FP 업그레이드 - 디바이스 상태 모니터링

목차

소개

이 문서에서는 6.7 및 7.0 릴리스에 추가된 새로운 디바이스 상태 모니터링 기능에 대해 설명합니다
.

배경 정보

마이그레이션한 원본:

https://confluence-eng-rtp2.cisco.com/conf/display/IFT/Change+Management+FP+7.0

https://confluence-eng-
rtp2.cisco.com/conf/pages/viewpage.action?spaceKey=IFT&title=Device+Health+Monitoring

문제:

상태 모니터링 시스템은 사후 대응적 디버깅 및 사전 대응적 조치를 위해 디바이스의 성능에 대한 가시성을 제공합니다.

종합적인 가시성 및 분석은 다음을 통해 얻을 수 있습니다.

- 주요 메트릭에 대한 추세 차트
- 이벤트 오버레이
- 맞춤형 대시보드
- 통합 상태 모니터링 아키텍처 - 모든 관리자에 대해 동일한 데이터 참조
- 많은 새로운 메트릭과 메트릭의 확장성으로 더 많은 기능 추가

7.0 릴리스의 새로운 기능

FP 7.0과 비교하여 새로운 기능 또는 차별화된 기능

- HA가 지원되는 FMC 대시보드
- FTD에 대한 110개 이상의 새로운 메트릭
- FTD 스플릿 브레인 시나리오에 대한 건강 알림
- 최신 상태 메트릭에 대한 사용자 지정 실행 시간 간격

혜택

- 다양한 하위 시스템 및 장치상의 리소스의 데이터를 상호 연결할 수 있는 기능을 제공하여 시스템 디버깅을 지원합니다.
- 다양한 시스템 성능 메트릭 가시성
- 용량 계획

6.7의 새로운 기능

이전 릴리즈와 비교하여 신규 또는 다름(상위 레벨):

- FMC에서 디바이스 상태 모니터링을 위한 새로운 사용자 인터페이스
- FTD Device REST API: device-metric API: 많은 새로운 메트릭이 추가되었습니다.
- FMC API: 새로운 API: 상태 알림, 상태 메트릭 및 구축 세부사항
- 시장 개요, 실제 애플리케이션
- 다양한 하위 시스템 및 장치상의 리소스의 데이터를 상호 연결할 수 있는 기능을 제공하여 시스템 디버깅을 지원합니다.
- 가시성
- 용량 계획

기능 개요

운영 방식

- FP 7.0의 디바이스 상태 모니터링
- 트렌드 차트, 오버레이 및 맞춤형 대시보드를 제공하는 FMC용 새 상태 대시보드
- FTD 대시보드에서 사용할 수 있는 새로운 FTD 메트릭
- 12개 카테고리를 포함하는 110개 이상의 메트릭
- FTD API: 외부 엔터티별로 쿼리할 수 있는 메트릭을 만듭니다.

모자 밑으로

- Telegraf(오픈 소스 메트릭 수집 프레임워크)를 사용하여 디바이스 상태 수집
- 데이터를 FMC로 내보냅니다(FMC에서 실행되고 연결된 디바이스를 폴링하는 Prometheus 사용).

추가 참고 사항

상태 모니터링 데이터를 사용할 수 있습니다.

- FMC 상태 대시보드의 시스템 메뉴(System > Health > Monitor)에서 액세스할 수 있습니다.
- FMC REST API에서
- FTD Device REST API를 통해 FDM에서 디바이스를 관리하는 경우

일부 메트릭(FMC 및 FTD 모두)은 기본적으로 비활성화되어 있습니다

- 상태 정책의 상태 모듈을 활성화하고 구축하여 일부 메트릭을 표시해야 합니다.

FP 6.7 IFT 사용자가 요청한 개선 사항 구현

- 기본적으로 자동 새로 고침
- 대시보드에서 사용자 지정 시간 범위로 필터링
- 인터페이스 선택기에서 사용자 정의 이름(및 물리적 인터페이스 이름)으로 인터페이스를 선택합니다.
- Health Monitor '홈' 페이지에서 교차 실행 디바이스 대시보드

FP 6.7의 디바이스 상태 모니터링

- 트렌드 차트, 오버레이 및 맞춤형 대시보드를 제공하는 FMC의 새 UI.
- FTD API: 외부 엔터티에서 동일한 메트릭을 쿼리할 수 있도록 합니다.

표지 아래:

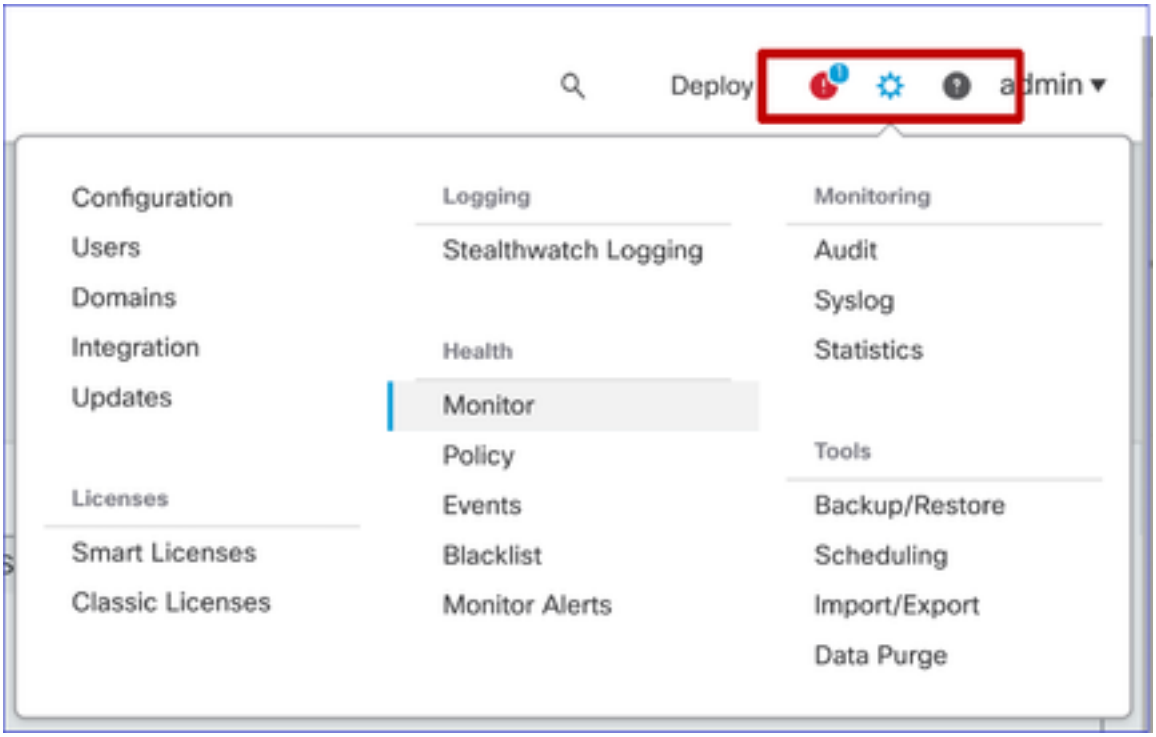
- Telegraf라는 오픈 소스 툴을 사용하여 디바이스의 상태를 수집합니다.
- 데이터를 FMC로 내보냅니다(FMC에서 실행 중인 opensource Time Series 데이터베이스, Prometheus 사용, 각 디바이스를 1분마다 폴링하여).
- 관리자: FMC, FMC REST API, FTD 디바이스 REST API

제한 사항 요약:

- 이 기능은 FDM GUI 또는 CDO에서 지원되지 않습니다
- 새 상태 모니터링 UI 내에서 FMC 자체를 모니터링하는 것은 지원되지 않습니다.
- 폴링 간격은 구성할 수 없습니다. 서로 다른 디바이스에 대해 서로 다른 폴링 간격을 구성할 수 없습니다. 모두 고정된 1분 간격으로 폴링됩니다.

구축 예

- 기능을 테스트하는 데 특정 구축이 필요하지 않습니다. FMC 및 디바이스를 FP 6.7로 업그레이드하기만 하면 됩니다.
- 상태 모니터링 데이터는 시스템 탭에서 액세스할 수 있는 FMC 상태 대시보드에서 사용할 수 있습니다.



사전 요구 사항 및 지원되는 플랫폼

지원되는 최소 소프트웨어 및 하드웨어 플랫폼

지원되는 최소 관리자 버전	관리되는 디바이스	최소 지원 관리되는 디바이스 버전 필요	참고
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	FTD에서만 지원됨
FTD 디바이스 REST API	FTD 6.7	FXOS 2.9.1 FTD 6.7	FTD 디바이스 REST API 전용 (FDM 또는 CDO GUI 아님)

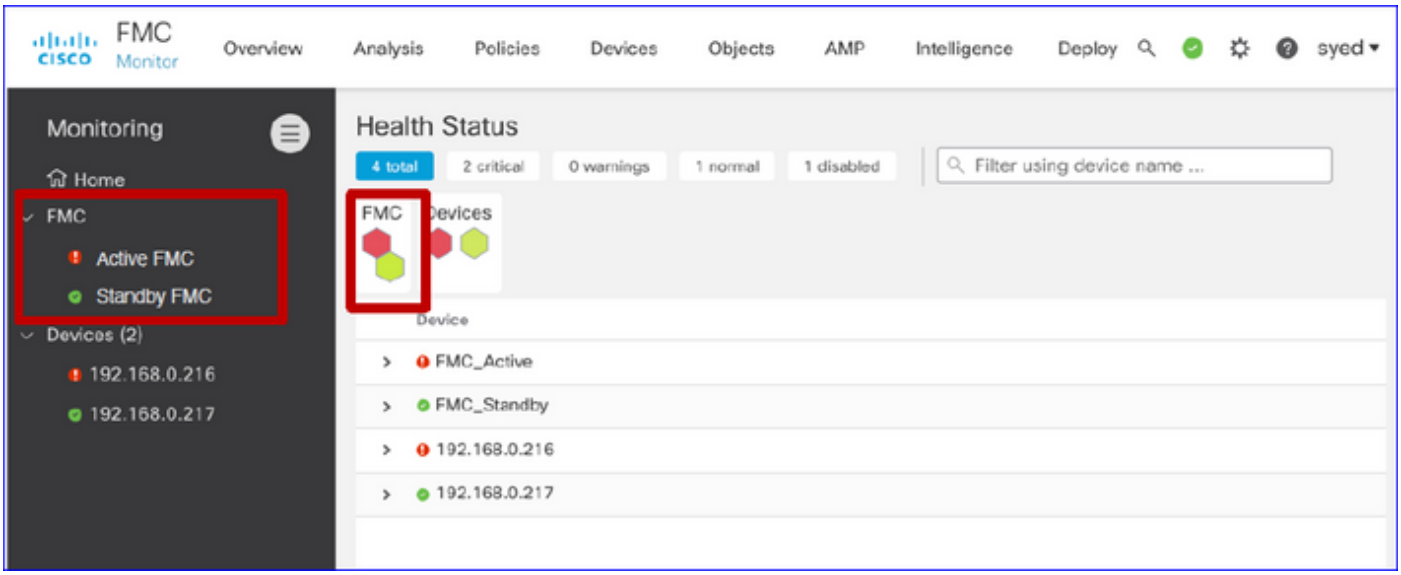
상호운용성

상호운용성에 대한 구체적인 요구 사항은 없습니다.

기능 세부사항 7.0

FMC UI: 독립형 및 HA 지원

상태 모니터링 페이지 탐색



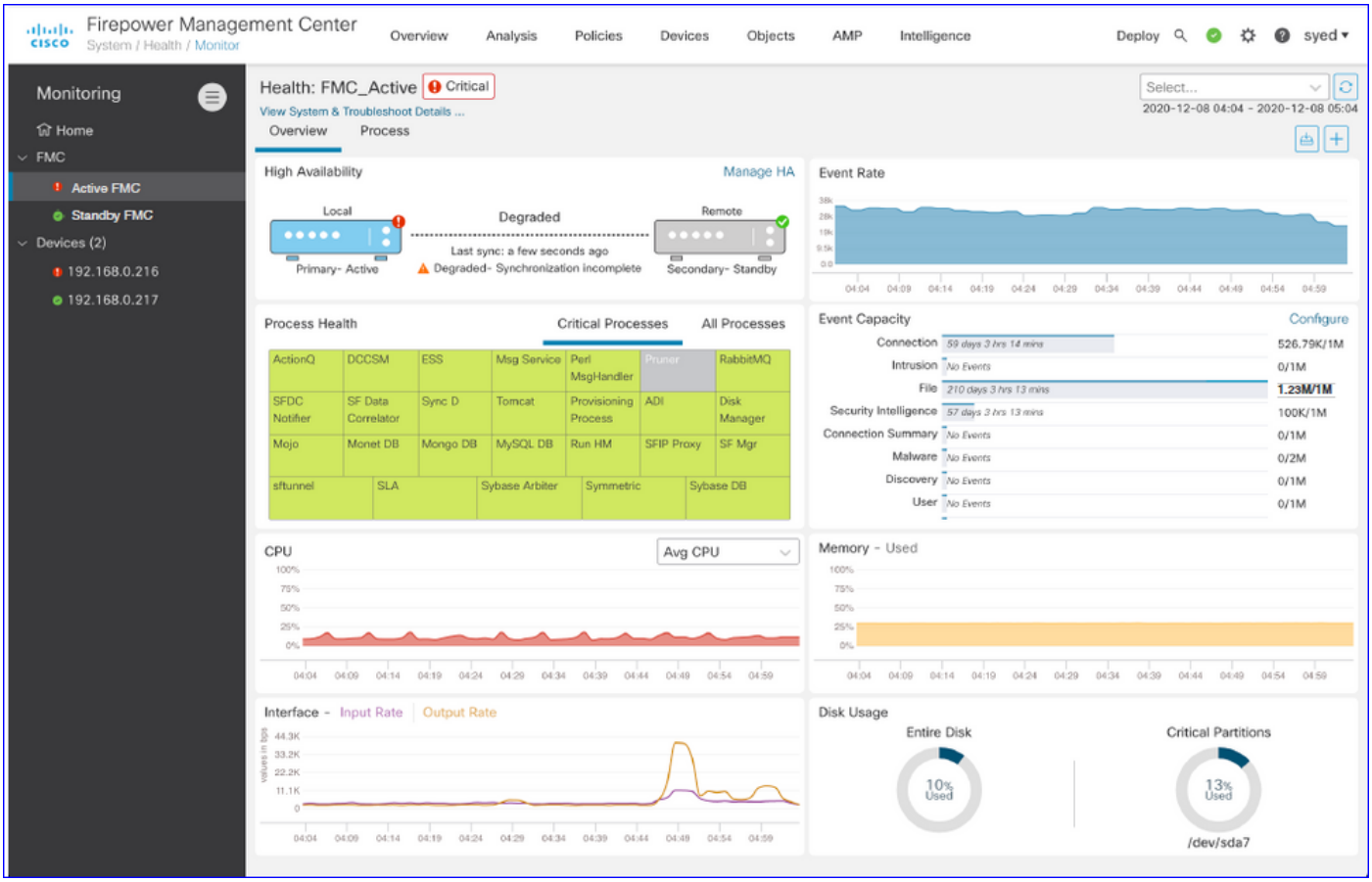
- 독립형 FMC는 단일 노드로 표시됩니다
- FMC HA가 노드 쌍으로 표시됨
- 각 FMC는 상태와 함께 표시됩니다

상태

- FMC HA는 트윈 육각형으로 표시됩니다.
- FMC 액티브 및 스탠바이 디바이스도 경고 테이블에 나열됩니다.

