、您必須立即切斷資料

a. 如果您想要使磁碟上的資料無法存取且仍能重複使用磁碟、請清理磁碟：
b. 如果儲存系統設定為HA配對、請停用接管功能。
c. 將權限層級設為進階：
`set -privilege advanced`
d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. 清理磁碟：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. 如果您想要使磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：
	b. 如果儲存系統設定為HA配對、請停用接管功能。
	c. 將權限層級設為進階：
	`set -privilege advanced`
	d. 銷毀磁碟： `storage encryption disk destroy -disk * -force -all-states true`
		儲存系統會出現問題、使系統處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。

KMIP伺服器可供電、但儲存系統無法供電	a. 登入 KMIP 伺服器。 b. 銷毀與FIPS磁碟機或SED相關的所有金鑰、這些金鑰包含您要防止存取的資料。 如此可防止儲存系統存取磁碟加密金鑰。	KMIP伺服器或儲存系統無法使用電源

相關資訊

- "儲存加密磁碟銷毀"
- "儲存加密磁碟修改"
- "儲存加密磁碟清理"

當ONTAP中的驗證金鑰遺失時，將 FIPS 磁碟機或 SED 還原服務

如果您永久遺失FIPS磁碟機或SED的驗證金鑰、而且無法從KMIP伺服器擷取、系統會將其視為中斷。雖然您無法存取或恢復磁碟上的資料、但您可以採取步驟、讓SED的未使用空間再次可供資料使用。

開始之前

您必須是叢集管理員才能執行此工作。

關於這項工作

只有當您確定FIPS磁碟機或SED的驗證金鑰已永久遺失、而且無法還原時、才應使用此程序。

如果磁碟已分割、則必須先取消磁碟分割、才能開始此程序。

取消磁碟分割的命令僅在診斷層級可用，且只能在NetApp支援監督下執行。強烈建議您在繼續操作之前聯繫**NetApp**支援。 您也可以參考"NetApp知識庫：如何在ONTAP中取消對備用磁碟機的分割區"。

步驟

1. 將FIPS磁碟機或SED送回服務：

如果SED是…	請使用下列步驟…

未處於FIPS相容模式、或處於FIPS相容模式、且FIPS金鑰可供使用	a. 將權限層級設為進階：
	`set -privilege advanced`
	b. 將 FIPS 金鑰重設為預設製造安全 ID 0x0 ：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 確認作業成功：
	`storage encryption disk show-status`
	如果作業失敗、請使用本主題中的 PSID 程序。
	d. 清理損壞的磁碟：
	`storage encryption disk sanitize -disk disk_id`
	使用命令驗證作業是否成功 `storage encryption disk show-status` 繼續下一步之前。
	e. 解除清理磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	f. 檢查磁碟是否擁有擁有者：
	`storage disk show -disk disk_id`
	如果磁碟沒有擁有者、請指派一個擁有者。
	`storage disk assign -owner node -disk disk_id`
	i. 輸入要清理磁碟的節點節點節點的節點節點節點：
	`system node run -node node_name`
	執行 `disk sanitize release` 命令。
	g. 離開 nodesdroand 。再次解除磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	h. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
	`storage disk show -disk disk_id`

在FIPS相容模式中、FIPS金鑰無法使用、且SED標籤上印有PSID	a. 從磁碟標籤取得磁碟的PSID。
	b. 將權限層級設為進階：
	`set -privilege advanced`
	c. 將磁碟重設為原廠設定的設定：
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`
	使用命令驗證作業是否成功 `storage encryption disk show-status` 繼續下一步之前。
	d. 如果您執行的是 ONTAP 9.8P5 或更早版本、請跳至下一步。如果您執行的是 ONTAP 9.8P6 或更新版本、請將已清理的磁碟恢復故障。
	`storage disk unfail -disk disk_id`
	e. 檢查磁碟是否擁有擁有者：
	`storage disk show -disk disk_id`
	如果磁碟沒有擁有者、請指派一個擁有者。
	`storage disk assign -owner node -disk disk_id`
	i. 輸入要清理磁碟的節點節點節點的節點節點節點：
	`system node run -node node_name`
	執行 `disk sanitize release` 命令。
	f. 離開 nodesdroe ..再次解除磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	g. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
	`storage disk show -disk disk_id`

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟恢復到原始狀態"
- "儲存加密磁碟清理"
- "儲存加密磁碟顯示狀態"

在ONTAP中將 FIPS 驅動器或 SED 恢復為不受保護的模式

僅當節點的驗證金鑰ID設為預設值以外的值時、FIPS磁碟機或SED才會受到保護、不受未獲授權的存取。您可以使用命令將金鑰 ID 設為預設值，將 FIPS 磁碟機或 SED 恢復為未受保護模式 `storage encryption disk modify`。未受保護模式下的 FIPS 磁碟機或 SED 使用預設加密金鑰，而受保護模式下的 FIPS 磁碟機或 SED 則使用提供的加密金鑰。如果磁碟機上有加密資料，而且磁碟機重設為未受保護模式，則資料仍會加密，不會公開。

