

FMC에서 FTD 페일오버 이벤트 식별 및 분석

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[FMC의 장애 조치 이벤트](#)

[1단계. 상태 정책 컨피그레이션](#)

[2단계. 정책 할당](#)

[3단계. 장애 조치 이벤트 알림](#)

[4단계. 기록 장애 조치 이벤트](#)

[5단계. 고가용성 대시보드](#)

[6단계. 위협 방어 CLI](#)

[관련 정보](#)

소개

이 문서에서는 Secure Firewall Management Center GUI에서 Secure Firewall Threat Defense를 위한 장애 조치 이벤트를 식별하고 분석하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Secure Firewall Threat Defense)의 HA(고가용성) 설정
- Cisco FMC(Firewall Management Center)의 기본 사용 편의성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FMC v7.2.5
- Cisco Firepower 9300 Series v7.2.5

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

FMC는 Firepower 디바이스의 관리 센터일 뿐만 아니라 관리 및 컨피그레이션 옵션을 넘어, 로그와 이벤트를 실시간 및 과거로 분석하는 데 도움이 되는 그래픽 인터페이스도 제공합니다.

장애 조치에 대해 이야기할 때, 인터페이스에 장애 조치 이벤트를 분석하여 장애를 파악하는 데 도움이 되는 새로운 개선 사항이 있습니다.

