응답하지 않는 Cisco Secure Firewall 문제 해결

목차

소개

이 문서에서는 1xxx, 12xx, 21xx, 31xx, 41xx, 42xx 및 93xx 하드웨어 플랫폼에서 응답이 없는 Cisco FTD(Secure Firewall Threat Defense) 문제를 해결하기 위한 권장 단계에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure FTD 기본 사항(설치/구성)

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall 위협 방어
- Cisco Secure Firewall 관리 센터
- Cisco FXOS(Firepower eXtensible 운영 체제)

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco FTD 디바이스가 응답하지 않는 경우도 있습니다. 일반적인 증상은 다음과 같습니다.

- SSH 액세스 없음.
- 콘솔 액세스 없음.
- 콘솔 액세스는 작동하지만 로그인 자격 증명은 작동하지 않습니다.
- 통과 트래픽이 장치를 통과하지 못합니다.
- 인터페이스가 다운되었습니다(데이터 및/또는 관리).
- LED가 꺼져 있거나 주황색입니다(깜박이거나 고정되어 있음).
- 보안 모듈(4100, 9300)이 응답하지 않습니다.

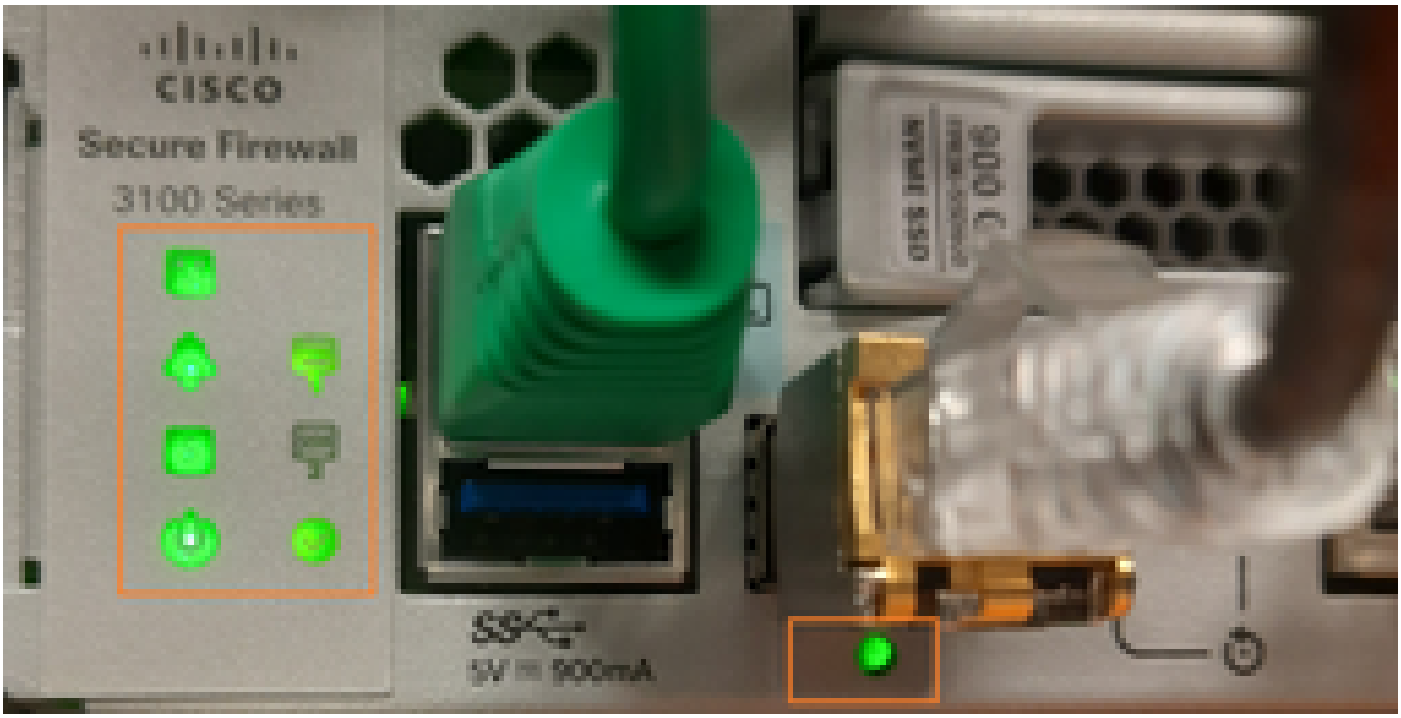
상황에 따라 일부는 참석하지 않을 것입니다. 예를 들어 통과 트래픽이 통과할 수 있지만 관리 액세스만 작동하지 않습니다.

