Extended Recovery Times and SSH Access Failures Due to CEPKI Trustpool Bundle Accumulation on NCS 1010 Node

Contents

Introduction

This document describes the extended recovery times and SSH access failures due to CEPKI Trustpool Bundle Accumulation on NCS 1010 Node (with Cisco IOS® XR 24.3.1, 25.1.1).

Issue

Intermittent extended recovery times are observed after reloading the Route Processor (RP) on NCS 1010 optical nodes. During the recovery period, SSH access to the device fails due to delays in Cisco Embedded Public Key Infrastructure (CEPKI) initialization. This prevents remote management and operational tasks on affected nodes. Syslog messages and SSH errors indicate that the SSHD process cannot retrieve host keys from CEPKI until initialization completes, resulting in SSH login failures. Recovery of SSH access is only observed after CEPKI completes initialization, often after 30–60 minutes. The issue is correlated with a large accumulation of trustpool bundles on the device, particularly on software releases 24.3.1 and 25.1.1.

Environment

- Technology: Optical Networking
- Product Family: NCS 1000 Series (NCS 1010 optical nodes)
- Software Versions: IOS XR 24.3.1, 25.1.1 (issue reproduced on both)
- Components: Route Processor (RP), CEPKI, SSHD process
- Operational Features: Call-Home, Smart Licensing applications
- Recent Observations: Extended recovery times, SSH access failures post-RP reload, high trustpool bundle accumulation

Resolution

In order to mitigate and resolve the CEPKI initialization delay and SSH access failure due to trustpool bundle accumulation, observe the steps mentioned. These steps are derived directly from validated engineering analysis and documented resolutions.

1. Check Trustpool Bundle Accumulation:

Run these commands in order to review the current trustpool bundle state and related certificate information. Example outputs are not available in the provided data.

Step 1. Review detailed NCS1010 technical information.

```
show tech ncs1010 detailed
```

Step 2. Review crypto session details.

```
show tech crypto session
```

Step 3. Review CEPKI technical support data.

```
show tech-support cepki
```

Step 4. Review the system database state.

```
show tech sysdb
```

Step 5. List all installed crypto CA certificates.

```
show crypto ca certificates
```

Step 6. Display trustpool bundle details.

```
show crypto ca trustpool detail
```

Step 7. Display trustpool status.

```
show crypto ca trustpool
```

Step 8. Display trustpool policy.

```
show crypto ca trustpool policy
```

2. Workaround for Affected Releases (24.3.1 and 25.1.1):

   In order to clean up accumulated trustpool bundles and force re-import, execute the mentioned commands sequentially. This process removes the trustpool certificates downloaded earlier and downloads the current bundle, helping to mitigate initialization delays.

   Step 1. Clean trustpool certificates prior to import.

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

   Step 2. Import the trustpool bundle.

   ```
   crypto ca trustpool import url
   ```

3. Permanent Fix (Upgrade Recommended):

   The underlying issue is resolved in Cisco IOS XR release 26.1.1 under Cisco Bug ID CSCwq39205. Upgrade to this release in order to ensure the system automatically clears previously downloaded trustpool certificates before downloading the current bundle. This maintains a clean and consistent trustpool state for future operations.

4. Call-Home Transport Method Advisory:

   Note that Cisco has announced End-of-Life (EoL) for the Call-Home transport method starting from

Cisco IOS XR release 25.3.1. Transition to the Smart Licensing transport method is strongly recommended for continued supportability. Refer to the provided Cisco advisories for more information.

Technical Indicators and Logs:

- Syslog:

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

- Syslog:

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

- SSH error:

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

- Observation: CEPKI process repeatedly updating certificates without End-of-Initialization (EOI) signal.
- Trustpool counts observed: 20 occurrences of 'Trustpool: Built-In', 768 of 'Trustpool: Downloaded'.

Cause

The root cause is the accumulation of multiple trustpool bundles on the device, triggered by repeated downloads via Call-Home and Smart Licensing applications. In the Cisco IOS XR releases 24.3.1 and 25.1.1, these applications download trustpool bundles without clearing previously stored certificates, resulting in delays for CEPKI initialization and SSH key retrieval. This behavior is addressed and fixed under Cisco Bug ID CSCwq39205.
in release 26.1.1, where the system now clears prior trustpool certificates before downloading new bundles.

Related Information

- Cisco Bug ID CSCwq39205 – Trustpool bundle should be cleared before downloading it again
- Cisco Bug ID CSCwq53226 – Call-Home transport method End-of-Life Advisory
- Cisco Advisory: Call-Home Migration to Smart Transport Notification
- Cisco Technical Support & Downloads