設定內建金鑰管理
ONTAP 9

NetApp
February 12, 2026

目錄

設定內建金鑰管理

啟用更新版本的更新版本、以利執行內建金鑰管理ONTAP

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。Onboard Key Manager符合FIPS-140-2第1級標準。

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager onboard enable` 每次將節點新增至叢集時的命令。在 MetroCluster 組態中、您必須執行 `security key-manager onboard enable` 先在本機叢集上執行 `security key-manager onboard sync` 在遠端叢集上、使用相同的複雜密碼。

詳細了解 `security key-manager onboard enable`和 `security key-manager onboard sync`在"指令參考資料ONTAP"。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。除了在 MetroCluster 中、您可以使用 `cc-mode-enabled=yes` 選項要求使用者在重新開機後輸入複雜密碼。

> 當「內建金鑰管理程式」在「一般條件」模式中啟用時 (`cc-mode-enabled=yes`）、系統行為會以下列方式變更：
>
> - 系統會監控在「一般準則」模式下運作時、連續嘗試失敗的叢集密碼。
>
> 如果已啟用NetApp儲存加密（NSE）、且您在開機時未輸入正確的叢集密碼、則系統將無法驗證其磁碟機並自動重新開機。若要修正此問題、您必須在開機提示字元中輸入正確的叢集密碼。一旦開機、系統最多可連續5次嘗試在24小時內、針對任何需要叢集密碼作為參數的命令、正確輸入叢集密碼。如果達到限制（例如、您連續5次未正確輸入叢集密碼）、則必須等待24小時逾時期間、或是重新啟動節點、才能重設限制。
>
> - 系統映像更新會使用NetApp RSA-3072程式碼簽署憑證搭配SHA-384程式碼簽署摘要、來檢查映像完整性、而非一般的NetApp RSA-2048程式碼簽署憑證和SHA-256程式碼簽署摘要。
>
> 升級命令透過檢查各種數位簽名來驗證影像內容是否已更改或損壞。如果驗證有效，映像更新將進入下一步。如果驗證無效，則影像更新失敗。詳細了解 `cluster image`在"指令參考資料ONTAP"。

> Onboard Key Manager可將金鑰儲存在揮發性記憶體中。當系統重新開機或停止時、揮發性記憶體內容會被清除。在正常操作條件下、系統停止時、揮發性記憶體內容將在30秒內清除。

開始之前

- 如果您使用NSE搭配外部金鑰管理（KMIP）伺服器、則必須刪除外部金鑰管理程式資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定命令：

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

   設 `cc-mode-enabled=yes`為要求使用者在重新開機後輸入金鑰管理密碼。MetroCluster 組態不支援此 `- cc-mode-enabled`選項。命令會 `security key-manager onboard enable`取代 `security key-manager setup`命令。

   下列範例會在叢集1上啟動金鑰管理程式設定命令、而不要求在每次重新開機後輸入通關密碼：

2. 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。

3. 在通關密碼確認提示下、重新輸入通關密碼。
4. 驗證系統是否建立了身份驗證金鑰：

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

   命令會 `security key-manager key query`取代 `security key-manager query key`命令。

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

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

系統會自動將關鍵管理資訊備份到叢集的複製資料庫（RDB）。您還應該手動備份此資訊以用於災難復原。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員金鑰查詢"
- "安全金鑰管理員板載啟用"
- "從外部金鑰管理移轉至內建金鑰管理"

啟用更新版本的更新版本ONTAP

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。Onboard Key

Manager符合FIPS-140-2第1級標準。

您可以使用板載金鑰管理器來保護叢集用於存取加密資料的金鑰。在存取加密磁碟區或自加密磁碟的每個叢集上啟用板載金鑰管理器。

關於這項工作

您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

密碼嘗試失敗後、您必須重新啟動節點。

開始之前

- 如果您將 NSE 與外部金鑰管理 (KMIP) 伺服器一起使用，請刪除外部金鑰管理器資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在配置板載金鑰管理器之前，請先配置MetroCluster環境。

步驟

1. 啟動金鑰管理程式設定：

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

   從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 此選項可要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。

   下列範例會在叢集1上開始設定金鑰管理程式、而不要求在每次重新開機後輸入通關密碼：

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

...

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

2. 輸入 `yes` 在提示下設定內建金鑰管理。
3. 在通關密碼提示字元中、輸入32到256個字元之間的通關密碼、或輸入「'cc-mode'」（64到256個字元之間的通關密碼）。

> 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. 驗證是否已為所有節點設定金鑰：

   `security key-manager show-key-store`

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

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

完成後

ONTAP會自動將金鑰管理資訊備份到叢集的複製資料庫 (RDB)。

設定板載金鑰管理器密碼後，請手動將資訊備份到儲存系統外部的安全位置。看"手動備份內建金鑰管理資訊"。

相關資訊

- "手動備份內建金鑰管理資訊"
- "安全金鑰管理程式設定"
- "安全金鑰管理員顯示金鑰庫"
- "從外部金鑰管理移轉至內建金鑰管理"

使用ONTAP板載金鑰管理將資料驗證金鑰指派給 FIPS 磁碟機或 SED

您可以使用 `storage encryption disk modify` 命令將資料驗證金鑰指派給 FIPS 磁碟機或 SED 。叢集節點使用此金鑰來存取磁碟機上的資料。

關於這項工作

自我加密磁碟機只有在驗證金鑰ID設定為非預設值時、才會受到保護、不受未獲授權的存取。製造商安全ID（MSID）具有金鑰ID 0x0、是SAS磁碟機的標準預設值。對於NVMe磁碟機、標準預設值為null金鑰、表示為空白金鑰ID。當您將金鑰ID指派給自我加密磁碟機時、系統會將其驗證金鑰ID變更為非預設值。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 指派資料驗證金鑰給FIPS磁碟機或SED：

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

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

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

2. 確認已指派驗證金鑰：

```
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>
[...]
```

相關資訊

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"