문제 해결

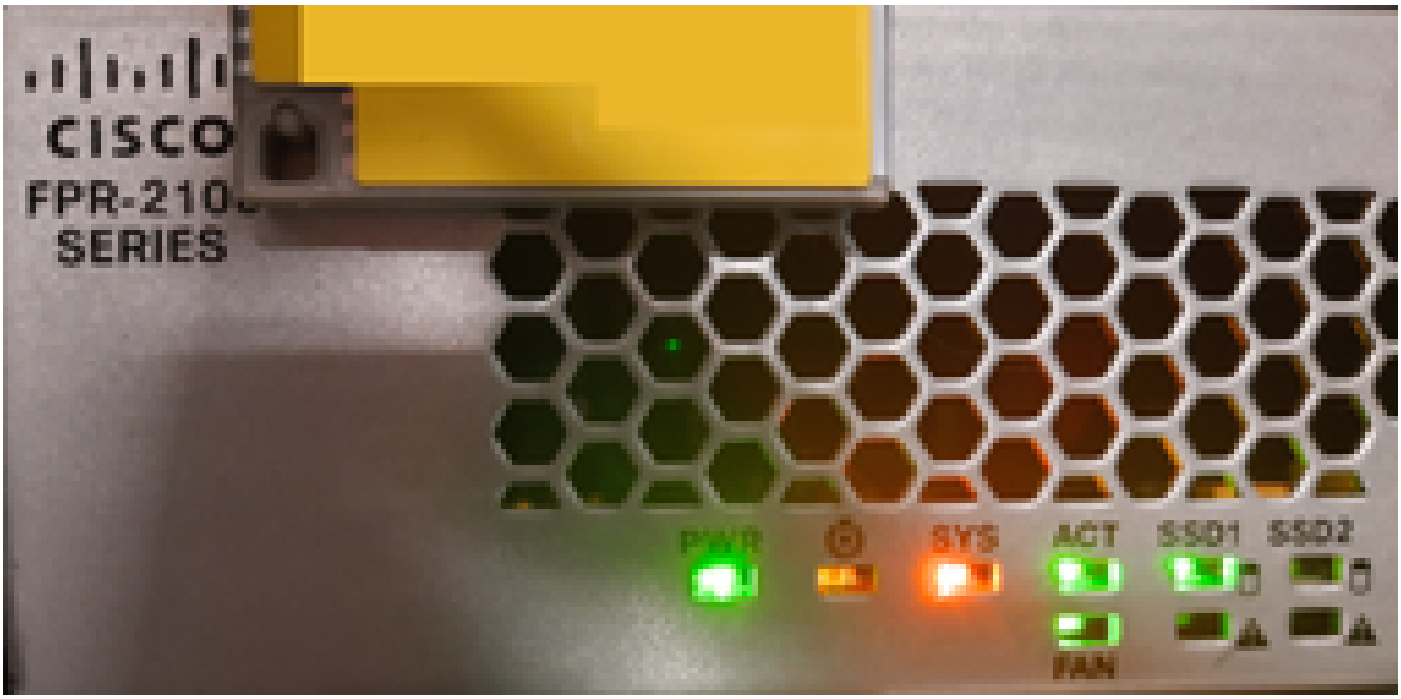
이 섹션에서는 사용자가 취해야 하는 권장 단계 및 작업에 대해 설명합니다. 자세한 분석을 위해 이 정보를 Cisco TAC에 제공할 수 있습니다.

1단계: 시각적 검사(전면 패널)

전면 패널 LED의 비디오 또는 사진을 찍습니다. 다음은 모든 LED가 선명하게 보이는 몇 가지 예입니다.



다음 사진에서 SYS LED는 디바이스 문제를 나타냅니다.



장치 모델의 하드웨어 가이드를 참조하여 LED에 대한 추가 정보를 확인할 수 있습니다. 예를 들면 다음과 같습니다.

