Oplossen van intermitterende SSH-toegangsfout op IOS XE-apparaten veroorzaakt door aanmeldingsblok stille modus

Inhoud

uitgifte

Apparaten met IOS XE-software vertonen intermitterende SSH-toegangsfouten. SSH-verbindingen worden soms geaccepteerd en soms geweigerd zonder een consistent patroon. Console-toegang tot de apparaten wordt niet beïnvloed. Voor een mislukte SSH-sessie bevestigen de pakketopnamen die op het getroffen apparaat zijn uitgevoerd dat het apparaat zelf TCP RST-pakketten verstuurde onmiddellijk na ontvangst van de TCP SYN van de client, voordat de SSH-sessie zelfs kon beginnen te onderhandelen. Met de opdracht foutopsporing ip tcp transacties ingeschakeld, de volgende foutopsporing uitvoer illustreert het TCP RST gedrag:

```
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
```

Controleer de volgende items om ze uit te sluiten als bijdragende oorzaken:

- Gebruik de opdracht show ip ssh om te bevestigen dat SSH is ingeschakeld op het apparaat.
- Gebruik de opdracht show tcp brief om te bevestigen dat TCP poort 22 luistert binnen het IOSd-proces.
- Er is geen "no port" fout in de show ip traffic of debug ip error command output
- VTY-regels worden niet volledig verbruikt; de opdrachtuitvoer van show line toont niet alle bezette regels.
- Het probleem blijft bestaan nadat een toegangsklasse-configuratie op de VTY-lijnen is

verwijderd.

De buffer voor het vastleggen van apparaten toonde een zeer hoog volume aan herhaalde verificatiefouten en de stille modus die actief is:

```
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
```

Een login-uitgang weergeven op het moment van de storing toont het apparaat in de stille modus op het moment van de SSH-storing.

milieu

- Cisco Catalyst 9500 Series Switches (core switch en managed switch stacks)
- SSH is ingeschakeld voor externe toegang tot het apparaat
- Inlogblokkeringsconfiguratie actief op het apparaat: aanmeldingsblok voor 120 pogingen 3 binnen 60

resolutie

Dit probleem wordt veroorzaakt doordat de stille modus Login Block voortdurend wordt geactiveerd door een groot aantal mislukte verificatiepogingen. Om het probleem op te lossen, gebruikt u een ACL met toegangsklasse voor de stille modus voor vertrouwde SSH-beheerapparaten.

Inlogblok configureren met een ACL voor vertrouwde IP-toegangsklasse in stille modus

Configureer de functie voor het aanmeldingsblok en implementeer een ACL (Access Control List) voor toegang in de stille modus. Met deze ACL kunnen vertrouwde beheerhosts en subnetten de

handhaving van de stille modus omzeilen terwijl de bescherming van het aanmeldingsblok actief blijft voor alle andere bronnen.

1. Definieer een uitgebreide ACL met de naam die de vertrouwde beheerhosts en -subnetten toestaat. In het volgende voorbeeld zijn twee specifieke IP-adressen voor jumphosts en één /22-beheersubnet toegestaan. Pas de vermeldingen aan aan de vertrouwde beheerbronnen in de omgeving:

```
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
```

Voor ACL entry constructie:

- Gebruik het trefwoord host gevolgd door een enkel IP-adres om een specifieke beheerhost toe te staan (bijvoorbeeld een jumpserver).
- Als u een volledig subnet wilt toestaan, geeft u het netwerkadres op, gevolgd door het juiste jokermasker.

2. Pas de ACL toe op de toegangsklasse voor de stille modus, zodat bronnen die overeenkomen met de ACL, verbinding mogen maken, zelfs wanneer de stille modus actief is:

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

3. Schakel de opdracht blok-voor-configuratie opnieuw in als deze is verwijderd:

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

4. De configuratie opslaan:

```
device# write memory
```

5. Controleer het systeemlogboek om te zien of de stille modus nog steeds wordt geactiveerd en of de huidige aanmeldingsmodus:

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

Aanpak van de onderliggende oorzaak van de aanhoudende verificatiefout

De op ACL gebaseerde oplossing die hierboven wordt beschreven, behandelt het symptoom (SSH wordt geblokkeerd door de stille modus), maar pakt de onderliggende oorzaak niet aan, namelijk het hoge volume van herhaalde verificatiefouten. Deze storingen zijn wat continu de stille modus activeert. Om het probleem volledig op te lossen, moet het frequente authenticatieprobleem worden onderzocht en opgelost.

Oorzaak

De intermitterende SSH-toegangsfouten worden veroorzaakt doordat de functie IOS-XE Login Block stille modus inschakelt vanwege een groot aantal herhaalde mislukte verificatiepogingen. Voorbeeld van inlogblok voor configuratie:

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

Deze configuratie instrueert het IOS XE-apparaat om de stille modus in te voeren en alle nieuwe aanmeldingsverbindingen gedurende 120 seconden te blokkeren wanneer 3 of meer mislukte aanmeldpogingen worden gedetecteerd in een venster van 60 seconden. Een groot aantal mislukte verificatiepogingen activeert de stille inlogmodus voortdurend. De handhaving in de stille modus is globaal en is van toepassing op alle VTY-lijnen en alle TCP-poorten die voor SSH zijn geconfigureerd. Wanneer de stille modus actief is, verzendt het apparaat onmiddellijk een TCP RST-pakket nadat het een nieuw TCP SYN-pakket heeft ontvangen van een bron die niet expliciet is toegestaan door een ACL voor toegang tot de stille modus, waardoor de SSH-sessie niet kan worden ingesteld.

Gerelateerde inhoud

- Cisco IOS-XE Security Configuration Guide: Aanmeldingsverbeteringen (aanmeldingsblok-voor en toegang in stille modus-klasse)
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.