憑證與驗證
SANtricity 11.6

NetApp
February 12, 2024

目錄

憑證與驗證 1
憑證管理 1
存取管理 8

憑證與驗證

憑證管理

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。

簽署的憑證

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Unified Manager、您可以管理主機管理系統上瀏覽器的憑證、以及探索到的儲存陣列中的控制器。

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。

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：

- 根-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。
- 中級：從根目錄下分出的是中繼憑證。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：在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。

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。

Unified Manager認證

Unified Manager介面會與主機系統上的Web Services Proxy一起安裝。當您開啟瀏覽器並嘗試連線至Unified Manager時、瀏覽器會檢查數位憑證、以驗證主機是否為信任來源。如果瀏覽器找不到伺服器的CA簽署憑證、則會開啟警告訊息。您可以從這裡繼續前往網站、接受該工作階段的自我簽署憑證。或者、您也可以從CA取得已簽署的數位憑證、因此您不會再看到警告訊息。

控制器的憑證

在Unified Manager工作階段期間、當您嘗試存取沒有CA簽署憑證的控制器時、可能會看到其他安全訊息。在此情況下、您可以永久信任自我簽署的憑證、或是匯入控制器的CA簽署憑證、讓Web服務Proxy伺服器能夠驗證這些控制器傳入的用戶端要求。

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。
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。
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。
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」。

期限	說明
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。
信任存放區	信任存放區是一個儲存庫、其中包含來自信任的第三方（例如CA）的憑證。
Web服務Proxy	Web服務Proxy可透過標準HTTPS機制提供存取、讓系統管理員能夠設定儲存陣列的管理服務。Proxy可安裝在Windows或Linux主機上。Unified Manager介面與Web Services Proxy搭售。

使用方法

使用**CA**簽署的憑證

您可以取得及匯入CA簽署的憑證、以安全存取裝載Unified Manager的管理系統。

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、不會顯示憑證功能。

關於這項工作

使用CA簽署的憑證是兩個步驟的程序。

步驟**1**：完成並提交**CSR**

您必須先產生憑證簽署要求（CSR）檔案、然後將其傳送至CA。

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

本工作說明如何產生您傳送給CA的CSR檔案、以接收裝載Unified Manager和Web Services Proxy之系統的已簽署管理憑證。您必須提供組織的相關資訊、以及主機系統的IP位址或DNS名稱。

> 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. 選擇*憑證管理*。
2. 從*管理*索引標籤、選取*完整的csr*。

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：您的主機系統或企業所在的城市。
    - 州/地區（選用）：主機系統或企業所在的州或地區。
    - 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。
4. 輸入主機系統的下列相關資訊：
    - 一般名稱：安裝Web服務Proxy之主機系統的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Unified Manager。請勿包含http：//或https：//。
    - 備用**IP**位址-如果一般名稱是IP位址、您可以選擇輸入主機系統的任何其他IP位址或別名。對於多個項目、請使用以逗號分隔的格式。
    - 備用**DNS**名稱-如果通用名稱是DNS名稱、請輸入主機系統的任何其他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。
5. 單擊*完成*。

    CSR檔案會下載至您的本機系統。下載的資料夾位置取決於您的瀏覽器。

6. 將CSR檔案提交給CA、並以PEEM或DER格式要求簽署的憑證。

完成後

等待CA傳回憑證檔案、然後前往 "步驟2：匯入管理憑證"。

步驟**2**：匯入管理憑證

收到簽署的憑證後、請匯入安裝Unified Manager介面的主機系統的憑證鏈結。

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。
- 您已產生憑證簽署要求（.CSR檔案）、並將其傳送至CA。
- CA傳回信任的憑證檔案。
- 憑證檔案會安裝在您的本機系統上。
- 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、一或多個中繼憑證及伺服器憑證。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。

步驟

1. 選擇*憑證管理*。
2. 從*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. 按一下*瀏覽*以先選取根和中繼檔案、然後選取伺服器憑證。

