Содержание

Введение

Этот документ описывает, как обратиться к изменению , которое произошло 18 марта 2016, в которых, веб-серверах что tools.cisco.com хоста были перемещены на сертификат SHA 2. После той миграции некоторые устройства ASAv не в состоянии соединяться с Умным Порталом Лицензирования программного обеспечения (который размещен на tools.cisco.com), когда они регистрируют маркер ID или в то время как они пытаются возобновить существующие авторизации. Это было полно решимости быть связанной с сертификатом проблемой. В частности новый сертификат, который представлен ASAv, подписан другим Промежуточным Центром сертификации, чем ASAv ожидает и предварительно загрузил.

Проблема

Когда попытка предпринята для регистрации ASAv к Умному Порталу Лицензирования программного обеспечения, регистрационным сбоям с соединением или сбоем связи. **Регистрация show license** и команды **лицензии профиля call-home test** показывают эти выходные данные.

```
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)
```

Однако ASAv может решить tools.cisco.com и подключение на порте TCP 443 с эхо-запросом TCP.

Системные журналы и выходные данные отладки

Вывод системного журнала на ASAv после предпринятой регистрации покажет это:

```
%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 .
```

Для получения дополнительной информации выполните эти отладки при попытке другой регистрации. Ошибки Уровня защищенных сокетов замечены.

```
%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 .
```

В частности это сообщение замечено как часть тех выходных данных:

```
%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 .
```

В конфигурации ASAv по умолчанию существует точка доверия, названная _SmartCallHome_ServerCA, которому загрузили сертификат и выполненный к имени субъекта "cn=Verisign Защищенный сервер Класса 3 CA - 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
```

Однако в предыдущие системные журналы, ASA указывает, что это получает сертификат от Умного Портала Лицензирования программного обеспечения, подписанного промежуточным звеном, вызванным "cn=Symantec Защищенный сервер Класса 3 CA - G4".

> **Примечание:** Имена субъекта подобны, но имеют два различия; Verisign по сравнению с Symantec вначале и G3 по сравнению с G4 в конце.

Решение

ASAv должен загрузить trustpool, который содержит надлежащее промежуточное звено и/или корневые сертификаты для проверки цепочки.

В Версии 9.5.2 и позже, ASAv настроили trustpool для автоимпортирования в 22:00 местного времени устройства:

```
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
```

Если это - начальная установка, и Поиски в системе доменных имен (DNS) и интернет-соединение еще не были подключены в то время, то автоимпорт не успешно выполнился и должен быть завершен вручную.

На более старых версиях, такой как 9.4.x, автоимпорт trustpool не настроен на устройстве и должен быть импортирован вручную.

На любой версии эта команда импортирует trustpool и соответствующие сертификаты:

```
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
```

Проверка

Как только trustpool импортирован или ручной командой, или путем ожидания до окончания 22:00 по местному времени, эта команда проверяет , что существуют установленные сертификаты в 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
```

> **Примечание:** В предыдущих выходных данных отказал последний импорт автоматического обновления, так как DNS не был в рабочем состоянии прошлый раз, это попыталось автоматически, таким образом, это все еще показывает последний результат автоимпорта, как подведено. Однако руководство trustpool обновление было выполнено и действительно успешно обновляло trustpool (который является, почему это показывает 14 установленных сертификатов).

После того, как trustpool установлен, маркерная регистрационная команда может быть выполнена снова для регистрации ASAv в Умном Портале Лицензирования программного обеспечения.

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

Если ASAv был уже зарегистрирован к Умному Порталу Лицензирования программного обеспечения, но обновления авторизации отказали, те могут также быть предприняты

вручную.

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

Дополнительные сведения

- Умное управление сертификатами лицензии
- Настройте автоматический импорт сертификатов Trustpool
- Cisco Systems – техническая поддержка и документация