管理SAML驗證設定

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

目錄

管理SAML驗證設定

設定遠端驗證設定之後、您可以啟用安全聲明標記語言（SAML）驗證、讓遠端使用者先經過安全身分識別供應商（IDP）的驗證、才能存取Unified Manager Web UI。

請注意、啟用SAML驗證後、只有遠端使用者才能存取Unified Manager圖形化使用者介面。本機使用者和維護使用者將無法存取UI。此組態不會影響存取維護主控台的使用者。

身分識別供應商要求

將Unified Manager設定為使用身分識別供應商（IDP）來為所有遠端使用者執行SAML驗證時、您必須知道某些必要的組態設定、才能成功連線至Unified Manager。

您必須在IDP伺服器中輸入Unified Manager URI和中繼資料。您可以從Unified ManagerSAML驗證頁面複製此資訊。Unified Manager被視為安全性聲明標記語言（SAML）標準中的服務供應商（SP）。

支援的加密標準

- 進階加密標準（AES）：AES-128和AES-256
- 安全雜湊演算法（SHa）：SHA-1和SHA-256

已驗證的身分識別供應商

- Shibboleth
- Active Directory Federation Services（ADFS）

ADFS組態需求

- 您必須依下列順序定義三個宣告規則、Unified Manager才能剖析此信賴方信任項目的ADFS SAML回應。

請款規則	價值
Sam-account-name	名稱ID
Sam-account-name	urn:oID：0.9.2342.19200300.1001.1
權杖群組-不合格的名稱	urn:oID：1.3.6.1.4.1.5923.1.5.1.1

- 您必須將驗證方法設定為「表單驗證」、否則使用者在使用Internet Explorer登出Unified Manager時可能會收到錯誤訊息。請遵循下列步驟：
  a. 開啟ADFS管理主控台。
  b. 按一下左樹狀檢視中的「驗證原則」資料夾。
  c. 在右側的「Actions（動作）」下、按一下「Edit Global Primary驗證Policy（編輯全域主要驗
  d. 將內部網路驗證方法設為「Forms驗證」、而非預設的「Windows驗證」。

- 在某些情況下、當Unified Manager安全性憑證簽署CA時、會拒絕透過IDP登入。有兩種因應措施可解決此問題：
  - 請依照連結中所述的指示、針對連結的依賴方之鏈結CA憑證、停用在ADFS伺服器上的撤銷檢查：

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - 讓CA伺服器位於ADFS伺服器內、以簽署Unified Manager伺服器認證要求。

其他組態需求

- Unified Manager時鐘偏移設定為5分鐘、因此IDP伺服器與Unified Manager伺服器之間的時間差異不可超過5分鐘、否則驗證將會失敗。
- 當使用者嘗試使用Internet Explorer存取Unified Manager時、可能會看到訊息*網站無法顯示頁面*。如果發生這種情況、請務必取消勾選*工具*>*網際網路選項*>*進階*中的「HTTP錯誤訊息的友善程度」選項。

啟用SAML驗證

您可以啟用安全聲明標記語言（SAML）驗證、讓遠端使用者在存取Unified Manager Web UI之前、先經過安全身分識別供應商（IDP）的驗證。

開始之前

- 您必須已設定遠端驗證、並驗證是否成功。
- 您必須建立至少一個具備OnCommand 「管理員」角色的遠端使用者或遠端群組。
- Identity Provider（IDP）必須由Unified Manager支援、且必須加以設定。
- 您必須擁有IDP URL和中繼資料。
- 您必須擁有IDP伺服器的存取權。

關於這項工作

從Unified Manager啟用SAML驗證後、使用者必須先使用Unified Manager伺服器主機資訊設定IDP、才能存取圖形化使用者介面。因此您必須準備好完成連線的兩個部分、才能開始組態程序。IDP可在設定Unified Manager之前或之後進行設定。

啟用SAML驗證後、只有遠端使用者才能存取Unified Manager圖形化使用者介面。本機使用者和維護使用者將無法存取UI。此組態不會影響存取維護主控台、Unified Manager命令或ZAPI的使用者。

