Web服務Proxy

E-Series storage systems

NetApp
January 20, 2026

目錄

Web服務Proxy

瞭解 SANtricity Web 服務 Proxy

《支援Web服務Proxy》SANtricity 是一款RESTful API伺服器、安裝於主機系統上、可管理數百個全新舊版NetApp E系列儲存系統。Proxy內含SANtricity 支援類似功能的Web型介面-《支援統一化管理程式（Cisco Unified Manager）」。

安裝總覽

安裝及設定Web服務Proxy的步驟如下：

1. "檢閱安裝與升級需求"。
2. "下載並安裝Web Services Proxy檔案"。
3. "登入API和Unified Manager"。
4. "設定Web服務Proxy"。

如需詳細資訊、請參閱

- Unified Manager：Proxy安裝包含SANtricity 以Web為基礎的支援功能、可讓您存取較新的E系列和EF系列儲存系統。如需詳細資訊、請參閱Unified Manager線上說明、您可從其使用者介面或取得 "軟體文件網站SANtricity"。
- 代表狀態傳輸（REST）：Web服務是一種RESTful API、可讓您存取幾乎所有SANtricity 的功能、因此您應該熟悉REST概念。如需詳細資訊、請參閱 "架構樣式與網路型軟體架構設計"。
- JavaScript物件標記法（Json）：由於Web服務中的資料是透過Json編碼、因此您應該熟悉Json程式設計概念。如需詳細資訊、請參閱 "JSON.簡介"。

深入瞭解Web服務

瞭解 SANtricity Web 服務和 Unified Manager

在安裝及設定Web服務Proxy之前、請先閱讀Web服務與SANtricity 《Overview of Web Services》（英文）《Overview of Web Services》（英文）和《Overview Unified Manager》（英文）。

Web服務

Web服務是一種應用程式設計介面（API）、可讓您設定、管理及監控NetApp E系列和EF系列儲存系統。透過發出API要求、您可以完成E系列儲存系統的組態、資源配置及效能監控等工作流程。

使用Web Services API管理儲存系統時、您應熟悉下列事項：

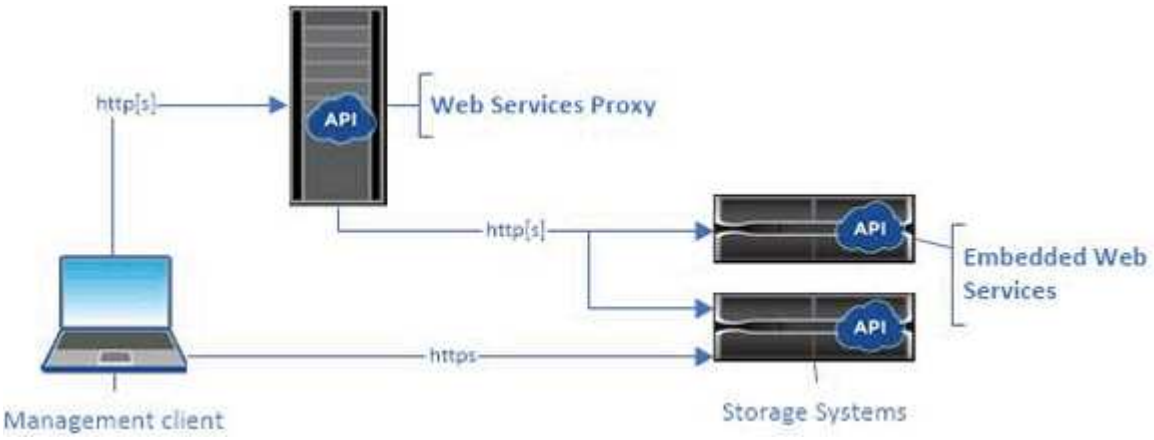
- JavaScript物件標記法（Json）：由於Web服務中的資料是透過Json編碼、因此您應該熟悉Json程式設計概念。如需詳細資訊、請參閱 "JSON.簡介"。

- 代表狀態傳輸（REST）：Web服務是一種RESTful API、可讓您存取幾乎所有SANtricity 的功能、因此您應該熟悉REST概念。如需詳細資訊、請參閱 "架構樣式與網路型軟體架構設計"。
- 程式設計語言概念–Java和Python是Web Services API最常用的程式設計語言、但任何可發出HTTP要求的程式設計語言都足以進行API互動。

Web服務有兩種實作：

- * 嵌入式 * ： RESTful API 伺服器內嵌於執行 NetApp SANtricity 11.30 或更新版本之 E2800/EF280 儲存系統的每個控制器，執行 SANtricity 11.40 或更新版本的 E5700/EF570 ，執行 SANtricity 11.60 或更新版本的 EF300 或 EF600 ，以及執行 SANtricity 11.90 或更新版本的 E4000 。無需安裝。
- * Proxy*- SANtricity 《Sesome Web Services Proxy》（英文）是Windows或Linux伺服器上獨立安裝的RESTful API伺服器。此主機型應用程式可管理數百個全新和舊版NetApp E系列儲存系統。一般而言、您應該將Proxy用於具有10個以上儲存系統的網路。Proxy比內嵌API更有效率地處理多個要求。

API的核心可在兩種實作中使用。



下表提供Proxy與內嵌版本的比較。

考量	**Proxy**	內嵌
安裝	需要主機系統（Linux或Windows）。您可以從下載Proxy "NetApp支援網站" 或開啟 "DockerHub"。	無需安裝或啟用。
安全性	預設為最低安全性設定。 安全性設定很低、讓開發人員能夠快速輕鬆地開始使用API。如果需要、您可以使用與內嵌版本相同的安全性設定檔來設定Proxy。	預設為高安全性設定。 由於API直接在控制器上執行、因此安全性設定很高。例如、它不允許HTTP存取、而且會停用HTTPS的所有SSL和舊版TLS加密傳輸協定。
集中管理	從單一伺服器管理所有儲存系統。	僅管理其內嵌的控制器。

