

릴리스 17.12.1~17.12.4를 실행하는 Catalyst Center 관리 IOS-XE 디바이스의 PKI 인증서 갱신 실패로 인해 원격 분석 연결이 다운된 상태로 복원합니다.

소개

이 문서에서는 텔레메트리 연결이 실패하는 이유와 이를 복원하는 방법에 대해 설명합니다.

- Cisco IOS XE 디바이스의 운영 체제에서 Cisco 버그 ID CSCwk39268로 인해 Cisco IOS XE 디바이스에서 sdn-network-infra-iwan 인증서(Cisco Catalyst Center - Cisco IOS® XE 디바이스)의 자동 갱신이 실패하여 Cisco IOS XE 디바이스의 텔레메트리가 Catalyst Center로 전송되었습니다.
- 인증서는 1년간 유효하며, 일반적으로 Catalyst Center에서 만료 60일 전에 자동으로 갱신합니다.
- 이 문제의 영향을 받거나 영향을 받을 가능성이 있는 고객은 Catalyst Center에서 팝업 메시지를 볼 수 있습니다.

영향을 받는 릴리스:

- 버전 17.12.1-17.12.4를 실행하는 Cisco IOS XE 네트워크 디바이스를 관리하는 Catalyst Center 2.3.7.11 이전 릴리스

해결 방법:

고객은 이 세 가지 옵션 중 하나를 사용하여 문제를 해결해야 합니다.

옵션 1: Catalyst Center를 2.3.7.11 또는 2.3.7.9 PSMU60 또는 2.3.7.10 PSMU110으로 업그레이드합니다. SMU(Software Maintenance Update)는 Cisco Catalyst Center GUI의 System(시스템) > Software Management(소프트웨어 관리)에서 업그레이드할 수 있습니다.

옵션 2: 영향받는 Cisco IOS XE 디바이스를 17.12.5 이상의 Cisco 권장 릴리스로 업그레이드합니다

옵션 3: Catalyst Center GUI에서 텔레메트리를 강제 푸시하고 신뢰 지점에 대한 해시 알고리즘을 디바이스에서 sha512로 다음과 같이 업데이트합니다.

1. Menu(메뉴) > Provision(프로비저닝) > Inventory(인벤토리)로 이동합니다
2. 호스트 이름으로 디바이스 선택
3. Actions(작업) > Telemetry(원격 분석) > Update Telemetry Settings(원격 분석 설정 업데이트)를 선택합니다.
4. 강제 구성 밀어넣기 사용
5. 마법사를 진행하고 작업을 제출합니다.

영향을 받는 Cisco IOS XE 장치 식별:

1단계: 영향을 받는 Cisco IOS XE 디바이스에서 디바이스 인증서 및 신뢰 지점 상태를 확인합니다.

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

샘플 출력:

```
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
...
```

참고: 종료 날짜 및 갱신 날짜가 디바이스의 현재 날짜 이전이면 인증서가 만료됩니다.

2단계: 디바이스의 오류 로그를 확인합니다.

샘플 출력:

```
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.
```

3단계: Catalyst Center에 대한 디바이스의 텔레메트리 상태 확인

샘플 출력:

```
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
```

참고: 이 예에서는 텔레메트리 연결이 Connecting(연결) 상태에서만 작동 중이 아닙니다.

추가 정보:

(a.) 여러 Cisco IOS XE 디바이스의 경우 Design(설계) > CLI Templates(CLI 템플릿) 툴에서 CLI 템플릿을 프로비저닝하여 Catalyst Center에서 이 템플릿을 푸시할 수 있습니다.

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

나. 해시 업데이트 후 텔레메트리 강제 푸시

1. Menu(메뉴) > Provision(프로비저닝) > Inventory(인벤토리)로 이동합니다
2. 호스트 이름으로 디바이스 선택
3. Actions(작업) > Telemetry(원격 분석) > Update Telemetry Settings(원격 분석 설정 업데이트)를 선택합니다.
4. 강제 구성 밀어넣기 사용
5. 마법사를 진행하고 작업을 제출합니다.

FAQ: SMU를 설치하면 이미 영향을 받은 시스템이 수정됩니까, 아니면 예방적 시스템입니까?
SMU는 예방 수칙이며 문제가 발생하기 전에 설치해야 합니다. 문제가 이미 발생한 경우 SMU를 설치해도 문제가 자동으로 해결되지 않습니다. 기존의 실패한 시스템을 복구하려면 옵션 3을 선택합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.