

Schritte zur Verlängerung eines abgelaufenen selbstsignierten Zertifikats im Cyber Vision Center

Inhalt

[Einleitung](#)

[Problem](#)

[Lösung](#)

[Schritte zum Regenerieren des Center-Zertifikats](#)

[Schritte zur Neugenerierung des Sensorzertifikats](#)

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Verlängerung eines abgelaufenen selbstsignierten Zertifikats (Self-Signed Certificate, SSC) in einem Cisco Cyber Vision Center beschrieben.

Problem

Zertifikate, die vom Zentrum für die Kommunikation mit den Sensoren für die Web-Schnittstelle verwendet werden (sofern kein externes Zertifikat vorhanden ist), werden beim ersten Start des Zentrums generiert und gelten für **2 Jahre** (mit einer zusätzlichen Nachfrist von 2 Monaten). Wenn die Zeit abgelaufen ist, können die Sensoren keine Verbindung mehr zum Center herstellen. Die folgenden Fehler werden in den Protokollen angezeigt:

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

Darüber hinaus zeigt die Verbindung zur Webbenutzeroberfläche einen Fehler an oder wird je nach Webbrowser blockiert, wenn kein externes Zertifikat verwendet wird.

Lösung

Sie gilt für Version 4.2.x. Ab Version 4.2.1 ist dies auch über die Web-GUI möglich.

Schritte zum Regenerieren des Center-Zertifikats

1. Aktuelles Zertifikat überprüfen

```
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. Ein neues Zertifikat generieren

Sie müssen den im vorherigen Schritt erhaltenen Common Name (aus dem Feld "subject=CN") verwenden, um das neue Zertifikat zu generieren.

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

3. Starten Sie das Center neu.

Bei Bereitstellungen mit Local Center und Global Center ist es wichtig, die Registrierung der Local Center aufzuheben und sie erneut anzumelden.

Schritte zur Neugenerierung des Sensorzertifikats

Wenn das Center-Zertifikat abgelaufen ist, laufen möglicherweise einige Sensorzertifikate bald ab, da diese ebenfalls zwei Jahre nach der Erstellung des Sensors im Center gültig sind.

- Für Sensoren, die mit der Erweiterung installiert sind, wird bei der erneuten Bereitstellung ein neues Zertifikat verwendet.
- Für manuell bereitgestellte Sensoren:

1. Generieren Sie ein neues Zertifikat auf dem Center mit der Seriennummer des Sensors:

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

Beachten Sie die vom Befehl zurückgegebene ID.

2. Ermitteln Sie die Sensor-ID für diesen 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€œ
```

3. Aktualisieren der Datenbank für den Sensor mit der Zertifikat-ID

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

Bei der Seriennummer des Zertifikats muss es sich um den im ersten Schritt ermittelten Wert und die Sensor-ID des Sensors handeln.

4. Laden Sie das Bereitstellungspaket für diesen Sensor über die Web-GUI herunter.
5. Wiederholen Sie die Bereitstellung mit diesem Bereitstellungspaket.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.