在您完成此頁面上的SAML組態之後、Unified Manager會自動重新啟動。

步驟

1. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。
2. 在「設定/驗證」頁面中、選取「* SAML驗證*」標籤。
3. 選取「啟用**SAML**驗證」核取方塊。

隨即顯示設定IDP連線所需的欄位。

4. 輸入IDP URI和IDP中繼資料、以將Unified Manager伺服器連線至IDP伺服器。

   如果IDP伺服器可直接從Unified Manager伺服器存取、您可以在輸入IDP URI之後按一下*擷取IDP中繼資料*按鈕、自動填入IDP中繼資料欄位。

5. 複製Unified Manager主機中繼資料URI、或將主機中繼資料儲存至XML文字檔。

   您現在可以使用此資訊來設定IDP伺服器。

6. 按一下「 * 儲存 * 」 。

   隨即顯示訊息方塊、確認您要完成組態並重新啟動Unified Manager。

7. 按一下*「Confirm and Logout*（確認並登出）」、Unified Manager即會重新啟動。

結果

下次授權的遠端使用者嘗試存取Unified Manager圖形介面時、他們會在IDP登入頁面中輸入其認證資料、而非在Unified Manager登入頁面中輸入認證資料。

完成後

如果尚未完成、請存取IDP並輸入Unified Manager伺服器URI和中繼資料、以完成組態。

使用ADFS做為身分識別供應商時、Unified Manager GUI不會遵守ADFS逾時、會繼續運作、直到Unified Manager工作階段逾時為止。在Windows、Red Hat或CentOS上部署Unified Manager時、您可以使用下列Unified Manager CLI命令來變更GUI工作階段逾時： `um option set absolute.session.timeout=00:15:00`此命令會將Unified Manager GUI工作階段逾時設定為15分鐘。

變更用於SAML驗證的身分識別供應商

您可以變更Unified Manager用來驗證遠端使用者的身分識別供應商（IDP）。

開始之前

- 您必須擁有IDP URL和中繼資料。
- 您必須擁有IDP的存取權。

關於這項工作

新的IDP可在設定Unified Manager之前或之後進行設定。

步驟

1. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。

2. 在「設定/驗證」頁面中、選取「* SAML驗證*」標籤。
3. 輸入將Unified Manager伺服器連線至IDP所需的新IDP URI和IDP中繼資料。

   如果IDP可直接從Unified Manager伺服器存取、您可以在輸入IDP URL後按一下*擷取IDP中繼資料*按鈕、自動填入IDP中繼資料欄位。

4. 複製Unified Manager中繼資料URI、或將中繼資料儲存至XML文字檔。
5. 按一下「儲存組態」。

   隨即顯示訊息方塊、確認您要變更組態。

6. 按一下「確定」。

完成後

存取新的IDP、然後輸入Unified Manager伺服器URI和中繼資料以完成組態。

下次授權的遠端使用者嘗試存取Unified Manager圖形介面時、他們會在新的IDP登入頁面中輸入其認證資料、而非在舊的IDP登入頁面中輸入認證資料。

在Unified Manager安全性憑證變更之後更新SAML驗證設定

若對安裝在Unified Manager伺服器上的HTTPS安全性憑證進行任何變更、都必須更新SAML驗證組態設定。如果您重新命名主機系統、指派主機系統的新IP位址、或手動變更系統的安全性憑證、則會更新憑證。

關於這項工作

變更安全性憑證並重新啟動Unified Manager伺服器之後、SAML驗證將無法運作、使用者將無法存取Unified Manager圖形介面。您必須更新IDP伺服器和Unified Manager伺服器上的SAML驗證設定、才能重新啟用使用者介面的存取。

