



安全金鑰管理 SANtricity 11.5

NetApp
February 12, 2024

目錄

安全金鑰管理	1
概念	1
使用方法	4
常見問題集	12

安全金鑰管理

概念

磁碟機安全功能的運作方式

磁碟機安全性是一項儲存陣列功能、可透過全磁碟加密（FDE）磁碟機或聯邦資訊處理標準（FIPS）磁碟機提供額外的安全層級。當這些磁碟機搭配磁碟機安全功能使用時、它們需要安全金鑰才能存取其資料。當磁碟機從陣列中實際移除時、除非安裝在另一個陣列中、否則無法運作、此時磁碟機將處於「安全性鎖定」狀態、直到提供正確的安全金鑰為止。

如何實作磁碟機安全性

若要實作磁碟機安全性、請執行下列步驟。

1. 為您的儲存陣列配備可安全使用的磁碟機、包括FDE磁碟機或FIPS磁碟機。（對於需要FIPS支援的磁碟區、請僅使用FIPS磁碟機。在磁碟區群組或集區中混合使用FIPS和FDE磁碟機、將會將所有磁碟機視為FDE磁碟機。此外、FDE磁碟機無法新增至All FIPS Volume群組或Pool、也無法作為備援磁碟機使用。）
2. 建立安全金鑰、這是控制器和磁碟機共用的字元字串、用於讀取/寫入存取。您可以從控制器的持續記憶體建立內部金鑰、或從金鑰管理伺服器建立外部金鑰。若要管理外部金鑰、必須使用金鑰管理伺服器建立驗證。
3. 為集區和磁碟區群組啟用磁碟機安全性：
 - 建立集區或磁碟區群組（請在候選資料表的「安全功能」欄中尋找*「是」）。
 - 當您建立新的Volume時、請選取資源池或Volume群組（請在「資源池和Volume群組候選項目」表中、尋找「安全功能」旁邊的*「是*」）。

磁碟機安全性如何在磁碟機層級運作

具有安全功能的磁碟機（FDE或FIPS）會在寫入期間加密資料、並在讀取期間解密資料。此加密和解密不會影響效能或使用者工作流程。每個磁碟機都有其專屬的加密金鑰、永遠無法從磁碟機傳輸。

磁碟機安全功能可透過安全的磁碟機提供額外的保護層。當這些磁碟機上的磁碟區群組或集區被選為「磁碟機安全性」時、磁碟機會先尋找安全金鑰、然後才允許存取資料。您可以隨時為集區和磁碟區群組啟用磁碟機安全功能、而不會影響磁碟機上的現有資料。不過、您必須清除磁碟機上的所有資料、才能停用磁碟機安全性。

磁碟機安全性如何在儲存陣列層級運作

有了磁碟機安全功能、您就能建立安全金鑰、並在儲存陣列中啟用安全功能的磁碟機和控制器之間共用。只要關閉和開啟磁碟機的電源、安全啟用的磁碟機就會變更為安全鎖定狀態、直到控制器套用安全金鑰為止。

如果從儲存陣列移除啟用安全功能的磁碟機、然後重新安裝到不同的儲存陣列、磁碟機將會處於「安全性鎖定」狀態。重新定位的磁碟機會先尋找安全金鑰、然後才能再次存取資料。若要解除資料鎖定、請從來源儲存陣列套用安全金鑰。成功解除鎖定程序之後、重新定位的磁碟機會使用已儲存在目標儲存陣列中的安全金鑰、而且不再需要匯入的安全金鑰檔案。



對於內部金鑰管理、實際的安全金鑰會儲存在無法存取的控制器位置。它不是人類可讀的格式、也不是使用者可存取的格式。

磁碟機安全性如何在磁碟區層級運作

當您從具有安全功能的磁碟機建立集區或磁碟區群組時、也可以針對這些集區或磁碟區群組啟用「磁碟機安全性」。「磁碟機安全性」選項可讓磁碟機及相關的磁碟區群組和集區安全無虞、而且啟用安全無虞。

在建立啟用安全功能的Volume群組和集區之前、請務必記住下列準則：

- Volume群組和集區必須完全由具有安全功能的磁碟機所組成。（對於需要FIPS支援的磁碟區、請僅使用FIPS磁碟機。在磁碟區群組或集區中混合使用FIPS和FDE磁碟機、將會將所有磁碟機視為FDE磁碟機。此外、FDE磁碟機無法新增至All FIPS Volume群組或Pool、也無法作為備援磁碟機使用。）
- Volume群組和集區必須處於最佳狀態。

