

对SMA中SAML的“检索元数据信息时出错”错误进行故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[相关信息](#)

简介

本文档介绍如何对安全管理设备(SMA)中安全断言标记语言(SAML)的错误“检索元数据信息时出错”进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- ADFS (Active Directory联合身份验证服务)
- SAML与SMA集成
- [已安装OpenSSL](#)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- SMA AsyncOs版本11.x.x
- SMA AsyncOs版本12.x.x

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。

背景信息

思科内容安全管理设备现在支持SAML 2.0单点登录(SSO)，以便最终用户可以访问垃圾邮件隔离区，并使用用于访问其组织内其他启用SAML 2.0 SSO的服务的相同凭证。例如，您启用了Ping Identity作为SAML身份提供程序(IdP)，并在Ally、Salesforce和Dropbox上拥有启用了SAML 2.0 SSO的帐户。将思科内容安全管理设备配置为作为服务提供商(SP)支持SAML 2.0 SSO时，最终用

用户可以一次性登录并访问所有这些服务，包括垃圾邮件隔离区。

问题

选择Download Metadata for SAML时，会出现“Error occurred while retrieving metadata information”，如图所示：

The screenshot shows the Cisco M100V Content Security Management Virtual Appliance interface. The top navigation bar includes 'Management Appliance', 'Email', and 'Web'. Below this, there are tabs for 'Centralized Services', 'Network', and 'System Administration'. The main content area is titled 'SAML' and displays an error message: 'Error - Error occurred while retrieving metadata information'. Below the error message, there is a table for 'Service Provider' configuration. The table has columns for 'SP Profile Name', 'Entity ID', 'Assertion Consumer URL', 'Metadata', and 'Delete'. A single entry is shown with 'MyLab_SAML' as the SP Profile Name, 'sma.mexesa.com:83' as the Entity ID, and 'https://sma.mexesa.com:83/' as the Assertion Consumer URL. A 'Download Metadata' button is visible in the Metadata column. Below the Service Provider table, there is an 'Identity Provider' section with an 'Add Identity Provider...' button and a message stating 'No Identity Provider Profiles have been defined.'

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com:83	https://sma.mexesa.com:83/	Download Metadata	

解决方案

步骤1.在邮件安全设备(ESA)上创建新的自签名证书。

确保通用名称与实体ID URL相同，但不含端口号，如图所示：

View Certificate sma.mexesa.com

Add Certificate	
Certificate Name:	MySAML_Cert
Common Name:	sma.mexesa.com
Organization:	Tizoncito Inc
Organization Unit:	IT Security
City (Locality):	CDMX
State (Province):	CDMX
Country:	MX
Signature Issued By:	Common Name (CN): sma.mexesa.com Organization (O): Tizoncito Inc Organizational Unit (OU): IT Security Issued On: Jun 5 20:52:27 2019 GMT Expires On: Jun 4 20:52:27 2020 GMT

步骤2. 导出带有.pfx扩展名的新证书，键入密码并将其保存在计算机上。

步骤3. 打开Windows终端并输入这些命令，提供上一步的口令。

- 运行以下命令以导出私钥：

```
openssl pkcs12 -in created_certificate.pfx -nocerts -out certificateprivatekey.pem -nodes
```

- 运行以下命令以导出证书：

```
openssl pkcs12 -in created_certificate.pfx -nokeys -out certificate.pem
```

步骤4. 在此过程结束时，必须有两个新文件：**certificateprivatekey.pem**和**certificate.pem**。在服务提供商配置文件中上传这两个文件，并使用与导出证书相同的密码。

步骤5. SMA要求两个文件均采用.PEM格式才能正常工作，如图所示。

Edit Service Provider Settings

Service Provider Settings

Profile Name:

Configuration Settings:

Entity ID:

Name ID Format:

Assertion Consumer URL:

SP Certificate: No file selected.

Private Key: No file selected.

