Unified Manager

SANtricity 11.8

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/e-series-santricity-118/um-admin/overview-interface-unified.html on January 31, 2025. Always check docs.netapp.com for the latest.

目錄

Unified Manager 6 提供多個陣列管理功能 1
主介面 1
儲存陣列 4
設定匯入 10
陣列群組 17
升級 20

Unified Manager 6 提供多個陣列管理功能

主介面

Unified Manager介面總覽

Unified Manager是網路型介面、可讓您在單一檢視畫面中管理多個儲存陣列。

主頁

登入Unified Manager時、主頁會開啟*管理-全部*。在此頁面中、您可以捲動瀏覽網路中探索到的儲存陣列清單、檢視其狀態、以及在單一陣列或陣列群組上執行作業。

導覽側邊列

您可以從導覽側邊列存取Unified Manager的功能。

區域	說明
管理	探索網路中的儲存陣列、啟動SANtricity 適用於陣列的《支援系統管理程式》、將設定從一個陣列匯入多個陣列、以及管理陣列群組。選取陣列名稱旁的核取方塊、即可對陣列名稱執行作業、例如匯入設定和建立陣列群組。每一列結尾的省略符號會提供即時功能表、以便在單一陣列上執行作業、例如重新命名。
營運	檢視批次作業的進度、例如將設定從一個陣列匯入另一個陣列。 當儲存陣列處於非最佳狀態時、部分作業無法使用。
憑證管理	管理要在瀏覽器和用戶端之間驗證的憑證。
存取管理	為Unified Manager介面建立使用者驗證。
支援	檢視技術支援選項、資源和聯絡人。

介面設定與說明

在介面右上角、您可以存取「說明」和其他文件。您也可以存取管理選項、這些選項可從登入名稱旁的下拉式清單中取得。

使用者登入和密碼

目前登入系統的使用者會顯示在介面右上角。

如需使用者和密碼的詳細資訊、請參閱：

- "設定管理密碼保護"

- "變更管理密碼"
- "變更本機使用者設定檔的密碼"

支援的瀏覽器

Unified Manager可從多種瀏覽器存取。

支援下列瀏覽器和版本。

瀏覽器	最低版本
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

必須安裝Web服務Proxy、並可供瀏覽器使用。

設定管理密碼保護

您必須使用系統管理員密碼來設定Unified Manager、以防止其遭到未獲授權的存取。

管理密碼和使用者設定檔

首次啟動Unified Manager時、系統會提示您設定管理員密碼。擁有管理員密碼的任何使用者都可以變更儲存陣列的組態。

除了管理員密碼之外、Unified Manager介面還包含預先設定的使用者設定檔、其中有一個或多個角色對應到這些設定檔。如需更多資訊、請參閱 "存取管理的運作方式"。

無法變更使用者和對應。只能修改密碼。若要變更密碼、請參閱：

- "變更管理密碼"
- "變更本機使用者設定檔的密碼"

工作階段逾時

在單一管理工作階段期間、軟體只會提示您輸入一次密碼。工作階段預設在閒置30分鐘後逾時、此時您必須再次輸入密碼。如果其他使用者從其他管理用戶端存取軟體、並在工作階段進行期間變更密碼、則下次嘗試組態作業或檢視作業時、系統會提示您輸入密碼。

基於安全考量、您只能在軟體進入「鎖定」狀態之前、嘗試輸入密碼五次。在此狀態下、軟體會拒絕後續的密碼嘗試。您必須等待10分鐘、才能重設為「正常」狀態、才能再次嘗試輸入密碼。

您可以調整工作階段逾時、也可以一併停用工作階段逾時。如需更多資訊、請參閱 "管理工作階段逾時"。

變更管理密碼

您可以變更用於存取Unified Manager的管理密碼。

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。
- 您必須知道目前的管理密碼。

關於這項工作

選擇密碼時請謹記以下準則：

- 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. 從表中選擇* admin*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、請勾選核取方塊、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*。

管理工作階段逾時

您可以設定Unified Manager的逾時、讓使用者在指定時間後中斷非作用中工作階段的連線。

關於這項工作

Unified Manager的工作階段逾時預設為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 工作階段達到其上限時、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. 從功能表列中、選取使用者登入名稱旁的下拉式箭頭。
2. 選擇*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）。

   您可以設定的最短逾時時間為15分鐘。

   > 若要停用工作階段逾時、請清除*設定時間長度…*核取方塊。

4. 按一下「 * 儲存 * 」。

儲存陣列

探索總覽

若要管理儲存資源、您必須先探索網路中的儲存陣列。

如何探索陣列？

使用「新增/探索」頁面、尋找並新增您要在組織網路中管理的儲存陣列。您可以探索多個陣列、也可以探索單一陣列。若要這麼做、請輸入網路IP位址、然後Unified Manager會嘗試個別連線至該範圍內的每個IP位址。

深入瞭解：

- "探索陣列的考量事項"
- "探索多個儲存陣列"
- "探索單一陣列"

如何管理陣列？

發現陣列後、請前往*管理-全部*頁面。在此頁面中、您可以捲動瀏覽網路中探索到的儲存陣列清單、檢視其狀態、以及在單一陣列或陣列群組上執行作業。

如果您想要管理單一陣列、可以選取該陣列並開啟System Manager。

深入瞭解：

- "存取System Manager的考量事項"
- "管理個別的儲存陣列"
- "檢視儲存陣列狀態"

概念

探索陣列的考量事項

在Unified Manager能夠顯示及管理儲存資源之前、它必須先探索您要在組織網路中管理的儲存陣列。您可以探索多個陣列、也可以探索單一陣列。

探索多個儲存陣列

如果您選擇探索多個陣列、請輸入網路IP位址範圍、然後Unified Manager會嘗試個別連線至該範圍內的每個IP位址。任何已成功連線的儲存陣列都會顯示在「Discover（探索）」頁面上、並可新增至您的管理網域。

探索單一儲存陣列

如果您選擇探索單一陣列、請在儲存陣列中輸入其中一個控制器的單一IP位址、然後新增個別的儲存陣列。

> Unified Manager只會探索並顯示指派給控制器之範圍內的單一IP位址或IP位址。如果指派給這些控制器的替代控制器或IP位址超出此單一IP位址或IP位址範圍、Unified Manager將不會發現或顯示這些控制器。不過、新增儲存陣列之後、所有相關的IP位址都會被探索並顯示在「管理」檢視中。

使用者認證

在探索過程中、您必須為每個要新增的儲存陣列提供管理員密碼。

Web服務憑證

在探索過程中、Unified Manager會驗證探索到的儲存陣列是否使用受信任來源的憑證。Unified Manager使用兩種類型的憑證型驗證來驗證其與瀏覽器建立的所有連線：

- 信任的憑證

  對於Unified Manager探索到的陣列、您可能需要安裝其他由憑證授權單位提供的信任憑證。

  使用*匯入*按鈕匯入這些憑證。如果您之前已連線至此陣列、則其中一個或兩個控制器憑證會在其憑證鏈結中過期、撤銷或遺失根憑證或中繼憑證。在管理儲存陣列之前、您必須先更換過期或撤銷的憑證、或是新增遺失的根憑證或中繼憑證。

- 自我簽署的憑證

  也可以使用自我簽署的憑證。如果系統管理員嘗試探索陣列而不匯入簽署的憑證、Unified Manager會顯示錯誤對話方塊、讓系統管理員接受自我簽署的憑證。儲存陣列的自我簽署憑證會標示為信任、儲存陣列也會新增至Unified Manager。

  如果您不信任儲存陣列的連線、請選取*取消*、然後在將儲存陣列新增至Unified Manager之前驗證儲存陣列的安全性憑證策略。

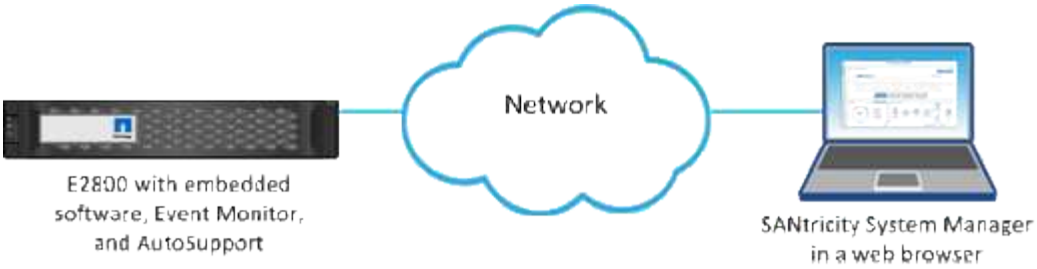
存取**System Manager**的考量事項

您可以選取一或多個儲存陣列、並在想要設定及管理儲存陣列時、使用「啟動」選項來開啟System Manager。

System Manager是控制器上的內嵌應用程式、透過乙太網路管理連接埠連線至網路。它包含所有陣列型功能。

若要存取System Manager、您必須具備：

- 此處列出的陣列機型之一："E系列硬體總覽"
- 透過網頁瀏覽器連線到網路管理用戶端的頻外連線。



探索陣列

探索多個儲存陣列

您會發現多個陣列、偵測管理伺服器所在子網路上的所有儲存陣列、並自動將探索到的陣列新增至管理網域。

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。
- 儲存陣列必須正確設定和設定。
- 儲存陣列密碼必須使用System Manager的「存取管理」方塊來設定。
- 若要解析不受信任的憑證、您必須擁有來自憑證授權單位（CA）的信任憑證檔案、而且憑證檔案可在本機系統上使用。

探索陣列是一個多步驟程序。

步驟**1**：輸入網路位址

您可以輸入網路位址範圍、以便在本機子網路中搜尋。任何已成功連線的儲存陣列都會顯示在「Discover（探索）」頁面上、而且可能會新增至您的管理網域。

如果您因任何原因而需要停止探索作業、請按一下*停止探索*。

步驟

1. 從「管理」頁面選取*「新增/探索」*。

   此時會出現「新增/探索」對話方塊。

2. 選取*「Discover all storage Array within a network range（探索網路範圍內的所有儲存陣列）」選項按鈕。
3. 輸入起始網路位址和結束網路位址、以在本機子網路中搜尋、然後按一下*「Start Discovery」（開始探索）*。

   探索程序隨即開始。此探索程序可能需要數分鐘的時間才能完成。探索頁面上的表格會隨著儲存陣列的探索而填入。

   > 如果未找到可管理的陣列、請確認儲存陣列已正確連線至您的網路、且其指派的位址在範圍內。按一下「新增探索參數」以返回「新增/探索」頁面。

4. 檢閱探索到的儲存陣列清單。

5. 選取您要新增至管理網域之任何儲存陣列旁的核取方塊、然後按一下*下一步*。

   Unified Manager會對您要新增至管理網域的每個陣列執行認證檢查。您可能需要解析任何與該陣列相關的自我簽署憑證和不受信任的憑證。

6. 單擊*下一步*繼續執行精靈中的下一步。

步驟2：在探索期間解決自我簽署的憑證

在探索過程中、系統會驗證儲存陣列是否使用受信任來源的憑證。

步驟

1. 執行下列其中一項：
   - 如果您信任已探索儲存陣列的連線、請繼續執行精靈中的下一個卡片。自我簽署的憑證會標示為信任、儲存陣列也會新增至Unified Manager。
   - 如果您不信任儲存陣列的連線、請選取*「取消」*、然後在將每個儲存陣列的安全性憑證策略新增至Unified Manager之前驗證。
2. 單擊*下一步*繼續執行精靈中的下一步。

步驟 3 ：在探索期間解決不受信任的憑證

當儲存陣列嘗試建立與Unified Manager的安全連線、但連線無法確認為安全時、就會發生不受信任的憑證。在陣列探索程序期間、您可以匯入由信任的第三方所發行的憑證授權單位（CA）憑證（或CA簽署的憑證）、以解決不受信任的憑證。

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. 選取您要解析不受信任憑證之任何儲存陣列旁的核取方塊、然後選取「**匯入」按鈕。

   隨即開啟一個對話方塊、用於匯入信任的憑證檔案。

2. 按一下*瀏覽*以選取儲存陣列的憑證檔案。

   檔案名稱會顯示在對話方塊中。

3. 按一下*匯入*。

   檔案會上傳並驗證。

   > 任何未解決的不受信任憑證問題儲存陣列、都不會新增至Unified Manager。

4. 單擊*下一步*繼續執行精靈中的下一步。

步驟 **4** ：提供密碼

您必須輸入要新增至管理網域之儲存陣列的密碼。

步驟

1. 輸入您要新增至Unified Manager的每個儲存陣列密碼。
2. *選用：*將儲存陣列與群組建立關聯：從下拉式清單中、選取要與所選儲存陣列建立關聯的群組。
3. 單擊*完成*。

完成後

儲存陣列會新增至您的管理網域、並與選取的群組相關聯（若有指定）。

> Unified Manager連線至指定的儲存陣列可能需要數分鐘的時間。

探索單一陣列

使用「新增/探索單一儲存陣列」選項、手動探索及新增單一儲存陣列至組織的網路。

開始之前

- 儲存陣列必須正確設定和設定。
- 儲存陣列密碼必須使用System Manager的「存取管理」方塊來設定。

步驟

1. 從「管理」頁面選取*「新增/探索」*。

   此時會出現「新增/探索」對話方塊。

2. 選取*「Discover a son那個 儲存陣列*」選項按鈕。
3. 輸入儲存陣列中其中一個控制器的IP位址、然後按一下*「Start Discovery」（開始探索）*。

