지원되지 않는 GoDaddy R1 인증서 체인으로 인한 Webex Calling Survivability Gateway 동기화 실패 해결

목차

문제

Survivability Gateway(mcyitsrtr001.centralwire.com 및 prtitsrtr001.centralwire.com)가 Control Hub에 등록되었지만 동기화하지 못했습니다. mcyitsrtr001.centralwire.com에 중점을 둔 문제 해결. 동기화 시도가 오류 메시지와 함께 계속 실패했습니다.

```
Sync failed due to internal server error (code - 31117)
```

2026년 8월 5일 동기화 시도 중에 처음 관찰되었습니다. 텔레메트리 및 Webex 백엔드(pylon) 로그를 분석한 결과 게이트웨이에서 Webex 서비스에서 지원하지 않는 GoDaddy R1v1 인증서 체인(GoDaddy TLS Root CA - R1 계층 구조)을 제공하고 있다는 것이 밝혀져 인증서 체인이 거부되고 동기화가 실패합니다.

환경

- 2개의 관리 게이트웨이가 보고되었습니다. mcyitsrtr001.centralwire.com 및 prtitsrtr001.centralwire.com(mcyitsrtr001.centralwire.com에 중점을 둔 문제 해결)
- IOS® XE 버전: 17.12.6(SGW 노드), 17.15.06(MGW)
- Webex SGW(Calling Survivability Gateway) 컨피그레이션
- R1v1 중간 CA를 사용하는 GoDaddy TLS 인증서 체인
- 인증서 체인: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

해결

신뢰할 수 있는 인증서 경로를 설정하기 위해 인증서 교차 서명 해결 방법을 구현하여 문제를 해결했습니다. 이 솔루션에는 새로운 GoDaddy R1 계층 구조를 신뢰할 수 있는 Go Daddy 루트 인증 기관(G2)에 체인으로 지정하기 위해 GoDaddy R1-to-G2 교차 서명 인증서를 설치하는 것이 포함됩니다.

참고: 인증서를 변경하는 동안 crypto pki trustpool import clean 명령이 게이트웨이의 NETCONF-YANG/DMI 서비스를 중단하여 커넥터를 잠시 오프라인 상태로 전환했습니다. `192.168.217.55:830`에 대한 소켓을 열 수 없습니다. 이는 6-7단계를 통해 복구되었으며, 원본 동기화 실패가 아닌 유지 보수의 부작용이었습니다.

1단계: Cisco Trustpool 번들 설치

Go Daddy Root Certificate Authority - G2가 포함된 Cisco 신뢰 풀 번들을 설치합니다.

```
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_union.p7b
```

`import clean`은 전체 신뢰 풀을 교체합니다. 이 경우 신뢰 풀에 종속된 서비스가 중단될 수 있습니다(앞서 나열한 커넥터-오프라인 메모 참조). 신중하게 사용하십시오.

2단계: G2 루트 인증서 확인

Go Daddy Root Certificate Authority - G2가 있는지 확인합니다.

```
show crypto pki trustpool | include GoDaddy|Go Daddy
```

3단계: 자체 서명 R1 신뢰 지점 제거

기존의 자체 서명 R1 신뢰 지점을 제거합니다(인증서를 제거하라는 메시지가 표시되면 yes로 응답).

```
no crypto pki trustpoint GoDaddyRootR1
```

4단계: 교차 서명된 R1 인증서 설치

교차 서명된 R1 인증서를 사용하여 새 신뢰 지점을 만듭니다(제목: GoDaddy TLS 루트 CA - R1, 발급자: Go Daddy Root Certificate Authority - G2):

```
crypto pki trustpoint GoDaddyCrossR1
enrollment terminal
revocation-check none
exit
crypto pki authenticate GoDaddyCrossR1
<paste cross-signed R1 PEM – Subject: GoDaddy TLS Root CA - R1, Issuer: Go Daddy Root Certificate Autho
quit
yes
```

5단계: 인증서 체인 확인

이제 체인이 올바르게 확인되는지 확인합니다.

```
show crypto pki certificates webex-sgw
show crypto pki certificates GoDaddyCrossR1
```

6단계: NETCONF 서비스 재시작

HTTP(S) 서버 및 NETCONF-YANG 서비스 반송(disable과 enable 사이에 약 60초 대기):

```
conf t
no netconf-yang
no ip http secure-server
```

```
no ip http server
end
```

60초 동안 기다린 다음 다시 활성화합니다.

```
conf t
ip http server
ip http secure-server
netconf-yang
end
write memory
```

7단계: 게이트웨이 다시 로드(필요한 경우)

서비스를 다시 시작한 후에도 NETCONF-YANG이 계속 제대로 작동하지 않으면 라우터를 다시 로드하여 DMI를 완전히 다시 초기화하십시오.

```
reload
```

주의: 가능해요 여기에 언급된 세부사항에는 실행될 경우 중대한 영향을 미칠 수 있는 절차 또는 명령이 포함되어 있는 것으로 보입니다. 실행 또는 권장 전에 위의 절차 또는 명령이 SME 또는 사업부에서 평가되었는지 확인하십시오.

8단계: 해결 확인

게이트웨이가 다시 온라인 상태가 되면 Control Hub에서 SGW 재동기화를 트리거하고 동기화 작업이 성공적으로 완료되었는지 오류 코드 31117 또는 "Certificate Server Trusted check failed" 메시지가 표시되지 않는지 확인합니다. Confirmed resolved — 게이트웨이에서 전체 리프 → R1v1 → R1(발급자 G2) 체인을 제시했으며 교차 서명 해결 후 동기화가 성공적으로 완료되었습니다.

원인

근본 원인이 인증서 신뢰 실패로 식별되었습니다. 존속성 게이트웨이는 Webex Calling의 신뢰할 수 있는 인증 기관 목록에 포함되지 않은 GoDaddy TLS Root CA - R1 계층(특히 GoDaddy TLS Intermediate CA DV - R1v1)을 사용하여 인증서 체인을 표시하고 있었습니다.

Webex 백엔드(pylon)가 SIP 인증 정보 요청 중에 서버 인증서 신뢰 확인을 수행할 때 신뢰할 수 있는 루트 인증서에 대한 유효한 인증 경로를 만들지 못했습니다. 이로 인해 SunCertPathBuilderException이 발생하여 "요청한 대상에 대한 유효한 인증 경로를 찾을 수 없습니다."라는 오류가 발생하여 HTTP 400 응답 및 동기화 중단이 발생했습니다.

Webex Calling은 이전 GoDaddy/Starfield 루트(예: Go Daddy Root Certificate Authority - G2)만 신뢰하지만 최신 "GoDaddy TLS"(R1/R1v1) 계층은 신뢰하지 않습니다.

관련 콘텐츠

- Webex Hybrid Services에 지원되는 인증 기관
- GoDaddy 인증서 저장소
- Cisco 기술 지원 및 다운로드

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.