FMC에서 FTD 페일오버 이벤트 식별 및 분석

목차

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.

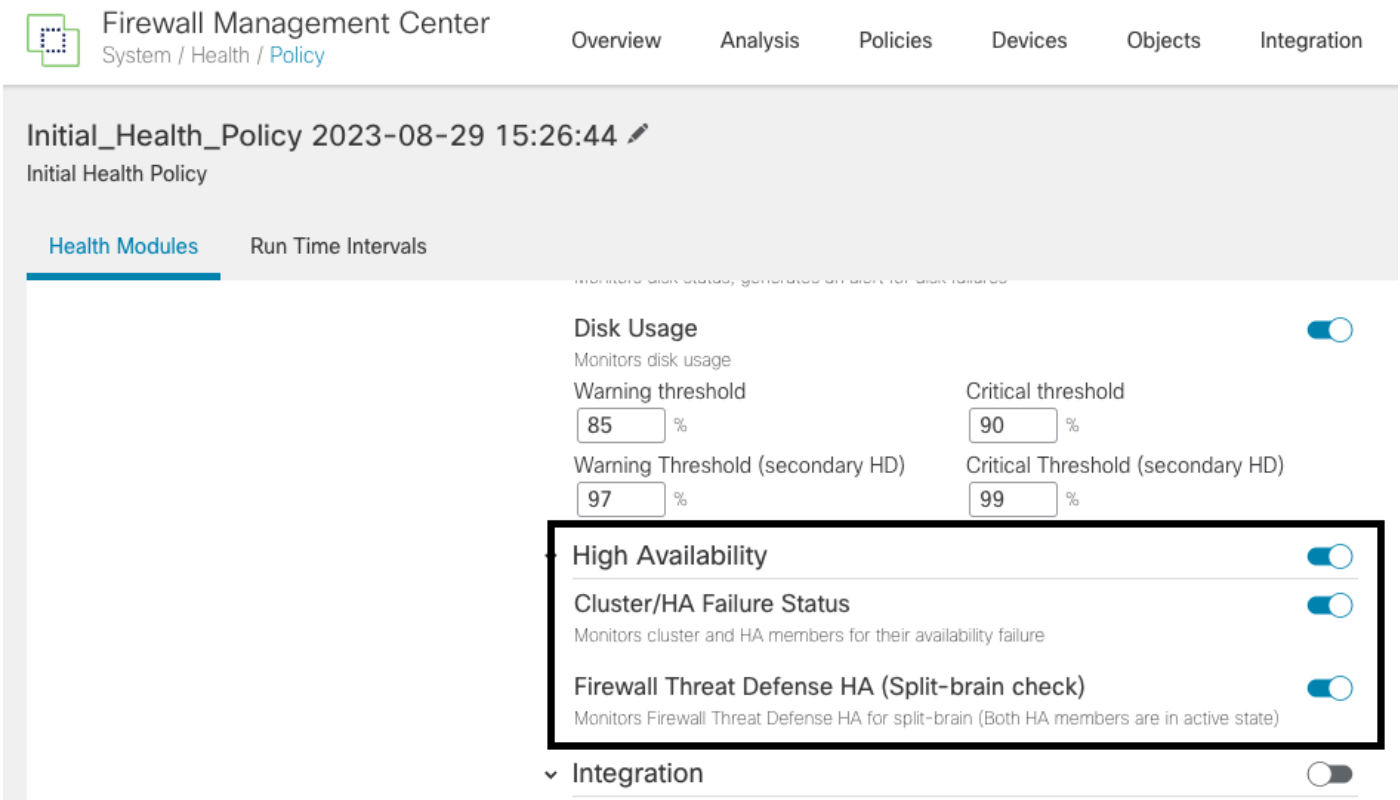
FMC의 장애 조치 이벤트

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 Avilability.

이 이미지는 상태 정책의 HA 컨피그레이션에 대해 설명합니다.



