設定安全金鑰
SANtricity 11.7

NetApp
February 12, 2024

目錄

設定安全金鑰

建立內部安全金鑰

若要使用「磁碟機安全性」功能、您可以建立內部安全金鑰、由儲存陣列中的控制器和具有安全功能的磁碟機共用。內部金鑰會保留在控制器的持續記憶體上。

開始之前

- 必須在儲存陣列中安裝具有安全功能的磁碟機。這些磁碟機可以是全磁碟加密（FDE）磁碟機、也可以是聯邦資訊處理標準（FIPS）磁碟機。
- 必須啟用磁碟機安全功能。否則、在此工作期間會開啟「無法建立安全金鑰」對話方塊。如有必要、請聯絡您的儲存設備廠商、以取得啟用磁碟機安全功能的指示。

如果儲存陣列中同時安裝FDE和FIPS磁碟機、則它們都會共用相同的安全金鑰。

關於這項工作

在此工作中、您可以定義要與內部安全金鑰建立關聯的識別碼和密碼。

磁碟機安全性密碼與儲存陣列的管理員密碼無關。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*建立內部金鑰*。

   如果您尚未產生安全性金鑰、則會開啟「建立安全性金鑰」對話方塊。

3. 在下列欄位中輸入資訊：

   - 定義安全金鑰識別碼-您可以接受預設值（儲存陣列名稱和時間戳記、由控制器韌體產生）、或輸入您自己的值。最多可輸入189個英數字元、不含空格、符號或符號。

     系統會自動產生其他字元、並附加到您輸入字串的兩端。產生的字元可確保識別碼是唯一的。

   - 定義密碼/重新輸入密碼-輸入並確認密碼。此值可包含8到32個字元、且必須包含下列各項：
     - 大寫字母（一個或多個）。請記住、密碼區分大小寫。
     - 數字（一或多個）。
     - 非英數字元、例如！、*、@（一或多個）。

     請務必記錄您的輸入項目以供日後使用。如果您需要從儲存陣列移除啟用安全功能的磁碟機、則必須知道識別碼和密碼、才能解除鎖定磁碟機資料。

4. 按一下「 * 建立 * 」。

   安全金鑰儲存在無法存取的控制器位置。除了實際的金鑰、還有一個加密的金鑰檔案、可從瀏覽器下載。

下載檔案的路徑可能取決於瀏覽器的預設下載位置。

5. 記錄您的金鑰識別碼、密碼和下載金鑰檔的位置、然後按一下*關閉*。

結果

您現在可以建立啟用安全功能的Volume群組或集區、也可以在現有的Volume群組和集區上啟用安全功能。

只要關閉磁碟機的電源、然後再次開啟、所有啟用安全功能的磁碟機都會變更為「安全性鎖定」狀態。在此狀態下、資料將無法存取、直到控制器在磁碟機初始化期間套用正確的安全金鑰為止。如果有人實際移除鎖定的磁碟機並將其安裝在其他系統中、安全鎖定狀態會防止未獲授權存取其資料。

完成後

您應該驗證安全金鑰、以確保金鑰檔案未毀損。

建立外部安全金鑰

若要將磁碟機安全功能搭配金鑰管理伺服器使用、您必須建立外部金鑰、並由金鑰管理伺服器和儲存陣列中具有安全功能的磁碟機共用。

開始之前

- 必須在陣列中安裝具有安全功能的磁碟機。這些磁碟機可以是全磁碟加密（FDE）磁碟機、也可以是聯邦資訊處理標準（FIPS）磁碟機。

  如果儲存陣列中同時安裝FDE和FIPS磁碟機、則它們都會共用相同的安全金鑰。

- 必須啟用磁碟機安全功能。否則、在此工作期間會開啟「無法建立安全金鑰」對話方塊。如有必要、請聯絡您的儲存設備廠商、以取得啟用磁碟機安全功能的指示。
- 您有已簽署的儲存陣列控制器用戶端憑證檔案、而且您已將該檔案複製到您正在存取System Manager的主機。用戶端憑證會驗證儲存陣列的控制器、因此金鑰管理伺服器可以信任其金鑰管理互通性傳輸協定（KMIP）要求。
- 您必須從金鑰管理伺服器擷取憑證檔案、然後將該檔案複製到您正在存取System Manager的主機。金鑰管理伺服器憑證會驗證金鑰管理伺服器、因此儲存陣列可以信任其IP位址。您可以將根、中繼或伺服器憑證用於金鑰管理伺服器。