모델	LED 정보
1010	https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010/overvie
1100	https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-11001/overvi
1210CE, 1210CP, 1220CX	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1210-20/hw-install-121
1230, 1240, 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install-1
2100	https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100/ov
3100	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/3100/fw-3100-install/m-
4110, 4120, 4140,	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/ov

4150	
4112, 4115, 4125, 4145	https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5/overview.ht
4200	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200-install/m-
9300	https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300/b_

2단계: 시각적 검사(후면 패널)

후면 패널의 LED를 비디오로 촬영하거나 사진을 찍습니다. 예를 들면 다음과 같습니다.

전원 LED(Power LED)가 표시되지 않는 경우:

- 전원 공급 장치를 재장착합니다(해당하는 경우).
- 가능하면 전원 공급 장치를 교체해 보십시오.

3단계: 팬 확인

어플라이언스 뒷면의 팬이 실행 중인지 확인합니다.

4단계: 물리적 환경 검사

디바이스에서 발생하는 소음이나 냄새가 있는지 확인합니다.

5단계: 콘솔 및 관리 포트 검사

콘솔 및 관리 포트가 제대로 연결되어 있는지 확인합니다. 문제가 관리 포트에만 있는 경우 SFP(해당되는 경우 항상)와 네트워크 케이블을 변경하십시오.

6단계: 관리 IP 연결 테스트

디바이스의 관리 IP를 ping(ICMP)해 봅니다.

7단계: 인접 디바이스 검사

인접 디바이스의 포트 상태를 확인합니다. 예를 들면 다음과 같습니다.

<#root>

switch#

show interface description | i FW-4215-1

```
Gi7/1                          up             up       FW-4215-1 ETH1/1
Gi7/2                          up             up       FW-4215-1 ETH1/2
Gi7/3                          up             up       FW-4215-1 MGMT
```

8단계: HA/클러스터 디바이스 검사

고가용성(HA) 또는 클러스터 설정의 경우 피어 디바이스에서 문제 해결 번들을 수집합니다.

9단계: 콘솔 로그 수집

노트북 컴퓨터를 콘솔 포트에 연결하고 표시된 메시지를 복사합니다. 화면의 모든 메시지를 보려면

위쪽/아래쪽 키보드 키 또는 PageUp을 눌러보십시오.

10단계: 콜드 재부팅 수행

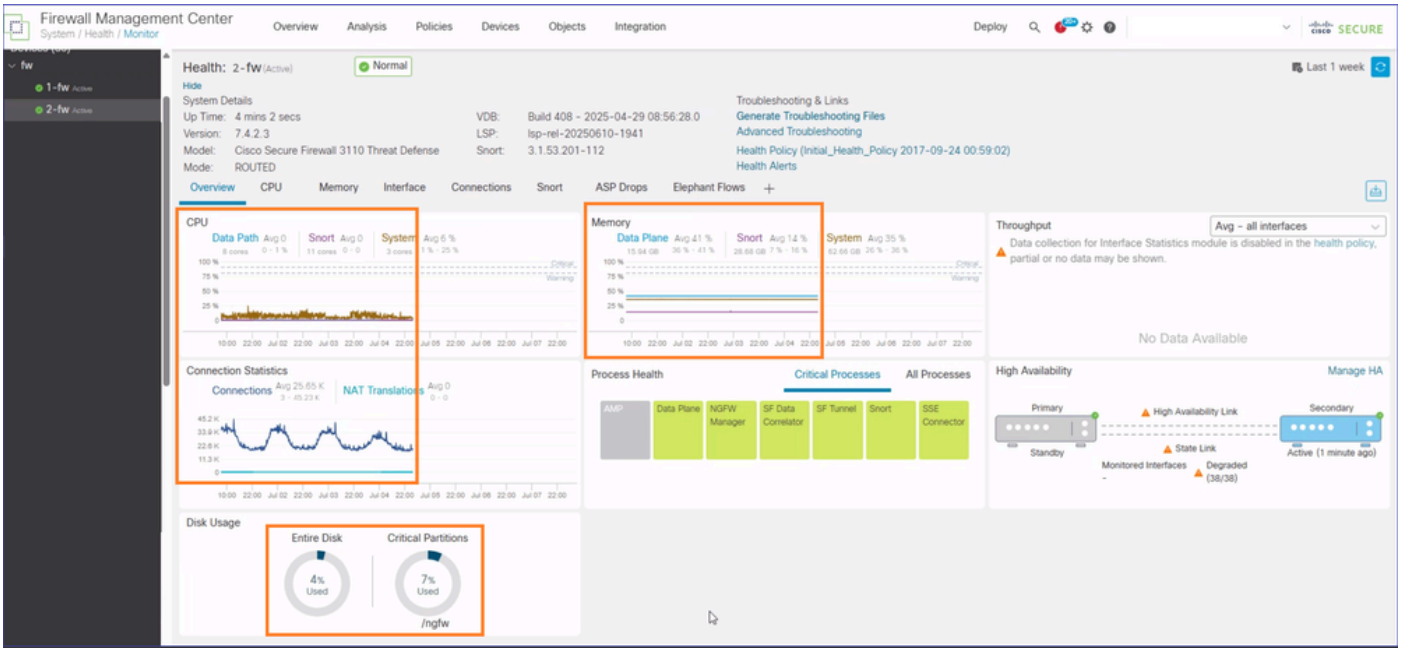
노트북 컴퓨터가 콘솔 포트에 연결된 경우:

