階段6.完成升級

Upgrade controllers

NetApp
July 05, 2024

目錄

階段6.完成升級

第 6 階段總覽

在第6階段期間、您將確認新節點已正確設定、如果新節點已啟用加密、則您可以設定及設定儲存加密或NetApp Volume Encryption。您也應該取消委任舊節點、然後恢復SnapMirror作業。

步驟

1. "使用KMIP伺服器管理驗證"
2. "確認新的控制器已正確設定"
3. "在新的控制器模組上設定儲存加密"
4. "在新的控制器模組上設定NetApp Volume或Aggregate Encryption"
5. "取消委任舊系統"
6. "恢復SnapMirror作業"

使用KMIP伺服器管理驗證

您可以使用金鑰管理互通性通訊協定（ KMIP ）伺服器來管理驗證金鑰。

步驟

1. 新增控制器：

   「安全金鑰管理程式外部啟用」

2. 新增金鑰管理程式：

   「安全金鑰管理程式外部附加伺服器-金鑰伺服器_key_manager_server_ip_address_」

3. 驗證金鑰管理伺服器是否已設定、且可供叢集中的所有節點使用：

   「安全金鑰管理程式外部顯示狀態」

4. 將驗證金鑰從所有連結的金鑰管理伺服器還原至新節點：

   「安全金鑰管理程式外部還原-node_new_控制 器名稱_」

確認新的控制器已正確設定

若要確認設定正確、您必須啟用HA配對。您也必須驗證node3和node4是否可以存取彼此的儲存設備、以及它們是否擁有屬於叢集上其他節點的資料LIF。此外、您必須確認node3擁有node1的Aggregate、而node4擁有node2的Aggregate、而且兩個節點的磁碟區都在線上。

步驟

1. 對節點2進行檢查後、會啟用節點2叢集的儲存容錯移轉和叢集HA配對。完成作業後、兩個節點都會顯示為已完成、系統會執行一些清除作業。
2. 確認已啟用儲存容錯移轉：

   「容錯移轉顯示」

   下列範例顯示啟用儲存容錯移轉時命令的輸出：

   ```
   cluster::> storage failover show
                      Takeover
   Node      Partner  Possible   State Description
   --------- -------  --------   ------------------
   node3     node4    true       Connected to node4
   node4     node3    true       Connected to node3
   ```

3. 使用下列命令檢查輸出、確認node3和node4屬於同一個叢集：

   「叢集展示」

4. 使用下列命令檢查輸出、確認節點3和節點4可以存取彼此的儲存設備：

   「torage容錯移轉顯示-欄位、本機磁碟遺失、合作夥伴磁碟遺失」

5. 使用下列命令檢查輸出、確認節點3和節點4都不擁有叢集中其他節點所擁有的資料lifs主目錄：

   「網路介面展示」

   如果節點3或節點4都不擁有叢集中其他節點所擁有的資料生命週期、請將資料生命週期還原為其主擁有者：

   網路介面回復

6. 驗證node3是否擁有node1的集合體、以及node4是否擁有node2的集合體：

   ```
   storage aggregate show -owner-name <node3>

   storage aggregate show -owner-name <node4>
   ```

7. 判斷是否有任何磁碟區離線：

   ```
   volume show -node <node3> -state offline

   volume show -node <node4> -state offline
   ```

8. 如果有任何磁碟區離線、請將它們與您在一節中擷取的離線磁碟區清單進行比較 "準備節點以進行升級"並在每個Volume上使用一次下列命令、視需要將任何離線磁碟區上線：

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

9. 針對每個節點使用下列命令、安裝新節點的新授權：

   `system license add -license-code <license_code,license_code,license_code…>`

   授權代碼參數接受28個大寫字母字元金鑰的清單。您可以一次新增一個授權、也可以一次新增多個授權、以英文分隔每個授權金鑰。

10. 使用下列其中一個命令、從原始節點移除所有舊授權：

    「系統授權清除-未使用-過期」

    ```
    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - 刪除所有過期的授權：

      「系統授權清除-過期」

    - 刪除所有未使用的授權：

      「系統授權清理-未使用」

    - 在節點上使用下列命令、從叢集刪除特定授權：

      ```
      system license delete -serial-number <node1_serial_number> -package *

      system license delete -serial-number <node2_serial_number> -package *
      ```

    將顯示下列輸出：

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    輸入「y」以移除所有套件。

11. 使用下列命令並檢查輸出、確認已正確安裝授權：

    「系統授權展示」

    您可以比較輸出與您在區段中擷取的輸出 "準備節點以進行升級"。

12. [unset_maxwait_system_commands] 如果在組態中使用自我加密磁碟機、而且您已將變數設 `kmip.init.maxwait` 為 `off` （例如、在中 "安裝並開機節點4、步驟24"）、則必須取消設定變數：

    ```
    set diag; systemshell -node <node_name> -command sudo kenv -u -p
    kmip.init.maxwait
    ```

13. [[Step13]在兩個節點上使用下列命令來設定SP：

```
system service-processor network modify -node <node_name>
```

請參閱 "參考資料" 如需SP及_SURE9.8 ONTAP 命令的相關資訊、請連結至_System Administration Reference（系統管理參考資料）：Manual Page Reference（手冊頁參考）_、以取得有關係統「服務處理器網路修改」命令的詳細資訊。

