



設定

SANtricity 11.6

NetApp
February 12, 2024

目錄

設定	1
警示	1
系統：儲存陣列設定	13
系統：iSCSI設定	26
系統：NVMe設定	37
系統：附加功能	43
系統：安全金鑰管理	47
存取管理	60
憑證	87

設定

警示

概念

警示的運作方式

警示會通知系統管理員儲存陣列上發生的重要事件。警示可透過電子郵件、SNMP設陷和系統記錄傳送。

警示程序的運作方式如下：

1. 系統管理員可在System Manager中設定下列一或多種警示方法：
 - 電子郵件-訊息會傳送至電子郵件地址。
 - * SNMP *- SNMP設陷會傳送至SNMP伺服器。
 - 系統日誌-訊息會傳送至系統日誌伺服器。
2. 當儲存陣列的事件監視器偵測到問題時、它會將該問題的相關資訊寫入事件記錄（可從*功能表：Support[事件記錄]*取得）。例如、問題可能包括電池故障、從最佳化移至離線的元件、或是控制器中的備援錯誤等事件。
3. 如果事件監控器判定事件為「alertable」（警示表）、則會使用設定的警示方法（電子郵件、SNMP及/或系統記錄）傳送通知。所有重大事件都會被視為「警示」、以及一些警告和資訊事件。

警示組態

您可以從「初始設定」精靈（僅限電子郵件警示）或「警示」頁面設定警示。若要檢查目前的組態、請前往*功能表：設定[警示]*。

警示區塊會顯示警示組態、這可以是下列其中一項：

- 未設定。
- 已設定；至少已設定一種警示方法。若要判斷要設定哪些警示方法、請將游標指向方塊。

警示資訊

警示可包含下列類型的資訊：

- 儲存陣列名稱。
- 與事件記錄項目相關的事件錯誤類型。
- 事件發生的日期和時間。
- 活動的簡短說明。



系統記錄警示遵循RFC 3164訊息標準。

瞭解警示條款如何適用於您的儲存陣列。

元件	說明
事件監控	事件監視器位於儲存陣列上、並作為背景工作執行。當事件監控器偵測到儲存陣列上的異常狀況時、會將有關問題的資訊寫入事件記錄。問題可能包括電池故障、從最佳狀態移至離線狀態的元件、或是控制器中的備援錯誤等事件。如果事件監控器判定事件為「alertable」（警示表）、則會使用設定的警示方法（電子郵件、SNMP及/或系統記錄）傳送通知。所有重大事件都會被視為「警示」、以及一些警告和資訊事件。
郵件伺服器	郵件伺服器用於傳送和接收電子郵件警示。伺服器使用簡易郵件傳輸傳輸傳輸協定（Simple Mail Transfer Protocol、簡稱SMTP）。
SNMP	簡易網路管理傳輸協定（SNMP）是一種網際網路標準傳輸協定、用於管理和共用IP網路上裝置之間的資訊。
SNMP設陷	SNMP設陷是傳送至SNMP伺服器的通知。陷阱包含儲存陣列重大問題的相關資訊。
SNMP設陷目的地	SNMP設陷目的地是執行SNMP服務之伺服器的IPv4或IPv6位址。
社群名稱	社群名稱是類似SNMP環境中網路伺服器密碼的字串。
mib檔案	管理資訊庫（mib）檔案定義儲存陣列中所監控及管理的資料。必須使用SNMP服務應用程式在伺服器上複製及編譯。支援網站上的System Manager軟體可提供此mib檔案。
mib變數	管理資訊庫（MIB）變數可傳回儲存陣列名稱、陣列位置、以及回應SNMP GetRequest的聯絡人等值。
系統記錄	syslog是網路裝置用來傳送事件訊息至記錄伺服器的傳輸協定。
UDP	使用者資料包傳輸協定（UDP）是傳輸層傳輸協定、可在其封包標頭中指定來源連接埠和目的地連接埠號碼。

使用方法

管理電子郵件警示

設定郵件伺服器和收件者的警示

若要設定電子郵件警示、您必須指定警示收件者的郵件伺服器位址和電子郵件位址。最多允許20個電子郵件地址。

開始之前

- 郵件伺服器的位址必須是可用的。位址可以是IPV4或IPV6位址、也可以是完整網域名稱。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

- 必須提供電子郵件地址、才能作為警示傳送者使用。這是警示訊息「寄件者」欄位中顯示的位址。在SMTP傳輸協定中需要寄件者位址、否則會產生錯誤。
- 警示收件者的電子郵件地址必須可供使用。收件者通常是網路管理員或儲存管理員的位址。您最多可以輸入20個電子郵件地址。

關於這項工作

此工作說明如何設定郵件伺服器、輸入寄件者和收件者的電子郵件地址、以及測試從「警示」頁面輸入的所有電子郵件地址。



您也可以從初始設定精靈設定電子郵件警示。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取*電子郵件*索引標籤。

如果尚未設定電子郵件伺服器、「電子郵件」標籤會顯示「設定郵件伺服器」。

3. 選擇*設定郵件伺服器*。

「設定郵件伺服器」對話方塊隨即開啟。

4. 輸入郵件伺服器資訊、然後按一下「儲存」。

- 郵件伺服器位址-輸入郵件伺服器的完整網域名稱、IPv4位址或IPv6位址。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

- 電子郵件寄件者地址-輸入有效的電子郵件地址、作為電子郵件寄件者。此地址會出現在電子郵件訊息的「寄件者」欄位中。
- 在電子郵件中加入聯絡資訊-若要在警示訊息中包含寄件者的聯絡資訊、請選取此選項、然後輸入姓名和電話號碼。按一下「儲存」後、電子郵件地址會出現在「警示」頁面的「電子郵件」標籤中。

5. 選取*新增電子郵件*。

「新增電子郵件」對話方塊隨即開啟。

6. 輸入警示收件者的一或多個電子郵件地址、然後按一下*「Add*（新增*）」。

電子郵件地址會顯示在「警示」頁面上。

7. 如果您想確定電子郵件地址有效、請按一下*測試所有電子郵件*、將測試訊息傳送給收件者。

結果

設定電子郵件警示之後、每當發生警示事件時、事件監視器都會將電子郵件訊息傳送給指定的收件者。

編輯警示的電子郵件地址

您可以變更接收電子郵件警示的收件者電子郵件地址。

開始之前

您要編輯的電子郵件地址必須在「警示」頁面的「電子郵件」標籤中定義。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取*電子郵件*索引標籤。
3. 從*電子郵件地址*表格中、選取您要變更的地址、然後按一下最右側的*編輯*（鉛筆）圖示。

該列會變成可編輯的欄位。

4. 輸入新地址、然後按一下*「Save*（勾號）」圖示。



如果您要取消變更、請選取*取消*（X）圖示。

結果

「警示」頁面的「電子郵件」索引標籤會顯示更新的電子郵件地址。

新增警示的電子郵件地址

您最多可新增20個電子郵件警示收件者。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取*電子郵件*索引標籤。
3. 選取*新增電子郵件*。

「新增電子郵件」對話方塊隨即開啟。

4. 在空白欄位中、輸入新的電子郵件地址。如果您要新增多個地址、請選取*新增其他電子郵件*以開啟另一個欄位。
5. 按一下「* 新增 *」。

結果

「警示」頁面的「電子郵件」標籤會顯示新的電子郵件地址。

刪除郵件伺服器或電子郵件地址以取得警示

您可以移除先前定義的郵件伺服器、使警示不再傳送至電子郵件地址、或是移除個別的電子郵件地址。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取*電子郵件*索引標籤。
3. 從表格中、執行下列其中一項：
 - 若要移除郵件伺服器、使警示不再傳送至電子郵件地址、請選取郵件伺服器的列。
 - 若要移除電子郵件地址、使警示不再傳送至此地址、請選取您要刪除之電子郵件地址的列。表右上角的*刪除*按鈕可供選擇。
4. 按一下*刪除*、然後確認作業。

編輯郵件伺服器以取得警示

您可以變更用於電子郵件警示的郵件伺服器位址和電子郵件寄件者位址。

開始之前

您要變更的郵件伺服器位址必須是可用的。位址可以是IPV4或IPV6位址、也可以是完整網域名稱。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取*電子郵件*索引標籤。
3. 選擇*設定郵件伺服器*。

此時將打開Configure Mail Server（配置郵件服務器）對話框。

4. 編輯郵件伺服器位址、寄件者資訊及聯絡資訊。
 - 郵件伺服器位址-編輯郵件伺服器的完整網域名稱、IPv4位址或IPv6位址。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

- 電子郵件寄件者地址-編輯電子郵件地址、以作為電子郵件寄件者。此地址會出現在電子郵件訊息的「寄件者」欄位中。
- 在電子郵件中加入聯絡資訊-若要編輯寄件者的聯絡資訊、請選取此選項、然後編輯姓名和電話號碼。

5. 按一下「* 儲存 *」。

管理SNMP警示

設定SNMP警示的社群和目的地

若要設定簡單網路管理傳輸協定（SNMP）警示、您必須至少識別一部伺服器、讓儲存陣列的事件監控器能夠傳送SNMP設陷。此組態需要伺服器的社群名稱和IP位址。

開始之前

- 網路伺服器必須設定SNMP服務應用程式。您需要此伺服器的網路位址（無論是IPv4或IPv6位址）、事件監控器才能將陷阱訊息傳送到該位址。您可以使用多部伺服器（最多允許10部伺服器）。
- 必須建立社群名稱、僅包含可列印的Ascii字元。社群名稱是類似網路伺服器密碼的字串、通常由網路管理員建立。最多可建立256個社群。
- 管理資訊庫（mib）檔案已複製並使用SNMP服務應用程式在伺服器上編譯。此mib檔案定義要監控和管理的資料。

如果您沒有mib檔案、可以從NetApp支援網站取得：

- 前往 "[NetApp支援](#)"。
- 單擊* Downloads （下載）。
- 按一下*軟體*。
- 找SANtricity 到您的管理軟體（例如、《Sf2系統管理程式》）、然後按一下右側的「* Go！（執行！）」。
- 按一下最新版本上的「檢視與下載」。
- 按一下頁面底部的*繼續*。
- 接受EULA。
- 向下捲動直到看到* SNMP陷阱的mib檔案*、然後按一下連結下載檔案。

關於這項工作

本工作說明如何識別SNMP伺服器的設陷目的地、然後測試您的組態。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「* SNMP *」索引標籤。

如果尚未設定社群、SNMP索引標籤會顯示「Configure Communities」（設定社群）。

3. 選擇*設定社群*。

「組態社群」對話方塊隨即開啟。

4. 在「社群名稱」欄位中、輸入網路伺服器的一或多個社群字串、然後按一下「儲存」。

「警示」頁面會顯示「新增設陷目的地」。

5. 選取*新增設陷目的地*。

「新增設陷目的地」對話方塊隨即開啟。

6. 輸入一個或多個陷阱目的地、選取其相關的社群名稱、然後按一下*「Add*（新增*）」。

- 陷阱目的地-輸入執行SNMP服務之伺服器的IPV4或IPv6位址。
- 社群名稱-從下拉式清單中、選取此設陷目的地的社群名稱。（如果您只定義一個社群名稱、該名稱就會出現在此欄位中。）
- 傳送驗證失敗**Trap ***-如果您想要在**SNMP**要求因為無法辨識的社群名稱而遭拒時、發出警示陷阱目的

地、請選取此選項（核取方塊）。按一下「*新增」之後、陷阱目的地和相關的社群名稱會出現在「警示」頁面的「* SNMP *」索引標籤中。

7. 若要確定設陷有效、請從表格中選取設陷目的地、然後按一下*測試設陷目的地*、將測試設陷傳送到設定的位址。

結果

每當發生警示事件時、事件監視器會將SNMP設陷傳送至伺服器。

編輯SNMP設陷的社群名稱

您可以編輯SNMP設陷的社群名稱、也可以將不同的社群名稱與SNMP設陷目的地建立關聯。

開始之前

必須建立社群名稱、僅包含可列印的Ascii字元。社群名稱是類似網路伺服器密碼的字串、由網路管理員建立。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「* SNMP *」索引標籤。

陷阱目的地和社群名稱會出現在表格中。

3. 編輯社群名稱如下：

- 若要編輯社群名稱、請選取*設定社群*。輸入新的社群名稱、然後按一下「儲存」。社群名稱只能由可列印的Ascii字元組成。
- 若要將社群名稱與新的陷阱目的地建立關聯、請從表格中選取社群名稱、然後按一下最右側的*編輯*（鉛筆）圖示。從「Community Name（社群名稱）」下拉式清單中、選取SNMP設陷目的地的新社群名稱、然後按一下*「Save」（儲存）*（勾選）圖示。



如果您要取消變更、請選取*取消*（X）圖示。

結果

「警示」頁面的「* SNMP *」索引標籤會顯示更新的社群。

新增SNMP設陷的社群名稱

您最多可以新增256個SNMP設陷社群名稱。

開始之前

必須建立社群名稱。社群名稱是類似網路伺服器密碼的字串、通常由網路管理員建立。它僅包含可列印的Ascii字元。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「* SNMP *」索引標籤。

