在邮件安全设备中搜索和查看SAML身份验证

目录

简介

本文档介绍如何搜索显示邮件安全设备(ESA)如何处理SAML身份验证请求的日志条目。

背景信息

思科邮件安全设备(ESA)支持最终用户访问垃圾邮件隔离区和使用管理用户界面的管理员的SSO登录，该管理用户界面是基于XML的开放标准数据格式，使管理员能够在登录其中一个应用后无缝访问一组定义的应用。

要了解有关SAML的详细信息，请参阅SAML一般信息

要求

- 配置了外部身份验证的邮件安全设备。
- SAML集成到任何身份提供程序。

使用的组件

- 邮件安全设备访问命令行界面(CLI)。
- Gui日志订阅
- SAML DevTools扩展。有关详细信息，请参阅：适用于Chrome的SAML Devtools

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。

如何在ESA上搜索和查看SAML登录请求的身份验证日志？

身份验证日志订阅不显示有关SAML登录请求的信息。但是，信息会记录在GUI日志中。

日志的名称为*gui_logs*，日志类型为*Http_logs*。您可以在 **系统管理>日志订阅> gui_logs。**

您可以访问以下日志：

在命令行中：

- 使用SSH客户端，如Putty。通过端口22/SSH登录到ESA设备的CLI。
- 在命令行中，选择grep以搜索请求访问的用户的电邮地址。

加载CLI后，您可以搜索 Email address，如以下命令所示：

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

要成功登录，您会看到三个条目：

1. 由ESA生成的SAML请求，请求配置的身份提供方提供身份验证和授权数据。

```
GET /login?action=SAMLRequest
```

2. 通知SAML断言已正确建立。

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

3. SSO通知结果。

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

如果这三个条目未显示，则身份验证请求不会成功，并且与以下场景相关：

场景1：如果日志中仅显示SAML请求。

```
GET /login?action=SAMLRequest
```

身份提供程序拒绝身份验证请求，因为用户未分配到SAML应用或未向ESA添加错误的身份提供程序URL。

场景2：如果日志条目

```
Authorization failed on appliance, While fetching user privileges from group mapping
```

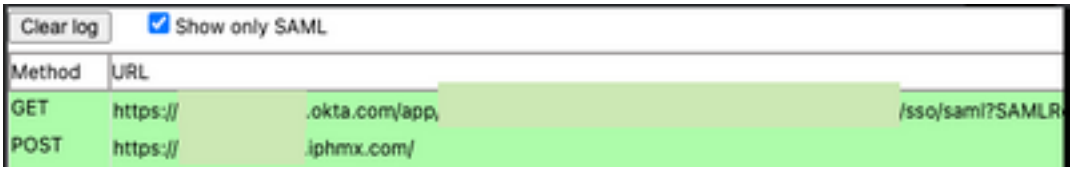
和 `An error occured during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response` 在日志中显示。

```
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.
```

在身份提供程序配置中检查分配给SAML应用程序的用户权限和组。

或者，SAML DevTools扩展可用于直接从Web浏览器检索SAML应用响应，如图所示：



相关信息

思科安全邮件网关用户指南

SAML DevTools扩展

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）。