FMC 대시보드

7.0의 FMC 상태 모니터링 대시보드



요약 보기:

- 고가용성
- 이벤트 속도 및 용량
- 프로세스 상태
- CPU
- 메모리
- 인터페이스
- 디스크

이 대시보드는 활성 및 대기 FMC에서 모두 사용할 수 있습니다. 사용자는 맞춤형 대시보드를 생성하여 자신이 선택한 메트릭을 모니터링할 수 있습니다.

FMC 대시보드: FMC HA 패널

HA 패널의 프로그램

- 현재 HA 상태
- 액티브 대 스탠바이
- 마지막 동기화 시간
- 디바이스 상태

FMC 대시보드: 이벤트 속도 및 용량

이벤트 속도

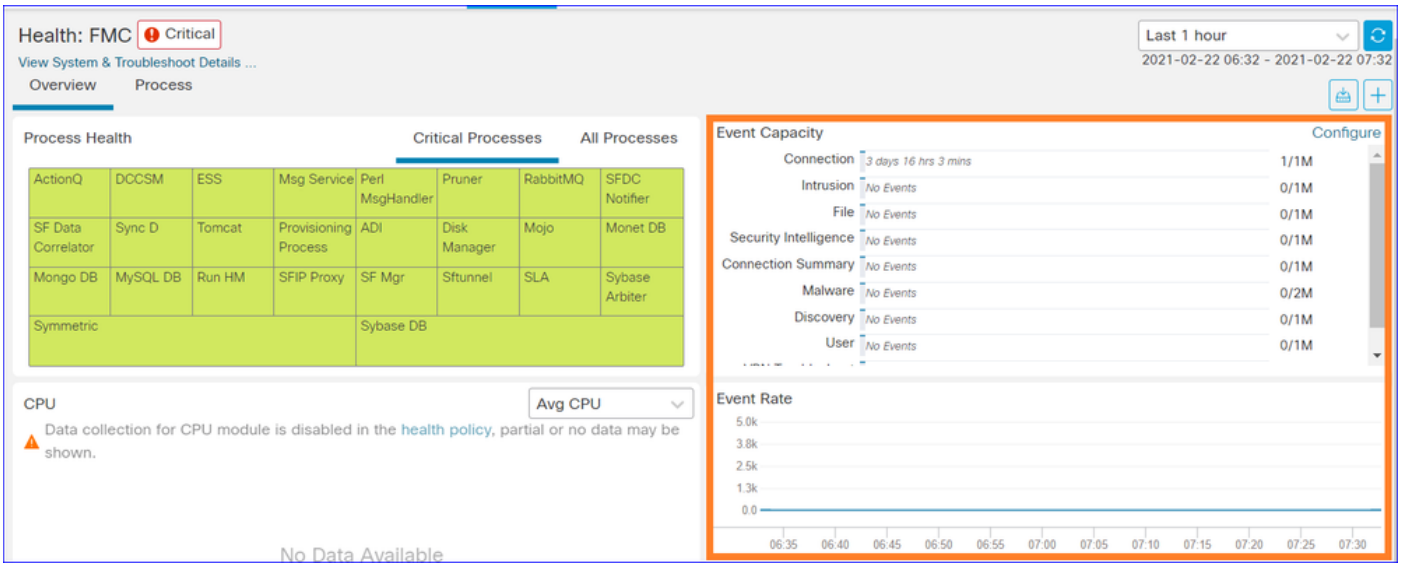
- 기본 행으로서의 최대 이벤트 속도
- FMC가 수신하는 전체 이벤트 비율

이벤트 용량

- 이벤트 범주별 현재 소비량
- 이벤트 보존 시간
- 현재 대 최대

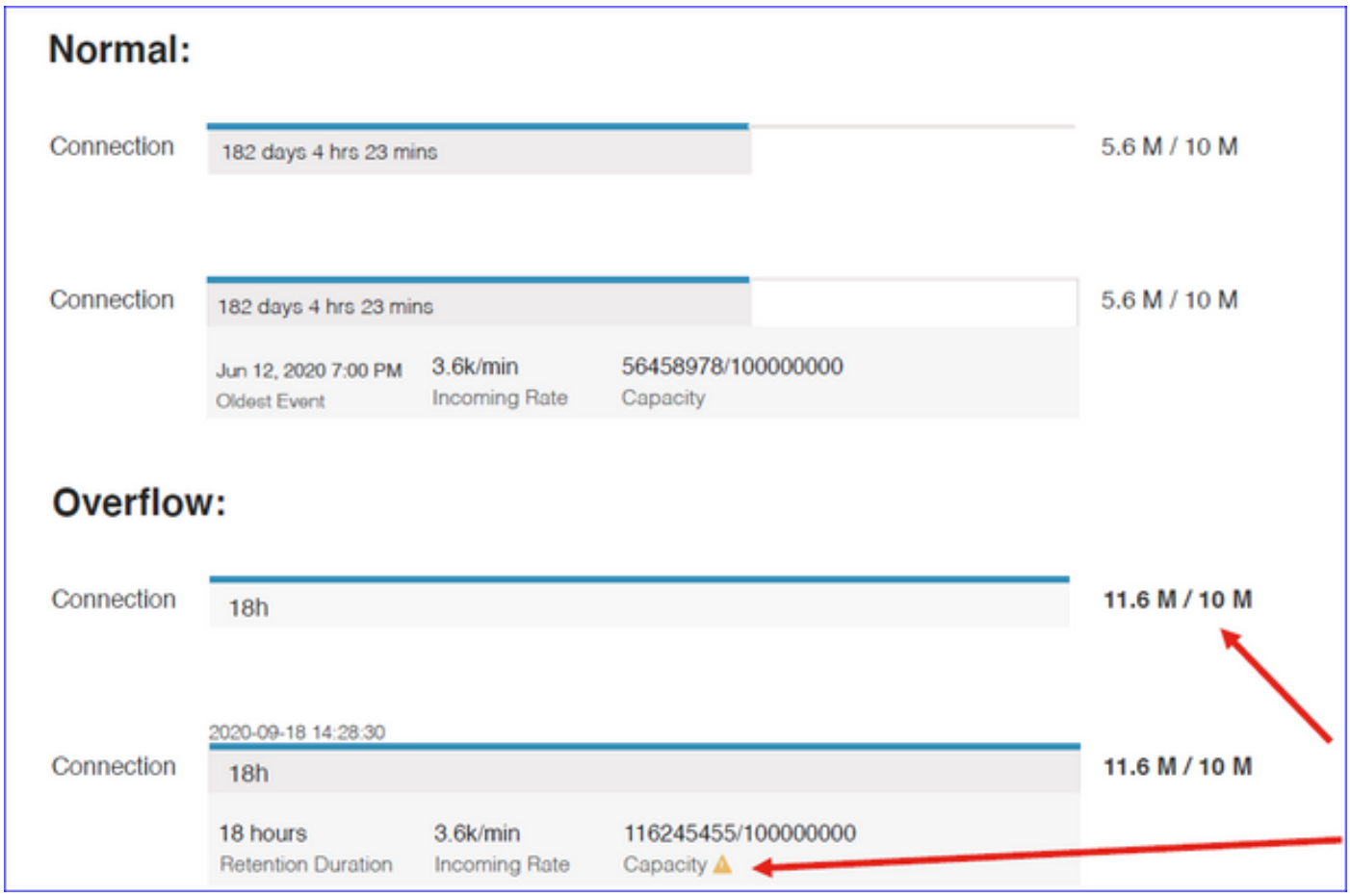
이벤트 용량

- 용량 오버플로 마커



FMC 대시보드: 이벤트 용량

일반 이벤트 용량 소비 상태



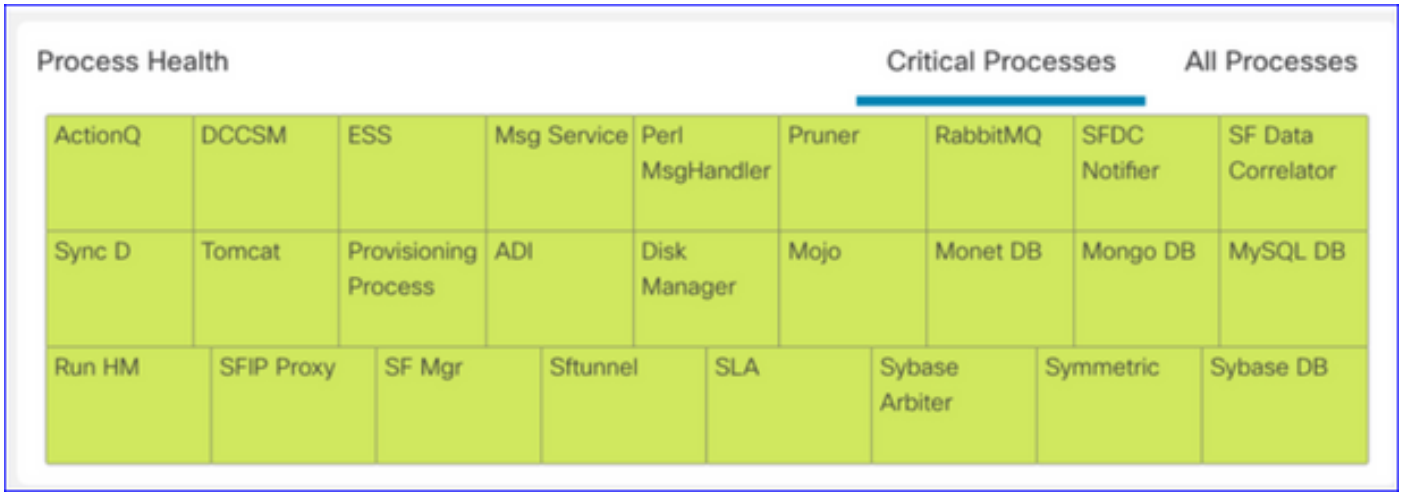
오버플로 시나리오 - 이벤트가 구성된 최대 용량을 초과하여 저장된 경우

- 굵은 텍스트는 오버플로를 나타냅니다.
- 경고 아이콘은 용량 오버플로를 강조 표시합니다

FMC 대시보드: FMC 프로세스 패널

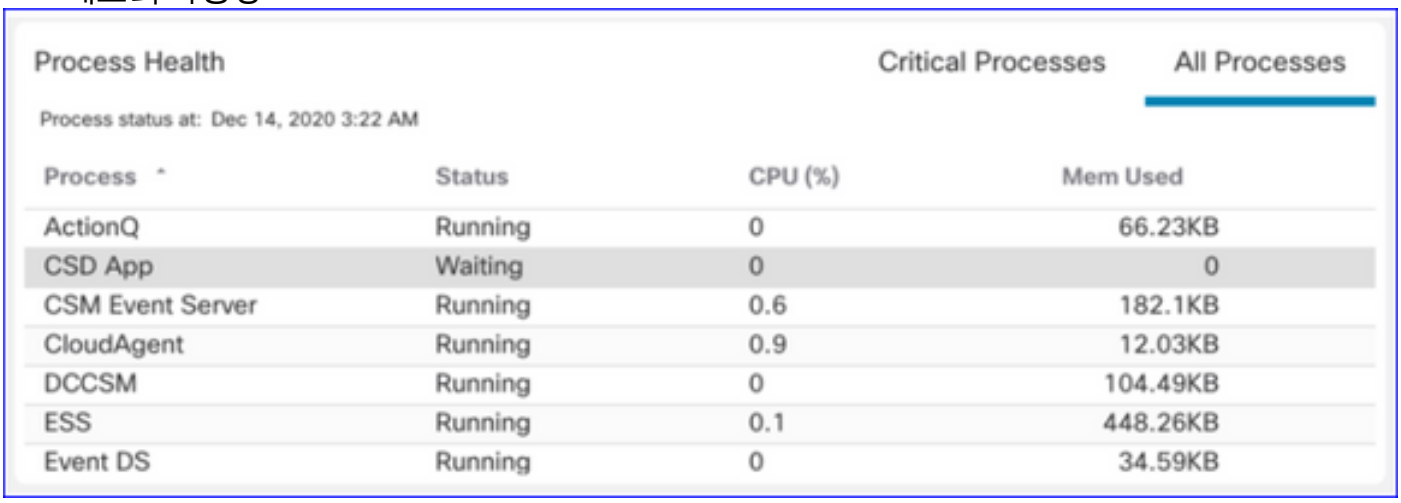
Critical Processes(중요 프로세스) 패널에는

- 프로세스 현재 상태
- 프로세스 재시작 횟수



프로세스 패널에는 모든 'pmconfig' 프로세스에 대한 다음 메트릭이 표시됩니다.

