存取管理

SANtricity 11.5

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/e-series-santricity-115/sm-settings/how-access-management-works.html on February 12, 2024. Always check docs.netapp.com for the latest.

目錄

存取管理

概念

存取管理的運作方式

存取管理是SANtricity 一種在《Sytricity System Manager》中建立使用者驗證的方法。驗證需要使用者以指派的認證登入這些系統。

存取管理組態和使用者驗證的運作方式如下：

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

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

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

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

   登入期間、系統會執行下列背景工作：

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

System Manager中可用的工作

存取工作取決於使用者指派的角色、包括下列項目：

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

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

使用者存取**SANtricity** 功能

設定本機使用者角色和目錄服務時、使用者必須先輸入認證、才能在「企業管理」視窗（EMW）中執行下列任一功能：

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

如果已針對儲存陣列設定SAML、使用者將無法使用EMW來探索或管理該陣列的儲存設備。

存取管理術語

瞭解存取管理條款如何適用於您的儲存陣列。

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

期限	說明
IDP	身分識別提供者（IDP）是外部系統、用於向使用者要求認證、以及判斷該使用者是否已成功驗證。IDP可設定為提供多因素驗證、並使用任何使用者資料庫、例如Active Directory。您的安全團隊負責維護IDP。
LDAP	輕量型目錄存取傳輸協定（LDAP）是用於存取及維護分散式目錄資訊服務的應用程式傳輸協定。此傳輸協定可讓許多不同的應用程式和服務連線至LDAP伺服器、以驗證使用者。
RBAC	角色型存取控制（RBAC）是一種根據個別使用者角色來管理電腦或網路資源存取的方法。RBAC控制會在儲存陣列上強制執行、並包含預先定義的角色。
SAML	安全聲明標記語言（SAML）是兩個實體之間驗證與授權的XML型標準。SAML允許多因素驗證、使用者必須提供兩個或多個項目來證明身分（例如密碼和指紋）。儲存陣列的內嵌SAML功能符合SAML2.0標準、可用於身分識別聲明、驗證及授權。
SP	服務供應商（SP）是控制使用者驗證與存取的系統。使用SAML設定存取管理時、儲存陣列會做為服務供應商、以要求身分識別供應商進行驗證。
SSO	單一登入（SSO）是一種驗證服務、可讓一組登入認證資料存取多個應用程式。

對應角色的權限

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

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

這些角色可讓使用者存取工作、如下所示：

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

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

具有本機使用者角色的存取管理

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

組態工作流程

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

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

   「admin」使用者可完整存取系統中的所有功能。

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

管理

只使用本機使用者角色進行驗證時、系統管理員可以執行下列管理工作：

- 變更密碼。
- 設定密碼的最小長度。
- 允許使用者不使用密碼登入。

使用目錄服務進行存取管理

對於存取管理、系統管理員可以使用LDAP（輕量型目錄存取傳輸協定）伺服器和目錄服務、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」權限的使用者設定檔登入到「功能不全系統管理程式」。

   「admin」使用者可完整存取系統中的所有功能。

2. 系統管理員會輸入LDAP伺服器的組態設定。設定包括網域名稱、URL及連結帳戶資訊。
3. 如果LDAP伺服器使用安全傳輸協定（LDAPS）、則系統管理員會上傳憑證授權單位（CA）憑證鏈結、以便在LDAP伺服器與儲存陣列之間進行驗證。
4. 建立伺服器連線後、系統管理員會將使用者群組對應至儲存陣列的角色。這些角色已預先定義、無法修改。
5. 系統管理員會測試LDAP伺服器與儲存陣列之間的連線。
6. 使用者使用指派的LDAP/Directory Services認證登入系統。

