系統
SANtricity 11.5

NetApp
February 12, 2024

目錄

系統 1
儲存陣列設定 1
iSCSI設定 13
系統：NVMe設定 26
附加功能 33
安全金鑰管理 36

系統

儲存陣列設定

概念

快取設定與效能

快取記憶體是控制器上暫用揮發性儲存設備的區域、存取時間比磁碟機媒體快。

透過快取、整體I/O效能可提升如下：

- 從主機要求讀取的資料可能已經在先前作業的快取中、因此不需要存取磁碟機。
- 寫入資料一開始會寫入快取、如此可釋出應用程式以繼續執行、而不需等待資料寫入磁碟機。

預設的快取設定符合大多數環境的需求、但您可以視需要加以變更。

儲存陣列快取設定

對於儲存陣列中的所有磁碟區、您可以從「System（系統）」頁面指定下列值：

- 清空的開始值：快取中觸發快取清空（寫入磁碟）的未寫入資料百分比。當快取保留指定的未寫入資料開始百分比時、就會觸發排清。依預設、當快取達到80%的完整容量時、控制器會開始排清快取。
- 快取區塊大小：每個快取區塊的最大大小、這是快取管理的組織單位。快取區塊大小預設為8 KiB、但可以設定為4、8、16或32 KiB。理想情況下、快取區塊大小應設定為應用程式的主要I/O大小。檔案系統或資料庫應用程式通常使用較小的大小、而較大的大小則適合需要大量資料傳輸或連續I/O的應用程式

Volume快取設定

對於儲存陣列中的個別磁碟區、您可以從「Volumes（磁碟區）」頁面（功能表：Storage[Volumes]）指定下列值：

- 讀取快取-讀取快取是儲存已從磁碟機讀取之資料的緩衝區。讀取作業的資料可能已經在先前作業的快取中、因此不需要存取磁碟機。資料會保留在讀取快取中、直到資料被清除為止。
  - 動態讀取快取預先擷取-動態快取讀取預先擷取可讓控制器在讀取磁碟機至快取的資料區塊時、將其他循序資料區塊複製到快取中。此快取可增加日後從快取中填入資料要求的機會。對於使用連續I/O的多媒體應用程式而言、動態快取讀取預先擷取非常重要預先擷取至快取的資料速率和數量、是根據主機讀取的速率和要求大小而自行調整。隨機存取不會將資料預先擷取至快取。停用讀取快取時、此功能不適用。
- 寫入快取：寫入快取是一種緩衝區、用於儲存來自主機的資料、但尚未寫入磁碟機。資料會保留在寫入快取中、直到寫入磁碟機為止。寫入快取可提高I/O效能。

> 可能會遺失資料：如果您啟用*寫入快取（不含電池）選項、而且沒有通用電源供應器來提供保護、則可能會遺失資料。此外、如果您沒有控制器電池、並且啟用「無電池寫入快取」選項、可能會遺失資料。

  - 無電池寫入快取-無電池寫入快取設定可讓寫入快取繼續、即使電池遺失、故障、電力完全耗盡或未充滿電也沒問題。通常不建議選擇不含電池的寫入快取、因為如果電力中斷、資料可能會遺失。一般而言、寫入快取會由控制器暫時關閉、直到電池充電或更換故障電池為止。

- 使用鏡射寫入快取-寫入快取搭配鏡射會在寫入某個控制器快取記憶體的資料同時寫入另一個控制器的快取記憶體時發生。因此、如果一個控制器故障、另一個控制器就能完成所有未完成的寫入作業。只有啟用寫入快取且存在兩個控制器時、才能使用寫入快取鏡射。使用鏡射進行寫入快取是建立磁碟區的預設設定。

自動負載平衡總覽

自動負載平衡功能可動態回應一段時間內的負載變更、並自動調整Volume控制器擁有權、以修正工作負載在控制器之間移動時發生的任何負載不平衡問題、進而改善I/O資源管理。

每個控制器的工作負載都會持續受到監控、並可在主機上安裝多重路徑驅動程式的協助下、在必要時自動取得平衡。當工作負載在各個控制器之間自動重新平衡時、儲存管理員可免除手動調整Volume控制器所有權以因應儲存陣列負載變更的負擔。

啟用「自動負載平衡」時、會執行下列功能：

- 自動監控及平衡控制器資源使用率。
- 視需要自動調整Volume控制器擁有權、藉此最佳化主機與儲存陣列之間的I/O頻寬。

啟用和停用自動負載平衡

所有儲存陣列預設會啟用自動負載平衡。

基於下列原因、您可能想要停用儲存陣列上的自動負載平衡：

- 您不想自動變更特定磁碟區的控制器擁有權、以平衡工作負載。
- 您所在的環境經過高度調校、有針對性地設定負載分配、以便在控制器之間達成特定的分配。

支援自動負載平衡功能的主機類型

即使已在儲存陣列層級啟用自動負載平衡、您為主機或主機叢集所選取的主機類型仍會直接影響該功能的運作方式。

在控制器之間平衡儲存陣列的工作負載時、「自動負載平衡」功能會嘗試移動兩個控制器都能存取、且只對應到能夠支援「自動負載平衡」功能的主機或主機叢集的磁碟區。

這種行為可防止主機因為負載平衡程序而失去對磁碟區的存取權；不過、對應到不支援自動負載平衡之主機的磁碟區存在、會影響儲存陣列平衡工作負載的能力。為了讓自動負載平衡能夠平衡工作負載、多重路徑驅動程式必須支援TPGS、且主機類型必須包含在下表中。

若要將主機叢集視為能夠自動負載平衡、該群組中的所有主機都必須能夠支援自動負載平衡。

支援自動負載平衡的主機類型	使用此多重路徑驅動程式
Windows或Windows叢集	採用NetApp E系列DSM的MPIO
Linux DM-MP（核心3.10或更新版本）	DM-MP搭配「scsi _dh _alua」裝置處理常式

支援自動負載平衡的主機類型	使用此多重路徑驅動程式
VMware	原生多路徑外掛程式（NMP）、 含「VMW_SATP_ALUA Storage Array Type」外掛程式

> 除了次要例外、不支援自動負載平衡的主機類型、無論是否啟用此功能、都會繼續正常運作。一個例外是、如果系統有容錯移轉、儲存陣列會在資料路徑傳回時、將未對應或未指派的磁碟區移回擁有控制器。不會移動任何對應或指派給非自動負載平衡主機的磁碟區。

請參閱 "互通性對照表工具" 以取得特定多重路徑驅動程式、作業系統層級和控制器磁碟機匣支援的相容性資訊。

驗證作業系統與自動負載平衡功能的相容性

在設定新（或移轉現有）系統之前、請先確認作業系統與自動負載平衡功能的相容性。

1. 前往 "互通性對照表工具" 尋找您的解決方案並驗證支援。

   如果您的系統執行的是Red Hat Enterprise Linux 6或SUSE Linux Enterprise Server 11、請聯絡技術支援部門。

2. 更新並設定「/etc/multipath.conf檔案」。
3. 請確認適用廠商和產品的「目錄附加裝置處理常式」和「目錄優先」都設為「是」、或使用預設設定。

預設主機作業系統類型

最初連接主機時、儲存陣列會使用預設的主機類型。它定義了儲存陣列中的控制器在存取磁碟區時、如何與主機作業系統搭配運作。如果需要變更儲存陣列的運作方式（相對於連接的主機）、您可以變更主機類型。

一般而言、在將主機連線至儲存陣列或連接其他主機之前、您會先變更預設的主機類型。

請謹記以下準則：

- 如果您打算連線至儲存陣列的所有主機都有相同的作業系統（同質主機環境）、請變更主機類型以符合作業系統。
- 如果您打算連線至儲存陣列（異質主機環境）的主機具有不同的作業系統、請變更主機類型以符合大多數主機作業系統。

  例如、如果您要將八個不同的主機連線至儲存陣列、而其中六個主機執行Windows作業系統、則必須選取Windows作為預設的主機作業系統類型。

- 如果大多數連線的主機都有不同的作業系統、請將主機類型變更為出廠預設值。

  例如、如果您要將八個不同的主機連線至儲存陣列、而其中兩個主機執行Windows作業系統、則有三個主機執行HP-UX作業系統、 另外三種作業系統是執行Linux作業系統、您必須選取「Factory Default」作為預設主機作業系統類型。

