

Uitgebreide hersteltijden en SSH-toegangsfouten door accumulatie van CEPKI Trustpool-bundels op NCS 1010-knooppunt

Inhoud

[Inleiding](#)

[uitgeven](#)

[milieu](#)

[resolutie](#)

[Oorzaak](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de verlengde hersteltijden en SSH-toegangsfouten als gevolg van de accumulatie van de CEPKI Trustpool-bundel op NCS 1010-knooppunt (met Cisco IOS® XR 24.3.1, 25.1.1).

uitgeven

Intermitterende verlengde hersteltijden worden waargenomen na het opnieuw laden van de Route Processor (RP) op NCS 1010 optische knooppunten. Tijdens de herstelperiode kan SSH-toegang tot het apparaat niet worden verleend vanwege vertragingen bij de initialisatie van Cisco Embedded Public Key Infrastructure (CEPKI). Dit voorkomt extern beheer en operationele taken op getroffen knooppunten. Syslog-berichten en SSH-fouten geven aan dat het SSHD-proces geen hostsleutels van CEPKI kan ophalen totdat de initialisatie is voltooid, wat resulteert in SSH-aanmeldingsfouten. Herstel van SSH-toegang wordt alleen waargenomen nadat CEPKI de initialisatie heeft voltooid, vaak na 30-60 minuten. Het probleem is gecorreleerd met een grote accumulatie van trustpool bundels op het apparaat, met name op software releases 24.3.1 en 25.1.1.

milieu

- Technologie: optische netwerken
- Productreeks: NCS 1000 reeks (NCS 1010 optische knooppunten)
- Softwareversies: IOS XR 24.3.1, 25.1.1 (probleem gereproduceerd op beide versies)
- Onderdelen: Routeprocessor (RP), CEPKI, SSHD-proces
- Operationele functies: Call-Home, Smart Licensing-toepassingen
- Recente waarnemingen: verlengde hersteltijden, SSH-toegangsfouten na herladen van RP, hoge bundelaccumulatie van trustpools

resolutie

Om de initialisatievertraging van CEPKI en het falen van SSH-toegang als gevolg van de accumulatie van trustpoolbundels te beperken en op te lossen, moet u de genoemde stappen volgen. Deze stappen zijn rechtstreeks afgeleid van gevalideerde technische analyse en gedocumenteerde resoluties.

1. Controleer Trustpool-bundelaccumulatie:

Voer deze opdrachten uit om de huidige status van de trustpool-bundel en de bijbehorende certificaatinformatie te bekijken. Voorbeeldresultaten zijn niet beschikbaar in de verstrekte gegevens.

Stap 1. Bekijk gedetailleerde technische informatie over NCS1010.

```
show tech ncs1010 detailed
```

Stap 2. Bekijk de details van de crypto-sessie.

```
show tech crypto session
```

Stap 3. Bekijk de technische ondersteuningsgegevens van CEPKI.

```
show tech-support cepki
```

Stap 4. Controleer de status van de systeemdatabase.

```
show tech sysdb
```

Stap 5. Lijst van alle geïnstalleerde crypto CA-certificaten.

```
show crypto ca certificates
```

Stap 6. Geef details van de trustpool-bundel weer.

```
show crypto ca trustpool detail
```

Stap 7. Geef de status van de vertrouwenpool weer.

```
show crypto ca trustpool
```

Stap 8. Betrouwbaarheidsbeleid weergeven.

```
show crypto ca trustpool policy
```

2. Workaround voor getroffen releases (24.3.1 en 25.1.1):

Om geaccumuleerde trustpoolbundels op te schonen en opnieuw importeren af te dwingen, voert u de genoemde opdrachten achtereenvolgens uit. Dit proces verwijdt de eerder gedownloade trustpoolcertificaten en downloadt de huidige bundel, waardoor initialisatievertragingen worden beperkt.

Stap 1. Schoon trustpoolcertificaten voorafgaand aan import.

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

Stap 2. Importeer de trustpool-bundel.

```
crypto ca trustpool import url
```

3. Permanente correctie (upgrade aanbevolen):

Het onderliggende probleem is opgelost in Cisco IOS XR release 26.1.1 onder Cisco Bug ID [CSCwq39205](#).

Upgrade naar deze release om ervoor te zorgen dat het systeem de eerder gedownloade trustpoolcertificaten automatisch wist voordat de huidige bundel wordt gedownload. Dit zorgt voor een schone en consistente trustpoolstatus voor toekomstige activiteiten.

4. Advies voor de call-home-transportmethode:

Cisco heeft End-of-Life (EoL) aangekondigd voor de Call-Home transportmethode vanaf Cisco IOS XR release 25.3.1. De overgang naar de vervoersmethode voor slimme licenties wordt ten zeerste aanbevolen voor blijvende ondersteuning. Raadpleeg de geleverde Cisco-adviezen voor meer informatie.

Technische indicatoren en logboeken:

- Syslog:

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

- Syslog:

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

- SSH-fout:

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

- Waarneming: CEPKI-proces waarbij certificaten herhaaldelijk worden bijgewerkt zonder EOI-

signaal (End-of-Initialization).

- Trustpool telt: 20 keer 'Trustpool: Built-In', 768 keer 'Trustpool: gedownload'.

Oorzaak

De hoofdoorzaak is de accumulatie van meerdere trustpoolbundels op het apparaat, veroorzaakt door herhaalde downloads via Call-Home en Smart Licensing-applicaties. In de Cisco IOS XR releases 24.3.1 en 25.1.1, deze toepassingen downloaden trustpool bundels zonder het wissen van eerder opgeslagen certificaten, wat resulteert in vertragingen voor CEPKI initialisatie en SSH key retrieval. Dit gedrag wordt aangepakt en opgelost onder Cisco Bug ID [CSCwq39205](#). In release 26.1.1, waarbij het systeem nu eerdere trustpoolcertificaten wist voordat nieuwe bundels werden gedownload.

Gerelateerde informatie

- [Cisco Bug ID CSCwq39205 – Trustpool-bundel moet worden gewist voordat u deze opnieuw downloadt](#)
- [Cisco Bug ID CSCwq53226 – Advies voor einde-levenscyclus-methode voor thuistransport](#)
- [Cisco-advies: migratie naar slim transport via call-home](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.