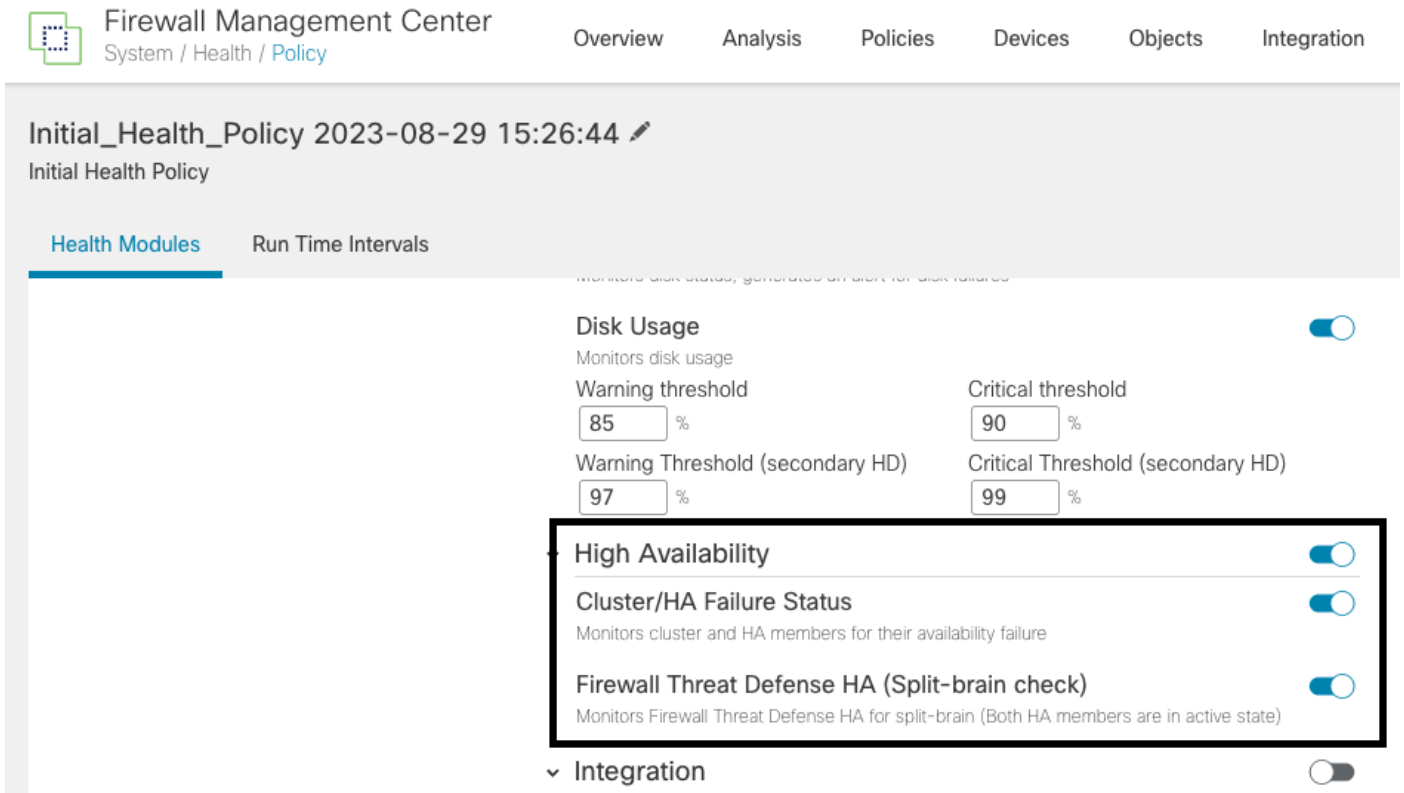
FMC의 장애 조치 이벤트

1단계. 상태 정책 컨피그레이션

Cluster/HA Failure Status(클러스터/HA 실패 상태) 모듈은 상태 정책에서 기본적으로 활성화되지만 Split-brain(스플릿 브레인) 확인 옵션도 활성화할 수 있습니다.

상태 정책에서 HA에 대한 옵션을 사용하려면 System > Health > Policy > Firewall Threat Defense Health Policy > High Availability.

이 이미지는 상태 정책의 HA 컨피그레이션에 대해 설명합니다.



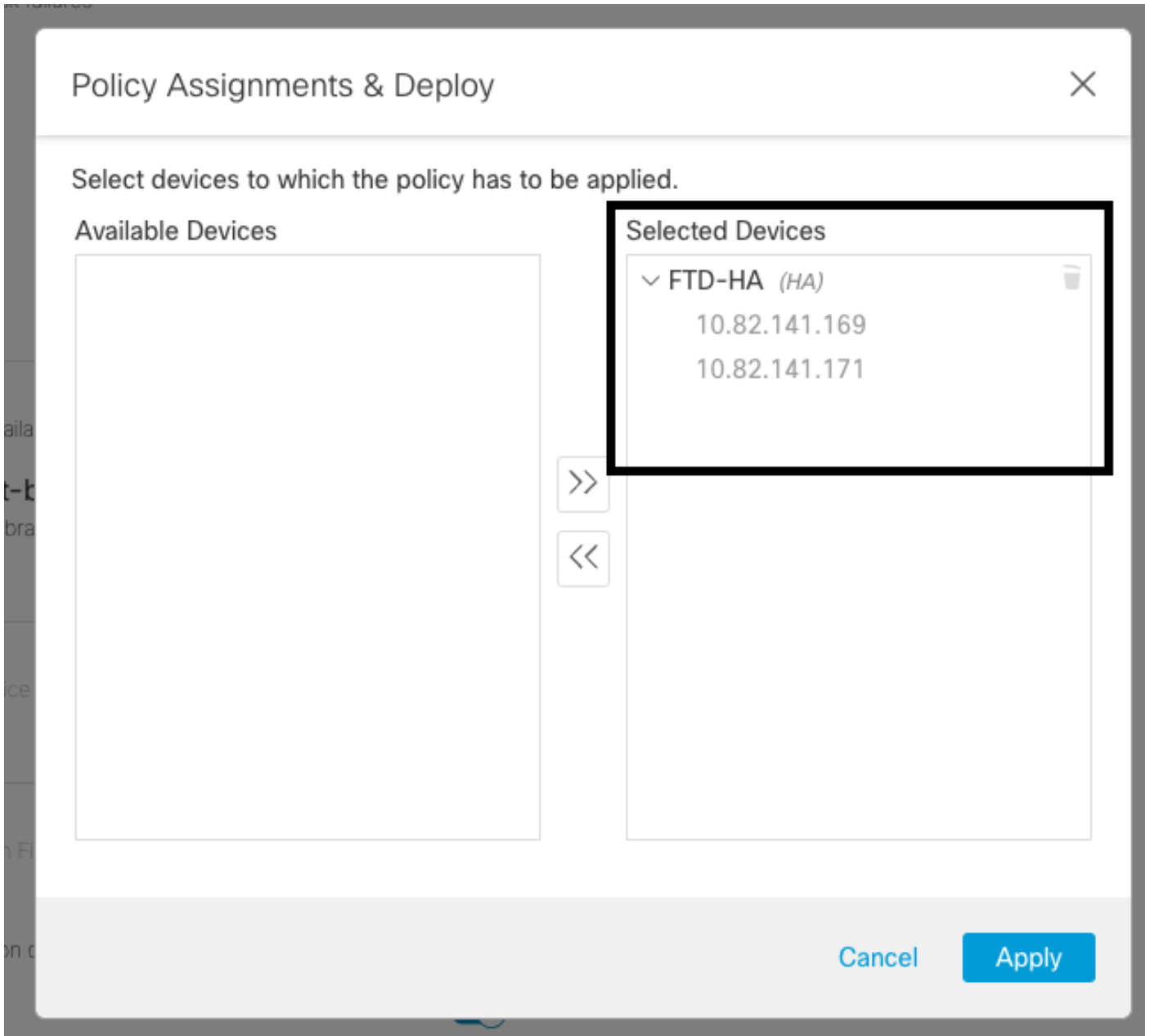
고가용성 상태 설정

2단계. 정책 할당

FMC에서 모니터링할 HA 쌍에 상태 정책이 할당되었는지 확인합니다.