使用方法

編輯儲存陣列名稱

您可以變更SANtricity 出現在「菜單系統管理程式」標題列中的儲存陣列名稱。

步驟

1. 選取功能表：設定[系統]。
2. 在「一般」下、尋找「名稱：」欄位。

   如果尚未定義儲存陣列名稱、此欄位會顯示「未知」。

3. 按一下儲存陣列名稱旁的*編輯*（鉛筆）圖示。

   此欄位將變成可編輯的。

4. 輸入新名稱。

   名稱可以包含字母、數字和特殊字元、包括底線（_）、破折號（-）和雜湊符號（#）。名稱不得包含空格。名稱的長度上限為30個字元。名稱必須是唯一的。

5. 按一下*「Save"（儲存）*（核取標記）圖示。

   > 如果您要關閉可編輯欄位而不進行變更、請按一下「取消（X）」圖示。

結果

這個新名稱會出現在SANtricity 「更新系統管理程式」的標題列中。

開啟儲存陣列定位器指示燈

若要在機櫃中找到儲存陣列的實體位置、您可以開啟其定位器（LED）指示燈。

步驟

1. 選取功能表：設定[系統]。
2. 在「一般」下、按一下「開啟儲存陣列定位器指示燈」。

   此時會開啟「開啟儲存陣列定位器指示燈」對話方塊、並開啟對應的儲存陣列定位器指示燈。

3. 當您實際找到儲存陣列後、請返回對話方塊、然後選取* Turn Off*。

結果

定位燈會關閉、對話方塊會關閉。

同步儲存陣列時鐘

如果未啟用網路時間傳輸協定（NTP）、您可以手動設定控制器上的時鐘、使其與管理用戶端（用來執行瀏覽器以存取SANtricity 「系統管理程式」的系統）同步。

關於這項工作

同步可確保事件記錄中的事件時間戳記與寫入主機記錄檔的時間戳記相符。在同步過程中、控制器仍可繼續使用並正常運作。

> 如果在System Manager中啟用NTP、請勿使用此選項來同步時鐘。NTP反而會使用SNTP（簡易網路時間傳輸協定）、自動將時鐘與外部主機同步。

> 同步後、您可能會發現效能統計資料遺失或偏移、排程受到影響（ASUP、快照等）、以及記錄資料中的時間戳記偏移。使用NTP可避免此問題。

步驟

1. 選取功能表：設定[系統]。
2. 在「一般」下、按一下「同步化儲存陣列時鐘」。

   「同步儲存陣列時鐘」對話方塊隨即開啟。它會顯示控制器和作為管理用戶端的電腦的目前日期和時間。

   > 對於單工儲存陣列、只會顯示一個控制器。

3. 如果對話方塊中顯示的時間不相符、請按一下* Synchronize*。

結果

同步成功之後、事件記錄和主機記錄的事件時間戳記相同。

儲存儲存陣列組態

您可以將儲存陣列的組態資訊儲存在指令碼檔案中、以節省使用相同組態設定其他儲存陣列的時間。

開始之前

儲存陣列不得執行任何變更其邏輯組態設定的作業。這些作業的範例包括建立或刪除磁碟區、下載控制器韌體、指派或修改熱備援磁碟機、或將容量（磁碟機）新增至磁碟區群組。

關於這項工作

儲存儲存陣列組態會產生命令列介面（CLI）指令碼、其中包含儲存陣列的儲存陣列設定、磁碟區組態、主機組態或主機對磁碟區指派。您可以使用此產生的CLI指令碼、將組態複寫到具有完全相同硬體組態的另一個儲存陣列。

但是、您不應該使用此產生的CLI指令碼來進行災難恢復。若要進行系統還原、請改用手動建立的組態資料庫備份檔案、或聯絡技術支援部門、從最新的「自動支援」資料取得此資料。

此作業_不會儲存下列設定：

- 電池壽命
- 控制器每日時間
- 非揮發性靜態隨機存取記憶體（NVSRAM）設定
- 任何優質功能

- 儲存陣列密碼
- 硬體元件的作業狀態和狀態
- Volume群組的作業狀態（最佳）和狀態除外
- 複製服務、例如鏡射和Volume複製

> 應用程式錯誤的風險-如果儲存陣列正在執行會變更任何邏輯組態設定的作業、請勿使用此選項。這些作業的範例包括建立或刪除磁碟區、下載控制器韌體、指派或修改熱備援磁碟機、或將容量（磁碟機）新增至磁碟區群組。

步驟

1. 選取功能表：設定[系統]。
2. 選擇*儲存儲存陣列組態*。
3. 選取您要儲存的組態項目：
   - 儲存陣列設定
   - * Volume組態*
   - 主機組態
   - 主機對磁碟區指派

   > 如果選擇*主機到磁碟區指派*項目、則預設也會選取*磁碟區組態*項目和*主機組態*項目。您必須儲存* Volume組態*和*主機組態*、才能儲存*主機對Volume指派*。

4. 按一下「 * 儲存 * 」。

   檔案會儲存在瀏覽器的「Downloads（下載）」資料夾中、名稱為「shorage-array-configuration．cfg」。

完成後

若要將儲存陣列組態載入另一個儲存陣列、請使用SANtricity NetApp統一化管理程式。

清除儲存陣列組態

若要從儲存陣列刪除所有集區、磁碟區群組、磁碟區、主機定義和主機指派、請使用「清除組態」作業。

開始之前

- 在清除儲存陣列組態之前、請先備份資料。

關於這項工作

有兩種「清除儲存陣列組態」選項：

- * Volume *（磁碟區）-通常您可以使用Volume（磁碟區）選項、將測試儲存陣列重新設定為正式作業儲存陣列。例如、您可以設定儲存陣列進行測試、然後在測試完成後、移除測試組態、並設定正式作業環境的儲存陣列。
- 儲存陣列-一般而言、您可以使用儲存陣列選項將儲存陣列移至其他部門或群組。例如、您可能正在工程中使用儲存陣列、現在Engineering正在推出新的儲存陣列、因此您想要將目前的儲存陣列移至「系統管理」、以

便將其重新設定。

Storage Array（儲存陣列）選項會刪除一些其他設定。

	Volume	儲存陣列
刪除資源池和Volume群組	x	x
刪除Volume	x	x
刪除主機和主機叢集	x	x
刪除主機指派	x	x
刪除儲存陣列名稱		x
將儲存陣列快取設定重設為預設值		x

資料遺失風險：此作業會刪除儲存陣列中的所有資料。（它不會執行安全清除。） 您無法在作業啟動後取消此作業。只有在技術支援人員的指示下、才執行此作業。

步驟

1. 選取功能表：設定[系統]。
2. 選擇*清除儲存陣列組態*。
3. 在下拉式清單中、選取* Volume 或 Storage Array*。
4. 選用：如果您要儲存組態（而非資料）、請使用對話方塊中的連結。
5. 確認您要執行此作業。

結果

- 刪除目前的組態、會破壞儲存陣列上的所有現有資料。
- 所有磁碟機均未指派。

設定登入橫幅

您可以建立登入橫幅、在使用SANtricity 者在「系統管理程式」中建立工作階段之前、先向使用者出示登入橫幅。橫幅可包含建議事項通知和同意訊息。

關於這項工作

建立橫幅時、橫幅會出現在對話方塊的登入畫面之前。

步驟

1. 選取功能表：設定[系統]。
2. 在「一般」區段下、選取「設定登入橫幅」。

「設定登入橫幅」對話方塊隨即開啟。

3. 輸入您要在登入橫幅中顯示的文字。

> 請勿使用HTML或其他標記標記進行格式化。

4. 按一下「 * 儲存 * 」。

結果

下次使用者登入System Manager時、會在對話方塊中開啟文字。使用者必須按一下「確定」以繼續登入畫面。

管理工作階段逾時

您可以在SANtricity 「靜態系統管理程式」中設定逾時、以便在指定時間後中斷使用者的非作用中工作階段連線。

關於這項工作

依預設、System Manager的工作階段逾時為30分鐘。您可以調整時間、也可以一併停用工作階段逾時。

> 如果使用陣列內嵌的安全聲明標記語言（SAML）功能來設定存取管理、則當使用者的SSO工作階段達到上限時、可能會發生工作階段逾時。這可能發生在System Manager工作階段逾時之前。

步驟

1. 選取功能表：設定[系統]。
2. 在「一般」區段下、選取「啟用/停用工作階段逾時」。

   「啟用/停用工作階段逾時」對話方塊隨即開啟。

3. 使用微調控制項來增加或減少時間（以分鐘為單位）。

   您可以為System Manager設定的最短逾時時間為15分鐘。

   > 若要停用工作階段逾時、請取消選取*設定時間長度…*核取方塊。

4. 按一下「 * 儲存 * 」。

變更儲存陣列的快取設定

對於儲存陣列中的所有磁碟區、您可以調整快取記憶體設定、以供排清和區塊大小。

關於這項工作

快取記憶體是控制器上暫用揮發性儲存設備的區域、其存取時間比磁碟機媒體快。若要調整快取效能、您可以調整下列設定：

快取設定	說明
開始需求快取排清	Start demand快取排清指定快取中觸發快取排清（寫入磁碟）的未寫入資料百分比。根據預設、當未寫入的資料達到80%容量時、快取排清功能就會啟動。較高的百分比是主要執行寫入作業的環境的理想選擇、因此新的寫入要求可透過快取處理、而無需移至磁碟。較低的設定值較佳、因為I/O不穩定（使用資料突發）、因此系統會在資料突發之間頻繁清除快取。不過、低於80%的開始百分比可能會導致效能降低。
快取區塊大小	快取區塊大小決定每個快取區塊的最大大小、這是快取管理的組織單位。根據預設、區塊大小為8 KiB。System Manager允許快取區塊大小為4、8、16或32 KiB。應用程式使用不同的區塊大小、會影響儲存效能。較小的尺寸是檔案系統或資料庫應用程式的理想選擇。較大的尺寸是產生連續I/O（例如多媒體）的應用程式的理想選擇。

步驟

1. 選取功能表：設定[系統]。
2. 向下捲動至*其他設定*、然後按一下*變更快取設定*。

   「變更快取設定」對話方塊隨即開啟。

3. 調整下列值：
   - 開始需求快取排清：選擇適合您環境中所用I/O的百分比。如果您選擇低於80%的值、可能會發現效能下降。
   - Cache block size（快取區塊大小）-選擇適合您應用程式的大小。
4. 按一下「 * 儲存 * 」。