   Unified Manager連線至指定的儲存陣列可能需要數分鐘的時間。

   > 當連線至指定控制器的IP位址失敗時、會出現「Storage Array Not平易近人（儲存陣列無法存取）」訊息。

4. 如果出現提示、請解決任何自我簽署的憑證。

   在探索過程中、系統會驗證探索到的儲存陣列是否使用受信任來源的憑證。如果無法找到儲存陣列的數位憑證、系統會提示您新增安全性例外狀況、以解決未由認可的憑證授權單位（CA）簽署的憑證。

5. 如果出現提示、請解析任何不受信任的憑證。

   當儲存陣列嘗試建立與Unified Manager的安全連線、但連線無法確認為安全時、就會發生不受信任的憑證。匯入由信任的第三方所發行的憑證授權單位（CA）憑證、以解決不受信任的憑證。

6. 單擊 * 下一步 * 。
7. *選用：*將探索到的儲存陣列與群組建立關聯：從下拉式清單中、選取要與儲存陣列建立關聯的群組。

預設會選取「All（全部）」群組。

8. 輸入要新增至管理網域之儲存陣列的管理員密碼、然後按一下*確定*。

完成後

儲存陣列會新增至Unified Manager、如果指定、也會新增至您所選的群組。

如果啟用自動支援資料收集功能、系統會自動為您新增的儲存陣列收集支援資料。

管理陣列

檢視儲存陣列狀態

Unified Manager會顯示每個已探索儲存陣列的狀態。

前往*管理-全部*頁面。在此頁面中、您可以檢視Web服務Proxy與該儲存陣列之間的連線狀態。

狀態指標如下表所述。

狀態	表示
最佳化	儲存陣列處於最佳狀態。沒有憑證問題、密碼有效。
密碼無效	提供無效的儲存陣列密碼。
不受信任的憑證	與儲存陣列的一或多個連線不受信任、因為HTTPS憑證為自我簽署且尚未匯入、或憑證已由CA簽署、且尚未匯入根和中繼CA憑證。
需要注意	儲存陣列發生問題、需要您介入修正。
穩固定位	儲存陣列處於鎖定狀態。
不明	從未聯絡過儲存陣列。當Web服務Proxy啟動且尚未與儲存陣列聯絡、或儲存陣列離線、且自Web服務Proxy啟動後從未聯絡過時、就會發生這種情況。
離線	Web Services Proxy先前曾聯絡過儲存陣列、但現在已失去與儲存陣列的所有連線。

管理個別的儲存陣列

當您想要執行管理作業時、可以使用「Launch」（啟動）選項來開啟一或多個儲存陣列的瀏覽器型系統管理員。

步驟

1. 從「Manage（管理）」頁面中、選取您要管理的一或多個儲存陣列。
2. 按一下 * 「 Launch * 」。

系統會開啟新視窗、並顯示System Manager登入頁面。

3. 輸入您的使用者名稱和密碼、然後按一下*登入*。

變更儲存陣列密碼

您可以在Unified Manager中更新用於檢視和存取儲存陣列的密碼。

開始之前

- 您必須以包含Storage管理權限的使用者設定檔登入。
- 您必須知道在System Manager中設定的儲存陣列目前密碼。

關於這項工作

在此工作中、您可以輸入儲存陣列的目前密碼、以便在Unified Manager中存取。如果在System Manager中變更陣列密碼、現在也必須在Unified Manager中變更該密碼、則可能需要這麼做。

步驟

1. 從「Manage（管理）」頁面、選取一或多個儲存陣列。
2. 選取功能表：「Uncommon Tasks（非正常工作）」[提供儲存陣列密碼]。
3. 輸入每個儲存陣列的密碼、然後按一下*「Save*」。

從**SANtricity NetApp**統一化管理程式移除儲存陣列

如果您不想再從Unified Manager進行管理、可以移除一或多個儲存陣列。

關於這項工作

您無法存取任何您移除的儲存陣列。不過、您可以將瀏覽器直接指向任何移除的儲存陣列IP位址或主機名稱、藉此建立連線至任何移除的儲存陣列。

移除儲存陣列不會影響儲存陣列或其資料。如果意外移除儲存陣列、可以再次新增。

步驟

1. 選取「管理」頁面。
2. 選取您要移除的一或多個儲存陣列。
3. 選取功能表：「Uncommon Tasks（非常見工作）」[移除儲存陣列]。

   儲存陣列會從SANtricity 整個畫面的所有畫面中移除、

設定匯入

設定匯入總覽

匯入設定功能可讓您執行批次作業、將設定從一個陣列匯入多個陣列。當您需要在網路中設定多個陣列時、此功能可節省時間。

可以匯入哪些設定？

您可以匯入警示方法、AutoSupport 支援各種功能的組態、目錄服務組態、儲存組態（例如磁碟區群組和集區）、以及系統設定（例如自動負載平衡）。

深入瞭解：

- "匯入設定的運作方式"
- "複寫儲存組態的需求"

如何執行批次匯入？

在要作為來源的儲存陣列上、開啟System Manager並設定所需的設定。然後從Unified Manager移至「管理」頁面、將設定匯入一或多個陣列。

深入瞭解：

- "匯入警示設定"
- "匯入AutoSupport 還原設定"
- "匯入目錄服務設定"
- "匯入儲存組態設定"
- "匯入系統設定"

概念

匯入設定的運作方式

您可以使用Unified Manager將設定從一個儲存陣列匯入至多個儲存陣列。匯入設定功能是批次作業、可在需要在網路中設定多個陣列時節省時間。

可供匯入的設定

下列組態可匯入多個陣列：

- 警示：警示通知方法、使用電子郵件、syslog伺服器或SNMP伺服器將重要事件傳送給系統管理員。
- 《》《》-一項功能、可監控儲存陣列的健全狀況、並將自動派單傳送給技術支援部門。AutoSupport
- 目錄服務：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）來管理的使用者驗證方法。
- 儲存組態-與下列項目相關的組態：
  - Volume（僅限厚磁碟區和非儲存庫磁碟區）
  - Volume群組與資源池
  - 熱備援磁碟機指派
- 系統設定-與下列項目相關的組態：
  - Volume的媒體掃描設定

- SSD 設定
- 自動負載平衡（不包括主機連線報告）

組態工作流程

若要匯入設定、請遵循此工作流程：

1. 在要作為來源的儲存陣列上、使用System Manager設定設定。
2. 在要用作目標的儲存陣列上、使用System Manager備份其組態。
3. 從Unified Manager移至*管理*頁面並匯入設定。
4. 從*作業*頁面、檢閱匯入設定作業的結果。

複寫儲存組態的需求

在將儲存組態從一個儲存陣列匯入另一個儲存陣列之前、請先檢閱相關要求和準則。

磁碟櫃

- 控制器所在的磁碟櫃必須在來源陣列和目標陣列上完全相同。
- 來源陣列和目標陣列上的機櫃ID必須相同。
- 擴充櫃必須裝入相同磁碟機類型的相同插槽（如果在組態中使用磁碟機、則不需要使用磁碟機的位置無關緊要）。

控制器

- 來源陣列和目標陣列之間的控制器類型可能不同（例如、從E2800匯入E5700）、但RBOD機箱類型必須相同。
- 來源陣列與目標陣列之間的HIC（包括主機的DA功能）必須相同。
- 不支援從雙工匯入至單工組態、但允許從單工匯入至雙工。
- FDE設定不包含在匯入程序中。

狀態

- 目標陣列必須處於最佳狀態。
- 來源陣列不需要處於最佳狀態。

儲存設備

- 只要目標上的磁碟區容量大於來源、來源陣列和目標陣列之間的磁碟機容量可能會有所不同。（目標陣列可能有較新、較大容量的磁碟機、但無法透過複寫作業完全設定成磁碟區。）
- 來源陣列上的磁碟集區磁碟區容量大於或等於64 TB、將會妨礙目標上的匯入程序。
- 精簡磁碟區不包含在匯入程序中。

使用批次匯入

匯入警示設定

您可以將警示組態從一個儲存陣列匯入其他儲存陣列。當您需要在網路中設定多個陣列時、這項批次作業可節省時間。

開始之前

- 警示是在System Manager中針對您要作為來源的儲存陣列進行設定（功能表：設定[警示]）。
- 在System Manager中備份目標儲存陣列的現有組態（功能表：設定[系統>儲存儲存儲存陣列組態]）。

關於這項工作

您可以為匯入作業選取電子郵件、SNMP或syslog警示。匯入的設定包括：

- 電子郵件警示-警示收件者的郵件伺服器位址和電子郵件位址。
- 系統記錄警示：系統記錄伺服器位址和udp連接埠。
- * SNMP alerts （**SNMP**警報）- SNMP伺服器的社群名稱和IP位址。

步驟

1. 在「管理」頁面中、按一下*匯入設定*。

   「匯入設定」精靈隨即開啟。

2. 在「選取設定」對話方塊中、選取*電子郵件警示*、* SNMP警示*或*系統記錄警示*、然後按「下一步」。

   此時會開啟一個對話方塊、供您選取來源陣列。

3. 在「選取來源」對話方塊中、選取含有您要匯入之設定的陣列、然後按一下「下一步」。
4. 在「選取目標」對話方塊中、選取一或多個陣列以接收新設定。

   > 韌體低於8.50的儲存陣列無法選取。此外、如果Unified Manager無法與陣列通訊（例如、陣列離線或有憑證、密碼或網路問題）、則陣列不會出現在此對話方塊中。

5. 單擊*完成*。

   「作業」頁面會顯示匯入作業的結果。如果作業失敗、您可以按一下其列以查看更多資訊。

結果

現在已將目標儲存陣列設定為透過電子郵件、SNMP或syslog傳送警示給系統管理員。

匯入**AutoSupport** 還原設定

您可以將AutoSupport 一個物件組態從一個儲存陣列匯入到其他儲存陣列。當您需要在網路中設定多個陣列時、這項批次作業可節省時間。

開始之前

- 在System Manager中為您要作為來源的儲存陣列設定支援（功能表：Support[支援中心]）AutoSupport 。
- 在System Manager中備份目標儲存陣列的現有組態（功能表：設定[系統>儲存儲存儲存陣列組態]）。

關於這項工作

匯入的設定包括獨立功能（基本AutoSupport 功能、AutoSupport 《不只支援此功能》、《不支援此功能》和《遠端診斷》）、維護時段、交付方法、 和分派排程。

步驟

1. 在「管理」頁面中、按一下*匯入設定*。

   「匯入設定」精靈隨即開啟。

2. 在Select Settings（選擇設置）對話框中，選擇* AutoSupport 還原*，然後單擊* Next*（下一步*）。

   此時會開啟一個對話方塊、供您選取來源陣列。

3. 在「選取來源」對話方塊中、選取含有您要匯入之設定的陣列、然後按一下「下一步」。
4. 在「選取目標」對話方塊中、選取一或多個陣列以接收新設定。

   > 韌體低於8.50的儲存陣列無法選取。此外、如果Unified Manager無法與陣列通訊（例如、陣列離線或有憑證、密碼或網路問題）、則陣列不會出現在此對話方塊中。

5. 單擊*完成*。

   「作業」頁面會顯示匯入作業的結果。如果作業失敗、您可以按一下其列以查看更多資訊。

結果

現在、目標儲存陣列的AutoSupport 功能與來源陣列的功能相同。

匯入目錄服務設定

您可以將目錄服務組態從一個儲存陣列匯入其他儲存陣列。當您需要在網路中設定多個陣列時、這項批次作業可節省時間。

開始之前

- 目錄服務是在System Manager中針對您要作為來源的儲存陣列進行設定（功能表：設定[Access Management（存取管理）]）。
- 在System Manager中備份目標儲存陣列的現有組態（功能表：設定[系統>儲存儲存儲存陣列組態]）。

關於這項工作

匯入的設定包括LDAP（輕量型目錄存取傳輸協定）伺服器的網域名稱和URL、以及LDAP伺服器使用者群組與儲存陣列預先定義角色的對應。

步驟

1. 在「管理」頁面中、按一下*匯入設定*。

   「匯入設定」精靈隨即開啟。

2. 在Select Settings（選擇設置）對話框中，選擇* Directory services（目錄服務），然後單擊* Next*（下一步）。

   此時會開啟一個對話方塊、供您選取來源陣列。

3. 在「選取來源」對話方塊中、選取含有您要匯入之設定的陣列、然後按一下「下一步」。
4. 在「選取目標」對話方塊中、選取一或多個陣列以接收新設定。

   > 韌體低於8.50的儲存陣列無法選取。此外、如果Unified Manager無法與陣列通訊（例如、陣列離線或有憑證、密碼或網路問題）、則陣列不會出現在此對話方塊中。

5. 單擊*完成*。

   「作業」頁面會顯示匯入作業的結果。如果作業失敗、您可以按一下其列以查看更多資訊。

結果

現在、目標儲存陣列已設定與來源陣列相同的目錄服務。

匯入系統設定

您可以將系統組態從一個儲存陣列匯入其他儲存陣列。當您需要在網路中設定多個陣列時、這項批次作業可節省時間。

開始之前

- 系統設定是在System Manager中針對您要作為來源的儲存陣列進行設定。
- 在System Manager中備份目標儲存陣列的現有組態（功能表：設定[系統>儲存儲存儲存陣列組態]）。

關於這項工作

匯入的設定包括磁碟區的媒體掃描設定、控制器的SSD設定、以及自動負載平衡（不包括主機連線報告）。

步驟

1. 在「管理」頁面中、按一下*匯入設定*。

   「匯入設定」精靈隨即開啟。

2. 在Select Settings（選擇設置）對話框中，選擇* System*（系統*），然後單擊* Next*（下一步*）。

   此時會開啟一個對話方塊、供您選取來源陣列。

3. 在「選取來源」對話方塊中、選取含有您要匯入之設定的陣列、然後按一下「下一步」。
4. 在「選取目標」對話方塊中、選取一或多個陣列以接收新設定。

   > 韌體低於8.50的儲存陣列無法選取。此外、如果Unified Manager無法與陣列通訊（例如、陣列離線或有憑證、密碼或網路問題）、則陣列不會出現在此對話方塊中。