安全金鑰管理的運作方式

當您實作磁碟機安全功能時、啟用安全功能的磁碟機（FIPS或FDE）需要安全金鑰才能存取資料。安全金鑰是一串字元、可在這些類型的磁碟機和儲存陣列中的控制器之間共用。

只要關閉和開啟磁碟機的電源、安全啟用的磁碟機就會變更為安全鎖定狀態、直到控制器套用安全金鑰為止。如果從儲存陣列中移除啟用安全功能的磁碟機、則磁碟機的資料會被鎖定。當磁碟機重新安裝在不同的儲存陣列中時、它會先尋找安全金鑰、然後再讓資料再次存取。若要解除資料鎖定、您必須套用原始的安全金鑰。

您可以使用下列其中一種方法來建立及管理安全性金鑰：

- 控制器持續記憶體的內部金鑰管理。
- 外部金鑰管理伺服器上的外部金鑰管理。

內部金鑰管理

內部金鑰會保留在控制器的持續記憶體上。若要實作內部金鑰管理、請執行下列步驟：

1. 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。
2. 確定磁碟機安全功能已啟用。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。
3. 建立內部安全金鑰、其中包括定義識別碼和密碼。識別碼是與安全金鑰相關聯的字串、儲存在控制器和與金鑰相關聯的所有磁碟機上。密碼用於加密安全金鑰以供備份之用。若要建立內部金鑰、請前往功能表：設定[系統>安全金鑰管理>建立內部金鑰]。

安全金鑰儲存在無法存取的控制位置。然後您可以建立啟用安全功能的Volume群組或集區、或是在現有的Volume群組和集區上啟用安全功能。

外部金鑰管理

外部金鑰是使用金鑰管理互通性傳輸協定（KMIP）、在獨立的金鑰管理伺服器上維護。若要實作外部金鑰管理、請執行下列步驟：

1. 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。
2. 確定磁碟機安全功能已啟用。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。
3. 完成並下載用戶端憑證簽署要求（CSR）、以便在儲存陣列與金鑰管理伺服器之間進行驗證。前往功能表：


設定[憑證>金鑰管理>完整的CSR]。

4. 使用下載的CSR檔案、從金鑰管理伺服器建立及下載用戶端憑證。
5. 請確定本機主機上有可用的用戶端憑證和金鑰管理伺服器的憑證複本。
6. 建立外部金鑰、包括定義金鑰管理伺服器的IP位址、以及KMIP通訊所使用的連接埠號碼。在此過程中、您也會載入憑證檔案。若要建立外部金鑰、請移至功能表：設定[系統>安全金鑰管理>建立外部金鑰]。

系統會以您輸入的認證資料連線至金鑰管理伺服器。然後您可以建立啟用安全功能的Volume群組或集區、或是在現有的Volume群組和集區上啟用安全功能。

推動安全性術語

瞭解磁碟機安全性條款如何適用於您的儲存陣列。

期限	說明
磁碟機安全功能	磁碟機安全性是一項儲存陣列功能、可透過全磁碟加密（FDE）磁碟機或聯邦資訊處理標準（FIPS）磁碟機提供額外的安全層級。當這些磁碟機搭配磁碟機安全功能使用時、它們需要安全金鑰才能存取其資料。當磁碟機從陣列中實際移除時、除非安裝在另一個陣列中、否則無法運作、此時磁碟機將處於「安全性鎖定」狀態、直到提供正確的安全金鑰為止。
FDE磁碟機	全磁碟加密（FDE）磁碟機在硬體層級對磁碟機執行加密。硬碟內含ASIC晶片、可在寫入期間加密資料、然後在讀取期間解密資料。
FIPS磁碟機	FIPS磁碟機使用聯邦資訊處理標準（FIPS）140-2第2級。它們基本上是FDE磁碟機、符合美國政府的標準、以確保強大的加密演算法和方法。FIPS磁碟機的安全性標準高於FDE磁碟機。
管理用戶端	本機系統（電腦、平板電腦等）、內含瀏覽器、可供存取System Manager。
密碼	<p>密碼用於加密安全金鑰以供備份之用。在磁碟機移轉或頭端切換後匯入備份安全金鑰時、必須提供用於加密安全金鑰的相同密碼。通關詞可以介於8到32個字元之間。</p> <div><p>磁碟機安全性密碼與儲存陣列的管理員密碼無關。</p></div>

