使用SAML

SANtricity 11.7

NetApp
February 12, 2024

目錄

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。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。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	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。 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。

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* 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 * 。