5. 單擊*完成*。

「作業」頁面會顯示匯入作業的結果。如果作業失敗、您可以按一下其列以查看更多資訊。

結果

現在、目標儲存陣列的系統設定與來源陣列相同。

匯入儲存組態設定

您可以將儲存組態從一個儲存陣列匯入其他儲存陣列。當您需要在網路中設定多個陣列時、這項批次作業可節省時間。

開始之前

- 儲存設備是針對SANtricity 您要用作來源的儲存陣列、在《Sys供 系統管理程式》中進行設定。
- 在System Manager中備份目標儲存陣列的現有組態（功能表：設定[系統>儲存儲存儲存陣列組態]）。
- 來源陣列和目標陣列必須符合下列需求：
  - 控制器所在的磁碟櫃必須相同。
  - 機櫃ID必須相同。
  - 擴充櫃必須裝入相同磁碟機類型的相同插槽。
  - RBOD機箱類型必須相同。
  - HIC（包括主機的資料保證功能）必須相同。
  - 目標陣列必須處於最佳狀態。
  - 目標陣列上的Volume容量大於來源陣列的容量。
- 您瞭解下列限制：
  - 不支援從雙工匯入至單工組態、但允許從單工匯入至雙工。
  - 來源陣列上的磁碟集區磁碟區容量大於或等於64 TB、將會妨礙目標上的匯入程序。
  - 精簡磁碟區不包含在匯入程序中。

關於這項工作

匯入的設定包括已設定的磁碟區（僅適用於完整磁碟區和非儲存庫磁碟區）、磁碟區群組、集區和熱備援磁碟機指派。

步驟

1. 在「管理」頁面中、按一下*匯入設定*。

   「匯入設定」精靈隨即開啟。

2. 在Select Settings（選擇設置）對話框中，選擇* Storage configuration（儲存配置），然後單擊* Next*（下一步）。

   此時會開啟一個對話方塊、供您選取來源陣列。

3. 在「選取來源」對話方塊中、選取含有您要匯入之設定的陣列、然後按一下「下一步」。
4. 在「選取目標」對話方塊中、選取一或多個陣列以接收新設定。

韌體低於8.50的儲存陣列無法選取。此外、如果Unified Manager無法與陣列通訊（例如、陣列離線或有憑證、密碼或網路問題）、則陣列不會出現在此對話方塊中。

5. 單擊*完成*。

「作業」頁面會顯示匯入作業的結果。如果作業失敗、您可以按一下其列以查看更多資訊。

結果

現在、目標儲存陣列已設定與來源陣列相同的儲存組態。

常見問題集

將匯入哪些設定？

匯入設定功能是批次作業、可將組態從一個儲存陣列載入至多個儲存陣列。在此作業期間匯入的設定取決於來源儲存陣列在System Manager中的設定方式。

下列設定可匯入多個儲存陣列：

- 電子郵件警示-設定包含電子郵件伺服器位址和警示收件者的電子郵件位址。
- 系統記錄警示-設定包括系統記錄伺服器位址和一個udp連接埠。
- * SNMP警示*-設定包含SNMP伺服器的社群名稱和IP位址。
- * AutoSupport 《》《設定》包括獨立的功能（基本AutoSupport 功能、AutoSupport 《不限需求》和《遠端診斷》）、維護時間、交付方法、 和分派排程。
- 目錄服務-組態包括LDAP（輕量型目錄存取傳輸協定）伺服器的網域名稱和URL、以及LDAP伺服器使用者群組與儲存陣列預先定義角色的對應。
- 儲存組態-組態包括磁碟區（僅限完整磁碟區和非儲存庫磁碟區）、磁碟區群組、集區和熱備援磁碟機指派。
- 系統設定-組態包括磁碟區的媒體掃描設定、控制器的SSD快取、以及自動負載平衡（不包括主機連線報告）。

為什麼我看不到所有的儲存陣列？

在匯入設定作業期間、目標選擇對話方塊中可能無法使用部分儲存陣列。

儲存陣列可能不會出現、原因如下：

- 韌體版本低於8.50。
- 儲存陣列已離線。
- 系統無法與該陣列通訊（例如、陣列有憑證、密碼或網路問題）。

陣列群組

群組總覽

在「管理群組」頁面中、您可以建立一組儲存陣列群組、以利管理。

什麼是陣列群組？

您可以將一組儲存陣列分組、來管理實體與虛擬化的基礎架構。您可能想要將儲存陣列分組、以便更輕鬆地執行監控或報告工作。

群組有兩種類型：

- 全部群組：「全部」群組為預設群組、包含組織中探索到的所有儲存陣列。您可以從主檢視畫面存取All群組。
- 使用者建立的群組-使用者建立的群組包含您手動選取要新增至該群組的儲存陣列。使用者建立的群組可從主檢視存取。

如何設定群組？

在「管理群組」頁面中、您可以建立群組、然後將陣列新增至該群組。

深入瞭解：

- "設定儲存陣列群組"

設定儲存陣列群組

您可以建立儲存群組、然後將儲存陣列新增至群組。

設定群組是兩個步驟的程序。

步驟**1**：建立群組

您先建立群組。儲存設備群組會定義哪些磁碟機提供組成磁碟區的儲存設備。

步驟

1. 在「Manage（管理）」頁面中、選取功能表：Manage Groups（管理群組）[Create storage Array group（建立儲存陣列群組）
2. 在*名稱*欄位中、輸入新群組的名稱。
3. 選取您要新增至新群組的儲存陣列。
4. 按一下「 * 建立 * 」。

步驟**2**：新增儲存陣列至群組

您可以將一個或多個儲存陣列新增至使用者建立的群組。

步驟

1. 從主檢視畫面選取*管理*、然後選取您要新增儲存陣列的群組。
2. 選取功能表：管理群組[新增儲存陣列至群組]。

3. 選取您要新增至群組的儲存陣列。
4. 按一下「新增」

從群組中移除儲存陣列

如果您不想再從特定儲存群組進行管理、可以從群組中移除一或多個託管儲存陣列。

關於這項工作

從群組中移除儲存陣列並不會以任何方式影響儲存陣列或其資料。如果您的儲存陣列是由System Manager管理、您仍然可以使用瀏覽器來管理。如果不小心從群組中移除儲存陣列、則可以再次新增。

步驟

1. 從「Manage（管理）」頁面、選取功能表：「Manage Groups [Remove storage Array from group（管理群組[從群組移除儲存陣列]
2. 從下拉式清單中、選取包含您要移除之儲存陣列的群組、然後按一下您要從群組中移除之每個儲存陣列旁的核取方塊。
3. 按一下「移除」。

刪除儲存陣列群組

您可以移除一或多個不再需要的儲存陣列群組。

關於這項工作

此作業只會刪除儲存陣列群組。與刪除群組相關聯的儲存陣列仍可透過「管理全部」檢視或與其相關聯的任何其他群組存取。

步驟

1. 從「Manage（管理）」頁面、選取功能表：Manage Groups（管理群組）[Delete storage Array group（刪除儲存陣列群組）]
2. 選取您要刪除的一或多個儲存陣列群組。
3. 按一下*刪除*。

重新命名儲存陣列群組

當目前名稱不再有意義或適用時、您可以變更儲存陣列群組的名稱。

關於這項工作

請謹記這些準則。

- 名稱可以包含字母、數字和特殊字元、例如底線（_）、連字號（-）和井號（#）。如果您選擇任何其他字元、則會出現錯誤訊息。系統會提示您選擇其他名稱。
- 名稱上限為30個字元。名稱中的任何前置和後置空格都會刪除。
- 使用易於理解和記住的獨特、有意義的名稱。
- 避免日後很快失去意義的任意名稱或名稱。

步驟

1. 從主檢視畫面選取*管理*、然後選取您要重新命名的儲存陣列群組。
2. 選取功能表：管理群組[重新命名儲存陣列群組]。
3. 在*群組名稱*欄位中、輸入群組的新名稱。
4. 按一下*重新命名。*

升級

升級中心總覽

從升級中心、您可以管理SANtricity 多個儲存陣列的支援功能、包括作業系統的功能和NVSRAM升級。

升級如何運作？

您可以下載最新的作業系統軟體、然後升級一或多個陣列。

升級工作流程

下列步驟提供執行軟體升級的高層級工作流程。

1. 您可從SANtricity Support網站下載最新的支援作業系統軟體檔案（如需支援頁面中的Unified Manager連結、請參閱）。將檔案儲存在管理主機系統（您在瀏覽器中存取Unified Manager的主機）上、然後解壓縮檔案。
2. 在Unified Manager中、您可以將SANtricity Sesome作業系統軟體檔案和NVSRAM/檔案載入儲存庫（儲存檔案的Web Services Proxy伺服器區域）。您可以從功能表：Upgrade Center[升級SANtricity 支援中心軟體或從Upgrade Center > Manage Software儲存庫]新增檔案。
3. 在檔案載入儲存庫之後、您可以選取要用於升級的檔案。從「Upgrade SANtricity EOSOS」（升級版作業系統）軟體頁面（功能表：Upgrade Center[升級SANtricity 版作業系統軟體]）中、選取SANtricity 「EOSR」軟體檔案和「NVSRAM/」檔案。選取軟體檔案後、相容儲存陣列的清單就會出現在此頁面上。然後選擇要使用新軟體升級的儲存陣列。（您無法選取不相容的陣列。）
4. 接著您可以立即開始軟體傳輸和啟動、也可以選擇稍後將檔案登入以進行啟動。在升級過程中、Unified Manager會執行下列工作：
   a. 對儲存陣列執行健全狀況檢查、以判斷是否存在任何可能妨礙升級完成的情況。如果有任何陣列未通過健全狀況檢查、您可以跳過該特定陣列並繼續升級其他陣列、或是停止整個程序、並疑難排解未通過的陣列。
   b. 將升級檔案傳輸至每個控制器。
   c. 重新啟動控制器、並啟動新SANtricity 的作業系統軟體、一次一個控制器。在啟動期間、現有SANtricity 的作業系統檔案會被新檔案取代。

   > 您也可以指定日後啟動軟體。

立即或分段升級

您可以立即啟動升級、或稍後再進行登入。您可以選擇稍後啟動、原因如下：

- 每天的時間-啟動軟體可能需要很長時間、因此您可能需要等待I/O負載變輕。控制器升級通常需要15到25分鐘才能完成、視I/O負載和快取大小而定。控制器會在啟動期間重新開機並容錯移轉、因此在升級完成之前、效能可能會比平常低。
- 套件類型：在升級其他儲存陣列上的檔案之前、您可能需要在一個儲存陣列上測試新的軟體和韌體。

若要啟動階段式軟體、請前往功能表：Support（升級中心）、然後按一下標示SANtricity 為「停止作業系統控制器軟體升級」的區域中的* Activate*。

健全狀況檢查

健全狀況檢查會在升級程序中執行、但您也可以在開始之前分別執行健全狀況檢查（前往功能表：Upgrade Center[預先升級健全狀況檢查]）。

健全狀況檢查會評估所有儲存系統元件、以確保升級能夠繼續進行。下列情況可能會導致升級無法進行：

- 指派的磁碟機故障
- 使用中的熱備援磁碟機
- 不完整的Volume群組
- 執行專屬作業
- 遺失磁碟區
- 控制器處於非最佳狀態
- 事件記錄事件過多
- 組態資料庫驗證失敗
- 使用舊版的DACStore磁碟機

升級前需要知道哪些資訊？

在升級多個儲存陣列之前、請先檢閱規劃中的重要考量事項。

目前版本

您可以SANtricity 從Unified Manager的「管理」頁面、針對每個探索到的儲存陣列、檢視目前的版本。版本會顯示在SANtricity 「更新OS軟體」欄位中。當您按一SANtricity 下每列的「還原OS版本」時、控制器韌體和NVSRAM資訊 會出現在快顯對話方塊中。

其他需要升級的元件

在升級過程中、您可能還需要升級主機的多重路徑/容錯移轉驅動程式或HBA驅動程式、以便主機能夠正確與控制器互動。

如需相容性資訊，請 "NetApp 互通性對照表"參閱。此外、請參閱適用於您作業系統的快速指南中的程序。Express 指南可從 "E系列與SANtricity 支援技術文件"取得。

雙控制器

如果儲存陣列包含兩個控制器、而且您已安裝多重路徑驅動程式、則儲存陣列可在升級時繼續處理I/O。在升級期間、會發生下列程序：

1. 控制器A將其所有LUN容錯移轉至控制器B
2. 在控制器A上進行升級
3. 控制器A會恢復其LUN及控制器B的所有LUN。
4. 在控制器B上進行升級

升級完成後、您可能需要在控制器之間手動重新分配磁碟區、以確保磁碟區回到正確的擁有控制器。

升級軟體與韌體

執行升級前健全狀況檢查

健全狀況檢查會在升級程序中執行、但您也可以在開始之前分別執行健全狀況檢查。健全狀況檢查會評估儲存陣列的元件、以確保升級能夠繼續進行。

步驟

1. 從主檢視畫面選取*管理*、然後選取功能表：升級中心[升級前狀況檢查]。

   「預先升級健全狀況檢查」對話方塊隨即開啟、並列出所有探索到的儲存系統。

2. 如有需要、請篩選或排序清單中的儲存系統、以便檢視目前未處於最佳狀態的所有系統。
3. 選取要執行健全狀況檢查之儲存系統的核取方塊。
4. 按一下* Start*。