期限	說明
具備安全功能的磁碟機	可安全使用的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、在讀取期間加密資料並解密資料。這些磁碟機被視為安全的磁碟機、因為它們可以使用磁碟機安全功能來提高安全性。如果已針對這些磁碟機所使用的磁碟區群組和集區啟用「磁碟機安全性」功能、磁碟機就會變成安全的- <i>enabled</i> 。
啟用安全功能的磁碟機	啟用安全功能的磁碟機可搭配磁碟機安全功能使用。當您啟用「磁碟機安全性」功能、然後將「磁碟機安全性」套用至安全的磁碟機上的集區或磁碟區群組時、磁碟機就會變成安全的已啟用。讀寫存取只能透過設定正確安全金鑰的控制器來使用。這項新增的安全功能可防止未獲授權存取從儲存陣列實體移除之磁碟機上的資料。
安全金鑰	<p>安全金鑰是儲存陣列中啟用安全功能的磁碟機與控制器之間共用的字元字串。只要關閉和開啟磁碟機的電源、安全啟用的磁碟機就會變更為安全鎖定狀態、直到控制器套用安全金鑰為止。如果從儲存陣列中移除啟用安全功能的磁碟機、則磁碟機的資料會被鎖定。當磁碟機重新安裝在不同的儲存陣列中時、它會先尋找安全金鑰、然後再讓資料再次存取。若要解除資料鎖定、您必須套用原始的安全金鑰。您可以使用下列其中一種方法來建立及管理安全性金鑰：</p> <ul style="list-style-type: none"> • 內部金鑰管理：在控制器的持續記憶體上建立及維護安全金鑰。 • 外部金鑰管理：在外部金鑰管理伺服器上建立及維護安全金鑰。
安全金鑰識別碼	安全性金鑰識別碼是在金鑰建立期間與安全性金鑰相關聯的字串。識別碼儲存在控制器和所有與安全金鑰相關聯的磁碟機上。

使用方法

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，將在此工作期間開啟*無法建立安全性金鑰*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金鑰、則會開啟「建立安全金鑰」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，將在此工作期間開啟*無法建立安全性金鑰*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。
- 用戶端和伺服器憑證可在本機主機上取得、因此儲存陣列和金鑰管理伺服器可以相互驗證。用戶端憑證會驗證控制器、而伺服器憑證則會驗證金鑰管理伺服器。

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）。
 - 金鑰管理連接埠編號：輸入金鑰管理互通性傳輸協定（KMIP）通訊所使用的連接埠編號。用於金鑰管理伺服器通訊的最常見連接埠號碼為5696。
 - 選擇「用戶端憑證」-按一下「第一次瀏覽」按鈕、選取儲存陣列控制器的憑證檔案。
 - 選取金鑰管理伺服器的伺服器憑證：按一下第二個「瀏覽」按鈕、選取金鑰管理伺服器的憑證檔案。
4. 單擊 * 下一步 *。
5. 在*建立/備份金鑰*下、於下列欄位中輸入資訊：
 - 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。

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：

「目前的金鑰管理方法：外部」

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。

變更安全金鑰

您隨時都可以用新的金鑰來取代安全性金鑰。如果您的公司可能發生安全漏洞、而且想要確保未獲授權的人員無法存取磁碟機的資料、您可能需要變更安全金鑰。

開始之前

安全金鑰已存在。

關於這項工作

本工作說明如何變更安全性金鑰、並以新的金鑰取代。完成此程序之後、舊金鑰即會失效。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*變更金鑰*。

「變更安全金鑰」對話方塊隨即開啟。

3. 在下列欄位中輸入資訊。

- 定義安全金鑰識別碼（僅限內部安全金鑰）。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。



其他字元會自動產生、並附加到您輸入字串的兩端。產生的字元有助於確保識別碼是唯一的。

- 定義密碼/重新輸入密碼-在每個欄位中、輸入您的密碼。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）。



