Resolución de la Falla de Acceso SSH Intermitente en Dispositivos IOS XE Causada por el Modo Silencioso de Bloqueo de Login

Contenido

Problema

Los dispositivos que ejecutan el software IOS XE presentan fallas de acceso SSH intermitentes. Las conexiones SSH a veces son aceptadas y a veces rechazadas sin un patrón consistente. El acceso a la consola de los dispositivos no se ve afectado. Para una sesión SSH fallida, las capturas de paquetes realizadas en el dispositivo afectado confirman que el dispositivo mismo estaba enviando paquetes RST TCP inmediatamente después de recibir el TCP SYN del cliente, antes incluso de que la sesión SSH pudiera comenzar a negociar. Con el comando debug ip tcp transactions habilitado, el siguiente resultado de depuración ilustra el comportamiento de 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
```

Verifique los siguientes elementos para descartarlos como causas que contribuyen:

- Utilice el comando show ip ssh para confirmar que SSH está habilitado en el dispositivo.
- Utilice el comando show tcp brief para confirmar que el puerto TCP 22 está escuchando dentro del proceso IOSd.
- No hay ningún error "no port" en la salida del comando show ip traffic o debug ip error
- Las líneas VTY no se consumen completamente; el resultado del comando show line no muestra todas las líneas ocupadas.
- El problema continúa después de eliminar cualquier configuración de clase de acceso en las

líneas VTY.

El buffer de registro del dispositivo mostró un volumen muy alto de fallas de autenticación repetidas, así como un modo silencioso activo:

```
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
```

Una salida show login en el momento del fallo muestra el dispositivo en modo silencioso en el momento del fallo de SSH.

Entorno

- Plataforma: Switches Catalyst de Cisco serie 9500 (switches de núcleo y pilas de switches gestionados)
- SSH está habilitado para el acceso remoto al dispositivo
- Configuración del bloque de inicio de sesión activa en el dispositivo: login block-for 120 intentos 3 dentro de 60

Resolución

Este problema se debe a que la función de modo silencioso Login Block se activa de forma persistente debido a un gran volumen de intentos de autenticación fallidos. Para resolver el problema, utilice una ACL de clase de acceso de modo silencioso para los dispositivos de administración SSH de confianza.

Configuración del Bloque de Login con una ACL de Clase de Acceso IP de Confianza en Modo Silencioso

Configure la función de bloqueo de inicio de sesión e implemente una ACL de clase de acceso en

modo silencioso (Lista de control de acceso). Esta ACL permite que los hosts de administración de confianza y las subredes omitan la aplicación del modo silencioso mientras la protección Bloque de inicio de sesión permanece activa para todos los demás orígenes.

1. Defina una lista de control de acceso ampliada con nombre que permita los hosts y las subredes de gestión de confianza. El siguiente ejemplo permite dos IP de host de salto específicas y una subred de administración /22. Ajuste las entradas para que coincidan con los orígenes de administración de confianza del entorno:

```
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
```

Para la construcción de entradas ACL:

- Utilice la palabra clave host seguida de una sola dirección IP para permitir un host de administración específico (por ejemplo, un servidor de salto).
- Para permitir una subred completa, especifique la dirección de red seguida de la máscara comodín adecuada.

2. Aplique la ACL a la clase de acceso de modo silencioso para que las fuentes que coincidan con la ACL puedan conectarse incluso cuando el modo silencioso esté activo:

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

3. Vuelva a habilitar el comando de configuración login block-for si fue eliminado:

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

4. Guarde la configuración:

```
device# write memory
```

5. Supervise el log del sistema para observar si se sigue activando el modo silencioso y el modo de inicio de sesión actual:

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

Cómo abordar la causa raíz de la falla de autenticación persistente

La solución alternativa basada en ACL descrita anteriormente aborda el síntoma (SSH bloqueado por el modo silencioso) pero no aborda la causa subyacente, que es el alto volumen de fallas de autenticación repetidas. Estos fallos son los que activan continuamente el modo silencioso. Para resolver completamente el problema, se debe investigar y resolver el problema de autenticación frecuente.

Causa

Las fallas de acceso SSH intermitentes son causadas por la función IOS-XE Login Block que ingresa en el modo silencioso debido a un alto volumen de intentos de autenticación fallidos repetidos. Ejemplo de bloque de inicio de sesión para configuración:

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

Esta configuración indica al dispositivo IOS XE que entre en modo silencioso y bloquee todas las nuevas conexiones de inicio de sesión durante 120 segundos cada vez que se detecten 3 o más intentos de inicio de sesión fallidos en una ventana de 60 segundos. Un gran volumen de intentos de autenticación fallidos activa constantemente el modo silencioso de inicio de sesión. La aplicación del modo silencioso es global y se aplica a todas las líneas VTY y a todos los puertos TCP configurados para SSH. Cuando el modo silencioso está activo, el dispositivo envía un paquete TCP RST inmediatamente después de recibir un nuevo paquete TCP SYN de cualquier fuente no permitida explícitamente por una ACL de clase de acceso de modo silencioso, lo que evita que se establezca la sesión SSH.

Contenido relacionado

- Guía de Configuración de Seguridad de Cisco IOS-XE: Mejoras en el inicio de sesión (clase de acceso de modo silencioso y bloqueo de inicio de sesión)
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).