Unified Manager

Proxy安裝套件包含Unified Manager、這是一個網路型介面、可讓您存取較新的E系列和EF系列儲存系統、例

如E2800、E5700、EF300和EF600。

在Unified Manager中、您可以執行下列批次作業：

- 從中央檢視檢視檢視多個儲存系統的狀態
- 探索網路中的多個儲存系統
- 將設定從單一儲存系統匯入多個系統
- 升級多個儲存系統的韌體

SANtricity Web 服務代理程式相容性與限制

下列相容性與限制適用於使用Web服務Proxy。

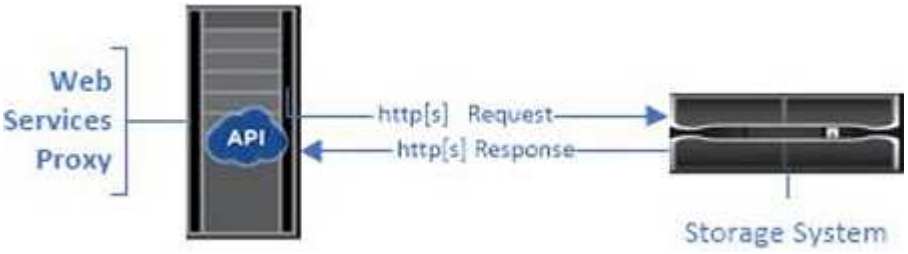
考量	相容性或限制
HTTP支援	Web服務Proxy允許使用HTTP或HTTPS。（基於安全考量、內嵌版本的Web Services需要HTTPS。）
儲存系統與韌體	Web Services Proxy可管理所有E系列儲存系統、包括混合使用舊系統與最新E2800、EF280、E5700、EF570、EF300、 和EF600系列系統。
IP支援	Web服務Proxy可支援IPV4傳輸協定或IPv6傳輸協定。 當Web服務Proxy嘗試從控制器組態自動探索管理位址時、IPv6傳輸協定可能會失敗。可能導致故障的原因包括IP位址轉送期間發生問題、或是儲存系統啟用IPv6、但伺服器卻未啟用IPv6。
NVSRAM.檔案名稱限制	Web Services Proxy使用NVSRAM/檔案名稱來準確識別版本資訊。因此、您無法在NVSRAM/檔案名稱與Web服務Proxy搭配使用時加以變更。Web服務Proxy可能無法將重新命名的NVSRAM/檔案辨識為有效的韌體檔案。
Symbol網路	Symbol Web是REST API中的URL。它可存取幾乎所有的符號呼叫。SYMBOL函數是下列URL的一部分： http://host:port/devmgr/storage-system/storage陣列ID/symbol / symbol功能+ 停用符號的儲存系統可透過Web服務Proxy支援。

瞭解 **SANtricity Web** 服務 **Proxy API** 基礎知識

在Web Services API中、HTTP通訊涉及要求回應週期。

要求中的**URL**元素

無論使用何種程式設計語言或工具、對Web服務API的每個呼叫都有類似的結構、包含URL、HTTP動詞和Accept標頭。



所有要求都包含URL、如下例所示、並包含表格中所述的元素。

https://webservices.name.com:8443/devmgr/v2/storage-systems+`

區域	說明
HTTP傳輸 「https：//」	Web服務Proxy可啟用HTTP或HTTPS。 基於安全考量、內嵌式Web服務需要HTTPS。
基礎URL和連接埠 webservices.name.com:8443`	每個要求都必須正確路由傳送至作用中的Web服務執行個體。需要FQDN（完整網域名稱）或執行個體的IP位址、以及聆聽連接埠。根據預設、Web Services會透過連接埠8080（用於HTTP）和連接埠8443（用於HTTPS）進行通訊。 對於Web服務Proxy、兩個連接埠都可以在Proxy安裝期間或wsconfig.xml檔案中變更。在執行各種管理應用程式的資料中心主機上、連接埠爭用很常見。 對於內嵌式Web服務、控制器上的連接埠無法變更；安全連線的連接埠預設為連接埠8443。

區域	說明
API路徑 「Devmgr/v2/storage系統」	會要求Web Services API中的特定REST資源或端點。大多數端點的形式如下： 「Devmgr/v2/<資源>/[id]」 API路徑包含三個部分： • 「Devmgr"（裝置管理員）是Web Services API的命名空間。 • 「v2」代表您正在存取的API版本。您也可以使用「utils」存取登入端點。 • 「系統」是文件中的一項類別。

支援的**HTTP verb**

支援的HTTP verb包括GET、POST及DELETE：

- 「Get要求」用於唯讀要求。
- POST要求用於建立和更新物件、以及可能會影響安全性的讀取要求。
- 刪除要求通常用於從管理中移除物件、完全移除物件、或是重設物件的狀態。

目前、Web Services API不支援PUT或修補程式。您可以改用POST來提供這些動詞的典型功能。

接受標頭

傳回要求本文時、Web Services會以Json格式傳回資料（除非另有指定）。某些用戶端預設要求「'text/html」或類似的內容。在這些情況下、API會以HTTP代碼406回應、表示無法以這種格式提供資料。最佳實務做法是針對您預期Json為回應類型的任何情況、將Accept標頭定義為「application/json」。在未傳回回應本文的其他情況下（例如刪除）、提供Accept標頭不會造成任何非預期的影響。

回應

向API提出要求時、回應會傳回兩項重要資訊：

- HTTP狀態代碼-指出要求是否成功。
- 可選的回應本文-通常提供代表資源狀態的Json實體或實體、以提供更多故障性質的詳細資料。

您必須檢查狀態代碼和內容類型標頭、以判斷所產生的回應本文的外觀。對於HTTP狀態代碼200-203-4222、Web服務會傳回回應的Json實體。對於其他HTTP狀態代碼、Web Services通常不會傳回額外的Json實體、因為規格不允許（204）、或是狀態是自我說明。下表列出常見的HTTP狀態代碼和定義。它也會指出是否傳回Json實體中與每個HTTP程式碼相關的資訊。

HTTP狀態代碼	說明	**Json**本文
200正常	表示回應成功。	是的

HTTP狀態代碼	說明	Json本文
201已建立	表示已建立物件。此程式碼僅用於少數罕見的情況、而非200個狀態。	是的
已接受202	表示已接受要求以非同步要求的形式處理、但您必須提出後續要求才能取得實際結果。	是的
203非權威資訊	類似於200個回應、但Web Services無法保證資料是最新的（例如、目前只有快取資料可用）。	是的
204無內容	表示作業成功、但沒有回應實體。	否
400個錯誤要求	表示要求中提供的Json實體無效。	否
401未獲授權	表示發生驗證失敗。未提供任何認證、或使用者名稱或密碼無效。	否
403禁止	授權失敗、表示已驗證的使用者無權存取要求的端點。	否
找不到404	表示無法找到所要求的資源。此程式碼適用於不存在的API或識別碼所要求的不存在資源。	否
無法處理的實體	表示要求通常格式良好、但輸入參數無效、或儲存系統的狀態不允許Web Services滿足要求。	是的
424失敗相依性	用於Web服務Proxy、表示所要求的儲存系統目前無法存取。因此、Web服務無法滿足要求。	否
429太多要求	表示已超過要求上限、應於稍後重試。	否

瞭解 **SANtricity Web** 服務 **Proxy** 術語

下列條款適用於Web服務Proxy。

期限	定義
API	應用程式設計介面（API）是一組可讓開發人員與裝置通訊的傳輸協定和方法。Web服務API用於與E系列儲存系統通訊。
ASUP	支援（ASUP）AutoSupport 功能會收集客戶支援套裝組合中的資料、並自動將訊息檔案傳送給技術支援部門、以進行遠端疑難排解和問題分析。
端點	端點是透過API提供的功能。端點包含HTTP動詞、加上URI路徑。在Web服務中、端點可以執行探索儲存系統和建立磁碟區等工作。
HTTP Verb	HTTP動詞是端點的對應動作、例如擷取和建立資料。在Web服務中、HTTP動詞包括POST、GET 和DELETE。
JSON	JavaScript物件標記法（Json）是一種結構化資料格式、類似於XML、使用最小、可讀的格式。Web服務中的資料是透過Json編碼。
休息/休息	代表狀態傳輸（REST）是鬆散的規格、可定義API的架構樣式。由於大多數REST API並未完全符合規格、因此它們被稱為「準則」或「類似標準」。 一般而言、「準」API不受程式語言限制、具有下列特性： • HTTP型、遵循傳輸協定的一般語意 • 結構化資料（Json、XML等）的產生者和使用者 • 物件導向（相對於作業導向） Web Services是RESTful API、幾乎能存取SANtricity所有的功能。
儲存系統	儲存系統是E系列陣列、包括磁碟櫃、控制器、磁碟機、軟體、 和韌體。
Symbol API	SYMBOL是用於管理E系列儲存系統的舊版API。Web Services API的基礎實作使用符號。
Web服務	Web服務是NetApp專為開發人員設計的API、可用於管理E系列儲存系統。Web服務有兩種實作：內嵌在控制器上、另一個可安裝在Linux或Windows上的Proxy。

