ASAv聪明的许可授权的失败由于证书握手失败

目录

[简介](#)
[问题](#)
[Syslog和Debug输出](#)
[解决方案](#)
[验证](#)
[相关信息](#)

简介

本文描述如何讨论在三月18发生， 2016网络服务器主机tools.cisco.com被移植到SHA-2证书的更改。以后迁移，一些ASAv设备不能连接到聪明的软件许可授权在tools.cisco.com主机)的门户(当他们注册ID标记时或，当他们尝试更新现有授权时。确定这是一个证书相关的问题。特别地，新证书比ASAv被提交对的ASAv由一不同的中间签字认证机关预计和预先了输入。

问题

当尝试做出注册ASAv到聪明的软件许可授权的门户时，注册失效与连接或通信故障。**显示许可证注册**和**呼叫到家测验配置文件准许**show命令这些输出。

```
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 error
ASAv# call-home test profile License
INFO: Sending test message to  https://tools.cisco.com/its/service/oddce/services/DDCEService...
ERROR: Failed: CONNECT_FAILED(35)
```

然而， ASAv在与TCP ping的TCP端口443能解决tools.cisco.com和连接。

Syslog和Debug输出

在ASAv的系统日志输出在一个已尝试注册以后将显示此：

```
%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 .

欲知详情，当您尝试另一个注册时，请运行这些调试。安全套接层错误被看到。

%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 .

特别地，作为该输出一部分，此消息被看到：

%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 .

在默认ASAv配置中，有呼叫有一证书装载和发出对主题名称“cn=Verisign等级3安全服务器CA - G3"的_SmartCallHome_ServerCA的信任点。

```
ASAv# show crypto ca certificate
CA 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
```

然而，在上一个Syslog， ASA表明从中间签字的聪明的软件许可授权的门户获得证书呼叫“cn=Symantec等级3安全服务器CA - G4"。

注意：主题名称是类似的，但是有两差异; Verisign与首先Symantec和G3与在末端的G4。

解决方案

ASAv需要下载包含适当的中间和根证明为了验证一系列的trustpool。

在版本9.5.2和以上， ASAv有trustpool配置的自动导入在下午10:00设备本地时间：

```
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
```

如果这是初始安装，并且域名系统(DNS)查找和Internet连接不是那时，则自动导入未成功并且需要手工完成。

在更旧的版本，例如9.4.x， trustpool自动导入在设备没有配置并且需要手工导入。

在所有版本，此命令导入trustpool和相关证书：

```
ASAv# crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b
Root file signature verified.
You are about to update the current trusted certificate pool
with the 17145 byte file at http://www.cisco.com/security/pki/trs/ios_core.p7b
Do you want to continue? (y/n)
Trustpool import:
   attempted:  14
   installed:  14
   duplicates: 0
   expired:    0
   failed:     0
```

验证

一旦trustpool导入由手工的命令，或者通过等待在下午10:00本地时间之后，此命令验证有在trustpool的安装的证书：

```
ASAv# show crypto ca trustpool policy
14 trustpool certificates installed
Trustpool auto import statistics:
    Last import result: FAILED
    Next scheduled import at 22:00:00 UTC Wed Mar 23 2016
Trustpool 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
```

注意：在上一个请输出自动地尝试失败的最后auto-update导入，因为DNS不是可操作的上次，因此仍然显示最后自动导入结果如失败。然而，一次手工的trustpool更新运行了和成功更新是的trustpool (为什么显示安装的14证书)。

在trustpool安装后，令牌的注册命令可以再运行为了注册与聪明的软件许可授权的门户的ASAv。

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

如果ASAv已经注册到聪明的软件许可授权的门户，但是失败的授权续订，那些可能手工也尝试。

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

相关信息

- 聪明的许可证证书管理
- 配置Trustpool证书自动导入
- 技术支持和文档 - Cisco Systems