解决由登录块安静模式导致的IOS XE设备间断SSH访问故障

目录

问题

运行IOS XE软件的设备出现间歇性SSH访问故障。有时会接受SSH连接，有时会以不一致的模式予以拒绝。对设备的控制台访问不受影响。对于失败的SSH会话，在受影响设备上执行的数据包捕获可确认设备自身在接收客户端的TCP SYN后立即发送TCP RST数据包，SSH会话甚至可以开始协商。启用命令debug ip tcp transactions后，以下调试输出说明了TCP RST行为：

```
Aug 21 19:46:04.697: Reserved port 0 in Transport Port Agent for TCP IP type 0
Aug 21 19:46:04.697: TCP: sending RST, seq 0, ack 1013312911
Aug 21 19:46:04.697: TCP: sent RST to 10.x.x.x:43266 from 10.x.x.x:22
Aug 21 19:46:04.698: Released port 0 in Transport Port Agent for TCP IP type 0 delay 0
Aug 21 19:46:04.698: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
Aug 21 19:46:04.698: TCB destroyed
```

验证以下项目，以排除作为贡献原因的项目：

- 使用命令show ip ssh确认设备上已启用SSH。
- 使用命令show tcp brief确认TCP端口22在IOSd进程内部侦听。
- show ip traffic或debug ip error命令输出中没有“no port”错误
- VTY线路未完全消耗；show line的命令输出未显示所有线路都忙。
- 删除VTY线路上的任何access-class配置后，问题仍然存在。

设备日志记录缓冲区显示了大量的重复身份验证失败以及处于活动状态的安静模式：

```
Aug 21 12:24:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: test_user] [Source: LOCAL] [localport:
Aug 21 12:24:32: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 0 secs, [user: tes
```

发生故障时的show login输出显示设备在SSH发生故障时处于静默模式。

环境

- 平台：Cisco Catalyst 9500系列交换机（核心交换机和管理型交换机堆叠）
- 已启用SSH以远程访问设备
- 设备上的登录块配置处于活动状态：login block-for 120 attempts 3 within 60

分辨率

此问题是由大量失败的身份验证尝试持续触发的Login Block quiet模式功能引起的。要解决此问题，请对受信任SSH管理设备使用安静模式访问类ACL。

使用安静模式受信任IP访问类ACL配置登录块

配置登录块功能并实施安静模式访问类ACL（访问控制列表）。 此ACL允许受信任的管理主机和子网绕过静默模式实施，同时登录块保护对于所有其他源保持活动状态。

1.定义允许受信任的管理主机和子网的命名扩展ACL。以下示例允许两个特定跳转主机IP和一个/22管理子网。调整条目以匹配环境中的受信任管理源：

```
device# configure terminal
device(config)# ip access-list extended quietmode_trusted_ip
device(config-ext-nacl)# 10 permit ip host <trusted_host_1_ip> any
device(config-ext-nacl)# 20 permit ip host <trusted_host_2_ip> any
device(config-ext-nacl)# 30 permit ip <subnet_address> <wildcard_mask> any
device(config-ext-nacl)# exit
```

对于ACL条目结构：

- 使用host关键字，后跟单个IP地址，以允许特定管理主机（例如，跳转服务器）。

- 要允许整个子网，请指定网络地址，后跟适当的通配符掩码。

2.将ACL应用于静默模式访问类，这样即使静默模式处于活动状态，也允许匹配ACL的源连接：

```
device(config)# login quiet-mode access-class quietmode_trusted_ip
device(config)# end
```

3.如果删除了login block-for配置命令，请重新启用该命令：

```
device# configure terminal
device(config)# login block-for 120 attempts 3 within 60
device(config)# end
```

4.保存配置：

```
device# write memory
```

5.监控系统日志，观察是否继续触发安静模式和当前登录模式：

```
device# show logging
device# show login
```

解决持续身份验证失败的根本原因

上述基于ACL的解决方法可解决症状（SSH被安静模式阻止），但无法解决根本原因，即身份验证失败的重复数量很大。这些故障会持续触发静默模式。为了充分解决这个问题，需要调查并解决频繁的身份验证问题。

原因

由于大量反复失败的身份验证尝试，IOS-XE Login Block功能进入静默模式会导致间歇性SSH访问

失败。login block-for配置示例：

```
login block-for 120 attempts 3 within 60
```

此配置指示IOS XE设备进入静默模式，并在60秒的窗口中检测到3次或更多次失败的登录尝试时，在120秒内阻止所有新的登录连接。大量失败的身份验证尝试持续触发登录静默模式。静默模式实施是全局的，适用于为SSH配置的所有VTY线路和所有TCP端口。当静默模式处于活动状态时，设备在收到来自静默模式访问类ACL未明确允许的任何源的新TCP SYN数据包时立即发送TCP RST数据包，从而阻止建立SSH会话。

相关内容

- Cisco IOS-XE安全配置指南：登录增强功能（login block-for和quiet-mode access-class）
- 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）。