1. 모든 전원 케이블을 뽑고 다시 꽂기 전에 몇 분 정도 기다립니다.
2. 장애 조치 설정 또는 클러스터 설정의 경우 액티브/액티브 또는 클러스터 불안정의 위험을 최소화하기 위해 HA 또는 CCL 링크를 포함하여 영향을 받는 유닛의 모든 데이터 인터페이스를 인접한 스위치 디바이스에서 분리하거나 종료할 수 있습니다.
3. 그런 다음 전원 케이블을 다시 연결하고 디바이스의 전원을 켭니다.
4. ~5분 정도 기다립니다.
5. 콘솔 출력을 수집합니다.

디바이스가 정상적으로 종료되지 않았고 디바이스가 작동 중이었던 경우(전면 패널 LED가 켜져 있는 경우) 콜드 리부팅으로 인해 데이터베이스가 손상될 수 있습니다. 콜드 리부팅으로 디바이스가 가동되는 경우, 문제 해결 번들을 수집하고 Cisco TAC에 문의하십시오.

11단계: FMC에서 상태 모니터 그래프 수집

디바이스가 복구되고 FMC에 의해 관리되는 경우 System > Health > Monitor로 이동하여 디바이스를 선택합니다. 강조 표시된 그래프에 초점을 맞추어 무응답 상태가 되기 전의 디바이스 상태(예: 높은 메모리, 높은 CPU, 높은 디스크 사용률 등)를 파악합니다.



12단계: 디스크 문제 확인

비작동 시나리오(4100):

<#root>

```
FW4100#

show server storage


Server 1/1:
    RAID Controller 1:
        Type: SATA
        Vendor: Cisco Systems Inc
        Model: FPR4K-PT-01
        Serial: JAD12345678
        HW Revision:
        PCI Addr: 00:31.2
        Raid Support:
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Unknown

        Local Disk 1:
           Vendor: Micron
           Model: 5300 MTFD
           Serial: MSA123456AB
           HW Rev:
           Operability: N/A


       Presence: Missing <-----


           Size (MB): 200000
           Drive State: Online
           Power State: Active
           Link Speed: 6 Gbps
           Device Type: SSD

          Local Disk Config Definition:
             Mode: NO RAID
             Description:
             Protect Configuration: No
```

디스크가 작동하는 3100의 샘플 출력:

<#root>

```
FW3105#

show server storage


Server 1/1:
    Disk Controller 1:
        Type: SOFTRAID
        Vendor: Cisco Systems Inc
        Model: FPR_SOFTRAID
```

```
        HW Revision:
        PCI Addr:
        Raid Support: raid1
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Optimal

        Local Disk 1:
            Presence: Equipped
            Model: SAMSUNG MZQL2960HCJR-00A07
            Serial: S64FNT0AB12345


Operability: Operable   <---


            Size (MB): 858306
            Device Type: SSD
            Firmware Version: GDC5A02Q

        Virtual Drive 1:
            Type: Raid
            Blocks: 878906048
            Operability: Degraded
            Presence: Equipped
            Size (MB): 858306
            Drive State: Degraded
```

디스크가 작동하는 4100의 샘플 출력:

```
<#root>

FW4125#

show server storage


Server 1/1:
    RAID Controller 1:
        Type: SATA
        Vendor: Cisco Systems Inc
        Model: FPR4K-PT-01
        Serial: JAD1234567
        HW Revision:
        PCI Addr: 00:31.2
        Raid Support:
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Unknown

        Local Disk 1:
            Vendor: TOSHIBA
            Model: KHK61RSE
            Serial: 11BS1234567AB
            HW Rev: 0


Operability: Operable
```

```
        Presence: Equipped
        Size (MB): 800000
        Drive State: Online
        Power State: Active
        Link Speed: 6 Gbps
        Device Type: SSD

    Local Disk Config Definition:
        Mode: No RAID
        Description:
        Protect Configuration: No
```

13단계: 로그 분석

방화벽 디바이스가 복구되고 백엔드 로그를 분석하려는 경우, 문제 해결 번들을 생성하고 표에 나와 있는 파일을 확인하십시오. 다음 사항에 유의하십시오.