   執行健全狀況檢查時、進度會顯示在對話方塊中。

5. 健全狀況檢查完成後、您可以按一下每列右側的省略符號（...）、以檢視更多資訊並執行其他工作。

> 如果有任何陣列未通過健全狀況檢查、您可以跳過該特定陣列並繼續升級其他陣列、或是停止整個程序、並疑難排解未通過的陣列。

升級**SANtricity** 作業系統

使用最新的軟體和NVSRAM,升級一或多個儲存陣列以確保您擁有所有最新的功能和錯誤修復。控制器NVSRAM-是控制器檔案、可指定控制器的預設設定。

開始之前

- 執行SANtricity 《支援Web服務Proxy與SANtricity Unified Manager的主機系統上有最新的支援功能。
- 您知道現在或之後是否要啟動軟體升級。

  您可以選擇稍後啟動、原因如下：

  - 每天的時間-啟動軟體可能需要很長時間、因此您可能需要等待I/O負載變輕。控制器會在啟動期間容錯移轉、因此在升級完成之前、效能可能會比平常低。
  - 套件類型：在升級其他儲存陣列上的檔案之前、您可能會想要在一個儲存陣列上測試新的作業系統軟體。

系統必須執行 SANtricity OS 11.70.5 、才能升級至 11.8.x 或更新版本。

關於這項工作

```
[NOTE]
====
資料遺失或有損壞儲存陣列的風險-升級期間請勿變更儲存陣列。維持儲存陣列的電力。

====
.步驟
. 如果您的儲存陣列只包含一個控制器、或是未使用多重路徑驅動程式、請停止儲存陣列的
I/O活動、以避免應用程式錯誤。如果您的儲存陣列有兩個控制器、而且安裝了多重路徑驅動程式、則
不需要停止I/O活動。
. 從主檢視畫面選取*管理*、然後選取您要升級的一或多個儲存陣列。
. 選擇功能表：Upgrade Center[升級SANtricity 版作業系統軟體]。
+
此時會出現「Upgrade SANtricity VMware OS軟體」頁面。

. 從 NetApp 支援網站將最新的 SANtricity 作業系統軟體套件下載到您的本機電腦。
+
.. 按一下*「新增檔案至軟體儲存庫」*。
.. 按一下連結以尋找最新的* SANtricity 《支援作業系統下載*》。
.. 按一下*下載最新版本*連結。
.. 請依照其餘指示、將SANtricity 作業系統的支援檔案和NVSRAM/檔案下載到您的本機機器。


+
[NOTE]
====
8.42版及更新版本需要數位簽署的韌體。如果您嘗試下載未簽署的韌體、將會顯示錯誤、且下載會中
止。

====
. 選取您要用來升級控制器的OS軟體檔案和NVSRAM..
+
.. 從* Select a SANtricity Se OS software
file*下拉式清單中、選取您下載到本機電腦的OS檔案。
+
如果有多個檔案可用、檔案會從最新日期排序至最舊日期。

+
[NOTE]
====
軟體儲存庫會列出與Web服務Proxy相關的所有軟體檔案。如果您沒有看到要使用的檔案、可以按一下
「*新增檔案至軟體儲存庫*」連結、瀏覽至您要新增的OS檔案所在的位置。
```

```
====
.. 從*選取一個NVSRAM*下拉式清單中、選取您要使用的控制器檔案。
+
如果有多個檔案、檔案會從最新日期排序至最舊日期。



. 在「相容儲存陣列」表中、檢閱與您所選OS軟體檔案相容的儲存陣列、然後選取您要升級的陣列。
+
**
您在「管理」檢視中選取且與所選韌體檔案相容的儲存陣列、預設會在「相容的儲存陣列」表格中選取。
** 無法以所選韌體檔案更新的儲存陣列無法在相容的儲存陣列表中選取、狀態*不相容
*會顯示此資訊。


. *選用：*若要將軟體檔案傳輸至儲存陣列、但不啟動它們、請選取
*將作業系統軟體傳輸至儲存陣列、將其標示為「已分段」、並於稍後時間啟動*核取方塊。
. 按一下* Start*。
. 視您選擇現在或之後啟動而定、請執行下列其中一項：
+
** 鍵入*
transfit*以確認您要在您選擇要升級的陣列上傳輸建議的作業系統軟體版本、然後按一下*
Transfing*。
+
若要啟動傳輸的軟體、請選取功能表：Upgrade Center[啟動分段作業系統軟體]。

** 鍵入*升級*以確認您要傳輸並啟動所選陣列上建議的作業系統軟體版本、然後按一下*升級*。
+
系統會將軟體檔案傳輸至您選擇要升級的每個儲存陣列、然後啟動重新開機以啟動該檔案。



+
升級作業期間會執行下列動作：

+
**
升級前的狀況檢查會在升級程序中執行。升級前的健全狀況檢查會評估所有儲存陣列元件、以確保升級能夠繼續進行。
** 如果儲存陣列的任何健全狀況檢查失敗、升級就會停止。您可以按一下省略符號（
...）、然後選取*「Save Log*」（儲存記錄
*）以檢閱錯誤。您也可以選擇置換健全狀況檢查錯誤、然後按一下*繼續*繼續升級。
** 您可以在升級前狀況檢查之後取消升級作業。


. *選用：*升級完成後、您可以按一下省略符號（...）、然後選取*「Save Log*」（儲存記錄
```

*）、查看特定儲存陣列的升級項目清單。
+
檔案會以名稱儲存在瀏覽器的「下載」資料夾中 `upgrade_log-<date>.json`。

[[ID137c857e348237d3d2186a28bbbbc7a5]]
= 啟動分段作業系統軟體
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以選擇立即啟動軟體檔案、或等到更方便的時間再啟動。此程序假設您選擇稍後啟動軟體檔案。

.關於這項工作
您可以在不啟動韌體檔案的情況下傳輸韌體檔案。您可以選擇稍後啟動、原因如下：

* *每天的時間*-啟動軟體可能需要很長時間、因此您可能需要等待I/O負載變輕。控制器會在啟動期間重新開機並容錯移轉、因此在升級完成之前、效能可能會比平常低。
* *套件類型*：在升級其他儲存陣列上的檔案之前、您可能需要在一個儲存陣列上測試新的軟體和韌體。

[NOTE]
====
啟動程序之後、您無法停止啟動程序。

====
.步驟
. 從主檢視畫面選取*管理*。如有必要、請按一下「Status（狀態）」欄、在頁面頂端排序所有狀態為「OS Upgrade（waiting activation）（OS升級（等待啟動））」的儲存陣列。
. 選取您要啟動軟體的一或多個儲存陣列、然後選取功能表：升級中心[啟動分段作業系統軟體]。
+
升級作業期間會執行下列動作：

+
**
升級前的狀況檢查會在啟動程序中執行。預先升級的健全狀況檢查會評估所有儲存陣列元件、以確保啟動作業能夠繼續進行。

** 如果儲存陣列的任何健全狀況檢查失敗、啟動就會停止。您可以按一下省略符號（
...）、然後選取*「Save Log*」（儲存記錄
*）以檢閱錯誤。您也可以選擇置換健全狀況檢查錯誤、然後按一下*繼續*繼續啟動。
**
您可以在升級前狀況檢查之後取消啟動作業。成功完成升級前的健全狀況檢查後、就會啟動。啟動所需的時間取決於儲存陣列組態和您要啟動的元件。

. *選用：*啟動完成後、您可以按一下省略符號（...）、然後選取*「Save Log*」（儲存記錄
*）、查看特定儲存陣列的啟動項目清單。
+
檔案會以名稱儲存在瀏覽器的「下載」資料夾中 `activate_log-<date>.json`。

[[IDe80441446d19ab8215d662ec1a032ec5]]
= 管理軟體儲存庫
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
軟體儲存庫會列出與Web服務Proxy相關的所有軟體檔案。

如果您沒有看到想要使用的檔案、可以使用「管理軟體儲存庫」選項、將一個或多個SANtricity支援更新的作業系統檔案匯入正在執行Web服務Proxy和Unified Manager的主機系統。您也可以選擇刪除SANtricity 軟體儲存庫中的一或多個可用的還原OS檔案。

.開始之前
如果您要新增SANtricity
無法使用的作業系統檔案、請確定您的本機系統上有可用的作業系統檔案。

.步驟
. 從主檢視畫面選取*管理*、然後選取功能表：升級中心[管理軟體儲存庫]。
+
此時會出現「管理軟體儲存庫」對話方塊。

. 請執行下列其中一項動作：
+
[cols="25h,~"]
|===

| 選項 | 來這裏吧…

a|
匯入
a|
.. 按一下*匯入*
.. 按一下*瀏覽*、然後瀏覽至您要新增的OS檔案所在的位置。
+
OS 檔案的檔案名稱類似於 `N2800-830000-000.dlp`。

.. 選取您要新增的一或多個OS檔案、然後按一下*匯入*。

a|
刪除
a|
.. 選取您要從軟體儲存庫中移除的一或多個OS檔案。
.. 按一下*刪除*。

|===

.結果
如果您選取匯入、檔案會上傳並驗證。如果您選取刪除、檔案會從軟體儲存庫中移除。

[[IDd072a0d5e2900d2ff74eb79d5185b4ec]]
= 清除分段作業系統軟體
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以移除分段作業系統軟體、以確保稍後不會意外啟動擱置的版本。移除分段作業系統軟體不會影響儲存陣列上目前執行的版本。

.步驟
. 從主檢視畫面選取*管理*、然後選取功能表：升級中心[清除分段作業系統軟體]。
+

「清除分段作業系統軟體」對話方塊隨即開啟、並列出所有已探索到且具有擱置軟體或NVSRAMs的儲存系統。

. 如有需要、請篩選或排序清單中的儲存系統、以便檢視所有已分段軟體的系統。
. 選取您要清除擱置軟體的儲存系統核取方塊。
. 按一下*清除*。
+
此操作的狀態會顯示在對話方塊中。

:leveloffset: -1

:leveloffset: -1

= 鏡射

:leveloffset: +1

[[IDac61fd4577d345cce1faf675f9ee0afb]]
= 鏡射總覽
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
使用鏡射功能、可在本機儲存陣列與遠端儲存陣列之間、非同步或同步複寫資料。

[NOTE]
====
EF600 或 EF300 儲存系統不提供同步鏡射功能。

====

== 什麼是鏡射？

支援非同步和同步的兩種鏡射類型。SANtricity非同步鏡射會根據需求或排程複製資料磁碟區、如此可將資料毀損或遺失所造成的停機時間減至最少或避免。同步鏡射可即時複寫資料磁碟區、確保持續可用。

```
深入瞭解：

* xref:{relative_path}mirroring-overview.html["鏡射的運作方式"]
* xref:{relative_path}mirroring-terminology.html["鏡射術語"]




== 如何設定鏡射？

您可以在Unified Manager中設定非同步或同步鏡射、然後使用System
Manager來管理同步作業。

深入瞭解：

* xref:{relative_path}mirroring-configuration-workflow.html["
鏡射組態工作流程"]
* xref:{relative_path}requirements-for-using-mirroring.html["使用鏡射的需求"]
* xref:{relative_path}create-asynchronous-mirrored-pair-
um.html["建立非同步鏡射配對"]
* xref:{relative_path}create-synchronous-mirrored-pair-
um.html["建立同步鏡射配對"]




= 概念

:leveloffset: +1


[[IDb4ac7e505f530bdcfdcfae1118cf51f6]]
= 鏡射的運作方式
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Unified Manager提供SANtricity
支援鏡射功能的組態選項、可讓系統管理員在兩個儲存陣列之間複寫資料、以保護資料。

[NOTE]
====
EF600 或 EF300 儲存系統不提供同步鏡射功能。
```

====

== 鏡射類型

支援非同步和同步的兩種鏡射類型。SANtricity

非同步鏡射會根據需求或排程複製資料磁碟區、如此可將資料毀損或遺失所造成的停機時間減至最少或避免。非同步鏡射會在特定時間點擷取主要磁碟區的狀態、並只複製自上次擷取映像以來所變更的資料。主站台可立即更新、而次要站台可在頻寬允許的情況下更新。這些資訊會在網路資源可用時快取並於稍後傳送。這類鏡射最適合用於定期程序、例如備份與歸檔。

同步鏡射可即時複寫資料磁碟區、確保持續可用。其目的是在兩個儲存陣列之一發生災難時、提供重要資料的複本、藉此達到零遺失資料的還原點目標（RPO）。複本會在每一刻與正式作業資料完全相同、因為每次寫入主要磁碟區時、都會寫入次要磁碟區。在將次要Volume更新為主要Volume所做的變更之前、主機不會收到寫入成功的確認訊息。這類鏡射是業務持續運作（例如災難恢復）的理想選擇。

== 鏡射類型之間的差異

下表說明兩種鏡射類型之間的主要差異。

[cols="1a,1a,1a"]
|===
| 屬性 | 非同步 | 同步

a|
複寫方法
a|
時間點-鏡像是隨需執行、或是根據使用者定義的排程自動執行。
a|
Continuous（持續）-鏡像會持續執行、從每個主機寫入複製資料。

a|
距離
a|
支援陣列之間的長距離傳輸。一般而言、距離僅受限於網路功能和通道擴充技術。
a|
限制在陣列之間的較短距離。一般而言、距離本機儲存陣列必須在10公里（6.2英哩）內、才能滿足延遲和應用程式效能需求。

```
 a|
通訊方法
 a|
標準IP或光纖通道網路。
 a|
僅限Fibre Channel網路。




 a|
Volume類型
 a|
標準或精簡。
 a|
僅限標準。

|===



[[IDfa58f87306ea5dc4cf55f5882e7329bf]]
= 鏡射組態工作流程
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
您可以在Unified Manager中設定非同步或同步鏡射、然後使用System
Manager來管理同步作業。



== 非同步鏡射工作流程

非同步鏡射涉及下列工作流程：

. 在Unified Manager中執行初始組態：
+
.. 選取本機儲存陣列作為資料傳輸來源。
..
建立或選取現有的鏡射一致性群組、此群組是本機陣列上主要磁碟區的容器、也是遠端陣列上次要磁
碟區的容器。主要和次要磁碟區稱為「鏡射配對」。如果您是第一次建立鏡射一致性群組，請指定您
要執行手動或排程同步。
..
```