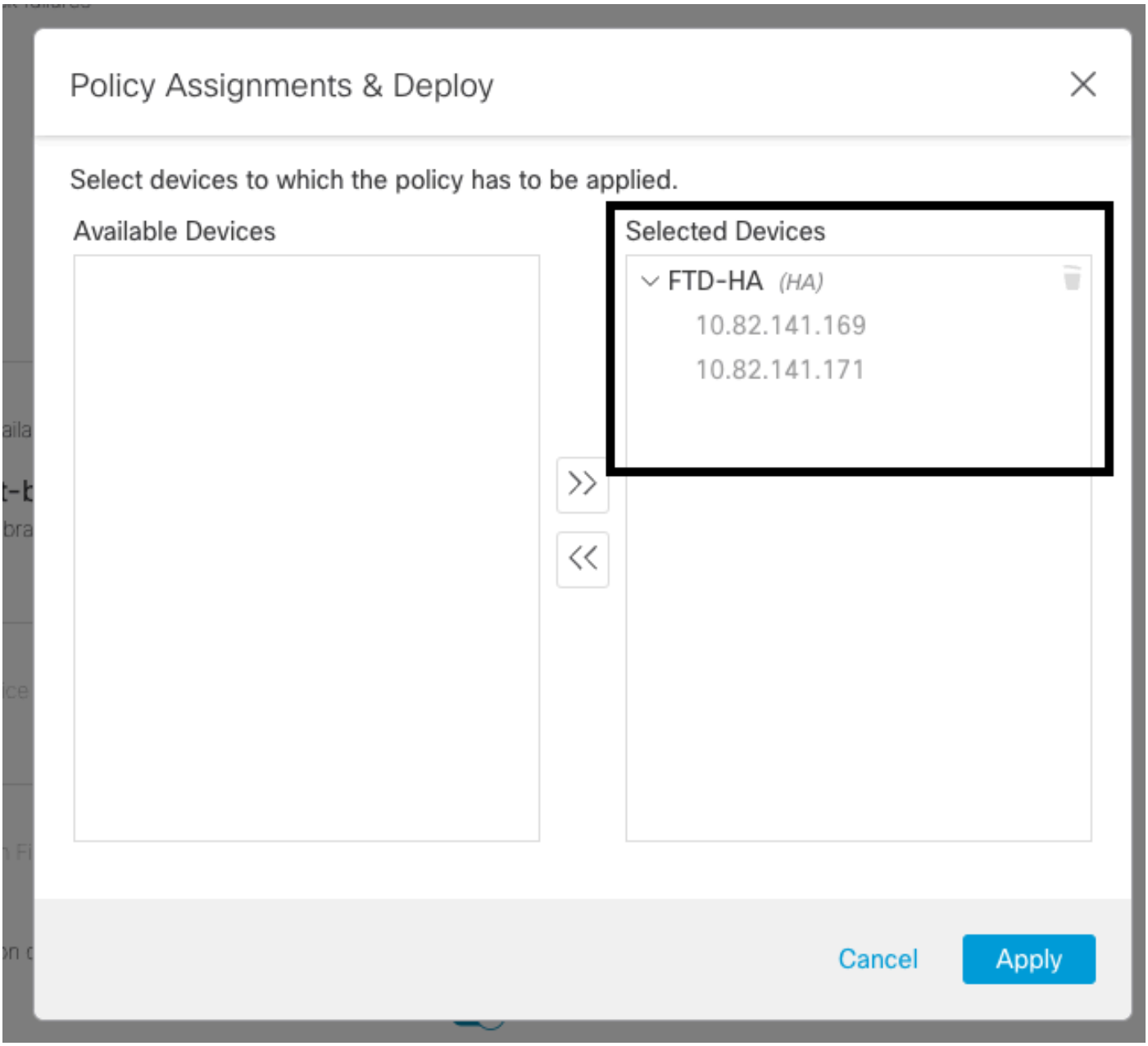
고가용성 상태 설정

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.