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

4. 按一下 * 變更 *。

新的安全性金鑰會覆寫先前的金鑰、但不再有效。



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*。

完成後

您應該驗證安全金鑰、以確保金鑰檔案未毀損。

從外部金鑰管理切換至內部金鑰管理

您可以將磁碟機安全性的管理方法從外部金鑰伺服器變更為儲存陣列所使用的內部方法。先前為外部金鑰管理所定義的安全金鑰、將用於內部金鑰管理。

開始之前

已建立外部金鑰。

關於這項工作

在此工作中、您將停用外部金鑰管理、並將新的備份複本下載到本機主機。現有的金鑰仍用於磁碟機安全性、但會在儲存陣列內部進行管理。

步驟

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

「停用外部金鑰管理」對話方塊隨即開啟。

3. 在*定義密語/重新輸入密語*中、輸入並確認密鑰備份的密語。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*停用*。

備份金鑰會下載到您的本機主機。

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

磁碟機安全性現在是透過儲存陣列進行內部管理。

完成後

- 您應該驗證安全金鑰、以確保金鑰檔案未毀損。

編輯金鑰管理伺服器設定

如果您已設定外部金鑰管理、則可以隨時檢視及編輯金鑰管理伺服器設定。

開始之前

必須設定外部金鑰管理。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*檢視/編輯金鑰管理伺服器設定*。
3. 在下列欄位中編輯資訊：
 - 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）。
 - KMIP連接埠號碼-輸入金鑰管理互通性傳輸協定（KMIP）通訊所使用的連接埠號碼。
4. 按一下「*儲存*」。

備份安全金鑰

建立或變更安全性金鑰之後、您可以建立金鑰檔的備份複本、以防原始檔案毀損。

開始之前

- 安全金鑰已存在。

關於這項工作

本工作說明如何備份您先前建立的安全金鑰。在此程序中、您會建立新的密碼來進行備份。此密碼不需要符合原始金鑰建立或上次變更時所使用的密碼。密碼只會套用至您正在建立的備份。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*備份金鑰*。

此時將打開*備份安全密鑰*對話框。

3. 在*定義密碼/重新輸入密碼*欄位中、輸入並確認此備份的密碼。

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）
- 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內容、以便日後使用。您需要密碼才能存取此安全性金鑰的備份。

4. 按一下*備份*。

安全金鑰的備份會下載到您的本機主機、然後會開啟「確認/記錄安全金鑰備份」對話方塊。



下載的安全金鑰檔案路徑可能取決於瀏覽器的預設下載位置。

5. 在安全位置記錄您的通關密碼、然後按一下*關閉*。

完成後

您應該驗證備份安全金鑰。

驗證安全金鑰

您可以驗證安全性金鑰、以確保其未毀損、並驗證密碼是否正確。

開始之前

已建立安全金鑰。

關於這項工作

本工作說明如何驗證您先前建立的安全金鑰。這是確保金鑰檔未毀損且密碼正確的重要步驟、如此可確保您在日後將啟用安全功能的磁碟機從一個儲存陣列移至另一個儲存陣列時、能夠存取磁碟機資料。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*驗證金鑰*。

「驗證安全金鑰」對話方塊隨即開啟。

3. 按一下「瀏覽」、然後選取金鑰檔（例如「drivesecure.slk」）。
4. 輸入與所選金鑰相關的密碼。

當您選取有效的金鑰檔和密碼時、*驗證*按鈕就會變成可用的。

5. 按一下*驗證*。

驗證結果會顯示在對話方塊中。

6. 如果結果顯示「安全金鑰已成功驗證」、請按一下*關閉*。如果出現錯誤訊息、請遵循對話方塊中顯示的建議指示。

使用安全金鑰解除磁碟機鎖定

如果您將啟用安全功能的磁碟機從一個儲存陣列移至另一個儲存陣列、則必須將適當的安全金鑰匯入新的儲存陣列。匯入金鑰會解除鎖定磁碟機上的資料。

開始之前

- 目標儲存陣列（您要移動磁碟機的位置）必須已設定安全金鑰。移轉的磁碟機將重新輸入目標儲存陣列。
- 您必須知道要解除鎖定之磁碟機的相關安全性金鑰。
- 安全金鑰檔案可在管理用戶端上使用（使用瀏覽器存取System Manager的系統）。如果您要將磁碟機移至由不同系統管理的儲存陣列、則必須將安全金鑰檔案移至該管理用戶端。