- 현재 상태
- CPU 사용
- 메모리 사용량



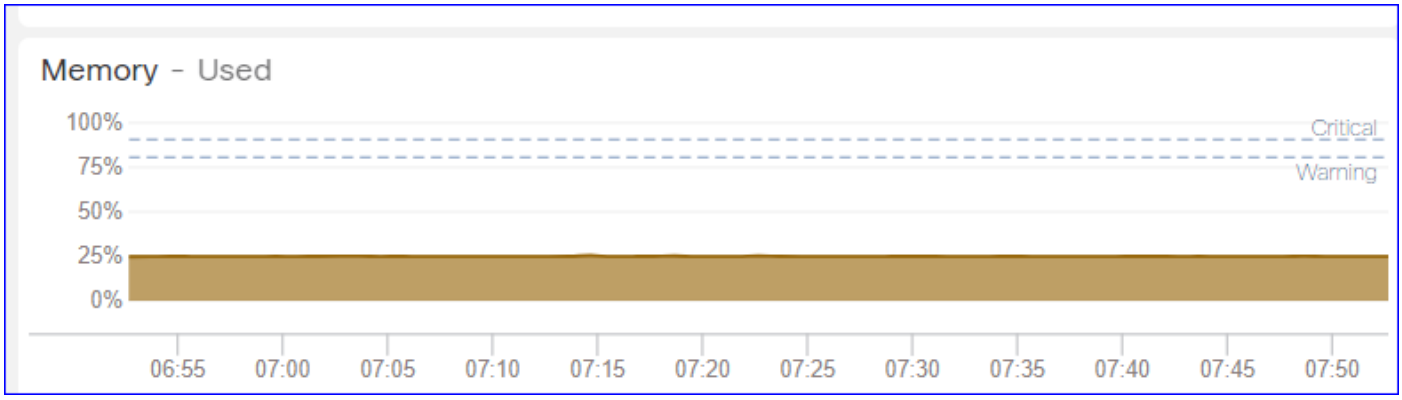
FMC 대시보드: FMC CPU

CPU 패널 표시

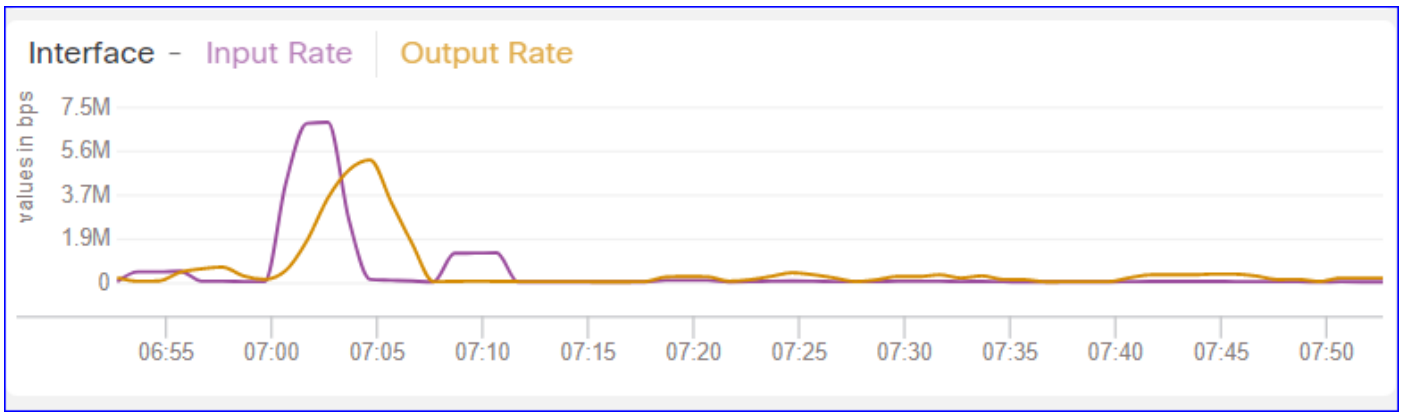
- 평균 CPU(기본값)
- 모든 코어

FMC 대시보드: 기타 패널

Memory(메모리) 패널에는 FMC의 전체 메모리 사용량이 표시됩니다.

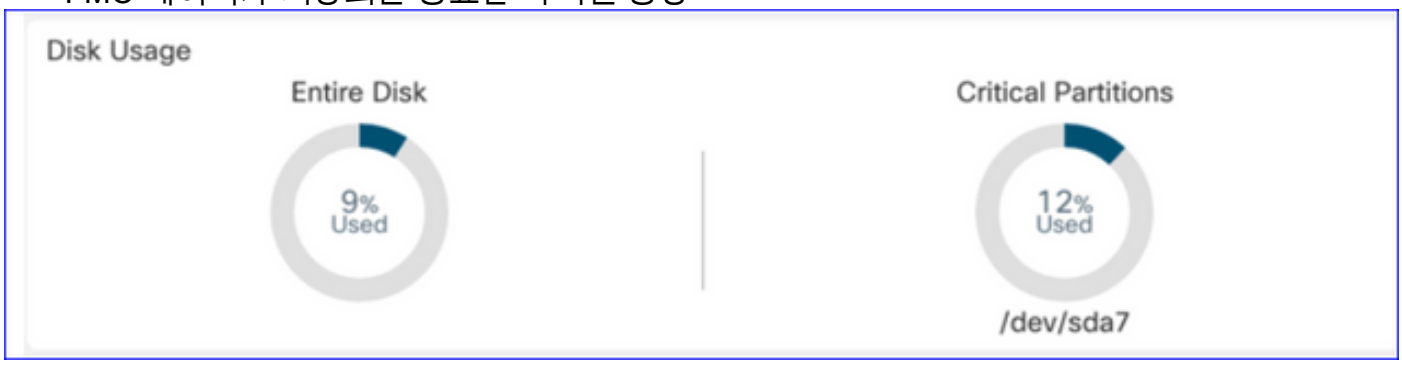


인터페이스 패널은 모든 인터페이스의 평균 입출력 속도를 표시합니다.



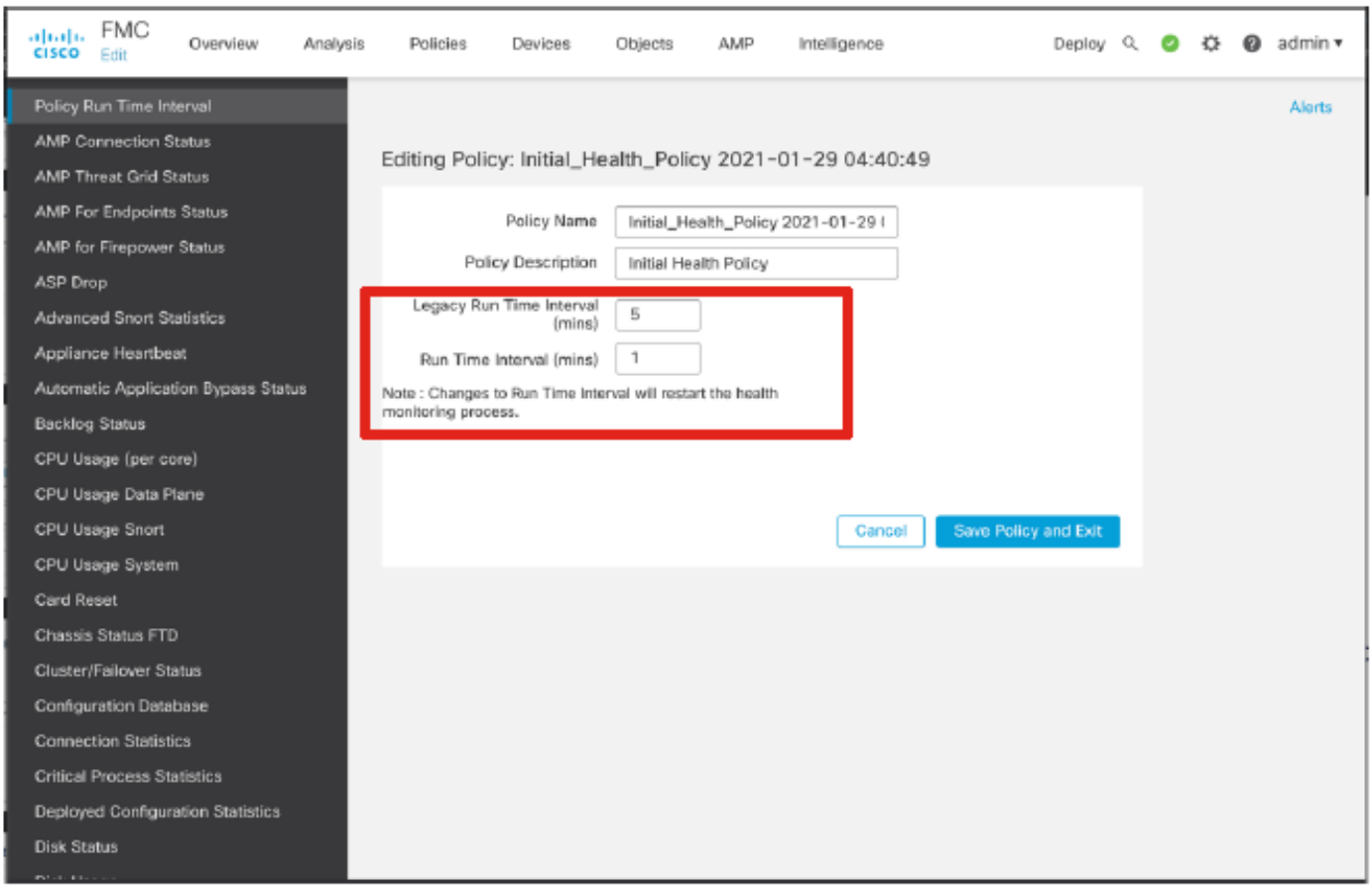
Disk(디스크) 패널 표시

- 전체 디스크 용량
- FMC 데이터가 저장되는 중요한 파티션 용량



실행 시간 간격

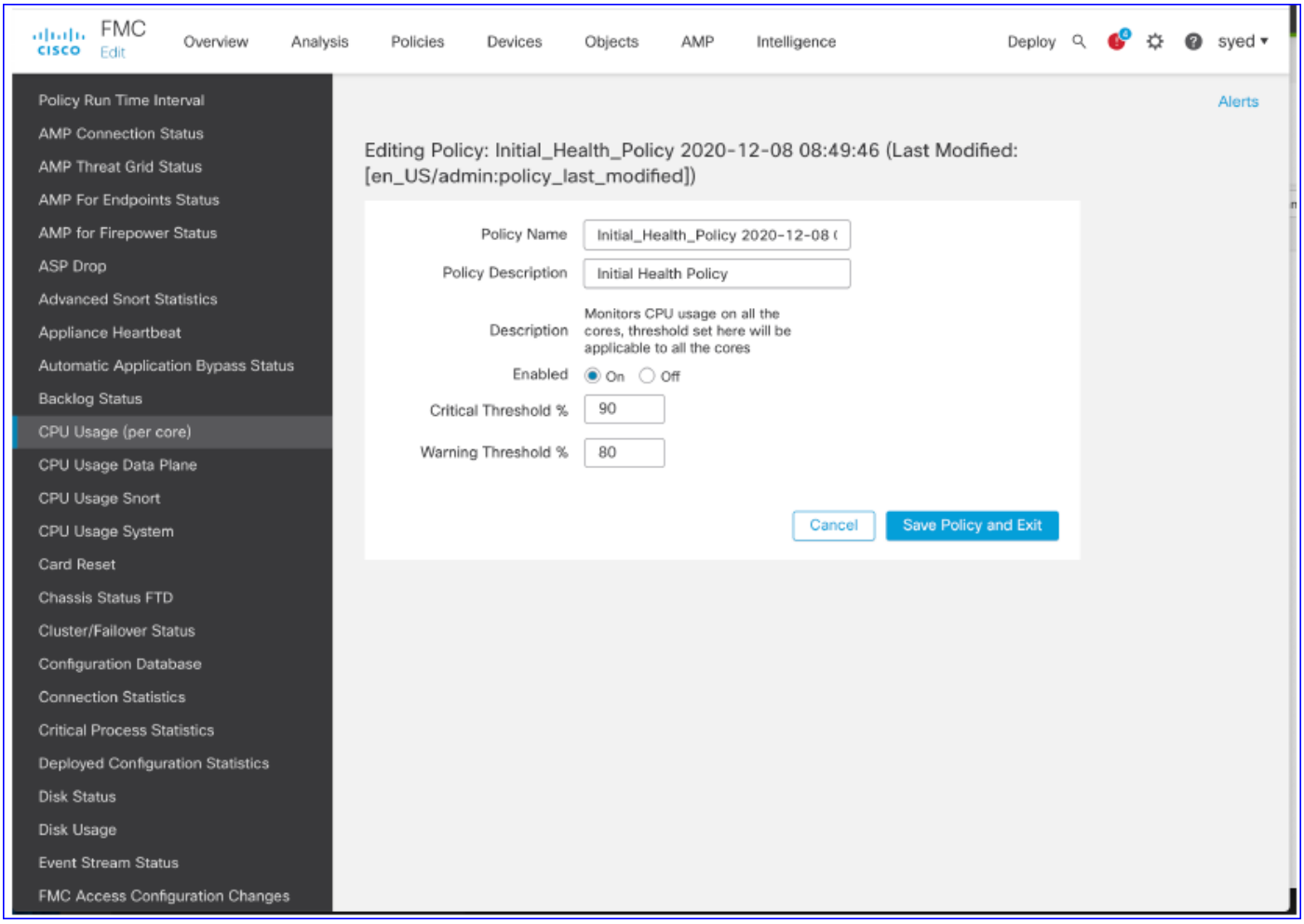
- 이전 상태 모듈의 실행 시간 간격이 'Legacy Run Time Interval'으로 이름이 바뀌었습니다.
- 'Run Time Interval'은 새로운 Telegraf 기반 상태 모듈을 대상으로 합니다.
- 전역 설정, 모든 디바이스에 영향을 미침
- Prometheus 스크랩 시간 재설정 및 상태 모니터링 프로세스를 다시 시작합니다.