設定主機連線報告

您可以啟用主機連線報告功能、讓儲存陣列持續監控控制器與已設定主機之間的連線、然後在連線中斷時發出警示。此功能預設為啟用。

關於這項工作

如果停用主機連線報告、系統將不再監控連線到儲存陣列的主機的連線或多重路徑驅動程式問題。

> 停用主機連線報告也會停用自動負載平衡、以監控及平衡控制器資源使用率。

步驟

1. 選取功能表：設定[系統]。
2. 向下捲動至*其他設定*、然後按一下*啟用/停用主機連線報告*。

   此選項下方的文字會指出目前是否已啟用或停用。

隨即開啟確認對話方塊。

3. 按一下「是」繼續。

   選取此選項、即可在啟用/停用之間切換功能。

設定自動負載平衡

*自動負載平衡*功能可確保來自主機的傳入I/O流量在兩個控制器之間動態管理及平衡。此功能預設為啟用、但您可以從System Manager停用此功能。

關於這項工作

啟用「自動負載平衡」時、會執行下列功能：

- 自動監控及平衡控制器資源使用率。
- 視需要自動調整Volume控制器擁有權、藉此最佳化主機與儲存陣列之間的I/O頻寬。

基於下列原因、您可能想要停用儲存陣列上的自動負載平衡：

- 您不想自動變更特定磁碟區的控制器擁有權、以平衡工作負載。
- 您所在的環境經過高度調校、有針對性地設定負載分配、以便在控制器之間達成特定的分配。

步驟

1. 選取功能表：設定[系統]。
2. 向下捲動至*其他設定*、然後按一下*啟用/停用自動負載平衡*。

   此選項下方的文字會指出功能目前已啟用或已停用。

   隨即開啟確認對話方塊。

3. 單擊* Yes*（是）繼續進行確認。

   選取此選項、即可在啟用/停用之間切換功能。

   > ⓘ 如果將此功能從停用移至啟用、也會自動啟用主機連線報告功能。

變更預設主機類型

使用變更預設主機作業系統設定、可變更儲存陣列層級的預設主機類型。一般而言、在將主機連線至儲存陣列或連接其他主機之前、您會先變更預設的主機類型。

關於這項工作

請謹記以下準則：

- 如果您打算連線至儲存陣列的所有主機都有相同的作業系統（同質主機環境）、請變更主機類型以符合作業系統。
- 如果您打算連線至儲存陣列（異質主機環境）的主機具有不同的作業系統、請變更主機類型以符合大多數主

機作業系統。

例如、如果您要將八個不同的主機連線至儲存陣列、而其中六個主機執行Windows作業系統、則必須選取Windows作為預設的主機作業系統類型。

- 如果大多數連線的主機都有不同的作業系統、請將主機類型變更為出廠預設值。

  例如、如果您要將八個不同的主機連線至儲存陣列、而其中兩個主機執行Windows作業系統、則有三個主機執行HP-UX作業系統、 另外三種作業系統是執行Linux作業系統、您必須選取「Factory Default」作為預設主機作業系統類型。

步驟

1. 選取功能表：設定[系統]。
2. 向下捲動至*其他設定*、然後按一下*變更預設主機作業系統類型*。
3. 選取您要做為預設值的主機作業系統類型。
4. 按一下 * 變更 * 。

啟用或停用舊版管理介面

您可以啟用或停用舊版管理介面（符號）、這是儲存陣列與管理用戶端之間的通訊方法。根據預設、舊版管理介面為開啟狀態。如果停用、儲存陣列和管理用戶端將使用更安全的通訊方法（REST API over https）；不過、如果停用某些工具和工作、可能會受到影響。

關於這項工作

此設定會影響下列作業：

- * on*（預設）-鏡射所需的設定、僅在E5700和E5600儲存陣列上運作的CLI命令、以及其他一些工具（例如快速連線公用程式和OCI介面卡）。
- 關：必要設定、可在儲存陣列與管理用戶端之間的通訊中強制執行機密性、以及存取外部工具。設定目錄伺服器（LDAP）時的建議設定。

步驟

1. 選取功能表：設定[系統]。
2. 向下捲動至*其他設定*、然後按一下*變更管理介面*。
3. 在對話方塊中、按一下* Yes（是）*繼續。

常見問題集

什麼是控制器快取？

控制器快取是一種實體記憶體空間、可簡化兩種類型的I/O（輸入/輸出）作業：控制器與主機之間、控制器與磁碟之間。

對於讀寫資料傳輸、主機和控制器會透過高速連線進行通訊。但是、從控制器後端到磁碟的通訊速度較慢、因為磁碟是相對較慢的裝置。

當控制器快取接收資料時、控制器會向主機應用程式確認它目前正在保留資料。如此一來、主機應用程式就不需

要等待I/O寫入磁碟。而是應用程式可以繼續作業。伺服器應用程式也能輕鬆存取快取的資料、不需要額外的磁碟讀取來存取資料。

控制器快取會以多種方式影響儲存陣列的整體效能：

- 快取會做為緩衝區、因此不需要同步處理主機和磁碟資料傳輸。
- 從主機進行讀取或寫入作業的資料可能位於先前作業的快取中、因此不需要存取磁碟。
- 如果使用寫入快取、則主機可以在將先前寫入作業的資料寫入磁碟之前、先傳送後續的寫入命令。
- 如果啟用快取預先擷取、則會最佳化循序讀取存取。快取預先擷取可讓讀取作業更容易在快取中找到資料、而非從磁碟讀取資料。

> 可能的資料遺失-如果您啟用*無電池寫入快取*選項、而且沒有通用電源供應器來保護資料、您可能會遺失資料。此外、如果您沒有控制器電池、並且啟用*無電池寫入快取*選項、則可能會遺失資料。

什麼是快取排清？

當快取中的未寫入資料量達到特定層級時、控制器會定期將快取資料寫入磁碟機。此寫入程序稱為「排清」。

控制器使用兩種演算法來排清快取：需求型與年齡型。控制器使用需求型演算法、直到快取資料量降至快取清除臨界值以下為止。根據預設、當80%的快取正在使用時、就會開始排清。

在System Manager中、您可以設定「開始需求快取排清」臨界值、以最佳方式支援環境中使用的I/O類型。在主要是寫入作業的環境中、您應該將「開始需求快取排清」百分比設定為高、以增加快取處理任何新寫入要求的可能性、而不需要移至磁碟。高百分比的設定會限制快取的清除次數、使快取中保留更多資料、進而增加快取命中次數的機率。

在I/O不穩定的環境中（使用資料突發）、您可以使用低快取排清功能、讓系統在資料突發之間頻繁排清快取。在處理各種負載的多元I/O環境中、或是當負載類型不明時、將臨界值設為良好的中間接地、設定為50%。請注意、如果您選擇低於80%的開始百分比、可能會看到效能降低、因為讀取主機所需的資料可能無法使用。選擇較低的百分比也會增加維護快取層級所需的磁碟寫入次數、進而增加系統負荷。

根據年齡的演算法會指定寫入資料在符合排清至磁碟資格之前、保留在快取中的時間段。控制器會使用根據年齡的演算法、直到快取齊面臨界值達到為止。預設值為10秒、但此時間段僅會在閒置期間計算。您無法在System Manager中修改排清時間、而是必須在命令列介面（CLI）中使用「Set Storage Array」（設定儲存陣列）命令。

> 可能的資料遺失-如果您啟用*無電池寫入快取*選項、而且沒有通用電源供應器來保護資料、您可能會遺失資料。此外、如果您沒有控制器電池、並且啟用*無電池寫入快取*選項、則可能會遺失資料。

什麼是快取區塊大小？

儲存陣列的控制器會將其快取組織成「區塊」、這是大小可為4、8、16或32 KiB的記憶體區塊。儲存系統上的所有磁碟區都共用相同的快取空間、因此磁碟區只能有一個快取區塊大小。

> 快取區塊與磁碟的邏輯區塊系統所使用的512位元組區塊不同。

應用程式使用不同的區塊大小、可能會影響儲存效能。根據預設、System Manager中的區塊大小為8 KiB、但您可以將值設為4、8、16或32 KiB。較小的尺寸是檔案系統或資料庫應用程式的理想選擇。對於需要大量資料傳輸、連續I/O或高頻寬（例如多媒體）的應用程式而言、較大的規模是理想的選擇。

何時應該同步儲存陣列時鐘？

如果您注意到System Manager中顯示的時間戳記與管理用戶端（透過瀏覽器存取System Manager的電腦）中顯示的時間戳記不一致、則應手動同步儲存陣列中的控制器時鐘。只有在System Manager中未啟用NTP（網路時間傳輸協定）時、才需要執行此工作。

> 我們強烈建議您使用NTP伺服器、而非手動同步時鐘。NTP會使用SNTP（簡易網路時間傳輸協定）、自動將時鐘與外部伺服器同步。

您可以從「系統」頁面的「同步儲存陣列時鐘*」對話方塊中、檢查同步狀態。如果對話方塊中顯示的時間不相符、請執行同步處理。您可以定期檢視此對話方塊、以指出控制器時鐘的時間顯示是否已偏離並不再同步。

