Fallas debido de autorización elegantes de ASAv para certificar el error del apretón de manos

Contenido

Introducción

Este documento describe cómo dirigir un cambio que ocurrió en marzo 18, 2016 en los cuales los web server que reciben tools.cisco.com fueron emigrados a un certificado SHA-2. Después esa migración, algunos dispositivos de ASAv no puede conectar con el portal elegante de la autorización del software (que se recibe en tools.cisco.com) cuando él registra un token ID o mientras que él intenta renovar las autorizaciones existentes. Éste fue determinado para ser un problema certificado-relacionado. Específicamente, el nuevo certificado que se presenta al ASAv es firmado por un diverso Certificate Authority intermedio que el ASAv espera y ha cargado.

Problema

Cuando una tentativa se hace para registrar un ASAv al portal elegante de la autorización del software, el registro falla con una conexión o una falla de comunicación. **Los comandos license del perfil de la prueba del registro de la licencia** y de la **llamada casera de la demostración** muestran estas salidas.

```
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)
```

Sin embargo, el ASAv puede resolver tools.cisco.com y conectar en el puerto TCP 443 con un ping TCP.

Salida de los syslog y debug

La salida de Syslog en el ASAv después de un registro frustrado mostrará esto:

%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 más información, ejecute estos debugs mientras que usted intenta otro registro. Se consideran los errores de Secure Socket Layer.

%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 .

Específicamente, este mensaje se considera como parte de esa salida:

%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 .

En la configuración predeterminada de ASAv, hay un trustpoint llamado el _SmartCallHome_ServerCA que tiene un certificado cargado y publicado servidor seguro CA de la clase 3 del cn=Verisign al asunto “- el 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
```

Sin embargo, en el Syslog anteriores, el ASA indica que consigue un certificado del portal elegante de la autorización del software firmado por un intermedio llamado “servidor seguro CA de la clase 3 del cn=Symantec - el G4".

> Nota: Los asuntos son similares, pero tienen dos diferencias; Verisign contra Symantec al principio y G3 contra el G4 en el extremo.

Solución

El ASAv necesita descargar un trustpool que contenga el intermedio y/o los certificados raíz apropiados para validar el encadenamiento.

En la versión 9.5.2 y posterior, el ASAv tiene la auto-importación configurada trustpool en la hora local del 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
```

Si esto es una instalación inicial, y las búsquedas del Sistema de nombres de dominio (DNS) y la conectividad a Internet no han estado encima de en aquel momento todavía, después la auto-importación no ha tenido éxito y necesita ser completada manualmente.

En las versiones anteriores, tales como 9.4.x, la auto-importación del trustpool no se configura en el dispositivo y necesita ser importada manualmente.

En cualquier versión, este comando importa el trustpool y los 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
```

Verificación

Una vez que el trustpool es importado por el comando manual, o esperando hasta después de la hora local de 10:00 PM, este comando verifica que haya Certificados instalados en el 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: En el anterior haga salir la importación más reciente del automóvil Update Button fallada puesto que el DNS no era operativo la última vez que intentó automáticamente, así que todavía muestra el resultado más reciente de la auto-importación según lo fallado. Sin embargo, una actualización manual del trustpool fue funcionada con y puso al día con éxito el trustpool (que es porqué muestra 14 Certificados instalados).

Después de que el trustpool esté instalado, el comando simbólico del registro se puede funcionar con otra vez para registrar el ASAv con el portal elegante de la autorización del software.

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

Si el ASAv fue registrado ya al portal elegante de la autorización del software, pero a las renovaciones de la autorización falladas, ésos se pueden también intentar manualmente.

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

Información Relacionada

- Administración de certificados elegante de la licencia
- Importación auto de la configuración de los Certificados de Trustpool
- Soporte Técnico y Documentación - Cisco Systems