ASA聪明的准许故障由于认证握手故障

Contents

Introduction

本文描述如何讨论发生2016年3月和2018年10月，网络服务器主机tools.cisco.com被移植到一个不同的根Certificate Authority (CA)认证的更改。以后该迁移，一些ASA (可适应的安全工具)设备不能连接到在tools.cisco.com主机)的聪明的软件准许门户(当他们注册一个ID令牌时或，当他们尝试更新现有的授权时。确定这是一个证书相关的问题。特别地，被提交对ASA的新证书由不同的中间CA比ASA签字预计和预先了输入。

问题

当尝试做出注册ASAv到聪明的软件准许门户时，注册失效与连接或通信故障。**显示许可证注册**和**呼叫到家测试配置文件许可证**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TCP端口443能解决tools.cisco.com和连接用TCP ping。

系统日志和调试输出

在ASAv的系统日志输出在一个尝试的注册以后将显示此：

%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，请运行这些调试指令。获取套接层错误被看到。

%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，有称为有一个认证被装载和被发行对主题名称“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，在早先Syslog， ASA表明从中间签字的聪明的软件准许门户获得认证称为“cn=Symantec等级3安全服务器CA - G4"。

Note:主题名称是类似的，但是有两个区别; 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被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
```

如果这是一次初始安装，并且域名系统(DNS)查找和互联网连通性不是那时，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被配置并且需要手工被导入。

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
```

Verify

一旦等待导入trustpool被手工的命令或在下午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
```

Note:在早先请输出自动地尝试失效的最后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发生故障。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)。

在安装后trustpool，令牌的注册命令可以再运行为了注册与聪明的软件准许门户的ASAv。

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

如果ASAv已经注册对聪明的软件准许门户，但是发生故障的授权续订，那些可能手工也尝试。

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

根CA证书更改- 2018年10月

tools.cisco.com的在星期五，根CA证书更改了， 2018年10月5日。

如果对http://www.cisco.com/security/pki/trs/ios_core.p7b的通信不允许， 2100's运行ASA的当前配置的ASAv的版本9.6(2)和以上和Firepower不会受此更改的影响。 有默认情况下在以前被提及的所有ASA巧妙的准许的平台被启用的认证自动导入功能。 输出“显示crypto加州trustpool’包含“QuoVadis根CA 2'认证：

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

对于新的配置，您能发出“crypto加州trustpool导入默认’命令和下载包含QuoVadis cert的默认Cisco cert套件。 如果那不工作您能手工安装cert ：

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

4100/9300运行ASA的平台

此问题影响运行ASA依靠Firepower可扩展操作系统在字段的一些4100/9300s (FXO)提供聪明的许可证信息：

受影响的单元：

```
FP9300-1-A-A-A /license # show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: CALO
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC
  Last Renewal Attempt: FAILED on Oct 09 17:32:59 2018 UTC
    Failure reason: Failed to authenticate server
```

解决方法步骤

要解决，您在FXO需要创建一新的信任点和送进身份验证数据：

```
FPR-2-A /license # scope security
FPR-2-A /security # enter trustpoint quovadis
FPR-2-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:    (THIS PART NEEDS TO BE COPY/PASTED)
>
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
>ENDOFBUF <---manually type this on a new line after the ----END OF CERTIFICATE---- line and
press ENTER
```

其次，请确认更改然后更新许可证：

```
FPR-2-A /license # scope security
FPR-2-A /security # enter trustpoint quovadis
FPR-2-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:    (THIS PART NEEDS TO BE COPY/PASTED)
>
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
>ENDOFBUF <---manually type this on a new line after the ----END OF CERTIFICATE---- line and
press ENTER
```

您应该当前验证准许被更新了：

```
FP9300-1-A-A-A /license/licdebug # show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
```

```
  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: CALO
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC
  Last Renewal Attempt: SUCCEEDED on Oct 09 17:39:07 2018 UTC
  Next Renewal Attempt: Apr 07 17:39:08 2019 UTC
  Registration Expires: Oct 09 17:33:07 2019 UTC

License Authorization:
  Status: AUTHORIZED on Oct 09 17:39:12 2018 UTC
  Last Communication Attempt: SUCCESS on Oct 09 17:39:12 2018 UTC
  Next Communication Attempt: Nov 08 17:39:12 2018 UTC
  Communication Deadline: Jan 07 17:33:11 2019 UTC
```

Related Information

- 聪明的许可证证书管理
- 配置Trustpool证书自动导入
- Technical Support & Documentation - Cisco Systems