關於這項工作

本工作說明如何解除鎖定已從儲存陣列移除並重新安裝至其他磁碟機的安全磁碟機中的資料。陣列發現磁碟機後、會出現「Needs Attention（需要注意）」條件、並顯示這些重新定位磁碟機的「Security Key Needs（需要安全金鑰）」狀態。您可以將磁碟機資料的安全金鑰匯入儲存陣列、以解除鎖定磁碟機資料。在此過程中、您可以選取安全金鑰檔案、然後輸入金鑰的密碼。



密碼與儲存陣列的管理員密碼不同。

如果新儲存陣列中安裝了其他已啟用安全功能的磁碟機、它們可能會使用與您匯入磁碟機不同的安全金鑰。在匯入程序期間、舊的安全金鑰僅用於解除鎖定您要安裝之磁碟機的資料。當解除鎖定程序成功時、新安裝的磁碟機會重新鎖定至目標儲存陣列的安全金鑰。

步驟

1. 選取功能表：設定[系統]。
2. 在*安全金鑰管理*下、選取*解除鎖定安全磁碟機*。

「解除鎖定安全磁碟機」對話方塊隨即開啟。任何需要安全金鑰的磁碟機都會顯示在表格中。

3. 您也可以將滑鼠游標移到磁碟機編號上、查看磁碟機的位置（機櫃編號和機櫃編號）。
4. 按一下*瀏覽*、然後選取與您要解除鎖定磁碟機對應的安全金鑰檔案。

您選取的金鑰檔會出現在對話方塊中。

5. 輸入與此金鑰檔相關的密碼。

您輸入的字元會被遮罩。

6. 按一下*解除鎖定*。

如果解除鎖定作業成功、對話方塊會顯示：「相關的安全磁碟機已解除鎖定。」

結果

當所有磁碟機都已鎖定、然後解除鎖定时、儲存陣列中的每個控制器都會重新開機。但是、如果目標儲存陣列中已有未鎖定的磁碟機、則控制器將不會重新開機。

常見問題集

在建立安全金鑰之前、我需要知道什麼？

安全金鑰由儲存陣列內的控制器和啟用安全功能的磁碟機共用。如果從儲存陣列中移除啟用安全功能的磁碟機、安全金鑰會保護資料免於未經授權的存取。

您可以使用下列其中一種方法來建立及管理安全性金鑰：

- 控制器持續記憶體的內部金鑰管理。
- 外部金鑰管理伺服器上的外部金鑰管理。

在建立內部安全金鑰之前、您必須執行下列動作：

1. 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。
2. 確定磁碟機安全功能已啟用。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。

然後您可以建立內部安全金鑰、其中包括定義識別碼和密碼。識別碼是與安全金鑰相關聯的字串、儲存在控制器和與金鑰相關聯的所有磁碟機上。密碼用於加密安全金鑰以供備份之用。完成後、安全金鑰會儲存在無法存取的控制器位置。然後您可以建立啟用安全功能的Volume群組或集區、或是在現有的Volume群組和集區上啟用安全功能。

在建立外部安全金鑰之前、您必須執行下列動作：

1. 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。
2. 確定磁碟機安全功能已啟用。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。
3. 完成並下載用戶端憑證簽署要求（CSR）、以便在儲存陣列與金鑰管理伺服器之間進行驗證。前往功能表：設定[憑證>金鑰管理>完整的CSR]。
4. 使用下載的CSR檔案、從金鑰管理伺服器建立及下載用戶端憑證。
5. 請確定本機主機上有可用的用戶端憑證和金鑰管理伺服器的憑證複本。

然後您可以建立外部金鑰、其中包括定義金鑰管理伺服器的IP位址、以及KMIP通訊所使用的連接埠號碼。在此過程中、您也會載入憑證檔案。完成後、系統會以您輸入的認證資料連線至金鑰管理伺服器。然後您可以建立啟用安全功能的Volume群組或集區、或是在現有的Volume群組和集區上啟用安全功能。

為什麼我需要定義密碼？

密碼用於加密及解密儲存在本機管理用戶端上的安全金鑰檔案。如果安全金鑰重新安裝在另一個儲存陣列中、則沒有密碼、就無法解密安全金鑰、也無法用來解除鎖定已啟用安全功能的磁碟機中的資料。