陷阱目的地和社群名稱會出現在表格中。

3. 選擇*設定社群*。

「設定社群」對話方塊隨即開啟。

4. 選取*新增其他社群*。
5. 輸入新的社群名稱、然後按一下「儲存」。

結果

新的社群名稱會出現在「警示」頁面的「* SNMP *」索引標籤中。

移除SNMP設陷的社群名稱

您可以移除SNMP設陷的社群名稱。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「* SNMP *」索引標籤。

設陷目的地和社群名稱會顯示在警示頁面上。

3. 選擇*設定社群*。

「組態社群」對話方塊隨即開啟。

4. 選取您要刪除的社群名稱、然後按一下最右側的*移除* (X) 圖示。

如果陷阱目的地與此社群名稱相關聯、則「確認移除社群」對話方塊會顯示受影響的陷阱目的地地址。

5. 確認操作、然後按一下*移除*。

結果

社群名稱及其相關的設陷目的地會從「警示」頁面中移除。

設定SNMP mib變數

對於SNMP警示、您可以選擇性地設定出現在SNMP設陷中的管理資訊庫 (MIB) 變數。這些變數可傳回儲存陣列名稱、陣列位置及聯絡人。

開始之前

必須使用SNMP服務應用程式在伺服器上複製及編譯mib檔案。

如果您沒有MIBA檔案、可以取得如下：

- 前往 ["NetApp支援"](#)。
- 單擊* Downloads (下載) 。
- 按一下*軟體*。
- 找SANtricity 到您的管理軟體 (例如、《Sf2系統管理程式》)、然後按一下右側的「* Go ! (執行!) 」。

- 按一下最新版本的*「View & Download*（檢視與下載*）」。
- 按一下頁面底部的*繼續*。
- 接受EULA。
- 向下捲動直到看到* SNMP陷阱的mib檔案*、然後按一下連結下載檔案。

關於這項工作

本工作說明如何定義SNMP設陷的mib變數。這些變數可傳回下列值以回應SNMP GetRequest：

- 「*SysName*」（儲存陣列名稱）
- 「*SysLocation*」（儲存陣列的位置）
- 「*SysContact*」（系統管理員名稱）

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「* SNMP *」索引標籤。
3. 選擇*設定SNMP mib變數*。

此時將打開Configure SNMP mib Variables（配置SNMP mib變量）對話框。

4. 輸入下列一或多個值、然後按一下*「Save（儲存）」*。
 - 名稱：mib變數'*SysName*'的值。例如、輸入儲存陣列的名稱。
 - 位置：mib變數'*SysLocation*'的值。例如、輸入儲存陣列的位置。
 - 聯絡人：mib變數'*SysContact*'的值。例如、輸入負責儲存陣列的管理員。

結果

這些值會出現在儲存陣列警示的SNMP設陷訊息中。

新增SNMP警示的設陷目的地

您最多可以新增10部伺服器來傳送SNMP設陷。

開始之前

- 您要新增的網路伺服器必須使用SNMP服務應用程式進行設定。您需要此伺服器的網路位址（無論是IPv4或IPv6位址）、事件監控器才能將陷阱訊息傳送到該位址。您可以使用多部伺服器（最多允許10部伺服器）。
- 必須建立社群名稱、僅包含可列印的Ascii字元。社群名稱是類似網路伺服器密碼的字串、通常由網路管理員建立。最多可建立256個社群。
- 管理資訊庫（mib）檔案已複製並使用SNMP服務應用程式在伺服器上編譯。此mib檔案定義要監控和管理的資料。

如果您沒有mib檔案、可以從NetApp支援網站取得：

- 前往 "[NetApp支援](#)"。
- 單擊* Downloads（下載）。

- 按一下*軟體*。
- 找SANtricity 到您的管理軟體（例如、《Sf2系統管理程式》）、然後按一下右側的「* Go！（執行！）」。
- 按一下最新版本的*「View & Download*（檢視與下載*）」。
- 按一下頁面底部的*繼續*。
- 接受EULA。
- 向下捲動直到看到* SNMP陷阱的mib檔案*、然後按一下連結下載檔案。

步驟

1. 選擇*設定*>*警示*。
2. 選取「* SNMP *」索引標籤。

目前定義的設陷目的地會出現在表格中。

3. 選取*新增設陷的設計*。

「新增設陷目的地」對話方塊隨即開啟。

4. 輸入一個或多個陷阱目的地、選取其相關的社群名稱、然後按一下*「Add*（新增*）」。
- 陷阱目的地-輸入執行SNMP服務之伺服器的IPV4或IPv6位址。
- 社群名稱-從下拉式清單中、選取此設陷目的地的社群名稱。（如果您只定義一個社群名稱、該名稱就會出現在此欄位中。）
- 傳送驗證失敗**Trap ***-如果您想要在**SNMP**要求因為無法辨識的社群名稱而遭拒時、發出警示陷阱目的地、請選取此選項（核取方塊）。按一下「*新增」之後、陷阱目的地和相關的社群名稱會出現在表格中。
5. 若要確定設陷有效、請從表格中選取設陷目的地、然後按一下*測試設陷目的地*、將測試設陷傳送到設定的位址。

結果

每當發生警示事件時、事件監視器會將SNMP設陷傳送至伺服器。

刪除設陷目的地

您可以刪除設陷目的地位址、使儲存陣列的事件監視器不再將SNMP設陷傳送到該位址。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「* SNMP *」索引標籤。

陷阱目的地位址會出現在表格中。

3. 選取設陷目的地、然後按一下頁面右上角的*刪除*。
4. 確認操作、然後按一下*刪除*。

目的地位址不再出現在*警示*頁面上。

結果

刪除的設陷目的地不再從儲存陣列的事件監視器接收SNMP設陷。

管理系統記錄警示

設定系統記錄伺服器以發出警示

若要設定syslog警示、您必須輸入syslog伺服器位址和udp連接埠。最多允許五部syslog伺服器。

開始之前

- 系統記錄伺服器位址必須可用。此位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 系統記錄伺服器的udp連接埠號碼必須可用。此連接埠通常為514。

關於這項工作

此工作說明如何輸入syslog伺服器的位址和連接埠、然後測試您輸入的位址。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「系統記錄」索引標籤。

如果尚未定義syslog伺服器、則「警示」頁面會顯示「新增Syslog伺服器」。

3. 按一下「新增**Syslog**伺服器」。

「新增**Syslog**伺服器」對話方塊隨即開啟。

4. 輸入一或多個syslog伺服器的資訊（最多五個）、然後按一下*「Add*（新增*）」。
 - 伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。
 - * udp Port*-通常syslog的udp連接埠為514。下表顯示已設定的syslog伺服器。
5. 若要傳送測試警示至伺服器位址、請選取*測試所有Syslog伺服器*。

結果

每當發生警示事件時、事件監控器都會傳送警示至syslog伺服器。

編輯系統記錄伺服器以取得警示

您可以編輯用於接收系統記錄警示的伺服器位址。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「系統記錄」索引標籤。
3. 從表中選取syslog伺服器位址、然後按一下最右側的*編輯*（鉛筆）圖示。

該列會變成可編輯的欄位。

4. 編輯伺服器位址和udp連接埠號碼、然後按一下*「Save*（勾選）」圖示。

結果

更新的伺服器位址會出現在表格中。

新增系統記錄伺服器以供警示

您最多可以新增五部伺服器來執行系統記錄警示。

開始之前

- 系統記錄伺服器位址必須可用。此位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 系統記錄伺服器的udp連接埠號碼必須可用。此連接埠通常為514。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「系統記錄」索引標籤。
3. 選擇* Add Syslog Servers*（添加Syslog服務器*）。

此時會開啟「新增Syslog伺服器」對話方塊。

4. 選取*新增其他syslog伺服器*。
5. 輸入syslog伺服器的資訊、然後按一下*「Add*（新增*）」。
- 系統記錄伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。
- * udp Port*-通常syslog的udp連接埠為514。



最多可設定五部syslog伺服器。

結果

系統記錄伺服器位址會出現在表格中。

刪除系統記錄伺服器以取得警示

您可以刪除syslog伺服器、使其不再接收警示。

步驟

1. 選取*功能表：設定[警示]*。
2. 選取「系統記錄」索引標籤。
3. 選取syslog伺服器位址、然後按一下右上角的*移除*。

「確認刪除Syslog伺服器」對話方塊隨即開啟。

4. 確認操作、然後按一下*刪除*。

結果

您移除的伺服器不再從事件監視器接收警示。

常見問題集

停用警示時該怎麼辦？

如果您希望系統管理員收到儲存陣列中發生重要事件的通知、您必須設定警示方法。

若為SANtricity 以《支援系統管理程式》管理的儲存陣列、您可從「警示」頁面設定警示。警示通知可透過電子郵件、SNMP設陷或系統記錄訊息傳送。此外、您也可以從初始設定精靈設定電子郵件警示。

如何設定SNMP或syslog警示？

除了電子郵件警示之外、您也可以設定要透過簡單網路管理傳輸協定（SNMP）設陷或透過系統記錄訊息傳送的警示。

若要設定SNMP或syslog警示、請前往功能表：設定[警示]。

為什麼陣列與警示之間的時間戳記不一致？

當儲存陣列傳送警示時、對於接收警示的目標伺服器或主機所在的時區而言、它不正確。相反地、儲存陣列會使用本機時間（GMT）來建立警示記錄所用的時間戳記。因此、您可能會看到儲存陣列與收到警示的伺服器或主機之間的時間戳記不一致。

由於儲存陣列在傳送警示時區不正確、因此警示上的時間戳記為相對於GMT-的時間區偏移值為零。若要計算適合您當地時區的時間戳記、您應該決定小時與時間的時差、然後從時間戳記中新增或減去該值。



若要避免此問題、請在儲存陣列控制器上設定網路時間傳輸協定（NTP）。NTP可確保控制器永遠同步至正確的時間。

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提供保護、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、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
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VMware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（NVS RAM）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、名為「shorage-array-configuration . cfg」。

完成後

若要將儲存的儲存陣列組態載入其他儲存陣列、請使用SANtricity 含有「-f」選項的指令行介面（SMcli）來套用「.cfg」檔案。



您也可以使用Unified Manager介面將儲存陣列組態載入其他儲存陣列（選取*功能表：「Manage（匯入設定）」*）。

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32 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。
- 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、能夠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VMware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。

關於這項工作

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。



對於EF600儲存系統、此功能預設為停用。

此設定會影響下列作業：

- 開啟（預設）-使用CLI和某些其他工具（例如OCI介面卡）設定鏡像所需的設定。
- 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*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？

儲存陣列的控制器將其快取組織成「區塊」、這是大小可為8、16、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。

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32 KiB、但您可以將值設為8、16、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」頁面上的「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。

系統：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CHAPSECUR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。
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。

期限	說明
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「System（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）。



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*功能表：設定[系統]*。
2. 在「* iSCSI設定*」下、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 Ports*（設定iSCSI連接埠*）選項。

3. 選取含有您要設定之iSCSI連接埠的控制器。
4. 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」。
5. 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*顯示更多連接埠設定*連結。

連接埠設定	說明
啟用IPv4 /啟用IPv6	<p>選取一個或兩個選項、以啟用對IPv4和IPv6網路的支援。</p> <div>  <p>如果您要停用連接埠存取、請取消選取這兩個核取方塊。</p> </div>
TCP接聽連接埠（按一下*顯示更多連接埠設定*即可取得）。	<p>如有必要、請輸入新的連接埠號碼。</p> <p>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。</p>
MTU大小（按一下*顯示更多連接埠設定*即可取得）。	<p>如有必要、請為最大傳輸單元（MTU）輸入新的位元組大小。</p> <p>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。</p>
啟用ICMP Ping回應	<p>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。</p>

如果您選取*啟用IPv4、則會在您按一下*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、則會在您按一下*下一步*之後、開啟一個對話方塊來選取**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[Next*（下一步）]之後、隨即開啟[IPv6設定]對話方塊。

- 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。

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*顯示更多設定*即可取得）。	<p>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。</p> <p>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。</p>

7. 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_secret_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」。

此時將出現「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「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：設定[系統]*。
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. 選用：*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。

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：設定[系統]*。
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*。

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. 選用：*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。

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：設定[系統]*。
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。

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。

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。

步驟

1. 選取*功能表：設定[系統]*
2. 在* iSER over InfiniBand settings 下、選取 Configure iSER over InfiniBand連接埠*。
3. 按一下要設定的InfiniBand連接埠上的iSER控制器。單擊 * 下一步 * 。
4. 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。
5. 單擊*完成*。
6. 按一下* Yes*、即可透過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。