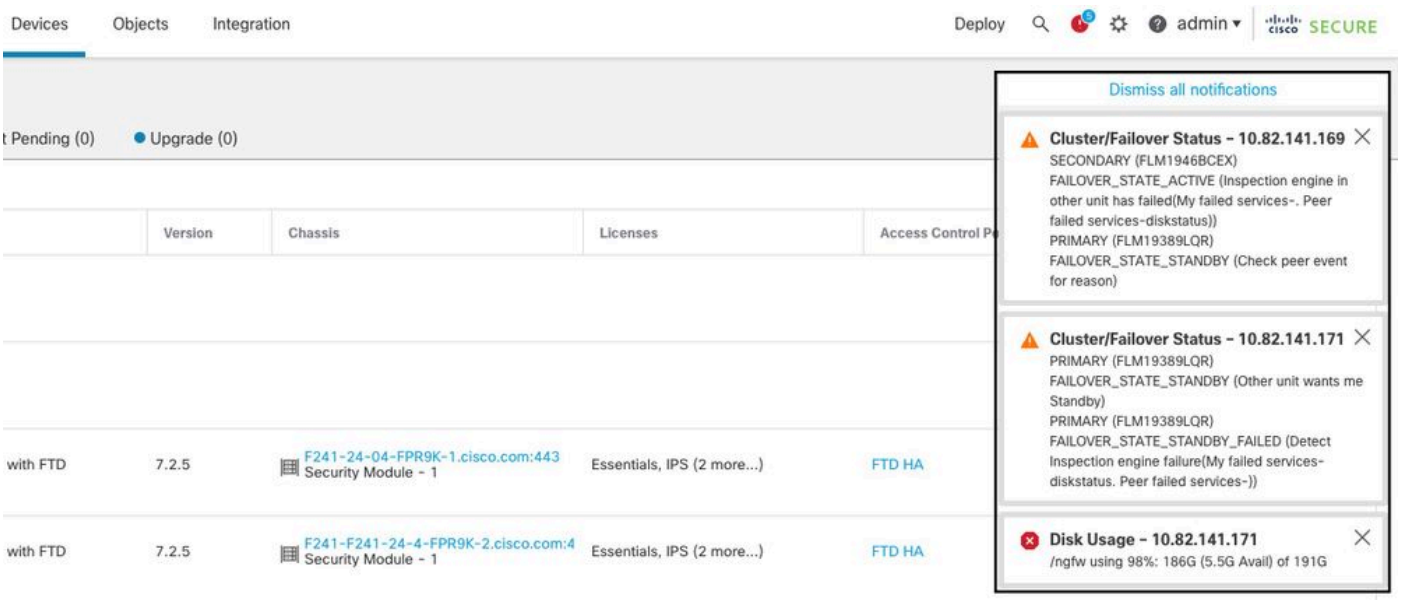
HA 할당

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.

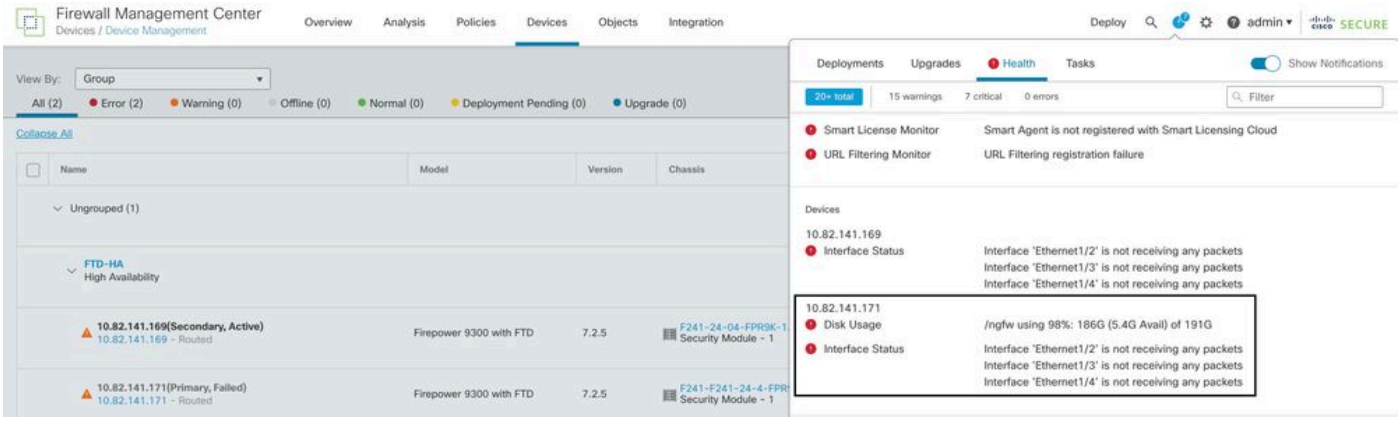
이 그림에서는 생성된 장애 조치 경고를 보여줍니다.



