Telemetrie-connectiviteit herstellen is mislukt als gevolg van PKI-certificaatvernieuwingsfouten op door Catalyst Center beheerde IOS-XE-apparaten waarop releases 17.12.1 tot en met 17.12.4 worden uitgevoerd.

Inleiding

Dit document beschrijft de redenen achter telemetrieverbindingen die falen en hoe ze te herstellen.

- Het automatisch vernieuwen van het dn-network-infra-iwancertificaat (Cisco Catalyst Center - Cisco IOS® XE-apparaat) kan mislukken op een Cisco IOS XE-apparaat vanwege Cisco bug ID CSCwk39268 op het Cisco IOS XE apparaat, waardoor telemetrie die van getroffen apparaten naar Catalyst Center wordt verzonden, naar beneden gaat.
- Het certificaat is een jaar geldig en wordt normaal gesproken automatisch verlengd door Catalyst Center ongeveer 60 dagen voor de vervaldatum.
- Klanten die te maken hebben met dit probleem, of waarschijnlijk te maken krijgen met dit probleem, kunnen een pop-upbericht in Catalyst Center zien.

Geïmpacteerde releases:

- Catalyst Center brengt voorafgaand aan 2.3.7.11 het beheer van Cisco IOS XE-netwerkapparaten uit met versies 17.12.1-17.12.4

Resolutie:

Klanten moeten een van deze drie opties gebruiken om het probleem op te lossen.

Optie 1: Catalyst Center upgraden naar 2.3.7.11 of 2.3.7.9 PSMU60 of 2.3.7.10 PSMU110. De SMU (Software Maintenance Update) is beschikbaar voor een upgrade onder System > Software Management in de Cisco Catalyst Center GUI.

Optie 2: Upgrade het uitgevoerde Cisco IOS XE-apparaat naar 17.12.5 of hoger van een door Cisco aanbevolen release.

Optie 3: Forceer-push telemetrie van de Catalyst Center GUI en update het hash-algoritme voor het trustpoint naar sha512 op het apparaat als volgt:

1. Navigeer naar Menu > Voorzieningen > Inventarisatie
2. Selecteer de apparaten op hostnaam
3. Selecteer Acties > Telemetrie > Telemetrie-instellingen bijwerken
4. Configuratie-push forceren inschakelen
5. Ga door de wizard en dien de taak in

Het getroffen Cisco IOS XE-apparaat identificeren:

Stap 1: Apparaatcertificaat en Trustpoint-status valideren op het getroffen Cisco IOS XE-apparaat.

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

Voorbeelduitvoer:

```
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
  ...
```

Opmerking: Als de einddatum en verlengingsdatum vóór de huidige datum op het apparaat liggen, is het certificaat verlopen.

Stap 2: Controleer het foutenlogboek op het apparaat.

Voorbeelduitvoer:

```
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.
```

Stap 3: Controleer de telemetriestatus van het apparaat naar Catalyst Center

Voorbeelduitvoer:

```
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
```

Opmerking: in dit voorbeeld is de telemetrieverbinding niet actief, alleen in de status Verbinden.

Aanvullende informatie:

a) Voor meerdere Cisco IOS XE-apparaten kan deze sjabloon vanuit Catalyst Center worden gepusht door CLI-sjablonen te leveren vanuit de gereedschappen Ontwerp > CLI-sjablonen:

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

(b.) Forceer telemetrie push na hash update

1. Navigeer naar Menu > Voorzieningen > Inventarisatie
2. Selecteer de apparaten op hostnaam
3. Selecteer Acties > Telemetrie > Telemetrie-instellingen bijwerken

4. Configuratie-push forceren inschakelen
5. Ga door de wizard en dien de taak in

FAQ: Is het installeren van de SMU een reeds getroffen systeem te repareren, of is het preventief?
De SMU is een preventieve oplossing en moet worden geïnstalleerd voordat het probleem zich voordoet. Als het probleem zich al heeft voorgedaan, wordt het probleem niet automatisch opgelost door de SMU te installeren. Selecteer Optie 3 om bestaande defecte systemen te herstellen.

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.