步驟

1. 選取*功能表：設定[系統]*。
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. 選用：*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）介面統計資料上的iSER。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	<div>1. 選取*硬體*。</div> <div>2. 選擇*顯示櫃背面*。</div> <div>3. 選取控制器。</div> <div>4. 選取*透過InfiniBand連接埠設定iSER*。</div> <div>或</div> <div>1. 選取*功能表：設定[系統]*。</div> <div>2. 向下捲動至* iSER over InfiniBand settings 、然後選取 Configure iSER over InfiniBand Ports*。</div>
檢視InfiniBand統計資料的iSER	<div>1. 選取*功能表：設定[系統]*。</div> <div>2. 向下捲動至「InfiniBand設定*上的* iSER」、然後選取「View iSER over InfiniBand Statistics *」。</div>

系統：NVMe設定

概念

NVMe總覽

有些控制器包含一個連接埠、可在光纖架構上實作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？

_NVMe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。NVMe儲存陣列（稱為_Subsystem）可由使用光纖的主機存取。NVMe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_namespace_）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。

期限	說明
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。
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「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。



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*功能表：設定[系統]*。
2. 在* NVMe over InfiniBand設定*下、選取* Configure NVMe over InfiniBand連接埠*。
3. 選取要設定NVMe over InfiniBand連接埠的控制器。單擊 * 下一步 *。
4. 從下拉式清單中選取您要設定的HIC連接埠、然後輸入IP位址。

如果您要使用支援200GB HIC的EF600儲存陣列、此對話方塊會顯示兩個IP位址欄位、一個用於實體連接埠（外部）、另一個用於虛擬連接埠（內部）。您應該為兩個連接埠指派唯一的IP位址。這些設定可讓主機在每個連接埠之間建立路徑、並讓HIC達到最大效能。如果您未將IP位址指派給虛擬連接埠、HIC將以大約一半的能力速度執行。

5. 單擊*完成*。

6. 按一下* Yes*、重設InfiniBand連接埠上的NVMe。

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「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。

步驟

1. 選取*功能表：設定[系統]*。
2. 在* NVMe over ROCE設定*下、選取* Configure NVMe over ROCE連接埠*。
3. 選取要設定NVMe over RoCE連接埠的控制器。單擊 * 下一步 *。
4. 從下拉式清單中選取您要設定的HIC連接埠。單擊 * 下一步 *。
5. 設定連接埠設定。

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*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、則會在您按一下*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、則會在您按一下*下一步*之後、開啟一個對話方塊來選取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[Next*（下一步）]之後、隨即開啟[IPv6設定]對話方塊。

1. 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。如果您要使用支援200GB HIC的EF600儲存陣列、此對話方塊會顯示兩組網路參數欄位、一個用於實體連接埠（外部）、另一個用於虛擬連接埠（內部）。您應該為兩個連接埠指派獨特的參數。這些設定可讓主機在每個連接埠之間建立路徑、並讓HIC達到最大效能。如果您未將IP位址指派給虛擬連接埠、HIC將以大約一半的能力速度執行。

2. 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* -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。
- * 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。此索引標籤僅會在NVMe over Fabrics連接埠可用時顯示。

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：設定[系統]*。
2. 選取*「View NVMe over Fabrics Statistic*」。
3. 選用：*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NVMe over Fabrics統計資料？

「View NVMe over Fabrics Statistics」（檢視NVMe over Fabrics統計資料）對話方塊會顯示NVMe子系統和RDMA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。此索引標籤僅會在NVMe over Fabrics連接埠可用時顯示。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	<ol style="list-style-type: none"> 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 *。 <p>或</p> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 * <p>或</p> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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*。

為什麼一個實體連接埠有兩個IP位址？

EF600儲存陣列可包含兩個HIC、一個是外部的、另一個是內部的。

在此組態中、外部HIC會連接至內部輔助HIC。您可以從外部HIC存取的每個實體連接埠、都有一個與內部HIC相關的虛擬連接埠。

若要達到最高200GB效能、您必須為實體和虛擬連接埠指派唯一的IP位址、讓主機能夠建立每個連接埠的連線。如果您未將IP位址指派給虛擬連接埠、HIC將以大約一半的能力速度執行。

為什麼一個實體連接埠有兩組參數？

EF600儲存陣列可包含兩個HIC、一個是外部的、另一個是內部的。

在此組態中、外部HIC會連接至內部輔助HIC。您可以從外部HIC存取的每個實體連接埠、都有一個與內部HIC相關的虛擬連接埠。

若要達到最高200GB效能、您必須為實體和虛擬連接埠指派參數、讓主機能夠建立每個連接。如果您未將參數指派給虛擬連接埠、HIC將以大約一半的能力速度執行。

系統：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、可能需要啟用金鑰。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、啟用識別碼和啟用功能代碼。
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的程式碼。對於功能套件、此程式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. 請前往*您產品的軟體授權*。
 - 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、啟用識別碼及功能啟動代碼。

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。



如果您想要停用優質功能、必須在命令列介面（CLI）中使用停用儲存陣列功能命令（「停用儲存陣列（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。

下載命令列介面（CLI）

您可以從System Manager下載命令列介面（CLI） 套件。CLI提供一種文字型方法、可用來設定及監控儲存陣列。它透過https通訊、並使用與外部安裝管理軟體套件中可用CLI相同的語法。不需要金鑰即可下載CLI。

開始之前

- 您必須在打算執行CLI命令的管理系統上提供Java執行時間環境（JRE）版本8及更新版本。

步驟

1. 選取*功能表：設定[系統]*。
2. 在*附加元件*下、選取*命令列介面*。

下載至瀏覽器的ZIP套件。

3. 將ZIP檔案儲存至管理系統、以便為儲存陣列執行CLI命令、然後擷取檔案。

您現在可以從作業系統提示字元（例如DOS C：提示字元）執行CLI命令。CLI命令參考可從System Manager使用者介面右上角的「說明」功能表取得。

系統：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内部金鑰管理。
- 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。移至*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	<div>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。</div> <div> 磁碟機安全性密碼與儲存陣列的管理員密碼無關。</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、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，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。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。
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*-輸入用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠號碼。
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*。

「備份安全金鑰」對話方塊隨即開啟。
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. *選用*：*將滑鼠移到磁碟機編號上方、即可查看磁碟機的位置（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内部金鑰管理。
- 外部金鑰管理伺服器上的外部金鑰管理。

在建立内部安全金鑰之前、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。

然後您可以建立内部安全金鑰、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。移至*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）。
- 如果您要重設鎖定的NVMe磁碟機、則必須輸入磁碟機的安全ID。若要找出安全ID、您必須實際移除磁碟機、並在磁碟機標籤上找到PSID字串（最多32個字元）。開始操作之前、請先確定已重新安裝磁碟機。

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功能時、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。

存取管理

概念

存取管理的運作方式

存取管理是SANtricity 一種在《Sytricity System Manager》中建立使用者驗證的方法。

存取管理組態和使用者的運作方式如下：

1. 系統管理員使用包含「安全性管理」權限的使用者設定檔登入System Manager。



首次登入時、使用者名稱「admin」會自動顯示、無法變更。「admin」使用者可完整存取系統中的所有功能。

2. 系統管理員會在使用者介面中導覽至「存取管理」。儲存陣列已預先設定為使用本機使用者角色、這是RBAC（角色型存取控制）功能的實作。
3. 系統管理員可設定下列一或多種驗證方法：
 - 本機使用者角色-驗證是透過儲存陣列中強制執行的RBAC功能來管理。本機使用者角色包括預先定義的使用者設定檔和具有特定存取權限的角色。系統管理員可以使用這些本機使用者角色做為單一驗證方法、或搭配目錄服務使用。除了為使用者設定密碼之外、不需要進行任何組態。
 - 目錄服務-驗證是透過LDAP（輕量型目錄存取傳輸協定）伺服器和目錄服務（例如Microsoft的Active Directory）來管理。系統管理員會連線至LDAP伺服器、然後將LDAP使用者對應至儲存陣列內嵌的本機使用者角色。
 - * SAML *-驗證是透過身分識別供應商（IDP）、使用安全聲明標記語言（SAML）2.0來管理。系統管理員會在IDP系統與儲存陣列之間建立通訊、然後將IDP使用者對應至儲存陣列內嵌的本機使用者角色。
4. 系統管理員會為使用者提供System Manager的登入認證。
5. 使用者輸入認證資料以登入系統。



如果使用SAML和SSO（單一登入）來管理驗證、系統可能會略過System Manager登入對話方塊。

登入期間、系統會執行下列背景工作：

- 根據使用者帳戶驗證使用者名稱和密碼。
- 根據指派的角色來決定使用者的權限。
- 讓使用者存取使用者介面中的工作。
- 在介面右上角顯示使用者名稱。

System Manager中可用的工作

存取工作取決於使用者指派的角色、包括下列項目：

- 儲存設備管理-對儲存物件（例如磁碟區和磁碟集區）的完整讀寫存取權、但無法存取安全性組態。
- 安全管理：存取存取管理、憑證管理、稽核記錄管理中的安全組態、以及開啟或關閉舊版管理介面（符號）的功能。
- 支援**admin**：存取儲存陣列上的所有硬體資源、故障資料、MEL事件及控制器韌體升級。無法存取儲存物件或安全性組態。
- 監控-對所有儲存物件的唯讀存取、但無法存取安全性組態。

無法使用的工作會呈現灰色、或不會顯示在使用者介面中。例如、擁有「監控」角色的使用者可以檢視所有關於磁碟區的資訊、但無法存取修改該磁碟區的功能。諸如*複製服務*和*新增至工作負載*等功能的索引標籤將會呈現灰色、僅提供*檢視/編輯設定*。

不受SANtricity 《不統一化管理程式》和SANtricity 《不統一化儲存管理程式》的限制

如果已針對儲存陣列設定SAML、使用者將無法從SANtricity 「支援整合管理程式」 SANtricity 或「支援儲存管理程式」介面探索或管理該陣列的儲存設備。

設定本機使用者角色和目錄服務時、使用者必須先輸入認證資料、才能執行下列任一功能：

- 重新命名儲存陣列
- 升級控制器韌體
- 正在載入儲存陣列組態
- 執行指令碼
- 嘗試在未使用的工作階段逾時時執行作用中作業

存取管理術語

瞭解存取管理條款如何適用於您的儲存陣列。

期限	說明
Active Directory	Active Directory（AD）是一項Microsoft目錄服務、用於Windows網域網路的LDAP。

期限	說明
連結	連結作業用於驗證目錄伺服器的用戶端。綁定通常需要帳戶和密碼認證、但有些伺服器允許匿名連結作業。
CA	憑證授權單位（CA）是信任的實體、可發行稱為數位憑證的電子文件、以確保國際網路安全。這些憑證可識別網站擁有者、以便在用戶端與伺服器之間進行安全連線。
憑證	憑證可識別站台的擁有者、以確保安全性、防止攻擊者模擬站台。憑證包含網站擁有者的相關資訊、以及認證（簽署）此資訊的信任實體身分。
IDP	身分識別提供者（IDP）是外部系統、用於向使用者要求認證、以及判斷該使用者是否已成功驗證。IDP可設定為提供多因素驗證、並使用任何使用者資料庫、例如Active Directory。您的安全團隊負責維護IDP。
LDAP	輕量型目錄存取傳輸協定（LDAP）是用於存取及維護分散式目錄資訊服務的應用程式傳輸協定。此傳輸協定可讓許多不同的應用程式和服務連線至LDAP伺服器、以驗證使用者。
RBAC	角色型存取控制（RBAC）是一種根據個別使用者角色來管理電腦或網路資源存取的方法。RBAC控制會在儲存陣列上強制執行、並包含預先定義的角色。
SAML	安全聲明標記語言（SAML）是兩個實體之間驗證與授權的XML型標準。SAML允許多因素驗證、使用者必須提供兩個或多個項目來證明身分（例如密碼和指紋）。儲存陣列的內嵌SAML功能符合SAML2.0標準、可用於身分識別聲明、驗證及授權。
SP	服務供應商（SP）是控制使用者驗證與存取的系統。使用SAML設定存取管理時、儲存陣列會做為服務供應商、以要求身分識別供應商進行驗證。
SSO	單一登入（SSO）是一種驗證服務、可讓一組登入認證資料存取多個應用程式。

對應角色的權限

在儲存陣列上強制執行的RBAC（角色型存取控制）功能包括預先定義的使用者設定檔、其中有一個或多個角色對應到這些設定檔。每個角色都有權限存取SANtricity 功能、可在《系統管理程式》中執行各項工作。

使用者設定檔和對應角色可從任一系統管理員使用者介面的*功能表：設定[Access Management（存取管理）>本機使用者角色]*存取。

這些角色可讓使用者存取工作、如下所示：

- 儲存設備管理-對儲存物件（例如磁碟區和磁碟集區）的完整讀寫存取權、但無法存取安全性組態。
- 安全管理：存取存取管理、憑證管理、稽核記錄管理中的安全組態、以及開啟或關閉舊版管理介面（符號）的功能。

- 支援**admin**：存取儲存陣列上的所有硬體資源、故障資料、MEL事件及控制器韌體升級。無法存取儲存物件或安全性組態。
- 監控-對所有儲存物件的唯讀存取、但無法存取安全性組態。