從本機儲存陣列選取主要磁碟區、然後決定其保留容量。保留容量是指用於複製作業的實體配置容量。
.. 選取遠端儲存陣列做為傳輸的目的地、次要磁碟區、然後決定其保留容量。
..
開始從主要磁碟區傳輸初始資料至次要磁碟區。視磁碟區大小而定、此初始傳輸可能需要數小時的時間。

. 檢查初始同步的進度：
+
.. 在Unified Manager中、啟動本機陣列的System Manager。
.. 在System Manager中、檢視鏡射作業的狀態。鏡射完成後、鏡射配對的狀態為「最佳」。

. 您也可以在System
Manager中重新排程或手動執行後續資料傳輸。只有新的和變更的區塊會從主要Volume傳輸到次要Volume。
+
[NOTE]
====
由於非同步複寫是定期的、因此系統可以整合變更的區塊並節省網路頻寬。寫入處理量和寫入延遲的影響最小。

====

== 同步鏡射工作流程

同步鏡射涉及下列工作流程：

. 在Unified Manager中執行初始組態：
+
.. 選取本機儲存陣列作為資料傳輸來源。
.. 從本機儲存陣列選取主要磁碟區。
.. 選取遠端儲存陣列做為資料傳輸的目的地、然後選取次要Volume。
.. 選取同步與重新同步優先順序。
..
開始從主要磁碟區傳輸初始資料至次要磁碟區。視磁碟區大小而定、此初始傳輸可能需要數小時的時間。

. 檢查初始同步的進度：
+
.. 在Unified Manager中、啟動本機陣列的System Manager。
.. 在System

Manager中、檢視鏡射作業的狀態。鏡射完成後、鏡射配對的狀態為「最佳」。這兩個陣列嘗試透過正常作業保持同步。只有新的和變更的區塊會從主要Volume傳輸到次要Volume。

. 您也可以在System Manager中變更同步處理設定。
+
[NOTE]
====
由於同步複寫是持續的、因此這兩個站台之間的複寫連結必須提供足夠的頻寬功能。

====

[[ID6ab477a90dc8591c7cca99517483667d]]
= 鏡射術語
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
瞭解鏡射術語如何適用於您的儲存陣列。

[cols="25h,~"]
|===
| 期限 | 說明

a|
本機儲存陣列
a|
本機儲存陣列是您要執行的儲存陣列。

a|
鏡射一致性群組
a|
鏡射一致性群組是一個或多個鏡射配對的容器。對於非同步鏡射作業、您必須建立鏡射一致性群組。群組中的所有鏡射配對都會同時重新同步、因此保留一致的還原點。

同步鏡射不使用鏡射一致性群組。

a|
鏡射配對
a|
鏡射配對由兩個磁碟區組成、一是主要磁碟區、另一是次要磁碟區。

在非同步鏡射中、鏡射配對一律屬於鏡射一致性群組。寫入作業會先執行至主要磁碟區、然後複寫至次要磁碟區。鏡射一致性群組中的每個鏡射配對都會共用相同的同步處理設定。

a|
主要Volume
a|
鏡射配對的主要Volume是要鏡射的來源Volume。

a|
遠端儲存陣列
a|
遠端儲存陣列通常被指定為次要站台、而次要站台通常會在鏡射組態中保留資料的複本。

a|
保留容量
a|
保留容量是指用於任何複製服務作業和儲存物件的實體配置容量。主機無法直接讀取。

這些磁碟區是必要的、因此控制器可以持續儲存必要的資訊、以維持鏡射在作業狀態。其中包含差異記錄和寫入時複製資料等資訊。

a|
次要Volume
a|
鏡射配對的次要Volume通常位於次要站台、並保留資料的複本。

a|
同步
a|
在本機儲存陣列與遠端儲存陣列之間進行初始同步時、便會進行同步。當主要和次要磁碟區在通訊中斷後變成非同步時、也會發生同步。當通訊連結再次運作時、任何未複寫的資料都會同步至次要Volu

me的儲存陣列。

|===

[[ID34d28111eae98edc47050d0e0a771e83]]
= 使用鏡射的需求
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您打算設定鏡射、請謹記下列需求。

== Unified Manager

* Web服務Proxy服務必須正在執行。
* Unified Manager必須透過HTTPS連線在本機主機上執行。
* Unified Manager必須顯示儲存陣列的有效SSL
憑證。您可以接受自我簽署的憑證、或使用Unified
Manager安裝自己的安全性憑證、並瀏覽至功能表：「Certificate [Certificate
Management（憑證管理）」。

== 儲存陣列

[NOTE]
====
EF600 或 EF300 儲存陣列不提供同步鏡射功能。

====
* 您必須有兩個儲存陣列。
* 每個儲存陣列都必須有兩個控制器。
* 這兩個儲存陣列必須在Unified Manager中探索。
* 主陣列和次陣列中的每個控制器都必須設定乙太網路管理連接埠、而且必須連線至您的網路。
* 儲存陣列的韌體版本最低為7.84。（每個作業系統都能執行不同的版本。）
* 您必須知道本機和遠端儲存陣列的密碼。
*
您必須在遠端儲存陣列上擁有足夠的可用容量、才能建立等於或大於您要鏡射之主要磁碟區的次要磁

碟區。
* 具有光纖通道（FC）或iSCSI主機連接埠的控制器支援非同步鏡射、而同步鏡射僅支援具有FC主機連接埠的控制器。

== 連線需求

透過FC介面進行鏡射（非同步或同步）需要下列項目：

* 儲存陣列的每個控制器都會將其編號最高的FC主機連接埠專用於鏡射作業。
* 如果控制器同時具有基礎FC連接埠和主機介面卡（HIC）FC連接埠、則編號最高的連接埠位於HIC上。登入專用連接埠的任何主機都會登出、而且不會接受任何主機登入要求。此連接埠上的I/O要求僅接受參與鏡射作業的控制器。
* 專用鏡射連接埠必須連接至支援目錄服務和名稱服務介面的FC架構環境。特別是、參與鏡射關係的控制器之間、不支援使用FC-AL和點對點作為連線選項。

透過iSCSI介面進行鏡射（僅限非同步）需要下列項目：

* 與FC不同、iSCSI不需要專用連接埠。在iSCSI環境中使用非同步鏡射時、不需要將任何儲存陣列的前端iSCSI連接埠專用於非同步鏡射；這些連接埠會共用以進行非同步鏡射流量和主機對陣列I/O連線。
* 控制器會維護一份遠端儲存系統清單、iSCSI啟動器會嘗試建立工作階段。成功建立iSCSI連線的第一個連接埠、用於與該遠端儲存陣列進行所有後續通訊。如果通訊失敗、則會嘗試使用所有可用的連接埠來建立新的工作階段。
* iSCSI連接埠是以連接埠為基礎、在陣列層級進行設定。組態訊息和資料傳輸的控制器間通訊使用全域設定、包括下列設定：
+
** VLAN：本機和遠端系統必須具有相同的VLAN設定才能進行通訊
** iSCSI接聽連接埠
** 巨型框架
** 乙太網路優先順序

[NOTE]
====
iSCSI互連控制器通訊必須使用主機連線連接埠、而非管理乙太網路連接埠。

====

== 鏡射Volume候選

* 在鏡射配對的主要和次要磁碟區上、RAID層級、快取參數和區段大小可能會有所不同。
+

NOTE: 對於 EF600 和 EF300
控制器、非同步鏡射配對的主要和次要磁碟區必須符合相同的傳輸協定、磁碟匣層級、區段大小、安全類型和 RAID 層級。非合格的非同步鏡射配對不會出現在可用磁碟區清單中。

* 次要Volume必須至少與主要Volume一樣大。
* 一個Volume只能參與一個鏡射關係。
* 對於同步鏡射配對、主要和次要磁碟區必須是標準磁碟區。它們不能是精簡磁碟區或快照磁碟區。
*
對於同步鏡射、特定儲存陣列支援的磁碟區數量有限制。請確定儲存陣列上已設定的磁碟區數量少於支援的限制。當同步鏡射處於作用中狀態時、所建立的兩個保留容量磁碟區會根據磁碟區限制進行計數。
* 對於非同步鏡射、主要磁碟區和次要磁碟區必須具有相同的磁碟機安全功能。
+
** 如果主要Volume支援FIPS、則次要Volume必須具備FIPS功能。
** 如果主要Volume支援FDE、則次要Volume必須具備FDE功能。
** 如果主要磁碟區未使用磁碟機安全性、則次要磁碟區不得使用磁碟機安全性。

== 保留容量

非同步鏡射：

*
主磁碟區和鏡射配對中的次要磁碟區需要保留容量磁碟區、以便記錄寫入資訊、以便從控制器重設和其他暫時性中斷中恢復。
* 由於鏡射配對中的主要Volume和次要
Volume都需要額外的保留容量、因此您必須確保在鏡射關係中、兩個儲存陣列都有可用的可用容量。

同步鏡射：

*
主要磁碟區和次要磁碟區需要保留容量、以便記錄寫入資訊、以便從控制器重設和其他暫時性中斷中恢復。
* 啟動同步鏡射時、會自動建立保留容量磁碟區。由於鏡射配對中的主要Volume和次要
Volume都需要保留容量、因此您必須確保兩個參與同步鏡射關係的儲存陣列都有足夠的可用容量。

== 磁碟機安全功能

*
如果您使用的是具有安全功能的磁碟機、則主要磁碟區和次要磁碟區必須具有相容的安全性設定。此限制並未強制執行、因此您必須自行驗證。
*
如果您使用的是具有安全功能的磁碟機、則主磁碟區和次要磁碟區應該使用相同的磁碟機類型。此限制並未強制執行、因此您必須自行驗證。
* 如果您使用的是Data Assurance（DA）、則主要Volume和次要Volume必須具有相同的DA設定。

:leveloffset: -1

= 設定鏡射

:leveloffset: +1

[[IDb2b31c377f333bfd45dff48bc9608e94]]
= 建立非同步鏡射配對
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
若要設定非同步鏡射、您可以建立鏡射配對、其中包含本機陣列上的主要磁碟區、以及遠端陣列上的次要磁碟區。

.開始之前
建立鏡射配對之前、請先滿足Unified Manager的下列需求：

* Web服務Proxy服務必須正在執行。
* Unified Manager必須透過HTTPS連線在本機主機上執行。
* Unified Manager必須顯示儲存陣列的有效SSL
憑證。您可以接受自我簽署的憑證、或使用Unified
Manager安裝自己的安全性憑證、並瀏覽至功能表：「Certificate [Certificate
Management（憑證管理）」。

此外、請務必滿足下列儲存陣列與磁碟區的需求：

* 每個儲存陣列都必須有兩個控制器。
* 這兩個儲存陣列必須在Unified Manager中探索。
* 主陣列和次陣列中的每個控制器都必須設定乙太網路管理連接埠、而且必須連線至您的網路。
* 儲存陣列的韌體版本最低為7.84。（每個作業系統都能執行不同的版本。）
* 您必須知道本機和遠端儲存陣列的密碼。
*
您必須在遠端儲存陣列上擁有足夠的可用容量、才能建立等於或大於您要鏡射之主要磁碟區的次要磁碟區。
* 您的本機和遠端儲存陣列是透過光纖通道架構或iSCSI介面來連接。
* 您已建立要用於非同步鏡射關係的主要和次要磁碟區。
* 次要Volume必須至少與主要Volume一樣大。

.關於這項工作
建立非同步鏡射配對的程序是多步驟程序。

== 步驟1：建立或選取鏡射一致性群組

在此步驟中、您可以建立新的鏡射一致性群組、或選取現有的群組。鏡射一致性群組是主要和次要磁碟區（鏡射配對）的容器、並為群組中的所有配對指定所需的重新同步方法（手動或自動）。

.步驟
. 從「*管理*」頁面中、選取您要用於來源的本機儲存陣列。
. 選取功能表：「Actions（動作）」[建立非同步鏡射配對]。
+
「建立非同步鏡射配對」精靈隨即開啟。

. 選取現有的鏡射一致性群組或建立新的群組。
+
若要選取現有的群組、請確定已選取*現有的鏡射一致性群組*、然後從表格中選取群組。一致性群組可包含多個鏡射配對。

+
若要建立新群組、請執行下列步驟：

+
.. 選取*新的鏡射一致性群組*、然後按一下*下一步*。
..
輸入最能描述兩個儲存陣列之間鏡射磁碟區資料的唯一名稱。名稱只能由字母、數字和特殊字元組成：底線（_）、破折號（-）和雜湊符號（#）。名稱不得超過30個字元、且不得包含空格。
.. 選取您要與本機儲存陣列建立鏡射關係的遠端儲存陣列。
+
[NOTE]

```
====
如果您的遠端儲存陣列受到密碼保護、系統會提示您輸入密碼。

====
.. 選擇要手動或自動同步鏡射配對：
+
*** *手動*-
選取此選項可手動啟動此群組中所有鏡射配對的同步。請注意、稍後若要執行重新同步、您必須啟動主儲存陣列的System Manager、然後移至功能表：Storage[非同步鏡射鏡射]、從*鏡射一致性群組*索引標籤中選取群組、然後選取功能表：More（更多）[手動重新同步]。
*** *自動*-從上一次更新開始到下一次更新開始、選取所需的時間間隔（*分鐘*、*小時*或*天*）。例如，如果同步處理時間間隔設為 30 分鐘，且同步處理程序從下午 4 ： 00 開始，則下一個程序會在下午 4 ： 30 開始


.. 選取所需的警示設定：
+
*** 針對手動同步、請指定接收警示的臨界值（以剩餘容量百分比定義）。
*** 對於自動同步、您可以設定三種警示方法：
當同步尚未在特定時間長度內完成、遠端陣列上的恢復點資料早於特定時間限制、以及保留容量接近特定臨界值（由剩餘容量百分比定義）時。




. 選擇 *Next* （下一步<<步驟 2 ：選取主要 Volume>>）並轉至。
+
如果您定義了新的鏡射一致性群組、Unified Manager會先在本機儲存陣列上建立鏡射一致性群組、然後在遠端儲存陣列上建立鏡射一致性群組。您可以針對每個陣列啟動System Manager、以檢視及管理鏡射一致性群組。

+
[NOTE]
====
如果Unified Manager成功在本機儲存陣列上建立鏡射一致性群組、但無法在遠端儲存陣列上建立、則會自動從本機儲存陣列刪除鏡射一致性群組。如果Unified Manager嘗試刪除鏡射一致性群組時發生錯誤、您必須手動刪除該群組。

====




== 步驟 2 ：選取主要 Volume

在此步驟中、您可以選取要用於鏡射關係的主要磁碟區、然後分配其保留容量。當您在本機儲存陣列
```

