Resolve Intermittent SSH Access Failure on IOS XE Devices Caused by Login Block Quiet Mode

Contents

Issue

Devices running IOS XE software exhibit intermittent SSH access failures. SSH connections are sometimes accepted and sometimes refused with no consistent pattern. Console access to the devices is not affected. For a failed SSH session, packet captures performed on the affected device confirm that the device itself was sending TCP RST packets immediately upon receiving the client's TCP SYN, before the SSH session could even begin to negotiate. With the command **debug ip tcp transactions** enabled, the following debug output illustrates the TCP RST behavior:

```
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
```

Verify the following items to rule them out as contributing causes:

- Use the command **show ip ssh** to confirm SSH is enabled on the device.
- Use the command **show tcp brief** to confirm TCP port 22 is listening inside of the IOSd process.
- There is no "no port" error in the **show ip traffic** or **debug ip error** command output
- VTY lines are not fully consumed; the command output of **show line** does not show all lines busy.
- The issue remains after removing any **access-class** configuration on the VTY lines.

The device logging buffer showed a very high volume of repeated authentication failures, as well as quiet mode being active:

```
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
```

A **show login** output at the time of the failure shows the device in quiet-mode at the time of the SSH failure.

Environment

- Platform: Cisco Catalyst 9500 Series Switches (core switch and managed switch stacks)
- SSH is enabled for remote access to the device
- Login Block configuration active on the device: **login block-for 120 attempts 3 within 60**

Resolution

This issue is caused by the **Login Block** quiet mode feature being persistently triggered by a high volume of failed authentication attempts. To resolve the issue, use a quiet-mode access-class ACL for trusted SSH management devices.

Configure Login Block with a Quiet-Mode Trusted IP Access-Class ACL

Configure the login block feature and implement a quiet-mode access-class ACL (Access Control List). This ACL allows trusted management hosts and subnets to bypass quiet mode enforcement while the Login Block protection remains active for all other sources.

1. Define a named extended ACL that permits the trusted management hosts and subnets. The following example permits two specific jump host IPs and one /22 management subnet. Adjust the entries to match the trusted management sources in the environment:

```
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
```

For ACL entry construction:

- Use the **host** keyword followed by a single IP address to permit a specific management host (e.g., a jump server).

- To permit an entire subnet, specify the network address followed by the appropriate wildcard mask.

2. Apply the ACL to the quiet-mode access-class so sources matching the ACL are permitted to connect even when quiet mode is active:

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

3. Re-enable the **login block-for** configuration command if it was removed:

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

4. Save the configuration:

```
device# write memory
```

5. Monitor the system log to observe whether quiet mode continues to be triggered and the current login mode:

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

Addressing the persistent Authentication Failure Root Cause

The ACL-based workaround described above addresses the symptom (SSH being blocked by quiet mode) but does not address the underlying cause, which is the high volume of repeated authentication failures. These failures are what continuously trigger quiet mode. To fully resolve the issue, the frequent authentication problem should be investigated and resolved.

Cause

The intermittent SSH access failures are caused by the IOS-XE **Login Block** feature entering quiet mode

due to a high volume of repeated failed authentication attempts. Example **login block-for** configuration:

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

This configuration instructs the IOS XE device to enter quiet mode and block all new login connections for 120 seconds whenever 3 or more failed login attempts are detected within a 60-second window. A high volume of failed authentication attempts constantly triggers login quiet mode. Quiet mode enforcement is global and applies to all VTY lines and all TCP ports configured for SSH. When quiet mode is active, the device sends a TCP RST packet immediately upon receiving a new TCP SYN packet from any source not explicitly permitted by a quiet-mode access-class ACL, preventing the SSH session from being established.

Related Content

- Cisco IOS-XE Security Configuration Guide: Login Enhancements (login block-for and quiet-mode access-class)
- Cisco Technical Support & Downloads