Contenu

Introduction

Ce document décrit comment adresser une modification qui s'est produite en mars 18, 2016 dans lesquels des web server qui hébergent tools.cisco.com ont été migrés vers un certificat SHA-2. Ensuite ce transfert, quelques périphériques d'ASAv ne se connectent pas au portail intelligent de licence logicielle (qui est hébergé sur tools.cisco.com) quand ils enregistrent un jeton d'ID ou tandis qu'ils tentent de renouveler des autorisations existantes. Ceci a été déterminée pour être une question liée au certificat. Spécifiquement, le nouveau certificat qui est présenté à l'ASAv est signé par une autorité de certification intermédiaire différente que l'ASAv prévoit et a préchargé.

Problème

Quand une tentative est faite pour enregistrer un ASAv au portail intelligent de licence logicielle, l'enregistrement échoue avec une panne de connexion ou de communication. Les commandes de **permis de profil d'enregistrement** et de **call-home test de show license** affichent ces sorties.

```
ASAv# show license registration        Registration Status: Retry In Progress.
Registration Start Time: Mar 22 13:25:46 2016 UTC        Registration Status: Retry In Progress.
Registration Start Time: Mar 22 13:25:46 2016 UTC        Last Retry Start Time: Mar 22 13:26:32
2016 UTC.        Next Scheduled Retry Time: Mar 22 13:45:31 2016 UTC.        Number of Retries:
1.        Last License Server response time: Mar 22 13:26:32 2016 UTC.        Last License
Server response message: Communication message send response errorASAv# call-home test profile
LicenseINFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...ERROR: Failed:
CONNECT_FAILED(35)
```

Cependant, l'ASAv peut résoudre tools.cisco.com et se connecter sur le port TCP 443 à un ping de TCP.

Syslog et sortie de débogage

La sortie de Syslog sur l'ASAv après un enregistrement tenté affichera ceci :

```
%ASA-3-717009: Certificate validation failed. No suitable trustpoints found to validate
certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:
cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc.
- For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=US, issuer name:
ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US .%ASA-3-717009:
Certificate validation failed. No suitable trustpoints found to validate
certificate serial number: 513FB9743870B73440418699FF, subject name:
cn=Symantec Class 3 Secure Server CA - G4,ou=Symantec Trust Network,o=Symantec
Corporation,c=US, issuer name: cn=VeriSign Class 3 Public Primary Certification Authority
- G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,
```

```
o=VeriSign\, Inc.,c=US .
```

Pour de plus amples informations, exécutez ces derniers met au point tandis que vous tentez un autre enregistrement. Des erreurs de Secure Socket Layer sont vues.

```
%ASA-3-717009: Certificate validation failed. No suitable trustpoints found to validate
certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:
cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc.
- For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=US, issuer name:
ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US .%ASA-3-717009:
Certificate validation failed. No suitable trustpoints found to validate
certificate serial number: 513FB9743870B73440418699FF, subject name:
cn=Symantec Class 3 Secure Server CA - G4,ou=Symantec Trust Network,o=Symantec
Corporation,c=US, issuer name: cn=VeriSign Class 3 Public Primary Certification Authority
- G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,
o=VeriSign\, Inc.,c=US .
```

Spécifiquement, ce message est vu en tant qu'élément de cette sortie :

```
%ASA-3-717009: Certificate validation failed. No suitable trustpoints found to validate
certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:
cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc.
- For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=US, issuer name:
ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US .%ASA-3-717009:
Certificate validation failed. No suitable trustpoints found to validate
certificate serial number: 513FB9743870B73440418699FF, subject name:
cn=Symantec Class 3 Secure Server CA - G4,ou=Symantec Trust Network,o=Symantec
Corporation,c=US, issuer name: cn=VeriSign Class 3 Public Primary Certification Authority
- G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,
o=VeriSign\, Inc.,c=US .
```