為何務必記錄安全金鑰資訊？

如果您遺失安全金鑰資訊且沒有備份、則在重新部署啟用安全功能的磁碟機或升級控制器時、可能會遺失資料。您需要安全金鑰才能解除鎖定磁碟機上的資料。

請務必記錄安全金鑰識別碼、關聯的密碼、以及安全金鑰檔案儲存所在的本機主機位置。

備份安全金鑰之前、我需要知道什麼？

如果您的原始安全金鑰毀損、而且您沒有備份、則當磁碟機從一個儲存陣列移轉到另一個儲存陣列時、您將無法存取這些資料。

在備份安全金鑰之前、請謹記下列準則：

- 請確定您知道原始金鑰檔的安全金鑰識別碼和密碼。



只有內部金鑰使用識別碼。當您建立識別碼時、會自動產生其他字元、並附加到識別碼字串的兩端。產生的字元可確保識別碼是唯一的。

- 您可以為備份建立新的密碼。此密碼不需要符合原始金鑰建立或上次變更時所使用的密碼。密碼只會套用至您所建立的備份。



「磁碟機安全性」密碼不應與儲存陣列的管理員密碼混淆。磁碟機安全性密碼可保護安全金鑰的備份。系統管理員密碼可保護整個儲存陣列、避免遭到未獲授權的存取。

- 備份安全金鑰檔案會下載到您的管理用戶端。下載檔案的路徑可能取決於瀏覽器的預設下載位置。請務必記錄安全金鑰資訊的儲存位置。

在解除鎖定安全磁碟機之前、我需要知道什麼？

若要從移轉至新儲存陣列的安全磁碟機解除資料鎖定、您必須匯入其安全金鑰。

在解除鎖定啟用安全功能的磁碟機之前、請謹記下列準則：

- 目標儲存陣列（您要移動磁碟機的位置）必須已有安全金鑰。移轉的磁碟機將重新輸入目標儲存陣列。
- 對於您要移轉的磁碟機、您知道安全金鑰識別碼和安全金鑰檔案對應的密碼。
- 安全金鑰檔案可在管理用戶端上使用（使用瀏覽器存取System Manager的系統）。

什麼是讀寫存取能力？

「磁碟機設定」視窗包含*磁碟機安全性*屬性的相關資訊。「讀取/寫入存取」是在磁碟機資料已鎖定時顯示的其中一個屬性。

若要檢視*磁碟機安全性*屬性、請前往「硬體」頁面。選取磁碟機、按一下*檢視設定*、然後按一下*顯示更多設定*。在頁面底部、磁碟機解鎖時、讀取/寫入存取屬性值為*是*。磁碟機鎖定時、讀取/寫入存取屬性值為*否、無效的安全金鑰*。您可以匯入安全金鑰來解除鎖定安全磁碟機（前往功能表：設定[系統>解除鎖定安全磁碟機]）。

驗證安全金鑰需要知道什麼？

建立安全金鑰之後、您應該驗證金鑰檔、以確保它不會毀損。

如果驗證失敗、請執行下列動作：

- 如果安全金鑰識別碼與控制器上的識別碼不符、請找出正確的安全金鑰檔案、然後再試一次驗證。
- 如果控制器無法解密安全金鑰以進行驗證、您可能輸入的密碼不正確。請仔細檢查密碼、必要時重新輸入密碼、然後再次嘗試驗證。如果錯誤訊息再次出現、請選取金鑰檔的備份（若有）、然後重新嘗試驗證。
- 如果仍無法驗證安全金鑰、則原始檔案可能已毀損。建立金鑰的新備份並驗證該複本。

內部安全金鑰與外部安全金鑰管理有何不同？

當您實作*磁碟機安全性*功能時、您可以使用內部安全金鑰或外部安全金鑰、在從儲存陣列移除已啟用安全功能的磁碟機時鎖定資料。

安全金鑰是一串字元、可在已啟用安全功能的磁碟機和儲存陣列中的控制器之間共用。內部金鑰會保留在控制器的持續記憶體上。外部金鑰是使用金鑰管理互通性傳輸協定（KMIP）、在獨立的金鑰管理伺服器上維護。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。