

SMAのSAMLの「Error occurred while retrieving metadata information」エラーのトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[関連情報](#)

概要

このドキュメントでは、セキュリティ管理アプライアンス(SMA)のSecurity Assertion Markup Language(SAML)の「メタデータ情報の取得中にエラーが発生しました」のトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ADFS (Active Directory フェデレーションサービス)
- SMAとのSAML統合
- [OpenSSLのインストール](#)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- SMA AsyncOsバージョン11.x.x
- SMA AsyncOsバージョン12.x.x

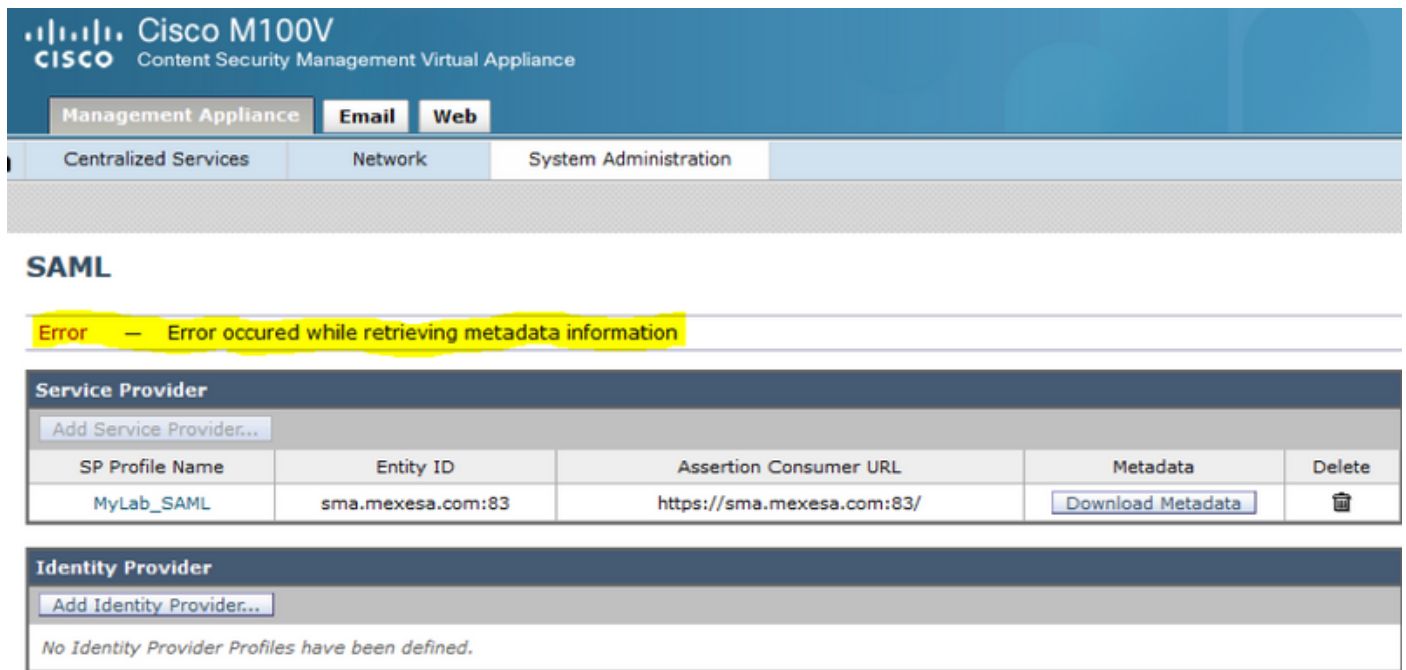
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Ciscoコンテンツセキュリティ管理アプライアンス(SMA)では、SAML 2.0シングルサインオン(SSO)がサポートされるようになりました。これにより、エンドユーザはスパム隔離にアクセスし、組織内の他のSAML 2.0 SSO対応サービスへのアクセスに使用されているのと同じクレデンシャルを使用できます。たとえば、SAML IDプロバイダー(IdP)としてPing Identityを有効にし、SAML 2.0 SSOが有効になっているRally、Salesforce、およびDropboxのアカウントを持つとします。SAML 2.0 SSOをサービスプロバイダー(SP)としてサポートするようにCiscoコンテンツセキュリティ管理アプライアンスを設定すると、エンドユーザは一度サインインするだけで、スパム隔離を含むすべてのサービスにアクセスできます。

問題

[Download Metadata for SAML]を選択すると、次の図に示すように「Error occurred while retrieving metadata information」というエラーが表示されます。



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' configurations. The table has five columns: 'SP Profile Name', 'Entity ID', 'Assertion Consumer URL', 'Metadata', and 'Delete'. One row is visible with the following data: 'MyLab_SAML', 'sma.mexesa.com:83', 'https://sma.mexesa.com:83/', and a 'Download Metadata' button. Below the table, there is a section for 'Identity Provider' with an 'Add Identity Provider...' button and a message: '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	