安裝與設定

檢閱 **SANtricity Web** 服務 **Proxy** 的安裝與升級需求

安裝Web服務Proxy之前、請先檢閱安裝需求和升級考量事項。

安裝需求

您可以在Windows或Linux主機系統上安裝及設定Web服務Proxy。

Proxy安裝包括下列需求。

需求	說明
主機名稱限制	請確定您打算安裝Web Services Proxy的伺服器主機名稱僅包含Ascii字母、數字和連字號（-）。此需求是因為Java KeyTool的限制、用於為伺服器產生自我簽署的憑證。如果伺服器的主機名稱包含任何其他字元、例如底線（_）、則Webserver在安裝後將無法啟動。
作業系統	您可以在下列作業系統上安裝Proxy： • Linux • Windows 如需作業系統和韌體相容性的完整清單、請參閱 "NetApp 互通性對照表工具"。
Linux：其他考量事項	Webserver需要Linux標準基礎程式庫（init-Functions）才能正常運作。您必須為作業系統安裝lsb / insserv.套件。如需詳細資訊、請參閱讀我檔案的「其他必要套件」一節。
多個執行個體	您只能在伺服器上安裝一個Web服務Proxy執行個體、不過您可以在網路內的多個伺服器上安裝Proxy。
容量規劃	Web服務Proxy需要足夠的記錄空間。請確定您的系統符合下列可用磁碟空間需求： • 所需安裝空間：-275 MB • 最小記錄空間：200 MB • 系統記憶體：2 GB；堆空間預設為1 GB 您可以使用磁碟空間監控工具來驗證可用的磁碟機空間、以供持續儲存和記錄。
授權	Web服務Proxy是免費的獨立產品、不需要授權金鑰。然而、適用的版權與服務條款仍適用。如果您以圖形或主控台模式安裝Proxy、則必須接受終端使用者授權合約（EULA）。

升級考量

如果您要從舊版升級、請注意某些項目會保留或移除。

- 對於Web服務Proxy、會保留先前的組態設定。這些設定包括使用者密碼、所有探索到的儲存系統、伺服器憑證、信任的憑證、以及伺服器執行時間組態。
- 對於Unified Manager、SANtricity 先前載入儲存庫中的所有還原OS檔案都會在升級期間移除。

安裝或升級**SANtricity Web Services Proxy** 和**SANtricity Unified Manager** 文件

安裝作業包括下載檔案、然後在Linux或Windows伺服器上安裝Proxy套件。您也可以依照下列指示升級Proxy。

下載**Web**服務**Proxy**檔案

您可以從NetApp支援網站的軟體下載頁面下載安裝檔案和讀我檔案。

下載套件包括Web服務Proxy和Unified Manager介面。

步驟

1. 前往 "NetApp支援-下載"。
2. 選取* E系列SANtricity 《Web服務Proxy》 *。
3. 請依照指示下載檔案。請確定您為伺服器選取正確的下載套件（例如、適用於Windows的exe、適用於Linux的Bin或RPM）。
4. 將安裝檔案下載至您要安裝Proxy和Unified Manager的伺服器。

安裝在**Windows**或**Linux**伺服器上

您可以使用三種模式（圖形、主控台或無聲）之一、或使用RPM檔案（僅限Linux）來安裝Web服務Proxy和Unified Manager。

開始之前

- "檢閱安裝需求"。
- 請確定您已將正確的安裝檔案（適用於Windows的exe；適用於Linux的bin）下載到要安裝Proxy和Unified Manager的伺服器。

圖形模式安裝

您可以在Windows或Linux的圖形模式下執行安裝。在圖形模式中、提示會出現在Windows型介面中。

步驟

1. 存取您下載安裝檔案的資料夾。
2. 啟動Windows或Linux的安裝、如下所示：

    - Windows --雙擊安裝文件：

        「antricity _webservices：windows_x64-n.n.nn.nds.exe」

。Linux --執行下列命令：「antricity _webservices－Linux _x64-n.n.n.nn.bin」

在上述檔案名稱中、「n.n.n.nn.nnn.nnn」代表版本編號。

安裝程序隨即開始、並SANtricity 出現NetApp Web Services Proxy + Unified Manager開機畫面。

3. 依照螢幕上的提示進行。

安裝期間、系統會提示您啟用多項功能、並輸入一些組態參數。如有必要、您可以稍後在組態檔中變更這些選項。

在升級期間、系統不會提示您輸入組態參數。

4. 出現Webserver started（Webserver已啟動）訊息時、按一下「* OK（確定）*」以完成安裝。

此時將顯示Install Complete（安裝完成）對話框。

5. 如果您要啟動Unified Manager或互動式API文件、請按一下核取方塊、然後按一下「完成」。

主控台模式安裝

您可以在Windows或Linux的主控台模式下執行安裝。在主控台模式中、提示會出現在終端機視窗中。

步驟

1. 執行下列命令：「<安裝檔案名稱>-I Console」

在上述命令中、「<安裝檔案名稱>」代表您下載的Proxy安裝檔案名稱（例如：「antricity」_webservices：windows_x64-n.n.nn.nnns.exe」）。

若要在安裝程序期間隨時取消安裝、請在命令提示字元中輸入「quit」。

安裝程序隨即開始、並出現「啟動安裝程式」（Introduction）訊息。

2. 依照螢幕上的提示進行。

安裝期間、系統會提示您啟用多項功能、並輸入一些組態參數。如有必要、您可以稍後在組態檔中變更這些選項。

在升級期間、系統不會提示您輸入組態參數。

3. 安裝完成後、請按* Enter *退出安裝程式。

無聲模式安裝

您可以在Windows或Linux的Silent模式下執行安裝。在無訊息模式中、終端機視窗不會顯示任何傳回訊息或指令碼。

步驟

1. 執行下列命令：「<安裝檔名>-I silent'

在上述命令中、「<安裝檔案名稱>」代表您下載的Proxy安裝檔案名稱（例如：「antricity」_webservices

：windows_x64-n.n.nn.nnns.exe」）。

2. 按* Enter *。

   安裝程序可能需要幾分鐘的時間才能完成。成功安裝後、終端機視窗會出現命令提示字元。

RPM命令安裝（僅限Linux）

對於與RPM套件管理系統相容的Linux系統、您可以使用選用的RPM檔案來安裝Web Services Proxy。

步驟

1. 將RPM檔案下載至您要安裝Proxy和Unified Manager的伺服器。
2. 開啟終端機視窗。
3. 輸入下列命令：

   ```
   rpm -U santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
   ```

   在上述命令中、「n.n.n.nn.nnn.nfn」代表版本編號。

   安裝程序可能需要幾分鐘的時間才能完成。成功安裝後、終端機視窗會出現命令提示字元。

登入 SANtricity Web 服務 Proxy API 和 Unified Manager

Web Services包含API文件、可讓您直接與REST API互動。它也包含Unified Manager、這是一個瀏覽器型介面、可用來管理多個E系列儲存系統。

登入Web Services API

安裝Web Services Proxy之後、您可以在瀏覽器中存取互動式API文件。

API文件會與每個Web服務執行個體一起執行、也可從NetApp支援網站取得靜態PDF格式的文件。若要存取互動式版本、請開啟瀏覽器並輸入指向Web服務所在位置的URL（內嵌版本的控制器或Proxy的伺服器）。

