로그인 블록 자동 모드로 인해 IOS XE 디바이스에서 간헐적인 SSH 액세스 오류 해결

목차

문제

IOS XE 소프트웨어를 실행 중인 디바이스에서는 간헐적인 SSH 액세스 오류가 발생합니다. SSH 연결은 일관성이 없는 패턴으로 허용되거나 거부되는 경우가 있습니다. 디바이스에 대한 콘솔 액세스는 영향을 받지 않습니다. 실패한 SSH 세션의 경우, 영향을 받는 디바이스에서 수행된 패킷 캡처는 SSH 세션이 협상을 시작하기도 전에 디바이스 자체가 클라이언트의 TCP SYN을 받는 즉시 TCP RST 패킷을 전송했음을 확인합니다. debug ip tcp transactions 명령이 활성화된 상태에서 다음 디버그 출력은 TCP RST 동작을 보여줍니다.

```
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
```

다음 항목을 확인하여 원인이 되는 항목을 제외합니다.

- show ip ssh 명령을 사용하여 디바이스에서 SSH가 활성화되어 있는지 확인합니다.
- show tcp brief 명령을 사용하여 TCP 포트 22가 IOSd 프로세스 내에서 수신 대기하고 있는지 확인합니다.
- show ip traffic 또는 debug ip error 명령 출력에 "no port" 오류가 없습니다
- VTY 라인이 완전히 소비되지 않음 show line의 명령 출력에서는 모든 회선이 사용 중인 상태로 표시되지 않습니다.
- VTY 라인에서 액세스 클래스 컨피그레이션을 제거한 후에도 문제가 유지됩니다.

디바이스 로깅 버퍼에서 매우 많은 양의 반복된 인증 실패와 자동 모드가 활성 상태로 나타났습니다.

```
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
```

show login output at the failure는 SSH 실패 시 디바이스를 자동 모드로 표시합니다.

환경

- 플랫폼: Cisco Catalyst 9500 Series 스위치(코어 스위치 및 관리형 스위치 스택)
- 디바이스에 대한 원격 액세스에 SSH가 사용됩니다.
- 디바이스에서 활성화된 로그인 블록 컨피그레이션: 60개 이내의 120회 시도에 대한 로그인 블록

해결

이 문제는 로그인 블록 자동 모드 기능이 많은 양의 실패한 인증 시도에 의해 지속적으로 트리거되어 발생합니다. 이 문제를 해결하려면 신뢰할 수 있는 SSH 관리 디바이스에 대해 quiet-mode access-class ACL을 사용합니다.

Quiet-Mode Trusted IP Access-Class ACL로 로그인 블록 구성

로그인 블록 기능을 구성하고 자동 모드 액세스 클래스 ACL(Access Control List)을 구현합니다. 이 ACL을 사용하면 다른 모든 소스에 대해 로그인 차단 보호가 활성 상태를 유지하는 동안 신뢰할 수 있는 관리 호스트 및 서브넷이 자동 모드 적용을 우회할 수 있습니다.

1. 신뢰할 수 있는 관리 호스트 및 서브넷을 허용하는 명명된 확장 ACL을 정의합니다. 다음 예는 두 개의 특정 점프 호스트 IP 및 하나의 /22 관리 서브넷을 허용합니다. 환경의 신뢰할 수 있는 관리 소스와 일치하도록 항목을 조정합니다.

```
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
```

ACL 항목 구성의 경우:

- 특정 관리 호스트(예: 점프 서버)를 허용하려면 host 키워드 뒤에 단일 IP 주소를 사용합니다.
- 전체 서브넷을 허용하려면 네트워크 주소 뒤에 적절한 와일드카드 마스크를 지정합니다.

2. ACL을 자동 모드 액세스 클래스에 적용하여 자동 모드가 활성화된 경우에도 ACL과 일치하는 소스가 연결되도록 합니다.

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

3. 제거된 경우 login block-for configuration 명령을 다시 활성화합니다.

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

4. 구성을 저장합니다.

```
device# write memory
```

5. 시스템 로그를 모니터링하여 자동 모드가 계속 트리거되는지 그리고 현재 로그인 모드가 계속 트리거되는지 확인합니다.

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

지속적인 인증 실패 근본 원인 해결

위에서 설명한 ACL 기반 해결 방법은 증상(SSH가 자동 모드로 차단됨)을 해결하지만 반복되는 인증 실패가 많은 근본적인 원인을 해결하지는 않습니다. 이러한 실패가 지속적으로 자동 모드를 트리거하는 이유입니다. 문제를 완전히 해결하려면 빈번한 인증 문제를 조사하고 해결해야 합니다.

원인

간헐적인 SSH 액세스 실패는 많은 양의 반복적인 인증 시도 실패로 인해 IOS-XE Login Block 기능이 자동 모드로 전환되어 발생합니다. 컨피그레이션에 대한 로그인 블록 예:

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

이 컨피그레이션은 IOS XE 디바이스에 60초 윈도우 내에서 3번 이상의 실패한 로그인 시도가 탐지될 때마다 자동 모드로 전환하고 120초 동안 모든 새 로그인 연결을 차단하도록 지시합니다. 많은 양의 실패한 인증 시도는 로그인 자동 모드를 지속적으로 트리거합니다. 자동 모드 적용은 전역 모드이며 SSH에 대해 구성된 모든 VTY 라인 및 모든 TCP 포트에 적용됩니다. 자동 모드가 활성화된 경우, 디바이스는 자동 모드 액세스 클래스 ACL에서 명시적으로 허용하지 않는 소스에서 새 TCP SYN 패킷을 수신하면 즉시 TCP RST 패킷을 전송하여 SSH 세션을 설정할 수 없게 합니다.

관련 콘텐츠

- Cisco IOS-XE 보안 컨피그레이션 가이드: 로그인 개선 사항(login block-for and quiet-mode access-class)
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.