如果使用者沒有特定工作的權限、則該工作會呈現灰色、或不會顯示在使用者介面中。

具有本機使用者角色的存取管理

對於存取管理、系統管理員可以使用儲存陣列中強制執行的RBAC（角色型存取控制）功能。這些功能稱為「本機使用者角色」。

組態工作流程

本機使用者角色是針對儲存陣列預先設定的。若要使用本機使用者角色進行驗證、系統管理員可以執行下列動作：

1. 系統管理員SANtricity 使用包含「安全管理」權限的使用者設定檔登入到「功能不全系統管理程式」。



「admin」使用者可完整存取系統中的所有功能。

2. 系統管理員會檢閱預先定義且無法修改的使用者設定檔。
3. *選用：*系統管理員會為每個使用者設定檔指派新密碼。
4. 使用者使用指派的認證登入系統。

管理

只使用本機使用者角色進行驗證時、系統管理員可以執行下列管理工作：

- 變更密碼。
- 設定密碼的最小長度。
- 允許使用者不使用密碼登入。

使用目錄服務進行存取管理

對於存取管理、系統管理員可以使用LDAP（輕量型目錄存取傳輸協定）伺服器 and 目錄服務、例如Microsoft的Active Directory。

組態工作流程

如果在網路中使用LDAP伺服器和目錄服務、則組態作業如下：

1. 系統管理員SANtricity 使用包含「安全管理」權限的使用者設定檔登入到「功能不全系統管理程式」。



「admin」使用者可完整存取系統中的所有功能。

2. 系統管理員會輸入LDAP伺服器的組態設定。設定包括網域名稱、URL及連結帳戶資訊。
3. 如果LDAP伺服器使用安全傳輸協定（LDAPS）、則系統管理員會上傳憑證授權單位（CA）憑證鏈結、以便

在LDAP伺服器與儲存陣列之間進行驗證。

4. 建立伺服器連線後、系統管理員會將使用者群組對應至儲存陣列的角色。這些角色已預先定義、無法修改。
5. 系統管理員會測試LDAP伺服器與儲存陣列之間的連線。
6. 使用者使用指派的LDAP/Directory Services認證登入系統。

管理

使用目錄服務進行驗證時、系統管理員可以執行下列管理工作：

- 新增目錄伺服器。
- 編輯目錄伺服器設定。
- 將LDAP使用者對應至本機使用者角色。
- 移除目錄伺服器。

使用SAML進行存取管理

對於存取管理、系統管理員可以使用陣列內嵌的安全聲明標記語言（SAML）2.0功能。

組態工作流程

SAML組態運作方式如下：

1. 系統管理員使用包含「安全性管理」權限的使用者設定檔登入System Manager。



「admin」使用者可以完整存取System Manager中的所有功能。

2. 系統管理員會移至「存取管理」下的「* SAML」索引標籤。
3. 系統管理員會設定與身分識別供應商（IDP）的通訊。IDP是一種外部系統、用於向使用者要求認證、並判斷使用者是否已成功驗證。若要設定與儲存陣列的通訊、系統管理員會從IDP系統下載IDP中繼資料檔案、然後使用System Manager將檔案上傳至儲存陣列。
4. 系統管理員會在服務供應商與IDP之間建立信任關係。服務供應商會控制使用者授權；在此情況下、儲存陣列中的控制器會扮演服務供應商的角色。若要設定通訊、系統管理員會使用System Manager匯出每個控制器的服務供應商中繼資料檔案。接著、系統管理員會從IDP系統將這些中繼資料檔案匯入IDP。



系統管理員也應確保IDP支援在驗證時傳回名稱ID的功能。

5. 系統管理員會將儲存陣列的角色對應至IDP中定義的使用者屬性。為達成此目的、系統管理員會使用System Manager建立對應。
6. 系統管理員會測試SSO登入IDP URL。此測試可確保儲存陣列與IDP之間的通訊。



一旦啟用SAML、您就無法透過使用者介面停用SAML、也無法編輯IDP設定。如果您需要停用或編輯SAML組態、請聯絡技術支援部門以取得協助。

7. 系統管理員可從System Manager啟用儲存陣列的SAML。
8. 使用者使用SSO認證登入系統。

管理

使用SAML進行驗證時、系統管理員可以執行下列管理工作：

- 修改或建立新的角色對應
- 匯出服務供應商檔案

存取限制

啟用SAML時、使用者無法從SANtricity「支援統一化管理程式」或SANtricity「支援儲存管理程式」介面探索或管理該陣列的儲存設備。

此外、下列用戶端無法存取儲存陣列服務和資源：

- 企業管理所需時間（EMW）
- 命令列介面（CLI）
- 軟體開發人員套件（SDK）用戶端
- 頻內用戶端
- HTTP基本驗證REST API用戶端
- 使用標準REST API端點登入

使用方法

檢視本機使用者角色

從「本機使用者角色」索引標籤、您可以檢視使用者設定檔與預設角色的對應。這些對應是儲存陣列中強制執行的RBAC（角色型存取控制）的一部分。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

無法變更使用者設定檔和對應。只能修改密碼。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*本機使用者角色*索引標籤。

下表顯示使用者設定檔：

- 根系統管理（admin）-擁有系統中所有功能存取權的超級系統管理員。此使用者設定檔包含所有角色。
- * Storage admin*（儲存設備）：負責所有儲存資源配置的管理員。此使用者設定檔包含下列角色：儲存管理員、支援管理員及監控。
- 安全管理（安全性）：負責安全性組態的使用者、包括存取管理、憑證管理及啟用安全功能的磁碟機功能。此使用者設定檔包含下列角色：安全性管理和監控。
- 支援管理（支援）：負責硬體資源、故障資料及韌體升級的使用者。此使用者設定檔包含下列角色

：Support Admin和Monitor。

- 。監控（監控）-對系統具有唯讀存取權的使用者。此使用者設定檔僅包含「監控」角色。

變更密碼

您可以在「存取管理」中變更每個使用者設定檔的使用者密碼。

開始之前

- 您必須以本機系統管理員的身分登入、其中包含root系統管理權限。
- 您必須知道本機系統管理員密碼。

關於這項工作

選擇密碼時請謹記以下準則：

- 任何新的本機使用者密碼必須符合或超過最小密碼的目前設定（在「檢視/編輯設定」中）。
- 密碼區分大小寫。
- 設定後置空格時、不會從密碼中刪除。如果密碼中包含空格、請務必小心。
- 為了提高安全性、請使用至少15個英數字元、並經常變更密碼。



在System Manager中變更密碼也會在命令列介面（CLI）中變更密碼。此外、密碼變更也會導致使用者的作用中工作階段終止。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*本機使用者角色*索引標籤。
3. 從表格中選取使用者。

「變更密碼」按鈕隨即可用。

4. 選擇*變更密碼*。

「變更密碼」對話方塊隨即開啟。

5. 如果未設定本機使用者密碼的最小密碼長度、您可以勾選此方塊、要求選取的使用者輸入密碼以存取儲存陣列、然後輸入所選使用者的新密碼。
6. 輸入您的本機系統管理員密碼、然後按一下*變更*。

結果

如果使用者目前登入、密碼變更會導致使用者的作用中工作階段終止。

變更本機使用者密碼設定

您可以設定儲存陣列上所有新的或更新的本機使用者密碼所需的最小長度。您也可以允許本機使用者在不輸入密碼的情況下存取儲存陣列。

開始之前

- 您必須以本機系統管理員的身分登入、其中包含root系統管理權限。

關於這項工作

設定本機使用者密碼的最小長度時、請謹記下列準則：

- 設定變更不會影響現有的本機使用者密碼。
- 本機使用者密碼的最小長度設定必須介於0到30個字元之間。
- 任何新的本機使用者密碼必須符合或超過目前的最小長度設定。
- 如果您希望本機使用者在未輸入密碼的情況下存取儲存陣列、請勿設定密碼的最小長度。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*本機使用者角色*索引標籤。
3. 選取*檢視/編輯設定*按鈕。

「本機使用者密碼設定」對話方塊隨即開啟。

4. 執行下列其中一項：
 - 若要允許本機使用者存取儲存陣列（而不輸入密碼）、請取消核取「至少需要所有本機使用者密碼」核取方塊。
 - 若要設定所有本機使用者密碼的最小密碼長度、請勾選「要求所有本機使用者密碼至少為」核取方塊、然後使用微調方塊設定所有本機使用者密碼的最小長度要求。

任何新的本機使用者密碼必須符合或超過目前設定。

5. 按一下「* 儲存 *」。

新增目錄伺服器

若要設定存取管理驗證、您可以在儲存陣列與LDAP伺服器之間建立通訊、然後將LDAP使用者群組對應至陣列的預先定義角色。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 必須在目錄服務中定義使用者群組。
- LDAP伺服器認證必須可用、包括網域名稱、伺服器URL、以及可選的連結帳戶使用者名稱和密碼。
- 對於使用安全傳輸協定的LDAPS伺服器、LDAP伺服器的憑證鏈結必須安裝在本機機器上。

關於這項工作

新增目錄伺服器的程序分為兩個步驟。首先輸入網域名稱和URL。如果您的伺服器使用安全傳輸協定、則如果CA憑證是由非標準簽署授權單位簽署、您也必須上傳該憑證以進行驗證。如果您有綁定帳戶的認證、也可以輸入使用者帳戶名稱和密碼。接下來、您可以將LDAP伺服器的使用者群組對應至儲存陣列的預先定義角色。




在新增LDAP伺服器的程序期間、舊版管理介面將會停用。舊版管理介面（符號）是儲存陣列與管理用戶端之間的通訊方法。停用時、儲存陣列和管理用戶端會使用更安全的通訊方法（REST API over https）。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 從*目錄服務*索引標籤、選取*新增目錄伺服器*。

此時將打開Add Directory Server（添加目錄服務器）對話框。

3. 在*伺服器設定*索引標籤中、輸入LDAP伺服器的認證資料。

設定	說明
組態設定	網域
輸入LDAP伺服器的網域名稱。若為多個網域、請在以逗號分隔的清單中輸入網域。網域名稱用於登入 (<i>username@domain</i>)、以指定要驗證的目錄伺服器。	伺服器URL
以「LDAP[s]/* host* : * port*」的形式輸入存取LDAP伺服器的URL。	上傳憑證 (選用)
<div data-bbox="245 905 302 957"></div> <p data-bbox="358 779 477 1083">此欄位只有在上述伺服器URL欄位中指定LDAP S傳輸協定時才會顯示。</p> <p data-bbox="212 1136 513 1272">按一下*瀏覽*並選取要上傳的CA憑證。這是用於驗證LDAP伺服器的信任憑證或憑證鏈結。</p>	連結帳戶 (選用)
輸入唯讀使用者帳戶、以便針對LDAP伺服器進行搜尋查詢、並在群組內進行搜尋。以LDAP類型格式輸入帳戶名稱。例如、如果繫結使用者稱為「bindacc」、則您可以輸入一個值、例如「CN=bindacct,CN=Users、DC=cpoc、DC=local」。	連結密碼 (選用)

設定		說明
 <p>當您在上方輸入連結帳戶時、就會顯示此欄位。</p> <p>輸入綁定帳戶的密碼。</p>		在新增之前先測試伺服器連線
	<p>如果您要確保儲存陣列能夠與您輸入的LDAP伺服器組態通訊、請選取此核取方塊。按一下對話方塊底部的*「Add*（新增*）」之後、就會進行測試。如果選取此核取方塊且測試失敗、則不會新增組態。您必須解決錯誤或取消選取核取方塊、才能跳過測試並新增組態。</p>	**權限設定
搜尋基礎DN		輸入要搜尋使用者的LDAP內容、通常格式為「CN=Users、DC=cOPC、DC=local」。
使用者名稱屬性		輸入繫結至使用者ID以進行驗證的屬性。例如：「AMAccountName」。
群組屬性		輸入使用者的群組屬性清單、以用於群組對角色對應。例如：「memberof、managedObjects」。

- 按一下「**角色對應」索引標籤。
- 將LDAP群組指派給預先定義的角色。一個群組可以有多個指派的角色。

欄位詳細資料

設定	說明
對應	群組DN
指定要對應之LDAP使用者群組的群組辨別名稱(DN)。	角色



所有使用者（包括系統管理員）都必須具備「監控」角色。沒有監控角色的任何使用者、System Manager將無法正常運作。

1. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。
2. 完成對應後、按一下*「Add*（新增*）」。

系統會執行驗證、確保儲存陣列和LDAP伺服器能夠通訊。如果出現錯誤訊息、請檢查在對話方塊中輸入的認證資料、並視需要重新輸入資訊。

編輯目錄伺服器設定和角色對應

如果您先前在Access Management中設定了目錄伺服器、則可以隨時變更其設定。設定包括伺服器連線資訊和群組對角色對應。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 必須定義目錄伺服器。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*目錄服務*索引標籤。
3. 如果定義了多個伺服器、請從表格中選取您要編輯的伺服器。
4. 選取*檢視/編輯設定*。

