# Résolution des défaillances d'accès SSH intermittentes sur les périphériques IOS XE causées par le mode silencieux de blocage de connexion

## Table des matières

## Problème

Les périphériques exécutant le logiciel IOS XE présentent des pannes d'accès SSH intermittentes. Les connexions SSH sont parfois acceptées et parfois refusées sans motif cohérent. L'accès console aux périphériques n'est pas affecté. Dans le cas d'une session SSH ayant échoué, les captures de paquets effectuées sur le périphérique concerné confirment que le périphérique lui-même envoyait des paquets RST TCP immédiatement après avoir reçu le SYN TCP du client, avant même que la session SSH puisse commencer à négocier. Lorsque la commande debug ip tcp transactions est activée, le résultat de débogage suivant illustre le comportement 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
```

Vérifiez les éléments suivants pour les exclure en tant que causes contributives :

- Utilisez la commande show ip ssh pour confirmer que SSH est activé sur le périphérique.
- Utilisez la commande show tcp brief pour confirmer que le port TCP 22 écoute à l'intérieur du processus IOSd.
- Il n'y a pas d'erreur « no port » dans le résultat de la commande show ip traffic ou debug ip error
- les lignes VTY ne sont pas entièrement consommées ; le résultat de la commande show line

n'affiche pas toutes les lignes occupées.

- Le problème persiste après la suppression de toute configuration access-class sur les lignes VTY.

La mémoire tampon de journalisation du périphérique présentait un volume très élevé d'échecs d'authentification répétés, ainsi que le mode silencieux actif :

```
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
```

Une sortie show login au moment de la défaillance montre le périphérique en mode silencieux au moment de la défaillance SSH.

## Environnement

- Plate-forme : Commutateurs de la gamme Cisco Catalyst 9500 (commutateurs principaux et piles de commutateurs administrables)
- SSH est activé pour l'accès à distance au périphérique
- Login Bloquer la configuration active sur le périphérique : login block-for 120 attempts 3 within 60

## Résolution

Ce problème est causé par la fonctionnalité de mode silencieux Login Block qui est continuellement déclenchée par un grand nombre de tentatives d'authentification ayant échoué. Pour résoudre le problème, utilisez une liste de contrôle d'accès de classe d'accès en mode silencieux pour les périphériques de gestion SSH approuvés.

### Configuration du bloc de connexion avec une liste de contrôle d’accès de classe d’accès IP sécurisée en mode silencieux

Configurez la fonctionnalité de blocage de connexion et implémentez une liste de contrôle d’accès access-class en mode silencieux (Access Control List). Cette liste de contrôle d’accès permet aux hôtes et sous-réseaux de gestion approuvés de contourner l’application du mode silencieux tandis que la protection Login Block reste active pour toutes les autres sources.

1. Définissez une liste de contrôle d’accès étendue nommée qui autorise les hôtes et sous-réseaux de gestion approuvés. L'exemple suivant autorise deux adresses IP d'hôte de saut spécifiques et un sous-réseau de gestion /22. Ajustez les entrées en fonction des sources de gestion approuvées dans l'environnement :

```
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
```

Pour la construction des entrées ACL :

- Utilisez le mot clé host suivi d'une adresse IP unique pour autoriser un hôte de gestion spécifique (par exemple, un serveur de saut).
- Pour autoriser un sous-réseau entier, spécifiez l'adresse réseau suivie du masque générique approprié.

2. Appliquez la liste de contrôle d’accès à la classe access-class en mode silencieux afin que les sources correspondant à la liste de contrôle d’accès soient autorisées à se connecter même lorsque le mode silencieux est actif :

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

3. Réactivez la commande de configuration login block-for si elle a été supprimée :

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

4. Enregistrez la configuration :

```
device# write memory
```

5. Surveillez le journal système pour vérifier si le mode silencieux continue à être déclenché et le mode de connexion actuel :

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

### Résolution de la cause première de l'échec d'authentification persistant

La solution de contournement basée sur ACL décrite ci-dessus résout le symptôme (SSH bloqué par le mode silencieux) mais ne résout pas la cause sous-jacente, qui est le volume élevé d'échecs d'authentification répétés. Ces défaillances sont ce qui déclenche continuellement le mode silencieux. Pour résoudre complètement le problème, le problème fréquent d'authentification doit être examiné et résolu.

## Motif

Les échecs d'accès SSH intermittents sont causés par la fonction IOS-XE Login Block qui passe en mode silencieux en raison d'un grand nombre de tentatives d'authentification répétées et infructueuses. Exemple de configuration login block-for :

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

Cette configuration indique au périphérique IOS XE de passer en mode silencieux et de bloquer toutes les nouvelles connexions pendant 120 secondes chaque fois que 3 tentatives de connexion infructueuses ou plus sont détectées dans une fenêtre de 60 secondes. Un grand nombre de tentatives d'authentification échouées déclenche constamment le mode silencieux de connexion. L'application du mode silencieux est globale et s'applique à toutes les lignes VTY et à tous les ports TCP configurés pour SSH. Lorsque le mode silencieux est actif, le périphérique envoie un paquet RST TCP immédiatement après avoir reçu un nouveau paquet SYN TCP d'une source non explicitement autorisée par une liste de contrôle d'accès de classe d'accès en mode silencieux, empêchant ainsi l'établissement de la session SSH.

## Autres informations utiles

- Guide de configuration de la sécurité Cisco IOS-XE : Améliorations de connexion (login block-for et quiet-mode access-class)
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.