



使用**SAML** SANtricity 11.7

NetApp
February 12, 2024

目錄

使用SAML	1
設定 SAML	1
變更SAML角色對應	5
匯出SAML服務供應商檔案	6

使用SAML

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。

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每個控制器的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。
- 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

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



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



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

設定SAML驗證是一個多步驟程序。

步驟1：上傳IDP中繼資料檔案

若要為儲存陣列提供IDP連線資訊、請將IDP中繼資料匯入System Manager。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。IDP需要此中繼資料、才能與控制器建立信任關係、並處理授權要求。檔案包含控制器網域名稱或IP位址等資訊、以便IDP與服務供應商通訊。

步驟

1. 按一下「匯出服務供應商檔案」連結。

「匯出服務供應商檔案」對話方塊隨即開啟。

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

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

3. 從本機系統中、找出您匯出的服務供應商中繼資料檔案。

每個控制器都有一個XML格式的檔案。

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

步驟3：對應角色

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

開始之前

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

步驟

1. 按一下「*對應系統管理程式*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。一個群組可以有許多指派的角。

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。支援規則運算式。這些特殊的規則運算式字元必須以反斜線轉義（\）如果它們不是正則表達式模式的一部分： \[\] \{ \} \< \> * \+ \- \= \! \? \^ \\$	
角色	<p>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。必須搭配其他角色才能登入系統管理員、才能使用監控角色。至少一個群組也需要安全管理員角色。</p> <p>對應的角色包括下列權限：</p> <ul style="list-style-type: none"> • 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。



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。



*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. 類型 enable，然後單擊 **Enable**。
3. 輸入SSO登入測試的使用者認證資料。

結果

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

變更SAML角色對應

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

開始之前

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

步驟

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

此時會開啟「角色對應」對話方塊。

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



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

欄位詳細資料

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



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

5. （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。
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 * 。

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。