

Stappen om een verlopen zelfondertekend certificaat in Cyber Vision Center te verlengen

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Stappen om het Center Certificate te regenereren](#)

[Stappen om het sensorcertificaat te regenereren](#)

Inleiding

Dit document beschrijft de stappen in kwestie om een verlopen zelfondertekend certificaat (SSC) op een Cisco Cyber Vision Center te verlengen.

Probleem

Certificaten die door het centrum worden gebruikt voor communicatie met de sensoren voor de webinterface (indien er geen extern certificaat is) worden gegenereerd bij de eerste start van het centrum en zijn geldig voor **2 jaar** (met een extra respijtperiode van 2 maanden). Zodra de tijd is bereikt, zullen de sensoren niet meer met het centrum kunnen verbinden, die de volgende soorten fouten in de logboeken tonen:

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

Bovendien zal verbinding maken met de web-UI een fout weergeven of worden geblokkeerd afhankelijk van de webbrowser als er geen extern certificaat in gebruik is.

Oplossing

Het is van toepassing voor versie 4.2.x. Voor versies 4.2.1 en hoger kan dit ook via de Web GUI.

Stappen om het Center Certificate te regenereren

1. Het huidige certificaat valideren

```
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. Een nieuw certificaat genereren

U moet de algemene naam (uit het veld "subject=CN") gebruiken die u in de vorige stap hebt gekregen om het nieuwe certificaat te genereren

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

3. Start het centrum opnieuw op.

Bij implementaties met zowel Local Center als Global Center is het van essentieel belang om de Local Centers uit te schrijven en opnieuw in te schrijven.

Stappen om het sensorcertificaat te regenereren

Als het centrumcertificaat is verlopen, is het mogelijk dat sommige sensorcertificaten op het punt staan te verlopen aangezien die ook 2 jaar geldig zijn vanaf het moment dat de sensor in het centrum wordt gecreëerd.

- Voor sensoren die met de extensie zijn geïnstalleerd, gebruikt hergroeperen een nieuw certificaat.
- Voor sensoren die handmatig zijn geïmplementeerd:

1. Genereer een nieuw certificaat in het midden met het serienummer van de sensor:

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

Noteer de id die door de opdracht is teruggegeven

2. De sensor-id voor deze sensor ophalen

```
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. Werk de database voor de sensor bij met certificaat-id

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

Het serienummer van het certificaat moet de waarde zijn die uit de eerste stap wordt verkregen en moet de identificatiecode van de sensor hebben

4. Download het provisioningpakket voor deze sensor van de Web GUI

5. Herstelt de implementatie met dit provisioningpakket

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.