上選取主要磁碟區時、系統會顯示該鏡射配對的所有合格磁碟區清單。任何不符合使用資格的磁碟區都不會顯示在該清單中。

您在本機儲存陣列上新增至鏡射一致性群組的任何磁碟區、都將在鏡射關係中扮演主要角色。

.步驟
. 從合格磁碟區清單中、選取您要用作主要磁碟區的磁碟區、然後按一下*「下一步*」來配置保留容量。
. 從符合資格的候選名單中、選取主要Volume的保留容量。
+
請謹記下列準則：

+
** 保留容量的預設設定是基本 Volume 容量的 20%、通常這種容量就足夠了。如果您變更百分比、請按一下*重新整理候選項目*。
** 所需容量會因主要磁碟區I/O寫入的頻率和大小、以及保留容量所需的時間而有所不同。
** 一般而言、如果存在下列其中一項或兩項條件、請選擇較大的保留容量：
+
*** 您打算長期保留鏡射配對。
*** 由於I/O活動頻繁、一線磁碟區上的資料區塊將會有很大比例改變。使用歷史效能資料或其他作業系統公用程式、協助您判斷主要磁碟區的典型I/O活動。

. 選擇 *Next* （下一步<<步驟 3 ：選取次要 Volume>>）並轉至。

== 步驟 3 ：選取次要 Volume

在此步驟中、您可以選取要用於鏡射關係的次要Volume、然後分配其保留容量。當您在遠端儲存陣列上選取次要磁碟區時、系統會顯示該鏡射配對的所有合格磁碟區清單。任何不符合使用資格的磁碟區都不會顯示在該清單中。

您在遠端儲存陣列上新增至鏡射一致性群組的任何磁碟區、都會在鏡射關係中擔任次要角色。

.步驟
. 從合格磁碟區清單中、選取您要在鏡射配對中作為次要磁碟區的磁碟區、然後按一下*「下一步*」來配置保留容量。
. 從符合資格的候選名單中、選取次要Volume的保留容量。
+
請謹記下列準則：

+

** 保留容量的預設設定是基本 Volume 容量的 20%
、通常這種容量就足夠了。如果您變更百分比、請按一下*重新整理候選項目*。
** 所需容量會因主要磁碟區I/O寫入的頻率和大小、以及保留容量所需的時間而有所不同。
** 一般而言、如果存在下列其中一項或兩項條件、請選擇較大的保留容量：
+
*** 您打算長期保留鏡射配對。
*** 由於
I/O活動頻繁、一線磁碟區上的資料區塊將會有很大比例改變。使用歷史效能資料或其他作業系統公用程式、協助您判斷主要磁碟區的典型I/O活動。

. 選取*完成*以完成非同步鏡射順序。

.結果
Unified Manager會執行下列動作：

* 開始在本機儲存陣列與遠端儲存陣列之間進行初始同步。
* 在本機儲存陣列和遠端儲存陣列上建立鏡射配對的保留容量。

NOTE:
如果要鏡射的磁碟區是精簡磁碟區、則在初始同步期間、只會將已配置的區塊（已配置的容量而非報告的容量）傳輸至次要磁碟區。如此可減少完成初始同步所需傳輸的資料量。

[[ID77938529888670b98ad3b36e31b6b6d5]]
= 建立同步鏡射配對
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
若要設定同步鏡射、您可以建立鏡射配對、其中包含本機陣列上的主要磁碟區、以及遠端陣列上的次要磁碟區。

[NOTE]
====
EF600或EF300儲存系統無法使用此功能。

```
====
.開始之前
建立鏡射配對之前、請先滿足Unified Manager的下列需求：

* Web服務Proxy服務必須正在執行。
* Unified Manager必須透過HTTPS連線在本機主機上執行。
* Unified Manager必須顯示儲存陣列的有效SSL
憑證。您可以接受自我簽署的憑證、或使用Unified
Manager安裝自己的安全性憑證、並瀏覽至功能表：「Certificate [ Certificate
Management（憑證管理）」。


此外、請務必滿足下列儲存陣列與磁碟區的需求：

* 您計畫用於鏡射的兩個儲存陣列都會在Unified Manager中找到。
* 每個儲存陣列都必須有兩個控制器。
* 主陣列和次陣列中的每個控制器都必須設定乙太網路管理連接埠、而且必須連線至您的網路。
* 儲存陣列的韌體版本最低為7.84。（每個作業系統都能執行不同的版本。）
* 您必須知道本機和遠端儲存陣列的密碼。
* 您的本機和遠端儲存陣列是透過光纖通道架構來連接。
* 您已建立要用於同步鏡射關係的主要和次要磁碟區。
* 主Volume必須是標準Volume。它不能是精簡磁碟區或快照磁碟區。
* 次要Volume必須是標準Volume。它不能是精簡磁碟區或快照磁碟區。
* 次要Volume應至少與主要Volume一樣大。


.關於這項工作
建立同步鏡射配對的程序是多步驟程序。



== 步驟 1 ：選取主要 Volume

在此步驟中、您可以選取要用於同步鏡射關係的主要Volume。當您在本機儲存陣列上選取主要磁碟區時、系統會顯示該鏡射配對的所有合格磁碟區清單。任何不符合使用資格的磁碟區都不會顯示在該清單中。您選取的磁碟區在鏡射關係中具有主要角色。

.步驟
. 從「*管理*」頁面中、選取您要用於來源的本機儲存陣列。
. 選取功能表：「Actions（動作）」[建立同步鏡射配對]。
+
「建立同步鏡射配對」精靈隨即開啟。

. 從符合資格的Volume清單中、選取您要做為鏡射中主要Volume的Volume。
. 選擇 *Next* （下一步<<步驟 2 ：選取次要 Volume>>）並轉至。
```

== 步驟 2 ：選取次要 Volume

在此步驟中、您可以選取要用於鏡射關係的次要Volume。當您在遠端儲存陣列上選取次要磁碟區時、系統會顯示該鏡射配對的所有合格磁碟區清單。任何不符合使用資格的磁碟區都不會顯示在該清單中。您選取的磁碟區將在鏡射關係中擔任次要角色。

.步驟
. 選取您要與本機儲存陣列建立鏡射關係的遠端儲存陣列。
+
[NOTE]
====
如果您的遠端儲存陣列受到密碼保護、系統會提示您輸入密碼。

====
+
** 儲存陣列會依其儲存陣列名稱列出。如果您尚未命名儲存陣列、則會將其列為「unnamed（未命名）」。
** 如果您要使用的儲存陣列不在清單中、請確定已在Unified Manager中找到該陣列。

. 從符合資格的Volume清單中、選取您要在鏡射中作為次要Volume的Volume。
+
[NOTE]
====
如果選擇的次要Volume容量大於主要Volume、則可用容量僅限於主要Volume的大小。

====
. 單擊 * 下一步 * 並轉至<<步驟3：選取同步處理設定>>。

== 步驟3：選取同步處理設定

在此步驟中、您可以選取設定、決定在通訊中斷後如何同步處理資料。您可以設定主要磁碟區的控制器擁有者在通訊中斷後、將資料與次要磁碟區重新同步的優先順序。您也必須選取手動或自動重新同步原則。

.步驟
. 使用滑桿列設定同步處理優先順序。
+
同步處理優先順序會決定在通訊中斷之後、與服務I/O要求相比、系統資源有多少用於完成初始同步處理和重新同步作業。

+

此對話方塊上設定的優先順序同時適用於主要Volume和次要Volume。您可以稍後前往System Manager並選取功能表：Storage（同步鏡射）> More（更多）> Edit Settings（編輯設定）、以修改主磁碟區的速率。

+
同步優先順序有五種：

+
** 最低
** 低
** 中
** 高
** 最高
+
如果同步優先順序設定為最低速率、則會優先處理I/O活動、而且重新同步作業需要較長時間。如果同步優先順序設定為最高速率、則重新同步作業會優先處理、但儲存陣列的I/O活動可能會受到影響。

. 選擇是手動或自動重新同步遠端儲存陣列上的鏡射配對。
+
** *手動*（建議選項）-
選取此選項、即可在將通訊還原至鏡射配對後、要求手動恢復同步。此選項提供最佳的資料恢復機會。
** *自動*-選取此選項可在將通訊還原至鏡射配對後自動開始重新同步。
+
若要手動恢復同步、請移至System Manager並選取功能表：Storage[同步鏡射]、在表格中反白顯示鏡射配對、然後在* More *（更多*）下選取* Resumed*（恢復*）。

. 按一下「*完成*」以完成同步鏡射順序。

.結果
啟動鏡射後、系統會執行下列動作：

* 開始在本機儲存陣列與遠端儲存陣列之間進行初始同步。
* 設定同步優先順序和重新同步原則。
* 保留控制器HIC編號最高的連接埠、以進行鏡射資料傳輸。
+
只有鏡射配對中次要Volume的遠端慣用控制器擁有者、才會接受在此連接埠上接收的I/O要求。（允許保留主磁碟區。）

*
建立兩個保留容量磁碟區、每個控制器各一個磁碟區、用於記錄寫入資訊、以便從控制器重設和其他暫時性中斷中恢復。

```
+
每個磁碟區的容量為128個mib。不過、如果將磁碟區放在資源池中、則每個磁碟區將保留4 GiB。



.完成後
移至System Manager並選取功能表：首頁[檢視進行中的作業
]以檢視同步鏡射作業的進度。這項作業可能會耗費大量時間、並可能影響系統效能。



:leveloffset: -1


= 常見問題集

:leveloffset: +1


[[ID4fe54f08bfa73640eb15880dae695c6d]]
= 在建立鏡射一致性群組之前、我需要知道什麼？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
在建立鏡射一致性群組之前、請遵循下列準則。

符合Unified Manager的下列需求：

* Web服務Proxy服務必須正在執行。
* Unified Manager必須透過HTTPS連線在本機主機上執行。
* Unified Manager必須顯示儲存陣列的有效SSL
憑證。您可以接受自我簽署的憑證、或使用Unified
Manager安裝自己的安全性憑證、並瀏覽至功能表：「Certificate [ Certificate
Management（憑證管理）」。


此外、請務必滿足下列儲存陣列需求：

* 這兩個儲存陣列必須在Unified Manager中探索。
* 每個儲存陣列都必須有兩個控制器。
* 主陣列和次陣列中的每個控制器都必須設定乙太網路管理連接埠、而且必須連線至您的網路。
* 儲存陣列的韌體版本最低為7.84。（每個作業系統都能執行不同的版本。）
```

```
* 您必須知道本機和遠端儲存陣列的密碼。
* 您的本機和遠端儲存陣列是透過光纖通道架構或iSCSI介面來連接。


[NOTE]
====
EF600 或 EF300 儲存系統不提供同步鏡射功能。

====




[[IDc1dcc3ee79763954a68b59a0c0be51f3]]
= 建立鏡射配對之前、我需要知道什麼？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
在建立鏡射配對之前、請遵循下列準則。

* 您必須有兩個儲存陣列。
* 每個儲存陣列都必須有兩個控制器。
* 這兩個儲存陣列必須在Unified Manager中探索。
* 主陣列和次陣列中的每個控制器都必須設定乙太網路管理連接埠、而且必須連線至您的網路。
* 儲存陣列的韌體版本最低為7.84。（每個作業系統都能執行不同的版本。）
* 您必須知道本機和遠端儲存陣列的密碼。
*
您必須在遠端儲存陣列上擁有足夠的可用容量、才能建立等於或大於您要鏡射之主要磁碟區的次要磁碟區。
* 具有光纖通道（FC）或iSCSI主機連接埠的控制器支援非同步鏡射、而同步鏡射僅支援具有FC主機連接埠的控制器。


[NOTE]
====
EF600 或 EF300 儲存系統不提供同步鏡射功能。

====




[[ID1f95cc6021411eff34e722d0e0e4e9dc]]
= 為什麼要變更這個百分比？
:allow-uri-read:
```

```
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
保留容量通常是基礎磁碟區的20%、用於非同步鏡射作業。通常這種容量是足夠的。

所需的容量會因寫入基礎磁碟區的頻率和大小、以及您打算使用儲存物件複製服務作業的時間而有所不同。一般而言、如果存在下列其中一項或兩項條件、請為保留容量選擇較大的百分比：

* 如果特定儲存物件的複製服務作業壽命很長、
* 如果由於
I/O活動頻繁、基礎磁碟區上的資料區塊百分比會大幅變動。使用歷史效能資料或其他作業系統公用程式、協助您判斷基礎磁碟區的典型I/O活動。




[[ID41d0a530c03680468f2c6b4c4e5f21b1]]
= 為什麼我會看到多個保留容量的候選對象？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
如果某個集區或Volume群組中有多個Volume符合您為儲存物件選取的容量百分比量、您就會看到多個候選磁碟區。

您可以變更要保留在基礎磁碟區上進行複製服務作業的實體磁碟機空間百分比、以重新整理建議的候選磁碟機清單。根據您的選擇、將會顯示最佳的候選對象。



[[IDe8845d4d64304fa7483ab786100cb4b1]]
= 為什麼我看不到所有磁碟區？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
當您選取鏡射配對的主要Volume時、會有一個清單顯示所有符合資格的Volume。
```

