Resolva a falha de acesso SSH intermitente em dispositivos IOS XE causada pelo modo silencioso do bloco de login

Contents

Problema

Os dispositivos que executam o software IOS XE exibem falhas intermitentes de acesso SSH. As conexões SSH às vezes são aceitas e às vezes recusadas sem um padrão consistente. O acesso do console aos dispositivos não é afetado. Para uma sessão SSH com falha, as capturas de pacotes realizadas no dispositivo afetado confirmam que o próprio dispositivo estava enviando pacotes TCP RST imediatamente após receber o TCP SYN do cliente, antes mesmo que a sessão SSH pudesse começar a negociar. Com o comando debug ip tcp transactions habilitado, a seguinte saída de depuração ilustra o comportamento 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 os itens a seguir para excluí-los como causas de contribuição:

- Use o comando show ip ssh para confirmar se o SSH está habilitado no dispositivo.
- Use o comando show tcp brief para confirmar se a porta TCP 22 está ouvindo dentro do processo IOSd.
- Não há erro "no port" na saída dos comandos show ip traffic ou debug ip error
- As linhas VTY não são totalmente consumidas; a saída do comando show line não mostra todas as linhas ocupadas.
- O problema permanece após a remoção de qualquer configuração de classe de acesso nas linhas VTY.

O buffer de registro do dispositivo mostrou um volume muito alto de falhas de autenticação repetidas, bem como o modo silencioso ativo:

```
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
```

Uma saída show login no momento da falha mostra o dispositivo no modo silencioso no momento da falha de SSH.

Ambiente

- Plataforma: Switches Cisco Catalyst 9500 Series (switch central e pilhas de switch gerenciado)
- O SSH está habilitado para acesso remoto ao dispositivo
- Configuração de Bloqueio de Logon ativa no dispositivo: bloco de login - para 120 tentativas 3 dentro de 60

Resolução

Esse problema é causado pelo recurso de modo silencioso Bloco de Logon disparado persistentemente por um alto volume de tentativas de autenticação com falha. Para resolver o problema, use uma ACL de classe de acesso de modo silencioso para dispositivos de gerenciamento SSH confiáveis.

Configurar o bloco de login com uma ACL de classe de acesso IP confiável no modo silencioso

Configure o recurso de bloqueio de login e implemente uma ACL de classe de acesso de modo silencioso (Lista de controle de acesso). Essa ACL permite que hosts e sub-redes de gerenciamento confiável ignorem a aplicação do modo silencioso, enquanto a proteção de Bloco de Login permanece ativa para todas as outras origens.

1. Defina uma ACL estendida nomeada que permita os hosts e sub-redes de gerenciamento confiáveis. O exemplo a seguir permite dois IPs de host de salto específicos e uma sub-rede de gerenciamento /22. Ajuste as entradas para corresponderem às origens de gerenciamento confiável no 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
```

Para a construção da entrada ACL:

- Use a palavra-chave host seguida por um único endereço IP para permitir um host de gerenciamento específico (por exemplo, um servidor de salto).
- Para permitir uma sub-rede inteira, especifique o endereço de rede seguido pela máscara curinga apropriada.

2. Aplique a ACL à classe de acesso de modo silencioso para que as origens correspondentes à ACL possam se conectar mesmo quando o modo silencioso estiver ativo:

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

3. Reative o comando de configuração login block-for se ele tiver sido removido:

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

4. Salve a configuração:

```
device# write memory
```

5. Monitore o log do sistema para observar se o modo silencioso continua a ser acionado e o modo de login atual:

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

Abordando a causa raiz da falha de autenticação persistente

A solução alternativa baseada em ACL descrita acima trata do sintoma (SSH sendo bloqueado pelo modo silencioso), mas não trata da causa subjacente, que é o alto volume de falhas de autenticação repetidas. Essas falhas são o que aciona continuamente o modo silencioso. Para resolver completamente o problema, o problema frequente de autenticação deve ser investigado e resolvido.

Causa

As falhas intermitentes de acesso SSH são causadas pelo recurso IOS-XE Login Block entrar no modo silencioso devido a um alto volume de repetidas tentativas de autenticação com falha. Exemplo de bloqueio de login para configuração:

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

Essa configuração instrui o dispositivo IOS XE a entrar no modo silencioso e bloquear todas as novas conexões de login por 120 segundos sempre que 3 ou mais tentativas de login com falha forem detectadas em uma janela de 60 segundos. Um alto volume de tentativas de autenticação com falha dispara constantemente o modo silencioso de login. A aplicação do modo silencioso é global e se aplica a todas as linhas VTY e a todas as portas TCP configuradas para SSH. Quando o modo silencioso está ativo, o dispositivo envia um pacote TCP RST imediatamente após receber um novo pacote TCP SYN de qualquer origem não permitida explicitamente por uma ACL de classe de acesso de modo silencioso, impedindo que a sessão SSH seja estabelecida.

Conteúdo relacionado

- Guia de configuração de segurança do Cisco IOS-XE: Aprimoramentos de login (login block-for e quiet-mode access-class)

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.