

Étapes de renouvellement d'un certificat auto-signé expiré dans Cyber Vision Center

Table des matières

[Introduction](#)

[Problème](#)

[Solution](#)

[Étapes de régénération du certificat du centre](#)

[Étapes de régénération du certificat de capteur](#)

Introduction

Ce document décrit les étapes impliquées pour renouveler un certificat auto-signé (SSC) expiré sur un centre Cisco Cyber Vision Center.

Problème

Les certificats utilisés par le centre pour communiquer avec les capteurs de l'interface Web (s'il n'y a pas de certificat externe) sont générés au premier démarrage du centre et sont valides pendant **2 ans** (avec un délai de grâce supplémentaire de 2 mois). Une fois l'heure atteinte, les capteurs ne pourront plus se connecter au centre, affichant les types d'erreurs suivants dans les journaux :

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

En outre, la connexion à l'interface utilisateur Web affichera une erreur ou sera bloquée en fonction du navigateur Web si aucun certificat externe n'est utilisé.

Solution

Il s'applique à la version 4.2.x. Pour les versions 4.2.1 et ultérieures, il est également possible de le faire à partir de l'interface utilisateur graphique Web.

Étapes de régénération du certificat du centre

1. Valider le certificat actuel

```
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. Générez un nouveau certificat

Vous devez utiliser le nom commun (du champ « subject=CN ») obtenu à l'étape précédente pour générer le nouveau certificat

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

3. Redémarrez le Centre.

Pour les déploiements avec Local Center et Global Center, il est essentiel de désinscrire les Local Centers et de les réinscrire.

Étapes de régénération du certificat de capteur

Si le certificat du centre a expiré, il est possible que certains certificats de capteur arrivent à expiration, car ils sont également valides 2 ans après la création du capteur dans le centre.

- Pour les capteurs installés avec l'extension, le redéploiement utilisera un nouveau certificat.
- Pour les capteurs qui ont été déployés manuellement :

1. Générez un nouveau certificat sur le centre avec le numéro de série du capteur :

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

Notez l'ID renvoyé par la commande

2. Obtenir l'ID du capteur pour ce capteur

```
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+00
```

3. Mettez à jour la base de données du capteur avec l'ID de certificat

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

La série du certificat doit correspondre à la valeur obtenue lors de la première étape et à l'id du capteur

4. Téléchargez le package de mise en service pour ce capteur à partir de l'interface utilisateur graphique Web

5. Répétez le déploiement avec ce package de mise en service

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.