Délais de récupération étendus et échecs d'accès SSH dus à l'accumulation d'ensembles de pools de confiance CEPKI sur le noeud NCS 1010

Table des matières

Introduction

Ce document décrit les temps de récupération étendus et les échecs d'accès SSH dus à l'accumulation d'ensembles de pools de confiance CEPKI sur le noeud NCS 1010 (avec Cisco IOS® XR 24.3.1, 25.1.1).

Problème

Des temps de récupération étendus intermittents sont observés après le rechargement du processeur de routage (RP) sur les noeuds optiques NCS 1010. Au cours de la période de récupération, l'accès SSH au périphérique échoue en raison de retards dans l'initialisation de l'infrastructure à clé publique intégrée Cisco (CEPKI). Cela empêche la gestion à distance et les tâches opérationnelles sur les noeuds affectés. Les messages Syslog et les erreurs SSH indiquent que le processus SSHD ne peut pas récupérer les clés d'hôte de CEPKI tant que l'initialisation n'est pas terminée, ce qui entraîne des échecs de connexion SSH. La récupération de l'accès SSH n'est observée qu'après l'initialisation de CEPKI, souvent après 30 à 60 minutes. Le problème est corrélé avec une importante accumulation de bundles de pools de confiance sur le périphérique, en particulier sur les versions logicielles 24.3.1 et 25.1.1.

Environnement

- Technologie : Réseau optique
- Gamme de produits : Gamme NCS 1000 (noeuds optiques NCS 1010)
- Versions logicielles : IOS XR 24.3.1, 25.1.1 (problème reproduit sur les deux)
- Composants: Processeur de routage, CEPKI, processus SSHD
- Fonctionnalités opérationnelles : Applications Call-Home, Smart Licensing

- Observations récentes : Temps de récupération étendus, échecs d'accès SSH après rechargement RP, accumulation de faisceaux de pools de confiance élevée

Résolution

Afin d'atténuer et de résoudre le retard d'initialisation CEPKI et la défaillance d'accès SSH due à l'accumulation de faisceaux de pools de confiance, observez les étapes mentionnées. Ces étapes sont directement dérivées d'une analyse d'ingénierie validée et de résolutions documentées.

1. Vérifier l'accumulation des bundles Trustpool :

   Exécutez ces commandes afin de revoir l'état actuel du bundle trustpool et les informations de certificat associées. Les exemples de sorties ne sont pas disponibles dans les données fournies.

   Étape 1 : examen des informations techniques détaillées du NCS1010

   ```
   show tech ncs1010 detailed
   ```

   Étape 2 : examen des détails de la session de chiffrement

   ```
   show tech crypto session
   ```

   Étape 3. Examiner les données du soutien technique du CEPKI.

   ```
   show tech-support cepki
   ```

   Étape 4. Vérifiez l'état de la base de données système.

   ```
   show tech sysdb
   ```

Étape 5. Répertoriez tous les certificats d’autorité de certification de chiffrement installés.

```
show crypto ca certificates
```

Étape 6. Affichez les détails du bundle trustpool.

```
show crypto ca trustpool detail
```

Étape 7 : affichage de l’état du pool de confiance

```
show crypto ca trustpool
```

Étape 8. Affichez la stratégie trustpool.

```
show crypto ca trustpool policy
```

2. Solution pour les versions affectées (24.3.1 et 25.1.1) :

Afin de nettoyer les ensembles de pools de confiance accumulés et de forcer la réimportation, exécutez les commandes mentionnées séquentiellement. Ce processus supprime les certificats de pool de confiance téléchargés précédemment et télécharge le bundle actuel, ce qui permet de réduire les délais d'initialisation.

Étape 1. Nettoyez les certificats du pool de confiance avant l’importation.

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

Étape 2. Importez le bundle trustpool.

```
crypto ca trustpool import url
```

3. Correctif permanent (mise à niveau recommandée) :

   Le problème sous-jacent est résolu dans Cisco IOS XR version 26.1.1 sous l'ID de bogue Cisco CSCwq39205.
   Effectuez une mise à niveau vers cette version afin de vous assurer que le système efface automatiquement les certificats trustpool précédemment téléchargés avant de télécharger l'offre groupée actuelle. L'état du pool de confiance reste ainsi propre et cohérent pour les opérations futures.

4. Avis sur la méthode de transport Call-Home :

   Notez que Cisco a annoncé la fin de vie de la méthode de transport Call-Home à partir de la version 25.3.1 de Cisco IOS XR. La transition vers la méthode de transport Smart Licensing est fortement recommandée pour une prise en charge continue. Reportez-vous aux conseils Cisco fournis pour plus d'informations.

Indicateurs et journaux techniques :

- Syslog:

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

- Syslog:

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

- Erreur SSH :

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

- Observation : Le processus CEPKI met à jour de façon répétée les certificats sans signal de fin d'initialisation (EOI).
- Nombre de pools de confiance observés : 20 occurrences de 'Trustpool : Intégré', 768 de 'Trustpool : Téléchargé ».

Motif

La cause principale est l'accumulation de plusieurs ensembles de pools de confiance sur le périphérique, déclenchée par des téléchargements répétés via les applications Call-Home et Smart Licensing. Dans les versions 24.3.1 et 25.1.1 de Cisco IOS XR, ces applications téléchargent des ensembles de pools de confiance sans effacer les certificats précédemment stockés, ce qui entraîne des retards pour l'initialisation CEPKI et la récupération de la clé SSH. Ce comportement est corrigé et corrigé sous l'ID de bogue Cisco CSCwq39205.
dans la version 26.1.1, où le système efface maintenant les certificats trustpool précédents avant de télécharger de nouveaux bundles.

Informations connexes

- ID de bogue Cisco CSCwq39205 - L'offre groupée Trustpool doit être supprimée avant de la télécharger à nouveau
- ID de bogue Cisco CSCwq53226 - Méthode de transport Call-Home - Avis de fin de vie
- Conseil Cisco : Migration Call-Home vers Smart Transport Notification
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.