Dépannage d'une défaillance de formation de cluster d'équilibrage de charge VPN après la mise à niveau ASA ou FTD vers la version de durcissement Septembre 2026

Table des matières

- Problème
- Environnement
- Résolution
  - Option 1: Mise à niveau complète (recommandée)
  - Option 2: Méthode de mise à niveau transparente (ASA uniquement)
  - Étapes de vérification
- Motif
- Autres informations utiles

Problème

Après la mise à niveau des périphériques Cisco ASA ou FTD vers l'une des versions publiées dans le cadre de la version de sécurisation renforcée de septembre 2026, les clusters d'équilibrage de charge VPN (VPN LB) ne se forment pas. Les périphériques connaissent des échecs de connexion répétés, comme indiqué dans le résultat du débogage :

```
device# debug vpnlb 125
debug vpnlb enabled at level 125
device# 5718045: Created peer[198.51.100.1]
5718012: Sent HELLO request to [198.51.100.1]
```

```
5718061: Inbound socket read fail: context=0.
7718036: Process timeout for req-type[13], exid[304], peer[198.51.100.1]
6718038: Slave processed 1 timeouts
5718028: Send OOS indicator failure to [198.51.100.1]
5718056: Deleted Master peer, IP 198.51.100.1
5718044: Deleted peer[198.51.100.1]
7718017: Got timeout for unknown peer[198.51.100.1] msg type[25]
```

Lorsque le chiffrement de cluster est désactivé, le cluster d'équilibrage de charge VPN se forme correctement. Cependant, la réactivation du cryptage entraîne l'échec de la formation du cluster et aucun message de débogage IKEv1 n'est affiché malgré la configuration terminée.

Cette question n'affecte que la coordination entre les membres au sein du groupe ; Les sessions client VPN d'accès à distance ne sont pas abandonnées. Le membre de cluster affecté ne participe pas à l'équilibrage de charge VPN tant qu'il n'est pas mis à niveau.

Environnement

- Cisco Secure Firewall ASA ou FTD
- Version du logiciel ASA ou FTD contenant le correctif pour la version de durcissement : Septembre 2026
- Configuration de l'équilibrage de charge VPN avec chiffrement de cluster activé
- Stratégies IKEv1 configurées pour la communication de cluster

Résolution

Deux options validées sont disponibles pour résoudre ce problème :

Option 1: Mise à niveau complète (recommandée)

Mettez à niveau tous les membres du cluster vers la même version du logiciel ASA ou FTD. Le cluster se reforme automatiquement une fois que tous les membres exécutent la même version.

Tant que tous les membres du cluster n'ont pas été mis à niveau, les membres qui exécutent des versions plus anciennes restent désynchronisés de ceux qui exécutent des versions plus récentes.

Étape 1: Vérifier les versions logicielles actuelles sur tous les membres du cluster :

```
device# show version
```

Étape 2: Mettez à niveau les membres restants du cluster vers la même version logicielle ASA ou FTD.

Étape 3: Vérifiez la formation du cluster après toutes les mises à niveau :

```
device# show vpn load-balancing
```

Option 2: Méthode de mise à niveau transparente (ASA uniquement)

Supprimez temporairement la clé de cluster sur tous les membres pendant le processus de mise à niveau, puis réappliquez-la après la mise à niveau de tous les périphériques.

Étape 1: Supprimez la clé de cluster de tous les membres du cluster :

```
device(config)# vpn load-balancing
device(config-load-balancing)# no cluster key
```

Étape 2: Mettez à niveau tous les membres du cluster vers la même version du logiciel ASA.

Étape 3: Réappliquez la clé de cluster à tous les membres après la fin de la mise à niveau :

```
device(config)# vpn load-balancing
device(config-load-balancing)# cluster key your-cluster-key
```

Important : La simple suppression du chiffrement de cluster ne suffit pas : la clé de cluster doit être complètement supprimée lors du processus de mise à niveau.

Cette solution de contournement ne s'applique pas aux périphériques FTD, car le chiffrement est obligatoire pour les périphériques FTD gérés par FMC.

Étapes de vérification

Après avoir implémenté l'une ou l'autre option, vérifiez le bon fonctionnement du cluster.

Étape 1: Vérifiez les versions actuelles du logiciel sur tous les membres du cluster :

```
device# show version
```

Étape 2: Vérifiez que le cluster s'est formé après toutes les mises à niveau :

```
device# show vpn load-balancing
```

Étape 3: Vérifiez la connectivité des homologues :

```
device# debug vpnlb 125
```

Étape 4: Vérifiez que les associations de sécurité IKEv1 sont établies, si le cryptage est activé :

```
device# show crypto ikev1 sa
```

Prenez connaissance de l'ID de bogue Cisco CSCww64385. Ce problème affecte la visibilité de la topologie et le temps de reconvergence, mais n'affecte pas les connexions VPN actives ni le transfert de trafic sur les périphériques mis à niveau.

Motif

Ce problème est causé par une amélioration du renforcement de la sécurité qui ajoute l'authentification à la communication inter-membre du cluster d'équilibrage de charge VPN. Le protocole de sécurité renforcée est incompatible avec les versions ASA ou FTD antérieures, ce qui empêche la formation de clusters dans les déploiements de versions mixtes. Il en résulte une incompatibilité de protocole dans laquelle :

- Les noeuds mis à niveau appliquent le protocole v5 authentifié
- Les noeuds de pré-mise à niveau utilisent le protocole v4 non authentifié
- Les membres mis à niveau nécessitent le protocole renforcé avec lequel les membres plus anciens ne peuvent pas communiquer
- La formation du cluster échoue jusqu'à ce que tous les membres utilisent la même version de protocole

Autres informations utiles

- 'ID de bogue Cisco CSCww64385'
- 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.