Échec de l'interface de gestion FTD après la mise à niveau de 7.4.3 à 7.6.4

Table des matières

Problème

Après la mise à niveau d'une paire Cisco Secure Firewall 3130 Threat Defense (FTD) High Availability (HA) de la version 7.4.3 à la version 7.6.4, l'unité principale a semblé échouer à 99 % sur le centre de gestion des pare-feu (FMC) et n'a plus répondu. L'unité secondaire a été mise à niveau et est devenue active dans la paire haute disponibilité. L'unité principale ne répondait pas aux connexions SSH et le FMC n'a pas pu communiquer avec elle.

Après enquête, cette erreur critique a été observée sur FXOS :

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

Les journaux de mise à niveau FTD ont montré que la mise à niveau s'était réellement terminée correctement (100 % effectués), mais que le service SFTunnel ne démarrait pas correctement, empêchant la communication entre FTD et FMC. Le périphérique pouvait envoyer une requête ping à lui-même, à sa passerelle et à l'unité FTD homologue, mais ne pouvait pas atteindre les FMC qui résidaient sur des sous-réseaux différents.

Environnement

- Paire de pare-feu Cisco Secure Firewall 3130 Threat Defense HA
- Version logicielle originale : DFT 7.4.3
- Version du logiciel cible : FTD 7.6.4 (build 69)
- Système d'exploitation extensible Cisco Firepower (FX-OS) v2.16.1 (build 147)

- Interface de gestion configurée avec un adressage IP statique
- Serveurs FMC situés sur des sous-réseaux différents du réseau de gestion FTD

Résolution

Le problème a été résolu en reconfigurant complètement l'interface de gestion sur l'unité FTD concernée. Les étapes suivantes ont été effectuées :

Étape 1: Connectez-vous au FTD via l'accès à la console car SSH ne fonctionnait pas.

Étape 2: Vérifiez l'état d'achèvement de la mise à niveau en consultant les journaux de mise à niveau :

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

Étape 3: Confirmez la défaillance de l'interface de gestion sur FXOS :

```
device# show fault
```

Étape 4: Essayez un dépannage de base en reconfigurant l'adresse IP de gestion (cela n'a pas résolu le problème).

Étape 5: Effectuez un redémarrage à froid (cela n'a pas résolu le problème).

Étape 6: Désactivez complètement l'interface management0 de l'interface de ligne de commande FTD :

```
configure network management-interface disable management0
```

Étape 7: Réactivez l'interface management0 :

```
configure network management-interface enable management0
```

Étape 8: Reconfigurez les paramètres réseau de l'interface de gestion :

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

Étape 9: Vérifiez que les alertes FXOS ont été effacées et que le FTD peut maintenant envoyer une requête ping au FMC :

```
root@device:/# ping <FMC_IP_address>
```

Étape 10: Redémarrez le service SFTunnel à l'aide du script manage_procs.pl :

```
manage_procs.pl restart sftunnel
```

Étape 11: Vérifiez la connectivité du tunnel SFT :

```
root@device:/# sftunnel_status.pl
```

Étape 12: Testez la fonctionnalité de basculement pour vous assurer que les opérations de haute disponibilité fonctionnent correctement.

Une fois ces étapes effectuées, le FTD a pu communiquer correctement avec le FMC et tous les tests de connectivité et de basculement ont réussi. La mise à niveau du correctif peut alors être appliquée sans problème.

Motif

La cause principale était l'échec de l'initialisation correcte de l'interface de gestion après la mise à niveau FTD de 7.4.3 à 7.6.4, malgré le succès du processus de mise à niveau. La configuration de l'interface de gestion hors bande de la machine à état fini (FSM) a échoué pendant le processus de mise à niveau, empêchant l'interface de gestion d'établir une connectivité appropriée. Ce comportement a été documenté dans le bogue Cisco ayant l'ID CSCww08417.

Ce problème est similaire aux défauts signalés précédemment, à savoir l'ID de bogue Cisco CSCwj04154 et l'ID de bogue Cisco CSCwa69303, mais se produit dans des conditions différentes. La défaillance de l'interface de gestion a créé une fausse impression d'échec de la mise à niveau à 99 %, alors qu'en réalité la mise à niveau s'était terminée avec succès mais que la connectivité de gestion était rompue.

Autres informations utiles

- ID de bogue Cisco CSCww08417 - Échec possible du démarrage de l'interface de gestion FTD après la mise à niveau
- Guide de compatibilité de Cisco Secure Firewall Threat Defense
- 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.