任何不符合使用資格的磁碟區都不會顯示在該清單中。磁碟區可能不符合下列任一原因的資格：

* Volume並非最佳。
* Volume已參與鏡射關係。
*
對於同步鏡射、鏡射配對中的主要和次要磁碟區必須是標準磁碟區。它們不能是精簡磁碟區或快照磁碟區。
* 對於非同步鏡射、精簡磁碟區必須啟用自動擴充。

NOTE: 對於 EF600 和 EF300
控制器、非同步鏡射配對的主要和次要磁碟區必須符合相同的傳輸協定、磁碟匣層級、區段大小、安全類型和 RAID 層級。非合格的非同步鏡射配對不會出現在可用磁碟區清單中。

[[ID0d93a38863b85cbf506ed648de3b3c1a]]
= 為什麼我看不到遠端儲存陣列上的所有磁碟區？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
當您在遠端儲存陣列上選取次要Volume時、清單會顯示該鏡射配對的所有適用磁碟區。

任何不符合使用資格的磁碟區、都不會顯示在該清單中。Volume可能不符合下列任何理由：

* 此磁碟區為非標準磁碟區、例如快照磁碟區。
* Volume並非最佳。
* Volume已參與鏡射關係。
* 對於非同步鏡射、主要磁碟區與次要磁碟區之間的精簡磁碟區屬性不相符。
* 如果您使用的是Data Assurance（DA）、則主要Volume和次要Volume必須具有相同的DA設定。
+
** 如果主磁碟區已啟用DA、則必須啟用次要磁碟區DA。
** 如果主要Volume未啟用DA、則次要Volume不得啟用DA。

* 對於非同步鏡射、主要磁碟區和次要磁碟區必須具有相同的磁碟機安全功能。
+
** 如果主要Volume支援FIPS、則次要Volume必須具備FIPS功能。
** 如果主要Volume支援FDE、則次要Volume必須具備FDE功能。
** 如果主要磁碟區未使用磁碟機安全性、則次要磁碟區不得使用磁碟機安全性。

[[ID15b3fed24e74dd16c935b68ef96c1d94]]
= 同步處理優先順序對同步處理速率有何影響？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
同步處理優先順序會定義與系統效能相關的同步處理活動所需的處理時間。

主磁碟區的控制器擁有者會在背景執行此作業。同時、控制器擁有者會處理本機I/O寫入主要磁碟區的作業、並將相關的遠端寫入作業處理至次要磁碟區。由於重新同步會將控制器處理資源從I/O活動中轉移、因此重新同步可能會影響主機應用程式的效能。

請記住這些準則、以協助您判斷同步處理優先順序可能需要多久、以及同步處理優先順序如何影響系統效能。

這些優先率可供選擇：

* 最低
* 低
* 中
* 高
* 最高

最低的優先順序率可支援系統效能、但重新同步需要較長時間。最高優先順序率支援重新同步、但系統效能可能會受損。

這些準則大致上與優先順序的差異大致相同。

[cols="45h,~"]
|===
| 完整同步的優先順序率 | 相較於最高同步率、所耗用的時間

a|
最低
a|
最高優先率約為八倍。

```
 a|
低
 a|
最高優先率約為六倍。




 a|
中
 a|
以最高優先率計算、約為三倍半。




 a|
高
 a|
以最高優先率計算、長度約為兩倍。

|===
Volume大小和主機I/O速率負載會影響同步時間比較。



[[ID69d8d786bcccc906f15dab2c10e7a6cf]]
= 為什麼建議使用手動同步原則？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
建議手動重新同步、因為它可讓您以最佳的方式來管理重新同步程序、以提供最佳的資料恢復機會。

如果您使用自動重新同步原則、且在重新同步期間發生間歇性通訊問題、則次要磁碟區上的資料可能會暫時毀損。重新同步完成後、資料將會修正。



:leveloffset: -1


:leveloffset: -1
```

```
= 憑證

:leveloffset: +1


[[ID058742f86aea26d2d3eb3507517476ab]]
= 憑證總覽
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
「憑證管理」可讓您建立憑證簽署要求（CSR）、匯入憑證、以及管理現有的憑證。



== 什麼是憑證？

_Certificates_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。憑證有兩種類型：_簽署的憑證_由憑證授權單位（CA）驗證、_自我簽署的憑證_則由實體擁有者（而非第三方）驗證。

深入瞭解：

* xref:{relative_path}how-certificates-work-unified.html["憑證的運作方式"]
* xref:{relative_path}certificate-terminology-unified.html["憑證術語"]




== 如何設定憑證？

從「憑證管理」中、您可以設定裝載Unified
Manager的管理站台憑證、也可以匯入陣列中控制器的憑證。

深入瞭解：

* xref:{relative_path}use-ca-signed-certificate-um.html["管理系統使用
CA簽署的憑證"]
* xref:{relative_path}import-array-certificates-unified.html["
匯入陣列的憑證"]
```

```
= 概念

:leveloffset: +1


[[ID73f4ce5f297aa55a5e9fc5dbc71a5a04]]
= 憑證的運作方式
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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。

[NOTE]
====
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。




[[IDacd880f47dd7201d1227de97f78e5cdb]]
= 憑證術語
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
下列條款適用於憑證管理。

[cols="25h,~"]
|===
| 期限 | 說明

a|
CA
a|
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。

a|
CSR
a|
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。

a|
憑證
a|
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。

a|
憑證鏈結
a|
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。

a|
中介憑證
a|
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。

a|
Keystore
a|
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。

a|
根憑證
a|
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。

a|
簽署的憑證
a|
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」。

a|
自我簽署的憑證
a|
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。

a|
伺服器憑證
a|
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。

a|

```
信任存放區
 a|
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。

|===




:leveloffset: -1


[[ID86b4c2326665e9914f6276def3b06b54]]
= 管理系統使用CA簽署的憑證
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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簽署的憑證是三個步驟的程序。



== 步驟1：完成CSR檔案

您必須先產生憑證簽署要求（CSR）檔案、以識別您的組織和安裝Web服務Proxy和Unified
Manager的主機系統。

[NOTE]
====
或者，您也可以使用 Openssl 等工具產生 CSR 檔案<<步驟2：提交CSR檔案>>，然後跳至。

====
.步驟
. 選擇*憑證管理*。
. 從「管理」索引標籤中、選取*完整的csr*。
. 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。

. 輸入下列有關安裝Web服務Proxy的主機系統資訊：
+
** *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://.DNS名稱不能以萬用字元開頭。
** *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。DNS名稱不能以萬用字元開頭。

. 確認主機資訊正確無誤。如果不是、當您嘗試匯入CA時、從CA傳回的憑證將會失敗。
. 單擊*完成*。
. 前往 <<步驟2：提交CSR檔案>>。

== 步驟2：提交CSR檔案

建立憑證簽署要求（CSR）檔案之後、您會將其傳送至憑證授權單位（CA）、以接收裝載Unified Manager和Web Services Proxy之系統的簽署管理憑證。

NOTE: E系列系統要求簽署的憑證使用PEm格式（Base64 Ascii
編碼）、其中包含下列檔案類型：.pem、.crt、.cer或.key。

.步驟
. 找到下載的CSR檔案。
+
下載的資料夾位置取決於您的瀏覽器。

. 將CSR檔案提交給CA（例如、Verisign或Digiting）、並以PEV格式要求簽署的憑證。
+
[CAUTION]
====
* 將 CSR 檔案提交給 CA 之後，請勿重新產生其他 CSR 檔案。 *每當您產生
CSR時、系統都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系統的Keystore中。當您收到簽署的憑證並匯入時、系統會確保私密金鑰和公開金鑰都是原始配對。如果金鑰不符、簽署的憑證將無法運作、您必須向CA要求新的憑證。

```
====
. 當 CA 傳回簽署的憑證時，請移至<<步驟 3 ：匯入管理憑證>>。




== 步驟 3 ：匯入管理憑證

從憑證授權單位（CA）收到簽署的憑證後、請將憑證匯入安裝Web服務Proxy和Unified
Manager介面的主機系統。

.開始之前
* 您已從CA收到簽署的憑證。這些檔案包括根憑證、一或多個中繼憑證和伺服器憑證。
* 如果CA提供鏈結的憑證檔案（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，然後選取功能表：所有工作 [ 匯出 ]
）。建議使用Base 64編碼。匯出完成後、會針對鏈中的每個憑證檔案顯示一個CER.檔案。
* 您已將憑證檔案複製到執行Web服務Proxy的主機系統。


.步驟
. 選擇*憑證管理*。
. 從「管理」索引標籤中、選取*匯入*。
+
隨即開啟一個對話方塊、用於匯入憑證檔案。

. 按一下*瀏覽*以先選取根和中繼憑證檔案、然後選取伺服器憑證。如果您是從外部工具產生
CSR、也必須匯入與CSR一起建立的私密金鑰檔案。
+
檔案名稱會顯示在對話方塊中。

. 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。



[[ID6ac6868476449b1265198668bb5f9a8a]]
= 重設管理憑證
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
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
此工作會從安裝Web服務Proxy和Unified
Manager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
. 選取 * 設定 > 憑證 * 。
. 選擇 *Array Management* 選項卡，然後選擇 *Reset* 。
+
隨即開啟「確認重設管理憑證」對話方塊。

. 在欄位中輸入 `reset`，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。



= 使用陣列憑證

:leveloffset: +1


[[ID8353dfa5b8bcc278a21f94194bd23ac3]]
= 匯入陣列的憑證
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

如有必要、您可以匯入儲存陣列的憑證、以便透過裝載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System Manager匯入儲存陣列控制器的憑證。

.步驟
. 選擇*憑證管理*。
. 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。

. 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。

. 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。

[[IDa7f4bdf278fedce679a7307401c68cfd]]
= 刪除信任的憑證
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[CAUTION]
====
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

. 選擇*憑證管理*。
. 選取*信任的*索引標籤。
. 在表格中選取一或多個憑證、然後按一下*刪除*。
+
[NOTE]
====
*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。

. 確認刪除、然後按一下*刪除*。
+
該憑證會從表格中移除。

[[IDe25371947507ef7fb1c8c73bf32eca61]]
= 解決不受信任的憑證
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
當儲存陣列嘗試建立與Unified Manager的安全連線、但連線無法確認為安全時、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
. 選擇*憑證管理*。
. 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。

. 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。

. 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。

```
:leveloffset: -1
```

= 管理憑證

```
:leveloffset: +1
```

```
[[IDd697eb2b92ea0e60782bf1d04927d1bf]]
= 檢視憑證
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```
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
. 選擇*憑證管理*。
. 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。

. 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*。

[[IDa4f9704ada4bdf80b9f2037e5ac0eb89]]
= 匯出憑證
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. 選擇*憑證管理*。
. 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。

. 從頁面選取憑證、然後按一下列結尾的省略符號。

```
. 按一下「*匯出*」、然後儲存憑證檔案。
. 在憑證檢視器應用程式中開啟檔案。




:leveloffset: -1


:leveloffset: -1


= 存取管理

:leveloffset: +1


[[ID22779b7cbc8e824f8b650029c75b0f06]]
= 存取管理總覽
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
存取管理是一種在Unified Manager中設定使用者驗證的方法。



== 有哪些驗證方法可用？

提供下列驗證方法：

* *本機使用者角色*-驗證是透過
RBAC（角色型存取控制）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。
* *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。
* * SAML *-驗證是透過使用SAML 2.0的身分識別供應商（IDP）來管理。


深入瞭解：

* xref:{relative_path}how-access-management-works-
unified.html["存取管理的運作方式"]
* xref:{relative_path}access-management-terminology-
```

```
unified.html["存取管理術語"]
* xref:{relative_path}permissions-for-mapped-roles-
unified.html["對應角色的權限"]
* xref:{relative_path}access-management-with-saml.html["SAML"]




== 如何設定存取管理？

此功能已預先設定為使用本機使用者角色。SANtricity如果您想要使用LDAP、可以在「存取管理」頁面下進行設定。

深入瞭解：

* xref:{relative_path}access-management-with-local-user-roles-
unified.html["具有本機使用者角色的存取管理"]
* xref:{relative_path}access-management-with-directory-services-
unified.html["使用目錄服務進行存取管理"]
* xref:{relative_path}configure-saml.html["設定SAML 功能"]




= 概念

:leveloffset: +1


[[IDf05e14e11e96f14f596e76e6691e0feb]]
= 存取管理的運作方式
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
使用Access Management在Unified Manager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：

. 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。
```

+
[NOTE]
====
首次登入時，系統會自動顯示使用者名稱 `admin`，且無法變更。
`admin`使用者可完全存取系統中的所有功能。首次登入時必須設定密碼。

====
.
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。
. 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。
** * 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。

. 系統管理員可為使用者提供Unified Manager的登入認證。
. 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。

```
[[ID04c6312e6b632555978701515f512509]]
= 存取管理術語
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
瞭解存取管理條款如何適用於Unified Manager。

[cols="25h,~"]
|===
| 期限 | 說明


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




 a|
連結
 a|
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。




 a|
CA
 a|
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。




 a|
憑證
 a|
```