정책을 할당하려면 System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

이 이미지는 HA 쌍에 상태 정책을 할당하는 방법을 보여줍니다.



HA 할당

정책이 할당되고 저장되면 FMC에서 자동으로 FTD에 적용합니다.

3단계. 장애 조치 이벤트 알림

HA의 컨피그레이션에 따라 장애 조치 이벤트가 트리거되면 장애 조치 실패를 설명하는 팝업 알림이 표시됩니다.

이 그림에서는 생성된 장애 조치 경고를 보여줍니다.

Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

t Pending (0) ● Upgrade (0)

	Version	Chassis	Licenses	Access Control P
with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:4 Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Cluster/Failover Status - 10.82.141.169 ✕
 SECONDARY (FLM1946BCEX)
 FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services-. Peer failed services-diskstatus))
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Check peer event for reason)

Cluster/Failover Status - 10.82.141.171 ✕
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Other unit wants me Standby)
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure(My failed services-diskstatus. Peer failed services-))

Disk Usage - 10.82.141.171 ✕
 /ngfw using 98%: 186G (5.5G Avail) of 191G

장애 조치 알림

또한 다음 사이트로 이동할 수 있습니다 Notifications > Health 장애 조치 상태 알림을 시각화합니다.

이 그림에서는 알림 아래의 장애 조치 알림을 보여 줍니다.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

View By: Group

All (2) ● Error (2) ● Warning (0) ● Offline (0) ● Normal (0) ● Deployment Pending (0) ● Upgrade (0)

Collapse All

Name	Model	Version	Chassis
10.82.141.169(Secondary, Active) 10.82.141.169 - Routed	Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1 Security Module - 1
10.82.141.171(Primary, Failed) 10.82.141.171 - Routed	Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR Security Module - 1

Deployments Upgrades ● Health Tasks Show Notifications

20+ total 15 warnings 7 critical 0 errors

- Smart License Monitor Smart Agent is not registered with Smart Licensing Cloud
- URL Filtering Monitor URL Filtering registration failure

Devices

10.82.141.169

- Interface Status Interface 'Ethernet1/2' is not receiving any packets
- Interface 'Ethernet1/3' is not receiving any packets
- Interface 'Ethernet1/4' is not receiving any packets

10.82.141.171

- Disk Usage /ngfw using 98%: 186G (5.4G Avail) of 191G
- Interface Status Interface 'Ethernet1/2' is not receiving any packets
- Interface 'Ethernet1/3' is not receiving any packets
- Interface 'Ethernet1/4' is not receiving any packets

HA 알림

4단계. 기록 장애 조치 이벤트

FMC는 과거에 발생한 장애 조치 이벤트를 시각화할 수 있는 방법을 제공합니다. 이벤트를 필터링하려면 System > Health > Events > Edit Search 모듈 이름을 Cluster/Failover Status로 지정합니다. 또한 Status(상태)에 따라 필터를 적용할 수 있습니다.

이 그림에서는 장애 조치 이벤트를 필터링하는 방법을 보여 줍니다.

General Information

Module Name	Cluster/Failover Status	Disk Status, Interface Status
Value		25
Description		Sample Description
Units		unit
Status	Warning	Critical, Warning, Normal, Recovered
Device		device1.example.com, *.example.com, 192.168.1.3

장애 조치 필터 메시지

특정 날짜 및 시간에 대한 이벤트를 표시하려면 시간 설정을 조정할 수 있습니다. 시간 설정을 수정하려면 System > Health > Events > Time.

이 그림에서는 시간 설정을 수정하는 방법을 보여 줍니다.

The screenshot shows the 'Health Monitoring Time Window' configuration page in the Firewall Management Center. The 'Expanding Time Window' dropdown is selected. The page displays a calendar for September 2023 and various time window presets: 1 hour, 6 hours, 1 day, 1 week, 2 weeks, and 1 month. The 'Current' preset is set to 'Day'. The page also shows a table of health events on the right side.

시간 필터

이벤트가 식별되면 이벤트의 이유를 확인하려면 설명 아래에 커서를 놓습니다.

이 그림에서는 장애 조치 이유를 확인할 수 있는 방법을 보여줍니다.