什麼是主機連線報告？

啟用主機連線報告時、儲存陣列會持續監控控制器與已設定主機之間的連線、然後在連線中斷時發出警示。

如果纜線鬆脫、毀損或遺失、或主機發生其他問題、可能會中斷連線。在這些情況下、系統可能會開啟Recovery Guru訊息：

- 主機備援遺失-如果任一控制器無法與主機通訊、就會開啟。
- 主機類型不正確-如果儲存陣列上未正確指定主機類型、就會開啟、這可能會導致容錯移轉問題。

在重新啟動控制器所需時間可能超過連線逾時時間的情況下、您可能會想要停用主機連線報告功能。停用此功能會抑制「Recovery Gurus」訊息。

> 停用主機連線報告也會停用自動負載平衡、以監控及平衡控制器資源使用量。不過、如果您重新啟用主機連線報告、則自動負載平衡功能不會自動重新啟用。

iSCSI設定

概念

iSCSI術語

瞭解iSCSI術語如何適用於您的儲存陣列。

期限	說明
CHAP	Challenge Handshake驗證傳輸協定（CHAP）方法會在初始連結期間驗證目標和啟動器的身分識別。驗證是以稱為CHAP*SECUR*的共用安全金鑰為基礎。
控制器	控制器由主機板、韌體和軟體組成。它控制磁碟機並實作System Manager功能。

期限	說明
DHCP	動態主機組態傳輸協定（DHCP）是一種用於網際網路傳輸協定（IP）網路的傳輸協定、可用來動態分配網路組態參數、例如IP位址。
IB	InfiniBand（IB）是高效能伺服器與儲存系統之間資料傳輸的通訊標準。
ICMP Ping回應	網際網路控制訊息傳輸協定（ICMP）是網路電腦的作業系統用來傳送訊息的傳輸協定。ICMP訊息會判斷主機是否可連線、以及從該主機取得封包所需的時間。
IQN	iSCSI合格名稱（IQN）識別碼是iSCSI啟動器或iSCSI目標的唯一名稱。
商用	RDMA的iSCSI擴充（iSER）是一種傳輸協定、可延伸iSCSI傳輸協定、以透過RDMA傳輸（例如InfiniBand或乙太網路）進行操作。
iSNS	網際網路儲存名稱服務（iSNS）是一種傳輸協定、可在TCP/IP網路上自動探索、管理及設定iSCSI和光纖通道裝置。
MAC位址	乙太網路使用媒體存取控制識別碼（MAC位址）來區分連接同一個實體傳輸網路介面上兩個連接埠的獨立邏輯通道。
管理用戶端	管理用戶端是指安裝瀏覽器以存取System Manager的電腦。
MTU	最大傳輸單元（MTU）是可在網路中傳送的最大封包或框架。
RDMA	遠端直接記憶體存取（RDMA）是一項技術、可讓網路電腦在主記憶體中交換資料、而不需涉及任一部電腦的作業系統。
未命名的探索工作階段	啟用未命名探索工作階段選項時、iSCSI啟動器不需要指定目標IQN來擷取控制器資訊。

使用方法

設定**iSCSI**連接埠

如果您的控制器包含iSCSI主機連線、您可以從「硬體」頁面或「系統」頁面設定iSCSI連接埠設定。

開始之前

- 您的控制器必須包含iSCSI連接埠、否則iSCSI設定將無法使用。
- 您必須知道網路速度（連接埠與主機之間的資料傳輸率）。

關於這項工作

本工作說明如何從「硬體」頁面存取iSCSI連接埠組態。您也可以從「System（系統）」頁面存取組態（功能表：「Settings[System]（設定[系統]）」）。

iSCSI設定與功能僅在儲存陣列支援iSCSI時才會顯示。

步驟

1. 選取*硬體*。
2. 如果圖形顯示磁碟機、請按一下*顯示磁碟櫃背面*。

   圖形會變更、以顯示控制器而非磁碟機。

3. 按一下要設定iSCSI連接埠的控制器。

   此時會出現控制器的內容功能表。

4. 選取*設定iSCSI連接埠*。

   僅當System Manager偵測到控制器上的iSCSI連接埠時、才會顯示* Configure iSCSI連接埠*選項。

   此時將打開Configure iSCSI Portes（配置iSCSI端口）對話框。

5. 在下拉式清單中、選取您要設定的連接埠、然後按一下「下一步」。
6. 選取組態連接埠設定、然後按一下「下一步」。

   若要查看所有連接埠設定、請按一下對話方塊右側的「Show More port settings（顯示更多連接埠設定）」連結。

欄位詳細資料

連接埠設定	說明
啟用IPV4 /啟用IPv6	選取一個或兩個選項、以啟用對IPv4和IPv6網路的支援。附註：如果您要停用連接埠存取、請取消選取這兩個核取方塊。
TCP接聽連接埠（按一下「Show More port settings（顯示更多連接埠設定）」即可取得。）	如有必要、請輸入新的連接埠號碼。 接聽連接埠是控制器用來接聽來自主機iSCSI啟動器之iSCSI登入的TCP連接埠號碼。預設的接聽連接埠為3260。您必須輸入3260或49152到65535.之間的值。
MTU大小（按一下「Show More port settings（顯示更多連接埠設定）」即可取得。）	如有必要、請為最大傳輸單元（MTU）輸入新的位元組大小。 預設的最大傳輸單元（MTU）大小為每個框架1500位元組。您必須輸入介於1500和9000之間的值。
啟用ICMP Ping回應	選取此選項可啟用網際網路控制訊息傳輸協定（ICMP）。網路電腦的作業系統會使用此傳輸協定來傳送訊息。這些ICMP訊息可判斷主機是否可連線、以及從該主機取得封包所需的時間。

如果您選取「啟用IPV4」、則會在按「下一步」之後開啟一個對話方塊、供您選取「IPV4設定」。如果您選取「啟用IPv6」、則會在按「下一步」之後開啟一個對話方塊、供您選取IPv6設定。如果您同時選取這兩個選項、則會先開啟[IPV4設定]對話方塊、然後按一下[下一步]之後、隨即開啟IPv6設定對話方塊。

7. 自動或手動設定IPv6和/或IPv6設定。若要查看所有連接埠設定、請按一下對話方塊右側的*顯示更多設定*連結。

欄位詳細資料

連接埠設定	說明
自動取得組態	選取此選項可自動取得組態。
手動指定靜態組態	選取此選項、然後在欄位中輸入靜態位址。（如有需要、您可以剪下地址並貼到欄位中。） 對於IPV4、請加入網路子網路遮罩和閘道。對於IPv6、請包含可路由的IP位址和路由器IP位址。
啟用VLAN支援（按一下「Show More settings（顯示更多設定）」即可取得。）	選取此選項可啟用VLAN並輸入其ID。VLAN是一種邏輯網路、其運作方式類似於實體獨立於其他實體和虛擬區域網路（LAN）、這些區域網路由相同的交換器、相同的路由器或兩者支援。
啟用乙太網路優先順序（按一下「Show More settings（顯示更多設定）」即可取得。）	選取此選項可啟用決定存取網路優先順序的參數。使用滑桿選取介於1（最低）和7（最高）之間的優先順序。 在共享區域網路（LAN）環境（例如乙太網路）中、許多站台可能會爭用網路存取權。存取權以先到先得的方式提供。兩個站台可能會同時嘗試存取網路、這會導致兩個站台都關機並等待、然後再試一次。交換式乙太網路只有一個站台連接到交換器連接埠、此程序就會最小化。

8. 單擊*完成*。

設定**iSCSI**驗證

為了加強iSCSI網路的安全性、您可以在控制器（目標）和主機（啟動器）之間設定驗證。System Manager使用Challenge Handshake驗證傳輸協定（CHAP）方法、在初始連結期間驗證目標和啟動器的身分。驗證是以稱為CHAP*SECUR*的共用安全金鑰為基礎。

開始之前

您可以在設定目標（控制器）的CHAP機密之前或之後、設定啟動器（iSCSI主機）的CHAP機密。在遵循此工作的指示之前、您應該等到主機先建立iSCSI連線、然後在個別主機上設定CHAP機密。建立連線之後、主機的IQN名稱及其CHAP機密會列在iSCSI驗證的對話方塊中（如本工作所述）、您不需要手動輸入這些名稱。

關於這項工作

您可以選取下列其中一種驗證方法：

- 單向驗證-使用此設定可讓控制器驗證iSCSI主機的身分識別（單向驗證）。
- 雙向驗證-使用此設定可允許控制器和iSCSI主機執行驗證（雙向驗證）。此設定可讓控制器驗證iSCSI主機的身分識別、進而驗證控制器的身分識別、進而提供第二層安全性。

如果您的儲存陣列支援iSCSI、則iSCSI設定與功能僅會顯示在「設定」頁面上。

步驟

1. 選取功能表：設定[系統]。
2. 在「* iSCSI設定*」下、按一下「組態驗證」。

   此時會出現「設定驗證」對話方塊、顯示目前設定的方法。也會顯示是否有任何主機已設定CHAP機密。

3. 選取下列其中一項：
   - 無驗證-如果您不希望控制器驗證iSCSI主機的身分識別、請選取此選項、然後按一下「完成」。對話方塊隨即關閉、您將完成組態設定。
   - 單向驗證-若要允許控制器驗證iSCSI主機的身分識別、請選取此選項、然後按*「下一步*」以顯示「設定目標CHAP」對話方塊。
   - 雙向驗證-若要允許控制器和iSCSI主機執行驗證、請選取此選項、然後按「下一步」以顯示「設定目標CHAP」對話方塊。
4. 對於單向或雙向驗證、請輸入或確認控制器（目標）的CHAP機密。CHAP密碼必須介於12到57個可列印的Ascii字元之間。