此時會開啟「目錄伺服器設定」對話方塊。

5. 在*伺服器設定*索引標籤中、變更所需的設定。

設定	說明
組態設定	網域
LDAP伺服器的網域名稱。若為多個網域、請在以逗號分隔的清單中輸入網域。網域名稱用於登入（ <i>username@domain</i> ）、以指定要驗證的目錄伺服器。	伺服器URL
以「LDAP[s]//* host* : * port*」形式存取LDAP伺服器的URL。	連結帳戶（選用）

設定	說明
用於針對LDAP伺服器進行搜尋查詢及在群組內搜尋的唯讀使用者帳戶。	連結密碼（選用）
綁定帳戶的密碼。（輸入連結帳戶時、會顯示此欄位。）	儲存前先測試伺服器連線
檢查儲存陣列是否能與LDAP伺服器組態通訊。在您按一下對話方塊底部的*「Save"（儲存）*之後、就會進行測試。如果選取此核取方塊且測試失敗、則不會變更組態。您必須解決錯誤或取消選取核取方塊、才能跳過測試並重新編輯組態。	權限設定
搜尋基礎DN	要搜尋使用者的LDAP內容、通常格式為「CN=Users、DC=cOPC、DC=local」。
使用者名稱屬性	繫結至使用者ID以進行驗證的屬性。例如：「AMAccountName」。
群組屬性	使用者上的群組屬性清單、用於群組對角色對應。例如：「memberof、managedObjects'。

6. 在*角色對應*索引標籤中、變更所需的對應。

設定	說明
對應	群組DN
要對應之LDAP使用者群組的網域名稱。	角色



所有使用者（包括系統管理員）都必須具備「監控」角色。沒有監控角色的任何使用者、System Manager將無法正常運作。

7. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。

8. 按一下「* 儲存 *」。

結果

完成此工作之後、任何作用中的使用者工作階段都會終止。只會保留目前的使用者工作階段。

移除目錄伺服器

若要中斷目錄伺服器與儲存陣列之間的連線、您可以從「存取管理」頁面移除伺服器資訊。如果您設定了新的伺服器、然後想要移除舊的伺服器、則可能需要執行此工作。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

完成此工作之後、任何作用中的使用者工作階段都會終止。只會保留目前的使用者工作階段。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*目錄服務*索引標籤。
3. 從清單中選取您要刪除的目錄伺服器。
4. 按一下「移除」。

「移除目錄伺服器」對話方塊隨即開啟。

5. 在欄位中輸入「移除」、然後按一下「移除」。

目錄伺服器組態設定、權限設定和角色對應都會移除。使用者無法再使用此伺服器的認證登入。

設定SAML

若要設定存取管理的驗證、您可以使用儲存陣列內嵌的安全聲明標記語言（SAML）功能。此組態會在身分識別供應商與儲存供應商之間建立連線。

關於這項工作

身分識別提供者（IDP）是外部系統、用於向使用者要求認證、以及判斷該使用者是否已成功驗證。IDP可設定為提供多因素驗證、並使用任何使用者資料庫、例如Active Directory。您的安全團隊負責維護IDP。服務供應商（SP）是控制使用者驗證與存取的系統。使用SAML設定存取管理時、儲存陣列會做為服務供應商、以要求身分識別供應商進行驗證。若要在IDP與儲存陣列之間建立連線、您可以在這兩個實體之間共用中繼資料檔案。接下來、您要將IDP使用者實體對應至儲存陣列角色。最後、您要先測試連線和SSO登入、再啟用SAML。



- SAML與目錄服務*。如果您在將目錄服務設定為驗證方法時啟用SAML、則SAML會取代System Manager中的目錄服務。如果稍後停用SAML、目錄服務組態會返回其先前的組態。



- *編輯和停用。*一旦啟用SAML、您就無法透過使用者介面停用SAML、也無法編輯IDP設定。如果您需要停用或編輯SAML組態、請聯絡技術支援部門以取得協助。

設定SAML驗證是一個多步驟程序。

步驟1：上傳IDP中繼資料檔案

若要為儲存陣列提供IDP連線資訊、請將IDP中繼資料匯入System Manager。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- IDP管理員已設定IDP系統。
- IDP管理員已確保IDP支援在驗證時傳回名稱ID的功能。
- 系統管理員已確保IDP伺服器與控制器時鐘同步（透過NTP伺服器或調整控制器時鐘設定）。
- IDP中繼資料檔案是從IDP系統下載、可在本機系統上使用、以存取System Manager。

關於這項工作

在此工作中、您會將IDP中的中繼資料檔案上傳至System Manager。IDP系統需要此中繼資料、才能將驗證要求重新導向至正確的URL、並驗證收到的回應。即使有兩個控制器、您也只需要上傳一個儲存陣列的中繼資料檔案。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取* SAML *索引標籤。

頁面會顯示組態步驟的總覽。

3. 按一下*匯入身分識別提供者（IDP）檔案*連結。

「匯入身分識別提供者檔案」對話方塊隨即開啟。

4. 按一下*瀏覽*以選取並上傳您複製到本機系統的IDP中繼資料檔案。

選取檔案後、將會顯示IDP實體ID。

5. 按一下*匯入*。

步驟2：匯出服務供應商檔案

若要在IDP與儲存陣列之間建立信任關係、請將服務供應商中繼資料匯入IDP。

開始之前

- 您知道儲存陣列中每個控制器的IP位址或網域名稱。

關於這項工作

在此工作中、您會從控制器匯出中繼資料（每個控制器一個檔案）。IDP需要此中繼資料、才能與控制器建立信任關係、並處理授權要求。檔案包含控制器網域名稱或IP位址等資訊、以便IDP與服務供應商通訊。

步驟

1. 按一下「匯出服務供應商檔案」連結。

「匯出服務供應商檔案」對話方塊隨即開啟。

2. 在*控制器A*欄位中輸入控制器IP位址或DNS名稱、然後按一下*匯出*將中繼資料檔案儲存至本機系統。如果儲存陣列包含兩個控制器、請針對「控制器B」欄位中的第二個控制器重複此步驟。

按一下「匯出」之後、服務供應商的中繼資料就會下載到您的本機系統。記下檔案的儲存位置。

3. 從本機系統中、找出您匯出的服務供應商中繼資料檔案。

每個控制器都有一個XML格式的檔案。

4. 從IDP伺服器匯入服務供應商中繼資料檔案、以建立信任關係。您可以直接匯入檔案、也可以從檔案手動輸入控制器資訊。

步驟3：對應角色

若要為使用者提供系統管理員的授權與存取權限、您必須將IDP使用者屬性和群組成員資格對應至儲存陣列的預先定義角色。

開始之前

- IDP管理員已在IDP系統中設定使用者屬性和群組成員資格。
- IDP中繼資料檔案會匯入System Manager。
- 每個控制器的服務供應商中繼資料檔案會匯入IDP系統、以建立信任關係。

關於這項工作

在此工作中、您可以使用System Manager將IDP群組對應至本機使用者角色。

步驟

1. 按一下對應System Manager角色的連結。

此時會開啟「角色對應」對話方塊。

2. 將IDP使用者屬性和群組指派給預先定義的角色。一個群組可以有多個指派的角色。

欄位詳細資料

設定	說明
對應	使用者屬性
指定要對應之SAML群組的屬性（例如「memberof」）。	屬性值
指定要對應群組的屬性值。	角色



所有使用者（包括系統管理員）都必須具備「監控」角色。沒有監控角色的任何使用者、System Manager將無法正常運作。

3. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。



啟用SAML之後、即可修改角色對應。

4. 完成對應後、請按一下*「Save（儲存）」*。

步驟4：測試SSO登入

為了確保IDP系統和儲存陣列能夠通訊、您可以選擇性地測試SSO登入。此測試也會在啟用SAML的最後步驟中執行。

開始之前

- IDP中繼資料檔案會匯入System Manager。
- 每個控制器的服務供應商中繼資料檔案會匯入IDP系統、以建立信任關係。

步驟

1. 選取「測試SSO登入」連結。

隨即開啟對話方塊、供您輸入SSO認證。

2. 輸入具有「安全性管理」權限和「監控」權限的使用者登入認證。

系統會在測試登入時開啟對話方塊。

3. 尋找「Test Successful（測試成功）」訊息。如果測試成功完成、請前往下一個步驟啟用SAML。

如果測試未成功完成、則會出現錯誤訊息、並提供進一步資訊。請確定：

- 使用者屬於具有「安全性管理」和「監控」權限的群組。
- 您為IDP伺服器上傳的中繼資料正確無誤。
- SP中繼資料檔案中的控制器位址正確。

步驟5：啟用SAML

最後一步是啟用SAML使用者驗證。

開始之前

- IDP中繼資料檔案會匯入System Manager。
- 每個控制器的服務供應商中繼資料檔案會匯入IDP系統、以建立信任關係。
- 至少設定一個「監控」和一個「安全管理員」角色對應。

關於這項工作

本工作說明如何完成SAML使用者驗證組態。在此過程中、系統也會提示您測試SSO登入。上一步說明SSO登入測試程序。



*編輯和停用。*一旦啟用SAML、您就無法透過使用者介面停用SAML、也無法編輯IDP設定。如果您需要停用或編輯SAML組態、請聯絡技術支援部門以取得協助。

步驟

1. 從「* SAML *」標籤中、選取「*啟用SAML *」連結。

「*確認啟用SAML」對話方塊隨即開啟。

2. 輸入「enable」、然後按一下「* Enable（啟用）」。
3. 輸入SSO登入測試的使用者認證資料。

結果

系統啟用SAML之後、會終止所有作用中工作階段、並開始透過SAML驗證使用者。

變更SAML角色對應

如果您先前已針對存取管理設定SAML、則可以變更IDP群組與儲存陣列預先定義角色之間的角色對應。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- IDP管理員已在IDP系統中設定使用者屬性和群組成員資格。
- 已設定並啟用SAML。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取* SAML *索引標籤。
3. 選擇*角色對應*。

此時會開啟「角色對應」對話方塊。

4. 將IDP使用者屬性和群組指派給預先定義的角色。一個群組可以有多个指派的角
色。



請注意、在啟用SAML時、您不會移除權限、否則您將無法存取System Manager。

欄位詳細資料

設定	說明
對應	使用者屬性
指定要對應之SAML群組的屬性（例如「memberof」）。	屬性值
指定要對應群組的屬性值。	角色



所有使用者（包括系統管理員）都必須具備「監控」角色。沒有監控角色的任何使用者、System Manager將無法正常運作。

1. *可選：*單擊*添加另一個映射*以輸入更多的組對角色映射。

2. 按一下「* 儲存 *」。

結果

完成此工作之後、任何作用中的使用者工作階段都會終止。只會保留目前的使用者工作階段。

匯出SAML服務供應商檔案

如有必要、您可以匯出儲存陣列的服務供應商中繼資料、然後將檔案重新匯入身分識別供應商（IDP）系統。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 已設定並啟用SAML。

關於這項工作

在此工作中、您會從控制器匯出中繼資料（每個控制器一個檔案）。IDP需要此中繼資料、才能與控制器建立信任關係、並處理驗證要求。檔案包含IDP可用於傳送要求的控制器網域名稱或IP位址等資訊。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取* SAML *索引標籤。
3. 選取*匯出*。

「匯出服務供應商檔案」對話方塊隨即開啟。

4. 針對每個控制器、按一下*匯出*、將中繼資料檔案儲存至您的本機系統。



每個控制器的網域名稱欄位為唯讀。

記下檔案的儲存位置。

5. 從本機系統中、找出您匯出的服務供應商中繼資料檔案。

每個控制器都有一個XML格式的檔案。

6. 從IDP伺服器匯入服務供應商中繼資料檔案。您可以直接匯入檔案、也可以從檔案手動輸入控制器資訊。
7. 按一下 * 關閉 *。

檢視稽核記錄活動

透過檢視稽核記錄、具有「安全管理」權限的使用者可以監控使用者動作、驗證失敗、無效的登入嘗試、以及使用者工作階段壽命。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*稽核記錄*索引標籤。

稽核記錄活動會以表格格式顯示、其中包含下列資訊欄：

- 日期/時間-儲存陣列偵測到事件的時間戳記（以GMT[時間]為準）。
 - 使用者名稱：與事件相關的使用者名稱。對於儲存陣列上的任何未驗證動作、「N/A」會顯示為使用者名稱。未驗證的動作可能會由內部Proxy或其他機制觸發。
 - 狀態代碼-作業的HTTP狀態代碼（200、400等）、以及與事件相關的說明文字。
 - * URL access*-完整URL（包括主機）和查詢字串。
 - 用戶端IP位址-與事件相關聯之用戶端的IP位址。
 - 來源：與事件相關的記錄來源、可以是System Manager、CLI、Web Services或Support Shell。
3. 使用「稽核記錄」頁面上的選項來檢視及管理事件。