The screenshot shows the 'Table View of Health Events' page in the Firewall Management Center. The 'Description' column is highlighted, showing a detailed error message: 'PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAIL...'. The message includes details about the failover state and the reason for the failure: 'PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure:My failed services-diskstatus. Peer failed services-)).

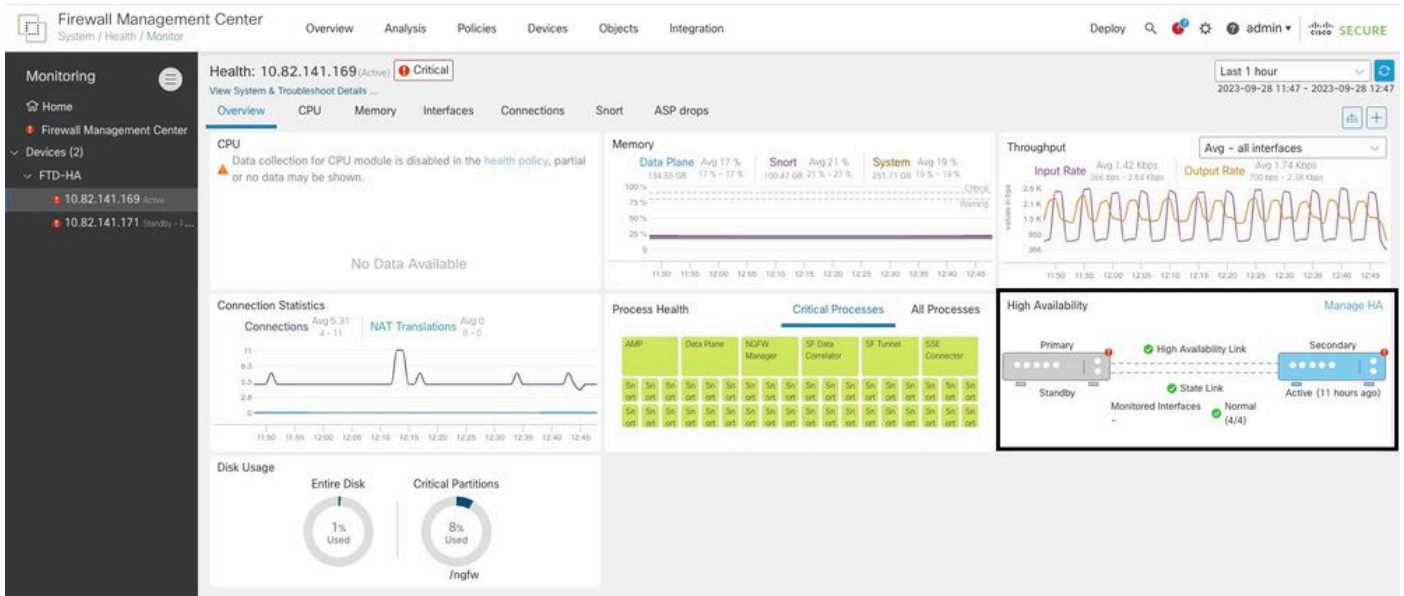
장애 조치 세부 정보

5단계. 고가용성 대시보드

장애 조치를 모니터링하는 또 다른 방법은 System > Health Monitor > Select Active or Standby Unit.