管理

使用目錄服務進行驗證時、系統管理員可以執行下列管理工作：

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

使用SAML進行存取管理

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

組態工作流程

SAML組態運作方式如下：

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

   「admin」使用者可以完整存取System Manager中的所有功能。

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

   系統管理員也應確保IDP支援在驗證時傳回名稱ID的功能。

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

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

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

管理

使用SAML進行驗證時、系統管理員可以執行下列管理工作：

- 修改或建立新的角色對應

- 匯出服務供應商檔案

存取限制

啟用SAML時、下列用戶端無法存取儲存陣列服務和資源：

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

使用方法

檢視本機使用者角色

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

開始之前

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

關於這項工作

無法變更使用者設定檔和對應。只能修改密碼。

步驟

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

   下表顯示使用者設定檔：

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

變更密碼

您可以在「存取管理」中變更每個使用者設定檔的使用者密碼。

開始之前

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

關於這項工作

選擇密碼時請謹記以下準則：

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

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

步驟

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

   「變更密碼」按鈕隨即可用。

4. 選擇*變更密碼*。

   「變更密碼」對話方塊隨即開啟。

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

結果

如果使用者目前登入、密碼變更會導致使用者的作用中工作階段終止。

變更本機使用者密碼設定

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

開始之前

- 您必須以本機系統管理員的身分登入、其中包含root系統管理權限。

關於這項工作

設定本機使用者密碼的最小長度時、請謹記下列準則：

- 設定變更不會影響現有的本機使用者密碼。

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

步驟

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

   「本機使用者密碼設定」對話方塊隨即開啟。

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

     任何新的本機使用者密碼必須符合或超過目前設定。

5. 按一下「 * 儲存 * 」。

新增目錄伺服器

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

開始之前

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

關於這項工作

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

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

步驟

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

「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」、則您可以輸入一個值、例如「CN=bindacct,CN=Users、DC=cpoc、DC=local」。	連結密碼（選用）
當您在上方輸入連結帳戶時、就會顯示此欄位。 輸入綁定帳戶的密碼。	在新增之前先測試伺服器連線
如果您要確保儲存陣列能夠與您輸入的LDAP伺服器組態通訊、請選取此核取方塊。按一下對話方塊底部的*「Add*（新增*）」之後、就會進行測試。如果選取此核取方塊且測試失敗、則不會新增組態。您必須解決錯誤或取消選取核取方塊、才能跳過測試並新增組態。	**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」。

設定	說明
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。沒有監控角色的任何使用者、System Manager將無法正常運作。

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

   此時會開啟「目錄伺服器設定」對話方塊。

5. 在*伺服器設定*索引標籤中、變更所需的設定。

設定	說明
組態設定	網域
LDAP伺服器的網域名稱。若為多個網域、請在以逗號分隔的清單中輸入網域。網域名稱用於登入（*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）
綁定帳戶的密碼。（輸入連結帳戶時、會顯示此欄位。）	儲存前先測試伺服器連線
檢查儲存陣列是否能與LDAP伺服器組態通訊。按一下對話方塊底部的「儲存」之後、就會進行測試。如果選取此核取方塊且測試失敗、則不會變更組態。您必須解決錯誤或取消選取核取方塊、才能跳過測試並重新編輯組態。	權限設定
搜尋基礎DN	要搜尋使用者的LDAP內容、通常格式為「CN=Users、DC=cOPC、DC=local」。
使用者名稱屬性	繫結至使用者ID以進行驗證的屬性。例如：「AMAccountName」。
群組屬性	使用者上的群組屬性清單、用於群組對角色對應。例如：「memberof、managedObjects'。

