Tempos de Recuperação Estendidos e Falhas de Acesso SSH Devido à Acumulação de Pacote de Trustpool CEPKI no Nó NCS 1010

Contents

Introdução

Este documento descreve os tempos de recuperação estendidos e as falhas de acesso SSH devido ao CEPKI Trustpool Bundle Accumulation no Nó NCS 1010 (com Cisco IOS® XR 24.3.1, 25.1.1).

Problema

Os tempos de recuperação estendidos intermitentes são observados após a recarga do RP (Route Processor) nos nós ópticos do NCS 1010. Durante o período de recuperação, o acesso SSH ao dispositivo falha devido a atrasos na inicialização do Cisco Embedded Public Key Infrastructure (CEPKI). Isso evita tarefas operacionais e de gerenciamento remoto nos nós afetados. Mensagens de syslog e erros de SSH indicam que o processo SSHD não pode recuperar chaves de host do CEPKI até que a inicialização seja concluída, resultando em falhas de login de SSH. A recuperação do acesso SSH só é observada após a conclusão da inicialização do CEPKI, geralmente após 30-60 minutos. O problema está correlacionado a um grande acúmulo de pacotes de pool de confiança no dispositivo, particularmente nas versões de software 24.3.1 e 25.1.1.

Ambiente

- Tecnologia: Redes óticas
- Linha de produtos: NCS 1000 Series (nós ópticos NCS 1010)
- Versões de software: IOS XR 24.3.1, 25.1.1 (problema reproduzido em ambos)
- Componentes: Processador de Rota (RP), CEPKI, processo SSHD
- Recursos operacionais: Aplicativos Call-Home e Smart Licensing
- Observações recentes: Tempos de recuperação estendidos, falhas de acesso SSH após o recarregamento do RP, acúmulo de pacotes de pool confiável alto

Resolução

Para atenuar e resolver o retardo de inicialização de CEPKI e a falha de acesso SSH devido ao acúmulo de pacotes de pool confiável, observe as etapas mencionadas. Essas etapas são derivadas diretamente da análise de engenharia validada e das resoluções documentadas.

1. Verifique a acumulação de pacotes Trustpool:

   Execute estes comandos para revisar o estado atual do pacote do pool confiável e as informações de certificado relacionadas. Saídas de exemplo não estão disponíveis nos dados fornecidos.

   Etapa 1. Revise as informações técnicas detalhadas do NCS1010.

   ```
   show tech ncs1010 detailed
   ```

   Etapa 2. Revisar os detalhes da sessão de criptografia.

   ```
   show tech crypto session
   ```

   Etapa 3. Revise os dados de suporte técnico do CEPKI.

   ```
   show tech-support cepki
   ```

   Etapa 4. Revise o estado do banco de dados do sistema.

   ```
   show tech sysdb
   ```

Etapa 5. Listar todos os certificados de autoridade de certificação de criptografia instalados.

```
show crypto ca certificates
```

Etapa 6. Exibir detalhes do pacote trustpool.

```
show crypto ca trustpool detail
```

Etapa 7. Exibir o status do pool confiável.

```
show crypto ca trustpool
```

Etapa 8. Exibir a política de pool confiável.

```
show crypto ca trustpool policy
```

2. Solução alternativa para versões afetadas (24.3.1 e 25.1.1):

Para limpar os pacotes acumulados do pool de confiança e forçar a reimportação, execute os comandos mencionados sequencialmente. Esse processo remove os certificados trustpool baixados anteriormente e baixa o pacote atual, ajudando a reduzir os atrasos de inicialização.

Etapa 1. Limpe os certificados do pool confiável antes da importação.

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

Etapa 2. Importar o pacote trustpool.

```
crypto ca trustpool import url
```

3. Correção permanente (atualização recomendada):

   O problema subjacente é resolvido no Cisco IOS XR versão 26.1.1 na ID de bug Cisco CSCwq39205.
   Atualize para esta versão para garantir que o sistema limpe automaticamente os certificados de pool confiável baixados anteriormente antes de baixar o pacote atual. Isso mantém um estado de pool confiável limpo e consistente para operações futuras.

4. Aviso do método de transporte Call-Home:

   Observe que a Cisco anunciou EoL (End-of-Life) para o método de transporte Call-Home a partir do Cisco IOS XR versão 25.3.1. A transição para o método de transporte Smart Licensing é altamente recomendada para oferecer suporte contínuo. Consulte os avisos da Cisco fornecidos para obter mais informações.

Indicadores técnicos e registros:

- Syslog:

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

- Syslog:

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

- Erro de SSH:

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

- Observação: O processo CEPKI atualiza repetidamente os certificados sem sinal de fim de

inicialização (EOI).
- Contagens de pools confiáveis observadas: 20 ocorrências de 'Trustpool: Embutido', 768 de 'Trustpool: Baixado'.

Causa

A causa principal é o acúmulo de vários pacotes de pool confiável no dispositivo, disparado por downloads repetidos via aplicativos Call-Home e Smart Licensing. Nas versões 24.3.1 e 25.1.1 do Cisco IOS XR, esses aplicativos fazem download de pacotes de pool confiável sem limpar os certificados armazenados anteriormente, resultando em atrasos para a inicialização de CEPKI e recuperação de chave SSH. Esse comportamento é endereçado e corrigido na ID de bug Cisco CSCwq39205.
na versão 26.1.1, em que o sistema agora limpa os certificados de pool confiável anteriores antes de fazer o download de novos pacotes.

Informações Relacionadas

- ID de bug Cisco CSCwq39205 - O pacote Trustpool deve ser apagado antes de ser baixado novamente
- ID de bug Cisco CSCwq53226 - Aviso de fim da vida útil do método de transporte Call-Home
- Consultoria da Cisco: Migração do Call-Home para notificação do Smart Transport
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.