对外部身份验证的SAML Azure组匹配失败进行故障排除

目录

简介

本文档介绍如何对外部身份验证的Azure Active Directory SAML组声明失败进行故障排除。

先决条件

外部身份验证位于Cisco安全邮件网关、Cisco安全邮件和Web Manager设备上。

要求

Cisco 建议您了解以下主题：

- SAML 2.0 SSO已配置且至少对一个测试帐户起作用。
- 已在设备上启用组映射，并配置为使用组声明：Microsoft架构 — 身份声明组。
- 访问Entra ID以修改应用的组声明配置。

使用的组件

- 产品：思科安全邮件网关(ESA)和思科安全邮件和网络管理器(SMA)(如果配置为SAML 2.0单点登录(SSO))。
- 身份提供程序(IdP):Microsoft Entra ID(Azure AD)。
- 授权方法：基于SAML组声明的设备角色/权限分配（组映射）。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

症状

- 当用户被显式映射（例如，通过用户ID）时SSO成功，但当授权依赖于组映射时SSO失败。
- SSO日志显示组属性或组映射不匹配错误。

原因

当用户是超过150个组成员时，Microsoft Entra ID不会在SAML断言中发出预期的组声明(Microsoft Schemas - Identity Claims Group)。而是发出Microsoft Schemes - Claims Group，设备无法使用该组进行角色映射。

故障排除

适用于：使用Microsoft Entra ID(Azure AD)配置SAML 2.0 SSO，其中设备使用SAML组声明进行授权（组映射）。

验证SSO日志

在思科安全邮件设备上，从gui日志收集单点登录(SSO)身份验证尝试日志。例如，运行命令:

```
grep -i sso gui_logs
```

如果问题与身份提供程序(IdP)断言中的组映射有关，则SSO日志可以显示以下错误消息：

```
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, wh
"An error occurred during SSO authentication. Details: Please check the configured Group Mapping values
```

捕获SAML响应

要确认问题是否由大量组成员身份引起，请在失败的SAML身份验证尝试期间收集超文本传输协议(HTTP)存档(HAR)文件。使用浏览器开发人员工具或认可的浏览器扩展。请勿使用公共在线解码器或第三方上传工具检查SAML响应。

步骤:

1. 打开browser developer 工具，然后开始网络捕获。
2. 导航到Cisco Secure Email Gateway或Cisco Secure Email and Web Manager Web界面。
3. 启动SAML单点登录(SSO)流并重现授权故障。
4. 将捕获的会话导出为HAR文件。

注意：具体步骤因浏览器而异。使用支持的浏览器方法，保持SAML响应在工作站的本地位置。

分析HAR文件

使用HAR文件验证Microsoft Entra ID在SAML断言中返回哪个组属性。

1. 在浏览器开发工具中打开HAR文件。
2. 找到SAML响应请求，如图1所示。
3. 复制SAMLResponse字段的值。在图像1中，在value=之后识别引号之间的编码值。
4. 通过使用已批准的脱机方法对Base64编码的SAMLResponse值进行解码。例如，使用本地命令行实用程序：

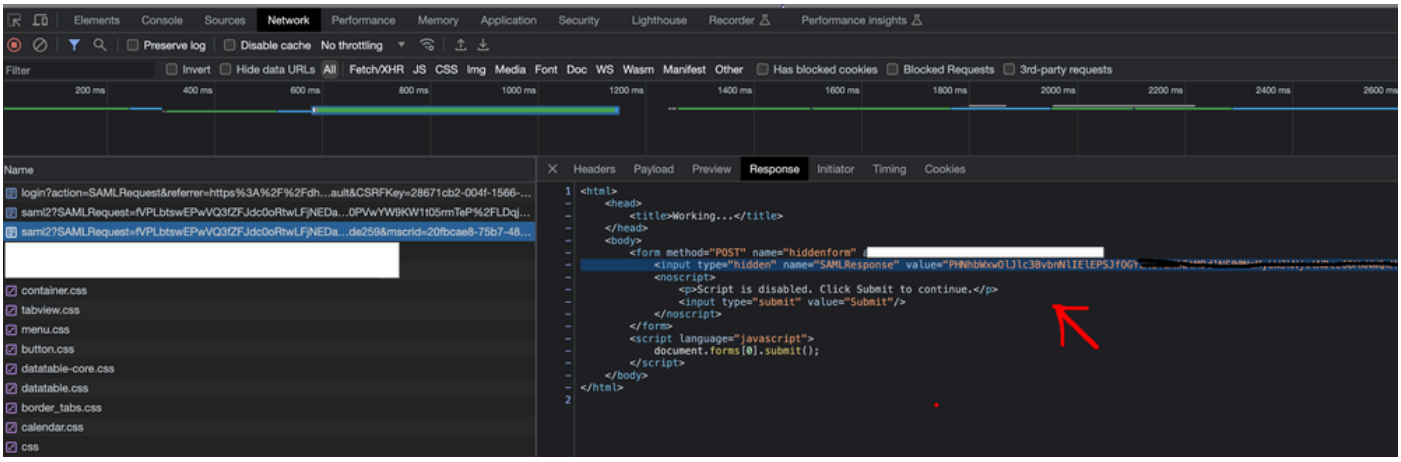
```
# macOS/Linux
printf '%s' "


        " | base64 --decode > saml_response.xml

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


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

5. 检查解码的XML，并验证Microsoft Entra ID是返回预期组属性还是返回备用链接属性。



确定Azure组声明行为

在工作场景中，解码的SAML响应包含预期组属性：Microsoft架构 — 身份声明组。发生此问题时，Microsoft Entra ID将返回Microsoft架构 — 声明组，而不是预期的组属性。

出现此行为是因为Microsoft Entra ID限制了SAML组声明中发出的组数。如果SAML断言包含超过150个组成员身份，Azure AD将返回groups.link属性而不是groups属性。思科安全邮件设备无法使

用groups.link进行角色映射，因此授权失败。

分辨率

修改Microsoft Entra ID应用程序，以便SAML断言返回设备的可用组声明。目标是防止Azure AD返回Microsoft架构 — 声明组而不是预期的组属性。

1. 在Azure AD中，打开用于Cisco安全邮件网关或Cisco安全邮件和Web管理器SAML身份验证的企业应用程序。
2. 导航到SAML 令牌属性或组声明配置。
3. 将group claims设置更改为Groups assigned to the application（如果该设置满足部署要求）。
4. 确保受影响的管理员帐户仅分配给设备授权所需的组。
5. 保存Azure AD configuration并尝试启动新的SAML 。
6. 在设备上，运行命令grep -i sso gui.current from /data/pub/gui_logs，并确认以前的授权错误不再出现。
7. 验证解码SAML 响应，并确认Azure AD返回Microsoft架构 — 身份声明组，而不是Microsoft架构 — 声明组。

注意：如果所需的Azure AD组声明配置不可用或不符合部署要求，请与Microsoft Entra ID管理员或Microsoft支持团队联系。

相关信息

- Microsoft了解：配置应用的组声明
- MuleSoft:Azure AD SAML组属性限制

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。