从7.4.3升级到7.6.4后的FTD管理接口故障

目录

问题

将思科安全防火墙3130威胁防御(FTD)高可用性(HA)对从7.4.3版升级到7.6.4版后，主设备在防火墙管理中心(FMC)完成99%后似乎发生故障，变得无响应。辅助设备已成功升级，并在HA对中变为活动状态。主设备未响应SSH连接，FMC无法与其通信。

经调查，在FXOS上发现此严重故障：

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

FTD升级日志显示升级实际上已成功完成（100%完成），但SFTunnel服务未正确启动，导致FTD和FMC之间无法通信。设备可以ping通自身、其网关和对等FTD单元，但无法到达位于不同子网上的FMC。

环境

- 思科安全防火墙3130威胁防御HA对
- 原始软件版本：FTD 7.4.3
- 目标软件版本：FTD 7.6.4（内部版本69）
- Cisco Firepower可扩展操作系统(FX-OS)v2.16.1（内部版本147）
- 使用静态IP编址配置的管理接口
- FMC服务器位于FTD管理网络以外的子网

分辨率

通过在受影响的FTD设备上完全重新配置管理接口解决了此问题。执行以下步骤：

步骤 1：由于SSH不起作用，请通过控制台访问连接到FTD。

步骤 2：通过检查升级日志验证升级完成状态：

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

步骤 3：确认FXOS上的管理接口故障：

```
device# show fault
```

步骤 4：尝试通过重新配置管理IP地址进行基本故障排除（这未解决问题）。

步骤 5：执行冷重新启动（这未解决问题）。

步骤 6：从FTD CLI完全禁用management0接口：

```
configure network management-interface disable management0
```

步骤 7：重新启用management0接口：

```
configure network management-interface enable management0
```

步骤 8::重新配置管理接口的网络设置：

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

步骤 9：验证是否已清除FXOS警报，并且FTD现在可以ping通FMC:

```
root@device:/# ping <FMC_IP_address>
```

步骤 10：使用manage_procs.pl脚本重新启动SFTunnel服务：

```
manage_procs.pl restart sftunnel
```

步骤 11：验证SFTunnel连接：

```
root@device:/# sftunnel_status.pl
```

步骤 12：测试故障转移功能，确保HA操作正常运行。

完成这些步骤后，FTD能够与FMC正确通信，并且所有连接和故障切换测试均成功。然后，可以应用修补程序升级，而不会出现问题。

原因

根本原因是管理接口未能在FTD从7.4.3升级到7.6.4后正确初始化，尽管升级过程已成功完成。带外管理接口配置有限状态机(FSM)在升级过程中失败，导致管理接口无法建立正确的连接。此行为已记录在Cisco Bug ID CSCww08417中。

此问题与之前报告的缺陷Cisco Bug ID CSCwj04154和Cisco Bug ID CSCwa69303类似，但发生在不同的条件下。99%完成时，管理接口故障造成升级失败的假象，实际上升级已成功完成，但管理连接已断开。

相关内容

- Cisco Bug ID CSCww08417 - FTD管理接口升级后可能无法启动

- 思科安全防火墙威胁防御兼容性指南
- 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）。