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。憑證資訊會顯示在「憑證管理」頁面上。

重設管理憑證

您可以將管理憑證還原為原始的原廠自我簽署狀態。

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

此工作會從SANtricity 安裝了Web服務Proxy和支援服務的主機系統刪除目前的管理憑證。重設憑證後、主機系統會恢復使用自我簽署的憑證。

步驟

1. 選擇*憑證管理*。
2. 從*管理*索引標籤、選取*重設*。

   此時將打開一個*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

系統會從伺服器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。

匯入陣列的憑證

如有必要、您可以匯入儲存陣列的憑證、以便使用裝載SANtricity 了VMware Unified Manager的系統進行驗證。憑證可以由憑證授權單位（CA）簽署、也可以自行簽署。

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。
- 如果您要匯入信任的憑證、則必須使用SANtricity NetApp System Manager匯入儲存陣列控制器的憑證。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。

   此頁面顯示針對儲存陣列所報告的所有憑證。

3. 選取*功能表：匯入[憑證]*以匯入CA憑證、或選取*功能表：匯入[自我簽署的儲存陣列憑證]*以匯入自我簽署的憑證。

   若要限制檢視、您可以使用*顯示…*篩選的憑證欄位、或按一下其中一個欄位標題來排序憑證列。

4. 在對話方塊中、選取憑證、然後按一下*匯入*。

   憑證已上傳並驗證。

檢視憑證

您可以檢視憑證的摘要資訊、包括使用憑證的組織、發行憑證的授權單位、有效期間及指紋（唯一識別碼）。

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. 選擇*憑證管理*。
2. 選取下列其中一個索引標籤：
   - 管理：顯示託管Web服務Proxy之系統的憑證。管理憑證可由憑證授權單位（CA）自行簽署或核准。可安全存取Unified Manager。
   - * Trusted （受信任的）-顯示Unified Manager可存取的憑證、以供儲存陣列和其他遠端伺服器（例如LDAP伺服器）使用。這些憑證可以從憑證授權單位（CA）核發、也可以自行簽署。
3. 若要查看有關憑證的詳細資訊、請選取其列、選取列尾端的省略符號、然後按一下*檢視*或*匯出*。

匯出憑證

您可以匯出憑證以檢視其完整詳細資料。

開始之前

若要開啟匯出的檔案、您必須擁有憑證檢視器應用程式。

步驟

1. 選擇*憑證管理*。
2. 選取下列其中一個索引標籤：
   - 管理：顯示託管Web服務Proxy之系統的憑證。管理憑證可由憑證授權單位（CA）自行簽署或核准。可安全存取Unified Manager。
   - * Trusted （受信任的）-顯示Unified Manager可存取的憑證、以供儲存陣列和其他遠端伺服器（例如LDAP伺服器）使用。這些憑證可以從憑證授權單位（CA）核發、也可以自行簽署。
3. 從頁面選取憑證、然後按一下列結尾的省略符號。
4. 按一下「匯出」、然後儲存憑證檔案。
5. 在憑證檢視器應用程式中開啟檔案。

刪除信任的憑證

您可以刪除一或多個不再需要的憑證、例如過期的憑證。

開始之前

請先匯入新的憑證、再刪除舊的憑證。

> 請注意、刪除根或中繼憑證可能會影響多個儲存陣列、因為這些陣列可以共用相同的憑證檔案。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。
3. 在表格中選取一或多個憑證、然後按一下*刪除*。

   > *刪除*功能不適用於預先安裝的憑證。

   「確認刪除信任的憑證」對話方塊隨即開啟。

4. 確認刪除、然後按一下*刪除*。

   該憑證會從表格中移除。

解決不受信任的憑證

當儲存陣列嘗試建立安全連線至SANtricity NetApp Unified Manager、但連線無法確認安全性時、就會發生不受信任的憑證。從「憑證」頁面、您可以從儲存陣列匯入自我簽署的憑證、或匯入由信任的第三方所核發的憑證授權單位（CA）憑證、藉此解決不受信任的憑證。

開始之前

- 您必須以包含「安全性管理」權限的使用者設定檔登入。
- 如果您打算匯入CA簽署的憑證：
  - 您已為儲存陣列中的每個控制器產生憑證簽署要求（.CSR檔案）、並將其傳送至CA。
  - CA傳回信任的憑證檔案。
  - 您可以在本機系統上使用憑證檔案。