選擇	說明
從...顯示事件	限制依日期範圍（過去24小時、過去7天、過去30天或自訂日期範圍）顯示的事件。
篩選器	限制以欄位中輸入的字元顯示的事件。請使用引號（"）表示完全相符的字詞、輸入「OR」以傳回一或多個字詞、或輸入破折號（-）以省略字詞。
重新整理	選擇* Refresh*（重新整理*）、將頁面更新為最新的事件。
檢視/編輯設定	選取*檢視/編輯設定*以開啟對話方塊、讓您指定要記錄的完整記錄原則和行動層級。
刪除事件	選取*刪除*可開啟對話方塊、讓您從頁面移除舊事件。
顯示/隱藏欄	<p>按一下*顯示/隱藏*欄圖示  可選擇要在表格中顯示的其他列。其他欄位包括：</p> <ul style="list-style-type: none"> • 方法：HTTP方法（例如POST、GET、DELETE等）。 • CLI命令已執行—針對安全CLI要求執行的CLI命令（語法）。 • * CLI傳回狀態*：CLI狀態代碼或用戶端輸入檔的要求。 • 符號程序-執行的符號程序。 • * SSH事件類型*-安全Shell（SSH）事件類型、例如登入、登出及login_fail。 • * SSH工作階段PID*- SSH工作階段的處理序ID編號。 • * SSH工作階段持續時間*-使用者登入的秒數。
切換欄篩選條件	按一下*切換*圖示  開啟每欄的篩選欄位。在欄位中輸入字元、以限制這些字元所顯示的事件。再按一下圖示以關閉篩選欄位。
復原變更	按一下「復原」圖示  可將表恢復為默認配置。
匯出	按一下「匯出」、將表格資料儲存至以逗號分隔的值（CSV）檔案。

定義稽核記錄原則

您可以變更覆寫原則及稽核記錄中記錄的事件類型。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

此工作說明如何變更稽核記錄設定、包括覆寫舊事件的原則、以及記錄事件類型的原則。

步驟

- 1. 選取*功能表：設定[Access Management（存取管理）]*。
- 2. 選取「**稽核記錄」索引標籤。
- 3. 選取*檢視/編輯設定*。

「稽核記錄設定」對話方塊隨即開啟。

- 4. 變更覆寫原則或記錄的事件類型。

欄位詳細資料

設定	說明
覆寫原則	<div><div>決定當達到最大容量時覆寫舊事件的原則：</div><div><ul style="list-style-type: none">• *當稽核日誌已滿*時、允許覆寫稽核日誌中最舊的事件；當稽核日誌達到50、000筆記錄時、會覆寫舊事件。• 要求手動刪除稽核記錄事件-指定不會自動刪除事件、而是在設定的百分比顯示臨界值警告。必須手動刪除事件。</div><div><div></div><div>如果停用覆寫原則、且稽核記錄項目達到上限、則沒有「安全管理」權限的使用者將無法存取System Manager。若要將系統存取權限還原給沒有「安全管理」權限的使用者、則指派給「安全管理」角色的使用者必須刪除舊的事件記錄。</div></div><div><div></div><div>如果將syslog伺服器設定為歸檔稽核記錄、則不適用覆寫原則。</div></div></div>
要記錄的行動層級	<div><div>決定要記錄的事件類型：</div><div><ul style="list-style-type: none">• 僅記錄修改事件-僅顯示使用者動作涉及變更系統的事件。• 記錄所有修改和唯讀事件-顯示所有事件、包括需要讀取或下載資訊的使用者動作。</div></div>

- 5. 按一下「* 儲存 *」。

從稽核記錄刪除事件

您可以清除舊事件的稽核記錄、以便更容易管理事件搜尋。您可以選擇在刪除時將舊事件儲存至CSV（以逗號分隔的值）檔案。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

此工作說明如何從稽核記錄中移除舊事件。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 選取*稽核記錄*索引標籤。
3. 選擇*刪除*。

「刪除稽核記錄」對話方塊隨即開啟。

4. 選取或輸入您要刪除的最舊事件數目。
5. 如果您要將刪除的事件匯出至CSV檔案（建議）、請保持核取方塊為選取狀態。在下一步中按一下「刪除」時、系統會提示您輸入檔案名稱和位置。否則、如果您不想將事件儲存至CSV檔案、請按一下核取方塊加以取消選取。
6. 按一下*刪除*。

隨即開啟確認對話方塊。

7. 在欄位中輸入「刪除」、然後按一下「刪除」。

最舊的事件會從「稽核記錄」頁面移除。

設定系統記錄伺服器進行稽核記錄

如果您想要將稽核記錄歸檔到外部syslog伺服器、可以設定該伺服器與儲存陣列之間的通訊。建立連線之後、稽核記錄會自動儲存至syslog伺服器。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 系統記錄伺服器位址、傳輸協定和連接埠號碼必須可用。伺服器位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 如果您的伺服器使用安全傳輸協定（例如TLS）、則您的本機系統必須具備憑證授權單位（CA）憑證。CA憑證可識別網站擁有者、以確保伺服器與用戶端之間的安全連線。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 從*稽核記錄*索引標籤中、選取*設定Syslog伺服器*。

此時將打開* Configure Syslog Servers*（配置Syslog服務器*）對話框。

3. 按一下「* 新增 *」。

「新增**Syslog**伺服器」對話方塊隨即開啟。

4. 輸入伺服器的資訊、然後按一下*「Add*（新增*）」。

- 伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。
- 傳輸協定-從下拉式清單中選取傳輸協定（例如TLS、udp或TCP）。
- 上傳憑證（選用）-如果您選取TLS傳輸協定、但尚未上傳簽署的CA憑證、請按一下*瀏覽*上傳憑證檔案。稽核記錄不會歸檔至沒有信任憑證的syslog伺服器。



如果憑證稍後失效、TLS交握將會失敗。因此、系統會在稽核記錄中張貼錯誤訊息、而不會再將訊息傳送到syslog伺服器。若要解決此問題、您必須修正syslog伺服器上的憑證、然後前往*功能表：設定[稽核記錄>設定Syslog伺服器>全部測試]*。

- * Port*（連接埠）-輸入syslog接收器的連接埠號碼。

按一下「新增」之後、「設定**Syslog**伺服器」對話方塊會開啟、並在頁面上顯示您設定的syslog伺服器。

5. 若要測試伺服器與儲存陣列的連線、請選取* Test All*。

結果

設定完成後、所有新的稽核記錄都會傳送到syslog伺服器。不會傳輸先前的記錄。

編輯稽核記錄的syslog伺服器設定

您可以變更為用於歸檔稽核記錄的syslog伺服器設定、也可以上傳伺服器的新憑證授權單位（CA）憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 系統記錄伺服器位址、傳輸協定和連接埠號碼必須可用。伺服器位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 如果您要上傳新的CA憑證、則必須在本機系統上提供該憑證。

步驟

1. 選取*功能表：設定[Access Management（存取管理）]*。
2. 從*稽核記錄*索引標籤中、選取*設定Syslog伺服器*。

已設定的syslog伺服器會顯示在頁面上。

3. 若要編輯伺服器資訊、請選取伺服器名稱右側的*編輯*（鉛筆）圖示、然後在下列欄位中進行所需的變更：
 - 伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。
 - 傳輸協定-從下拉式清單中選取傳輸協定（例如TLS、udp或TCP）。
 - * Port*（連接埠）-輸入syslog接收器的連接埠號碼。
4. 如果您將傳輸協定變更為安全TLS傳輸協定（從UDP或TCP）、請按一下*匯入信任的憑證*上傳CA憑證。
5. 若要測試與儲存陣列的新連線、請選取*「Test All（測試全部）」*。

結果

設定完成後、所有新的稽核記錄都會傳送到syslog伺服器。不會傳輸先前的記錄。

常見問題集

為什麼我無法登入？

如果您在嘗試登入System Manager時收到錯誤訊息、請檢閱這些可能的原因。

系統管理員可能會因為下列其中一項原因而發生登入錯誤：

- 您輸入的使用者名稱或密碼不正確。
- 您的權限不足。
- 目錄伺服器（若已設定）可能無法使用。如果是這種情況、請嘗試以本機使用者角色登入。
- 您嘗試多次登入失敗、這會觸發鎖定模式。請等待10分鐘以重新登入。
- 已觸發鎖定條件、且稽核記錄可能已滿。移至「存取管理」、並從稽核記錄中刪除舊事件。
- 已啟用SAML驗證。重新整理瀏覽器以登入。

由於下列原因之一、可能會發生遠端儲存陣列鏡射工作的登入錯誤：

- 您輸入的密碼不正確。
- 您嘗試多次登入失敗、這會觸發鎖定模式。請等待10分鐘再登入一次。
- 控制器上使用的用戶端連線數量已達上限。檢查多個使用者或用戶端。

新增目錄伺服器之前、我需要知道什麼？

在Access Management中新增目錄伺服器之前、請確定您符合下列需求。

- 必須在目錄服務中定義使用者群組。
- LDAP伺服器認證必須可用、包括網域名稱、伺服器URL、以及可選的連結帳戶使用者名稱和密碼。
- 對於使用安全傳輸協定的LDAPS伺服器、LDAP伺服器的憑證鏈結必須安裝在本機機器上。

我需要知道哪些關於對應至儲存陣列角色的資訊？

在將群組對應至角色之前、請先檢閱下列準則。

儲存陣列的內嵌RBAC（角色型存取控制）功能包括下列角色：

- 儲存設備管理-對儲存物件（例如磁碟區和磁碟集區）的完整讀寫存取權、但無法存取安全性組態。
- 安全管理：存取存取管理、憑證管理、稽核記錄管理中的安全組態、以及開啟或關閉舊版管理介面（符號）的功能。
- 支援**admin**：存取儲存陣列上的所有硬體資源、故障資料、MEL事件及控制器韌體升級。無法存取儲存物件或安全性組態。
- 監控-對所有儲存物件的唯讀存取、但無法存取安全性組態。

目錄服務

如果您使用的是LDAP（輕量型目錄存取傳輸協定）伺服器和目錄服務、請確定：

- 系統管理員已在目錄服務中定義使用者群組。
- 您知道LDAP使用者群組的群組網域名稱。
- 所有使用者（包括系統管理員）都必須具備「監控」角色。沒有監控角色的任何使用者、System Manager將無法正常運作。

SAML

如果您使用儲存陣列內嵌的安全聲明標記語言（SAML）功能、請確定：

- 身分識別供應商（IDP）管理員已在IDP系統中設定使用者屬性和群組成員資格。
- 您知道群組成員名稱。
- 所有使用者（包括系統管理員）都必須具備「監控」角色。沒有監控角色的任何使用者、System Manager將無法正常運作。

哪些外部管理工具可能會受此變更影響？

當您在System Manager中進行某些變更（例如切換管理介面或使用SAML進行驗證方法）時、部分外部工具和功能可能會受到限制、無法使用。

管理介面

直接與舊版管理介面（符號）通訊的工具（例如SANtricity、功能完善的SESSMI-S Provider或OnCommand Insight 功能完善的OCI（OCI））、除非已啟用「舊版管理介面」設定、否則無法運作。此外、如果停用此設定、則無法使用舊版CLI命令或執行鏡射作業。

如需詳細資訊、請聯絡技術支援部門。

SAML驗證

啟用SAML時、下列用戶端無法存取儲存陣列服務和資源：

- 企業管理所需時間（EMW）
- 命令列介面（CLI）
- 軟體開發人員套件（SDK）用戶端
- 頻內用戶端
- HTTP基本驗證REST API用戶端
- 使用標準REST API端點登入

如需詳細資訊、請聯絡技術支援部門。

在設定及啟用**SAML**之前、我需要知道哪些資訊？

在設定及啟用安全性聲明標記語言（SAML）功能以進行驗證之前、請確定您符合下列需求、並瞭解SAML限制。

需求

開始之前、請確定：

- 您的網路中已設定身分識別供應商（IDP）。IDP是一種外部系統、用於向使用者要求認證、並判斷使用者是否已成功驗證。您的安全團隊負責維護IDP。
- IDP管理員已在IDP系統中設定使用者屬性和群組。
- IDP管理員已確保IDP支援在驗證時傳回名稱ID的功能。
- 系統管理員已確保IDP伺服器與控制器時鐘同步（透過NTP伺服器或調整控制器時鐘設定）。
- IDP中繼資料檔案會從IDP系統下載、並可在本機系統上使用、以供存取System Manager。
- 您知道儲存陣列中每個控制器的IP位址或網域名稱。

限制

除了上述要求之外、請務必瞭解下列限制：

- 一旦啟用SAML、您就無法透過使用者介面停用SAML、也無法編輯IDP設定。如果您需要停用或編輯SAML組態、請聯絡技術支援部門以取得協助。建議您在最終組態步驟中啟用SAML之前先測試SSO登入。（系統也會在啟用SAML之前執行SSO登入測試。）
- 如果您日後停用SAML、系統會自動還原先前的組態（本機使用者角色和/或目錄服務）。
- 如果目錄服務目前設定為使用者驗證、則SAML會覆寫該組態。
- 設定SAML時、下列用戶端無法存取儲存陣列資源：
 - 企業管理所需時間（EMW）
 - 命令列介面（CLI）
 - 軟體開發人員套件（SDK）用戶端
 - 頻內用戶端
 - HTTP基本驗證REST API用戶端
 - 使用標準REST API端點登入