사용 가능한 메트릭

맞춤형 대시보드에 사용 가능한 메트릭

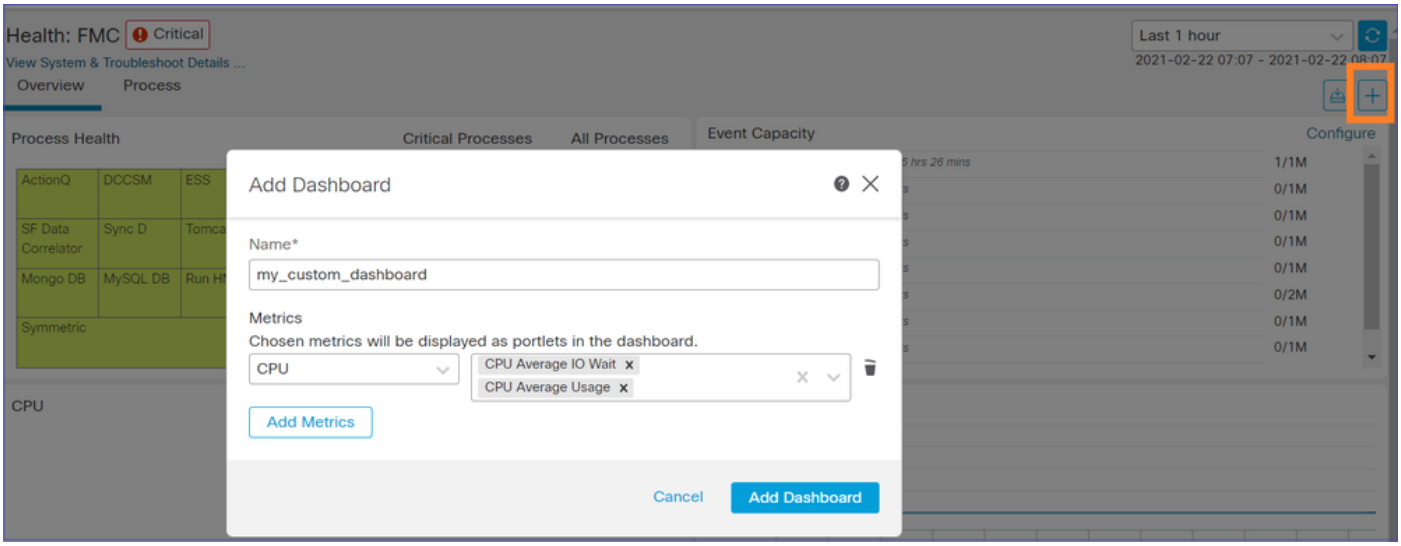
- 사용자가 사용자 지정 대시보드를 만들고자 하는 경우, 이러한 슬라이드는 사용 가능한 메트릭스에 대한 가이드입니다.
- 일부 메트릭을 사용자 지정 상태 대시보드에서 사용하려면 먼저 상태 정책에서 활성화해야 합니다



FMC UI: FMC 사용자 지정 대시보드

7.0의 새로운 FMC 모니터링 메트릭 범주

- CPU
- 메모리
- 인터페이스
- 디스크
- 이벤트
- 프로세스
- 래빗엠큐
- 사이베이스
- MySQL



FMC UI: FMC 메트릭

여러 카테고리에 걸쳐 40개의 메트릭이 추가되었습니다(사용자 지정 대시보드에서 사용 가능). 비활성화된 메트릭을 활성화하려면 연결된 상태 정책(**System > Health > Policy**)에서 해당 상태 **모듈을** 활성화합니다.

메트릭 그룹 이름	기본적으로 활성화됨	설명
CPU	아니요	FMC CPU 모니터링
메모리	예	FMC 메모리 모니터링
디스크	예	FMC 디스크 사용량 모니터링
인터페이스	예	FMC 인터페이스 모니터링
프로세스	예	FMC 프로세스 모니터링
이벤트	예	이벤트 속도 모니터링
MySQL	아니요	MySQL 모니터링
래빗엠큐	아니요	모니터 RabbitMQ
사이베이스	아니요	Sybase 모니터링

FTD: FP 7.0에 도입된 메트릭

기본적으로 활성화됨: 메트릭은 기본적으로 수집됩니다. 비활성화된 메트릭을 활성화하려면 연결된 상태 정책(System > Health > Policy)에서 해당 상태 모듈을 활성화합니다.

메트릭 그룹 이름	기본적으로 활성화됨	설명	플랫폼
섀시 상태	예	팬 속도 및 온도와 같은 다양한 섀시 매개변수를 모니터링합니다.	FPR2100 및 FPR1000 플랫폼에만 적용 가능
플로우 오프로드	예	하드웨어 플로우 오프로드 통계 모니터링	FPR9300에 적용 가능 및 FPR4100 플랫폼
ASP 삭제	예	Lina 측 패킷 삭제 모니터링	모두
적중 횟수	아니요	액세스 제어 정책 규칙의 적중 횟수 모니터링	모두
AMP Threat Grid 상태	예	AMP와의 연결 모니터링 위협 그리드	모두
AMP 연결 상태	아니요	FTD에서 AMP 클라우드 연결 모니터링	모두
SSE 커넥터 상태	아니요	FTD에서 SSE 클라우드 연결 모니터링	모두

NTP 상태	아니요	에서 NTP 클럭 동기화 매개변수를 모니터링합니다.	모두
VPN 통계	예	FTD S2S 및 RA VPN 터널 통계 모니터링	모두
경로 통계	예	Lina 측 패킷 삭제 모니터링	모두
Snort 3 성능 통계	예	특정 Snort3 성능 통계 모니터링(perfstats)	모두
xTLS 카운터	아니요	xTLS/SSL 흐름, 메모리 및 캐시 효율성 모니터링	모두

REST API, Syslog, SNMP

7.0에는 새로운 FMC 또는 FTD 디바이스 REST API가 도입되지 않았습니다. 기존 REST API는 7.0에 추가된 새로운 메트릭을 지원합니다.

Syslog 및 SNMP

Syslog

- 상태 모니터에 대한 syslog의 변경 없음

SNMP

- "SNMP Device Health Monitoring(SNMP 디바이스 상태 모니터링)"을 위한 별도의 TOI

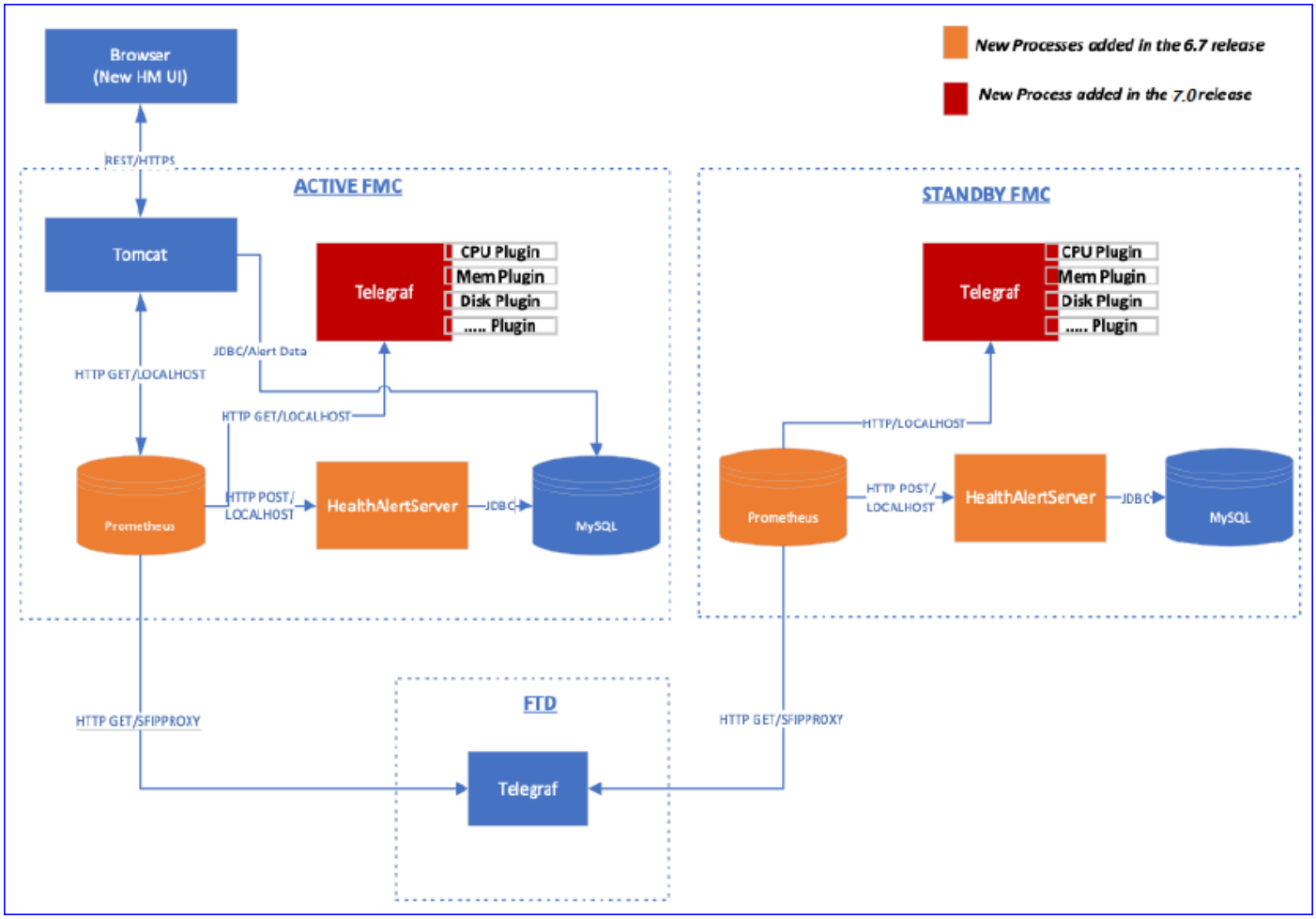
SAL/CTR/타사 제품 통합

- 'Azure Application Insights' 지원을 위한 별도의 TOI
- 'Health Monitoring'과 SAL/CTR/SecureX의 통합을 지원하기 위해 특별히 변경된 사항이 없음
- REST API는 서드파티 통합을 위해 활용 가능

소프트웨어 기술

아키텍처 개요

- FMC별 메트릭을 수집하기 위해 FMC에 Telegraf 상태 에이전트가 추가되었습니다.
- 프로메테우스는 텔레그래프에서 메트릭을 수집하고 시계열적으로 저장합니다.
- 값이 상태 정책에서 사용자가 구성한 임계값을 초과할 경우 알림이 생성됩니다.
- Telegraf 상태 에이전트는 메트릭을 수집하기 위한 오픈 소스 플러그인 기반 에이전트입니다. 1분마다 데이터를 수집합니다.
- FMC의 오픈 소스 시계열 데이터베이스인 Prometheus는 1분마다 디바이스에서 메트릭을 가져옵니다.



기능 세부사항 6.7

기능 기능 설명

FTD 상태 및 성능을 위한 새로운 NGFW 상태 모니터링

다음과 같은 사용자 지원

- 사후 대응적 디버깅(예: 근본 원인 분석 후 문제 발생)
- 사용 및 포화 수준 모니터링과 같은 사전 대응적 조치를 통해 잠재적 용량 문제를 파악하고 사용자가 용량 개선 또는 리팩터링을 수행하도록 지원합니다.

Cisco TAC 및 엔지니어링 팀에 유용한 기능:

- 시스템 문제의 격리 및 근본 원인 파악
- 개발 과정 및 운영 과정에서 시스템의 병목 지점을 파악합니다.

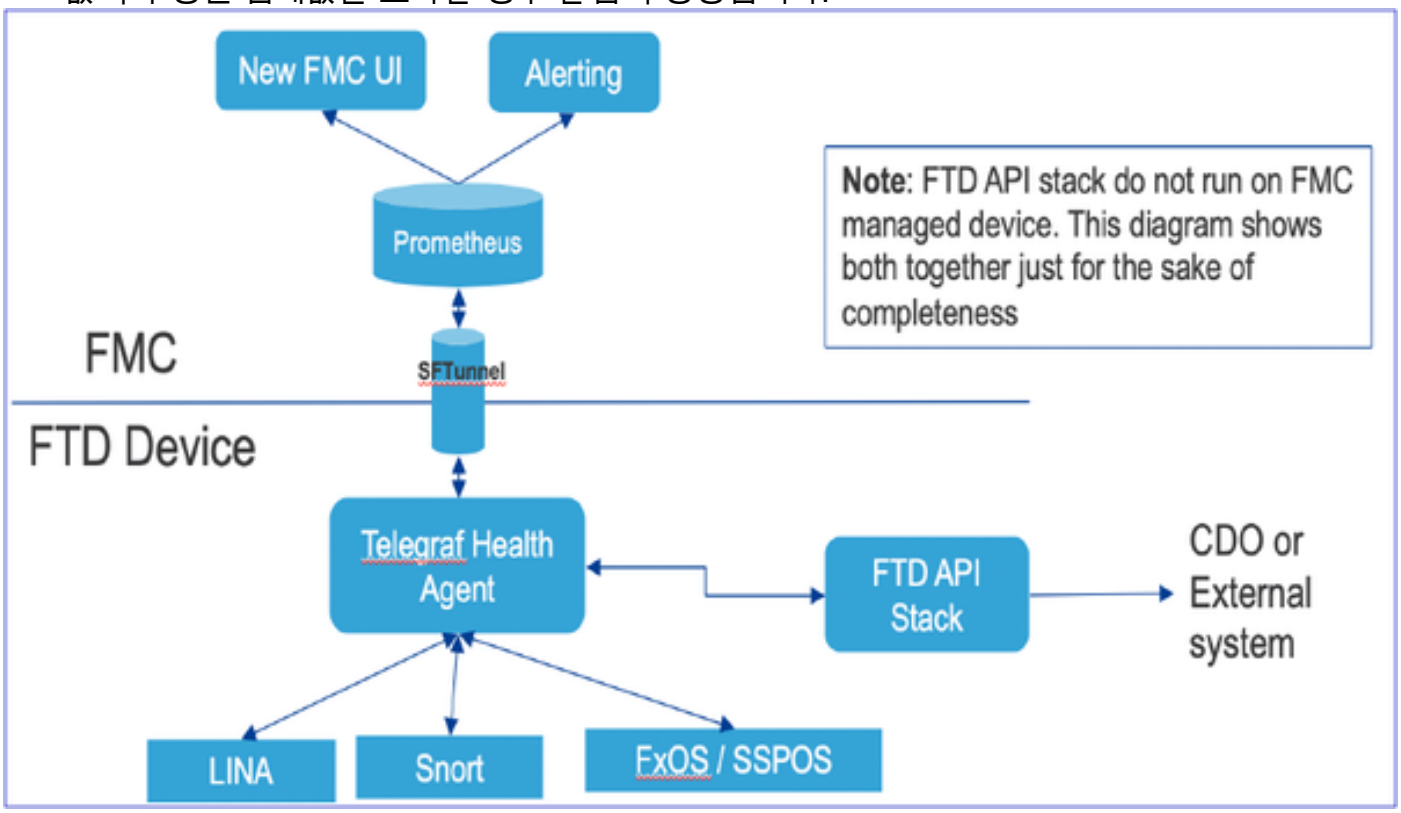
주요 내용

- **트렌드 차트**: 트렌드 차트를 사용하면 이상 징후를 쉽게 탐지하고 문제의 근본 원인을 파악할 수 있습니다. 시각적 검사 추세를 포착하고 서로 다른 메트릭 간에 상관관계를 그려 그 사이의 인과관계를 찾을 수 있다.
- **이벤트 오버레이**: 이벤트 오버레이는 구성 배포 및 SRU 업데이트와 같은 중요한 정보를 추세 차트에 표시하여 인과관계를 나타냅니다.
- **맞춤형 대시보드**: 사용자는 자신의 대시보드를 만들어 한 페이지에서 함께 보려는 메트릭을 그룹화할 수 있습니다.