- 1xxx, 12xx, 21xx(어플라이언스 모드), 31xx, 42xx 플랫폼의 경우 FTD 트러블슈팅 번들에는 \dir-archives\var-common-platform_ts\ 경로에 있는 FXOS의 섀시(FPRM) 번들도 포함됩니다. FPRM 번들의 내용을 추출해야 합니다.
- MI(Multi-Instance) 모드의 3100/4200에서는 https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400에 설명된 대로 FMC UI 또는 섀시 CLI(local-mgmt 명령 범위에서 show tech-support fprm detail)에서 섀시 TS 파일을 수집합니다.
- 41xx, 93xx 플랫폼에서는 https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400에 설명된 대로 섀시 UI 또는 FXOS CLI에서 섀시 번들을 별도로 생성해야 합니다
- 4100 및 9300 장치 플랫폼의 경우 FXOS 및 FTD 문제 해결 번들을 수집해야 합니다. 다른 모든 플랫폼의 경우 FTD 문제 해결 번들도 FXOS 문제 해결 번들을 포함하므로 FTD 문제 해결 번들로 충분합니다.
- ASA의 경우 복구 후 'show tech-support' 명령 출력이 그다지 유용하지 않습니다. FXOS 문제 해결 번들에 의존해야 합니다.
- 다른 플랫폼과 비교했을 때, 41xx, 93xx의 경우 2개의 트러블슈팅 번들이 있습니다. 섀시(BC1) 및 모듈 번들.
- 41xx, 93xx의 섀시 번들(BC1)에는 FPRM 및 CIMC 번들이 포함됩니다.
- 41xx, 93xx의 모듈 번들에는 주로 블레이드의 FXOS 로그가 포함되어 있습니다.
- ASA가 설치된 경우 섀시, FPRM 및 모듈 번들(해당하는 경우)과 ASA에서의 'show tech-support' 명령 출력만 의존해야 합니다.
- 플랫폼과 인시던트에 따라 모든 파일이 존재하는 것은 아닙니다.

트러블슈팅 번들의 파일 경로	설명/팁

FTD TS 번들: /dir-archives/var-log/messages*	정상 종 ng shut 열이 표 디바이스 'syslog- 문자열(
FTD TS 번들: /dir-archives/var-log/ASAconsole.log 4100/9300의 ASA인 경우 모듈 번들의 /opt/cisco/platform/logs/ASAconsole.log에서도 파일을 찾을 수 있습니다.	오류, 결 인합니다
FTD TS 번들: /dir-archives/var-log/dmesg.log	오류, 결 인합니다
FTD TS 번들: /dir-archives/var/log/ngfwManager.log*	오류, 결 인합니다 이 파일 터 이벤 도 포함
FTD TS 번들: /command-outputs/LINA_troubleshoot/show_tech_output.txt	'show fa 'show c 출력은 대한 추 할 수 있
FTD TS 번들: /command-outputs/ 파일 이름: · `ls opt-cisco-csp-cores _ grep core`_ do file -opt-cisco-csp-cores-_{CORE}_ done.output의 CORE · `ls var-common _ grep core`_ do file var-common-_{CORE}_ done.output의 CORE용 · `ls var-data-cores _ grep core`_ do file -var-data-cores-_{CORE}_ done.output의 CORE용	잠재적 추적)을
FTD TS 번들: /dir-archives/var/log/crashinfo/snort3-crashinfo.*	Snort3 확인합니

