Risoluzione degli errori di accesso SSH intermittenti sui dispositivi IOS XE causati dalla modalità non interattiva del blocco di accesso

Sommario

Problema

I dispositivi con software IOS XE mostrano errori di accesso SSH intermittenti. Le connessioni SSH vengono a volte accettate e altre rifiutate senza uno schema coerente. L'accesso da console ai dispositivi non è influenzato. In caso di sessione SSH non riuscita, le acquisizioni dei pacchetti eseguite sul dispositivo interessato confermano che il dispositivo stesso stava inviando pacchetti TCP RST subito dopo la ricezione del TCP SYN del client, prima che la sessione SSH potesse iniziare la negoziazione. Con il comando debug ip tcp transaction abilitato, l'output di debug seguente mostra il comportamento di TCP RST:

```
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
```

Verificare i seguenti elementi per escluderli come cause concorrenti:

- Per verificare che il protocollo SSH sia abilitato sul dispositivo, usare il comando show ip ssh.
- Utilizzare il comando show tcp brief per confermare che la porta TCP 22 è in ascolto sul processo IOSd.
- L'output del comando show ip traffic o debug ip error non contiene alcun errore "no port"
- le linee VTY non sono interamente consumate; l'output del comando show line non visualizza tutte le righe occupate.
- Il problema rimane dopo aver rimosso qualsiasi configurazione della classe di accesso sulle

linee VTY.

Il buffer di registrazione del dispositivo ha rilevato un volume molto elevato di errori di autenticazione ripetuti e la modalità non interattiva:

```
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
```

Se si visualizza l'output show login al momento del guasto, il dispositivo viene mostrato in modalità silenziosa al momento del guasto SSH.

Ambiente

- Piattaforma: Cisco Catalyst serie 9500 Switch (stack di switch core e stack di switch gestiti)
- SSH è abilitato per l'accesso remoto al dispositivo
- Configurazione del blocco di accesso attiva sul dispositivo: blocco login per 120 tentativi 3 entro 60

Risoluzione

Il problema è causato dalla modalità non interattiva del blocco dell'accesso attivata in modo persistente da un elevato volume di tentativi di autenticazione non riusciti. Per risolvere il problema, utilizzare un ACL con classe di accesso in modalità non interattiva per i dispositivi di gestione SSH attendibili.

Configurare il blocco di accesso con un ACL di classe di accesso IP attendibile in modalità non interattiva

Configurare la funzionalità di blocco dell'accesso e implementare un ACL (Access Control List) con classe di accesso in modalità non interattiva. Questo ACL consente agli host di gestione

trusted e alle subnet di ignorare l'applicazione della modalità non interattiva mentre la protezione del blocco di accesso rimane attiva per tutte le altre origini.

1. Definire un ACL esteso con nome che autorizzi gli host e le subnet di gestione trusted. Nell'esempio seguente vengono autorizzati due indirizzi IP host di collegamento specifici e una subnet di gestione /22. Regolare le voci in modo che corrispondano alle origini di gestione attendibili nell'ambiente:

```
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
```

Per la costruzione della voce ACL:

- Utilizzare la parola chiave host seguita da un singolo indirizzo IP per consentire un host di gestione specifico (ad esempio, un server di collegamento).
- Per autorizzare un'intera subnet, specificare l'indirizzo di rete seguito dalla maschera con caratteri jolly appropriata.

2. Applicare l'ACL alla classe di accesso in modalità non interattiva in modo che le origini corrispondenti all'ACL possano connettersi anche quando la modalità non interattiva è attiva:

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

3. Riattivare il comando login block-for configuration se è stato rimosso:

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

4. Salvare la configurazione:

```
device# write memory
```

5. Monitorare il registro di sistema per verificare se la modalità non interattiva continua ad essere attivata e la modalità di accesso corrente:

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

Risoluzione della causa principale degli errori di autenticazione persistenti

La soluzione basata su ACL descritta sopra affronta il problema (il protocollo SSH viene bloccato in modalità non interattiva) ma non risolve la causa sottostante, ossia il volume elevato di errori di autenticazione ripetuti. Questi errori attivano continuamente la modalità non interattiva. Per risolvere completamente il problema, è necessario esaminare e risolvere il problema relativo all'autenticazione frequente.

Causa

Gli errori di accesso SSH intermittenti sono causati dalla modalità non interattiva della funzione di blocco dell'accesso IOS-XE a causa di un elevato volume di tentativi di autenticazione non riusciti ripetuti. Esempio di blocco di login per la configurazione:

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

Questa configurazione indica al dispositivo IOS XE di entrare in modalità non interattiva e di bloccare tutte le nuove connessioni di accesso per 120 secondi ogni volta che entro una finestra di 60 secondi vengono rilevati 3 o più tentativi di accesso non riusciti. Un volume elevato di tentativi di autenticazione non riusciti attiva costantemente la modalità di accesso non interattivo. L'imposizione della modalità silenziosa è globale e si applica a tutte le linee VTY e a tutte le porte TCP configurate per SSH. Quando la modalità non interattiva è attiva, il dispositivo invia un pacchetto TCP RST immediatamente dopo aver ricevuto un nuovo pacchetto TCP SYN da qualsiasi origine non esplicitamente consentita da un ACL di classe di accesso in modalità non interattiva, in modo da impedire la creazione della sessione SSH.

Contenuto correlato

- Guida alla configurazione della protezione di Cisco IOS-XE: Miglioramenti all'accesso (login block-for e quiet-mode access-class)
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).