보안 방화벽 FTD 고가용성 동기화 인터페이스 확인 실패

목차

문제

고가용성(HA) 쌍의 FTD가 지속적으로 실패 상태로 표시되었습니다. 유닛 간의 IP 연결이 성공했음에도 불구하고 HA 피어 간의 컨피그레이션 동기화가 완료되지 않았습니다. 이 구축은 Cisco Secure Firewall Threat Defense 소프트웨어를 실행하는 새로운 구현이었지만 아직 프로덕션 환경에서는 구현되지 않았습니다.

기본 유닛이 최종 위치로 이동하고 HA 쌍을 먼저 중단하지 않고 관리 IP 주소가 변경된 후에 문제가 발생했습니다. HA 프로세스에서 모니터링되는 데이터 인터페이스에 대한 인터페이스 검사 실패를 감지했습니다. 이 경우 HA 상태 평가 로직이 트리거되어 기본 유닛을 Failed 역할에 배치했습니다.

환경

- FMC에서 관리하는 보안 방화벽 FTD HA
- 아직 프로덕션 상태가 아닌 마이그레이션 활동의 신규 구축

해결

해결 방법에는 HA 인터페이스 모니터링 컨피그레이션에서 선택된 데이터 인터페이스를 제거하여 잘못된 오류 탐지를 방지하는 것이 포함됩니다.

수행된 트러블슈팅 단계

1: 트러블슈팅 데이터를 통해 모니터링되는 데이터 인터페이스에서 HA 인터페이스 확인 실패가 확인되었지만 HA 피어 연결(하트비트 및 ping)은 계속 작동하고 있었습니다.

<#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: 관리 플레인 연결 문제가 아닌 인터페이스 모니터링 결과를 기반으로 HA 상태 전환이 발생했음을 확인했습니다.

<#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

구성 변경

1: HA 컨피그레이션이 인터페이스 상태 모니터링에서 영향받는 데이터 인터페이스를 제외하도록 업데이트되어 잘못된 장애 탐지를 방지합니다.

2: 컨피그레이션이 변경된 후 기본 FTD가 성공적으로 Standby Ready(대기 준비) 상태로 전환되어 적절한 HA 동기화 및 상태 안정성을 확인했습니다.

3: HA 장애 조치(failover) 테스트가 성공적으로 완료되었으며, 변경 후 HA 구성의 안정성을 검증했습니다.

예상 동작 설명

트러블슈팅 중에 관찰되는 이러한 동작은 설계에 따라 예상된 것입니다.

- FTD 피어에서 호스트 이름 복제: 활성 유닛 호스트 이름이 시스템 전체에 표시되기 때문에 동일한 호스트 이름을 표시하는 두 유닛 모두 FTD HA에서 동작이 발생할 수 있습니다(개선 요청 CSCwe31354에 따라 추적됨).
- IP 주소 소유권: Active FTD만 데이터 인터페이스에 활성 IP 주소를 표시하며, 이는 스플릿 브레인(split-brain) 상태를 방지하기 위한 설계에 의한 예상 동작입니다. 인터페이스 대기 IP 주소가 구성되어 있지 않으면 Standby Ready FTD는 인터페이스에 구성된 IP 주소가 없는 것으로 나타납니다.

원인

모니터링되는 데이터 인터페이스에서 고가용성 인터페이스 상태 확인 실패로 인해 기본 FTD가 실패로 표시되어 더 많은 운영 인터페이스가 있는 피어가 활성 상태를 유지합니다. 이러한 동작은 FTD High Availability의 설계에 따른 것이며 Cisco Secure Firewall HA 지침에 설명되어 있습니다. HA 프로세스에서 모니터링되는 데이터 인터페이스에 대한 인터페이스 검사 실패를 감지했습니다. 이 경우 HA 상태 평가 로직이 트리거되어 기본 유닛을 Failed 역할에 배치했습니다.

관련 콘텐츠

- Cisco Secure Firewall Device Manager 컨피그레이션 가이드 - 고가용성(장애 조치)
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.