6. 在*角色對應*索引標籤中、變更所需的對應。

設定	說明
對應	群組DN
要對應之LDAP使用者群組的網域名稱。	角色

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

7. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。

8. 按一下「 * 儲存 * 」。

結果

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

移除目錄伺服器

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

開始之前

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

關於這項工作

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

步驟

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

   「移除目錄伺服器」對話方塊隨即開啟。

5. 在欄位中輸入「移除」、然後按一下「移除」。

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

設定SAML

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

關於這項工作

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

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

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

設定SAML驗證是一個多步驟程序：

- 步驟1：上傳IDP中繼資料檔案
- 步驟2：匯出服務供應商檔案
- 步驟3：對應角色
- 步驟4：測試SSO登入
- 步驟5：啟用SAML

步驟**1**：上傳**IDP**中繼資料檔案

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

開始之前

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

關於這項工作

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

步驟

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

   頁面會顯示組態步驟的總覽。

3. 按一下*匯入身分識別提供者（IDP）檔案*連結。

   「匯入身分識別提供者檔案」對話方塊隨即開啟。

4. 按一下*瀏覽*以選取並上傳您複製到本機系統的IDP中繼資料檔案。

   選取檔案後、將會顯示IDP實體ID。

5. 按一下*匯入*。

步驟**2**：匯出服務供應商檔案

若要在IDP與儲存陣列之間建立信任關係、請將服務供應商中繼資料匯入IDP。

開始之前

- 您知道儲存陣列中每個控制器的IP位址或網域名稱。

關於這項工作

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

步驟

1. 按一下「匯出服務供應商檔案」連結。

   「匯出服務供應商檔案」對話方塊隨即開啟。

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

   按一下「匯出」後、服務供應商中繼資料便會下載到您的本機系統。記下檔案的儲存位置。

3. 從本機系統中、找出您匯出的服務供應商中繼資料檔案。

   每個控制器都有一個XML格式的檔案。

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

步驟**3**：對應角色

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

開始之前

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

關於這項工作

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

步驟

1. 按一下對應System Manager角色的連結。

   此時會開啟「角色對應」對話方塊。

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

欄位詳細資料

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

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

3. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。

啟用SAML之後、即可修改角色對應。

4. 完成對應後、請按一下*「Save（儲存）」*。

步驟**4**：測試**SSO**登入

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

開始之前

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

步驟

1. 選取「測試**SSO**登入」連結。

   隨即開啟對話方塊、供您輸入SSO認證。

2. 輸入具有「安全性管理」權限和「監控」權限的使用者登入認證。

   系統會在測試登入時開啟對話方塊。

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

   如果測試未成功完成、則會出現錯誤訊息、並提供進一步資訊。請確定：

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

步驟**5**：啟用**SAML**

最後一步是啟用SAML使用者驗證。

開始之前

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

關於這項工作

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

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

步驟

1. 從「* SAML *」標籤中、選取「*啟用SAML *」連結。

   「*確認啟用SAML」對話方塊隨即開啟。

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

結果

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

變更**SAML**角色對應

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

開始之前

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

步驟

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

   此時會開啟「角色對應」對話方塊。

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

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

欄位詳細資料

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

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

5. *（可選）：*單擊*添加另一個映射*以輸入更多的組對角色映射。
6. 按一下「 * 儲存 * 」。

結果

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

匯出SAML服務供應商檔案

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

開始之前

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

關於這項工作

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

步驟

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

   「匯出服務供應商檔案」對話方塊隨即開啟。

4. 針對每個控制器、按一下*匯出*、將中繼資料檔案儲存至您的本機系統。

每個控制器的網域名稱欄位為唯讀。

記下檔案的儲存位置。

5. 從本機系統中、找出您匯出的服務供應商中繼資料檔案。

   每個控制器都有一個XML格式的檔案。

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

檢視稽核記錄活動

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

開始之前

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

步驟

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

   *稽核日誌*活動會以表格格式顯示、其中包含下列資訊欄：

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

3. 使用「稽核記錄」頁面上的選項來檢視及管理事件。

選擇詳細資料

選擇	說明
從…顯示事件	限制依日期範圍（過去24小時、過去7天、過去30天或自訂日期範圍）顯示的事件。
篩選器	限制以欄位中輸入的字元顯示的事件。請使用引號（""）表示完全相符的字詞、輸入「OR」以傳回一或多個字詞、或輸入破折號（-）以省略字詞。
重新整理	選擇* Refresh*（重新整理*）、將頁面更新為最新的事件。
檢視/編輯設定	選取*檢視/編輯設定*以開啟對話方塊、讓您指定要記錄的完整記錄原則和行動層級。
刪除事件	選取*刪除*可開啟對話方塊、讓您從頁面移除舊事件。
顯示/隱藏欄	按一下*顯示/隱藏*欄圖示 可選擇要在表格中顯示的其他列。其他欄位包括： • 方法：HTTP方法（例如POST、GET、DELETE等）。 • **CLI**命令已執行—針對安全CLI要求執行的CLI命令（語法）。 • * CLI傳回狀態*：CLI狀態代碼或用戶端輸入檔的要求。 • 符號程序-執行的符號程序。 • * SSH事件類型*-安全Shell（SSH）事件類型、例如登入、登出及login_fail。 • * SSH工作階段PID*- SSH工作階段的處理序ID編號。 • * SSH工作階段持續時間*-使用者登入的秒數。
切換欄篩選條件	按一下*切換*圖示 開啟每欄的篩選欄位。在欄位中輸入字元、以限制這些字元所顯示的事件。再按一下圖示以關閉篩選欄位。
復原變更	按一下「復原」圖示 可將表恢復爲默認配置。
匯出	按一下「匯出」、將表格資料儲存至以逗號分隔的值（CSV）檔案。

定義稽核記錄原則

您可以變更覆寫原則及稽核記錄中記錄的事件類型。

開始之前

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

關於這項工作

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

步驟

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

   「稽核記錄設定」對話方塊隨即開啟。

4. 變更覆寫原則或記錄的事件類型。

   欄位詳細資料

設定	說明
覆寫原則	決定當達到最大容量時覆寫舊事件的原則： • *當稽核日誌已滿*時、允許覆寫稽核日誌中最舊的事件；當稽核日誌達到50、000筆記錄時、會覆寫舊事件。 • 要求手動刪除稽核記錄事件-指定不會自動刪除事件、而是在設定的百分比顯示臨界值警告。必須手動刪除事件。 如果停用覆寫原則、且稽核記錄項目達到上限、則沒有「安全性管理」權限的使用者將無法存取System Manager。若要將系統存取權限還原給沒有「安全性管理」權限的使用者、則指派給「安全性管理」角色的使用者必須刪除舊的事件記錄。 如果將syslog伺服器設定為歸檔稽核記錄、則不適用覆寫原則。
要記錄的行動層級	決定要記錄的事件類型： • 僅記錄修改事件-僅顯示使用者動作涉及變更系統的事件。 • 記錄所有修改和唯讀事件-顯示所有事件、包括需要讀取或下載資訊的使用者動作。

