在郵件安全裝置中搜尋和檢視SAML身份驗證

目錄

簡介

本文檔介紹如何搜尋顯示郵件安全裝置(ESA)如何處理SAML身份驗證請求的日誌條目。

背景資訊

思科郵件安全設備(ESA)支援終端使用者訪問垃圾郵件隔離區和使用管理使用者介面的管理員的SSO登入，該管理使用者介面是基於XML的開放式標準資料格式，允許管理員在登入到其中某個應用程式後無縫訪問一組定義的應用程式。

要瞭解有關SAML的詳細資訊，請參閱:SAML一般資訊

需求

- 配置了外部身份驗證的郵件安全裝置。
- SAML與任何身份提供程式的整合。

採用元件

- 電子郵件安全裝置對命令列介面(CLI)的訪問。
- Gui日誌訂閱
- SAML DevTools擴展。有關詳細資訊，請參閱：適用於Chrome的SAML開發工具

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

如何在ESA上搜尋和檢視SAML登入請求的身份驗證日誌？

身份驗證日誌訂閱不顯示有關SAML登入請求的資訊。但是，資訊會記錄在GUI日誌中。

日誌的名稱為*gui_logs*，日誌型別為*Http_logs*。您可以在以下頁面中看到此資訊： **系統管理>日誌訂閱> gui_logs。**

您可以訪問以下日誌：

在命令列中：

- 使用SSH客戶端（如Putty）。通過埠22/SSH登入到ESA裝置的CLI。
- 在命令列中，選擇grep以搜尋請求訪問許可權的使用者的電子郵件地址。

載入CLI後，您可以搜尋 Email address，如以下命令所示：

(Machine esa.cisco.com) (SERVICE)> grep "username@cisco.com" gui_logs

要成功登入，您會看到三個條目：

1. 由ESA生成的SAML請求，請求配置的身份提供商提供身份驗證和授權資料。

GET /login?action=SAMLRequest

2. 已正確建立通知SAML斷言。

Destination:/ Username:usernamehere@cisco.com Privilege:PrivilegeTypeHere session:SessionIdHere Action: The HTTPS session has been established successfully.

3. SSO通知結果。

Info: SSO authentication is successful for the user: username@cisco.com.

如果未顯示這三個條目，則身份驗證請求不成功，並且與以下方案相關：

場景1：如果日誌中只顯示SAML請求。

GET /login?action=SAMLRequest

身份提供方拒絕身份驗證請求，因為未將使用者分配到SAML應用程式或者未將錯誤的身份提供方URL新增到ESA。

場景2：如果日誌條目

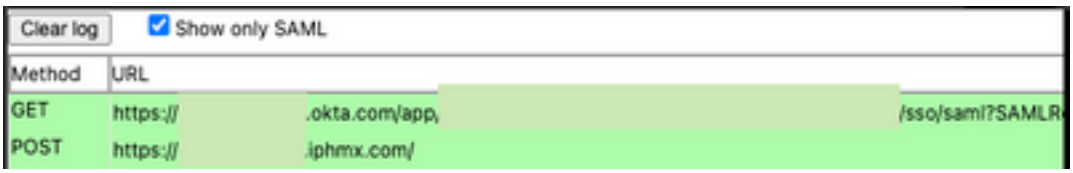
Authorization failed on appliance, While fetching user privileges from group mapping和 An error occured during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response 在日誌中顯示。

An error occured during SSO authentication. Details: User: usernamehere@cisco.com Authorization failed on appliance, While fetching user privileges from group mapping.

An error occured during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response.

在身份提供程式配置中檢查分配給SAML應用程式的使用者許可權和組。

或者，也可以使用SAML DevTools擴展直接從Web瀏覽器檢索SAML應用程式響應，如下圖所示：



相關資訊

思科安全電子郵件網關使用手冊

SAML DevTools擴展

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。