   如果先前已設定控制器的CHAP密碼、則會遮罩欄位中的字元。如有必要、您可以取代現有的字元（新字元不會遮罩）。

5. 執行下列其中一項：
   - 如果您要設定_單向 驗證、請按一下*完成*。對話方塊隨即關閉、您將完成組態設定。
   - 如果您要設定_雙向_驗證、請按一下*下一步*以顯示「設定啟動器CHAP」對話方塊。
6. 對於雙向驗證、請輸入或確認任何iSCSI主機（啟動器）的CHAP密碼、此密碼可介於12到57個可列印的Ascii字元之間。如果您不想為特定主機設定雙向驗證、請將「啟動器**CHAP**機密」欄位保留空白。

   如果先前已設定主機的CHAP密碼、則會遮罩欄位中的字元。如有必要、您可以取代現有的字元（新字元不會遮罩）。

7. 單擊*完成*。

結果

除非您未指定驗證、否則驗證會在控制器與iSCSI主機之間的iSCSI登入順序期間進行。

啟用**iSCSI**探索設定

您可以在iSCSI網路中啟用與探索儲存裝置相關的設定。「目標探索設定」可讓您使用網際網路儲存名稱服務（iSNS）傳輸協定來登錄儲存陣列的iSCSI資訊、並決定是否允許未命名的探索工作階段

開始之前

如果iSNS伺服器使用靜態IP位址、則該位址必須可用於iSNS登錄。同時支援IPV4和IPV6。

關於這項工作

您可以啟用下列與iSCSI探索相關的設定：

- 讓**iSNS**伺服器登錄目標-啟用後、儲存陣列會從iSNS伺服器登錄其iSCSI合格名稱（IQN）和連接埠資訊。此設定可允許進行iSNS探索、以便啟動器從iSNS伺服器擷取IQN和連接埠資訊。
- 啟用未命名探索工作階段-啟用未命名探索工作階段時、啟動器（iSCSI主機）不需要在探索型連線的登入順序期間提供目標（控制器）的IQN。停用時、主機確實需要提供IQN、才能建立與控制器的探索工作階段。然而、一般（I/O承載）工作階段一律需要目標IQN。停用此設定可防止未獲授權的iSCSI主機僅使用其IP位址連線至控制器。

> 如果您的儲存陣列支援iSCSI、則iSCSI設定與功能僅會顯示在「設定」頁面上。

步驟

1. 選取功能表：設定[系統]。
2. 在「* iSCSI設定*」下、按一下「檢視/編輯目標探索設定」。

   「目標探索設定」對話方塊隨即出現。在「Enable iSNS server…（啟用iSNS伺服器…）」欄位下方、對話方塊會指出控制器是否已登錄。

3. 若要登錄控制器、請選取*啟用iSNS伺服器以登錄我的目標*、然後選取下列其中一項：
   - 自動從**DHCP**伺服器取得組態-如果您要使用動態主機組態傳輸協定（DHCP）伺服器來設定iSNS伺服器、請選取此選項。請注意、如果您使用此選項、則控制器上的所有iSCSI連接埠也必須設定為使用DHCP。如有必要、請更新控制器iSCSI連接埠設定以啟用此選項。

     > 若要讓DHCP伺服器提供iSNS伺服器位址、您必須將DHCP伺服器設定為使用選項43 -「廠商專屬資訊」。 此選項必須包含以資料位元組為單位的iSNS伺服器IPv4位址：0xA-xd（10-13）。

   - 手動指定靜態組態-如果您要輸入iSNS伺服器的靜態IP位址、請選取此選項。（如有需要、您可以剪下地址並貼到欄位中。） 在欄位中、輸入一個IPv4位址或IPv6位址。如果您同時設定這兩者、則預設為使用IPV4。同時輸入TCP聆聽連接埠（使用預設值3205或輸入介於49152和6555之間的值）。
4. 若要允許儲存陣列參與未命名的探索工作階段、請選取*啟用未命名的探索工作階段*。
   - 啟用時、iSCSI啟動器不需要指定目標IQN來擷取控制器資訊。
   - 停用時、除非啟動器提供目標IQN、否則會禁止探索工作階段。停用未命名的探索工作階段可提供更高的安全性。
5. 按一下「 * 儲存 * 」。

結果

當System Manager嘗試將控制器登錄到iSNS伺服器時、會出現進度列。此程序可能需要五分鐘的時間。

檢視**iSCSI**統計資料套件

您可以檢視與儲存陣列的iSCSI連線相關資料。

關於這項工作

System Manager會顯示這些類型的iSCSI統計資料。所有統計資料均為唯讀、無法設定。

- 乙太網路**MAC**統計資料-提供媒體存取控制（MAC）的統計資料。Mac也提供稱為實體位址或MAC位址的定

址機制。MAC位址是指派給每個網路介面卡的唯一位址。MAC位址有助於將資料封包傳送到子網路內的目的地。

- 乙太網路**TCP/IP**統計資料-提供TCP/IP的統計資料、這是iSCSI裝置的傳輸控制傳輸協定（TCP）和網際網路傳輸協定（IP）。有了TCP、網路連線主機上的應用程式可以建立彼此的連線、藉此交換封包中的資料。IP是一種資料導向的傳輸協定、可透過封包交換式網路間通訊資料。分別顯示IPv6統計資料和IPv6統計資料。
- 本機目標/啟動器（傳輸協定）統計資料-顯示iSCSI目標的統計資料、提供區塊層級存取其儲存媒體的功能、並顯示儲存陣列在非同步鏡射作業中作為啟動器時的iSCSI統計資料。
- * DCBX作業狀態統計資料*-顯示各種資料中心橋接Exchange（DCBX）功能的作業狀態。
- * LLDP TLV統計資料*-顯示連結層探索通訊協定（LLDP）類型長度值（TLV）統計資料。
- * DCBX TLV統計資料*-顯示資料中心橋接（DCB）環境中識別儲存陣列主機連接埠的資訊。此資訊會與網路對等端點分享、以供識別和功能使用。

您可以將每個統計資料檢視為原始統計資料或是基準統計資料。原始統計資料是自控制器啟動以來所收集的所有統計資料。比較基準統計資料是自您設定基準時間以來所收集的時間點統計資料。

步驟

1. 選取功能表：Support（支援）[Support Center（支援中心）> Diagnostics（診斷）]索引標籤。
2. 選取*檢視iSCSI統計資料套件*。
3. 按一下索引標籤以檢視不同的統計資料集。
4. 若要設定基準線、請按一下*設定新的基準線*。

   設定基準可為統計資料的收集作業設定新的起點。所有iSCSI統計資料都使用相同的基準。

結束**iSCSI**工作階段

您可以結束不再需要的iSCSI工作階段。在非同步鏡射關係中、主機或遠端儲存陣列可能會發生iSCSI工作階段。

關於這項工作

您可能會因為下列原因而想要結束iSCSI工作階段：

- 未獲授權的存取-如果iSCSI啟動器已登入且不應具有存取權、您可以結束iSCSI工作階段、強制iSCSI啟動器離開儲存陣列。iSCSI啟動器可能已登入、因為無驗證方法可供使用。
- 系統停機-如果您需要關閉儲存陣列、但發現iSCSI啟動器仍在登入、您可以結束iSCSI工作階段、使iSCSI啟動器脫離儲存陣列。

步驟

1. 選取功能表：Support（支援）[Support Center（支援中心）> Diagnostics（診斷）]索引標籤。
2. 選取*檢視/結束iSCSI工作階段*。

   此時會顯示目前iSCSI工作階段的清單。

3. 選取您要結束的工作階段
4. 按一下*結束工作階段*、然後確認您要執行此作業。

檢視**iSCSI**工作階段

您可以檢視iSCSI與儲存陣列連線的詳細資訊。在非同步鏡射關係中、主機或遠端儲存陣列可能會發生iSCSI工作階段。

步驟

1. 選取功能表：Support（支援）[Support Center（支援中心）> Diagnostics（診斷）]索引標籤。
2. 選取*檢視/結束iSCSI工作階段*。

   此時會顯示目前iSCSI工作階段的清單。

3. 若要查看特定iSCSI工作階段的其他資訊、請選取工作階段、然後按一下*檢視詳細資料*。

欄位詳細資料

項目	說明
工作階段識別碼（SSID）	用於識別iSCSI啟動器與iSCSI目標之間工作階段的十六進位字串。SSID由ISID和TPGT組成。
啟動器工作階段ID（ISID）	工作階段識別碼的啟動器部分。啟動器會在登入期間指定ISID。
目標入口網站群組	iSCSI目標。
目標入口網站群組標籤（TPGT）	工作階段識別碼的目標部分。iSCSI目標入口網站群組的16位元數字識別碼。
啟動器iSCSI名稱	啟動器的全球唯一名稱。
啟動器iSCSI標籤	在System Manager中設定的使用者標籤。
啟動器iSCSI別名	也可與iSCSI節點相關聯的名稱。別名可讓組織將使用者友好字串與iSCSI名稱建立關聯。不過、別名並不能取代iSCSI名稱。啟動器iSCSI別名只能在主機上設定、不能在系統管理員中設定
主機	將輸入和輸出傳送至儲存陣列的伺服器。
連線ID（CID）	啟動器與目標之間工作階段內連線的唯一名稱。啟動器會產生此ID、並在登入要求期間將其呈現給目標。連線ID也會在登出時顯示、以關閉連線。
乙太網路連接埠識別碼	與連線相關聯的控制器連接埠。
啟動器IP位址	啟動器的IP位址。
協調登入參數	在iSCSI工作階段登入期間所處理的參數。
驗證方法	驗證想要存取iSCSI網路之使用者的技術。有效值為* CHAP*和*無*。
標頭摘要方法	顯示iSCSI工作階段可能標頭值的技術。「標題摘要」和「資料摘要」可以是*「無」或「CRC32C*」。兩者的預設值為*無*。
資料摘要方法	顯示iSCSI工作階段可能資料值的技術。「標題摘要」和「資料摘要」可以是*「無」或「CRC32C*」。兩者的預設值為*無*。
最大連線數	iSCSI工作階段所允許的最大連線數。最多可有1到4個連線。預設值為*1*。