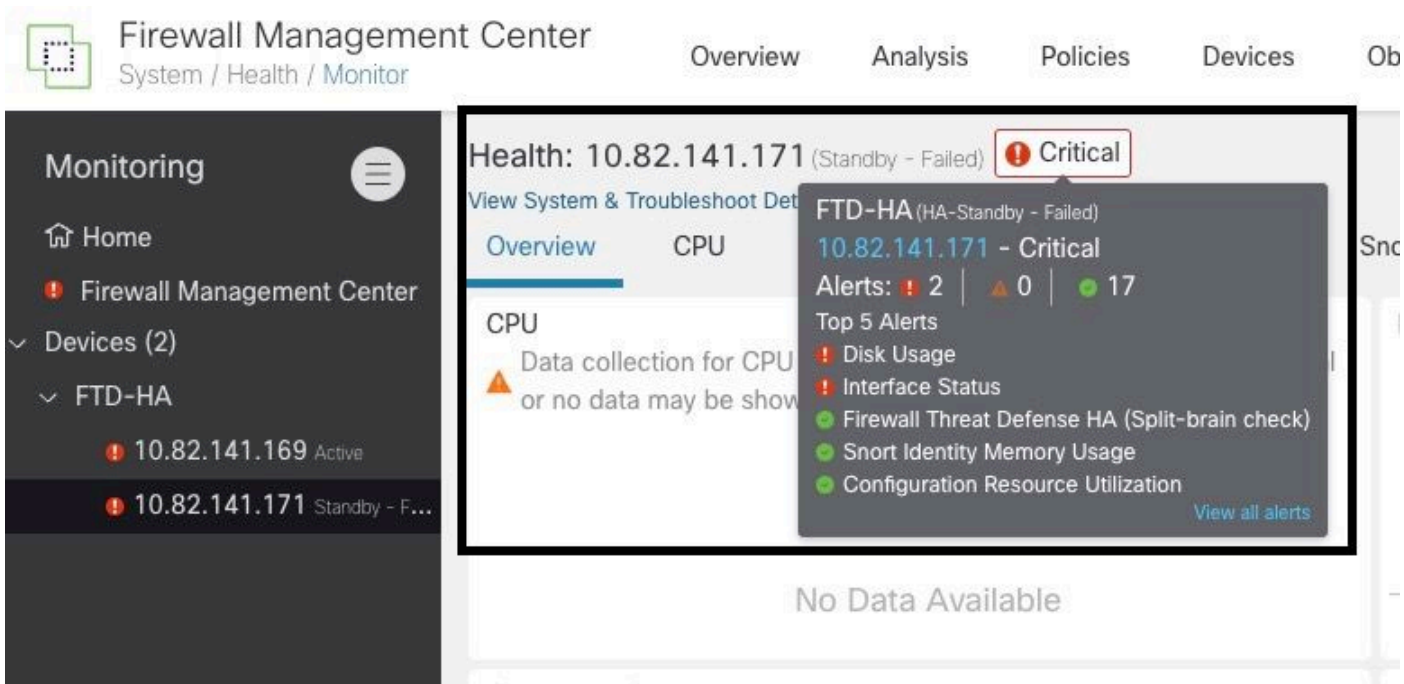
HA 모니터는 HA 및 상태 링크의 상태, 모니터링된 인터페이스, ROL, 각 유닛의 경고 상태에 대한 정보를 제공합니다.

이 그림에서는 HA 모니터를 보여 줍니다.



상태 그래픽

경고를 시각화하려면 System > Health Monitor > Select Active or Standby Unit > Select the Alerts.



경고

알림에 대한 자세한 내용을 보려면 [View all alerts > see more.](#)

이 그림에서는 장애 조치를 유발한 디스크 상태를 보여줍니다.

Health Alerts - 10.82.141.171

19 total 2 critical 0 warnings 7 normal [Export](#) [Run All](#)

Disk Usage Sep 28, 2023 12:47 PM
/ngfw using 98%: 186G (5.4G Avail) of 191G [see less](#)

Mount	Size	Free	Used	Percent
/mnt/boot	7.5G	7.3G	208M	3%
/opt/cisco/config	1.9G	1.8G	3.4M	1%
/opt/cisco/platform/logs	4.6G	4.3G	19M	1%
/var/data/cores	46G	43G	823M	2%
/opt/cisco/csp	684G	498G	187G	28%
/ngfw	191G	5.4G	186G	98%

Interface Status Sep 28, 2023 12:47 PM
Interface 'Ethernet1/2' is not receiving any packets
Interface 'Ethernet1/3' is not receiving any packets
Interface 'Ethernet1/4' is not receiving any packets [see more](#)

Appliance Heartbeat Sep 28, 2023 12:47 PM
All appliances are sending heartbeats correctly.

Automatic Application Bypass Status Sep 28, 2023 12:47 PM

알림 세부사항

6단계. 위협 방어 CLI

마지막으로, FMC에 대한 추가 정보를 수집하려면 [Devices > Troubleshoot > Threat Defense CLI](#). **Device(디바이스)** 및 실행할 명령과 같은 매개변수를 구성하고 [Execute](#).

이 그림에서는 명령의 예를 보여 줍니다 `show failover history` 장애 조치 실패를 식별할 수 있는 FMC에서 실행할 수 있습니다.



Device: 10.82.141.169

Command: show Parameter: failover history

Output

```
other unit has failed                                     due to disk failure
05:28:05 UTC Sep 28 2023
Active Drain                                             Active Applying Config   Inspection engine in
other unit has failed                                     due to disk failure
05:28:05 UTC Sep 28 2023
Active Applying Config                                   Active Config Applied     Inspection engine in
other unit has failed                                     due to disk failure
05:28:05 UTC Sep 28 2023
Active Config Applied                                   Active                    Inspection engine in
other unit has failed                                     due to disk failure
```

Back Execute

장애 조치 기록

관련 정보

- [FTD의 고가용성](#)
- [Firepower 어플라이언스에서 FTD 고가용성 설정](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.