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.

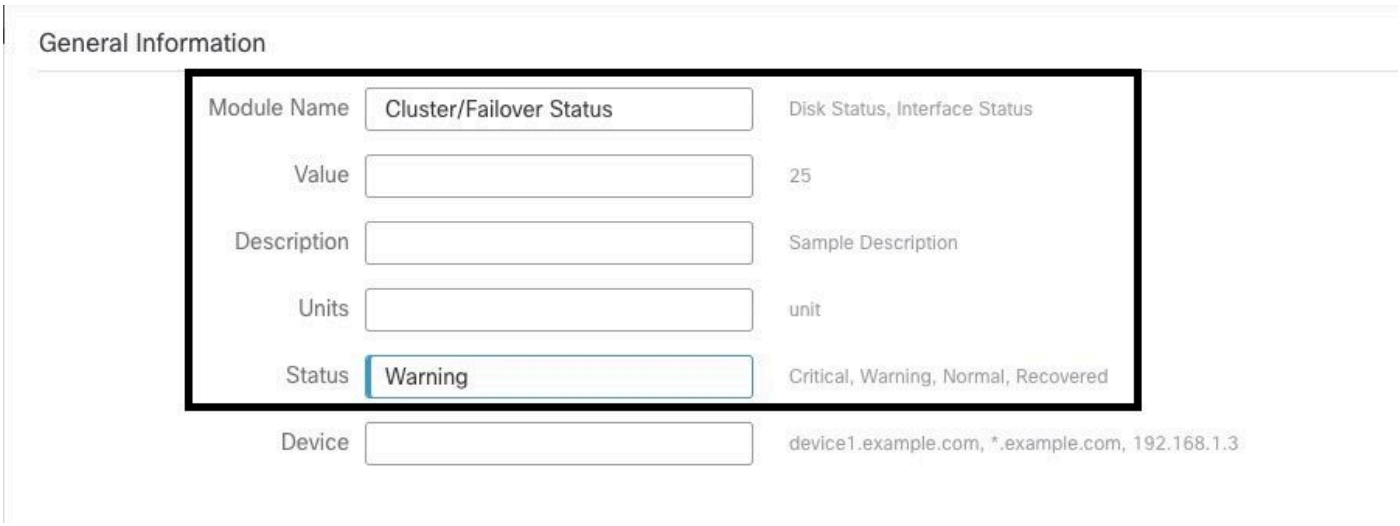


HA 알림

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.

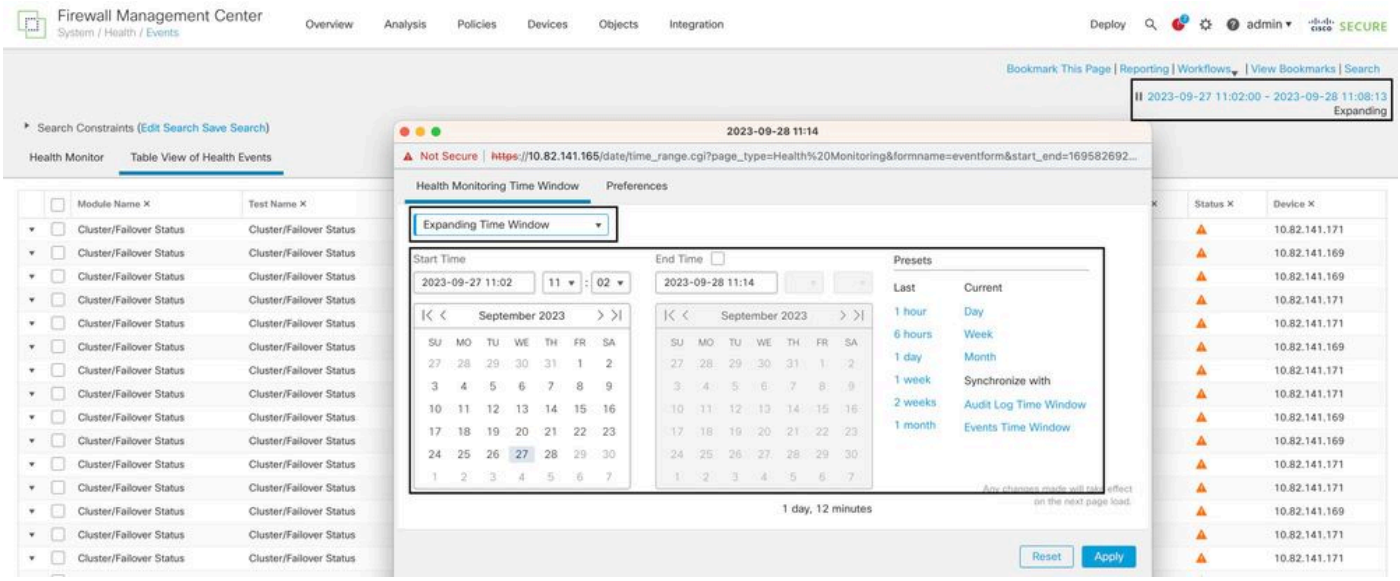
이 그림에서는 장애 조치 이벤트를 필터링하는 방법을 보여 줍니다.