  如需伺服器憑證的詳細資訊、請參閱金鑰管理伺服器的文件。

關於這項工作

在此工作中、您可以定義金鑰管理伺服器的IP位址及其使用的連接埠號碼、然後載入憑證以進行外部金鑰管理。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*建立外部金鑰*。

如果目前已設定內部金鑰管理、會開啟一個對話方塊、要求您確認是否要切換至外部金鑰管理。

「建立外部安全金鑰」對話方塊隨即開啟。

3. 在「連線至金鑰伺服器」下、於下列欄位中輸入資訊。
   - 金鑰管理伺服器位址-輸入用於金鑰管理之伺服器的完整網域名稱或IP位址（IPv4或IPv6）。
   - 金鑰管理連接埠號碼-輸入KMIP通訊所使用的連接埠號碼。用於金鑰管理伺服器通訊的最常見連接埠號碼為5696。

     選用：*如果您要設定備份金鑰伺服器、請按一下*新增金鑰伺服器、然後輸入該伺服器的資訊。如果無法連線至主金鑰伺服器、則會使用第二個金鑰伺服器。請確定每個金鑰伺服器都能存取相同的金鑰資料庫、否則陣列將會張貼錯誤、而且無法使用備份伺服器。

     一次只使用單一金鑰伺服器。如果儲存陣列無法連線至主要金鑰伺服器、陣列將會聯絡備份金鑰伺服器。請注意、您必須在兩部伺服器之間維持同位元檢查、否則可能導致錯誤。

   - 選擇用戶端憑證-按一下第一個*瀏覽*按鈕、選取儲存陣列控制器的憑證檔案。
   - 選擇金鑰管理伺服器的伺服器憑證-按第二個*瀏覽*按鈕、選取金鑰管理伺服器的憑證檔案。您可以為金鑰管理伺服器選擇根、中繼或伺服器憑證。
4. 單擊 * 下一步 * 。
5. 在「建立/備份金鑰」下、您可以建立備份金鑰以確保安全。
   - （建議）若要建立備份金鑰、請保持核取方塊為選取狀態、然後輸入並確認密碼。此值可包含8到32個字元、且必須包含下列各項：
     - 大寫字母（一個或多個）。請記住、密碼區分大小寫。
     - 數字（一或多個）。
     - 非英數字元、例如！、*、@（一或多個）。

     請務必記錄您的輸入項目以供日後使用。如果您需要從儲存陣列中移除已啟用安全功能的磁碟機、您必須知道解鎖磁碟機資料的密碼。

   +
   - 如果您不想建立備份金鑰、請取消選取核取方塊。

     請注意、如果您失去外部金鑰伺服器的存取權、而且您沒有備份金鑰、則當磁碟機移轉至其他儲存陣列時、您將無法存取這些磁碟機上的資料。此選項是在System Manager中建立備份金鑰的唯一方法。

6. 單擊*完成*。

系統會以您輸入的認證資料連線至金鑰管理伺服器。然後安全金鑰複本會儲存在您的本機系統上。

下載檔案的路徑可能取決於瀏覽器的預設下載位置。

7. 記下您的密碼和下載金鑰檔的位置、然後按一下*關閉*。

   此頁面會顯示下列訊息、並提供外部金鑰管理的其他連結：

   ```
   Current key management method: External
   ```

8. 選取*測試通訊*來測試儲存陣列與金鑰管理伺服器之間的連線。

   測試結果會顯示在對話方塊中。

結果

啟用外部金鑰管理時、您可以建立啟用安全功能的Volume群組或集區、也可以在現有的Volume群組和集區上啟用安全功能。

> 只要關閉磁碟機的電源、然後再次開啟、所有啟用安全功能的磁碟機都會變更為「安全性鎖定」狀態。在此狀態下、資料將無法存取、直到控制器在磁碟機初始化期間套用正確的安全金鑰為止。如果有人實際移除鎖定的磁碟機並將其安裝在其他系統中、安全鎖定狀態會防止未獲授權存取其資料。

完成後

您應該驗證安全金鑰、以確保金鑰檔案未毀損。