Web Services API實作OpenAPI規格（原本稱為Swagger規格）。

初次登入時、請使用「admin」認證資料。「管理員」被視為擁有所有功能和角色存取權的超級管理員。

步驟

1. 開啟瀏覽器。
2. 輸入內嵌或Proxy實作的URL：

   - 內嵌：`https://<controller>:<port>/devmgr/docs/`

     在此URL中、「<Controller（控制器）>」是控制器的IP位址或FQDN、而「<連接埠>」是控制器的管理連接埠號碼（預設為84443）。

   - Proxy：「https[s]//<server>:<port>/devmgr/docs/」

在此URL中、「<server>'是安裝Proxy之伺服器的IP位址或FQDN、而「<port>'是接聽連接埠號碼（HTTP預設為8080、HTTPS預設為84443）。

如果聆聽連接埠已在使用中、Proxy會偵測衝突並提示您選擇不同的聆聽連接埠。

API文件會在瀏覽器中開啟。

3. 當互動式API文件開啟時、請前往頁面右上角的下拉式功能表、然後選取* util*。
4. 按一下「登入」類別以查看可用的端點。
5. 按一下* POST：/login*端點、然後按一下* Try it*。
6. 首次登入時、請輸入admin作為使用者名稱和密碼。
7. 按一下*執行*。
8. 若要存取端點以進行儲存管理、請前往右上角的下拉式功能表、然後選取* v2*。

   此時會顯示端點的高層級類別。您可以瀏覽API文件、如表所述。

區域	說明
下拉式功能表	頁面右上角的下拉式功能表提供選項、可在API文件（V2）版本2、符號介面（符號V2）和API公用程式（utils）之間切換以供登入。 由於API文件的第1版為預先發佈版本、而且通常無法使用、因此下拉式功能表中不包含V1。
類別	API文件是依高層級類別（例如：管理、組態）來組織。按一下類別以查看相關的端點。
端點	選取一個端點、即可查看URL可能傳回的URL路徑、必要參數、回應實體及狀態代碼。
歡迎試用	按一下*試用*、直接與端點互動。此按鈕會在每個擴充檢視中提供給端點。 當您按一下按鈕時、會顯示用於輸入參數的欄位（若適用）。然後您可以輸入值、然後按一下*執行*。 互動式文件使用JavaScript直接向API提出要求、而非測試要求。

登入**Unified Manager**

安裝Web服務Proxy之後、您可以存取Unified Manager、在網路型介面中管理多個儲存系統。

若要存取Unified Manager、請開啟瀏覽器並輸入指向安裝Proxy的URL。支援下列瀏覽器和版本。

瀏覽器	最低版本
Google Chrome	79
Microsoft Internet Explorer	11.
Microsoft Edge	79
Mozilla Firefox	70
Safari	12.

步驟

1. 開啟瀏覽器並輸入下列URL：

   http：//<server>:<port>/um'

   在此URL中、「<server>'代表安裝Web服務Proxy之伺服器的IP位址或FQDN、而「<port>'代表接聽連接埠號碼（HTTP預設為8080、HTTPS預設為8443）。

   此時會開啟Unified Manager登入頁面。

2. 首次登入時、請輸入「admin」作為使用者名稱、然後設定並確認管理員使用者的密碼。

   密碼最多可包含30個字元。如需使用者和密碼的詳細資訊、請參閱Unified Manager線上說明的存取管理一節。

設定 **SANtricity Web** 服務 **Proxy**

您可以修改Web服務Proxy設定、以符合環境的獨特作業和效能需求。

停止或重新啟動**Webserver**

Webserver服務會在安裝期間啟動、並在背景執行。在某些組態工作期間、您可能需要停止或重新啟動Webserver服務。

步驟

1. 執行下列其中一項：

   - 若為Windows、請前往* Start*功能表、選取功能表：管理工具[服務]、找到* NetApp SANtricity SWeb Services*、然後選取*停止*或*重新啟動*。
   - 對於Linux、請針對您的作業系統版本選擇停止及重新啟動Webserver的方法。安裝期間、會出現快顯對話方塊、指出精靈啟動的項目。例如：

     "web_services代理Web伺服器已安裝並啟動。您可以使用systemctl start | stop | esstart| STATUS web_services_proxy.service`與IT互動

   與服務互動的最常見方法是使用「stystemctl」命令。

解決連接埠衝突

如果Web服務Proxy正在執行、而另一個應用程式位於定義的位址或連接埠、您可以解決wsconfig.xml檔案中的連接埠衝突。

步驟

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 將下列行新增至wsconfig.xml檔案、其中_n_是連接埠編號：

```
<sslport clientauth="request">*n*</sslport>
<port>n</port>
```

   下表顯示控制HTTP連接埠和HTTPS連接埠的屬性。

名稱	說明	父節點	屬性	必要
組態	組態的根節點	null	版本-組態架構目前為1.0版。	是的
Sslport	用於偵聽SSL要求的TCP連接埠。預設為8443.	組態	Clientauth	否
連接埠	偵聽HTTP要求的TCP連接埠、預設為8080。	組態	-	否

3. 儲存並關閉檔案。
4. 重新啟動Webserver服務、使變更生效。

設定負載平衡和/或高可用度

若要在高可用度（HA）組態中使用Web服務Proxy、您可以設定負載平衡。在HA組態中、通常是單一節點接收所有要求、而其他節點則處於待命狀態、或是所有節點之間的要求負載平衡。

Web服務Proxy可存在於高可用度（HA）環境中、無論要求的接收者為何、大多數API都能正常運作。中繼資料標記和資料夾是兩個例外、因為標記和資料夾儲存在本機資料庫中、而且不會在Web服務Proxy執行個體之間共用。

不過、在少數的要求中、會發生一些已知的時間問題。具體而言、一個Proxy執行個體的資料速度比小視窗的第二個執行個體快。Web服務Proxy包含特殊組態、可移除此時間問題。此選項預設不會啟用、因為它會增加服務要求所需的時間（以確保資料一致性）。若要啟用此選項、您必須將內容新增至.ini檔案（適用於Windows）或.SH檔案（適用於Linux）。

步驟

1. 執行下列其中一項：
   - Windows：開啟appserver64.ini檔案、然後新增「dload-Balance.enabled=true」屬性。

     例如：「vmarg.7=-dload-Balance.enable=true」
   - Linux：開啟webserver.sh檔案、然後新增「dload-Balance.enabled=true」屬性。

     例如：「Debug start_options="-Dload-Balance.enable=true」
2. 儲存您的變更。
3. 重新啟動Webserver服務、使變更生效。

停用**SYMBOL HTTPS**

您可以停用符號命令（預設設定）、並透過遠端程序呼叫（RPC）傳送命令。此設定可在wsconfig.xml檔案中變更。

根據預設、Web Services Proxy會透過HTTPS、針對執行SANtricity EOS08.40或更新版本的所有E2800系列和E5700系列儲存系統、傳送符號命令。透過HTTPS傳送的符號命令會驗證到儲存系統。如有需要、您可以停用HTTPS符號支援、並透過RPC傳送命令。每當設定符號over RPC時、所有對儲存系統的被動命令都會啟用而不需驗證。

使用RPC上的符號時、Web服務Proxy無法連線至停用符號管理連接埠的系統。

步驟

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 在"devicemgt.symbolclientstracy"項目中、將"https首選"值改為"rpcOnly"。