稽核記錄中記錄了哪些類型的事件？

稽核日誌可記錄修改事件、或同時記錄修改和唯讀事件。

視原則設定而定、會顯示下列類型的事件：

- 修改事件：系統管理程式中涉及系統變更（例如資源配置儲存設備）的使用者動作。
- 修改和唯讀事件：涉及系統變更的使用者動作、以及涉及檢視或下載資訊的事件、例如檢視磁碟區指派。

設定**syslog**伺服器之前、我需要什么？

您可以將稽核記錄歸檔至外部**syslog**伺服器。

在設定**syslog**伺服器之前、請記住下列準則。

- 請確定您知道伺服器位址、傳輸協定和連接埠號碼。伺服器位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 如果您的伺服器使用安全傳輸協定（例如TLS）、則您的本機系統必須具備憑證授權單位（CA）憑證。CA憑證可識別網站擁有者、以確保伺服器與用戶端之間的安全連線。
- 設定完成後、所有新的稽核記錄都會傳送到syslog伺服器。不會傳輸先前的記錄。
- 覆寫原則設定（可從*檢視/編輯設定*取得）不會影響使用syslog伺服器組態來管理記錄的方式。
- 稽核記錄遵循RFC 5424訊息格式。

系統記錄伺服器不再接收稽核記錄。我該怎麼辦？

如果您設定的syslog伺服器採用TLS傳輸協定、則伺服器在憑證因任何原因而失效時、將無法接收訊息。稽核記錄會張貼有關無效憑證的錯誤訊息。

若要解決此問題、您必須先修正syslog伺服器的憑證。一旦有效的憑證鏈結就位、請前往*功能表：設定[稽核記錄>設定Syslog伺服器>全部測試]*。

憑證

概念

憑證的運作方式

憑證是數位檔案、可識別網站和伺服器等線上實體、以便在網際網路上進行安全通訊。

憑證可確保Web通訊只能在指定的伺服器與用戶端之間以加密形式私下傳輸且不會變更。使用System Manager、您可以在主機管理系統（做為用戶端）上的瀏覽器與儲存系統（做為伺服器）中的控制器之間管理憑證。

憑證可以由信任的授權單位簽署、也可以自行簽署。「簽署」只是指有人驗證擁有者的身分、並判斷其裝置是否值得信任。儲存陣列會在每個控制器上隨附自動產生的自我簽署憑證。您可以繼續使用自我簽署的憑證、或是取得CA簽署的憑證、以便在控制器與主機系統之間建立更安全的連線。



雖然CA簽署的憑證可提供更好的安全保護（例如預防攔截式攻擊）、但如果您的網路規模較大、也需要支付昂貴的費用。相較之下、自我簽署的憑證較不安全、但完全免費。因此、自我簽署的憑證最常用於內部測試環境、而非正式作業環境。

簽署的憑證

已簽署的憑證會由信任的協力廠商組織之憑證授權單位（CA）驗證。簽署的憑證包括實體擁有者（通常是伺服器或網站）、憑證發行日期和到期日期、實體的有效網域、以及由字母和數字組成的數位簽章等詳細資料。

當您開啟瀏覽器並輸入網址時、系統會在背景執行憑證檢查程序、以判斷您是否要連線至內含有效CA簽署憑證的網站。一般而言、以簽署憑證保護的站台會在位址中包含掛鎖圖示和https指定名稱。如果您嘗試連線至不含CA簽署憑證的網站、瀏覽器會顯示網站不安全的警告。

CA會在應用程式處理期間採取步驟來驗證您的身分。他們可能會傳送電子郵件給您的註冊企業、驗證您的公司地址、並執行HTTP或DNS驗證。應用程式程序完成後、CA會傳送數位檔案給您、以便載入主機管理系統。通常、這些檔案包括信任鏈、如下所示：

- root（根）-在階層頂端是根憑證、其中包含用於簽署其他憑證的私密金鑰。根可識別特定的CA組織。如果您的所有網路裝置都使用相同的CA、則只需要一個根憑證。
- 中繼-從根目錄下分支是中繼憑證。CA會發出一或多個中繼憑證、做為受保護根憑證與伺服器憑證之間的中間人。
- 伺服器：鏈結底部是伺服器憑證、可識別您的特定實體、例如網站或其他裝置。儲存陣列中的每個控制器都需要個別的伺服器憑證。

自我簽署的憑證

儲存陣列中的每個控制器都包含預先安裝的自我簽署憑證。自我簽署的憑證與CA簽署的憑證類似、只是由實體擁有者（而非第三方）驗證。如同CA簽署的憑證、自我簽署的憑證也包含自己的私密金鑰、同時確保資料經過加密、並透過伺服器與用戶端之間的HTTPS連線傳送。不過、自我簽署的憑證並未使用與CA簽署的憑證相同的信任鏈結。

自我簽署的憑證並非瀏覽器的「信任」。每次您嘗試連線至僅包含自我簽署憑證的網站時、瀏覽器都會顯示警告訊息。您必須按一下警告訊息中的連結、以便繼續前往網站；如此一來、您基本上就會接受自我簽署的憑證。

用於金鑰管理伺服器的憑證

如果您使用具有磁碟機安全功能的外部金鑰管理伺服器、也可以管理該伺服器與控制器之間的驗證憑證。

憑證術語

下列條款適用於憑證管理。

期限	說明
CA	憑證授權單位（CA）是信任的實體、可發行稱為數位憑證的電子文件、以確保網際網路安全。這些憑證可識別網站擁有者、以便在用戶端與伺服器之間進行安全連線。
CSR	憑證簽署要求（CSR）是一則訊息、會從申請者傳送至憑證授權單位（CA）。CSR會驗證CA核發憑證所需的資訊。
憑證	憑證可識別站台的擁有者、以確保安全性、防止攻擊者模擬站台。憑證包含網站擁有者的相關資訊、以及認證（簽署）此資訊的信任實體身分。
憑證鏈結	將安全層新增至憑證的檔案階層。一般而言、此鏈包括階層頂端的一個根憑證、一個或多個中繼憑證、以及識別實體的伺服器憑證。
用戶端憑證	在安全金鑰管理方面、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IP位址。
中介憑證	一個或多個中繼憑證會從憑證鏈結的根目錄下分支。CA會發出一或多個中繼憑證、做為受保護根憑證與伺服器憑證之間的中間人。
金鑰管理伺服器憑證	在安全金鑰管理方面、金鑰管理伺服器憑證會驗證伺服器、因此儲存陣列可以信任其IP位址。

期限	說明
Keystore	Keystore是主機管理系統上的儲存庫、內含私密金鑰及其對應的公開金鑰和憑證。這些金鑰和憑證可識別您自己的實體、例如控制器。
OCSP伺服器	線上憑證狀態傳輸協定（OCSP）伺服器會判斷憑證授權單位（CA）是否在排定的到期日之前撤銷任何憑證、然後在憑證遭撤銷時、封鎖使用者存取伺服器。
根憑證	根憑證位於憑證鏈結階層的頂端、其中包含用於簽署其他憑證的私密金鑰。根可識別特定的CA組織。如果您的所有網路裝置都使用相同的CA、則只需要一個根憑證。
簽署的憑證	由憑證授權單位（CA）驗證的憑證。此資料檔案包含私密金鑰、可確保資料以加密形式透過HTTPS連線在伺服器與用戶端之間傳送。此外、已簽署的憑證還包含實體擁有者（通常是伺服器或網站）的詳細資料、以及由字母和數字組成的數位簽章。簽署的憑證使用信任鏈、因此最常用於正式作業環境。也稱為「CA簽署的憑證」或「管理憑證」。
自我簽署的憑證	自行簽署的憑證由實體擁有者驗證。此資料檔案包含私密金鑰、可確保資料以加密形式透過HTTPS連線在伺服器與用戶端之間傳送。其中也包含由字母和數字組成的數位簽名。自我簽署的憑證不會使用與CA簽署憑證相同的信任鏈結、因此最常用於測試環境。也稱為「預先安裝」憑證。
伺服器憑證	伺服器憑證位於憑證鏈結的底部。它會識別您的特定實體、例如網站或其他裝置。儲存系統中的每個控制器都需要個別的伺服器憑證。

使用方法

控制器使用**CA**簽署的憑證

您可以取得**CA**簽署的憑證、以便在控制器與瀏覽器之間進行安全通訊、以存取System Manager。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

關於這項工作

使用**CA**簽署的憑證是三個步驟的程序。

步驟1：完成並提交控制器的**CSR**

您必須先為儲存陣列中的每個控制器產生憑證簽署要求（CSR）檔案、然後將檔案提交給憑證授權單位（CA）。

開始之前

- 您必須知道每個控制器的IP位址或DNS名稱。

關於這項工作

CSR提供組織、控制器IP位址或DNS名稱的相關資訊、以及識別控制器中Web伺服器的金鑰配對。在此工作期間、如果儲存陣列中只有一個控制器、則會產生一個CSR檔案、如果有兩個控制器、則會產生兩個CSR檔案。



提交至CA後、請勿產生新的CSR。產生CSR時、系統會建立私密與公開金鑰配對。公開金鑰是CSR的一部分、而私密金鑰則保留在金鑰庫中。當您收到簽署的憑證並將其匯入Keystore時、系統會確保私密金鑰和公開金鑰都是原始配對。因此、在將新的CSR提交給CA之後、您不得產生新的CSR。如果您這麼做、控制器就會產生新的金鑰、而且您從CA收到的憑證將無法運作。

步驟

1. 選取*功能表：設定[憑證]*。
2. 從* Array Management（陣列管理）選項卡中選擇*完整的csr。



如果看到對話方塊提示您接受第二個控制器的自我簽署憑證、請按一下*「接受自我簽署的憑證*」繼續。

3. 輸入下列資訊、然後按一下*下一步*：

- 組織：貴公司或組織的完整法定名稱。包括尾碼、例如Inc.或Corp.
- 組織單位（選用）：您組織處理憑證的部門。
- 城市/地區：儲存陣列或企業所在的城市。
- 州/地區（選用）：儲存陣列或業務所在的州或地區。
- 國家ISO代碼：您所在國家/地區的兩位數ISO（國際標準化組織）代碼、例如US。



某些欄位可能會預先填入適當的資訊、例如控制器的IP位址。除非您確定預先填入的值不正確、否則請勿變更。例如、如果您尚未完成CSR、則控制器IP位址會設為「localhost。」在此情況下、您必須將「localhost」變更為控制器的DNS名稱或IP位址。

4. 驗證或輸入儲存陣列中控制器A的下列資訊：

- 控制器一般名稱-預設會顯示控制器A的IP位址或DNS名稱。請確定此位址正確無誤、而且必須完全符合您輸入的內容、才能在瀏覽器中存取System Manager。
- 控制器備用IP位址-如果通用名稱是IP位址、您可以選擇輸入控制器A的任何其他IP位址或別名對於多個項目、請使用以逗號分隔的格式。
- 控制器A備用DNS名稱-如果通用名稱是DNS名稱、請為控制器A輸入任何其他DNS名稱對於多個項目、請使用以逗號分隔的格式。如果沒有替代DNS名稱、但您在第一個欄位中輸入DNS名稱、請在此處複製該名稱。如果儲存陣列只有一個控制器、則可使用* Finish（完成）按鈕。如果儲存陣列有兩個控制器、則可使用 Next*按鈕。



當您初次建立CSR要求時、請勿按一下*跳過此步驟*連結。此連結是在錯誤恢復情況下提供的。在極少數情況下、CSR要求可能會在一個控制器上失敗、但在另一個控制器上失敗。此連結可讓您跳過在控制器A上建立CSR要求的步驟（如果已定義）、然後繼續下一步、在控制器B上重新建立CSR要求

5. 如果只有一個控制器、請按一下「完成」。如果有兩個控制器、請按「下一步」輸入控制器B的資訊（與上述相同）、然後按一下「完成」。

對於單一控制器、一個CSR檔案會下載到您的本機系統。對於雙控制器、會下載兩個CSR檔案。下載的資料夾位置取決於您的瀏覽器。

6. 找到下載的CSR檔案。資料夾位置取決於您的瀏覽器。

7. 將CSR檔案提交給CA、並以PEEM格式要求簽署的憑證。
8. 等待CA傳回憑證、然後前往 [\[步驟2：匯入控制器的簽署憑證\]](#)。

步驟2：匯入控制器的簽署憑證

收到簽署的憑證之後、您會匯入控制器的檔案。

開始之前

- CA傳回簽署的憑證檔案。
- 這些檔案可在您的本機系統上使用。
- 如果CA提供鏈結的憑證（例如.p7b檔案）、您必須將鏈結的檔案解壓縮至個別檔案：根憑證、一或多個中繼憑證、以及識別控制器的伺服器憑證。您可以使用Windows「certmgr」公用程式來解壓縮檔案（按一下滑鼠右鍵並選取*功能表：All Tasks（所有工作）[Export（匯出）]*）。匯出完成後、會針對鏈中的每個憑證檔案顯示一個CER.檔案。

