對外部身份驗證的SAML Azure組匹配失敗進行故障排除

目錄

簡介

本文檔介紹如何對外部身份驗證的Azure Active Directory SAML組宣告失敗進行故障排除。

必要條件

外部身份驗證位於Cisco Secure Email Gateway、Cisco Secure Email和Web Manager裝置上。

需求

思科建議您瞭解以下主題：

- SAML 2.0 SSO已配置且至少為一個測試帳戶工作正常。
- 已在裝置上啟用組對映，並配置為使用組宣告：Microsoft架構 — 身份宣告組。
- 訪問Entra ID以修改應用程式的組宣告配置。

採用元件

- 產品：配置用於SAML 2.0單一登入(SSO)時，思科安全電子郵件網關(ESA)和思科安全電子郵件和網路管理器(SMA)。
- 身份提供程式(IdP):Microsoft Entra ID(Azure AD)。
- 授權方法：基於SAML組宣告（組對映）的裝置角色/許可權分配。

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。

症狀

- 當使用者被顯式對映（例如，通過使用者ID）時，SSO成功；當授權依賴於組對映時，SSO失敗。
- SSO日誌顯示組屬性或組對映不匹配錯誤。

原因

如果使用者是超過150個組的成員，Microsoft Entra ID不會在SAML斷言中發出預期的組宣告(Microsoft Schemas - Identity Claims Group)。相反，它會發出Microsoft Schemes - Claims Group，裝置無法使用該組進行角色對映。

疑難排解

適用於：使用Microsoft Entra ID(Azure AD)配置SAML 2.0 SSO，其中裝置使用SAML組宣告進行授權（組對映）。

驗證SSO日誌

在Cisco Secure Email裝置上，從GUI日誌收集單點登入(SSO)身份驗證嘗試日誌。例如，運行以下命令:

```
grep -i sso gui_logs
```

如果問題與身份提供程式(IdP)斷言中的組對映有關，則SSO日誌可以顯示以下錯誤消息：

```
grep -i sso gui_logs
"An error occurred during SSO authentication. Details: Please check the configured Group Attributes, it
"An error occurred during SSO authentication. Details: User: XXXXX Authorization failed on appliance, w
"An error occurred during SSO authentication. Details: Please check the configured Group Mapping values
```

捕獲SAML響應

要確認問題是否由大量組成員身份引起，請在失敗的SAML身份驗證嘗試期間收集超文本傳輸協定(HTTP)存檔(HAR)檔案。使用瀏覽器開發人員工具或經核准的瀏覽器擴展。請勿使用公共線上解碼器或第三方上傳工具檢查SAML響應。

程序:

1. 開啟browser developer 工具並啟動network 擷取。
2. 導航到思科安全電子郵件網關或思科安全電子郵件和Web管理器Web介面。
3. 啟動SAML單一登入(SSO)流並重現授權失敗。
4. 將捕獲的會話匯出為HAR檔案。

附註：具體步驟因瀏覽器而異。使用支援的瀏覽器方法，將SAML響應保留為工作站的本地響應。

分析HAR檔案

使用HAR檔案驗證Microsoft Entra ID在SAML斷言中返回哪個組屬性。

1. 在瀏覽器開發工具中開啟HAR檔案。
2. 找到SAML 響應請求，如圖1所示。
3. 複製SAMLResponse欄位的值。在影象1中，在value=之後識別引號之間的編碼值。