   例如：

   「<env key="devicemgt.symbolclientstrysistic"> rpcOnly（/env>`）」
3. 儲存檔案。

設定跨來源資源共用

您可以設定跨來源資源共用（CORS）、這是一種機制、使用額外的HTTP標頭來提供在一個來源執行的Web應用程式、以便從不同來源的伺服器存取所選資源。

CORS由工作目錄中的cors.cfg檔案處理。CORS組態預設為開啟、因此不限制跨網域存取。

如果沒有組態檔、CORS將會開啟。但如果cors.cfg檔案存在、則會使用該檔案。如果cors.cfg檔案是空的、您就無法提出CORS要求。

步驟

1. 開啟位於工作目錄中的cors.cfg檔案。

2. 將所需的行新增至檔案。

   CORS組態檔中的每一行都是要比對的規則運算式模式。來源標頭必須符合cors.cfg檔案中的一行。如果有任何線路模式符合來源標頭、則允許提出要求。比較完整的來源、而不只是主機元素。

3. 儲存檔案。

要求會在主機上根據下列通訊協定進行比對：

- 將localhost與任何傳輸協定配對：-`*localhost*
- 僅將localhost與HTTPS配對：-`https://localhost*`

解除安裝 **SANtricity Web** 服務 **Proxy**

若要移除Web服務Proxy和Unified Manager、您可以使用任何模式（圖形化、主控台、無聲或RPM檔案）、無論您使用何種方法來安裝Proxy。

圖形模式解除安裝

您可以在Windows或Linux的圖形模式下執行解除安裝。在圖形模式中、提示會出現在Windows型介面中。

步驟

1. 啟動Windows或Linux的解除安裝、如下所示：
   - Windows --轉到包含uninstall_web_services代理卸載文件的目錄。預設目錄位於下列位置：C：/Program Files/NetApp/SANtricity Web Services Proxy/。按兩下「uninstall_web_services _proxy.exe」。

     或者、您也可以前往功能表：「控制台」「程式集」>「解除安裝程式」、然後選取「NetApp SANtricity Web服務Proxy」。

   - Linux --轉到包含Web Services Proxy卸載文件的目錄。預設目錄位於下列位置：+ 「/opt/netapp/SANtricity」網路服務代理伺服器/ uninstall_web_services Proxy
2. 執行下列命令：

   "uninstall_web_services代理-i GUI（uninstall_web_services代理-i GUI）"

   此時會出現「BIOS Web Services Proxy」開機畫面。SANtricity

3. 在「解除安裝」對話方塊中、按一下「解除安裝」。

   此時會出現「卸載程式」進度列、並顯示進度。

4. 出現「解除安裝完成」訊息時、按一下「完成」。

主控台模式解除安裝

您可以在Windows或Linux的主控台模式下執行解除安裝。在主控台模式中、提示會出現在終端機視窗中。

步驟

1. 移至uninstall_web_services Proxy目錄。
2. 執行下列命令：

   "uninstall_web_services代理-i控制檯"

   解除安裝程序隨即開始。

3. 卸載完成後，按* Enter鍵退出安裝程序。

無聲模式解除安裝

您可以在Windows或Linux的Silent模式下執行解除安裝。在無訊息模式中、終端機視窗不會顯示任何傳回訊息或指令碼。

步驟

1. 移至uninstall_web_services Proxy目錄。
2. 執行下列命令：

   "uninstall_web_services代理-i silent"

   解除安裝程序會執行、但終端機視窗不會顯示任何傳回訊息或指令碼。成功解除安裝Web服務Proxy之後、終端機視窗中會出現命令提示字元。

RPM命令解除安裝（僅限**Linux**）

您可以使用RPM命令、從Linux系統解除安裝Web Services Proxy。

步驟

1. 開啟終端機視窗。
2. 輸入下列命令列：

   「rpm -e SANtricity網路服務」

   解除安裝程序可能會留下不屬於原始安裝的檔案。手動刪除這些檔案、以完全移除Web服務Proxy。

在 **SANtricity Web** 服務 **Proxy** 中管理使用者存取

為了安全起見、您可以管理使用者對Web服務API和Unified Manager的存取。

存取管理總覽

存取管理包括角色型登入、密碼加密、基本驗證及LDAP整合。

角色型存取

角色型存取控制（RBAC）可將預先定義的使用者與角色建立關聯。每個角色都會將權限授與特定層級的功能。

下表說明每個角色。

角色	說明
資訊安全管理	SSL與憑證管理：
儲存設備管理	對儲存系統組態的完整讀寫存取權。
儲存設備。監控	唯讀存取、可檢視儲存系統資料。
support.admin	存取儲存系統上的所有硬體資源、並支援AutoSupport 諸如恢復（ASUP）等作業。

預設使用者帳戶是在users.properties檔案中定義。您可以直接修改users.properties檔案、或使用Unified Manager中的存取管理功能來變更使用者帳戶。

下表列出可用於Web服務Proxy的使用者登入資訊。

預先定義的使用者登入	說明
管理	超級管理員、可存取所有功能並包含所有角色。對於Unified Manager、您必須在首次登入時設定密碼。
儲存設備	負責所有儲存資源配置的管理員。此使用者包括下列角色：儲存設備管理員、support.admin及儲存設備監控。在設定密碼之前、此帳戶會停用。
安全性	負責安全組態的使用者。此使用者包括下列角色：Security、admin和storage、監控。在設定密碼之前、此帳戶會停用。
支援	負責硬體資源、故障資料和韌體升級的使用者。此使用者包括下列角色：support.admin和storage。監控。在設定密碼之前、此帳戶會停用。
監控	具有系統唯讀存取權的使用者。此使用者僅包含儲存設備監控角色。在設定密碼之前、此帳戶會停用。
RW（舊陣列的舊版）	RW（讀取/寫入）使用者包括下列角色：儲存區.admin、support.admin及儲存區.Monitor。在設定密碼之前、此帳戶會停用。
RO（舊陣列的舊版）	RO（唯讀）使用者僅包含儲存設備。監控角色。在設定密碼之前、此帳戶會停用。

密碼加密

對於每個密碼、您可以使用現有的SHA256密碼編碼來套用額外的加密程序。這項額外的加密程序會針對每個SHA256雜湊加密、隨機套用一組位元組至每個密碼（SALT）。Salted SHA256加密會套用至所有新建立的密碼。

在Web Services Proxy 3.0發行之前、密碼只能透過SHA256雜湊進行加密。任何現有的SHA256純雜湊加密密碼都會保留此編碼、而且在users.properties檔案下仍然有效。不過、SHA256純雜湊加密密碼不如使用Salted SHA256加密的密碼安全。

基本驗證

根據預設、會啟用基本驗證、這表示伺服器會傳回基本驗證挑戰。此設定可在wsconfig.xml檔案中變更。

LDAP

輕量型目錄存取傳輸協定（LDAP）是一種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、可用於Web服務Proxy。LDAP整合可讓使用者驗證角色、並將角色對應至群組。

