

Blocage et blocage du déploiement de CLISH pendant la commande ping/traceroute de CLISH à long terme

Table des matières

Problème

Sur les plates-formes Cisco Secure Firewall Firepower (versions 7.6.4, 7.7 et 10.0.0), lorsque plusieurs sessions SSH sont actives sur le même périphérique, l'exécution d'une commande longue (telle qu'une requête ping continue) dans une session à l'aide de l'interface CLI CLISH empêche d'autres commandes CLI de se terminer dans d'autres sessions ou CLISH. Par exemple, si un administrateur lance une requête ping continue dans une session CLISH SSH et tente d'exécuter des commandes show dans une autre session CLISH, les commandes suivantes se bloquent jusqu'à ce que la commande longue se termine ou soit abandonnée. Dans certaines versions, la requête ping longue ne peut pas être abandonnée CLISH, conduisant à un verrouillage de déploiement ou CLISH. L'utilisation directe du mode expert ou du moteur LINA (via le support système `diagnostic-cli`) permet un fonctionnement sans ce comportement de blocage.

Environnement

- Plates-formes matérielles Cisco Secure Firewall Firepower : Gammes 1000, 1200 et 4200
- Versions logicielles : 7.6.4, 7.7, 10.0.0
- Plusieurs sessions SSH (utilisateurs identiques ou différents) sur le même périphérique
- CLISH interface CLI
- Mode expert et utilisation de la CLI de diagnostic LINA
- Testé avec des commandes : ping, traceroute, show sip, show ip, show conn, show xlate
- Problème reproduit sur les appareils FPR1010, FPR1200 et FPR4200
- Défauts associés: CSCws82823, CSCwb84748

Résolution

Le problème présente les symptômes suivants :

- Établissez deux sessions SSH vers le périphérique en utilisant des informations d'identification d'utilisateur différentes ou identiques.
- Dans la session 1, exécutez une requête ping de longue durée avec un nombre élevé de répétitions à partir de l'invite FTD CLISH.

```
> ping 1.1.1.1 repeat 2000
```

ATTENTION : si vous effectuez un test, essayez avec des nombres de comptage plus petits, un nombre tel que 2000 peut prendre des heures.

REMARQUE : une commande ping/traceroute dans CLISH n'affiche pas de caractères de progression comme on le voit normalement directement dans l'interface de ligne de commande LINA.

- Dans la session 2, essayez d'exécuter une autre commande LINA dans CLISH, telle que « show sip ».

```
> show sip
```

- La commande de la session 2 ne se termine pas tant que la requête ping de la session 1 n'est pas terminée ou abandonnée.

Cette résolution est disponible :

- Abandonnez la commande initiale prolongée avec Ctrl+C pour éviter le blocage et le blocage du déploiement CLISH.
- Dans les versions affectées, les requêtes ping longues dans CLISH ne peuvent pas être abandonnées par Ctrl+C ou en fermant la session SSH.
- Si vous tentez de le faire, le processus principal continue et CLISH reste verrouillé pour les autres commandes LINA.
- Si le FTD se trouve dans un tel état, ou s'il est suspecté que le FTD est entré dans un tel état avec une requête ping bloquée et prolongée, un redémarrage du FTD est nécessaire pour récupérer.
- Pour éviter le blocage de CLISH/déploiement, exécutez directement les commandes LINA à l'aide du moteur LINA. Cette méthode ne présente pas de comportement défectueux.

```
> system support diagnostic-cli  
firepower# ping 1.1.1.1 repeat 2000
```

- Les commandes exécutées via l'interface de ligne de commande de diagnostic LINA ne bloquent pas les processus CLISH ou de déploiement dans d'autres sessions. Cependant, la prise en charge par le système de l'interface de ligne de commande de diagnostic autorise seulement un utilisateur CLI par session.

Considérations et observations supplémentaires :

- Les commandes traceroute peuvent généralement être abandonnées dans CLISH,

mais elles peuvent toujours entraîner un blocage temporaire (~3 minutes) des nouvelles commandes LINA dans d'autres sessions.

- Les opérations de déploiement lancées à partir du Centre de gestion du pare-feu sécurisé ou du Gestionnaire de périphériques peuvent être retardées ou bloquées si une requête ping de longue durée est active dans CLISH, car les deux processus utilisent des méthodes synchrones et attendent la fin (jusqu'à 10 minutes).
- Ce comportement de blocage est par conception pour les opérations de processus synchrones ; cependant, l'incapacité d'abandonner a été introduite par le défaut.

Motif

La cause principale est un défaut (ID de bogue Cisco CSCws82823) qui a supprimé par inadvertance le code requis de certaines commandes CLI dans CLISH, empêchant le moteur LINA de reconnaître et de gérer correctement les commandes qui s'exécutent depuis longtemps. Cela a entraîné la perte de la fonctionnalité d'abandon de Ctrl+C et a entraîné le blocage de CLISH, bloquant d'autres commandes et opérations de déploiement jusqu'à ce que la commande longue soit terminée. Le comportement de blocage est dû à la nature synchrone du traitement des commandes CLISH.

Autres informations utiles

- [Référence des commandes de Cisco Secure Firewall Threat Defense : Utilisation de l'interface de ligne de commande \(CLI\)](#)
- [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.