關於這項工作

如果符合下列任一項條件、您可能需要安裝其他信任的CA憑證：

- 您最近新增了儲存陣列。
- 一個或兩個憑證都已過期。
- 一個或兩個憑證均已撤銷。
- 一或兩個憑證都遺失根或中繼憑證。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。

   此頁面顯示針對儲存陣列所報告的所有憑證。

3. 選取*功能表：匯入[憑證]*。若要匯入CA憑證或*功能表：匯入[自我簽署的儲存陣列憑證]*以匯入自我簽署的憑證。

   若要限制檢視、您可以使用*顯示…*篩選的憑證欄位、或按一下其中一個欄位標題來排序憑證列。

4. 在對話方塊中選取憑證、然後按一下*匯入*。

   憑證已上傳並驗證。

存取管理

概念

存取管理的運作方式

使用存取管理功能、在SANtricity 《統一化管理程式》中建立使用者驗證。

組態工作流程

存取管理組態的運作方式如下：

1. 系統管理員使用包含安全管理員權限的使用者設定檔登入Unified 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。首次登入時必須設定密碼。

2. 系統管理員會在使用者介面中導覽至「存取管理」、其中包含預先設定的本機使用者角色。這些角色是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RBAC功能來管理。本機使用者角色包括具有特定存取權限的預先定義使用者和角色。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使用者對應至本機使用者角色。
4. 系統管理員可為使用者提供Unified Manager的登入認證。
5. 使用者輸入認證資料以登入系統。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。
   - 讓使用者能夠存取使用者介面中的功能。

- 在上方橫幅中顯示使用者名稱。

Unified Manager提供的功能

存取功能取決於使用者指派的角色、包括下列項目：

- 儲存設備管理-完整讀寫陣列上的儲存物件存取權、但無法存取安全性組態。
- 安全管理：存取存取管理與憑證管理中的安全性組態。
- 支援**admin**：存取儲存陣列、故障資料及MEL事件上的所有硬體資源。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。

無法使用的功能會呈現灰色、或不會顯示在使用者介面中。

存取管理術語

瞭解存取管理條款如何套用SANtricity 至《統一化管理程式》。

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。
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。
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。
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。Unified Manager包含預先定義的角色。
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。
Web服務Proxy	Web服務Proxy可透過標準HTTPS機制提供存取、讓系統管理員能夠設定儲存陣列的管理服務。Proxy可安裝在Windows或Linux主機上。Unified Manager介面可與Web Services Proxy搭配使用。

對應角色的權限

RBAC（角色型存取控制）功能包括預先定義的使用者、其中有一或多個角色對應至他們。每個角色都包含存取SANtricity 功能、可在「統一化管理程式」中存取工作。

這些角色可讓使用者存取工作、如下所示：

- 儲存設備管理-完整讀寫陣列上的儲存物件存取權、但無法存取安全性組態。
- 安全管理：存取存取管理與憑證管理中的安全性組態。
- 支援**admin**：存取儲存陣列、故障資料及MEL事件上的所有硬體資源。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功能的權限、則該功能可能無法選取、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

系統管理員可以使用SANtricity 在NetApp Unified Manager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

本機使用者角色是在系統中預先設定的。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. 系統管理員使用包含安全管理員權限的使用者設定檔登入Unified Manager。

   「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

系統管理員可以使用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。

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 使用包含安全管理員權限的使用者設定檔登入到NetApp的《統一化管理程式》。

> 「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）、則系統管理員會在LDAP伺服器和安裝Web服務Proxy的主機系統之間、上傳憑證授權單位（CA）憑證鏈結進行驗證。
4. 建立伺服器連線之後、系統管理員會將使用者群組對應至本機使用者角色。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Web服務Proxy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。
- 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、您可以檢視使用者與預設角色之間的對應。這些對應是在Web Services Proxy for SANtricity the Unified Manager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