項目	說明
目標別名	與目標相關的標籤。
啟動器別名	與啟動器相關的標籤。
目標IP位址	iSCSI工作階段目標的IP位址。不支援DNS名稱。
初始R2T	初始「準備傳輸」狀態。狀態可以是*是*或*否*。
最大突發長度	此iSCSI工作階段的最大SCSI有效負載（以位元組為單位）。最大突發長度可介於512至262,144（256 KB）之間。預設值為* 262,144（256 KB）*。
第一次爆發長度	此iSCSI工作階段的非主動式資料SCSI有效負載（以位元組為單位）。第一個脈衝長度可介於512至131,072（128 KB）之間。預設值為* 65536（64 KB）*。
預設等待時間	在連線終止或連線重設後、嘗試連線之前所需等待的最小秒數。預設的等待時間值可介於0到3、600之間。預設值為* 2 *。
預設保留時間	連線終止或連線重設後仍可進行連線的最大秒數。保留的預設時間可介於0到3、600之間。預設值為* 20*。
最大未處理R2T	此iSCSI工作階段未處理的「準備傳輸」上限。最大未處理準備傳輸值可為1至16。預設值為* 1*。
錯誤恢復層級	此iSCSI工作階段的錯誤恢復層級。錯誤恢復層級值永遠設定為* 0*。
最大接收資料區段長度	啟動器或目標可在任何iSCSI有效負載資料單元（PDU）中接收的資料量上限。
目標名稱	目標的正式名稱（非別名）。以_iqn_格式的目標名稱。
啟動器名稱	啟動器的正式名稱（非別名）。使用_iqn_或_EUI_格式的啟動器名稱。

4. 若要將報告儲存至檔案、請按一下*儲存*。

   檔案會以「iscso-site-connections．txt」檔案名稱儲存在瀏覽器的「Downloads（下載）」資料夾中。

在**InfiniBand**連接埠上設定**iSER**

如果您的控制器包含透過InfiniBand連接埠的iSER、您可以設定與主機的網路連線。組態設定可從「硬體」頁面或「系統」頁面取得。

開始之前

- 您的控制器必須在InfiniBand連接埠上包含iSER；否則、System Manager無法使用iSER over InfiniBand設定。
- 您必須知道主機連線的IP位址。

關於這項工作

您可以從「硬體」頁面或功能表：「設定」[系統]存取InfiniBand組態上的iSER。本工作說明如何從「硬體」頁面設定連接埠。

> 僅當儲存陣列的控制器在InfiniBand連接埠上包含iSER時、才會顯示iSER over InfiniBand設定和功能。

步驟

1. 選取*硬體*。
2. 如果圖形顯示磁碟機、請按一下*顯示磁碟櫃背面*。

   圖形會變更、以顯示控制器而非磁碟機。

3. 按一下要設定的InfiniBand連接埠上的iSER控制器。

   此時會出現控制器的內容功能表。

4. 選取*透過InfiniBand連接埠設定iSER *。

   此時將打開Configure iSER over InfiniBand Portes（在InfiniBand端口上配置iSER）對話框。

5. 在下拉式清單中、選取您要設定的HIC連接埠、然後輸入主機的IP位址。
6. 按一下「設定」。
7. 完成組態、然後按一下「是」、透過InfiniBand連接埠重設iSER。

檢視**InfiniBand**統計資料的**iSER**

如果您的儲存陣列控制器包含透過InfiniBand連接埠的iSER、您可以檢視有關主機連線的資料。

關於這項工作

System Manager會顯示下列類型的iSER（相對於InfiniBand統計資料）。所有統計資料均為唯讀、無法設定。

- 本機目標（傳輸協定）統計資料-提供iSER over InfiniBand目標的統計資料、顯示區塊層級存取其儲存媒體的情形。
- * InfiniBand介面統計資料* iSER：提供InfiniBand介面上所有iSER連接埠的統計資料、其中包括效能統計資料、以及與每個交換器連接埠相關的連結錯誤資訊。

您可以將每個統計資料檢視為原始統計資料或是基準統計資料。原始統計資料是自控制器啟動以來所收集的所有統計資料。比較基準統計資料是自您設定基準時間以來所收集的時間點統計資料。

您可以從「System（系統）」頁面（功能表：「Settings[System]（設定[系統]）」）或「Support（支援）」頁面、透過InfiniBand統計資料存取iSER。這些指示說明如何從「支援」頁面存取統計資料。

步驟

1. 選取功能表：Support（支援）[Support Center（支援中心）> Diagnostics（診斷）]索引標籤。
2. 選取*檢視InfiniBand統計資料*上的iSER。
3. 按一下索引標籤以檢視不同的統計資料集。
4. 若要設定基準線、請按一下*設定新的基準線*。

   設定基準可為統計資料的收集作業設定新的起點。同樣的基準適用於InfiniBand統計資料上的所有iSER。

常見問題集

使用**iSNS**伺服器進行登錄時會發生什麼事？

使用網際網路儲存名稱服務（iSNS）伺服器資訊時、可將主機（啟動器）設定為查詢iSNS伺服器、以便從目標（控制器）擷取資訊。

此登錄可為iSNS伺服器提供控制器的iSCSI合格名稱（IQN）和連接埠資訊、並允許在啟動器（iSCSI主機）和目標（控制器）之間進行查詢。

iSCSI自動支援哪些登錄方法？

iSCSI實作可支援網際網路儲存名稱服務（SNSs）探索方法、或使用「傳送目標」命令。

透過iSNS方法、可在啟動器（iSCSI主機）和目標（控制器）之間進行iSNS探索。您可以註冊目標控制器、以便為iSNS伺服器提供控制器的iSCSI合格名稱（IQN）和連接埠資訊。

如果未設定iSNS、iSCSI主機可在iSCSI探索工作階段期間傳送「傳送目標」命令。因此、控制器會傳回連接埠資訊（例如、Target IQN、連接埠IP位址、接聽連接埠和目標連接埠群組）。如果您使用的是iSNS、則不需要使用此探索方法、因為主機啟動器可以從iSNS伺服器擷取目標IP。

我要如何解讀**InfiniBand**統計資料的**iSER**？

「View iSER over InfiniBand Statistics *」（檢視InfiniBand統計資料*的iSER）對話方塊會顯示本機目標（傳輸協定）統計資料、以及InfiniBand（IB）介面統計資料。所有統計資料均為唯讀、無法設定。

- 本機目標（傳輸協定）統計資料-提供iSER over InfiniBand目標的統計資料、顯示區塊層級存取其儲存媒體的情形。
- * InfiniBand介面統計資料* iSER：提供InfiniBand介面上所有InfiniBand連接埠的iSER統計資料、其中包括效能統計資料、以及與每個交換器連接埠相關的連結錯誤資訊。

您可以將每個統計資料檢視為原始統計資料或是基準統計資料。原始統計資料是自控制器啟動以來所收集的所有統計資料。比較基準統計資料是自您設定基準時間以來所收集的時間點統計資料。

在**InfiniBand**上設定或診斷**iSER**還需要做什麼？

下表列出可用於設定及管理InfiniBand工作階段之iSER的System Manager功能。

僅當儲存陣列的控制器在InfiniBand主機管理連接埠上包含iSER時、才能使用iSER over InfiniBand設定。

透過**InfiniBand**設定及診斷**iSER**

行動	位置
在InfiniBand連接埠上設定iSER	1. 選取*硬體*。 2. 選擇*顯示櫃背面*。 3. 選取控制器。 4. 選取*透過InfiniBand連接埠設定iSER *。 或 1. 選取功能表：設定[系統]。 2. 向下捲動至* iSER over InfiniBand settings 、然後選取 Configure iSER over InfiniBand Ports*。
檢視InfiniBand統計資料的iSER	1. 選取功能表：設定[系統]。 2. 向下捲動至「InfiniBand設定*上的* iSER」、然後選取「View iSER over InfiniBand Statistics *」。

系統：NVMe設定

概念

NVMe總覽

有些控制器包含一個連接埠、可在InfiniBand光纖或RoCE（透過整合式乙太網路的RDMA）架構上實作NVMe（非揮發性記憶體Express）。NVMe可在主機與儲存陣列之間進行高效能通訊。

什麼是NVMe？

_NVM代表「非揮發性記憶體」、是許多儲存裝置類型所使用的持續記憶體。_NVMe（NVM Express）是標準化的介面或傳輸協定、專為高效能的與NVM裝置的多佇列通訊所設計。

什麼是NVMe over Fabrics？

NVMe over Fabrics（NVMe）是一種技術規格、可讓*NVMe*訊息型命令和資料在主機電腦和儲存設備之間透過網路傳輸。對於更新版本的作業系統*11.40*、*NVMe*儲存陣列（稱為_*Subsystem*）可由使用InfiniBand或RDMA架構的主機存取。SANtricityNVMe命令會在主機端和子系統端的傳輸抽象層中啟用和封裝。如此可將高效能NVMe介面端對端從主機延伸至儲存設備、並標準化及簡化命令集。