按照此程序確保 FIPS 驅動器或 SED 返回到不受保護的模式後任何加密資料都變得無法存取。一旦重置 FIPS 和資料金鑰 ID，任何現有資料都無法解密，且無法訪問，除非恢復原始金鑰。

如果HA配對使用加密SAS或NVMe磁碟機（SED、NSE、FIPS）、則在初始化系統之前、您必須針對HA配對內的所有磁碟機（開機選項4或9）執行此程序。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

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

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   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.
   ```

   使用以下命令確認作業成功：

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

   重複 show-status 指令，直到「Disks Begun」和「Disks Done」中的數字相同。

   ```
   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. 將節點的資料驗證金鑰ID設回預設的MSID 0x0：

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

   的價值 `-data-key-id` 無論您要將 SAS 或 NVMe 磁碟機恢復為未受保護模式、都應該設定為 0x0 。

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   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.
   ```

   使用以下命令確認作業成功：

   `storage encryption disk show-status`

   重複 show-status 指令，直到數字相同。當“disks began”和“disks done”中的數字相同時，操作完成。

維護模式

從支援功能9.7開始ONTAP 、您可以從維護模式重新輸入FIPS磁碟機的金鑰。只有在ONTAP 無法使用上一節中的指令時、才應使用維護模式。

步驟

1. 將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   `disk encrypt rekey_fips 0x0 disklist`

2. 將節點的資料驗證金鑰ID設回預設的MSID 0x0：

   `disk encrypt rekey 0x0 disklist`

3. 確認FIPS驗證金鑰已成功重新輸入：

   `disk encrypt show_fips`

4. 確認資料驗證金鑰已成功重新輸入：

   `disk encrypt show`

   您的輸出可能會顯示預設的MSID 0x0金鑰ID或金鑰伺服器所保留的64個字元值。。 `Locked?` 欄位是指資料鎖定。

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

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟顯示狀態"

移除 ONTAP 中的外部金鑰管理程式連線

當不再需要服務器時、您可以從節點中斷KMIP伺服器的連線。例如、當您轉換至Volume加密時、可能會中斷KMIP伺服器的連線。

關於這項工作

當您中斷KMIP伺服器與HA配對中某個節點的連線時、系統會自動中斷伺服器與所有叢集節點的連線。

如果您打算在中斷KMIP伺服器連線後繼續使用外部金鑰管理、請確定另一部KMIP伺服器可用於提供驗證金鑰。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 中斷KMIP伺服器與目前節點的連線：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,...`	不含更新版本ONTAP

在支援支援資源的環境中MetroCluster 、您必須在兩個叢集上為管理SVM重複執行這些命令。

下列 ONTAP 9.6 命令會停用連線至的兩個外部金鑰管理伺服器 `cluster1`，第一個命名的 `ks1`接聽預設連接埠 5696 、第二個連接埠的 IP 位址為 10.0.0.20 、接聽連接埠 24482 ：

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

深入瞭解 `security key-manager external remove-servers`及 `security key-manager delete` "指令參考資料ONTAP"。

修改ONTAP外部金鑰管理伺服器屬性

從 ONTAP 9.6 開始、您可以使用 `security key-manager external modify-server` 變更外部金鑰管理伺服器 I/O 逾時和使用者名稱的命令。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 此工作需要進階權限。
- 在這個支援對象環境中MetroCluster 、您必須在兩個叢集上為管理SVM重複這些步驟。

步驟

1. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 修改叢集的外部金鑰管理程式伺服器內容：

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

   超時值以秒表示。如果您修改使用者名稱、系統會提示您輸入新密碼。 如果您在叢集登入提示字元中執行命令、 *admin_SVM* 預設為目前叢集的管理SVM。您必須是叢集管理員、才能修改外部金鑰管理程式伺服器內容。

   下列命令會將的逾時值變更為 45 秒 `cluster1` 偵聽預設連接埠 5696 的外部金鑰管理伺服器：

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

3. 修改SVM的外部金鑰管理程式伺服器內容（僅限NVE）：

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

