ASA Smart Licensing Fails vanwege fouten in certificaathandleiding

Inhoud

Inleiding

Dit document beschrijft hoe een verandering moet worden aangepakt die plaatsvond op 1 maart 2016 en oktober 2018, waarin webservers die tools.cisco.com konden ontvangen, zijn gemigreerd naar een ander certificaat van de wortelautoriteit (CA). Na die migratie maken sommige ASA-apparaten (Adaptieve security applicatie) geen verbinding met het Smart Software Licensing Portal (dat wordt gehost door tools.cisco.com) wanneer ze een ID-token registreren of terwijl ze proberen bestaande licenties te vernieuwen. Dit werd vastgesteld als een afgifte van certificaten. Met name het nieuwe certificaat dat aan de ASA wordt voorgelegd, wordt ondertekend door een andere tussenpersoon dan de ASA verwacht en vooraf geladen.

Probleem

Wanneer een poging wordt gedaan om een ASAv te registreren bij het Smart Software Licensing Portal, mislukt de registratie bij een verbinding of communicatiestoornis. De opdrachten **voor** de **licentieregistratie van** de **show** en de **Call-home testprofiellicentie** tonen deze outputs.

```
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)
```

Maar de ASAv kan tools.cisco.com oplossen en verbinding maken met TCP poort 443 met een

TCP-ping.

Syslogs en debug-uitvoer

De Syslog-output van de ASAv na de poging tot registratie zal dit aantonen:

```
%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 .
```

Start deze debug-opdrachten voor meer informatie terwijl u een andere registratie probeert. Secure Socket Layer foutjes worden gezien.

```
debug license 255
debug license agent all
debug call-home all
debug ssl 255
```

Dit bericht wordt met name gezien als onderdeel van de output:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
failed@s3_clnt.c:1492
```

In de standaard ASAv-configuratie is er een betrouwbaar punt genaamd _SmartCallHome_ServerCA dat een certificaat heeft geladen en dat is afgegeven aan de onderwerpregel "cn=Versiing Class 3 Secure Server CA - G3".

```
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
```

In de vorige syslogs geeft de ASA echter aan dat er een certificaat is aangeschaft van het Smart Software Licensing Portal dat is ondertekend door een tussenpersoon genaamd "cn=Symantec Class 3 Secure Server CA - G4".

> Opmerking: De onderwerpnamen zijn vergelijkbaar, maar hebben twee verschillen: Verising vs. Symantec aan het begin en G3 vs. G4 aan het eind.

Oplossing

De ASAv moet een trustpool downloaden die de juiste intermediaire en/of wortelcertificaten bevat om de keten te valideren.

In versie 9.5.2 en later is de ASAv de trustpool ingesteld voor automatisch importeren op lokale tijd van 10:00 PM:

```
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
```

Als dit een eerste installatie is, en de raadpleging van het Domain Name System (DNS) en de internetconnectiviteit op dat moment nog niet zijn geïnstalleerd, dan is de auto-invoer niet geslaagd en moet handmatig worden voltooid.

Op oudere versies, zoals 9.4.x, wordt de automatische invoer van de trustpool niet op het apparaat ingesteld en moet handmatig worden geïmporteerd.

In elke versie importeert deze opdracht de trustpool en relevante certificaten:

```
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
```

Verifiëren

Zodra de trustpool wordt geïmporteerd door de handleiding of door te wachten tot na 10:00 uur lokale tijd, controleert deze opdracht of er geïnstalleerde certificaten in de trustpool zijn geïnstalleerd:

```
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
```

> Opmerking: In de vorige uitvoer is de laatste invoer zonder automatische bijwerking mislukt omdat DNS niet automatisch actief was, zodat de laatste keer dat deze werd gepoogd nog steeds het laatste resultaat van de auto-import wordt weergegeven als er niets is gebeurd. Er werd echter een handmatige update van de trustpool uitgevoerd en deze werd met succes bijgewerkt (zodat wordt aangegeven dat er 14 geïnstalleerde certificaten zijn geïnstalleerd).

Nadat de trustpool is geïnstalleerd, kan de penning-registratieopdracht opnieuw worden uitgevoerd om de ASAv te registreren bij het Smart Software Licensing Portal.

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

Als de ASAv al was geregistreerd op het Smart Software Licensing Portal, maar de vernieuwing van de toestemming is mislukt, kunnen deze ook handmatig worden geprobeerd.

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

Root CA-certificaatwijziging - oktober 2018

De basis CA certificaat voor tools.cisco.com werd gewijzigd op vrijdag 5 oktober 2018.

De huidige ASAv's versie 9.6(2) en later en Firepower 2100's actieve ASA zullen niet door deze verandering worden beïnvloed als communicatie naar http://www.cisco.com/security/pki/trs/ios_core.p7b niet is toegestaan. Er is een optie voor het automatisch importeren van certificaten die standaard is ingeschakeld voor alle ASA Smart Licensed platforms die eerder worden genoemd. De output van "show crypto ca trustpool" bevat het "QuoVadis Root CA 2"-certificaat:

```
CA Certificate
  Fingerprint: 5e397bddf8baec82e9ac62ba0c54002b
  Issuer Name:
```

```
    cn=QuoVadis Root CA 2
    o=QuoVadis Limited
    c=BM
  Subject Name:
    cn=QuoVadis Root CA 2
    o=QuoVadis Limited
    c=BM
```

Voor nieuwe implementaties kunt u de opdracht "crypto ca trustpool import default" uitgeven en de standaard Cisco cert bundel met de QuoVadis cert downloaden. Als dat niet werkt kunt u de cert handmatig installeren:

```
asa(config)# crypto ca trustpoint QuoVadisRootCA2
asa(config-ca-trustpoint)# enrollment terminal
asa(config-ca-trustpoint)# crl configure
asav(config-ca-crl)# crypto ca authenticate QuoVadisRootCA2
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----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-----

quit

INFO: Certificate has the following attributes:
Fingerprint:     5e397bdd f8baec82 e9ac62ba 0c54002b
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

4100/9300 platforms die ASA uitvoeren

Dit probleem heeft invloed op ongeveer 4100/9300 s in het veld die ASA uitvoeren dat afhankelijk is van Firepower eXtensible Operating System (FXOS) om slimme Licentie-informatie te leveren:

Betrokken eenheid:

```
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
```

Resolutie

Om op te lossen, moet u een nieuw betrouwbaar punt maken en de certificaatgegevens in FXOS invoeren:

```
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
```

Daarna moet u de wijziging doorvoeren en de licentie verlengen:

```
FPR-2-A /security/trustpoint* # comm
FPR-2-A /security/trustpoint # scope license
FPR-2-A /license # scope licdebug
FPR-2-A /license/licdebug # renew
```

U dient nu te controleren of de licentie is verlengd:

```
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
```

Gerelateerde informatie

- Smart Licentiebeheer
- Automatische invoer van Trustpool-certificaten instellen
- Technische ondersteuning en documentatie – Cisco Systems