在运行版本17.12.1至17.12.4的Catalyst Center托管IOS-XE设备上，由于PKI证书续订失败而恢复遥测连接。

目录

简介

受影响的版本：

分辨率：

- 选项1：当设备证书即将到期且尚未到期时：
- 选项 2：建议将Catalyst Center升级到2.3.7.11(GSMU 100)，如果不考虑升级到2.3.7.9(PSMU80)或2.3.7.10(PSMU140)。
- 选项3：将受影响的Cisco IOS XE设备升级到17.12.5或思科推荐版本的其他版本。

识别受影响的Cisco IOS XE设备：

- 步骤 1：验证受影响的Cisco IOS XE设备上的设备证书和信任点状态。
- 步骤 2：检查设备上的错误日志。
- 步骤 3：检查Catalyst Center中设备的遥测状态

其它信息：

常见问题:

简介

本文档介绍遥测连接失败的原因以及如何恢复它们。

- 由于Cisco Bug，thesdn-network-infra-iwancertificate(Cisco Catalyst Center - Cisco IOS® XE设备)的自动续订在Cisco IOS XE设备上可能会失败 ID CSCwk39268 在Cisco IOS XE设备的操作系统上，导致从受影响设备发送到Catalyst Center的遥测下降。
- 证书的有效期为一年，通常由Catalyst Center在证书到期前60天自动续订。
- 受此问题影响或可能受影响的客户可以在Catalyst Center中看到弹出消息。

受影响的版本：

- 2.3.7.11之前的Catalyst Center版本管理运行版本17.12.1-17.12.4的Cisco IOS XE网络设备

分辨率：

客户需要使用这三个选项之一来解决问题。

选项1:当设备证书即将到期且尚未到期时：

对于多个Cisco IOS XE设备，可以从Catalyst Center推送此模板。

1.访问Catalyst中心

登录到Catalyst Center。

从主菜单中，导航到设计> CLI模板。

2.创建模板项目

单击添加>新建项目。

输入项目名称，例如：PKI_Trustpoint_Changes。

单击 Continue。

3.创建新的CLI模板

选择新创建的项目。

单击添加>新建模板。

输入模板名称，例如：Configure_sdn_network_infra_iwan_Trustpoint。

将Template Type设置为Regular Template。

将Software Type（软件类型）设置为Cisco IOS XE。

为预期的Cisco IOS XE设备选择适当的设备系列或系列。

单击 Continue。

4.添加CLI配置

在模板编辑器中，输入以下命令：

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

5.提交模板

保存模板后，点击操作，然后选择Commit。

输入提交消息，例如：Update trustpoint hash to sha512。

确认提交。

6.创建网络配置文件

a. 为配置文件命名
b. 提供配置文件类型，例如交换
c. 转至“Day-N Template(s)”
d. 通过添加模板附加模板
e. 保存网络配置文件
f. 将网络配置文件分配到站点

7.将模板调配到设备

在Design > CLI Templates页面上，选择模板。

点击调配模板。

输入任务名称，例如:Trustpoint_Update_Device1。

在设备选择步骤中，仅选择Cisco IOS XE设备。

点击Next。

查看适用的模板分配。

由于不使用模板变量，请继续执行下一步。

在“预览”屏幕上，验证命令是否正确。

点击立即部署。

8.确认Catalyst Center中的部署状态：

导航到活动>任务。

验证部署已成功完成。

如果部署失败，请在重试之前查看任务详细信息和错误输出。

9.对其他设备重复上述步骤

为每个Cisco IOS XE设备单独重复此部署过程。

为每个设备使用单独的任务名称，以简化跟踪和故障排除。

10. 检验设备上的配置

部署完成后，连接到设备的CLI并运行：

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

确认运行配置包括以下行：

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

选项 2：建议将Catalyst Center升级到2.3.7.11(GSMU 100)，如果不考虑升级到2.3.7.9(PSMU80)或2.3.7.10(PSMU140)。

Catalyst Center GUI中System > Software Management下提供SMU（软件维护更新）。如果您无法看到SMU，请打开TAC服务请求并提供您的成员ID。

选项3：将受影响的Cisco IOS XE设备升级到17.12.5或更高版本的Cisco推荐版本。

识别受影响的Cisco IOS XE设备：

步骤 1： 验证受影响的Cisco IOS XE设备上的设备证书和信任点状态。

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

输出示例：

```
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
  ...
```

注意：如果结束日期和续订日期早于设备的当前日期，则证书已过期。

步骤 2：检查设备上的错误日志。

输出示例：

```
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.
```

步骤 3：检查Catalyst Center中设备的遥测状态

输出示例：

```
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
```

注意：在本示例中，遥测连接未启用，只是处于“连接”状态。

其它信息：

当设备证书已过期且设备处于降级状态时，请执行以下两个步骤：

步骤 1： 从Catalyst Center GUI强制推送遥感勘测

1. 导航到菜单>调配>库存
2. 按主机名选择设备
3. 选择操作>遥测>更新遥测设置
4. 启用强制配置推送
5. 继续完成向导并提交任务

步骤 2： 更新设备上的信任点tosha512的散列算法：

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

常见问题:

安装SMU是否修复了已受影响的系统，或者它是预防性的？
SMU是预防性修复程序，必须在问题发生之前进行安装。如果问题已经发生，则安装SMU不会自动清除问题。要恢复现有的故障系统，请参阅其他信息部分。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。