장애 조치 필터 메시지

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

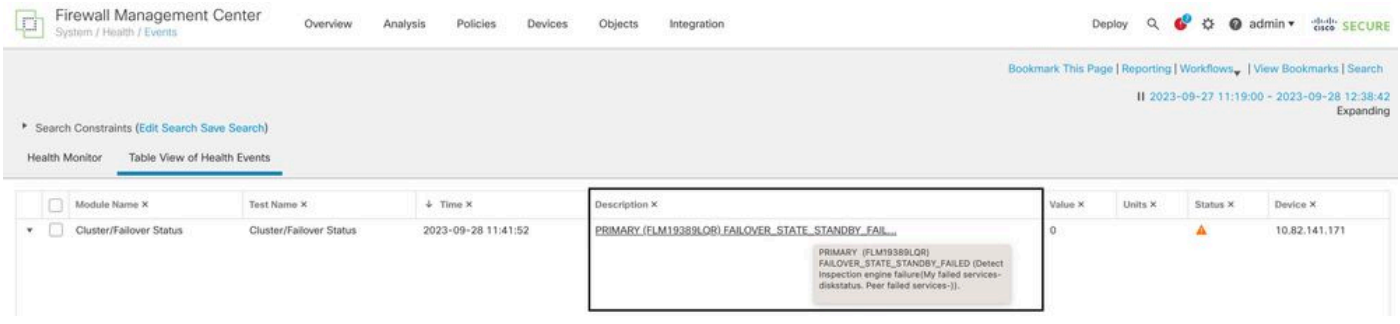
이 그림에서는 시간 설정을 수정하는 방법을 보여 줍니다.



시간 필터

이벤트가 식별되면 이벤트의 이유를 확인하려면 설명 아래에 커서를 놓습니다.

이 그림에서는 장애 조치 이유를 확인할 수 있는 방법을 보여줍니다.

