Restaurar a conectividade da telemetria inoperante devido a falhas de renovação de certificado PKI em dispositivos IOS-XE gerenciados pelo Catalyst Center executando versões 17.12.1 a 17.12.4.

Introdução

Este documento descreve os motivos por trás da falha das conexões de telemetria e como restaurá-las.

- A renovação automática do certificado dn-network-infra-iwan(Cisco Catalyst Center - dispositivo Cisco IOS® XE) pode falhar em um dispositivo Cisco IOS XE devido ao bug da Cisco ID CSCwk39268 no sistema operacional do dispositivo Cisco IOS XE, fazendo com que a telemetria enviada dos dispositivos afetados para o Catalyst Center seja desativada.
- O certificado é válido por um ano e normalmente é renovado automaticamente pelo Catalyst Center cerca de 60 dias antes de seu vencimento.
- Os clientes afetados por esse problema, ou que possam ser afetados, podem ver uma mensagem pop-up no Catalyst Center.

Versões afetadas:

- Catalyst Center versões anteriores a 2.3.7.11 gerenciando dispositivos de rede Cisco IOS XE executando versões 17.12.1-17.12.4

Resolução:

Os clientes devem usar qualquer uma dessas três opções para resolver o problema.

Opção 1: Atualize o Catalyst Center para 2.3.7.11 ou 2.3.7.9 PSMU60 ou 2.3.7.10 PSMU110. O SMU (Software Maintenance Update) estará disponível para atualização em System > Software Management na GUI do Cisco Catalyst Center.

Opção 2: Atualizar o dispositivo Cisco IOS XE afetado para a versão 17.12.5 ou posterior de uma versão recomendada da Cisco.

Opção 3: Force a telemetria push da GUI do Catalyst Center e atualize o algoritmo hash do ponto confiável para sha512 no dispositivo da seguinte maneira:

1. Navegue até Menu > Provisionar > Inventário
2. Selecione os dispositivos por nome de host
3. Selecione Ações > Telemetria > Atualizar configurações de telemetria
4. Habilitar push de configuração forçada
5. Prosseguir com o assistente e enviar a tarefa

Identificando o dispositivo Cisco IOS XE afetado:

Passo 1: Validar o Certificado do Dispositivo e o Status do Ponto Confiável no dispositivo Cisco IOS XE afetado.

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

Saída de exemplo:

```
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
  ...
```

Note: Se a data de término e a data de renovação forem anteriores à data atual no dispositivo, o certificado expirou.

Passo 2: Verifique o log de erros no dispositivo.

Saída de exemplo:

```
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.
```

Passo 3: Verifique o status de telemetria do dispositivo para o Catalyst Center

Saída de exemplo:

```
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
```

Note: Neste exemplo, a conexão de telemetria não está ativa, apenas no estado Conectando.

Informações adicionais:

(a.) Para vários dispositivos Cisco IOS XE, este modelo pode ser enviado do Catalyst Center provisionando modelos CLI das ferramentas Design > Modelos CLI:

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

(b.) Forçar Push de Telemetria Após Atualização de Hash

1. Navegue até Menu > Provisionar > Inventário
2. Selecione os dispositivos por nome de host
3. Selecione Ações > Telemetria > Atualizar configurações de telemetria
4. Habilitar push de configuração forçada

5. Prosseguir com o assistente e enviar a tarefa

FAQ: A instalação do SMU corrige um sistema já afetado ou é preventiva?
O SMU é uma correção preventiva e deve ser instalado antes que o problema ocorra. Se o problema já tiver ocorrido, a instalação do SMU não resolverá o problema automaticamente. Para recuperar sistemas com falha existentes, selecione a Opção 3.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.