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。

a|
LDAP
a|
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。

a|
RBAC
a|
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。

a|
SAML
a|
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、可用於識別聲明、驗證及授權。

a|
SSO
a|
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。

a|
Web服務Proxy
a|
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。

|===

```
[[IDae2934e2969bc9e20cc5ae342f1be4a0]]
= 對應角色的權限
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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Unified Manager工作的權限。

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。



[[ID2fb57817fc2daf5c9a1f5e07e585ac22]]
= 具有本機使用者角色的存取管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
系統管理員可以使用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：

. 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。
+
```

```
[NOTE]
====
 `admin`使用者可完全存取系統中的所有功能。

====
. 系統管理員會檢閱預先定義且無法修改的使用者設定檔。
. 系統管理員也可以為每個使用者設定檔指派新密碼。
. 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。




[[ID7cd78a6982d53aa3645f52a647141339]]
= 使用目錄服務進行存取管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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：

. 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。
+
[NOTE]
====
 `admin`使用者可完全存取系統中的所有功能。
```

```
====
. 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。
. 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。
.
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。
. 系統管理員會測試LDAP伺服器與Web服務Proxy之間的連線。
. 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。




[[IDfd0bdf4494d5291d1758901dca6101a5]]
= 使用SAML進行存取管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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：

. 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 。
+
```

```
[NOTE]
====
 `admin`使用者可完全存取 System Manager 中的所有功能。

====
. 系統管理員會移至「存取管理」下的「* SAML」索引標籤。
. 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、管理員會從 IDP 系統下載 IDP 中繼資料檔案、然後使用 Unified Manager
將檔案上傳至儲存陣列。
. 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、管理員可使用 Unified Manager
匯出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 系統將中繼資料檔案匯入 IDP
。
+
[NOTE]
====
系統管理員也應確保IDP支援在驗證時傳回名稱ID的功能。

====
. 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。為達此目的、管理員使用
Unified Manager 來建立對應。
. 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。
+
[CAUTION]
====
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。

====
. 從 Unified Manager 、系統管理員可為儲存陣列啟用 SAML 。
. 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、使用者無法從舊版 Storage Manager 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

:leveloffset: -1

= 使用本機使用者角色

:leveloffset: +1

[[ID9649c80a401e2d8e81eb7f01a253c876]]
= 檢視本機使用者角色
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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Unified Manager的Web Services Proxy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
. 選擇*存取管理*。
. 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。

[[ID34331febeebd4e983c558dad7335955e]]
= 變更本機使用者設定檔的密碼
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. 選擇*存取管理*。
. 選取*本機使用者角色*索引標籤。

. 從表格中選取使用者。
+
「變更密碼」按鈕隨即可用。

. 選擇*變更密碼*。
+
「變更密碼」對話方塊隨即開啟。

.
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。
. 在兩個欄位中輸入所選使用者的新密碼。
. 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。

[[IDba0680bd3d576abd67099fdf2e7e42d4]]
= 變更本機使用者密碼設定
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. 選擇*存取管理*。
. 選取*本機使用者角色*索引標籤。

. 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。

. 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。

. 按一下「 * 儲存 * 」。

:leveloffset: -1

= 使用目錄服務

:leveloffset: +1

[[ID6549b9d4f5b5b2bba1c57bd32ad264b5]]
= 新增目錄伺服器
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
若要設定存取管理驗證、您需要在LDAP伺服器和執行Unified Manager Web Services Proxy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
. 選擇*存取管理*。
. 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。

. 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
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 說明

a|
組態設定

a|
網域
a|
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。

a|
伺服器URL
a|
以的形式輸入用於訪問 LDAP 服務器的 URL `ldap[s]://*host*:*port*` 。

a|
上傳憑證（選用）
a|

NOTE: 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。

a|
連結帳戶（選用）
a|
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，如果綁定用戶稱爲 "bindacct" ，則可以輸入一個值，例如 `CN=bindacct,CN=Users,DC=cpoc,DC=local`。

a|
連結密碼（選用）
a|

NOTE: 當您輸入連結帳戶時、會顯示此欄位。

輸入綁定帳戶的密碼。

a|
在新增之前先測試伺服器連線
a|
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。

a|
權限設定

a|
搜尋基礎DN
a|
輸入 LDAP 內容以搜尋使用者，通常是以的形式 `CN=Users, DC=cpoc, DC=local`。

```
 a|
使用者名稱屬性
 a|
輸入繫結至使用者ID以進行驗證的屬性。例如 `sAMAccountName`：。




 a|
群組屬性
 a|
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
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 說明



 a|
*對應*




 a|
群組DN
 a|
指定要對應之LDAP使用者群組的群組辨別名稱（DN）。支援規則運算式。如果這些特殊的規則運算式字元不是一般運算式模式的一部分、則必須以反斜槓（\）轉義：\.[]{}()<<*+-=!?^$|




 a|
角色
 a|
按一下欄位、然後選取要對應至群組DN的其中一個本機使用者角色。您必須個別選取要納入此群組的每個角色。監控角色必須與其他角色搭配使用、才能登入SANtricity 到NetApp Unified Manager。對應的角色包括下列權限：

** *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。

|===
====
+

NOTE: 所有使用者（包括系統管理員）都必須具備「監控」角色。

. 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。
. 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。

[[ID98252796f50d7d91525484cc318319c8]]
= 編輯目錄伺服器設定和角色對應
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. 選擇*存取管理*。
. 選取*目錄服務*索引標籤。
. 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。
. 選取*檢視/編輯設定*。
+
此時將打開Directory Server Settings（目錄服務器設置）對話框。

. 在*伺服器設定*索引標籤中、變更所需的設定。
+
.欄位詳細資料
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 說明

a|
組態設定

a|
網域
a|
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。

a|
伺服器URL
a|
以形式存取 LDAP 伺服器的 URL `ldap[s]://host:port` 。

a|
連結帳戶（選用）
a|
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。

a|
連結密碼（選用）
a|
綁定帳戶的密碼。（輸入連結帳戶時、會顯示此欄位。）

a|
儲存前先測試伺服器連線

a|
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。

a|
權限設定

a|
搜尋基礎DN
a|
要搜尋使用者的 LDAP 內容，通常為 `CN=Users, DC=cpoc, DC=local`。

a|
使用者名稱屬性
a|
繫結至使用者ID以進行驗證的屬性。例如
`sAMAccountName`：。

a|
群組屬性
a|
使用者上的群組屬性清單、用於群組對角色對應。例如
`memberOf, managedObjects`：。

|===
====
. 在*角色對應*索引標籤中、變更所需的對應。
+
.欄位詳細資料
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 說明

a|
對應

```
 a|
群組DN
 a|
要對應之LDAP使用者群組的網域名稱。支援規則運算式。如果這些特殊的規則運算式字元不是規則運算式模式的一部分、則必須以反斜槓（\）轉義：

\.[]{}()<>*+-=!?^$|




 a|
角色
 a|
要對應至群組DN的角色。您必須個別選取要納入此群組的每個角色。監控角色必須與其他角色搭配使用、才能登入SANtricity 到NetApp Unified Manager。這些角色包括：

** *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。



|===
====
+

NOTE: 所有使用者（包括系統管理員）都必須具備「監控」角色。

. 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。
. 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。



[[ID07bfcd615f210d01dd3f0de68d79a1c9]]
= 移除目錄伺服器
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
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
. 選擇*存取管理*。
. 選取*目錄服務*索引標籤。
. 從清單中選取您要刪除的目錄伺服器。
. 按一下「*移除*」。
+
此時會開啟「移除目錄伺服器」對話方塊。

. 在欄位中輸入 `remove`，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。

:leveloffset: -1

= 使用SAML

:leveloffset: +1

[[ID18379bca43a8ed888a5b2aadc92d3090]]
= 設定SAML 功能
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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。
* 您必須知道儲存陣列中控制器的 IP 位址或網域名稱。
* 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。
* 管理員已確保 IDP 伺服器和控制器時鐘同步（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、並可在用於存取 Unified Manager
的本機系統上使用。

.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。

[NOTE]
====
* 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
Unified 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。

====
[CAUTION]
====
* 編輯與停用。 *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 Unified 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。

.步驟
. 選取功能表：設定[Access Management（存取管理）]。
. 選取* SAML *索引標籤。
+
頁面會顯示組態步驟的總覽。

. 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。

. 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。

. 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。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
. 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。

. 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。
+
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。

. 在本機系統中、找出您匯出的 XML 格式服務供應商中繼資料檔案。
. 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 Unified Manager 的授權和存取權、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 Unified Manager 。
* 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
. 按一下 * 對應 Unified Manager* 角色的連結。
+
此時會開啟「角色對應」對話方塊。

. 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
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 說明

a|
對應

a|
使用者屬性
a|
指定要對應之SAML群組的屬性（例如「memberof」）。

a|
屬性值
a|
指定要對應群組的屬性值。支援規則運算式。(`\`如果這些特殊的規則運算式字元不是規則運算式模式的一部分，則必須以反斜線轉義）： \.[]{}()<>*+-=!?^$|

a|
角色
a|
按一下欄位、然後選取要對應至屬性的其中一個儲存陣列角色。您必須個別選取要納入的每個角色。必須搭配其他角色使用「監控」角色、才能登入 Unified Manager
。至少一個群組也需要安全管理員角色。

對應的角色包括下列權限：

** *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。

|===
====
+
[NOTE]
====
所有使用者（包括系統管理員）都必須具備「監控」角色。如果沒有「監控」角色、 Unified Manager 將無法為任何使用者正確運作。

====
. 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。
+
[NOTE]
====
啟用SAML之後、即可修改角色對應。

====
. 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 Unified Manager 。
* 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
. 選取「*測試SSO登入*」連結。
+
隨即開啟對話方塊、供您輸入SSO認證。

. 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。

. 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。

.開始之前
* IDP 中繼資料檔案會匯入 Unified Manager 。
* 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。

[CAUTION]
====
* 編輯與停用。 *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
. 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。

. 鍵入 `enable`，然後單擊 *Enable* 。
. 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。

[[ID031a087d890fab7d97018ab5084b9c21]]

```
= 變更SAML角色對應
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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
. 選取功能表：設定[Access Management（存取管理）]。
. 選取* SAML *索引標籤。
. 選擇*角色對應*。
+
此時會開啟「角色對應」對話方塊。

. 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。
+
[CAUTION]
====
請注意、啟用 SAML 時、您不會移除權限、否則您將無法存取 Unified Manager 。

====
+
.欄位詳細資料
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 說明


 a|
*對應*



 a|
```

使用者屬性
a|
指定要對應之SAML群組的屬性（例如「memberof」）。

a|
屬性值
a|
指定要對應群組的屬性值。

a|
角色
a|
按一下欄位、然後選取要對應至屬性的其中一個儲存陣列角色。您必須個別選取要納入此群組的每個角色。必須搭配其他角色使用「監控」角色、才能登入 Unified Manager
。必須將安全管理員角色指派給至少一個群組。對應的角色包括下列權限：

** *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。

|===
====
+

NOTE: 所有使用者（包括系統管理員）都必須具備「監控」角色。如果沒有「監控」角色、
Unified Manager 將無法為任何使用者正確運作。

. （可選）單擊* Add another mapping（添加另一個映射）*以輸入更多的組對角色映射。
. 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。

[[IDd9ce7d9496d55c0d7edda976ad9e72a9]]

```
= 匯出SAML服務供應商檔案
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
如有必要、您可以匯出儲存陣列的服務供應商中繼資料、並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。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
. 選取功能表：設定[Access Management（存取管理）]。
. 選取* SAML *索引標籤。
. 選取*匯出*。
+
「匯出服務供應商檔案」對話方塊隨即開啟。

. 按一下 * 匯出 * 將中繼資料檔案儲存至您的本機系統。
+
[NOTE]
====
網域名稱欄位為唯讀。

====
+
記下檔案的儲存位置。

. 在本機系統中、找出您匯出的 XML 格式服務供應商中繼資料檔案。
. 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、也可以手動輸入控制器資訊。
. 按一下 * 關閉 * 。
```

```
:leveloffset: -1


= 常見問題集

:leveloffset: +1


[[ID79ddbccdb49c40946f4da519bab9d2e0]]
= 為什麼我無法登入？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
如果您在嘗試登入時收到錯誤訊息、請檢閱這些可能的原因。

下列其中一項原因可能導致登入錯誤：

* 您輸入的使用者名稱或密碼不正確。
* 您的權限不足。
* 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。
* 已啟用SAML驗證。重新整理瀏覽器以登入。




[[ID746ef2310f8799b59650f4bc686a1928]]
= 新增目錄伺服器之前、我需要知道什麼？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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。
```

```
[[ID60af53246510ad470218468fb8b0909e]]
= 我需要知道哪些關於對應至儲存陣列角色的資訊？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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。


[NOTE]
====
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。




== 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。
* 您知道要對應群組的屬性值。支援規則運算式。
(`\`如果這些特殊的正則表達式字符不是正則表達式模式的一部分，則必須使用反斜槓進行轉義）：
+
[listing]
----
\.[]{}()<>*+-=!?^$|
----
* 所有使用者（包括系統管理員）都必須具備「監控」角色。如果沒有「監控」角色、 Unified
```

```
Manager 將無法為任何使用者正確運作。




[[ID7c092d09d706dcb7ea78869853150c1e]]
= 在設定及啟用SAML之前、我需要知道哪些資訊？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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SA
ML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。
* 管理員已確保 IDP 伺服器和控制器時鐘同步（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、並可在用於存取 Unified Manager
的本機系統上使用。
* 您知道儲存陣列中控制器的 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 
```

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

<<<
版權資訊

Copyright © 2025 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 保留隨時變更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

link:http://www.netapp.com/TM[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。