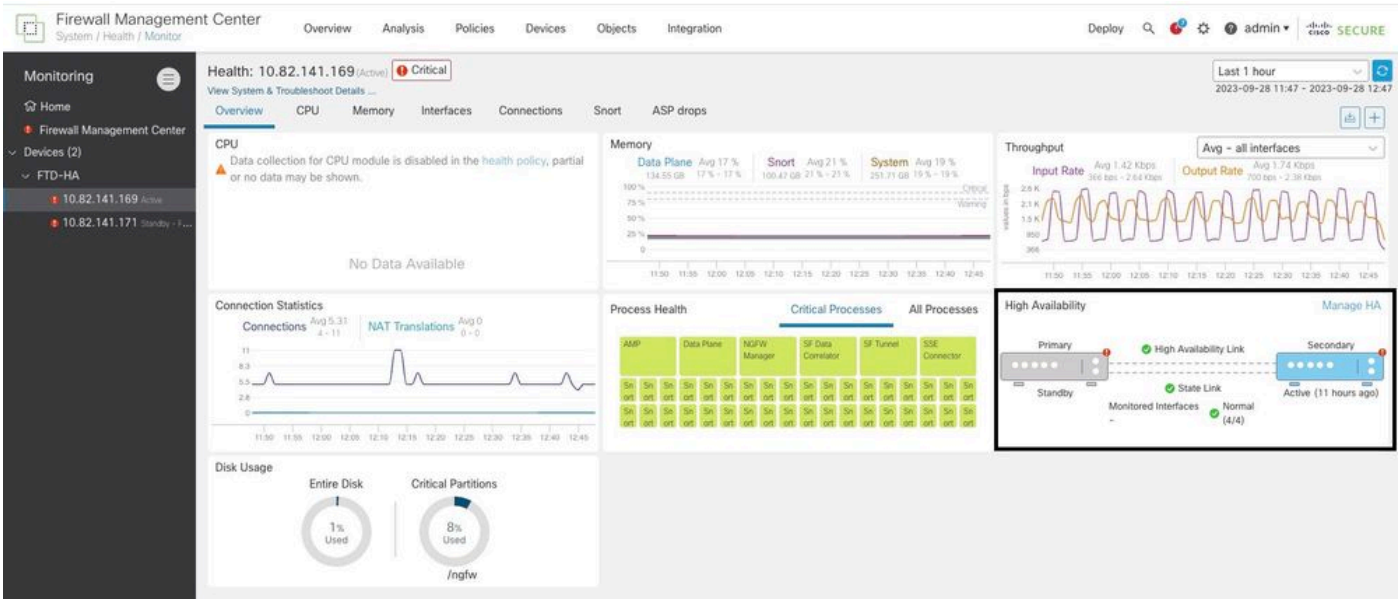


5단계. 고가용성 대시보드

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

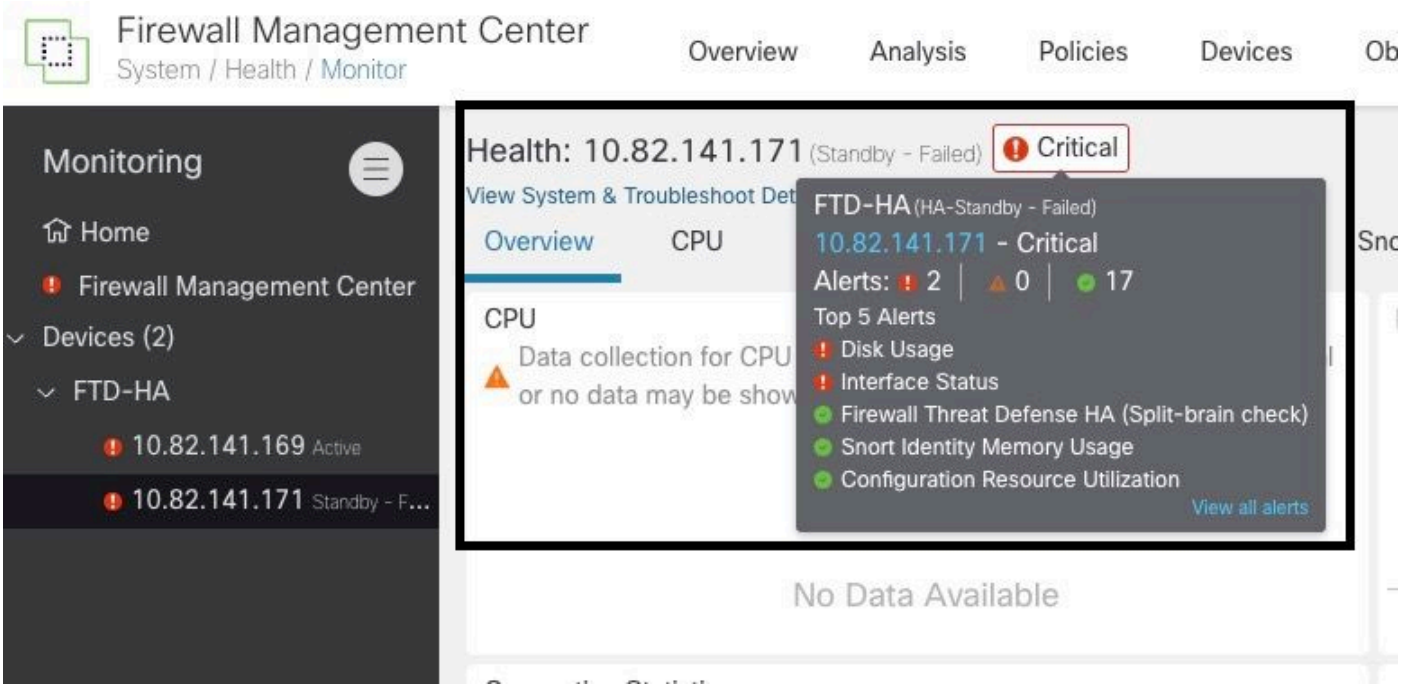
HA 모니터는 HA 및 상태 링크의 상태, 모니터링된 인터페이스, ROL, 각 유닛의 경고 상태에 대한 정보를 제공합니다.

