# Licenciar de ASAv Smart falhas devido para certificate a falha do aperto de mão

## Índice



## Introdução

Este documento descreve como endereçar uma mudança que ocorra em março 18, 2016 em que os web server que hospedam tools.cisco.com foram migrados a um certificado SHA-2. Em seguida essa migração, alguns dispositivos de ASAv não conecta ao portal esperto licenciar do software (que está hospedado em tools.cisco.com) quando registra um token ID ou quando tentar renovar autorizações existentes. Esta foi determinada ser uma edição certificado-relacionada. Especificamente, o certificado novo que é apresentado ao ASAv é assinado por um Certificate Authority intermediário diferente do que o ASAv espera e preloaded.

## Problema

Quando uma tentativa é feita para registrar um ASAv ao portal esperto licenciar do software, o registro falha com uma conexão ou uma falha de comunicação. **O registro de licença da mostra** e os **comandos license call-home do perfil do teste** mostram estas saídas.

```
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)
```

Contudo, o ASAv pode resolver tools.cisco.com e conectá-lo na porta TCP 443 com um sibilo TCP.

### Saída dos syslog e debug

As saídas de SYSLOG no ASAv após um registro tentado mostrarão esta:

```
%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 .
```

Para mais informações, execute estes debuga quando você tentar um outro registro. Os erros de Secure Socket Layer são considerados.

```
%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 .
```

Especificamente, esta mensagem é considerada como parte dessa saída:

```
%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 .
```

Na configuração de ASAv do padrão, há um ponto confiável chamado o _SmartCallHome_ServerCA que tem um certificado carregado e emitido servidor seguro CA da classe 3 cn=Verisign ao nome do sujeito do “- 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
```

Contudo, o nos Syslog precedentes, o ASA indica que obtém um certificado do portal esperto licenciar do software assinado por um intermediário chamado do “servidor seguro CA da classe 3 cn=Symantec - G4".

> Nota: Os nomes do sujeito são similares, mas têm duas diferenças; Verisign contra Symantec no início e G3 contra o G4 na extremidade.

# Solução

O ASAv precisa de transferir um trustpool que contenha o intermediário e/ou os certificados de raiz apropriados a fim validar a corrente.

Na versão 9.5.2 e mais recente, o ASAv tem a auto-importação configurada trustpool no horário local do dispositivo de 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
```

Se esta é uma instalação inicial, e as consultas do Domain Name System (DNS) e a conectividade de Internet não foram acima de naquele tempo ainda, a seguir a auto-importação não sucedeu e precisa de ser terminada manualmente.

Em umas versões mais velhas, tais como 9.4.x, a auto-importação do trustpool não é configurada no dispositivo e precisa de ser importada manualmente.

Em toda a versão, este comando importa o trustpool e os Certificados relevantes:

```
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
```

# Verificar

Uma vez que o trustpool é importado pelo comando manual, ou esperando até depois do horário local de 10:00 PM, este comando verifica que há Certificados instalados no trustpool:

```
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
```

> Nota: No precedente output a última importação da atualização automática falhada desde que o DNS não era operacional a última vez onde tentou automaticamente, assim que ainda mostra o último resultado da auto-importação como falhado. Contudo, uma atualização manual do trustpool foi executada e atualizou com sucesso o trustpool (que é porque mostra 14 Certificados instalados).

Depois que o trustpool é instalado, o comando simbólico do registro pode ser executado outra vez a fim registrar o ASAv com o portal esperto licenciar do software.

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

Se o ASAv foi registrado já ao portal esperto licenciar do software, mas às renovações da autorização falhadas, aqueles podem igualmente ser tentados manualmente.

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

# Informações Relacionadas

- Gerenciamento certificado esperto da licença
- Configurar a auto importação de Certificados de Trustpool
- Suporte Técnico e Documentação - Cisco Systems