如需設定LDAP功能的相關資訊、請參閱Unified Manager介面或互動式API文件的LDAP區段中的組態選項。

設定使用者存取權

您可以對密碼套用額外加密、設定基本驗證、以及定義角色型存取、藉此管理使用者存取。

對密碼套用額外加密

為了達到最高安全等級、您可以使用現有的SHA256密碼編碼、對密碼套用額外的加密。

這項額外的加密程序會針對每個SHA256雜湊加密、隨機套用一組位元組至每個密碼（SALT）。Salted SHA256加密會套用至所有新建立的密碼。

步驟

1. 開啟users.properties檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - （Linux）-/opt/netapp/SANtricity網路服務Proxy /資料/組態
2. 以純文字重新輸入加密密碼。
3. 執行「Recurepasswds」命令列公用程式以重新加密密碼、或只要重新啟動Web Services Proxy即可。此公用程式安裝在Web Services Proxy的根安裝目錄中。

   或者、只要透過Unified Manager執行密碼編輯、您就可以更改和散列本機使用者密碼。

設定基本驗證

預設會啟用基本驗證、這表示伺服器會傳回基本驗證挑戰。如果需要、您可以在wsconfig.xml檔案中變更該設定。

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 指定假（未啟用）或真（已啟用）、以修改檔案中的下列行。

例如：「<env key="enable-base-auth">true（真）」）

3. 儲存檔案。
4. 重新啟動Webserver服務、使變更生效。

設定角色型存取

若要限制使用者存取特定功能、您可以修改為每個使用者帳戶指定的角色。

Web服務Proxy包含角色型存取控制（RBAC）、其中的角色與預先定義的使用者相關聯。每個角色都會將權限授與特定層級的功能。您可以直接修改users.properties檔案、以變更指派給使用者帳戶的角色。

您也可以使用Unified Manager中的存取管理來變更使用者帳戶。如需詳細資訊、請參閱Unified Manager提供的線上說明。

步驟

1. 開啟users.properties檔案、位於：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - （Linux）-/opt/netapp/SANtricity網路服務Proxy /資料/組態
2. 找出您要修改的使用者帳戶（儲存、安全、監控、支援、RW、 或RO)。

   請勿修改管理使用者。這是擁有所有功能存取權的超級使用者。

3. 視需要新增或移除指定的角色。

   角色包括：

   - 資訊安全管理：SSL與憑證管理。
   - Storage・admin -對儲存系統組態的完整讀寫存取權。
   - Storage・Monitor（儲存設備監控器）-唯讀存取、可檢視儲存系統資料。
   - support.admin：存取儲存系統上的所有硬體資源、並支援AutoSupport 諸如恢復（ASUP）等作業。

     所有使用者（包括系統管理員）都需要儲存設備監控角色。

4. 儲存檔案。

管理 SANtricity Web 服務 Proxy 中的安全性和憑證

為確保Web服務Proxy的安全性、您可以指定SSL連接埠名稱、並管理憑證。憑證可識別網站擁有者、以確保用戶端與伺服器之間的安全連線。

啟用SSL

Web服務Proxy使用安全通訊端層（SSL）來確保安全性、此功能可在安裝期間啟用。您可以在wsconfig.xml檔案中變更SSL連接埠名稱。

步驟

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 新增或變更SSL連接埠號碼、類似下列範例：

```
<sslport clientauth="request">8443</sslport>
```

結果

當伺服器啟動時、伺服器會尋找Keystore和信任存放區檔案。

- 如果伺服器找不到Keystore、伺服器會使用第一個偵測到的非迴路IPV4位址的IP位址來產生Keystore、然後將自我簽署的憑證新增至Keystore。
- 如果伺服器找不到信任存放區、或未指定信任存放區、則伺服器會使用Keystore做為信任存放區。

略過憑證驗證

為了支援安全連線、Web Services Proxy會根據自己的信任憑證來驗證儲存系統的憑證。如果需要、您可以指定Proxy在連線至儲存系統之前略過該驗證。

開始之前

- 所有儲存系統連線都必須安全無虞。

步驟

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 在"trust．all.array"項中輸入"true"、如範例所示：

```
<env key="trust.all.arrays">true</env>
```

3. 儲存檔案。

產生並匯入主機管理憑證

憑證可識別網站擁有者、以確保用戶端與伺服器之間的安全連線。若要為安裝Web服務Proxy的主機系統產生及匯入憑證授權單位（CA）憑證、您可以使用API端點。

若要管理主機系統的憑證、請使用API執行下列工作：

- 為主機系統建立憑證簽署要求（CSR）。
- 將CSR檔案傳送至CA、然後等待他們傳送憑證檔案給您。

- 將簽署的憑證匯入主機系統。

> 您也可以在Unified Manager介面中管理憑證。如需詳細資訊、請參閱Unified Manager中的線上說明。

步驟

1. 登入 "互動式API文件"。
2. 移至右上角的下拉式功能表、然後選取* v2*。
3. 展開「管理」連結、然後向下捲動至「/憑證」端點。
4. 產生CSR檔案：
   a. 選取* POST：/certificates 、然後選取 Try it Out *。

      Web伺服器會重新產生自我簽署的憑證。然後、您可以在欄位中輸入資訊、以定義用於產生CSR的一般名稱、組織、組織單位、替代ID及其他資訊。

   b. 在「範例值」窗格中新增必要資訊、以產生有效的CA憑證、然後執行命令。

      > 請勿再次呼叫* POST：/certificates 或 POST：/certificates /RESET*、否則您必須重新產生CSR。當您撥打* POST：/憑證*或* POST：/憑證/重設*時、您會產生新的自我簽署憑證、其中含有新的私密金鑰。如果您傳送的CSR是在伺服器上私密金鑰上次重設之前產生的、則新的安全性憑證將無法運作。您必須產生新的CSR並要求新的CA憑證。

   c. 執行「取得：/憑證/伺服器」端點、確認目前的憑證狀態為自我簽署的憑證、其中含有從* POST ：/certificates *命令新增的資訊。

      此時伺服器憑證（以別名「j防eat」表示）仍為自我簽署。

   d. 展開* post：/certificates /匯出*端點、選取* Try it out 、輸入**CSR**檔案的檔案名稱、然後按一下*執行。
5. 將「fileUrl」複製並貼到新的瀏覽器索引標籤下載CSR檔案、然後將CSR檔案傳送到有效的CA、以申請新的Web伺服器憑證鏈結。
6. 當CA發行新的憑證鏈結時、請使用憑證管理工具來解密根、中繼和Web伺服器憑證、然後將它們匯入Web服務Proxy伺服器：
   a. 展開* post：/sslconfig/server*端點、然後選取* Try it out *。
   b. 在*別名*欄位中輸入CA根憑證的名稱。
   c. 在* replaceMainServerCertificated*欄位中選取*「假*」。
   d. 瀏覽並選取新的CA根憑證。
   e. 按一下*執行*。
   f. 確認已成功上傳憑證。
   g. 針對CA中繼憑證重複CA憑證上傳程序。
   h. 重複新Web伺服器安全性憑證檔案的憑證上傳程序、除非在這個步驟中、請在* replaceMainServerCertificated*下拉式清單中選取* true*。
   i. 確認已成功匯入Web伺服器安全性憑證。
   j. 若要確認新的根、中繼及Web伺服器憑證可在Keystore中使用、請執行* Get/certificates/server*。

7. 選取並展開* POST：/憑證/重新載入*端點、然後選取*試用*。出現提示時、無論是否要重新啟動兩個控制器、請選取*假*。（「True」僅適用於雙陣列控制器。） 按一下*執行*。

