Pasos para renovar un certificado autofirmado caducado en Cyber Vision Center

Contenido

Introducción

En este documento se describen los pasos necesarios para renovar un certificado autofirmado (SSC) caducado en un Cisco Cyber Vision Center.

Problema

Los certificados utilizados por el centro para la comunicación con los sensores para la interfaz web (si no hay un certificado externo) se generan al inicio del centro y son válidos durante **2 años** (con un período de gracia adicional de 2 meses). Una vez alcanzado el tiempo, los sensores ya no podrán conectarse al centro, mostrando el siguiente tipo de errores en los registros:

```
2023-08-04T09:47:53+00:00 c4819831-bf01-4b3c-b127-fb498e50778d sensorsyncd[1]: 04/08/2023 09:47:53 senso
```

Además, si se conecta a la interfaz de usuario web, se mostrará un error o se bloqueará en función del navegador web si no hay ningún certificado externo en uso.

Solución

Es aplicable para la versión 4.2.x. Para las versiones 4.2.1 y posteriores, también se puede realizar desde la GUI web.

Pasos para regenerar el certificado del centro

1. Validar el certificado actual

```
root@center:~# openssl x509 -subject -startdate -enddate -noout -in /data/etc/ca/center-cert.pem
subject=CN = CenterDemo
notBefore=Aug 8 11:42:30 2022 GMT
notAfter=Oct 6 11:42:30 2024 GMT
```

2. Genere un nuevo certificado
Debe utilizar el nombre común (del campo "subject=CN") obtenido del paso anterior para generar el nuevo

certificado

```
root@center:~# sbs-pki --newcenter=CenterDemo
6C89E224EBC77EF6635966B2F47E140C
```

3. Reinicie el centro.

En las implementaciones con centros locales y centros globales, es fundamental anular el registro de los centros locales e inscribirlos de nuevo.

Pasos para regenerar el certificado del sensor

Si el certificado del centro ha caducado, es posible que algunos certificados de sensor estén a punto de caducar, ya que también son válidos 2 años desde el momento en que se crea el sensor en el centro.

- Para los sensores instalados con la extensión, la redistribución utilizará un nuevo certificado.
- Para los sensores que se han desplegado manualmente:

1. Genere un nuevo certificado en el centro con el número de serie del sensor:

```
root@center:~# sbs-pki --newsensor=FCWTEST
326E50A526B23774CBE2507D77E28379
```

Observe la ID devuelta por el comando

2. Obtenga la identificación del sensor para este sensor

```
root@center:~# sbs-sensor list
c6e38190-f952-445a-99c0-838f7b4bbee6
    FCWTEST (serial number=FCWTEST)
    version:
    status: ENROLLED
    mac:
    ip:
    capture mode: optimal
    model: IOX
    hardware:
    first seen on 2022-08-09 07:23:15.01585+00
    uptime 0
    last update on: 0001-01-01 00:00:00+00â€‹
```

3. Actualice la base de datos del sensor con el ID de certificado

```
root@center:~# sbs-db exec "UPDATE sensor SET certificate_serial='326E50A526B23774CBE2507D77E28379' WHEF
UPDATE 1
```

El número de serie del certificado debe ser el valor obtenido en el primer paso e identificar la ID del sensor del sensor

4. Descargue el paquete de aprovisionamiento para este sensor desde la GUI web

5. Rehaga la implementación con este paquete de aprovisionamiento

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).