5. 按一下「 * 儲存 * 」。

從稽核記錄刪除事件

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

開始之前

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

關於這項工作

此工作說明如何從稽核記錄中移除舊事件。

步驟

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

   「*刪除稽核記錄」對話方塊隨即開啟。

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

   隨即開啟確認對話方塊。

7. 在欄位中輸入「刪除」、然後按一下「刪除」。

   最舊的事件會從「稽核記錄」頁面移除。

設定系統記錄伺服器進行稽核記錄

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

開始之前

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

步驟

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

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

3. 按一下「 * 新增 * 」。

   「新增**Syslog**伺服器」對話方塊隨即開啟。

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

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

   - Port（連接埠）-輸入syslog接收器的連接埠號碼。按一下「新增」之後、「設定**Syslog**伺服器」對話方塊會開啟、並在頁面上顯示您設定的syslog伺服器。
5. 若要測試伺服器與儲存陣列的連線、請選取* Test All*。

結果

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

編輯稽核記錄的**syslog**伺服器設定

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

開始之前

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

步驟

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

   已設定的syslog伺服器會顯示在頁面上。

3. 若要編輯伺服器資訊、請選取伺服器名稱右側的*編輯*（鉛筆）圖示、然後在下列欄位中進行所需的變更：
   - 伺服器位址：輸入完整網域名稱、IPv4位址或IPv6位址。
   - Protocol（傳輸協定）-從下拉式清單中選取傳輸協定（例如TLS、UDP或TCP）。
   - Port（連接埠）-輸入syslog接收器的連接埠號碼。

4. 如果您將傳輸協定變更為安全TLS傳輸協定（從UDP或TCP）、請按一下*匯入信任的憑證*上傳CA憑證。
5. 若要測試與儲存陣列的新連線、請選取*「Test All（測試全部）」*。

結果

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

常見問題集

為什麼我無法登入？

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

系統管理員可能會因為下列其中一項原因而發生登入錯誤：

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

由於下列原因之一、可能會發生遠端儲存陣列鏡射工作的登入錯誤：

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

新增目錄伺服器之前、我需要知道什麼？

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

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

我需要知道哪些關於對應至儲存陣列角色的資訊？

在將群組對應至角色之前、請先檢閱下列準則。

儲存陣列的內嵌RBAC（角色型存取控制）功能包括下列角色：

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

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

目錄服務

如果您使用的是LDAP（輕量型目錄存取傳輸協定）伺服器和目錄服務、請確定：

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

SAML

如果您使用儲存陣列內嵌的安全聲明標記語言（SAML）功能、請確定：

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

哪些外部管理工具可能會受此變更影響？

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

管理介面

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

如需詳細資訊、請聯絡技術支援部門。

SAML驗證

啟用SAML時、下列用戶端無法存取儲存陣列服務和資源：

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

如需詳細資訊、請聯絡技術支援部門。

在設定及啟用**SAML**之前、我需要知道哪些資訊？

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

需求

開始之前、請確定：

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

限制

除了上述要求之外、請務必瞭解下列限制：

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

稽核記錄中記錄了哪些類型的事件？

稽核日誌可記錄修改事件、或同時記錄修改和唯讀事件。

視原則設定而定、會顯示下列類型的事件：

- 修改事件：系統管理程式中涉及系統變更（例如資源配置儲存設備）的使用者動作。

- 修改和唯讀事件：涉及系統變更的使用者動作、以及涉及檢視或下載資訊的事件、例如檢視磁碟區指派。

設定syslog伺服器之前、我需要知道什麼？

您可以將稽核記錄歸檔至外部syslog伺服器。

在設定syslog伺服器之前、請記住下列準則。

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

系統記錄伺服器不再接收稽核記錄。我該怎麼辦？

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

若要解決此問題、您必須先修正syslog伺服器的憑證。一旦有效的憑證鏈結就位、請前往功能表：「Settings[Audit Log（設定稽核記錄）> Configure Syslog Servers（設定Syslog伺服器）> Test All（全部測試）」。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變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 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。