이 그림에서는 HA 모니터를 보여 줍니다.



상태 그래픽

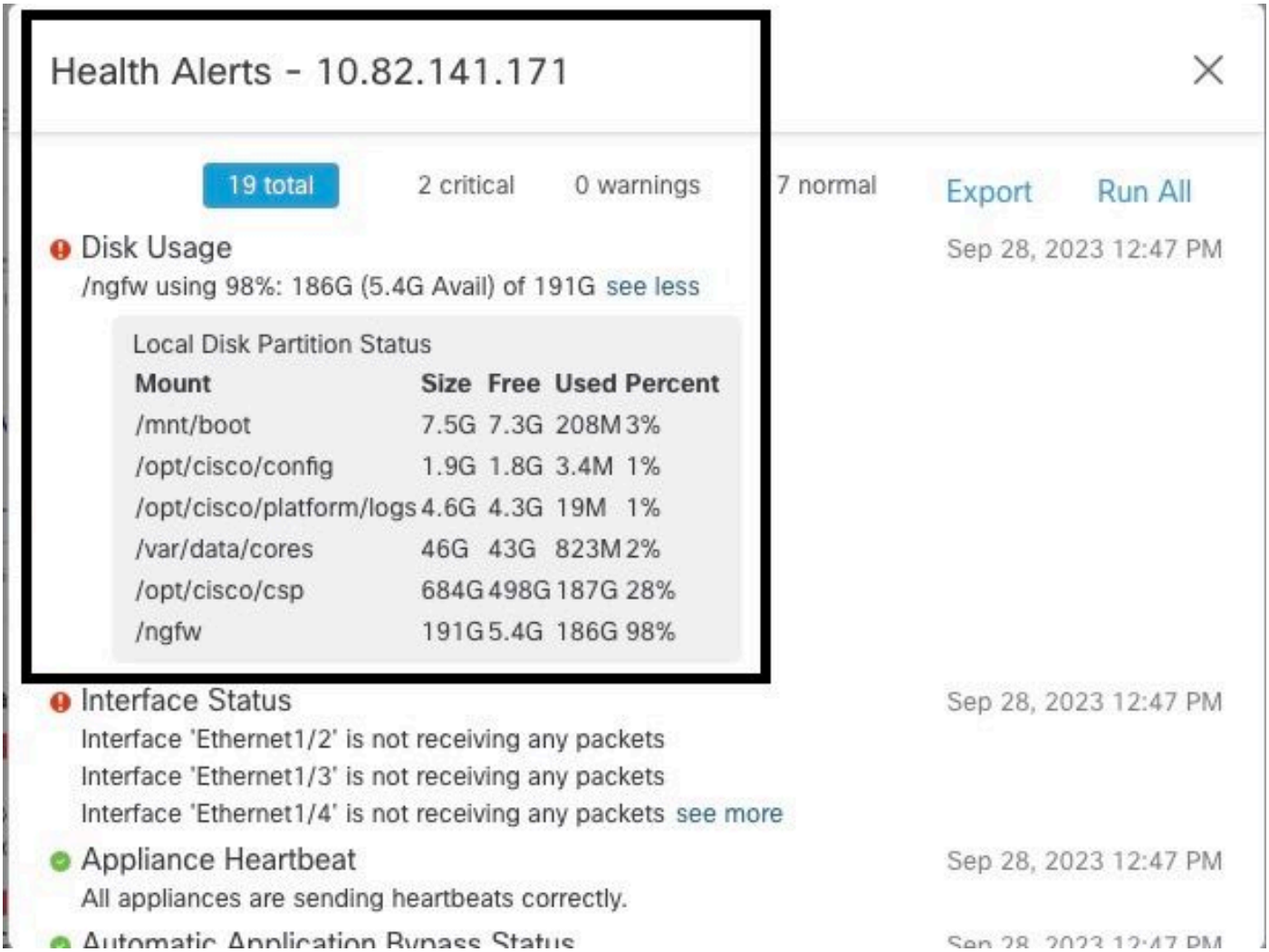
경고를 시각화하려면 System > Health Montitor > Select Active or Standby Unit > Select the Alerts.



