Sichere Firewall FTD High Availability Sync Interface - Fehler bei der Überprüfung

Inhalt

Problem

Die FTD in einem Hochverfügbarkeitspaar zeigte sich durchgängig im Status Failed (Fehlgeschlagen). Die Konfigurationssynchronisierung zwischen den HA-Peers wurde trotz erfolgreicher IP-Verbindungen zwischen den Geräten nicht abgeschlossen. Bei der Bereitstellung handelte es sich um eine neue Implementierung mit Cisco Secure Firewall Threat Defense-Software, die noch nicht in der Produktionsumgebung eingesetzt wurde.

Das Problem trat auf, nachdem die primäre Einheit an ihren endgültigen Standort verschoben und ihre Management-IP-Adresse geändert wurde, ohne dass zuvor das HA-Paar unterbrochen wurde. Der HA-Prozess erkannte fehlgeschlagene Schnittstellenprüfungen an überwachten Datenschnittstellen, wodurch die HA-Zustandsbewertungslogik ausgelöst wurde, um die primäre Einheit in die Rolle "Fehler" zu versetzen.

Umwelt

- Sichere Firewall FTD HA von FMC verwaltet
- Neue Bereitstellung einer Migrationsaktivität, noch nicht in der Produktion

Auflösung

Die Auflösung beinhaltete das Entfernen ausgewählter Datenschnittstellen aus der Überwachungskonfiguration der HA-Schnittstelle, um eine Erkennung falscher Fehler zu verhindern.

Durchgeführte Schritte zur Fehlerbehebung

1: Die Fehlerbehebung bestätigte, dass die HA-Schnittstelle Fehler an den überwachten Datenschnittstellen überprüft hat, während die HA-Peer-Verbindung (Heartbeat und Ping) weiterhin funktioniert.

<#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: Bestätigt, dass HA-Zustandsübergänge auf der Grundlage von Schnittstellenüberwachungsergebnissen und nicht von Verbindungsproblemen auf Verwaltungsebene stattfanden.

<#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
```

Konfigurationsänderungen

1: Die HA-Konfiguration wurde aktualisiert, um die betroffenen Datenschnittstellen von der Überwachung der Schnittstellenintegrität auszuschließen und so eine Erkennung falscher Fehler zu verhindern.

2: Nach den Konfigurationsänderungen wechselte die primäre FTD erfolgreich in den Status Standby Ready und bestätigte so die ordnungsgemäße HA-Synchronisierung und die Statusstabilität.

3: Der HA-Failover-Test wurde mit den erwarteten Ergebnissen erfolgreich abgeschlossen, um die Stabilität der HA-Konfiguration nach den Änderungen zu überprüfen.

Erwartete Verhaltensklarstellungen

Diese Verhaltensweisen, die während der Fehlerbehebung beobachtet wurden, werden vom Design her erwartet:

- Doppelte Hostnamen auf FTD-Peers: Beide Einheiten, die den gleichen Hostnamen anzeigen, werden in FTD HA erwartet, da der Hostname der aktiven Einheit systemweit angezeigt wird (verfolgt unter Erweiterungsanfrage CSCwe31354).
- Eigentümer der IP-Adresse: Nur die aktive FTD zeigt aktive IP-Adressen an

Datenschnittstellen an, was von der Konstruktion her erwartet wird, um Split-Brain-Bedingungen zu verhindern. Wenn keine Standby-IP-Adressen für die Schnittstelle konfiguriert sind, weist der FTD-Status "Standby Ready" den Anschein auf, dass keine IP-Adressen für die Schnittstellen konfiguriert sind.

Ursache

Der primäre FTD wurde als Failed (Ausgefallen) markiert, da bei überwachten Datenschnittstellen Fehler bei der Integritätsprüfung der Hochverfügbarkeits-Schnittstelle aufgetreten sind, wodurch der Peer mit mehr Betriebsschnittstellen aktiv bleibt. Dieses Verhalten wurde in FTD High Availability entworfen und ist in den Cisco Secure Firewall HA-Richtlinien dokumentiert. Der HA-Prozess erkannte fehlgeschlagene Schnittstellenprüfungen an überwachten Datenschnittstellen, wodurch die HA-Zustandsbewertungslogik ausgelöst wurde, um die primäre Einheit in die Rolle "Fehler" zu versetzen.

Verwandte Inhalte

- Konfigurationsleitfaden für den Cisco Secure Firewall Device Manager - Hohe Verfügbarkeit (Failover)
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.