14. 如果您要在新節點上設定無交換器叢集、請參閱 "參考資料" 若要連結至_NetApp支援網站_、請遵循_移轉至雙節點無交換器叢集_中的指示。

完成後

如果節點3和節點4上已啟用儲存加密、請完成一節 "在新的控制器模組上設定儲存加密"。否則、請完成本節 "取消委任舊系統"。

在新的控制器模組上設定儲存加密

如果新控制器的更換控制器或HA合作夥伴使用儲存加密、您必須設定新的儲存加密控制器模組、包括安裝SSL憑證和設定金鑰管理伺服器。

關於這項工作

此程序包括在新控制器模組上執行的步驟。您必須在正確的節點上輸入命令。

步驟

1. 確認金鑰管理伺服器仍可使用、狀態及驗證金鑰資訊：

   「安全金鑰管理程式外部顯示狀態」

   「安全金鑰管理程式內建show Backup」

2. 將上一步列出的金鑰管理伺服器新增至新控制器的金鑰管理伺服器清單。
   a. 新增金鑰管理伺服器：

      「安全金鑰管理程式外部附加伺服器-金鑰伺服器_key_manager_server_ip_address_」

   b. 針對每個列出的金鑰管理伺服器重複上一步。您最多可以連結四個金鑰管理伺服器。
   c. 確認已成功新增金鑰管理伺服器：

      「安全關鍵經理外部秀」

3. 在新的控制器模組上、執行金鑰管理設定精靈以設定及安裝金鑰管理伺服器。

   您必須安裝與現有控制器模組相同的金鑰管理伺服器。

   a. 在新節點上啟動金鑰管理伺服器設定精靈：

      「安全金鑰管理程式外部啟用」

   b. 完成精靈中的步驟以設定金鑰管理伺服器。
4. 將驗證金鑰從所有連結的金鑰管理伺服器還原至新節點：

「安全金鑰管理程式外部還原-node_new_控制 器名稱_」

在新的控制器模組上設定NetApp Volume或Aggregate Encryption

如果新控制器的更換控制器或高可用度（HA）合作夥伴使用NetApp Volume Encryption（NVE）或NetApp Aggregate Encryption（NAE）、您必須為NVE或NAE設定新的控制器模組。

關於這項工作

此程序包括在新控制器模組上執行的步驟。您必須在正確的節點上輸入命令。

內建金鑰管理程式

使用 Onboard Key Manager 設定 NVE 或 NAE 。

步驟

1. 將驗證金鑰從所有連結的金鑰管理伺服器還原至新節點：

   「安全金鑰管理程式內建同步」

外部金鑰管理

使用外部金鑰管理設定 NVE 或 NAE 。

步驟

1. 確認金鑰管理伺服器仍可使用、狀態及驗證金鑰資訊：

   「安全金鑰管理程式金鑰查詢節點節點」

2. 將上一步列出的金鑰管理伺服器新增至新控制器的金鑰管理伺服器清單：
   a. 新增金鑰管理伺服器：

      「安全金鑰管理程式外部附加伺服器-金鑰伺服器_key_manager_server_ip_address_」

   b. 針對每個列出的金鑰管理伺服器重複上一步。您最多可以連結四個金鑰管理伺服器。
   c. 確認已成功新增金鑰管理伺服器：

      「安全關鍵經理外部秀」

3. 在新的控制器模組上、執行金鑰管理設定精靈以設定及安裝金鑰管理伺服器。

   您必須安裝與現有控制器模組相同的金鑰管理伺服器。

   a. 在新節點上啟動金鑰管理伺服器設定精靈：

      「安全金鑰管理程式外部啟用」

   b. 完成精靈中的步驟以設定金鑰管理伺服器。
4. 將驗證金鑰從所有連結的金鑰管理伺服器還原至新節點：

   「安全金鑰管理程式外部還原」

   此命令需要OKM密碼

   如需詳細資訊、請參閱知識庫文章 "如何從 ONTAP 開機功能表還原外部金鑰管理程式伺服器組態"。

完成後

檢查是否有任何磁碟區因為驗證金鑰無法使用或無法連線到EKM伺服器而離線。使用「Volume online」命令將這些磁碟區重新連線。

取消委任舊系統

升級之後、您可以透過NetApp支援網站取消委任舊系統。汰換系統會告訴NetApp系統不再運作、並將其從支援資料庫中移除。

步驟

1. 請參閱 "參考資料" 連結至_NetApp支援網站_並登入。
2. 從功能表中選取*產品>我的產品*。
3. 在「檢視安裝的系統」頁面上、選擇您要用來顯示系統相關資訊的*選擇條件*。

   您可以選擇下列其中一項來找出您的系統：

   - 序號（位於裝置背面）
   - 「我的位置」的序號
4. 選取「執行！」

   表格會顯示叢集資訊、包括序號。
5. 在表中找到叢集、然後從「產品工具集」下拉式功能表中選取*「取消委任此系統*」。

恢復SnapMirror作業

您可以恢復在升級之前靜止的SnapMirror傳輸、並恢復SnapMirror關係。升級完成後、更新會如期進行。

步驟

1. 驗證目的地上的SnapMirror狀態：

   「napmirror show」
2. 恢復SnapMirror關係：

   ' napmirror resume -destination–vserver *vserver_name*'