- **Unified Health 모니터링 아키텍처**: 지표에 "관심 있는" 관리자와 관계없이 지표에 대한 단일 수집 및 내보내기 지점 FTD API 및 FMC는 동일한 메트릭 컬렉터의 데이터를 사용합니다.
- **지표의 확장성**: 플랫폼을 위한 아키텍처의 목표 중 하나는 새로운 지표를 쉽게 추가할 수 있는 것이었습니다. 이는 오픈 소스 메트릭 수집 및 스토리지 툴과 사용자 지정 가능한 대시보드를 사용하여 달성할 수 있습니다.

운영 방식

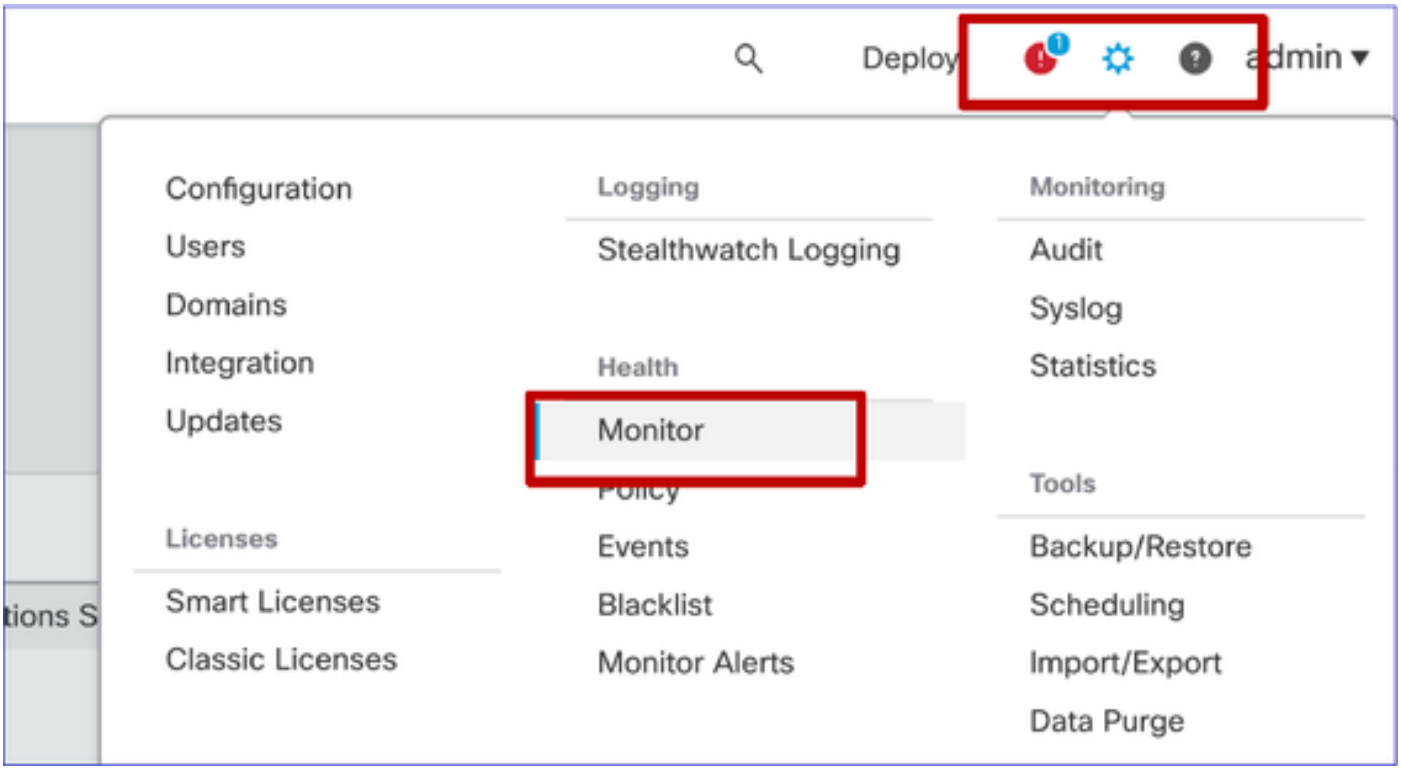
- Telegraf 상태 에이전트는 메트릭을 수집하기 위한 오픈 소스 플러그인 기반 에이전트입니다. 1분마다 정기적으로 데이터를 수집합니다.
- FMC의 오픈 소스 시계열 데이터베이스인 프로메테우스는 장치에서 주기적으로 1분마다 메트릭을 가져옵니다.
- 메트릭 값은 순간 데이터를 나타냅니다.
- 프로메테우스는 데이터를 시계열 형식으로 저장하며, 이는 UI에 의해 렌더링된다.
- 값이 구성된 임계값을 초과할 경우 알림이 생성됩니다.



FMC GUI

FMC UI: Health Status로 이동

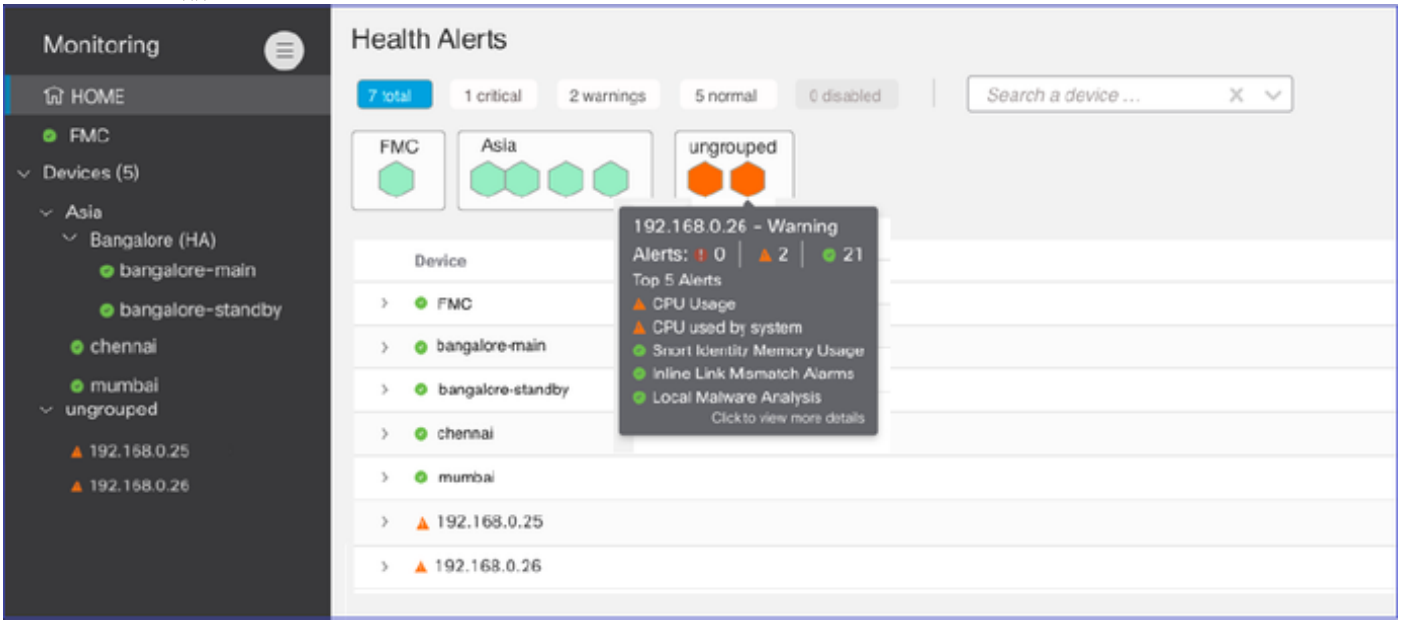
FMC에서 **System(시스템)** 아이콘 > Health(**상태) > Monitor(모니터링)**를 클릭하여 **Health Status(상태) 페이지로** 이동합니다.



FMC UI: 새 상태 페이지

Health Status 페이지는 FMC의 상태를 포함하여 FMC가 관리하는 모든 디바이스의 상태 개요를 표시하도록 설계되었습니다.

- 디바이스는 그룹/ha/클러스터에 따라 그룹화됩니다.
- 디바이스 왼쪽에 점이 있으면 상태가 표시됩니다
- 녹색 - 경보 없음
- 주황색 - 하나 이상의 상태 경고
- 빨간색 - 하나 이상의 중요 상태 경보
- 디바이스 상태를 나타내는 육각형을 가리키면 상태 요약이 표시됩니다.
- 경고 및 임계값에 대한 임계값은 상태 정책에서 FP 6.7 이전에 수행한 것과 동일한 방식으로 구성할 수 있습니다.



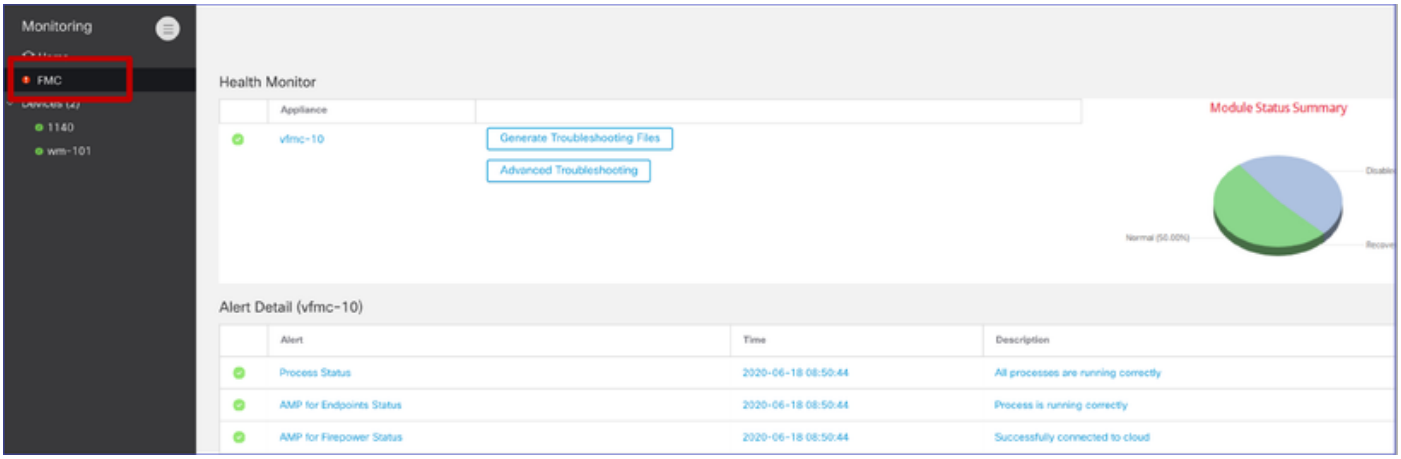
FMC UI: 디바이스 상태 이벤트

디바이스 경고와 관련된 상태 이벤트가 상태(심각도)별로 정렬되어 표시되게 하려면 아래쪽 패널에서 디바이스를 클릭합니다.