Enter passphrase:

Uploaded Certificate Details:

Issuer: C=MX\CN=sma.mexesa.com\L=CDMX\O=Tizoncito Inc\ST=CDMX\OU=IT Security

Subject: C=MX\CN=sma.mexesa.com\L=CDMX\O=Tizoncito Inc\ST=CDMX\OU=IT Security

Expiry Date: Jun 4 21:05:51 2020 GMT

Sign Requests

Sign Assertions

步骤6. 确保选中**Sign Assertions**复选框。

步骤7. 提交并确认更改，您必须能够下载元数据，如图所示。

SAML

Service Provider

Add Service Provider...

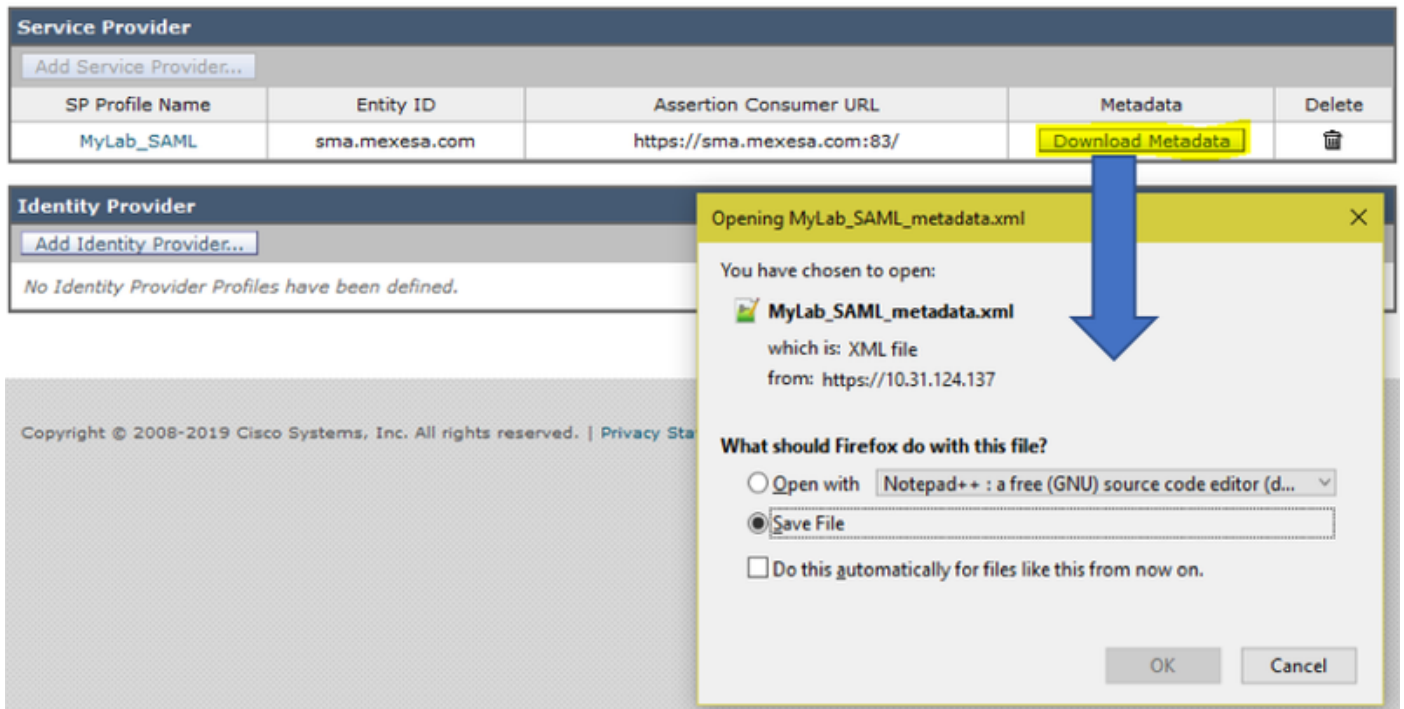
SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

Identity Provider

Add Identity Provider...

No Identity Provider Profiles have been defined.

Copyright © 2008-2019 Cisco Systems, Inc. All rights reserved. | Privacy Sta



相关信息

- [思科内容安全管理设备AsyncOS 11.0用户指南 — GD \(通用部署\)](#)
- [技术支持和文档 - Cisco Systems](#)

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）。