FTD TS 번들: /dir-archives/var/log/process_stderr.log*	백트레
Cisco
CSCwh
FTD TS 번들: /dir-archives/var/log/periodic_stats/	이 디렉
트 시간
을 제공
파일이
다.
FPRM 번들: 기술 지원 개요	'show fa
을 확인
FPRM 번들: /opt/cisco/platform/logs/kern.log	오류, 결
인합니
FPRM 번들: /opt/cisco/플랫폼/로그/메시지*	오류, 결
인합니
FPRM 번들: /opt/cisco/platform/logs/mce.log 동일한 파일이 모듈 번들(41xx, 93xx)에도 있습니다.	mce(Ma
Excepti
. 오류,
확인합
FPRM 번들: /opt/cisco/platform/logs/portmgr.out	오류, 결
인합니
FPRM 번들: /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	오류, 결
인합니
FPRM 번들: /opt/cisco/platform/logs/ssp-pm.log 동일한 파일이 모듈 번들(41xx, 93xx)에도 있습니다.	오류, 결
인합니
FPRM 번들: /opt/cisco/platform/logs/sma.log 동일한 파일이 모듈 번들(41xx, 93xx)에도 있습니다.	오류, 결
인합니
FPRM 번들: /opt/cisco/platform/logs/heimdall.log	오류, 결
인합니

FPRM 번들: /opt/cisco/platform/logs/ssp-shutdown.log 동일한 파일이 모듈 번들(41xx, 93xx)에도 있습니다.	재부팅 작되면 dmesg 행이 포 1000/2 서 사용
FPRM 번들: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	오류, 결 인합니
FPRM 번들: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	오류, 결 인합니
CIMC 번들(41xx, 93xx): /obfl/obfl-log*	오류, 결 인합니
CIMC 번들(41xx, 93xx): /CIMC1_TechSupport.tar.gz/CIMC1_TechSupport.tar/tmp/techsupport_pid*/CIMC1_TechSupport-nvram.tar.gz/CIMC1_TechSupport-nvram.tar/nv/etc/log/eng-repo/messages*	오류, 결 인합니 특히 CA
모듈 번들(41xx, 93xx): /tmp/mount_media.log/mount_media.log	오류, 결 인합니

14단계: 캡처

특정 인터페이스가 응답하지 않는 경우 방화벽 및 인접 디바이스에서 take 캡처를 수행합니다. 자세한 내용은 이 문서를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

또한 인접 디바이스의 ARP 및 CAM 테이블이 올바르게 채워져 있는지 확인합니다.

15단계: Cisco TAC에 제공할 추가 정보

위에 언급 한 항목 외에도 다음 정보를 제공하는 것이 좋습니다.

15a. 디바이스가 복구한 경우 문제 해결 번들을 수집합니다(자세한 내용은 13단계 확인).

150억 디바이스가 여전히 응답하지 않는 경우 다음 정보를 제공합니다.

- 하드웨어 정보(모델).
- 소프트웨어 정보.
- FMC 소프트웨어 정보(해당되는 경우).
- 구축(독립형/HA/클러스터).

15c 디바이스가 응답하지 않는 대략적인 시간(날짜/시간)입니다.

15일 디바이스가 응답하지 않게 되기 전의 대략적인 가동 시간

15e. 새 설정입니까, 기존 설정입니까?

15f 디바이스가 응답하지 않기 전에 마지막으로 수행한 작업은 무엇입니까?

15g. 디바이스가 응답하지 않는 시점부터 LINA(Firewall Data Plane) syslog가 생성됩니다(사고 발생 5분 전부터 로그를 가져오려고 시도). 모범 사례로서, 레벨 6(정보)에서 syslog를 구성하는 것이 좋습니다.

15시간 섀시에 syslog 서버를 구성한 경우(4100/9300의 FXOS) 로그를 제공합니다(사고 발생 5분 전에 시작).

15i. 사고 발생 시점부터 인접 디바이스의 Syslog입니다.

15j. 방화벽 디바이스와 인접 디바이스 간의 물리적 연결을 보여주는 토폴로지 다이어그램

일반적인 문제

오류: DME와 통신하는 동안 시간이 초과되었습니다.