Health monitoring(상태 모니터링) 페이지

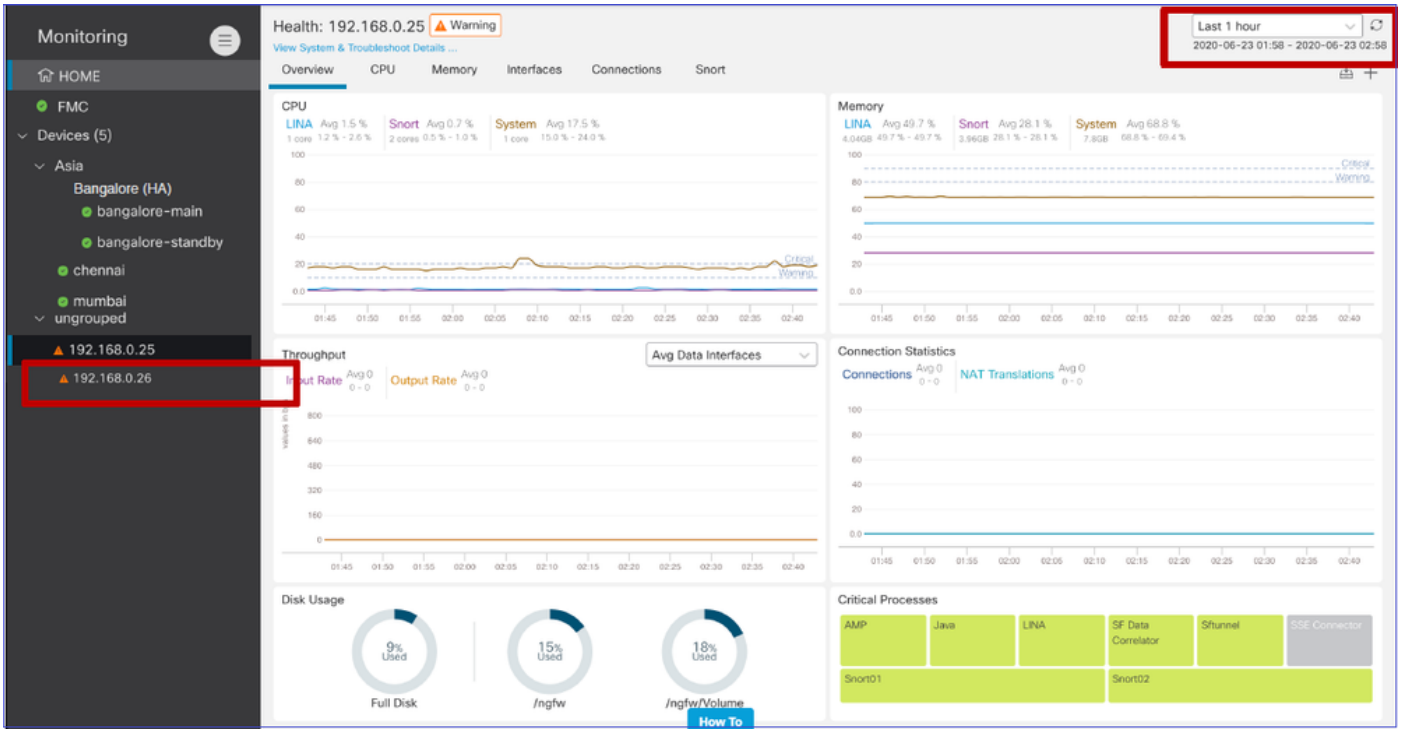
FMC UI: FMC 상태 모니터링이 변경되지 않음

FMC 상태 페이지는 여전히 기존 페이지입니다. 새 UI는 6.7 이상의 FTD에 대해서만 지원됩니다



FMC UI: 신규! 디바이스 대시보드

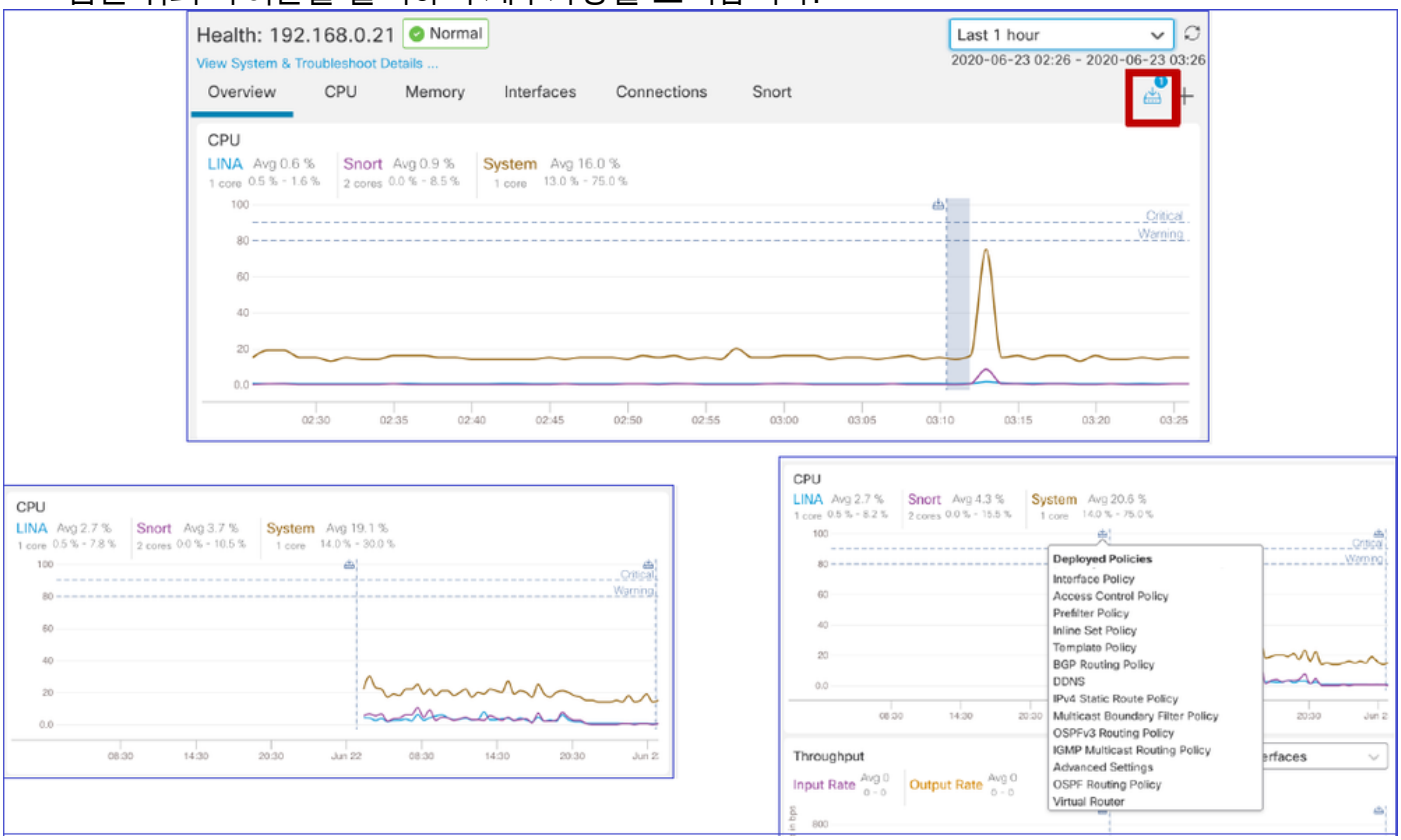
- 왼쪽 창에서 디바이스 이름을 클릭하여 디바이스의 상태 개요 페이지로 이동합니다.
- 상태 개요에는 모든 주요 상태 메트릭 추세 차트가 있습니다.
- 다양한 시간 범위를 사용할 수 있습니다(기본값 - 최근 1시간).
- Auto-refresh - 그래프 다시 로드



FMC UI: 배포 데이터 오버레이

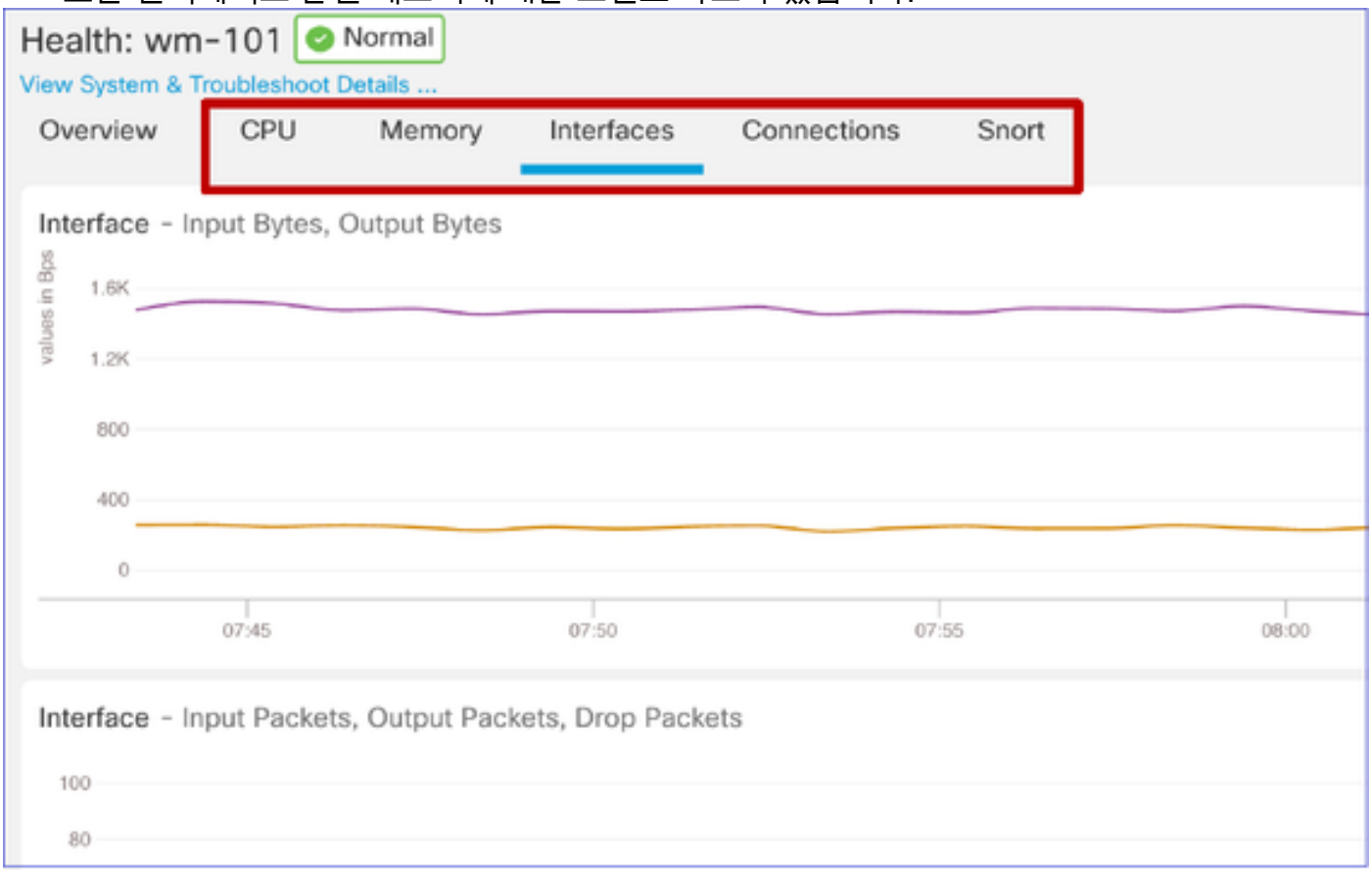
선택한 시간 범위를 기준으로 그래프에 구축 오버레이 세부사항을 표시하려면 구축 아이콘을 클릭합니다

- 아이콘은 선택한 시간 범위 동안의 배포 수를 나타냅니다.
- 대역은 구축 시작 및 종료 시간을 나타내는 것으로 나타납니다.
- 다중 구축의 경우 다중 밴드/라인이 나타납니다
- 점선 위의 아이콘을 클릭하여 세부사항을 표시합니다.

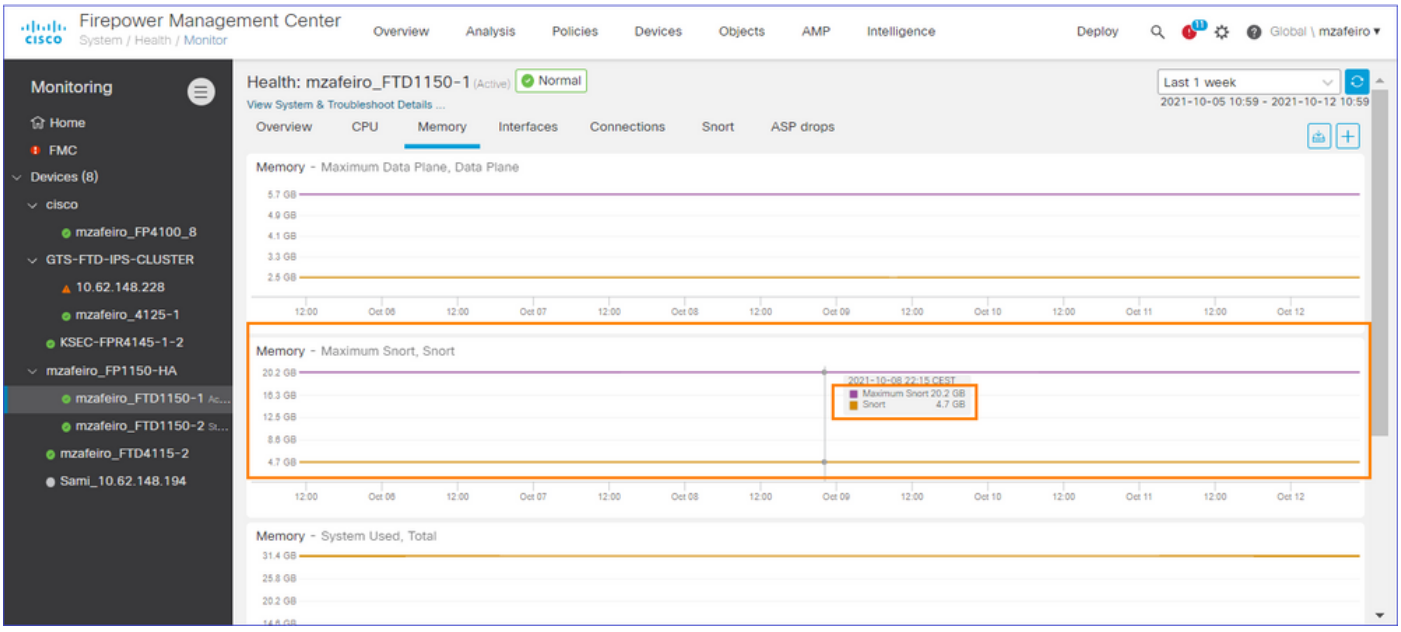


FMC UI: 디바이스 사전 구축 대시보드

- FMC UI에는 사전 구축된 상태 대시보드가 있습니다.
- 사전 구축된 이러한 대시보드에는 관련 메트릭이 그룹화되어 제공됩니다.
- 인터페이스 대시보드에는 입력/출력 바이트, 패킷, 서로 다른 인터페이스의 평균 패킷 크기 등 모든 인터페이스 관련 메트릭에 대한 트렌드 차트가 있습니다.



FTD Snort 메모리 - 어디에서 시작합니까?



UI 출력은 다음과 관련이 있습니다.

```
admin@FP1150-1:~$ sudo pmtool show CGroupsStatus | grep "Detectio" -A 20
[/dev/cgroups/memory/Detection]
Resources:
```

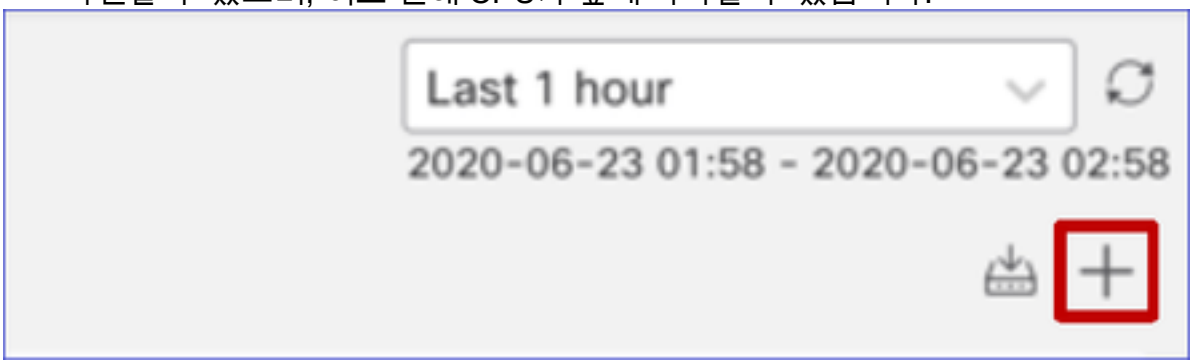
```
memory.memsw.failcnt: 0
memory.max_usage_in_bytes: 7,840,403,456
memory.limit_in_bytes: 21,719,199,744
memory.memsw.max_usage_in_bytes: 7,840,403,456
memory.usage_in_bytes: 5,035,372,544
memory.memsw.limit_in_bytes: 22,403,170,304
memory.failcnt: 0
memory.memsw.usage_in_bytes: 5,035,372,544
Procs:
<p9738> sfhassd
<p26746> snort
<p26747> snort
<p26748> snort
<p26749> snort
<p26750> snort
<p26751> snort
<p26752> snort
<p26753> snort
```

