

Résoudre l'erreur « Une erreur s'est produite lors de la récupération des informations de métadonnées » pour SAML dans SMA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner l'erreur "Erreur survenue lors de la récupération des informations de métadonnées" pour le langage SAML (Security Assertion Markup Language) dans l'appliance de gestion de la sécurité (SMA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ADFS (Active Directory Federation Services)
- Intégration SAML avec SMA
- [OpenSSL](#) installé

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- SMA AsyncOs version 11.x.x
- SMA AsyncOs version 12.x.x

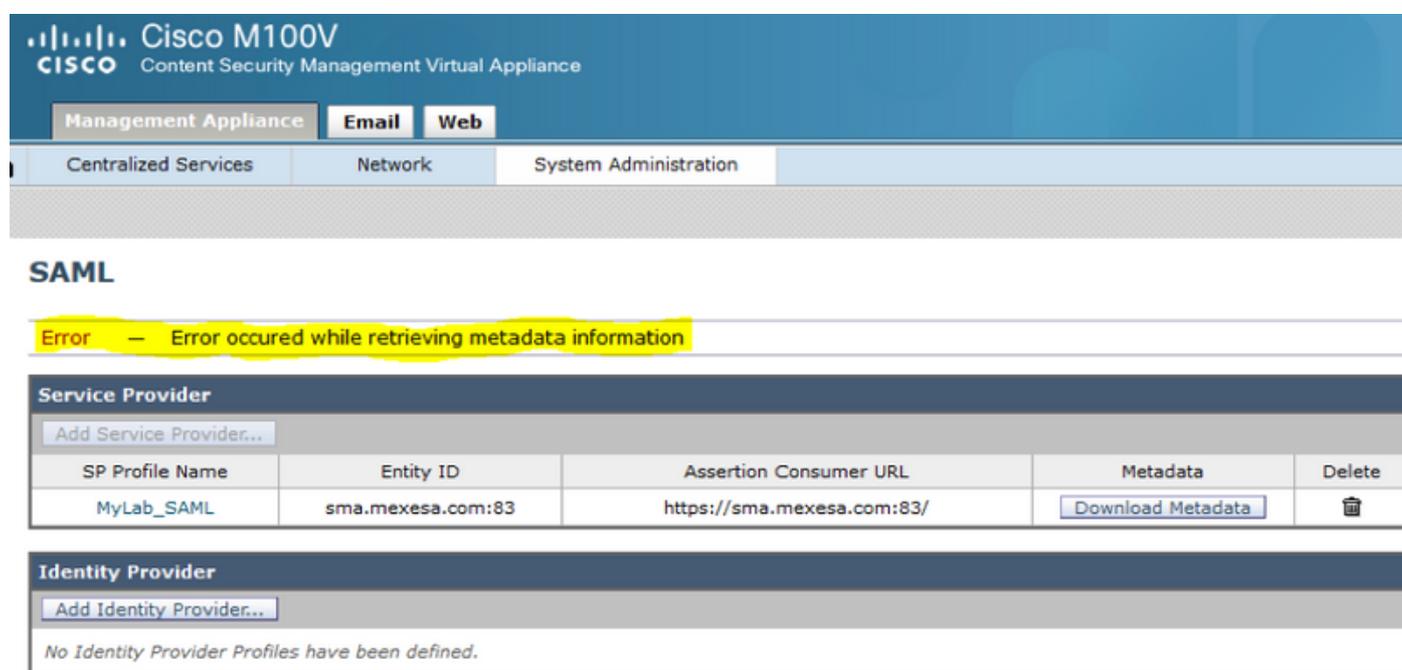
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Content Security Management Appliance prend désormais en charge l'authentification unique (SSO) SAML 2.0 afin que les utilisateurs finaux puissent accéder à la quarantaine du spam et utiliser les mêmes informations d'identification que celles utilisées pour accéder à d'autres services compatibles SSO SAML 2.0 au sein de leur organisation. Par exemple, vous activez l'identité Ping en tant que fournisseur d'identité SAML (IdP) et dispose de comptes sur Rally, Salesforce et Dropbox pour lesquels l'authentification unique SAML 2.0 est activée. Lorsque vous configurez l'appliance Cisco Content Security Management pour qu'elle prenne en charge l'authentification unique SAML 2.0 en tant que fournisseur de services (SP), les utilisateurs finaux peuvent se connecter une seule fois et avoir accès à tous ces services, y compris la quarantaine du spam.

Problème

Lorsque vous sélectionnez Télécharger les métadonnées pour SAML, vous obtenez l'erreur "Erreur survenue lors de la récupération des informations de métadonnées", comme indiqué dans l'image :



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 occured while retrieving metadata information'. Below the error message, there is a table of Service Providers. The table has columns for 'SP Profile Name', 'Entity ID', 'Assertion Consumer URL', 'Metadata', and 'Delete'. One entry is visible: 'MyLab_SAML' with Entity ID 'sma.mexesa.com:83' and Assertion Consumer URL 'https://sma.mexesa.com:83/'. A 'Download Metadata' button is present in the Metadata column for this entry. 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	

Solution

Étape 1 : création d'un certificat auto-signé sur l'appliance de sécurité de la messagerie (ESA)

Assurez-vous que le nom commun est identique à l'URL de l'ID d'entité, mais sans le numéro de port, comme indiqué dans l'image :



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

Étape 2. Exportez le nouveau certificat avec une extension .pfx, tapez une phrase de passe et enregistrez-la sur votre ordinateur.

