Etapas para renovar um certificado autoassinado expirado no Cyber Vision Center

Contents

Introdução

Este documento descreve as etapas envolvidas para renovar um certificado autoassinado (SSC) expirado em um Cisco Cyber Vision Center.

Problema

Os certificados utilizados pelo centro para a comunicação com os sensores da interface web (se não houver certificado externo) são gerados na primeira inicialização do centro e são válidos por **2 anos** (com um período de carência adicional de 2 meses). Uma vez atingido o tempo, os sensores não poderão mais se conectar ao centro, mostrando os seguintes tipos de erros nos registros:

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

Além disso, a conexão com a interface do usuário da Web exibirá um erro ou será bloqueada, dependendo do navegador da Web, se não houver certificado externo em uso.

Solução

Aplicável à versão 4.2.x. Nas versões 4.2.1 e posteriores, isso também pode ser feito na GUI da Web.

Etapas para gerar novamente o Certificado Central

1. Validar o certificado atual

```
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. Gerar um novo certificado
Você deve usar o Nome comum (do campo "subject=CN") obtido na etapa anterior para gerar o novo certificado

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

3. Reinicialize o Centro.

Em implantações com o Local Center e o Global Center, é essencial cancelar o registro dos Centros Locais e reinscrevê-los.

Etapas para regenerar o Certificado do Sensor

Se o certificado do centro tiver expirado, é possível que alguns certificados do sensor estejam prestes a expirar, pois eles também são válidos 2 anos a partir do momento em que o sensor é criado no centro.

- Para sensores instalados com a extensão, a reimplantação usará um novo certificado.
- Para sensores que foram implantados manualmente:

1. Gere um novo certificado no centro com o número de série do sensor:

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

Observe o ID retornado pelo comando

2. Obtenha o ID do 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. Atualizar o banco de dados para o sensor com a ID do certificado

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

O número de série do certificado deve ser o valor obtido da primeira etapa e id a identificação do sensor

4. Baixe o pacote de provisionamento para este sensor na GUI da Web

5. Refazer a implantação com este pacote de provisionamento

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.