Stellen Sie die Telemetrieverbindungen aufgrund von PKI-Zertifikatverlängerungsfehlern auf von Catalyst Center verwalteten IOS-XE-Geräten mit den Versionen 17.12.1 bis 17.12.4 wieder her.

Einleitung

In diesem Dokument werden die Ursachen für fehlgeschlagene Telemetrieverbindungen und ihre Wiederherstellung beschrieben.

- Die automatische Verlängerung des infra-iwancertificate für das SDN-Netzwerk (Cisco Catalyst Center - Cisco IOS® XE-Gerät) kann auf einem Cisco IOS XE-Gerät aufgrund der Cisco Bug-ID CSCwk39268 auf dem Cisco IOS XE-Gerät fehlschlagenund Telemetrie von betroffenen Geräten an Catalyst Center gesendet, um den Ausfall zu beheben.
- Das Zertifikat ist ein Jahr gültig und wird in der Regel automatisch von Catalyst Center ca. 60 Tage vor Ablauf des Zertifikats verlängert.
- Kunden, die von diesem Problem betroffen sind oder wahrscheinlich betroffen sein werden, wird eine Popup-Meldung im Catalyst Center angezeigt.

Betroffene Versionen:

- Catalyst Center-Versionen vor 2.3.7.11 zur Verwaltung von Cisco IOS XE-Netzwerkgeräten unter den Versionen 17.12.1-17.12.4

Auflösung:

Der Kunde muss eine dieser drei Optionen nutzen, um das Problem zu beheben.

Option 1: Aktualisieren Sie Catalyst Center auf 2.3.7.11 oder 2.3.7.9 PSMU60 oder 2.3.7.10 PSMU110. Das SMU (Software Maintenance Update) steht unter System > Software Management in der Cisco Catalyst Center-GUI für ein Upgrade zur Verfügung.

Option 2: Führen Sie ein Upgrade des betroffenen Cisco IOS XE-Geräts auf 17.12.5 oder höher

einer von Cisco empfohlenen Version durch.

Option 3: Erzwingen Sie Push-Telemetrie über die Catalyst Center-GUI, und aktualisieren Sie den Hash-Algorithmus für den Trustpoint wie folgt auf sha512 auf dem Gerät:

1. Navigieren Sie zu Menü > Provisionierung > Bestand
2. Auswahl der Geräte nach Hostname
3. Wählen Sie Aktionen > Telemetrie > Telemetrieeinstellungen aktualisieren aus.
4. Push für erzwungene Konfiguration aktivieren
5. Fahren Sie mit dem Assistenten fort, und senden Sie die Aufgabe.

Identifizierung des betroffenen Cisco IOS XE-Geräts:

Schritt 1: Überprüfen Sie das Gerätezertifikat und den Vertrauenspunktstatus auf dem betroffenen Cisco IOS XE-Gerät.

```
device# show crypto pki certificates verbose sdn-network-infra-iwan
```

Beispiel für das Ergebnis:

```
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 18831279321B12FA
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: device.example.net
    cn=C9300-48U_SN12345678_sdn-network-infra-iwan
    hostname=device.example.net
  Validity Date:
    start date: 11:39:55 cdt Jul 10 2025
    end   date: 11:39:55 cdt Jul 16 2025
    renew date: 06:51:54 cdt Jul 15 2025
  ...
```

Anmerkung: Wenn Enddatum und Verlängerungsdatum vor dem aktuellen Datum auf dem Gerät liegen, ist das Zertifikat abgelaufen.

Phase 2: Überprüfen Sie das Fehlerprotokoll auf dem Gerät.

Beispiel für das Ergebnis:

```
Device# show logging
%PKI-2-CERT_RENEW_FAIL: Certificate renewal failed for trustpoint sdn-network-infra-iwan
Reason : Failed to get ID certificate from CA server sdn-network-infra-iwan:Certificate renewal failed.
```

Schritt 3: Überprüfung des Telemetriestatus des Geräts auf Catalyst Center

Beispiel für das Ergebnis:

```
Device#show tel con all
Telemetry connections
Index Peer Address Port VRF Source Address State State Description
--------------------------------------------------------------------------------
36284 x.x.x.x 25103 0 x.x.x.x Connecting Connection request made to transport handler
```

Anmerkung: In diesem Beispiel ist die Telemetrieverbindung nicht aktiv, sondern nur im Status "Connecting" (Verbinden).

Zusätzliche Informationen:

(a) Für mehrere Cisco IOS XE-Geräte kann diese Vorlage von Catalyst Center per Push bereitgestellt werden, indem CLI-Vorlagen aus den Tools Design > CLI Templates bereitgestellt werden:

```
crypto pki trustpoint sdn-network-infra-iwan
no hash sha256
hash sha512
```

(b.) Telemetrie-Push nach Hash-Update erzwingen

1. Navigieren Sie zu Menü > Provisionierung > Bestand
2. Auswahl der Geräte nach Hostname

3. Wählen Sie Aktionen > Telemetrie > Telemetrieeinstellungen aktualisieren aus.
4. Push für erzwungene Konfiguration aktivieren
5. Fahren Sie mit dem Assistenten fort, und senden Sie die Aufgabe.

Häufig gestellte Fragen Behebt die Installation von SMU ein bereits betroffenes System oder ist sie vorbeugend?
SMU stellt eine vorbeugende Lösung dar und muss installiert werden, bevor das Problem auftritt. Wenn das Problem bereits aufgetreten ist, wird es durch die Installation von SMU nicht automatisch behoben. Wählen Sie Option 3 aus, um bestehende ausgefallene Systeme wiederherzustellen.

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.