NVMe儲存設備會以本機區塊儲存設備的形式呈現給主機。磁碟區（稱為_namespacity_）可以像任何其他區塊儲存設備一樣掛載到檔案系統。您可以使用REST API、SMcli或SANtricity Sys以上 系統管理程式、視需要配置

儲存設備。

什麼是NVMe合格名稱（NQN）？

NVMe合格名稱（NQN）用於識別遠端儲存目標。儲存陣列的NVMe合格名稱一律由子系統指派、不得修改。整個陣列只有一個NVMe合格名稱。NVMe合格名稱長度上限為223個字元。您可以將其與iSCSI合格名稱進行比較。

什麼是命名空間和命名空間ID？

命名空間相當於SCSI中的邏輯單元、與陣列中的磁碟區相關。命名空間ID（NSID）相當於SCSI中的邏輯單元編號（LUN）。您可以在命名空間建立時建立NSID、並將其設定為1到255之間的值。

什麼是NVMe控制器？

類似於SCSI I-T結點、代表主機啟動器到儲存系統目標的路徑、在主機連線程序期間建立的NVMe控制器可提供主機與儲存陣列中命名空間之間的存取路徑。主機的NQN加上主機連接埠識別碼、可唯一識別NVMe控制器。雖然NVMe控制器只能與單一主機建立關聯、但它可以存取多個命名空間。

您可以設定哪些主機可以存取哪些命名空間、並使用SANtricity 「支援系統管理程式」設定主機的命名空間ID。然後建立NVMe控制器時、會建立NVMe控制器可存取的命名空間ID清單、並用來設定允許的連線。

NVMe術語

瞭解NVMe術語如何適用於您的儲存陣列。

期限	說明
InfiniBand	InfiniBand（IB）是高效能伺服器與儲存系統之間資料傳輸的通訊標準。
命名空間	命名空間是NVM儲存設備、其格式化為區塊存取。它類似於SCSI中的邏輯單元、與儲存陣列中的磁碟區相關。
命名空間ID	命名空間ID是NVMe控制器的命名空間唯一識別碼、可設定為1到255之間的值。它類似於SCSI中的邏輯單元號碼（LUN）。
NQN	NVMe合格名稱（NQN）用於識別遠端儲存目標（儲存陣列）。
NVM	非揮發性記憶體（NVM）是許多儲存設備類型所使用的持續記憶體。
NVMe	非揮發性記憶體Express（NVMe）是專為Flash型儲存裝置（例如SSD磁碟機）所設計的介面。NVMe可降低I/O負荷、並與先前的邏輯裝置介面相比、提升效能。
NVMe	非揮發性記憶體Express over Fabrics（NVMe）是一種規格、可讓NVMe命令和資料在主機與儲存設備之間透過網路傳輸。
NVMe控制器	NVMe控制器是在主機連線程序期間建立的。它提供主機與儲存陣列中命名空間之間的存取路徑。

期限	說明
NVMe佇列	佇列用於透過NVMe介面傳遞命令和訊息。
NVMe子系統	採用NVMe主機連線的儲存陣列。
RDMA	遠端直接記憶體存取（RDMA）可在網路介面卡（NIC）硬體中實作傳輸傳輸協定、讓資料更直接地進出伺服器。
RoCE	RDMA over Converged Ethernet（RoCE）是一種網路傳輸協定、可透過乙太網路進行遠端直接記憶體存取（RDMA）。
SSD	固態磁碟（SSD）是使用固態記憶體（Flash）持續儲存資料的資料儲存裝置。SSD可模擬傳統硬碟機、並與硬碟機使用的介面相同。

使用方法

設定**NVMe over InfiniBand**連接埠

如果您的控制器包含NVMe over InfiniBand連線、您可以從「Hardware（硬體）」頁面或「System（系統）」頁面來設定NVMe連接埠設定。

開始之前

- 您的控制器必須包含一個NVMe over InfiniBand主機連接埠、否則系統管理員無法使用NVMe over InfiniBand設定。
- 您必須知道主機連線的IP位址。

關於這項工作

您可以從* Hardware （硬體）頁面或功能表：Settings[系統]存取NVMe over InfiniBand組態。本工作說明如何從「硬體」頁面設定連接埠。

> NVMe over InfiniBand設定和功能只有在儲存陣列的控制器包含NVMe over InfiniBand連接埠時才會顯示。

步驟

1. 選取*硬體*。
2. 如果圖形顯示磁碟機、請按一下*顯示磁碟櫃背面*。

   圖形會變更、以顯示控制器而非磁碟機。

3. 按一下要設定NVMe over InfiniBand連接埠的控制器。

   此時會出現控制器的內容功能表。

4. 選取*透過InfiniBand連接埠設定NVMe *。

   「*設定InfiniBand連接埠上的NVMe *」對話方塊隨即開啟。

5. 在下拉式清單中、選取您要設定的HIC連接埠、然後輸入主機的IP位址。
6. 按一下「設定」。
7. 完成組態、然後按一下* Yes*重設NVMe over InfiniBand連接埠。

設定**NVMe over RoCE**連接埠

如果您的控制器包含NVMe over RoCE（透過整合式乙太網路的RDMA）連線、您可以從「Hardware（硬體）」頁面或「System（系統）」頁面設定NVMe連接埠設定。

開始之前

- 您的控制器必須包含NVMe over RoCE主機連接埠、否則系統管理員無法使用NVMe over RoCE設定。
- 您必須知道主機連線的IP位址。

關於這項工作

您可以從* Hardware （硬體）頁面或功能表：Settings[系統]存取NVMe over RoCE組態。本工作說明如何從「硬體」頁面設定連接埠。

> NVMe over RoCE設定和功能只有在儲存陣列的控制器包含NVMe over RoCE連接埠時才會顯示。

步驟

1. 選取*硬體*。
2. 如果圖形顯示磁碟機、請按一下*顯示磁碟櫃背面*。

   圖形會變更、以顯示控制器而非磁碟機。

3. 按一下要設定NVMe over RoCE連接埠的控制器。

   此時會出現控制器的內容功能表。

4. 選取*透過RoCE連接埠設定NVMe *。

   「設定NVMe over RoCE連接埠」對話方塊隨即開啟。

5. 在下拉式清單中、選取您要設定的HIC連接埠。
6. 單擊 * 下一步 * 。

   若要查看所有連接埠設定、請按一下對話方塊右側的*顯示更多連接埠設定*連結。

欄位詳細資料

連接埠設定	說明
已設定乙太網路連接埠速度	選取與連接埠上SFP速度功能相符的速度。
啟用IPV4 /啟用IPv6	選取一個或兩個選項、以啟用對IPv4和IPv6網路的支援。 如果您要停用連接埠存取、請取消選取這兩個核取方塊。
MTU大小（按一下「Show More port settings（顯示更多連接埠設定）」即可取得。）	如有必要、請為最大傳輸單元（MTU）輸入新的位元組大小。 預設的最大傳輸單元（MTU）大小為每個框架1500位元組。您必須輸入介於1500和9000之間的值。

如果您選取「啟用IPV4」、則會在按「下一步」之後開啟一個對話方塊、供您選取「IPV4設定」。如果您選取「啟用IPv6」、則會在按「下一步」之後開啟一個對話方塊、供您選取IPv6設定。如果您同時選取這兩個選項、則會先開啟[IPV4設定]對話方塊、然後按一下[下一步]之後、隨即開啟IPv6設定對話方塊。

7. 自動或手動設定IPv6和/或IPv6設定。

欄位詳細資料

連接埠設定	說明
自動取得組態	選取此選項可自動取得組態。
手動指定靜態組態	選取此選項、然後在欄位中輸入靜態位址。（如有需要、您可以剪下地址並貼到欄位中。） 對於IPV4、請加入網路子網路遮罩和閘道。對於IPv6、請包含可路由的IP位址和路由器IP位址。

8. 單擊*完成*。

檢視**NVMe over Fabrics**統計資料

您可以檢視儲存陣列的NVMe over Fabrics連線相關資料。

關於這項工作

System Manager會顯示這些類型的NVMe over Fabrics統計資料。所有統計資料均為唯讀、無法設定。

- * NVMe子系統統計資料*-提供NVMe控制器的統計資料、包括逾時和連線故障。

- * RDMA介面統計資料*-提供RDMA介面的統計資料、包括接收和傳輸的封包資訊。

您可以將每個統計資料檢視為原始統計資料或是基準統計資料。原始統計資料是自控制器啟動以來所收集的所有統計資料。比較基準統計資料是自您設定基準時間以來所收集的時間點統計資料。

您可以從「System（系統）」頁面（功能表：「Settings[System]（設定[系統]）」）或「Support（支援）」頁面存取NVMe over Fabrics統計資料。這些指示說明如何從「支援」頁面存取統計資料。

步驟

1. 選取功能表：Support（支援）[Support Center（支援中心）> Diagnostics（診斷）]索引標籤。
2. 選取*「View NVMe over Fabrics Statistic*」。
3. 若要設定基準線、請按一下*設定新的基準線*。

   設定基準可為統計資料的收集作業設定新的起點。所有NVMe統計資料都使用相同的基準。

常見問題集

如何解讀**InfiniBand**上的**NVMe**統計資料？

「檢視**NVMe over Fabrics**統計資料」對話方塊會顯示NVMe子系統和NVMe over InfiniBand介面的統計資料。所有統計資料均為唯讀、無法設定。