   每個憑證/重新載入*端點通常會傳回成功的http 202回應。不過、重新載入Web伺服器信任存放區和Keystore憑證、確實會在API程序和Web伺服器憑證重新載入程序之間建立競爭條件。在極少數情況下、Web伺服器憑證重新載入可能會擊敗API處理。在這種情況下、即使重新載入成功完成、重新載入仍會失敗。如果發生這種情況、請繼續下一步。如果重新載入實際上失敗、則下一步也會失敗。

8. 關閉Web服務Proxy的目前瀏覽器工作階段、開啟新的瀏覽器工作階段、並確認可以建立新的安全瀏覽器連線至Web服務Proxy。

   透過無痕式或私有瀏覽工作階段、您可以開啟與伺服器的連線、而不使用先前瀏覽工作階段中儲存的任何資料。

登入鎖定功能

只能透過 REST API 設定，您可以限制內嵌式和 Proxy Web Services 的登入嘗試次數。根據您的設定，一旦超過 Web 服務的登入嘗試次數，就會啟用鎖定功能。

步驟

1. 登入 "互動式API文件"。
2. 移至右上角的下拉式功能表、然後選取* v2*。
3. 按一下「取得： / 設定 / 鎖定 * 」端點以擷取鎖定設定。
4. 按一下 * POST ： / 設定 / 鎖定 * 端點，然後按一下 * 試試看 * 來設定鎖定設定。

使用 SANtricity Web 服務 Proxy 管理儲存系統

若要管理網路中的儲存系統、您必須先探索儲存系統、然後將其新增至管理清單。

探索儲存系統

您可以設定自動探索或手動探索儲存系統。

自動探索儲存系統

您可以修改wsconfig.xml檔案中的設定、指定在網路中自動探索儲存系統。根據預設、IPv6自動探索會停用、並啟用IPv4。

您只需提供一個管理IP或DNS位址、即可新增儲存系統。當路徑尚未設定或路徑已設定且可旋轉時、伺服器會自動探索所有管理路徑。

> 如果您嘗試在初始連線之後、使用IPv6傳輸協定從控制器組態自動探索儲存系統、則此程序可能會失敗。可能導致故障的原因包括：在儲存系統上啟用IP位址轉送或IPv6時發生問題、但伺服器上卻未啟用IPv6。

開始之前

啟用IPv6探索設定之前、請先確認您的基礎架構支援IPv6連線至儲存系統、以減輕任何連線問題。

步驟

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 在自動探索字串中、視需要將設定從「true」變更為「假」。請參閱下列範例。

```
<env key="autodiscover.ipv6.enable">true</env>
```

> 當路徑設定完成、但未設定為伺服器可以路由傳送到位址時、會發生間歇性的連線錯誤。如果無法將IP位址設定為可從主機路由傳送、請關閉自動探索（將設定變更為「假」）。

3. 儲存檔案。

使用**API**端點探索及新增儲存系統

您可以使用API端點來探索儲存系統、並將其新增至受管理清單。此程序會在儲存系統與API之間建立管理連線。

> 本工作說明如何使用REST API探索及新增儲存系統、以便您在互動式API文件中管理這些系統。不過、您可能想要改用Unified Manager來管理儲存系統、因為Unified Manager提供簡單易用的介面。如需詳細資訊、請參閱Unified Manager提供的線上說明。

開始之前

若儲存系統SANtricity 使用的是11、30版及更新版本、則必須在SANtricity 「系統管理程式」介面中啟用符號的舊版管理介面。否則、探索端點就會失敗。您可以開啟System Manager來尋找此設定、然後前往功能表：設定[系統>其他設定>變更管理介面]。

步驟

1. 登入 "互動式API文件"。
2. 探索儲存系統、如下所示：
   a. 從API文件中、確定下拉式清單中選取* V2*、然後展開* Storage-Systems*類別。
   b. 按一下「* POST：/dredle*」端點、然後按一下「試試看」。
   c. 輸入表格中所述的參數。

startIP endIP	將字串取代為網路中一或多個儲存系統的起始和結束IP位址範圍。
使用代理程式	

將此值設為： • 是=使用頻內代理程式進行網路掃描。 • 否=請勿使用頻內代理程式進行網路掃描。
ConnectionTimeDOut
輸入連線逾時之前允許掃描的秒數。
最大連接埠使用
輸入用於網路掃描的連接埠數量上限。

d. 按一下*執行*。

ⓘ API動作會在使用者未提示的情況下執行。

探索程序會在背景執行。

a. 請確定程式碼傳回202。

b. 在「回應本文」下、找到要求ID傳回的值。您需要申請ID、才能在下個步驟中檢視結果。

3. 檢視探索結果、如下所示：

a. 按一下「* Get：/dredle*」端點、然後按一下「* Try it Out （*試用）」。

b. 輸入上一個步驟的要求ID。如果您將*要求ID*保留空白、端點預設為上次執行的要求ID。

c. 按一下*執行*。

d. 請確定程式碼傳回200。

e. 在回應本文中、找出您的Request ID和storageSystems字串。字串看起來類似下列範例：

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. 記下WWN、標籤和IP地址的值。您需要這些資源來執行下一步。

4. 新增儲存系統、如下所示：
   a. 按一下* POST：/STA-system*端點、然後按一下*試用*。
   b. 輸入表格中所述的參數。

ID
輸入此儲存系統的唯一名稱。您可以輸入標籤（顯示於Get:/Discovery的回應中）、但名稱可以是您選擇的任何字串。如果您未提供此欄位的值、Web Services會自動指派唯一的識別碼。
控制器地址
輸入回應中顯示的IP位址：Get/Discovery。對於雙控制器、請以逗號分隔IP位址。例如： 「IP位址1」、「IP位址2」
驗證
輸入「true」、您就能收到Web Services可連線至儲存系統的確認訊息。
密碼
輸入儲存系統的管理密碼。
WWN
輸入儲存系統的WWN（顯示在Get:/Discovery的回應中）。

   c. 刪除"enableTrace"之後的所有字串：true（真）、使整個字串集類似於下列範例：

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

   d. 按一下*執行*。
   e. 請確定程式碼回應為201、表示端點已成功執行。

「貼文：**/storage**系統」端點已排入佇列。您可以在下一步中使用* Get:/media-Systems*端點來檢視結果。

5. 確認新增清單、如下所示：
   a. 按一下* Get:/media-system*端點。

      不需要任何參數。

   b. 按一下*執行*。
   c. 請確定程式碼回應為200、表示端點已成功執行。
   d. 在回應本文中、尋找儲存系統詳細資料。傳回的值表示已成功新增至託管陣列清單、類似下列範例：

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```

擴充託管儲存系統的數量

根據預設、API最多可管理100個儲存系統。如果您需要管理更多資源、則必須滿足伺服器的記憶體需求。

伺服器設為使用512 MB記憶體。對於網路中每100個額外的儲存系統、請將250 MB新增至該數目。請勿增加比實際擁有的記憶體更多的記憶體。為您的作業系統和其他應用程式提供足夠的額外資源。

> 預設的快取大小為8、192個事件。MEL事件快取的大約資料使用量為每8、192個事件的1MB。因此、保留預設值後、儲存系統的快取使用量應約為1MB。

> 除了記憶體、Proxy也會針對每個儲存系統使用網路連接埠。Linux和Windows將網路連接埠視為檔案處理。作爲一項安全措施、大多數作業系統都會限制處理程序或使用者一次可以開啟的檔案處理數量。尤其是在Linux環境中、開放式TCP連線被視為檔案處理、Web服務Proxy很容易超過此限制。由於此修正程式是系統相依的、因此您應該參閱作業系統的文件、以瞭解如何提高此值。

