由于NCS 1010节点上的CEPKI Trustpool捆绑累积导致恢复时间延长和SSH访问失败

目录

简介

本文档介绍由于NCS 1010节点(使用Cisco IOS® XR 24.3.1、25.1.1)上的CEPKI Trustpool捆绑累积而延长的恢复时间和SSH访问故障。

问题

在NCS 1010光纤节点上重新加载路由处理器(RP)后，会观察到间歇性的延长恢复时间。在恢复期间，由于思科嵌入式公钥基础设施(CEPKI)初始化延迟，对设备的SSH访问失败。这可以防止受影响节点上的远程管理和操作任务。系统日志消息和SSH错误表明SSHD进程在初始化完成之前无法从CEPKI检索主机密钥，从而导致SSH登录失败。SSH访问的恢复仅在CEPKI完成初始化后观察到，通常在30-60分钟后。此问题与设备上大量累积的trustpool捆绑包有关，尤其是在软件版本24.3.1和25.1.1上。

环境

- 技术：光纤网络
- 产品系列：NCS 1000系列（NCS 1010光纤节点）
- 软件版本:IOS XR 24.3.1、25.1.1（两个版本均重现问题）
- 组件：路由处理器(RP)、CEPKI、SSHD进程
- 操作功能：Call-Home、智能许可应用
- 近期观察结果：恢复时间延长、RP重新加载后的SSH访问失败、高信任池捆绑累积

分辨率

为了缓解和解决CEPKI初始化延迟和SSH访问由于trustpool捆绑累积而导致的故障，请遵循上述步骤。这些步骤直接源于经过验证的工程分析和有文档记录的解决方案。

1. 检查Trustpool Bundle Cumulation:

运行这些命令以检查当前trustpool捆绑状态和相关证书信息。示例输出在提供的数据中不可用。

步骤1.查看详细的NCS1010技术信息。

```
show tech ncs1010 detailed
```

步骤2.检查加密会话详细信息。

```
show tech crypto session
```

步骤3.检查CEPKI技术支持数据。

```
show tech-support cepki
```

步骤4.查看系统数据库状态。

```
show tech sysdb
```

步骤5.列出所有已安装的加密CA证书。

```
show crypto ca certificates
```

步骤6.显示trustpool捆绑详细信息。

```
show crypto ca trustpool detail
```

步骤7.显示trustpool status。

```
show crypto ca trustpool
```

步骤8.显示信任池策略。

```
show crypto ca trustpool policy
```

2. 受影响版本（24.3.1和25.1.1）的解决方法：

要清除累积的trustpool捆绑包并强制重新导入，请依次执行上述命令。此过程删除之前下载的信任池证书并下载当前捆绑包，有助于缓解初始化延迟。

步骤1.在导入之前清理信任池证书。

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

步骤2.导入trustpool捆绑包。

```
crypto ca trustpool import url
```

3. 永久修复（建议升级）：

在Cisco IOS XR版本26.1.1中，Cisco Bug ID CSCwq下解决了基础问题39205.
升级到此版本，以确保系统在下载当前捆绑包之前自动清除以前下载的信任池证书。这样可为未来操作保持干净且一致的信任池状态。

4. Call-Home传输方法建议：

   请注意，思科已宣布从Cisco IOS XR版本25.3.1开始的Call-Home传输方法的寿命终止(EoL)。强烈建议过渡到智能许可传输方法以继续获得支持。有关详细信息，请参阅提供的思科建议。

技术指标和日志：

- 系统日志:

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

- 系统日志:

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

- SSH错误：

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

- 观察：CEPKI进程在没有初始化结束(EOI)信号的情况下重复更新证书。
- 观察到的Trustpool计数：20次出现“Trustpool:内置”，768个“Trustpool:已下载'。

原因

根本原因是设备上累积了多个信任池捆绑包，由Call-Home和智能许可应用的重复下载触发。在Cisco IOS XR版本24.3.1和25.1.1中，这些应用程序下载信任池捆绑包而不清除以前存储的证书，从而导致CEPKI初始化和SSH密钥检索延迟。此行为在Cisco Bug ID CSCwq39205下得到解决和修复。
在版本26.1.1中，系统现在会在下载新捆绑包之前清除以前的trustpool证书。

相关信息

- Cisco Bug ID CSCwq39205 — 应先清除Trustpool捆绑包，然后再重新下载
- Cisco Bug ID CSCwq53226 - Call-Home传输方法寿命终止建议

- 思科建议：Call-Home迁移至智能传输通知
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。