解決方法

ステップ1: Eメールセキュリティアプライアンス(ESA)で新しい自己署名証明書を作成します。

図に示すように、共通名がエンティティID URLと同じであるが、ポート番号が付いていないことを確認します。

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

ステップ2 : 新しい証明書を.pfx拡張子でエクスポートし、パスワードを入力してマシンに保存します。

ステップ3:Windows端末を開き、これらのコマンドを入力して、前のステップのパスワードを入力します。

- 次のコマンドを実行して、秘密キーをエクスポートします。

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

- 次のコマンドを実行して、証明書をエクスポートします。

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

ステップ4 : このプロセスの最後に、2つの新しいファイルが必要です。

certificateprivatekey.pemおよび**certificate.pem**を使用します。両方のファイルをサービスプロバイダープロファイルにアップロードし、証明書のエクスポートに使用するのと同じパスワードを使用します。

ステップ5 : 図に示すように、SMAが動作するには、両方のファイルが.PEM形式である必要があります。

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

ステップ6:[Sign Assertions] チェックボックスがオンになっていることを確認します。

ステップ7: 変更を送信してコミットします。図に示すように、メタデータをダウンロードできる必要があります。

SAML

Service Provider

Add Service Provider...

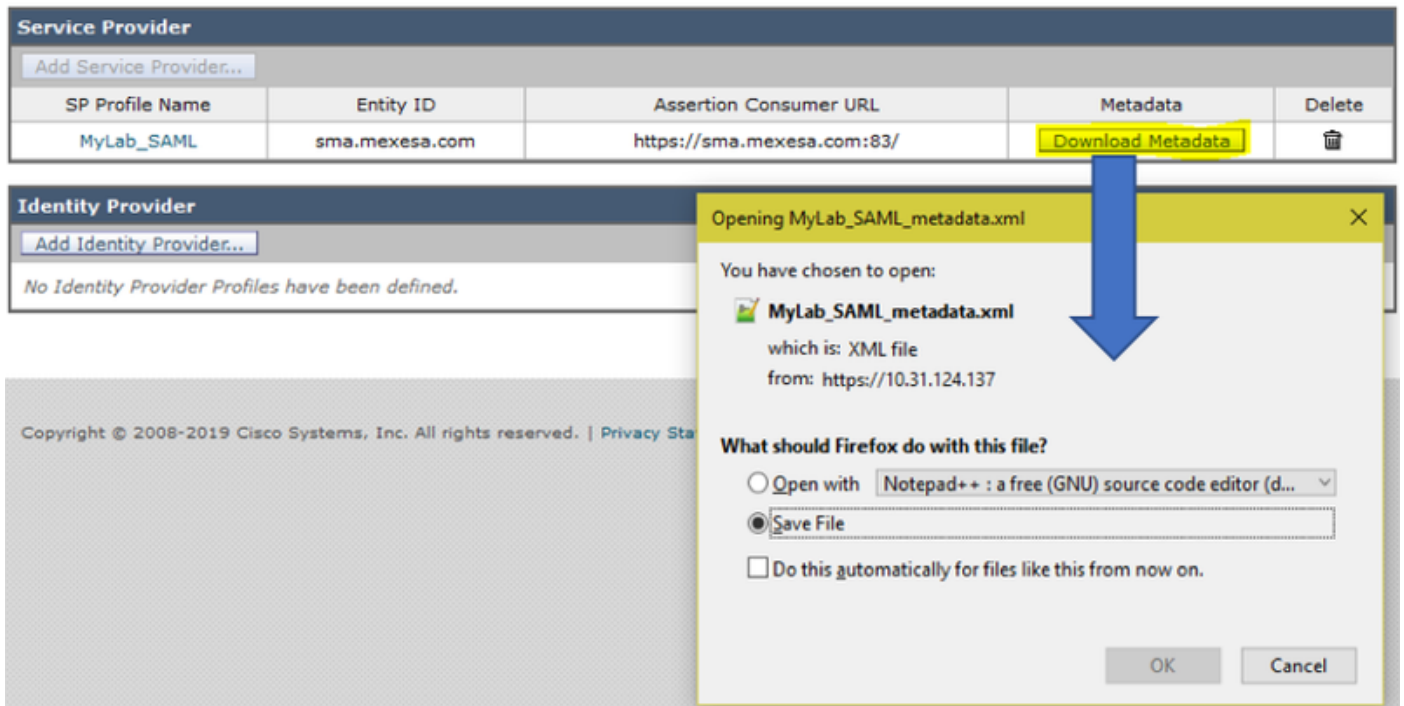
SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

Identity Provider

Add Identity Provider...

No Identity Provider Profiles have been defined.

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



Opening MyLab_SAML_metadata.xml

You have chosen to open:

MyLab_SAML_metadata.xml
which is: XML file
from: https://10.31.124.137

What should Firefox do with this file?

Open with Notepad++ : a free (GNU) source code editor (d...)

Save File

Do this automatically for files like this from now on.

OK Cancel

関連情報

- [AsyncOS 11.0 for Cisco Content Security Management Appliances ユーザガイド – GD \(一般導入\)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。