Restaurez la connectivité de télémétrie en panne en raison d'échecs de renouvellement de certificat PKI sur les périphériques IOS-XE gérés par Catalyst Center exécutant les versions 17.12.1 à 17.12.4.

Introduction

Ce document décrit les raisons de l'échec des connexions de télémétrie et comment les restaurer.

- Le renouvellement automatique du certificat dn-network-infra-iwancertificate (Cisco Catalyst Center - périphérique Cisco IOS® XE) peut échouer sur un périphérique Cisco IOS XE en raison de l'ID de bogue Cisco CSCwk39268 sur le système d'exploitation de ce périphérique Cisco IOS XE, provoquant la panne de la télémétrie envoyée par les périphériques affectés à Catalyst Center.
- Le certificat est valide pendant un an et est normalement renouvelé automatiquement par Catalyst Center environ 60 jours avant son expiration.
- Les clients affectés par ce problème, ou susceptibles d'être affectés, peuvent voir un message contextuel dans Catalyst Center.

Versions affectées :

- Versions de Catalyst Center antérieures à 2.3.7.11, gestion des périphériques réseau Cisco IOS XE exécutant les versions 17.12.1 à 17.12.4

Résolution :

Les clients doivent utiliser l'une ou l'autre de ces trois options pour résoudre le problème.

Option 1: Mettez à niveau Catalyst Center vers 2.3.7.11 ou 2.3.7.9 PSMU60 ou 2.3.7.10 PSMU110. La SMU (Software Maintenance Update) sera disponible pour la mise à niveau sous

System > Software Management dans l'interface graphique utilisateur de Cisco Catalyst Center.

Option 2 : Mettez à niveau le périphérique Cisco IOS XE concerné vers la version 17.12.5 ou ultérieure d'une version recommandée par Cisco.

Option 3 : télémétrie par force-push à partir de l'interface utilisateur graphique de Catalyst Center et mise à jour de l'algorithme de hachage pour le point de confiance vers sha512 sur le périphérique comme suit :

1. Accédez à Menu > Provisionner > Stock
2. Sélectionnez le ou les périphériques par nom d'hôte
3. Sélectionnez Actions > Telemetry > Update Telemetry Settings
4. Activer la transmission forcée de configuration
5. Poursuivez l'exécution de l'Assistant et soumettez la tâche

Identification du périphérique Cisco IOS XE affecté :

Étape 1: Validez le certificat de périphérique et l'état du point de confiance sur le périphérique Cisco IOS XE affecté.

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

Exemple de résultat :

```
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
  ...
```

Remarque : Si la date de fin et la date de renouvellement sont antérieures à la date du jour sur le périphérique, le certificat a expiré.

Étape 2: Vérifiez le journal des erreurs sur le périphérique.

Exemple de résultat :

```
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.
```

Étape 3: Vérifiez l'état de télémétrie du périphérique vers Catalyst Center

Exemple de résultat :

```
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
```

Remarque : Dans cet exemple, la connexion de télémétrie n'est pas active, juste à l'état Connecté.

Informations complémentaires :

(a.) Pour plusieurs périphériques Cisco IOS XE, ce modèle peut être poussé à partir de Catalyst Center en provisionnant des modèles CLI à partir des outils Design > CLI Templates :

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

(b.) Forcer la télémétrie après la mise à jour du hachage

1. Accédez à Menu > Provisionner > Stock
2. Sélectionnez le ou les périphériques par nom d'hôte
3. Sélectionnez Actions > Telemetry > Update Telemetry Settings
4. Activer la transmission forcée de configuration
5. Poursuivez l'exécution de l'Assistant et soumettez la tâche

FAQ : L'installation de la SMU répare-t-elle un système déjà affecté ou est-elle préventive ?
Le SMU est un correctif préventif et doit être installé avant que le problème ne se produise. Si le problème s'est déjà produit, l'installation de l'unité SMU ne le résoudra pas automatiquement. Pour restaurer les systèmes défaillants existants, sélectionnez l'option 3.

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.