Ripristinare la connettività di telemetria inattiva a causa di errori di rinnovo del certificato PKI su dispositivi IOS-XE gestiti da Catalyst Center con versioni da 17.12.1 a 17.12.4.

Introduzione

Questo documento descrive i motivi alla base degli errori delle connessioni di telemetria e come ripristinarle.

- Il rinnovo automatico del certificato dn-network-infra-wan (Cisco Catalyst Center - Cisco IOS® XE) può non riuscire su un dispositivo Cisco IOS XE a causa dell'ID bug Cisco CSCwk39268 sul sistema operativo del dispositivo Cisco IOS XE, causando l'interruzione della telemetria inviata dai dispositivi interessati al Catalyst Center.
- Il certificato è valido per un anno e viene normalmente rinnovato automaticamente da Catalyst Center circa 60 giorni prima della scadenza.
- I clienti interessati da questo problema, o che potrebbero essere interessati, possono visualizzare un messaggio popup in Catalyst Center.

Versioni interessate:

- Release di Catalyst Center precedenti alla versione 2.3.7.11 gestione di dispositivi di rete Cisco IOS XE con versioni 17.12.1-17.12.4

Risoluzione:

I clienti devono utilizzare una di queste tre opzioni per risolvere il problema.

Opzione 1: Aggiornare Catalyst Center alla versione 2.3.7.11 o 2.3.7.9 PSMU60 o 2.3.7.10 PSMU110. L'SMU (Software Maintenance Update) sarà disponibile per l'aggiornamento in System > Software Management nella GUI di Cisco Catalyst Center.

Opzione 2: aggiornare il dispositivo Cisco IOS XE interessato alla versione 17.12.5 o successive

di una versione consigliata di Cisco.

Opzione 3: forzare la telemetria dalla GUI di Catalyst Center e aggiornare l'algoritmo hash per il trust point a sha512 sul dispositivo come segue:

1. Passare a Menu > Assegna > Magazzino
2. Selezionare i dispositivi in base al nome host
3. Selezionare Azioni > Telemetria > Aggiorna impostazioni di telemetria
4. Abilita imposizione Push Di Configurazione
5. Procedere con la procedura guidata e inviare l'attività

Identificazione del dispositivo Cisco IOS XE interessato:

Passaggio 1: Convalidare lo stato del certificato e del punto di fiducia del dispositivo sul dispositivo Cisco IOS XE interessato.

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

Output di esempio:

```
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
  ...
```

Nota: Se la data di fine e la data di rinnovo sono precedenti alla data corrente sul dispositivo, il certificato è scaduto.

Passaggio 2: Controllare il registro errori sul dispositivo.

Output di esempio:

```
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.
```

Passaggio 3: Controlla lo stato della telemetria del dispositivo su Catalyst Center

Output di esempio:

```
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
```

Nota: In questo esempio la connessione di telemetria non è attiva, ma solo nello stato Connessione.

Ulteriori informazioni:

(a.) Per più dispositivi Cisco IOS XE, è possibile eseguire il push di questo modello da Catalyst Center eseguendo il provisioning dei modelli CLI dagli strumenti Design > Modelli CLI:

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

(b.) Forza Push Di Telemetria Dopo L'Aggiornamento Hash

1. Passare a Menu > Assegna > Magazzino
2. Selezionare i dispositivi in base al nome host

3. Selezionare Azioni > Telemetria > Aggiorna impostazioni di telemetria
4. Abilita imposizione Push Di Configurazione
5. Procedere con la procedura guidata e inviare l'attività

Domande frequenti: L'installazione dell'unità SMU risolve il problema di un sistema già danneggiato o è preventiva?
La SMU è una correzione preventiva e deve essere installata prima che si verifichi il problema. Se il problema si è già verificato, l'installazione della SMU non lo risolve automaticamente. Per ripristinare i sistemi guasti esistenti, selezionare l'opzione 3.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).