管理SAML驗證設定

Active IQ Unified Manager 9.14

NetApp
August 22, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/active-iq-unified-manager/config/reference_identity_provider_requirements_um.html on August 22, 2024. Always check docs.netapp.com for the latest.

目錄

管理SAML驗證設定 1
身分識別供應商要求 1
啟用SAML驗證 2
變更用於SAML驗證的身分識別供應商 3
在Unified Manager安全性憑證變更之後更新SAML驗證設定 4
停用SAML驗證 5
從維護主控台停用SAML驗證 5
SAML驗證頁面 6

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「Forms驗證」、否則使用者在登出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：

    "停用每個信賴方信任的撤銷檢查"

  - 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。

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。

您需要的是什麼

- 您必須已設定遠端驗證、並驗證是否成功。
- 您必須已建立至少一個具有應用程式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。

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. 在左導覽窗格中、按一下*一般*>* SAML驗證*。
2. 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。

3. 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。

4. 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。

5. 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。

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

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。

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。您可以按一下*一般*>*功能設定*>*無活動逾時*來變更GUI工作階段逾時。

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）。

您需要的是什麼

- 您必須擁有IDP URL和中繼資料。
- 您必須擁有IDP的存取權。

新的IDP可在設定Unified Manager之前或之後進行設定。

步驟

1. 在左導覽窗格中、按一下*一般*>* SAML驗證*。
2. 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。

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

   隨即顯示訊息方塊、確認您要變更組態。

5. 按一下「確定」。

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。

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. 使用更新的Unified Manager伺服器中的「sAML_sp_mendors.xml」新增信賴關係人信任項目。 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更新為「attribute-filer.xml」和「remale-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。

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. 在左導覽窗格中、按一下*一般*>* SAML驗證*。
2. 取消核取「啟用**SAML**驗證」核取方塊。
3. 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。

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

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。

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。這可能發生在設定錯誤或無法存取IDP的情況下。

您需要的是什麼

您必須以維護使用者的身分存取維護主控台。

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。

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。

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

SAML驗證頁面

您可以使用「SAML驗證」頁面來設定Unified Manager、以便透過安全的身分識別供應商（IDP）驗證使用SAML的遠端使用者、然後才能登入Unified Manager Web UI。

- 您必須具有應用程式管理員角色、才能建立或修改SAML組態。
- 您必須已設定遠端驗證。
- 您必須至少設定一個遠端使用者或遠端群組。

設定遠端驗證和遠端使用者之後、您可以選取「啟用SAML驗證」核取方塊、以使用安全的身分識別供應商來啟用驗證。

- * IDP URI*

  從Unified Manager伺服器存取IDP的URI。範例URI如下所示。

  ADFS範例URI：

  https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml+`

  Shibboleth範例URI：

  https://centos7.ntap2016.local/idp/shibboleth+`

- * IDP中繼資料*

  XML格式的IDP中繼資料。

  如果IDP URL可從Unified Manager伺服器存取、您可以按一下*擷取IDP中繼資料*按鈕來填入此欄位。

- 主機系統（**FQDN**）

  安裝期間定義的Unified Manager主機系統FQDN。如有必要、您可以變更此值。

- *主機URI *

  從IDP存取Unified Manager主機系統的URI。

- 主機中繼資料

  XML格式的主機系統中繼資料。

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。