無法變更使用者和對應。只能修改密碼。

步驟

1. 選擇*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：

- 管理：擁有系統中所有功能存取權的超級管理員。此使用者包含所有角色。
- 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：儲存管理員、支援管理員及監控。
- 安全性：負責安全性組態的使用者、包括存取管理和憑證管理。此使用者包括下列角色：安全性管理和監控。
- 支援：負責硬體資源、故障資料及韌體升級的使用者。此使用者包括下列角色：Support Admin和Monitor。
- 監控：擁有系統唯讀存取權的使用者。此使用者僅包含「監控」角色。
- * rw*（讀寫）-此使用者包括下列角色：儲存管理員、支援管理員及監控。
- * RO*（唯讀）-此使用者僅包含「監控」角色。

變更密碼

您可以在「存取管理」中變更每位使用者的使用者密碼。

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、不會從密碼中移除。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。

步驟

1. 選擇*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、您可以選取核取方塊、要求使用者輸入密碼才能存取系統。
6. 在兩個欄位中輸入所選使用者的新密碼。
7. 輸入您的本機系統管理員密碼以確認此作業、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系統。

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系統、請勿設定密碼的最小長度。

步驟

1. 選擇*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*。

   「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系統而不輸入密碼、請清除「要求所有本機使用者密碼至少為」核取方塊。
   - 若要設定所有本機使用者密碼的最小密碼長度、請選取「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、您需要在LDAP伺服器和執行Web Services Proxy for SANtricity the Unified Manager的主機之間建立通訊。然後將LDAP使用者群組對應至本機使用者角色。

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本機使用者角色。

步驟

1. 選擇*存取管理*。
2. 從*目錄服務*索引標籤、選取*新增目錄伺服器*。

   「新增目錄伺服器」對話方塊隨即開啟。

3. 在*伺服器設定*索引標籤中、輸入LDAP伺服器的認證資料。

欄位詳細資料

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（*username @domain*）、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）
此欄位只有在上述伺服器URL欄位中指定LDAPS傳輸協定時才會顯示。 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。	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「c=bindacct,cn=uss,c=cpoc,dc=local'」之類的值。	連結密碼（選用）

設定	說明
當您輸入連結帳戶時、會顯示此欄位。 輸入綁定帳戶的密碼。	在新增之前先測試伺服器連線
如果您要確保系統能夠與您輸入的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。	**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'。

4. 按一下「**角色對應」索引標籤。
5. 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。

6. 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。
7. 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. 選擇*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（*username@domain*）、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）
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）

設定	說明
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
檢查系統是否能與LDAP伺服器組態通訊。按一下「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。您必須解決錯誤或清除核取方塊、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。

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Web服務Proxy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. 選擇*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。

常見問題集

為什麼我無法登入？

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

Unified Manager的登入錯誤可能是因為下列原因之一：

- 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。

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、您必須符合特定需求。

- 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、請先檢閱準則。

RBAC（角色型存取控制）功能包括下列角色：

- 儲存設備管理-完整讀寫陣列上的儲存物件存取權、但無法存取安全性組態。
- 安全管理：存取存取管理與憑證管理中的安全性組態。
- 支援**admin**：存取儲存陣列、故障資料及MEL事件上的所有硬體資源。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。

> 所有使用者（包括系統管理員）都必須具備「監控」角色。

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。

什麼是本機使用者？

本機使用者會在系統中預先定義、並包含特定權限。

本機使用者包括：

- 管理：擁有系統中所有功能存取權的超級管理員。此使用者包含所有角色。首次登入時必須設定密碼。
- 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：儲存管理員、支援管理員及監控。在設定密碼之前、此帳戶會停用。
- 安全性：負責安全性組態的使用者、包括存取管理和憑證管理。此使用者包括下列角色：安全性管理和監控。在設定密碼之前、此帳戶會停用。
- 支援：負責硬體資源、故障資料及韌體升級的使用者。此使用者包括下列角色：Support Admin和Monitor。在設定密碼之前、此帳戶會停用。
- 監控：擁有系統唯讀存取權的使用者。此使用者僅包含「監控」角色。在設定密碼之前、此帳戶會停用。
- * rw*（讀寫）-此使用者包括下列角色：儲存管理員、支援管理員及監控。在設定密碼之前、此帳戶會停用。
- * RO*（唯讀）-此使用者僅包含「監控」角色。在設定密碼之前、此帳戶會停用。