이 정보는 엔지니어링 팀에서 제공한 것입니다. https://jira-eng-rtp3.cisco.com/jira/browse/FPSVZ-1033

FMC UI: 맞춤형 대시보드 생성 가능

사용자가 직접 사용자 지정 대시보드를 생성할 수 있음

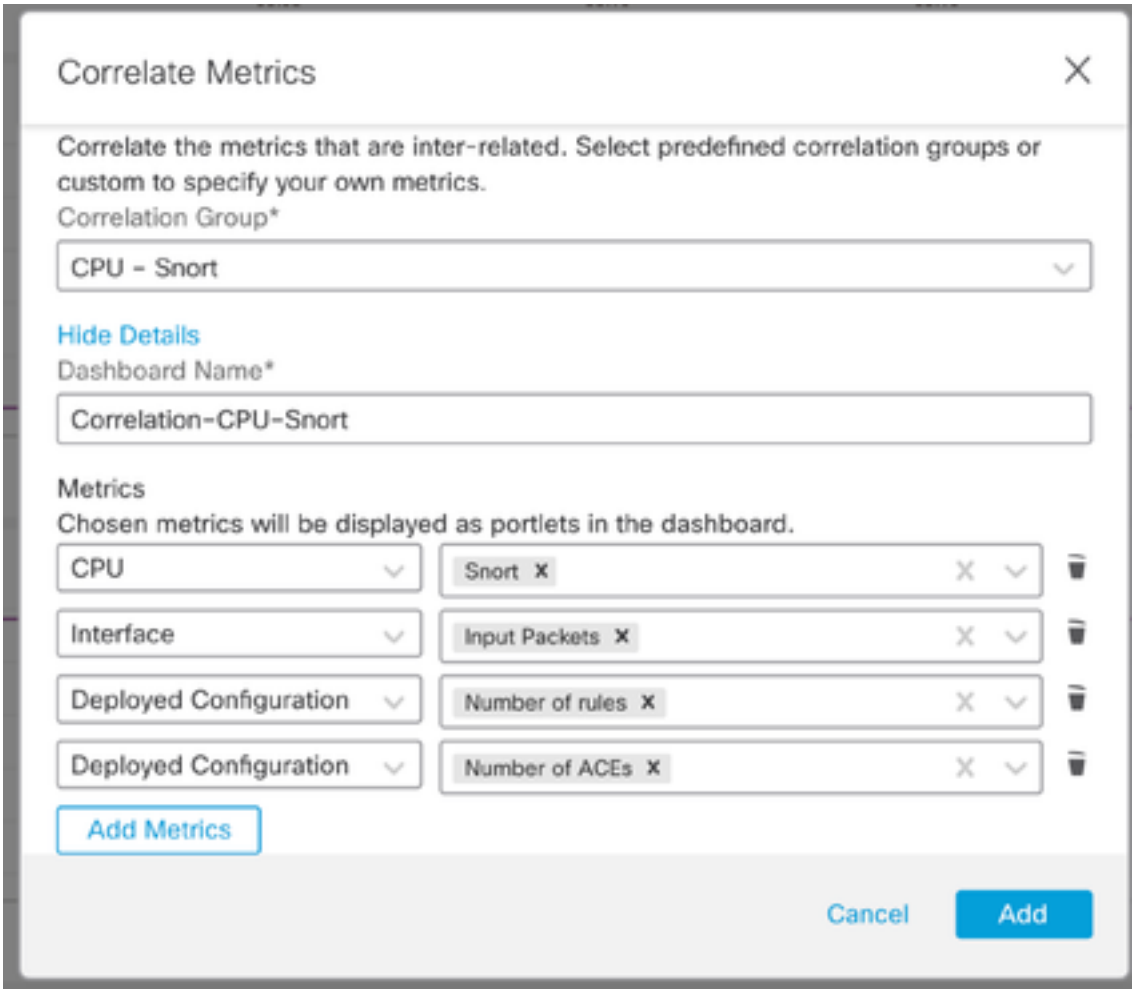
- 사용자는 사전 구축된 대시보드 외에도 사용자 지정 대시보드를 생성할 수 있습니다.
- 사용자 지정 대시보드에서 원하는 수만큼의 메트릭을 추가할 수 있습니다.
- 일반적으로 서로 다른 메트릭 그룹의 메트릭을 연계하여 문제의 근본 원인을 파악할 수 있는 경우 맞춤형 대시보드가 생성됩니다.
- Lina CPU가 높은 경우, CPS(Incoming Connection Per Second), 인터페이스 통계(기타) 등을 확인할 수 있으며, 이로 인해 CPU가 높게 나타날 수 있습니다.



FMC UI: 사용자 지정 대시보드 만들기

측정 단위 상관관계 대화 상자

- 사용자가 "+"를 클릭하여 사용자 지정 대시보드를 생성하면 Correlation Metrics(메트릭 상관관계) 창이 열립니다.
- 사용자는 함께 모니터링하고자 하는 다른 메트릭을 추가할 수 있습니다.



REST API

FMC REST API - 요약

FMC GET API	설명
/api/fmc_config/v1/domain/{domainUUID}/health/al 에르츠	그러면 다음에 대한 모든 상태 모듈의 상태가 반환 됩니다 지정된 UUID입니다.
/api/fmc_config/v1/domain/{domainUUID}/health/ 메트릭	API는 내부적으로 Time Series DB - Prometheus 및 반환 호출자.

FMC REST API - /health/alerts

다양한 필터 기준:

- startTime 및 endTime: 초 단위. 둘 다 함께 지정해야 합니다. 두 번 사이에 생성된 모든 알림 반환
- deviceUUID: 지정된 UUID에 대한 모든 알림을 반환합니다.
- 상태: 지정된 상태(빨간색, 노란색, 녹색)의 모든 경고를 반환합니다.
- ModuleID: 상태 모듈 ID 목록

샘플 출력:

```
{
  "items": [
    {
      "deviceUUID": "a04cb2da-8915-11ea-9d2e-da80fb1fedea",
      "moduleUUID": "980ca3ae-fd69-43c1-b3cc-d71ea394b2eb",
      "moduleID": "CPU",
      "timestamp": 1589271373,
      "status": "GREEN",
      "type": "HealthAlert"
    },
```


FMC REST API - /health/metrics

다양한 필터 기준:

- startTime 및 endTime: 초 단위. 둘 다 함께 지정해야 합니다. 두 번 사이에 생성된 모든 메트릭을 반환합니다.
- deviceUUID: 지정된 디바이스에 대한 모든 메트릭 반환
- 측정 단위: 지정된 이름(cpu, mem, disk)의 모든 측정 단위 반환
- 단계: 초 단위로 수행합니다. '단계'초마다 메트릭 값
- regexFilter: 메트릭 이름에 대한 Regex 필터 (예: snort)

샘플 출력

Sample output


```
```json
{
  "items": [
    {
      "deviceUUID": "d8c5ada2-a949-11ea-986f-83a5cef58c55",
      "metric": "cpu",
      "regexFilter": "cpu=~\"cpu1\"",
      "response": "{\"status\":\"success\",\"data\":{\"resultType\":\"matrix\",\"result\":[{\"metric\":{\"__name__\":\"cpu\",\
      "type": "HealthMetric"
    }
  ],
}
```


샘플 FMC REST 입력/출력

요청 URL:

https://u32c01p12-vrouter.cisco.com:10213/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/health/metrics?filter=deviceUUIDs:c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d;**metric:cpu;regexFilter:lina_cp_avg**;
startTime:1611294885.699;endTime:1611309285.699;step:60;

응답:

{

"링크":{

"항목":[{
```

"응답":{

"상태":"성공",

"데이터":{

"resultType":"matrix",

"결과":[{

"메트릭":{

"__name__":"cpu",

"cpu":"lina_cp_avg",

"인스턴스":"127.0.0.1:9273",

"작업":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d",

"uuid":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d"},

"값":[

[1611309165.699,"0.5"],

[1611309225.699,"0.5"],

[1611309285.699,"0.5"]

]

}

]}

}",

"deviceUUID":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d",

"메트릭":"cpu",

"regexFilter":"cpu=~"lina_cp_avg",

"유형":"메트릭"

}

FTD 디바이스 REST API

FTD 디바이스 REST API	설명
/devices/default/operational/metrics	모든 메트릭을 덤프합니다. 메트릭의 즉각적인 값

	이 반환됩니다.
/devices/default/operational/metrics/{objId}	{objId}로 식별된 특정 메트릭 덤프
/devices/default/operational/metricsschema	모든 측정 단위가 반환될 때 반환되는 출력의 덤프 스키마
	덤프됨(첫 번째 요청 가져오기)
/devices/default/operational/metricsschema/{objId}	특정 항목이 반환되는 경우 출력의 덤프 스키마 지정된 {objId}의 메트릭을 쿼리합니다.

FTD 디바이스 REST API: 메트릭 가져오기

메트릭에 대한 샘플 응답 본문

Curl

```
curl -X GET --header 'Accept: application/json' 'https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics'
```

Request URL

```
https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics
```

Response Body


```
{
  "items": [
    {
      "name": "mem.used_swap_snort",
      "metric": {
        "value": 0,
        "unit": "BYTE",
        "type": "numericdevicemetricvalue"
      },
      "timestamp": 1592316305,
      "dateTime": "2020-06-16T14:05:05Z",
      "id": "mem.used_swap_snort",
      "type": "devicemetricdata",
      "links": {
        "self": "https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics/mem.used_swap_snort"
      }
    },
    {
      "name": "mem.remaining_blocks_1550_bytes",
      "metric": {
```


Response Code

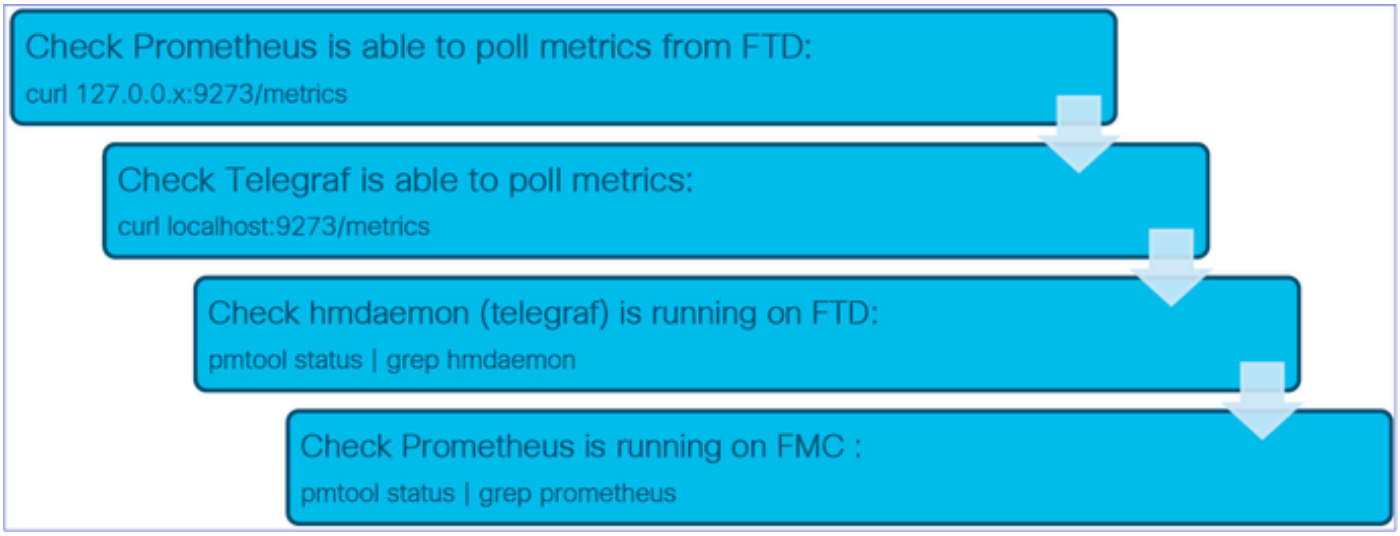
```
200
```

FTD 디바이스 REST API: 특정 메트릭 가져오기

특정 메트릭을 가져오려면 URL에서 해당 개체 ID를 지정합니다. 객체 ID는 측정 단위의 이름 필드입니다.

문제 해결/진단

진단 개요 - 일반적인 트러블슈팅 흐름



장치 문제 해결 및 로그인을 위한 중요 명령 및 파일

참고: 7.0 NPI에서는 포트 9273이 아니라 포트 9274를 언급합니다.

디바이스의 명령/파일	사용 용도
pmtool 상태 | grep hmdaemon	디바이스에서 telegraf가 실행 중인지 확인합니다.
curl localhost:9273/metrics	이 명령은 모두 가져오거나 텔레그래프에서 메트릭을 제공합니다.
curl localhost:9273/hm/<메트릭 이름>	O/P가 비어 있으면 Telegraf가 제대로 작동하지 않습니다.
pmtool 다시 시작byid hmdaemon	hmdaemon을 재시작하려면
/ngfw/var/log/hmdaemon.log	텔레그라프 로그가 저장되는 파일입니다.
/ngfw/etc/sf/telegraf_api.conf	telegraf 컨피그레이션을 캡처하는 파일입니다. 텔레그라프 구성에 대한 부분을 참조하십시오.

FMC 트러블슈팅에 포함된 강조 표시된 파일/명령 출력

FMC에서 문제 해결 및 로그인하는 데 필요한 중요 명령 및 파일

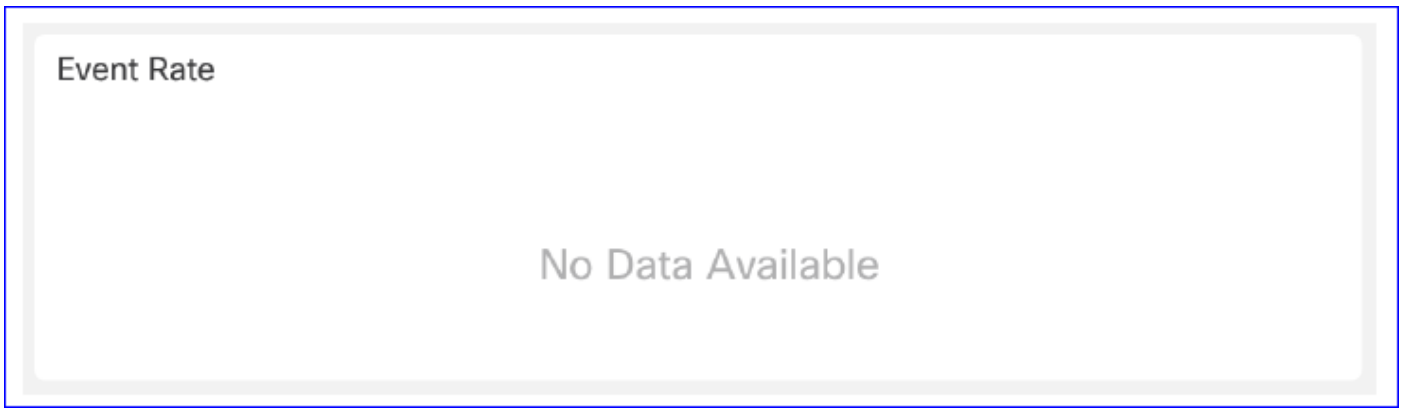
FMC의 명령/파일	사용 용도
pmtool 상태 | grep Prometheus	Prometheus가 디바이스에서 실행 중인지 확인합니다.
pmtool 다시 시작byid 프로메테우스	Prometeus를 다시 시작하려면
curl localhost:9090/metrics	9090 포트는 Prometheus 관리 포트입니다. /metrics 끝점은 자체 메트릭을 반환합니다.
curl localhost:9090/targets	**Prometheus로 구성된 대상을 나열하는 HTML 페이지입니다. 텍스트 끝점을 찾습니다.**
curl localhost:9090/alerts	활성 상태인 모든 경고를 나열하는 HTML 페이지. 그것은 장전이 훨씬 더 쉽다. 브라우저 및 검사에서
curl localhost:9090/rules	**구성 및 수락된 모든 규칙을 표시하는 HTML 페이지입니다. 구성된 규칙을 기준으로 이 항목을 확인할 수 있습니다.**
/var/opt/prometheus/	모든 프로메테우스 자료가 있는 디렉토리
/var/opt/prometheus/devicehm.yml	Prometheus의 기본 컨피그레이션 파일
/var/opt/prometheus/targets/	모든 대상(FTD Telegraf 인스턴스)이 저장되는 디렉토리입니다. 이 디렉토리 아래의 파일은 FMC에 의해 대상이 검색될 때 생성됩니다.
/var/opt/prometheus/rules/	모든 규칙 파일이 저장되는 디렉토리 적용된 상태 정책을 기반으로 각 디바이스에 대한 규칙 파일이 생성됩니다.
/var/opt/prometheus/data/	데이터 파일에는 모든 TSDB 데이터가 포함되어 있습니다. 이 디렉토리의 "du -h ."는 Prometheus에서 사용하는 스토리지를 제공합니다.
curl <target_ip>:9273/metrics	디바이스에서 메트릭 가져오기
/var/log/prometheus*	**프로메테우스 로그**