關於這項工作

本工作說明如何上傳憑證檔案。

步驟

1. 選取*功能表：設定[憑證]*。
2. 從* Array Management（陣列管理）選項卡中選擇 Import（匯入）。

隨即開啟一個對話方塊、用於匯入憑證檔案。

3. 按一下*瀏覽*按鈕、先選取根和中繼檔案、然後選取控制器的每個伺服器憑證。兩個控制器的根和中間檔案相同。每個控制器只有伺服器憑證是唯一的。

檔案名稱會顯示在對話方塊中。

4. 按一下*匯入*。

檔案已上傳並驗證。

結果

工作階段會自動終止。您必須再次登入、憑證才能生效。當您再次登入時、新的CA簽署憑證會用於您的工作階段。

重設管理憑證

您可以將控制器上的憑證從使用CA簽署的憑證還原為原廠設定的自我簽署憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- CA簽署的憑證必須先匯入。

關於這項工作

重設功能會從每個控制器刪除目前由CA簽署的憑證檔案。然後控制器將恢復使用自我簽署的憑證。

步驟

1. 選取*功能表：設定[憑證]*。
2. 從* Array Management（陣列管理）選項卡中選擇 Reset*（重置*）。

此時將打開確認*重置管理證書*對話框。

3. 在欄位中輸入「重設」、然後按一下「重設」。

瀏覽器重新整理之後、瀏覽器可能會封鎖對目的地站台的存取、並回報該站台使用HTTP嚴格傳輸安全性。當您切換回自我簽署的憑證時、就會出現這種情況。若要清除封鎖目的地存取的條件、您必須從瀏覽器清除瀏覽資料。

結果

控制器會恢復使用自我簽署的憑證。因此、系統會提示使用者手動接受其工作階段的自我簽署憑證。

檢視匯入的憑證資訊

在「憑證」頁面中、您可以檢視儲存陣列的憑證類型、發行授權單位及有效的憑證日期範圍。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

步驟

1. 選取功能表：設定[憑證]。
2. 選取其中一個索引標籤以檢視憑證的相關資訊。

索引標籤	說明
陣列管理	檢視針對每個控制器匯入的CA簽署憑證相關資訊、包括根檔案、中繼檔案和伺服器檔案。
值得信賴	<p>檢視所有其他類型的控制器匯入憑證的相關資訊。使用* Show certificates that are ...*（顯示...的憑證）下的篩選欄位、即可檢視使用者安裝或預先安裝的憑證。</p> <ul style="list-style-type: none">• 使用者安裝。使用者上傳至儲存陣列的憑證、可在控制器做為用戶端（而非伺服器）、LDAPS憑證及身分識別聯盟憑證時、包含信任的憑證。• 預先安裝。儲存陣列隨附的自我簽署憑證。
金鑰管理	檢視匯入外部金鑰管理伺服器之CA簽署憑證的相關資訊。

以用戶端身分匯入控制器的憑證

如果控制器因為無法驗證網路伺服器的信任鏈結而拒絕連線、您可以從信任的索引標籤匯入憑證、讓控制器（做為用戶端）接受來自該伺服器的通訊。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 憑證檔案會安裝在您的本機系統上。

關於這項工作

如果您想要允許其他伺服器聯絡控制器（例如使用TLS的LDAP伺服器或syslog伺服器）、可能需要從信任的索引標籤匯入憑證。

步驟

1. 選取*功能表：設定[憑證]*。
2. 從*信任的*索引標籤中、選取*匯入*。

隨即開啟一個對話方塊、用於匯入信任的憑證檔案。

3. 單擊*瀏覽*以選擇控制器的證書文件。

檔案名稱會顯示在對話方塊中。

4. 按一下*匯入*。

結果

檔案會上傳並驗證。

啟用憑證撤銷檢查

您可以啟用撤銷憑證的自動檢查、讓線上憑證狀態傳輸協定（OCSP）伺服器封鎖使用者建立不安全的連線。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- DNS伺服器是在兩個控制器上設定、可讓OCSP伺服器使用完整網域名稱。此工作可從「硬體」頁面取得。
- 如果您要指定自己的OCSP伺服器、必須知道該伺服器的URL。

關於這項工作

自動撤銷檢查有助於在CA未適當核發憑證或私密金鑰遭洩漏的情況下進行撤銷檢查。

在此工作期間、您可以設定OCSP伺服器、或使用憑證檔案中指定的伺服器。OCSP伺服器會判斷CA是否在排定的到期日之前撤銷任何憑證、然後在憑證撤銷時封鎖使用者存取站台。

步驟

1. 選取*功能表：設定[憑證]*。
2. 選取*信任的*索引標籤。



您也可以從*金鑰管理*索引標籤啟用撤銷檢查。

3. 按一下「不尋常工作」、然後從下拉式功能表中選取「啟用撤銷檢查」。

4. 選取*我要啟用撤銷檢查*、如此核取方塊中會出現核取符號、對話方塊中會出現其他欄位。
5. 在「* OCSP回應程式位址*」欄位中、您可以選擇性地輸入OCSP回應程式伺服器的URL。如果您未輸入位址、系統會使用憑證檔案中的OCSP伺服器URL。
6. 按一下*測試位址*、確定系統可以開啟連線至指定的URL。
7. 按一下「* 儲存 *」。

結果

如果儲存陣列嘗試連線至具有撤銷憑證的伺服器、則連線會遭拒、並記錄事件。

刪除信任的憑證

您可以刪除先前從信任索引標籤匯入的使用者安裝憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 如果您要以新版本更新信任的憑證、則必須先匯入更新的憑證、才能刪除舊的憑證。



如果您在匯入替代憑證之前刪除用於驗證控制器和其他伺服器（例如LDAP伺服器）的憑證、則可能會喪失系統存取權。

關於這項工作

此工作說明如何刪除使用者安裝的憑證。無法刪除預先安裝的自我簽署憑證。

步驟

1. 選取*功能表：設定[憑證]*。
2. 選取*信任的*索引標籤。

下表顯示儲存陣列的信任憑證。

3. 從表格中選取您要移除的憑證。
4. 按一下「功能表：非常見工作[刪除]」

隨即開啟「確認刪除信任的憑證」對話方塊。

5. 在欄位中輸入「刪除」、然後按一下「刪除」。

使用CA簽署的憑證來驗證金鑰管理伺服器

若要在金鑰管理伺服器與儲存陣列控制器之間進行安全通訊、您必須設定適當的憑證集。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

關於這項工作

在控制器和金鑰管理伺服器之間進行驗證是兩步驟的程序。

步驟1：完成並提交CSR、以便使用金鑰管理伺服器進行驗證

您必須先產生憑證簽署要求（CSR）檔案、然後使用CSR向金鑰管理伺服器信任的憑證授權單位（CA）要求簽署的用戶端憑證。您也可以使用下載的CSR檔案、從金鑰管理伺服器建立及下載用戶端憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

關於這項工作

此工作說明如何產生CSR檔案、然後您可以使用它來向金鑰管理伺服器信任的CA要求已簽署的用戶端憑證。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。在此工作期間、您必須提供組織的相關資訊。

步驟

1. 選取*功能表：設定[憑證]*。
2. 從*金鑰管理*索引標籤、選取*完整的csr*。
3. 輸入下列資訊：
 - 一般名稱-識別此CSR的名稱、例如儲存陣列名稱、將顯示在憑證檔案中。
 - 組織：貴公司或組織的完整法定名稱。包括尾碼、例如Inc.或Corp.
 - 組織單位（選用）：您組織處理憑證的部門。
 - 城市/地區：貴組織所在的城市或地區。
 - 州/地區（選用）：貴組織所在的州或地區。
 - 國家/地區ISO代碼-兩位數ISO（國際標準化組織）代碼、例如貴組織所在的美國。
4. 按一下*下載*。

CSR檔案會儲存至本機系統。

5. 從金鑰管理伺服器信任的CA要求已簽署的用戶端憑證。
6. 當您擁有用戶端憑證時、請前往 [\[步驟2：匯入金鑰管理伺服器的憑證\]](#)。

步驟2：匯入金鑰管理伺服器的憑證

下一步是匯入憑證、以便在儲存陣列與金鑰管理伺服器之間進行驗證。憑證有兩種類型：用戶端憑證會驗證儲存陣列的控制器、而金鑰管理伺服器憑證則會驗證伺服器。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 您有已簽署的用戶端憑證檔案（請參閱 [步驟1：完成並提交CSR、以便使用金鑰管理伺服器進行驗證](#)）、並將該檔案複製到您要存取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伺服器憑證檔案、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。



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

本工作說明如何上傳憑證檔案、以便在儲存陣列控制器與金鑰管理伺服器之間進行驗證。您必須同時載入控制器的用戶端憑證檔案、以及金鑰管理伺服器的伺服器憑證檔案。

步驟

1. 選取*功能表：設定[憑證]*。
2. 從*金鑰管理*索引標籤、選取*匯入*。

隨即開啟一個對話方塊、用於匯入憑證檔案。

3. 在* Select用戶端憑證*旁、按一下*瀏覽*按鈕、選取儲存陣列控制器的用戶端憑證檔案。

檔案名稱會顯示在對話方塊中。

4. 在*選取金鑰管理伺服器的伺服器憑證*旁、按一下*瀏覽*按鈕、選取金鑰管理伺服器的伺服器憑證檔案。

檔案名稱會顯示在對話方塊中。

5. 按一下*匯入*。

檔案會上傳並驗證。

匯出金鑰管理伺服器憑證

您可以將金鑰管理伺服器的憑證儲存到本機機器。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 必須先匯入憑證。

步驟

1. 選取*功能表：設定[憑證]*。
2. 選取*金鑰管理*索引標籤。
3. 從表格中選取您要匯出的憑證、然後按一下*匯出*。

隨即開啟「儲存」對話方塊。

4. 輸入檔案名稱、然後按一下*「Save*（儲存*）」。

常見問題集

為什麼會出現「無法存取其他控制器」對話方塊？

當您執行某些與CA憑證相關的作業（例如匯入憑證）時、可能會看到一個對話方塊、提示您接受第二個控制器的自我簽署憑證。

在具有兩個控制器（雙工組態）的儲存陣列中、SANtricity 如果無法與第二個控制器通訊、或是瀏覽器在作業的

某個時間點無法接受憑證、有時會出現此對話方塊。

如果此對話方塊開啟、請按一下*「接受自我簽署的憑證*」繼續。如果另一個對話方塊提示您輸入密碼、請輸入您用於存取System Manager的管理員密碼。

如果此對話方塊再次出現、且您無法完成憑證工作、請嘗試下列其中一個程序：

- 使用不同的瀏覽器類型來存取此控制器、接受憑證並繼續。
- 使用System Manager存取第二個控制器、接受自我簽署的憑證、然後返回第一個控制器並繼續。

如何知道需要將哪些憑證上傳至**System Manager**以進行外部金鑰管理？

對於外部金鑰管理、您可以匯入兩種類型的憑證、以便在儲存陣列和金鑰管理伺服器之間進行驗證、讓兩個實體彼此信任。

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。若要取得用戶端憑證、請使用System Manager為儲存陣列完成CSR。然後、您可以將CSR上傳至金鑰管理伺服器、然後從該伺服器產生用戶端憑證。取得用戶端憑證後、請將該檔案複製到您要存取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。從金鑰管理伺服器擷取伺服器憑證檔案、然後將該檔案複製到您正在存取System Manager的主機。

關於憑證撤銷檢查、我需要知道什麼？

System Manager可讓您使用線上憑證狀態傳輸協定（OCSP）伺服器來檢查撤銷的憑證、而非上傳憑證撤銷清單（CRL）。

撤銷的憑證不應再受到信任。憑證可能會因數種原因而遭撤銷；例如、如果憑證授權單位（CA）未適當核發憑證、私密金鑰遭洩漏、或是識別的實體未遵守原則要求。

在System Manager中建立OCSP伺服器的連線之後、儲存陣列會在連線至AutoSupport 某個伺服器、外部金鑰管理伺服器（EKMS）、SSL上的輕量型目錄存取傳輸協定（LDAPS）伺服器或Syslog伺服器時、執行撤銷檢查。儲存陣列會嘗試驗證這些伺服器的憑證、以確保這些憑證尚未撤銷。然後伺服器會傳回該憑證的「好」、「已撤銷」或「未知」值。如果憑證已撤銷、或陣列無法聯絡OCSP伺服器、則連線會遭到拒絕。



在System Manager或命令列介面（CLI）中指定OCSP回應程式位址、會覆寫在憑證檔案中找到的OCSP位址。

哪些類型的伺服器會啟用撤銷檢查？

儲存陣列會在連線AutoSupport 至某個伺服器、外部金鑰管理伺服器（EKMS）、輕量型SSL目錄存取傳輸協定（LDAPS）伺服器或Syslog伺服器時、執行撤銷檢查。

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。