- * NVMe子系統統計資料*-顯示NVMe控制器及其佇列的統計資料。NVMe控制器提供主機與儲存陣列中命名空間之間的存取路徑。您可以檢閱NVMe子系統統計資料、查看連線故障、重設和關機等項目。如需這些統計資料的詳細資訊、請按一下*檢視表格標題的圖例*。
- * RDMA介面統計資料*-提供RDMA介面上所有NVMe over Fabrics連接埠的統計資料、其中包括效能統計資料、以及與每個交換器連接埠相關的連結錯誤資訊。如需統計資料的詳細資訊、請按一下*檢視表格標題的圖例*。

您可以將每個統計資料檢視為原始統計資料或是基準統計資料。原始統計資料是自控制器啟動以來所收集的所有統計資料。比較基準統計資料是自您設定基準時間以來所收集的時間點統計資料。

如何解讀**NVMe over Fabrics**統計資料？

「檢視**NVMe over Fabrics**統計資料」對話方塊會顯示NVMe子系統和NVMe over RoCE介面的統計資料。所有統計資料均為唯讀、無法設定。

- * NVMe子系統統計資料*-顯示NVMe控制器及其佇列的統計資料。NVMe控制器提供主機與儲存陣列中命名空間之間的存取路徑。您可以檢閱NVMe子系統統計資料、查看連線故障、重設和關機等項目。如需這些統計資料的詳細資訊、請按一下*檢視表格標題的圖例*。
- * RDMA介面統計資料*-提供RDMA介面上所有NVMe over Fabrics連接埠的統計資料、其中包括效能統計資料、以及與每個交換器連接埠相關的連結錯誤資訊。如需統計資料的詳細資訊、請按一下*檢視表格標題的圖例*。

您可以將每個統計資料檢視為原始統計資料或是基準統計資料。原始統計資料是自控制器啟動以來所收集的所有統計資料。比較基準統計資料是自您設定基準時間以來所收集的時間點統計資料。

我還需要如何透過**InfiniBand**來設定或診斷**NVMe**？

下表列出可用於設定及管理InfiniBand上NVMe工作階段的System Manager功能。

> NVMe over InfiniBand設定只有在儲存陣列的控制器包含NVMe over InfiniBand連接埠時才能使用。

設定及診斷**InfiniBand**上的**NVMe**

行動	位置
設定NVMe over InfiniBand連接埠	1. 選取*硬體*。 2. 選擇*顯示櫃背面*。 3. 選取控制器。 4. 選取*透過InfiniBand連接埠設定NVMe *。 或 1. 選取功能表：設定[系統]。 2. 向下捲動至* NVMe over InfiniBand設定*、然後選取* Configure NVMe over InfiniBand Ports*。
檢視NVMe over InfiniBand統計資料	1. 選取功能表：設定[系統]。 2. 向下捲動至* NVMe over InfiniBand設定*、然後選取* View NVMe over Fabrics Statistic*。

我還需要做什麼才能透過**RoCE**來設定或診斷**NVMe**？

您可以從「硬體與設定」頁面設定及管理NVMe over RoCE。

> NVMe over RoCE設定僅適用於儲存陣列的控制器包含NVMe over RoCE連接埠的情況。

設定及診斷**NVMe over RoCE**

行動	位置
設定NVMe over RoCE連接埠	1. 選取*硬體*。 2. 選擇*顯示櫃背面*。 3. 選取控制器。 4. 選取*透過RoCE連接埠設定NVMe *。 或 1. 選取功能表：設定[系統]。 2. 向下捲動至* NVMe over roce設定*、然後選取* Configure NVMe over roce Ports*。
檢視NVMe over Fabrics統計資料	1. 選取功能表：設定[系統]。 2. 向下捲動至* NVMe over roce設定*、然後選取* View NVMe over Fabrics Statistic*。

附加功能

概念

附加功能的運作方式

附加元件是系統管理員標準組態中未包含的功能、需要啟用金鑰。附加功能可以是單一優質功能、也可以是隨附的功能套件。

下列步驟概述啟用優質功能或功能套件：

1. 取得下列資訊：
   - 機箱序號和功能啟用識別碼、可識別要安裝功能的儲存陣列。這些項目可在System Manager中取得。
   - 功能啟動代碼、您可在購買此功能時從Support網站取得。
2. 請聯絡您的儲存設備供應商、或存取Premium功能啟動網站、以取得功能金鑰。提供機箱序號、功能啟用識別碼和功能啟動代碼。
3. 使用System Manager、使用功能金鑰檔案啟用優質功能或功能套件。

附加功能術語

瞭解附加功能條款如何適用於您的儲存陣列。

期限	說明
功能啟用識別碼	功能啟用識別碼是識別特定儲存陣列的唯一字串。此識別碼可確保當您取得優質功能時、該識別碼僅與該特定儲存陣列相關聯。此字串會顯示在「系統」頁面的「附加元件」下方。
功能金鑰檔案	功能金鑰檔案是您用來解鎖及啟用優質功能或功能套件的檔案。
功能套件	功能套件是變更儲存陣列屬性的套件組合（例如、將傳輸協定從Fibre Channel變更為iSCSI）。功能套件需要特殊金鑰才能啟用。
優質功能	進階功能是額外的選項、需要一把鑰匙才能啟用。系統管理程式的標準組態並未包含此功能。

使用方法

取得功能金鑰檔案

若要在儲存陣列上啟用優質功能或功能套件、您必須先取得功能金鑰檔案。金鑰僅與一個儲存陣列相關聯。

關於這項工作

本工作說明如何收集功能的必要資訊、然後傳送功能金鑰檔案的要求。必要資訊包括：

- 機箱序號
- 功能啟用識別碼
- 功能啟動代碼

步驟

1. 在System Manager中、找出並記錄機箱序號。您可以將滑鼠游標移到「Support Center（支援中心）」方塊上方、以檢視此序號。
2. 在System Manager中、找到「啟用功能識別碼」。移至功能表：設定[系統]、然後向下捲動至*附加元件*。尋找*功能啟用識別碼*。記錄功能啟用識別碼的編號。
3. 找出並記錄功能啟動代碼。對於功能套件、此啟動代碼會在執行轉換的適當指示中提供。

   如需NetApp指示、請參閱 "NetApp E系列系統文件中心"。

   如需進階功能、您可以從Support網站存取啟動代碼、如下所示：

   a. 登入 "NetApp支援"。
   b. 前往功能表：產品[管理產品>軟體授權]。
   c. 輸入儲存陣列機箱的序號、然後按一下「執行」。

d. 請在*授權金鑰*欄中尋找功能啟動代碼。

e. 記錄所需功能的功能啟動代碼。

4. 請以下列資訊傳送電子郵件或文字文件給您的儲存供應商、以申請功能金鑰檔案：機箱序號、功能啟動代碼及功能啟用識別碼。

   您也可以前往 "NetApp授權啟動：儲存陣列優質功能啟動" 並輸入必要資訊以取得功能或功能套件。（本網站上的說明適用於優質功能、而非功能套件。）

完成後

當您有功能金鑰檔案時、可以啟用優質功能或功能套件。

啟用優質功能

進階功能是額外的選項、需要啟用金鑰。

開始之前

- 您已取得功能金鑰。如有必要、請聯絡技術支援部門以取得關鍵資訊。
- 您已在管理用戶端上載入金鑰檔（系統上有瀏覽器可供存取System Manager）。

關於這項工作

本工作說明如何使用System Manager來啟用優質功能。

> 如果您想要停用進階功能、則必須在命令列介面（CLI）中使用停用儲存陣列功能命令「（停用storageArray（featurePack | feature=featureAttributeList）」。

步驟

1. 選取功能表：設定[系統]。
2. 在*附加元件*下、選取*啟用優質功能*。

   「啟用優質功能」對話方塊隨即開啟。

3. 按一下*瀏覽*、然後選取金鑰檔。

   檔案名稱會顯示在對話方塊中。

4. 按一下「啟用」。

啟用功能套件

功能套件是變更儲存陣列屬性的套件組合（例如、將傳輸協定從Fibre Channel變更為iSCSI）。功能套件需要特殊的金鑰才能啟用。

開始之前

- 您已依照適當的指示執行轉換、並準備好系統以處理新的儲存陣列屬性。

> 轉換指示可從取得 "NetApp E系列系統文件中心"。

- 儲存陣列已離線、因此沒有主機或應用程式正在存取。
- 所有資料都會備份。
- 您已取得功能套件檔案。

  功能套件檔案會載入管理用戶端（系統上有瀏覽器可供存取System Manager）。

> 您必須排定停機維護時間、並停止主機與控制器之間的所有I/O作業。此外、請注意、在成功完成轉換之前、您無法存取儲存陣列上的資料。

關於這項工作

本工作說明如何使用System Manager來啟用功能套件。完成後、您必須重新啟動儲存陣列。

步驟

1. 選取功能表：設定[系統]。
2. 在*附加元件*下、選取*變更功能套件*。
3. 按一下*瀏覽*、然後選取金鑰檔。

   檔案名稱會顯示在對話方塊中。

4. 在欄位中輸入*變更*。
5. 按一下 * 變更 * 。

   功能套件移轉開始、控制器重新開機。會刪除未寫入的快取資料、以確保沒有I/O活動。兩個控制器都會自動重新開機、新功能套件才會生效。重新開機完成後、儲存陣列會返回回應狀態。

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。

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。

期限	說明
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	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。 ⓘ 磁碟機安全性密碼與儲存陣列的管理員密碼無關。
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-*enabled*.
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。

期限	說明
安全金鑰	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： • 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、然後解除鎖定時、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。