경고

알림에 대한 자세한 내용을 보려면 View all alerts > see more.

이 그림에서는 장애 조치를 유발한 디스크 상태를 보여줍니다.

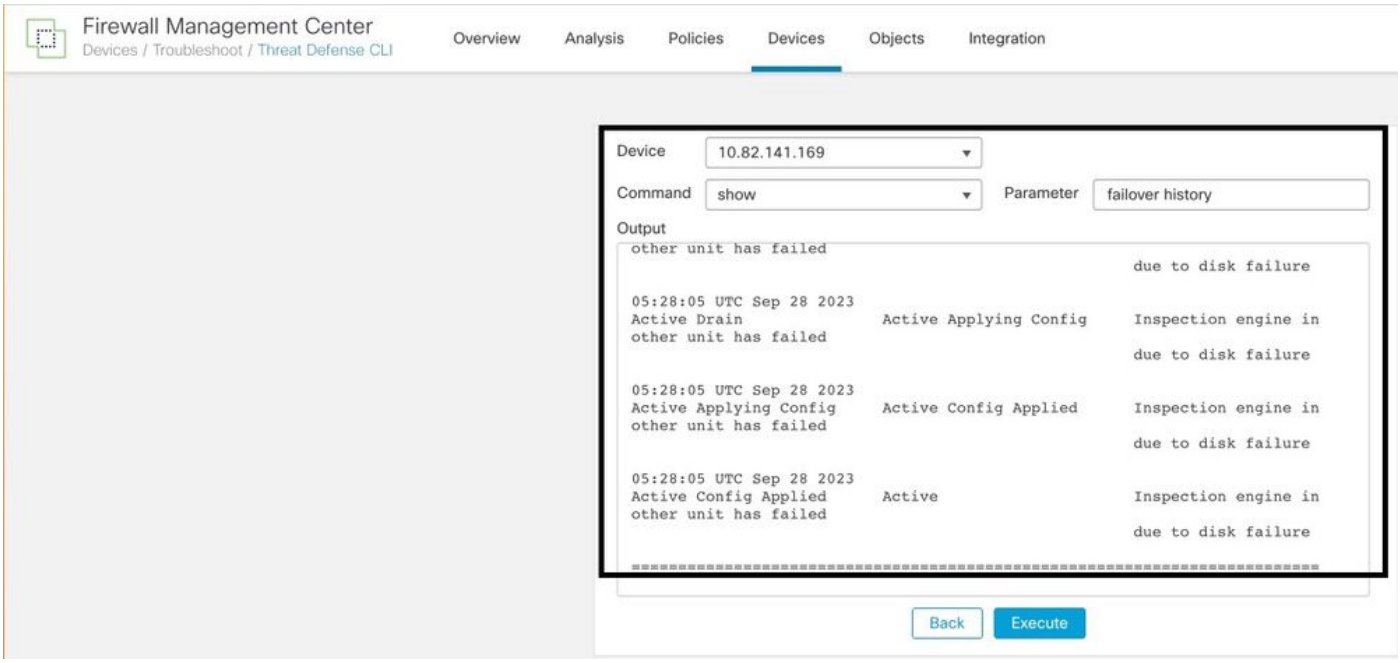


알림 세부사항

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.



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.