步驟

1. 執行下列其中一項：
   - 在Windows上、前往appserver64.init檔案。找到「vmarg.3=-Xmx512M」這一行
   - 在Linux上、前往webserver.sh檔案。找到行「Java_options="-Xmx512M"」
2. 若要增加記憶體容量、請將「512」換成所需的記憶體（以MB為單位）。
3. 儲存檔案。

管理 SANtricity Web 服務 Proxy 統計資料的自動輪詢

您可以針對探索到的儲存系統上的所有磁碟和磁碟區統計資料、設定自動輪詢。

統計資料總覽

統計資料提供有關資料收集率和儲存系統效能的資訊。

Web服務Proxy可存取下列類型的統計資料：

- 原始統計資料-資料收集時資料點的總計計數器。原始統計資料可用於總讀取作業或總寫入作業。
- 分析統計資料-間隔的計算資訊。分析統計資料的範例包括每秒讀取輸入/輸出作業（IOPs）或寫入處理量。

原始統計資料是線性的、通常需要至少兩個收集的資料點、才能從中衍生可用的資料。分析的統計資料是原始統計資料的推導、提供重要的指標。許多可從原始統計資料衍生的值、都會以可用的時間點格式顯示在分析統計資料中、以方便您使用。

無論是否啟用自動輪詢、您都可以擷取原始統計資料。您可以將「useclace=true」查詢字串新增至URL的結尾、以從上次輪詢擷取快取的統計資料。使用快取的結果可大幅提升統計資料擷取的效能。不過、多個呼叫的速率等於或小於設定的輪詢時間間隔快取、則會擷取相同的資料。

統計功能

Web服務Proxy提供API端點、可從支援的硬體模型和軟體版本擷取原始和分析的控制器及介面統計資料。

原始統計資料**API**

- 「」/「儲存系統」/「｛system-id｝/控制器統計資料」
- 「/儲存系統/｛system-id｝/磁碟機統計資料/｛選擇性磁碟ID清單｝」
- 「」/「儲存系統」/｛system-id｝/「介面統計資料」/「｛可選介面ID清單｝」
- 「/儲存系統/｛system-id｝/ Volume統計資料/｛Optional list of volume ID｝」

分析統計資料**API**

- 「/儲存系統/｛id｝/分析控制器統計資料/」
- 「/儲存系統/｛id｝/分析磁碟機統計資料/｛選擇性磁碟ID清單｝」
- 「/儲存系統/｛id｝/分析介面統計資料/｛可選介面ID清單｝」
- 「/儲存系統/｛id｝/分析磁碟區統計資料/｛可選磁碟區ID清單｝」

這些URL會從上次輪詢擷取分析的統計資料、而且只有在啟用輪詢時才可使用。這些URL包括下列輸入輸出資料：

- 每秒作業數
- 處理量（以每秒MB為單位）
- 回應時間（毫秒）

這些計算是根據統計輪詢迭代之間的差異而進行、這是儲存效能最常見的測量方法。這些統計資料優於未分析的統計資料。

> 系統啟動時、先前沒有統計資料集合可用來計算各種度量、因此分析的統計資料在啟動後至少需要一個輪詢週期才能傳回資料。此外、如果重設累積計數器、則下一個輪詢週期的資料數目將無法預測。

設定輪詢時間間隔

若要設定輪詢時間間隔、請修改wsconfig.xml檔案、以指定輪詢時間間隔（秒）。

> 由於統計資料會快取到記憶體中、因此每個儲存系統的記憶體使用量可能會增加約1.5 MB。

開始之前

- 儲存系統必須由Proxy探索。

步驟

1. 開啟wsconfig.xml檔案、網址為：
   - （Windows）- C：\Program Files\NetApp\SANtricity Web Services Proxy
   - （Linux）-/opt/netapp/SANtricity _web_services代理
2. 在「<env-entries >」標記中新增下列行、其中「n」是輪詢要求之間的間隔秒數：

   ```
   <env key="stats.poll.interval">n</env>
   ```

   例如、如果輸入60、輪詢會以60秒的時間間隔開始。也就是系統會要求輪詢在前一個輪詢期間完成後60秒開始（無論前一個輪詢期間的持續時間為何）。所有統計資料都會以擷取的確切時間加上時間戳記。系統會使用時間戳記或時間差異、以60秒計算為基礎。

3. 儲存檔案。

使用 SANtricity Web 服務 Proxy 管理 AutoSupport

您可以設定AutoSupport 收集資料的功能（ASUP）、然後自動將資料傳送給技術支援部門、以進行遠端疑難排解和問題分析。

概述（ASUP）AutoSupport

此功能會根據手動和排程型條件、自動將訊息傳輸至NetApp。AutoSupport

每AutoSupport 個VMware資訊都是記錄檔、組態資料、狀態資料和效能指標的集合。根據預設AutoSupport 、每週將下表所列的檔案傳輸給NetApp支援團隊一次。

檔案名稱	說明
x-headers-data.txt	包含X-header資訊的.txt檔案。
manifest.xml	詳述訊息內容的.xml檔案。
arraydata.xml	包含用戶端持續資料清單的.xml檔案。
appserver-config.txt	包含應用程式伺服器組態資料的.txt檔案。
wsconfig.txt	包含Web服務組態資料的.txt檔案。
host-info.txt	包含主機環境相關資訊的.txt檔案。
Server-logs.7z	包含每個可用Web伺服器記錄檔的.7z檔案。
client-info.txt	含有任意金鑰/值配對的.txt檔案、適用於特定應用程式的計數器、例如方法和網頁點閱。
WebService-profile.json	這些檔案包含Webservices設定檔資料、以及球衣監控統計資料。根據預設、會啟用澤西島監控統計資料。您可以在wsconfig.xml檔案中啟用和停用這些功能、如下所示： • 啟用：「<env key="enable.jersect.edics">true（真）」） • 停用：「<env key="enable.jersect.edics">false」

設定**AutoSupport** 功能

根據預設、安裝時會啟用此功能；不過、您可以變更該設定或修改交付類型。AutoSupport

啟用或停用**AutoSupport** 功能

在初始安裝Web Services Proxy時、會啟用或停用此功能、但您可以在ASUPConfig檔案中變更該設定。AutoSupport

您可以AutoSupport 透過ASUPConfig.xml檔案啟用或停用功能、如下列步驟所述。或者、您也可以使用*組態*和* POST / asup *透過API啟用或停用此功能、然後輸入「true」或「假」。

1. 在工作目錄中開啟ASUPConfig.xml檔案。
2. 找出<asupdata enable="Boolean_value" timestamp="timestamp"> 要使用的線路
3. 輸入「true」（啟用）或「false」（停用）。例如：

```
<asupdata enabled="false" timestamp="0">
```

時間戳記項目是多餘的。

4. 儲存檔案。

設定**AutoSupport** 供應功能

您可以將 AutoSupport 功能設定為使用 HTTPS 或 SMTP 傳送方法。HTTPS是預設的傳送方法。

1. 存取工作目錄中的ASUPConfig.xml檔案。
2. 在字串中、按下表所述輸入1、2或3、「<交付 類型="n">」：

價值	說明
1.	• HTTPS *（預設） <交付 類型="1">

2.	• SMTP*-若要正確設定AutoSupport 將「不確定」傳送類型設定為SMTP,您必須加入以下範例所示的SMTP郵件伺服器位址以及寄件者和收件者使用者電子郵件：
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`