Échec de la vérification de l'interface de synchronisation haute disponibilité FTD du pare-feu sécurisé

Table des matières

Problème

Le FTD d'une paire haute disponibilité (HA) était toujours affiché dans l'état Failed. La synchronisation de la configuration ne s'est pas terminée entre les homologues de haute disponibilité, malgré une connectivité IP réussie entre les unités. Il s'agissait d'une nouvelle mise en oeuvre exécutant le logiciel Cisco Secure Firewall Threat Defense, qui n'était pas encore en production.

Le problème est apparu après que l'unité principale a été déplacée vers son emplacement final et que son adresse IP de gestion a été modifiée sans rompre au préalable la paire haute disponibilité. Le processus de haute disponibilité a détecté des contrôles d'interface échoués sur les interfaces de données surveillées, ce qui a déclenché la logique d'évaluation de l'état de haute disponibilité pour placer l'unité principale dans un rôle Échec.

Environnement

- Pare-feu sécurisé FTD HA géré par FMC
- Nouveau déploiement d'une activité de migration, pas encore en production

Résolution

La résolution impliquait la suppression des interfaces de données sélectionnées de la configuration de surveillance d'interface haute disponibilité pour empêcher la détection de

défaillance erronée.

Étapes de dépannage effectuées

1: Les données de dépannage ont confirmé les échecs de vérification de l'interface haute disponibilité sur les interfaces de données surveillées, tandis que la connectivité des homologues haute disponibilité (pulsation et ping) est restée fonctionnelle.

<#root>

```
device# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FailOver Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 776 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.20(2)121, Mate 9.20(2)121
Serial Number: Ours SERIAL#, Mate SERIAL#
Last Failover at: 17:14:25 UTC Mar 16 2026


This host: Primary - Failed

        Active time: 0 (sec)
        slot 0: FPR-1120 hw/sw rev (2.0/9.20(2)121) status (Up Sys)


Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)
          Interface To-DC1-WAN (0.0.0.0): No Link (Waiting)


          Interface management (203.0.113.131/fe80::a610:b6ff:fe3d:e101): Normal (Monitored)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Active
        Active time: 184688 (sec)


Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)


          Interface To-DC1-WAN (10.230.2.2): Normal (Waiting)
          Interface management (203.0.113.130/fe80::6ae5:9eff:fee6:d681): Normal (Monitored)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
```

2: Confirmez que les transitions d'état de haute disponibilité se produisent en fonction des résultats de surveillance des interfaces et non des problèmes de connectivité du plan de gestion - effectué.

<#root>

```
device# show failover history
17:16:51 UTC Mar 16 2026
Standby Ready

Failed                      Interface check



This host:2
                                                    single_vf: To-DC1-ACC
                                                    single_vf: To-DC1-WAN

                                                    Other host:1
                                                    single_vf: To-DC1-ACC
```

Problèmes liés à la modification de la configuration

1: La configuration de haute disponibilité a été mise à jour pour exclure les interfaces de données affectées du contrôle d'état des interfaces, empêchant ainsi la détection de défaillances erronées.

2: Une fois la configuration modifiée, le FTD principal est passé avec succès à l'état Standby Ready, confirmant la synchronisation de haute disponibilité et la stabilité d'état appropriées.

3: Le test de basculement de haute disponibilité s'est terminé avec succès et les résultats attendus ont permis de valider la stabilité de la configuration de haute disponibilité après les modifications.

Clarifications de comportement attendues

Ces comportements observés lors du dépannage sont attendus et par conception :

- Noms d'hôte dupliqués sur les homologues FTD : Les deux unités affichant le même nom d'hôte ont le comportement attendu dans FTD HA, car le nom d'hôte de l'unité active est

présenté à l'échelle du système (suivi sous la demande d'amélioration CSCwe31354)

- Propriété des adresses IP : Seul le FTD actif affiche les adresses IP actives sur les interfaces de données, ce qui est un comportement attendu par la conception pour empêcher les conditions de « split-brain ». Si aucune adresse IP de secours d'interface n'est configurée, le FTD Standby Ready apparaît comme n'ayant aucune adresse IP configurée sur ses interfaces.

Motif

Le FTD principal a été marqué comme étant en échec en raison d'échecs de vérification de l'intégrité de l'interface de haute disponibilité sur les interfaces de données surveillées, ce qui a entraîné le maintien de l'homologue avec davantage d'interfaces opérationnelles actives. Ce comportement est conçu dans FTD High Availability et est documenté dans les directives de haute disponibilité de Cisco Secure Firewall. Le processus de haute disponibilité a détecté des contrôles d'interface échoués sur les interfaces de données surveillées, ce qui a déclenché la logique d'évaluation de l'état de haute disponibilité pour placer l'unité principale dans un rôle Échec.

Autres informations utiles

- Guide de configuration de Cisco Secure Firewall Device Manager - Haute disponibilité (basculement)
- 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.