NCS 1010 노드의 CEPKI 신뢰 풀 번들 축적으로 인한 복구 시간 연장 및 SSH 액세스 실패

목차

[소개](#)

[문제](#)

[환경](#)

[해결](#)

[원인](#)

[관련 정보](#)

소개

이 문서에서는 NCS 1010 노드(Cisco IOS® XR 24.3.1, 25.1.1 포함)에서 CEPKI 신뢰 풀 번들 축적으로 인한 확장 복구 시간 및 SSH 액세스 실패에 대해 설명합니다.

문제

NCS 1010 광 노드에서 RP(Route Processor)를 다시 로드한 후 간헐적으로 연장된 복구 시간이 관찰됩니다. 복구 기간 동안 CEPKI(Cisco Embedded Public Key Infrastructure) 초기화가 지연되어 디바이스에 대한 SSH 액세스가 실패합니다. 이렇게 하면 영향을 받는 노드에서 원격 관리 및 운영 작업을 수행할 수 없습니다. Syslog 메시지 및 SSH 오류는 초기화가 완료될 때까지 SSHD 프로세스가 CEPKI에서 호스트 키를 검색할 수 없으므로 SSH 로그인에 실패함을 나타냅니다. SSH 액세스의 복구는 CEPKI가 초기화를 완료한 후, 대개 30-60분 후에만 관찰됩니다. 이 문제는 디바이스, 특히 소프트웨어 릴리스 24.3.1 및 25.1.1에서 신뢰 풀 번들이 많이 누적되는 것과 관련이 있습니다.

환경

- 기술: 옵티컬 네트워킹
- 제품군: NCS 1000 Series(NCS 1010 옵티컬 노드)
- 소프트웨어 버전: IOS XR 24.3.1, 25.1.1 (두 버전에서 재발행)
- 구성 요소: RP(Route Processor), CEPKI, SSHD 프로세스
- 운영 기능: Call-Home, Smart Licensing 애플리케이션
- 최근 관찰: 복구 시간 연장, RP 다시 로드 후 SSH 액세스 실패, 높은 신뢰 풀 번들 누적

해결

신뢰 풀 번들 축적으로 인한 CEPKI 초기화 지연 및 SSH 액세스 실패를 완화 및 해결하려면 언급된 단계를 따르십시오. 이러한 단계는 검증된 엔지니어링 분석 및 문서화된 해결책에서 직접 도출됩니다.

1. 신뢰 풀 번들 축적을 확인합니다.

   현재 신뢰 풀 번들 상태 및 관련 인증서 정보를 검토하려면 다음 명령을 실행합니다. 제공된 데이터에서 예제 출력을 사용할 수 없습니다.

   1단계. 자세한 NCS1010 기술 정보를 검토합니다.

   ```
   show tech ncs1010 detailed
   ```

   2단계. 암호화 세션 세부사항을 검토합니다.

   ```
   show tech crypto session
   ```

   3단계. CEPKI 기술 지원 데이터를 검토합니다.

   ```
   show tech-support cepki
   ```

   4단계. 시스템 데이터베이스 상태를 검토합니다.

   ```
   show tech sysdb
   ```

   5단계. 설치된 모든 암호화 CA 인증서를 나열합니다.

   ```
   show crypto ca certificates
   ```

6단계. 신뢰 풀 번들 세부 정보를 표시합니다.

```
show crypto ca trustpool detail
```

7단계. 신뢰 풀 상태를 표시합니다.

```
show crypto ca trustpool
```

8단계. 신뢰 풀 정책을 표시합니다.

```
show crypto ca trustpool policy
```

2. 영향을 받는 릴리스(24.3.1 및 25.1.1)의 해결 방법:

누적된 신뢰 풀 번들을 정리하고 강제 다시 가져오기를 수행하려면 언급된 명령을 순차적으로 실행합니다. 이 프로세스에서는 이전에 다운로드한 신뢰 풀 인증서를 제거하고 현재 번들을 다운로드하므로 초기화 지연을 줄일 수 있습니다.

1단계. 가져오기 전에 신뢰 풀 인증서를 지웁니다.

```
crypto ca trustpool import url clean
```

2단계. 신뢰 풀 번들을 가져옵니다.

```
crypto ca trustpool import url
```

3. 영구 수정(업그레이드 권장):

   기본 문제는 Cisco IOS XR 릴리스 26.1.1의 Cisco 버그 ID CSCwq에서 해결됩니다39205. 시스템이 현재 번들을 다운로드하기 전에 이전에 다운로드한 신뢰 풀 인증서를 자동으로 지우도록 하려면 이 릴리스로 업그레이드하십시오. 이렇게 하면 향후 운영을 위해 깨끗하고 일관된 신뢰 풀 상태가 유지됩니다.

4. Call-Home 전송 방법 권고:

   Cisco는 Cisco IOS XR 릴리스 25.3.1부터 Call-Home 전송 방법에 대해 EoL(End-of-Life)을 발표했습니다. 지속적인 지원을 받으려면 Smart Licensing 전송 방법으로 전환하는 것이 좋습니다. 자세한 내용은 제공된 Cisco Advisories를 참조하십시오.

기술 지표 및 로그:

- Syslog:

```
sshd[21897]: main: failed to get keys from cepki
```

- Syslog:

```
cepki[274]: certificate database updated
```

- SSH 오류:

```
ssh: connect to host <node> port 22: Connection refused
```

- 관찰: CEPKI 프로세스가 EOI(End-of-Initialization) 신호 없이 인증서를 반복적으로 업데이트합니다.
- 관찰된 신뢰 풀 수: '신뢰 풀: 'Trustpool'의 768개 내장: 다운로드됨'.

원인

근본 원인은 디바이스에서 여러 신뢰 풀 번들이 누적되기 때문이며, 이는 Call-Home 및 Smart Licensing 애플리케이션을 통한 반복적인 다운로드에 의해 트리거됩니다. Cisco IOS XR 릴리스 24.3.1 및 25.1.1에서 이러한 애플리케이션은 이전에 저장된 인증서를 지우지 않고 신뢰 풀 번들을 다운로드하므로 CEPKI 초기화 및 SSH 키 검색이 지연됩니다. 이 동작은 Cisco Bug ID CSCwq39205에서 해결되고 수정됩니다.

릴리스 26.1.1에서는 이제 새 번들을 다운로드하기 전에 이전 신뢰 풀 인증서를 지웁니다.

관련 정보

- Cisco 버그 ID CSCwq39205 - 트러스트 풀 번들을 다시 다운로드하기 전에 지워야 합니다.
- Cisco 버그 ID CSCwq53226 - Call-Home 전송 방법 End-of-Life Advisory
- Cisco 자문: Call-Home에서 Smart Transport로의 마이그레이션 알림
- 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.