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.

Table des matières

Introduction

Versions affectées :

Résolution :

- Option 1 : lorsque le certificat du périphérique arrive à expiration et n'a pas encore expiré :
- Option 2: Il est recommandé de mettre à niveau Catalyst Center vers la version 2.3.7.11 (GSMU 100), si vous n'envisagez pas de mettre à niveau vers la version 2.3.7.9 (PSMU80) ou 2.3.7.10 (PSMU140).
- Option 3 :Mettez à niveau le périphérique Cisco IOS XEconcerné vers la version 17.12.5 ou ultérieure d'une version recommandée par Cisco.

Identification du périphérique Cisco IOS XE affecté :

- Étape 1: Validez le certificat du périphérique et l'état du point de confiance sur le périphérique Cisco IOS XE concerné.
- Étape 2: Vérifiez le journal des erreurs sur le périphérique.
- Étape 3: Vérifiez l'état de télémétrie du périphérique dans Catalyst Center

Informations complémentaires :

FAQ :

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 d'un bogue Cisco ID 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 : lorsque le certificat du périphérique arrive à expiration et n'a pas encore expiré :

Pour plusieurs périphériques Cisco IOS XE, ce modèle peut être envoyé depuis Catalyst Center.

1. Accédez à Catalyst Center

Connectez-vous à Catalyst Center.

Dans le menu principal, accédez à Design > CLI Templates.

2. Créez un modèle de projet

Cliquez sur Ajouter > Nouveau projet.

Entrez un nom de projet, par exemple : Changements_de_point_de_confiance PKI.

Cliquez sur Continuer.

3. Créez un nouveau modèle CLI

Sélectionnez le nouveau projet créé.

Cliquez sur Add > New Template.

Entrez un nom de modèle, par exemple : Configurer_sdn_network_infra_iwan_Trustpoint.

Définissez Template Type sur Regular Template.

Définissez le type de logiciel sur Cisco IOS XE.

Sélectionnez la famille ou la série de périphériques appropriée pour les périphériques Cisco IOS XE prévus.

Cliquez sur Continuer.

4. Ajouter la configuration CLI

Dans l'Éditeur de modèles, entrez les commandes suivantes :

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

5. Validez le modèle

Après avoir enregistré le modèle, cliquez surActions et sélectionnezValider.

Entrez un message de validation, par exemple : Mettre à jour le hachage du point de confiance en sha512.

Confirmez la validation.

6. Créer un profil réseau

a. Indiquez un nom de profil
b. Indiquez un type de profil, par exemple Commutation
c. Accédez à « Modèle(s) du jour N »
d. Joindre le modèle via Ajouter un modèle
e. Enregistrer le profil réseau
f. Attribuer le profil réseau à un site

7. Provisionner le modèle sur un périphérique

Sur la page Design > CLI Templates, sélectionnez le modèle.

Cliquez sur Provisionner les modèles.

Entrez un nom de tâche, par exemple : Trustpoint_Update_Device1.

Dans l'étape de sélection du périphérique, sélectionnez un périphérique Cisco IOS XE uniquement.

Cliquez sur Suivant.

Vérifiez l'affectation de modèle applicable.

Étant donné qu'aucune variable de modèle n'est utilisée, passez à l'étape suivante.

Dans l'écran Aperçu, vérifiez que les commandes sont correctes.

Cliquez sur Déployer maintenant.

8. Confirmez l'état du déploiement dans Catalyst Center :

Accédez àActivités > Tâches.

Vérifiez que le déploiement s'est terminé correctement.

Si le déploiement a échoué, vérifiez les détails de la tâche et le résultat de l'erreur avant de réessayer.

9. Répétez l' pour les périphériques supplémentaires

Répétez ce processus de déploiement pour chaque périphérique Cisco IOS XE individuellement.

Utilisez un nom de tâche distinct pour chaque périphérique afin de simplifier le suivi et le dépannage.

10. vérification de la configuration du périphérique

Une fois le déploiement terminé, connectez-vous à l'interface de ligne de commande du périphérique et exécutez :

```
show run | sec crypto pki trustpoint sdn-network-infra-iwan
```

Vérifiez que la configuration en cours comprend les lignes suivantes :

```
crypto pki trustpoint sdn-network-infra-iwan
hash sha512
```

Option 2: Il est recommandé de mettre à niveau Catalyst Center vers 2.3.7.11 (GSMU 100), si vous n'envisagez pas de mettre à niveau vers 2.3.7.9 (PSMU80) ou 2.3.7.10 (PSMU140).

La SMU (Software Maintenance Update) est disponible sous System > Software Management dans l'interface utilisateur graphique de Catalyst Center. Si vous ne pouvez pas voir la SMU, veuillez ouvrir une demande de service TAC et fournir votre ID de membre.

Option 3 : Mettez à niveau le périphérique Cisco IOS XE affecté vers17.12.5 ou version ultérieure d'une version recommandée par Cisco.

Identification du périphérique Cisco IOS XE affecté :

Étape 1: Validez le certificat du 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=C93OO-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 dans 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 :

Lorsque le certificat du périphérique a déjà expiré et que l'état du périphérique est dégradé, procédez comme suit :

Étape 1: Forcer la télémétrie push à partir de l'interface utilisateur graphique de Catalyst Center

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

Étape 2: Mettez à jour l'algorithme de hachage pour le point de confiance tosha512 sur le périphérique :

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

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 résout pas automatiquement. Pour récupérer des systèmes défaillants existants, consultez la section Informations supplémentaires.

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.