步驟

1. 登入維護主控台。
2. 在*主功能表*中、輸入*停用SAML驗證*選項的編號。

   畫面會顯示訊息、確認您要停用SAML驗證並重新啟動Unified Manager。

3. 使用更新的FQDN或IP位址啟動Unified Manager使用者介面、將更新的伺服器憑證接受到瀏覽器、然後使用維護使用者認證登入。
4. 在「設定/驗證」頁面中、選取「* SAML驗證*」索引標籤、然後設定IDP連線。
5. 複製Unified Manager主機中繼資料URI、或將主機中繼資料儲存至XML文字檔。
6. 按一下「 * 儲存 * 」。

   隨即顯示訊息方塊、確認您要完成組態並重新啟動Unified Manager。

7. 按一下*「Confirm and Logout*（確認並登出）」、Unified Manager即會重新啟動。
8. 存取您的IDP伺服器、然後輸入Unified Manager伺服器URI和中繼資料以完成組態。

身分識別供應商	組態步驟
ADFS	a. 刪除ADFS管理GUI中現有的信賴關係人信任項目。 b. 使用新增信賴關係人信任項目 `saml_sp_metadata.xml` 更新的Unified Manager伺服器。 c. 定義Unified Manager剖析此信賴方信任項目的ADFS SAML回應所需的三種宣告規則。 d. 重新啟動ADFS Windows服務。
Shibboleth	a. 將Unified Manager伺服器的新FQDN更新至 `attribute-filter.xml` 和 `relying-party.xml` 檔案： b. 重新啟動Apache TOMCAT Web伺服器、並等待連接埠8005上線。

9. 登入Unified Manager、並確認SAML驗證可在您的IDP中正常運作。

停用SAML驗證

若要停止透過安全身分識別供應商（IDP）驗證遠端使用者、然後再登入Unified Manager Web UI、您可以停用SAML驗證。停用SAML驗證時、已設定的目錄服務供應商（例如Active Directory或LDAP）會執行登入驗證。

關於這項工作

停用SAML驗證後、本機使用者和維護使用者除了能存取已設定的遠端使用者之外、也能存取圖形化使用者介面。

如果您無法存取圖形化使用者介面、也可以使用Unified Manager維護主控台停用SAML驗證。

停用SAML驗證後、Unified Manager會自動重新啟動。

步驟

1. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。
2. 在「設定/驗證」頁面中、選取「* SAML驗證*」標籤。
3. 取消核取「啟用**SAML**驗證」核取方塊。
4. 按一下「 * 儲存 * 」。

   隨即顯示訊息方塊、確認您要完成組態並重新啟動Unified Manager。

5. 按一下*「Confirm and Logout*（確認並登出）」、Unified Manager即會重新啟動。

結果

下次遠端使用者嘗試存取Unified Manager圖形化介面時、他們會在Unified Manager登入頁面輸入其認證資料、而非IDP登入頁面。

完成後

存取IDP並刪除Unified Manager伺服器URI和中繼資料。

從維護主控台停用SAML驗證

當無法存取Unified Manager GUI時、您可能需要從維護主控台停用SAML驗證。如果設定錯誤或無法存取IDP、可能會發生這種情況。

開始之前

您必須以維護使用者的身分存取維護主控台。

關於這項工作

停用SAML驗證時、已設定的目錄服務供應商（例如Active Directory或LDAP）會執行登入驗證。除了設定的遠端使用者之外、本機使用者和維護使用者也能存取圖形化使用者介面。

您也可以從UI的「設定/驗證」頁面停用SAML驗證。

停用SAML驗證後、Unified Manager會自動重新啟動。

步驟

1. 登入維護主控台。
2. 在*主功能表*中、輸入*停用SAML驗證*選項的編號。

   畫面會顯示訊息、確認您要停用SAML驗證並重新啟動Unified Manager。

3. 鍵入* y*、然後按Enter鍵、Unified Manager即會重新啟動。

結果

下次遠端使用者嘗試存取Unified Manager圖形化介面時、他們會在Unified Manager登入頁面輸入其認證資料、而非IDP登入頁面。

完成後

如有需要、請存取IDP並刪除Unified Manager伺服器URL和中繼資料。