Dans la configuration par défaut d'ASAv, il y a un point de confiance appelé le _SmartCallHome_ServerCA qui a un certificat chargé et fourni serveur sécurisé CA de la classe 3 de cn=Verisign à nom du sujet le « - G3".

```
ASAv# show crypto ca certificateCA Certificate  Status: Available  Certificate Serial Number:
6ecc7aa5a7032009b8cebc2d491  Certificate Usage: General Purpose  Public Key Type: RSA (2048
bits)  Signature Algorithm: SHA1 with RSA Encryption  Issuer Name:     cn=VeriSign Class 3
Public Primary Certification Authority - G5    ou=(c) 2006 VeriSign\, Inc. - For authorized use
only    ou=VeriSign Trust Network    o=VeriSign\, Inc.    c=US  Subject Name:     cn=VeriSign
Class 3 Secure Server CA - G3    ou=Terms of use at https://www.verisign.com/rpa (c)10
ou=VeriSign Trust Network    o=VeriSign\, Inc.    c=US  OCSP AIA:     URL:
http://ocsp.verisign.com  CRL Distribution Points:     [1]  http://crl.verisign.com/pca3-g5.crl
Validity Date:     start date: 00:00:00 UTC Feb 8 2010    end   date: 23:59:59 UTC Feb 7 2020
Associated Trustpoints: _SmartCallHome_ServerCA
```

Cependant, dans les les Syslog précédents, l'ASA indique qu'elle obtient un certificat du portail intelligent de licence logicielle signé par un intermédiaire appelé « le serveur sécurisé CA de la classe 3 de cn=Symantec - G4".

> Remarque: Les noms du sujet sont semblables, mais ont deux différences ; Verisign contre Symantec au début et G3 contre G4 à l'extrémité.

Solution

L'ASAv doit télécharger un trustpool qui contient l'intermédiaire et/ou les certificats racine appropriés afin de valider la chaîne.

Dans la version 9.5.2 et ultérieures, l'ASAv a le trustpool automatique-importation configurée à l'heure locale de périphérique de 10:00 P.M. :

```
ASAv# sh run crypto ca trustpool
crypto ca trustpool policy
auto-import
ASAv# sh run all crypto ca trustpool
crypto ca trustpool policy
revocation-check none
crl cache-time 60
crl enforcenextupdate
auto-import
auto-import url http://www.cisco.com/security/pki/trs/ios_core.p7b
auto-import time 22:00:00
```

Si c'est une installation initiale, et des consultations et connexion Internet de Système de noms de domaine (DNS) n'ont pas été vers le haut de à ce moment-là encore, alors l'automatique-importation n'a pas réussi et doit être terminée manuellement.

Sur des versions plus anciennes, telles que 9.4.x, l'automatique-importation de trustpool n'est pas configurée sur le périphérique et doit être importée manuellement.

Sur n'importe quelle version, cette commande importe le trustpool et les Certificats appropriés :

```
ASAv# crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7bRoot file
signature verified.You are about to update the current trusted certificate poolwith the 17145
byte file at http://www.cisco.com/security/pki/trs/ios_core.p7bDo you want to continue?
(y/n)Trustpool import:   attempted:  14   installed:  14   duplicates: 0   expired:    0
failed:     0
```

Vérifiez

Une fois que le trustpool est importé par la commande manuelle, ou en attendant jusqu'après l'heure locale de 10:00 P.M., cette commande vérifie qu'il y a les Certificats installés dans le trustpool :

```
ASAv# show crypto ca trustpool policy14 trustpool certificates installedTrustpool auto import
statistics:    Last import result: FAILED    Next scheduled import at 22:00:00 UTC Wed Mar 23
2016Trustpool Policy   Trustpool revocation checking is disabled   CRL cache time: 60 seconds
CRL next update field: required and enforced   Automatic import of trustpool certificates is
enabled   Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b   Download
time: 22:00:00   Policy Overrides:      None configured
```

> Remarque: Dans le précédent sortez la dernière importation d'automatique-mise à jour a manqué puisque les DN n'étaient pas opérationnels la dernière fois où elle a tentée automatiquement, ainsi elle donne toujours le dernier résultat d'automatique-importation comme manqué. Cependant, une mise à jour manuelle de trustpool a été exécutée et a avec succès mis à jour le trustpool (qui est pourquoi il affiche 14 Certificats installés).

Après que le trustpool soit installé, la commande symbolique d'enregistrement peut être exécutée de nouveau afin d'enregistrer l'ASAv avec le portail intelligent de licence logicielle.

```
ASAv# license smart register idtoken id_token force
```

Si l'ASAv était déjà enregistré au portail intelligent de licence logicielle, mais les renouvellements d'autorisation manquaient, ceux peuvent également être tentés manuellement.

```
ASAv# license smart renew auth
```

Informations connexes

- Gestion de certificat intelligente de permis
- Configurez l'importation automatique des Certificats de Trustpool
- Support et documentation techniques - Cisco Systems