Étape 3. Ouvrez un terminal Windows et entrez ces commandes, fournissez la phrase de passe de l'étape précédente.

- Exécutez la commande suivante pour exporter la clé privée :

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

- Exécutez cette commande pour exporter le certificat :

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

Étape 4. À la fin de ce processus, vous devez disposer de deux nouveaux fichiers : **certificateprivatekey.pem** et **certificate.pem**. Téléchargez les deux fichiers dans le profil de fournisseur de services et utilisez la même phrase de passe que pour exporter le certificat.

Étape 5. Le SMA nécessite que les deux fichiers soient au format .PEM pour fonctionner, comme illustré dans l'image.

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

Étape 6. Assurez-vous de cocher la case **Signer les assertions**.

Étape 7. Soumettez et validez les modifications, vous devez être en mesure de télécharger les métadonnées, comme indiqué dans l'image.

SAML

Service Provider

Add Service Provider...

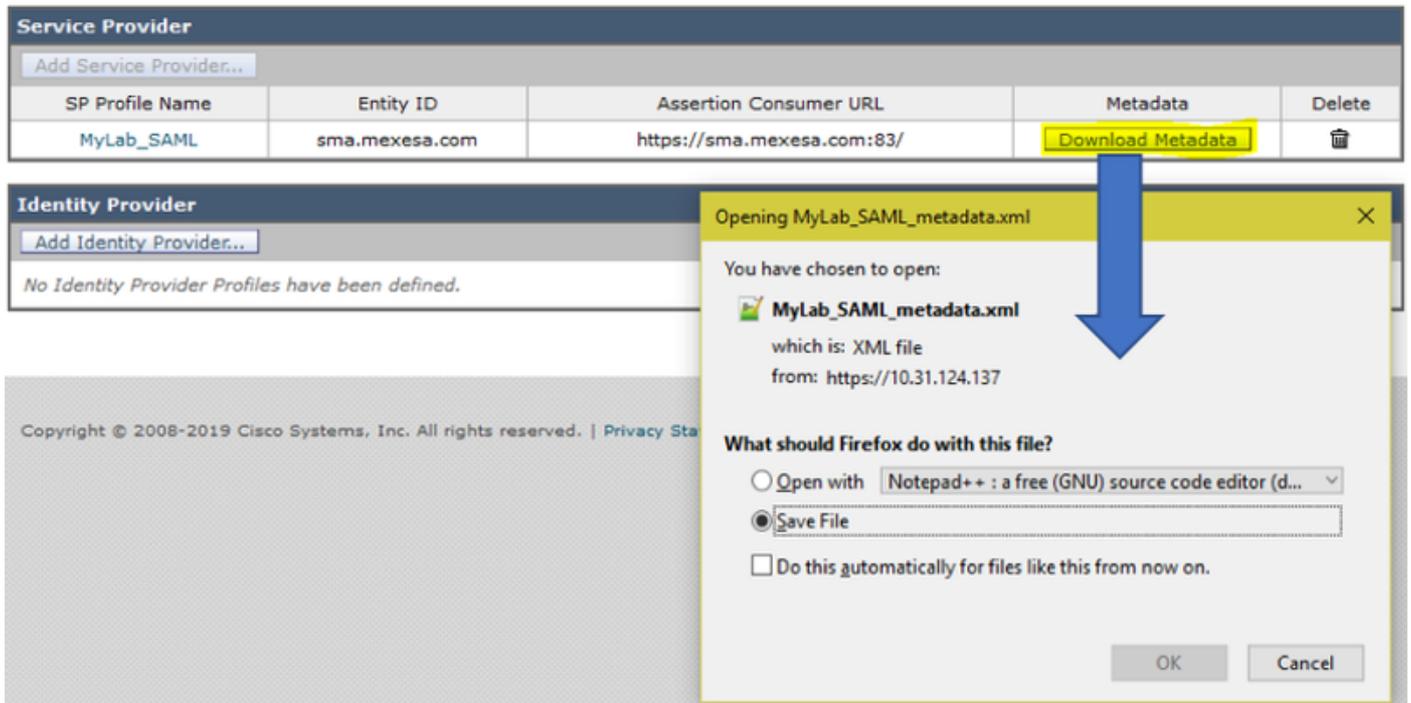
SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

Identity Provider

Add Identity Provider...

No Identity Provider Profiles have been defined.

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



Informations connexes

- [Guide de l'utilisateur d'AsyncOS 11.0 pour les appareils de gestion de la sécurité du contenu Cisco - GD \(General Deployment\)](#)
- [Support et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.