   超時值以秒表示。如果您修改使用者名稱、系統會提示您輸入新密碼。 如果您在 SVM 登入提示字元下執行命令、 *SVM* 預設為目前的 SVM 。您必須是叢集或SVM管理員、才能修改外部金鑰管理程式伺服器內容。

   下列命令會變更的使用者名稱和密碼 `svm1` 偵聽預設連接埠 5696 的外部金鑰管理伺服器：

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

4. 針對任何其他SVM重複最後一個步驟。

相關資訊

- "安全金鑰管理程式外部修改伺服器"

從 ONTAP 的內建金鑰管理移轉至外部金鑰管理

如果您想從內建金鑰管理切換至外部金鑰管理、則必須先刪除內建金鑰管理組態、才能啟用外部金鑰管理。

開始之前

- 對於硬體型加密、您必須將所有FIPS磁碟機或SED的資料金鑰重設為預設值。

  "將FIPS磁碟機或SED恢復為無保護模式"

- 對於軟體型加密、您必須取消加密所有磁碟區。

  "取消Volume資料加密"

- 您必須是叢集管理員才能執行此工作。

步驟

1. 刪除叢集的內建金鑰管理組態：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager onboard disable -vserver SVM`
不含更新版本ONTAP	`security key-manager delete-key-database`

深入瞭解 `security key-manager onboard disable`及 `security key-manager delete-key-database` "指令參考資料ONTAP"。

從外部金鑰管理切換到ONTAP板載金鑰管理

若要切換至板載金鑰管理，請在啟用板載金鑰管理之前刪除外部金鑰管理配置。

開始之前

- 對於硬體型加密、您必須將所有FIPS磁碟機或SED的資料金鑰重設為預設值。

  "將FIPS磁碟機或SED恢復為無保護模式"

- 您必須刪除所有外部金鑰管理程式連線。

  "刪除外部金鑰管理程式連線"

- 您必須是叢集管理員才能執行此工作。

步驟

轉換金鑰管理的步驟取決於您所使用的 ONTAP 版本。

更新版本**ONTAP**

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 使用命令：

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

   在支援支援資源的環境中MetroCluster 、您必須在兩個叢集上重複執行命令、才能使用管理SVM。

詳細了解 `security key-manager external disable`在"指令參考資料ONTAP"。

不含更新版本**ONTAP**

使用命令：

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

詳細了解 `security key-manager delete-kmip-config`在"指令參考資料ONTAP"。

相關資訊

- "安全金鑰管理員外部使用"

如果在ONTAP啟動過程中無法存取金鑰管理伺服器，會發生什麼情況

在開機期間、若為NSE設定的儲存系統無法觸及任何指定的金鑰管理伺服器、則執行某些預防措施以避免不必要的行為。ONTAP

如果儲存系統已設定為使用NSE、系統會重新鎖定SED、並開啟SED電源、則儲存系統必須從金鑰管理伺服器擷取所需的驗證金鑰、以驗證自己是否能存取資料。

儲存系統會嘗試聯絡指定的金鑰管理伺服器、最多三小時。如果之後儲存系統仍無法連絡到任何儲存系統、則開機程序會停止、儲存系統也會停止。

如果儲存系統成功連絡任何指定的金鑰管理伺服器、則會嘗試建立長達15分鐘的SSL連線。如果儲存系統無法與任何指定的金鑰管理伺服器建立SSL連線、開機程序會停止、儲存系統也會停止。

當儲存系統嘗試聯絡並連線至主要管理伺服器時、會在CLI中顯示失敗聯絡嘗試的詳細資訊。您可以隨時按Ctrl-C中斷聯絡活動嘗試

為了安全起見、SED僅允許有限數量的未授權存取嘗試、之後會停用對現有資料的存取。如果儲存系統無法連絡任何指定的金鑰管理伺服器以取得適當的驗證金鑰、則只能嘗試使用預設金鑰進行驗證、導致嘗試失敗並造成恐慌。如果儲存系統設定為在發生緊急情況時自動重新開機、則會進入開機迴圈、導致SED持續嘗試驗證失敗。

在這些情況下停止儲存系統的設計、是為了防止儲存系統進入開機迴圈、以及可能因超過某個連續驗證嘗試失敗次數的安全限制而永久鎖定的SED而導致意外的資料遺失。鎖定保護的限制和類型取決於製造規格和SED類型：

SED 類型	導致鎖定的連續驗證嘗試失敗次數	達到安全限制時的鎖定保護類型
HDD	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
X440_PHM2800MCTO 800GB NSE SSD搭配韌體版本NA00或NA01	5.	暫時性。鎖定功能只會在磁碟重新開機之前生效。
具有韌體版本NA00或NA01的X577_PHM2800MCTO 800GB NSE SSD	5.	暫時性。鎖定功能只會在磁碟重新開機之前生效。
X440_PHM2800MCTO 800GB NSE SSD、韌體版本更高	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
具有較高韌體版本的X577_PHM2800MCTO 800GB NSE SSD	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
所有其他SSD機型	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。

對於所有SED類型、成功驗證會將試用數重設為零。

如果您遇到儲存系統因為無法連線至任何指定的金鑰管理伺服器而停止運作的情況、則必須先識別並修正通訊故障的原因、然後再嘗試繼續開機儲存系統。

預設禁用ONTAP加密

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAP如有必要、您可以依預設停用整個叢集的加密功能。

開始之前

您必須是叢集管理員才能執行此工作、或是叢集管理員已委派權限的SVM管理員。

步驟

1. 若要在ONTAP 預設情況下停用對整個叢集的加密功能、請執行下列命令：

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