

FDM에서 고가용성 페어링 오류 troubleshooting

목차

문제

라이선스 등록 모드 불일치로 인해 보조 노드가 지속적으로 실패 상태로 전환되는 애플리케이션 동기화 중에 FTD 7.4.2.4를 실행하는 두 Cisco Firepower 1120 어플라이언스 간의 HA(고가용성) 페어링이 실패합니다. 발생한 특정 오류 메시지는 다음과 같습니다.

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

show app-sync-history 명령은 다음과 같은 메시지와 함께 반복되는 실패를 표시합니다.

```
App Sync Status: FAILURE
```

```
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

이 문제는 두 방화벽을 모두 재설정하고, 백업에서 컨피그레이션을 복원하고, 소프트웨어가 FTD 버전 7.4.2.4로 업데이트되고, VDB 및 Snort 버전이 업데이트되고, 라이선스가 새로운 토큰으로 다시 적용된 후에 발생했습니다. 보조 방화벽은 Failed(실패) 상태로 유지되어 HA 완료를 방해하고 방화벽 이중화에 영향을 줍니다.

환경

- 고가용성을 위해 구성된 Cisco Firepower 1120 NGFW 어플라이언스
- FTD(firepower Threat Defense) 버전 7.4.2.4-9
- Snort 검사 엔진: 3.1.53.203 - 175
- VDB: 425.0
- 위치 정보 데이터베이스: 2026-03-07-053

- Smart Licensing에서 PLR(Permanent License Reservation) 모드로 변환된 디바이스
- PLR 변환 후 클라우드 연결을 시도하는 기본 디바이스
- 두 디바이스 모두 백업에서 복원됨

해결

해결책에는 기본 디바이스와 보조 디바이스 간의 라이선스 등록 모드 불일치를 식별 및 수정하고, 클라우드 등록 해제를 수행하고, 전체 구축을 완료하는 작업이 포함됩니다.

1단계: 라이선스 등록 모드 불일치 확인

특정 실패 사유에 대해 app-sync-history를 확인하여 두 디바이스에서 모두 라이선스 등록 모드를 확인합니다.

```
show app-sync-history
```

출력에 다음을 나타내는 장애가 표시됩니다.

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

2단계: 클라우드 등록 취소 수행

Smart Licensing에서 PLR 모드로 전환한 후에도 기본 디바이스가 여전히 클라우드 연결을 시도하고 있으므로 클라우드 등록 취소가 필요합니다.

FDM UI에서 임시 프록시를 구성합니다(구성된 프록시가 없는 경우).

System Settings(시스템 설정) > See More(자세히 보기) > HTTP Proxy(HTTP 프록시) 탭으로 이동하여 임시로 더미 프록시를 구성합니다(나중에 제거할 수 있음).

FTD 디바이스에 SSH를 입력하고 커넥터 스크립트를 실행합니다.

```
ssh admin@<device-ip>
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

3단계: 포트 8989 충돌 해결

커넥터 스크립트가 다음 오류로 인해 실패하는 경우:

```
Error: listen tcp :8989: bind: address already in use
```

포트 8989(일반적으로 Cisco Success Network)를 사용하여 프로세스를 식별하고 종료합니다.

```
netstat -tulpn | grep 8989
kill <pid>
```

4단계: 클라우드 등록 취소 완료

포트 충돌을 해결한 후 커넥터 스크립트를 다시 실행합니다.

```
/ngfw/var/sf/bin/connector.sh
```

성공적으로 실행되면 다음과 유사한 출력이 표시되어야 합니다.

```
Starting connector
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https_proxy=http://1xx.xx.x
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http_proxy=http://1xx.xx.x
```

FDM GUI, System Settings(시스템 설정) > Cloud Services(클라우드 서비스) > Cloud Services(클라우드 서비스)로 이동하고 등록 취소 옵션을 클릭합니다. 디바이스가 클라우드 서비스에서 등록 취소되었는지 확인합니다.

5단계: 전체 구축 수행 및 HA 재개

클라우드 등록 해제 후에도 HA 페어링이 동일한 라이선스 불일치 오류로 계속 실패할 경우, FDM 인터페이스를 통해 액티브 유닛에서 전체 구축을 수행합니다.

Deploy(구축) > Deploy Now(지금 구축)로 이동하여 구축 프로세스를 완료합니다.

구축이 완료되면 HA 형성을 다시 시도합니다. 디바이스는 연결된 인터페이스와 준비 상태의 액티브-스탠바이 HA 쌍을 성공적으로 구성해야 합니다.

6단계: HA 상태 확인

성공적인 HA 형성 확인:

```
show failover
```

출력은 동기화 성공 시 적절한 HA 상태에서 두 유닛을 모두 표시해야 합니다.

원인

근본 원인은 기본 및 보조 Firepower 1120 디바이스 간의 라이선스 등록 모드 불일치입니다. 디바이스가 Smart Licensing에서 PLR(Permanent License Reservation) 모드로 변환되었습니다. 그러나 기본 디바이스가 계속 클라우드 연결을 시도하여 HA 검증 중에 라이선스 에이전트/내보내기 컴플라이언스 상태가 일치하지 않게 되었습니다. 이로 인해 응용 프로그램을 동기화하는 동안 FDM/FIM 유효성 검사에 반복적으로 실패했습니다. 또한 클라우드 등록 취소는 초기에 Cisco Success Network와 관련된 포트 8989 충돌로 인해 차단되었으며, 등록을 취소하기 전에 해결해야 했습니다.

관련 콘텐츠

- [Air-Gapped Network에 영구 라이선스 적용](#)
- [보안 방화벽 위협 방어 재이미지화](#)
- [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.