4. 使用已批准的離線方法對Base64編碼的SAMLResponse值進行解碼。例如，使用本地命令列實用程式：

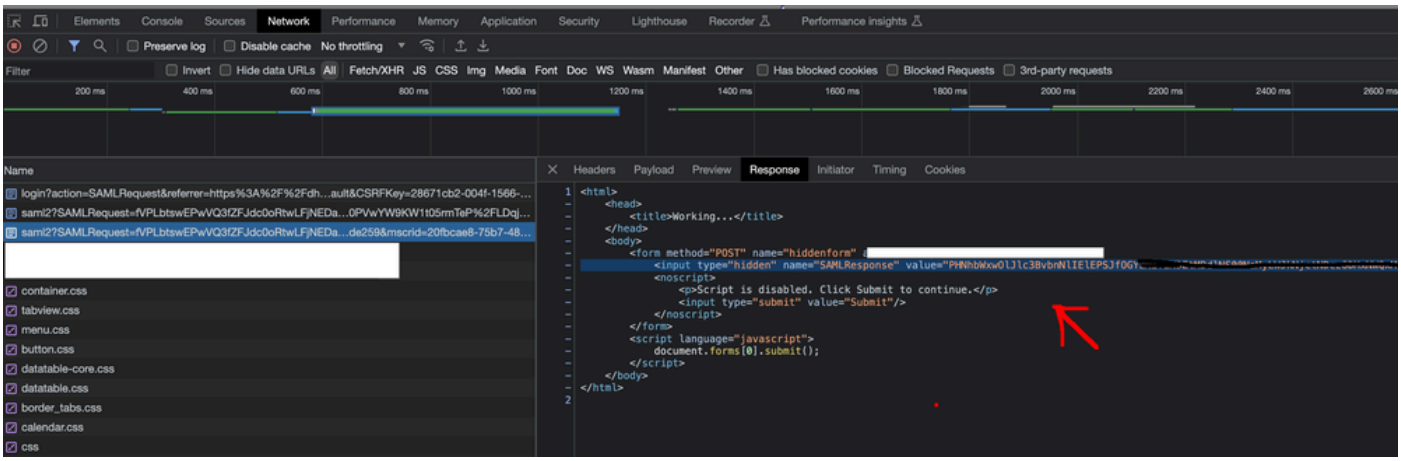
```
# macOS/Linux
printf '%s' "


        " | base64 --decode > saml_response.xml

# Windows PowerShell
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('


         ')) | Out-File -Encoding utf8 saml_response.xml
```

5. 檢查解碼的XML，並驗證Microsoft Entra ID是否返回預期的組屬性或備用連結屬性。



確定Azure組宣告行為

在工作方案中，解碼的SAML響應包含預期的groups屬性：Microsoft架構 — 身份宣告組。發生此問題時，Microsoft Entra ID將返回Microsoft方案 — 宣告組，而不是預期的組屬性。

出現此行為是因為Microsoft Entra ID限制了SAML組宣告中發出的組數。如果SAML斷言包含超過150個組成員身份，Azure AD將返回groups.link屬性而不是groups屬性。思科安全電子郵件裝置無法使用groups.link進行角色對映，因此授權失敗。

解析

修改Microsoft Entra ID應用程式，以便SAML斷言返回裝置的可用組宣告。目標是防止Azure AD返回Microsoft架構 — 宣告組，而不是預期的組屬性。

1. 在Azure AD中，開啟用於Cisco Secure Email Gateway或Cisco Secure Email and Web Manager SAML身份驗證的企業應用程式。
2. 導覽至SAML token attributes或group 宣告配置。
3. 將group claims設定更改為Groups assigned to the application（如果該設定滿足部署要求）。
4. 確保受影響的管理員帳戶僅分配給裝置授權所需的組。
5. 儲存Azure AD 配置並啟動新的SAML 登入嘗試。
6. 在裝置上，運行命令grep -i sso gui.current from /data/pub/gui_logs，並確認以前的授權錯誤不再出現。
7. 驗證解碼SAML 響應，並確認Azure AD返回Microsoft架構 — 標識宣告組，而不是Microsoft架構 — 宣告組。

附註：如果所需的Azure AD組宣告配置不可用或不符合部署要求，請與Microsoft Entra ID管理員或Microsoft支援團隊聯絡。

相關資訊

- Microsoft瞭解：配置應用程式的組宣告
- MuleSoft:Azure AD SAML組屬性限制

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）。