콘솔에 연결하여 다음을 확인하는 경우

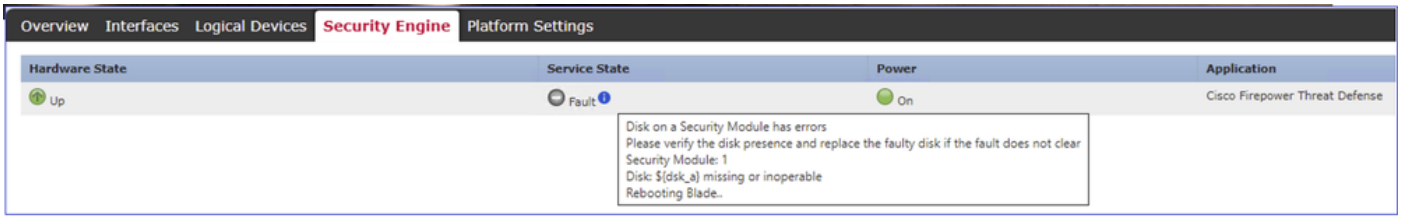
```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

대부분의 경우 이는 소프트웨어 문제를 나타냅니다.

권장 조치: Cisco TAC에 문의

디스크 오류: 누락 또는 작동 불능

이 출력은 디스크 관련 결함이 생성된 4100/9300 하드웨어 어플라이언스의 출력입니다.

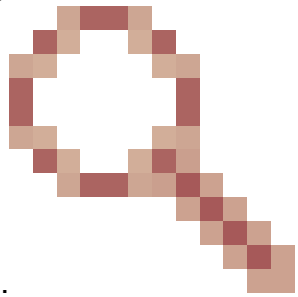


권장 조치: SSD 디스크를 다시 장착해 보십시오. 도움이 되지 않을 경우 섀시 문제 해결 번들을 수집하고 Cisco TAC에 문의하십시오.

필드 알림: FN72077 - FPR9300 및 FPR4100

- FPR9300 및 FPR4100 Series 보안 어플라이언스는 더 이상 네트워크 트래픽을 전달하지 않습니다.
- 유효한 자격 증명을 가진 사용자는 관리 콘솔에 로그인할 수 없습니다.
- CLI에서 오류 메시지 표시: "소프트웨어 오류: 실행 중 예외 발생: [오류: DME와 통신하는 동안 시간이 초과되었습니다.]

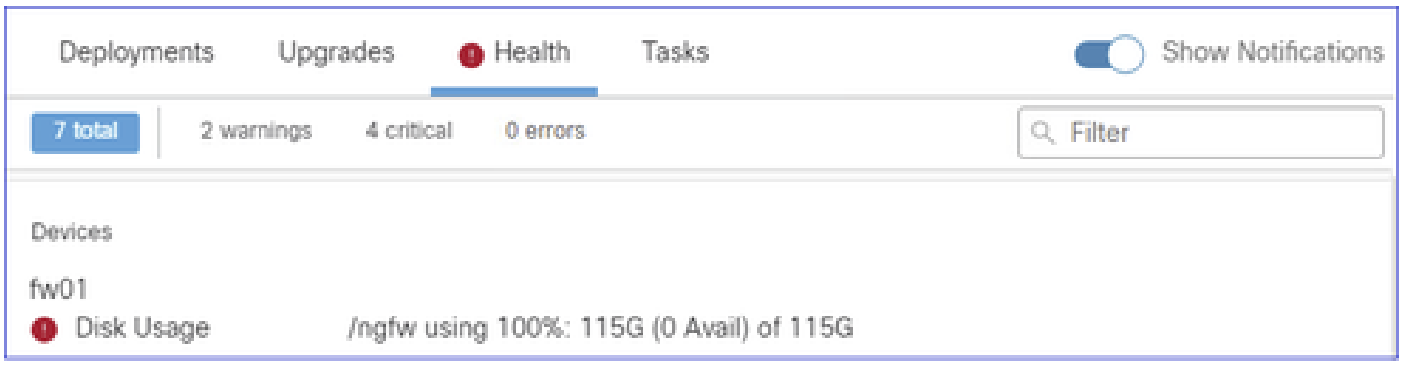
권장 조치: 이 문제를 일시적으로 복구하려면 4100/9300 섀시의 전원 사이클이 필요합니다. Cisco



버그 ID CSCvx99172에서 자세한 내용과 수정 사항이 있는 버전을 확인합니다.
(필드 알림: FN72077 - FPR9300 및 FPR4100 Series 보안 어플라이언스 - 일부 어플라이언스는 3.2년의 가동 시간 이후 트래픽을 전달하지 못할 수 있습니다.

디스크 사용률 100%

방화벽의 디스크 공간이 부족하면 디바이스가 응답하지 않을 수 있습니다. FMC에서 디바이스를 관리하는 경우 다음과 같은 상태 알림을 받을 수 있습니다.

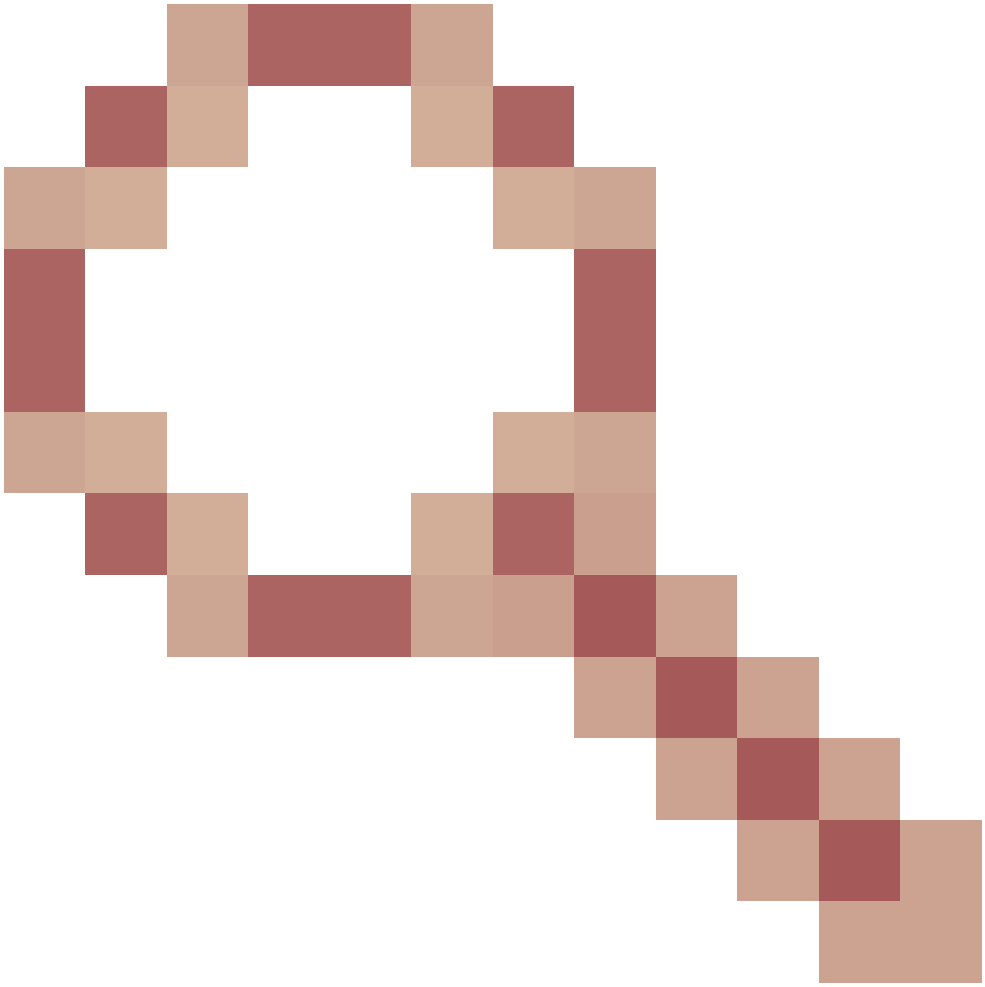


권장 조치: 소프트웨어 7.7.0 이상에서 FMC 및 FTD를 실행 중인 경우 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space에 설명된 절차를 사용하여 일부 디스크 공간을 지웁니다

실행 불가능하거나 도움이 되지 않는 경우 Cisco TAC에 문의하십시오.

정전 후 CSF 3100이 작동하지 않음

권장 조치: 다음 항목에 대한 수정 사항이 있는 소프트웨어 릴리스로 업그레이드:



Cisco 버그 ID CSCwm14729
정전 후 CSF 3100 Series가 재부팅되지 않으므로 수동 전원 사이클이 필요합니다.

Cisco Firepower 2100 Series 보안 어플라이언스: 일부 유닛에서 메모리 오류가 발생할 수 있습니다.

- 구성 요소 프로세스 문제로 인해 서비스 기간 5년 이내의 DIMM 장애
- 관련 FN: https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html
- 관련 Cisco 버그 ID CSCwb74948

권장 조치: DIMM 구성 요소 교체 또는 보안 어플라이언스 교체

참조

- https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html
- https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#

- https://www.cisco.com/c/en/us/support/docs/field-notices/720/fn72077.html
- https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/216245-collection-of-core-files-from-a-firepowe.html#anc6
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

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.