Troubleshoot에 포함된 강조 표시된 파일/명령 출력

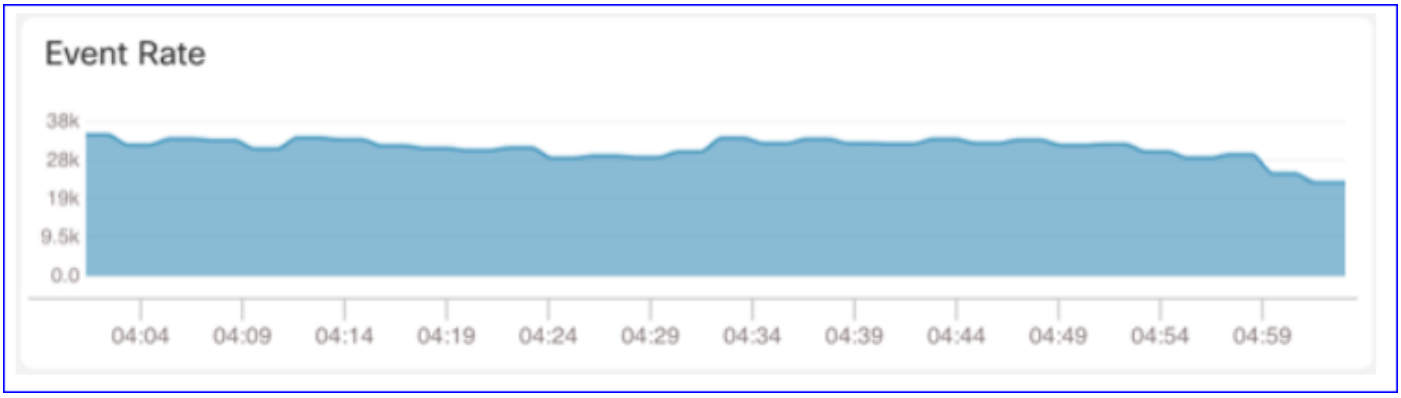
(디바이스)에서 데이터 수집 - GUI

GUI에 표시되는 시간 범위에 대한 데이터

Prometheus에 선택한 시간 범위에 대한 데이터가 없는 경우 GUI에서 대시보드 패널에 'No Data Available'을 표시합니다.



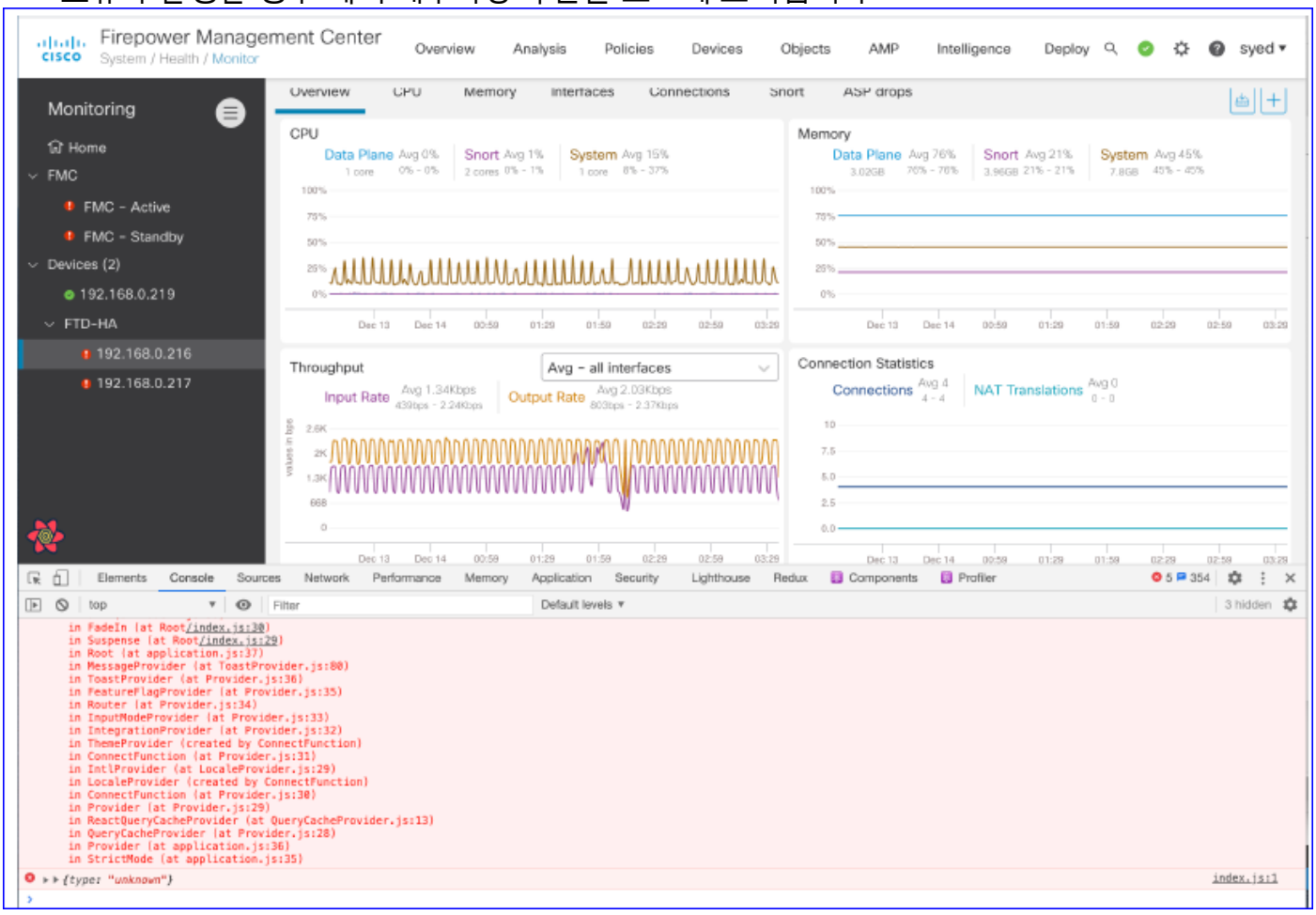
사용 가능한 데이터의 경우 다음과 같이 그래프가 나타납니다.



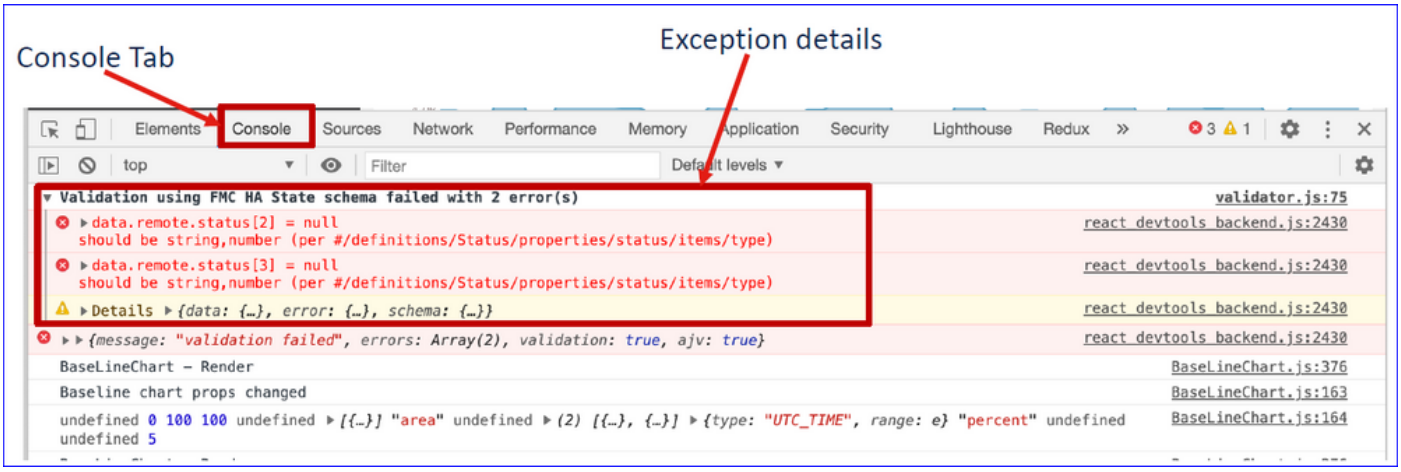
브라우저의 Console(콘솔) 및 Network(네트워크) 탭 사용

브라우저 콘솔 로그 및 네트워크 통화 로그

- 이 예에서는 Chrome 브라우저 개발자 콘솔이 표시됩니다
- 오류가 발생할 경우 예외 세부사항이 콘솔 로그에 표시됩니다



브라우저 콘솔 로그 예



(디바이스)에서 데이터 수집 — CLI

FMC에서 디버그 모드로 텔레그래프 활성화

1. FTD에서 expert 모드로 들어가서 sudo root 사용자로 로그인합니다
2. FTD에서 /etc/sf/fmc_telegraf_api.conf 파일을 엽니다.
3. "debug" 옵션의 주석 처리를 제거합니다.
4. 'pmtool HUPByID hmdaemon'을 실행하여 Telegraf 다시 로드
5. Telegraf는 디버그 모드에서 실행되며 /var/log/hmdaemon.log 파일에서 세분화된 디버그 메시지를 방출합니다

완료 시 "debug" 옵션에 대한 코멘트를 작성합니다.

제한 사항 세부 정보, 일반적인 문제 및 해결 방법

구현 참고 사항

- 메트릭의 정확도는 폴링 인스턴스 빈도에 따라 다릅니다.
- 그래프의 최대 데이터 해상도는 1440(1일 기간)입니다. 시간 범위가 크면 일부 데이터 포인트가 표시되지 않습니다.
- FTD 디바이스 REST API 출력은 JSON 형식입니다.
- FMC REST API 출력은 Prometheus 형식입니다. 프로메테우스 형식에 대한 자세한 내용은 을 /를 참조하십시오.

https://prometheus.io/docs/prometheus/latest/querying/api/

- Prometheus 형식은 (Grafana)와 같은 외부 도구를 유연하게 통합할 수 있게 해줍니다

참고: FMC 상태 정책에서 CPU 사용률 메트릭은 기본적으로 비활성화되어 있습니다. 연결된 상태 정책을 수정하여 활성화할 수 있습니다.

해결 방법 및 팁

그래프의 주석이 그래프 끝에서 깜박입니다.

- 이 문제를 방지하려면 커서를 천천히 이동하십시오.

그래프의 주석에는 표시되는 데이터를 제한하는 최대 길이가 있습니다.

- 이 경우 메트릭 패널에서 사용할 수 있는 필터 기능을 사용합니다.

6.7 릴리스의 구현 제한 사항

- 모든 디바이스 및 모든 메트릭에 대한 Prometheus 스크랩 간격은 1분으로 고정됩니다.
- FMC(/var/opt/prometheus/devicehm.yml)에서 Prometheus yaml 파일을 수정하여 Prometheus 스크랩 간격을 변경할 수 있습니다.
- FTD API 출력은 JSON 형식입니다.
- FMC 모니터링은 지원되지 않습니다. FTD만 지원됩니다.
- FMC 상태 정책에서 CPU 사용률 메트릭은 기본적으로 비활성화되어 있습니다. 연결된 상태 정책을 수정하여 활성화할 수 있습니다.

문제가 있을 경우 전송할 내용

제출하려는 로그 요약:

- UI 스크린샷
- Prometeus 및 hmdaemon 로그(문제 해결/진단 섹션 참조).
- Prometheus 데이터베이스 덤프(/var/opt/Prometheus/data directory)

FAQ(자주 묻는 질문)

Q: FMC만 해당합니까? CDO로 이동한 사용자의 FTD/FDM은 어떻습니까?

A: 이 UI는 FMC 전용이며 새 UI는 6.7의 FTD 디바이스에만 적용됩니다.

Q: Custom Dashboards(맞춤형 대시보드)는 6.7의 디바이스에만 적용됩니까?

A: 대시보드는 6.7의 FTD 디바이스에만 해당됩니다.

Q: 이 기능에 디바이스별로 특화된 항목이 있습니까? 이 모든 기능이 포함된 FTD를 지원하는 ANY 플랫폼을 위한 것인가요? 가상 플랫폼이 지원됩니까?

A: 가상 FTDv에서도 지원됩니다. 가져온 메트릭에 장치별 변형이 있을 수 있지만 이 기능은 모든 FTD 플랫폼에서 지원됩니다.

Q: 개방형 API를 통해 CDO 팀과 활발히 협력할 수 있습니까?

A: "오픈 API"는 REST API를 의미한다고 생각합니다. FMC REST API는 FTD Device REST API와 *다릅니다. FMC로 관리하는 경우 FTD 디바이스 REST API를 사용할 수 없습니다. FMC의 일부 기능에는 FMC REST API가 없습니다.

A: 인프라는 FTD Device REST API를 위해 마련되었으며 향후 릴리스를 준비합니다.

Q: Health Monitor 페이지의 시간 창 옆에 있는 다운로드 버튼("+" 근처)에서 해당 창에 표시된 상태 보고서 또는 그래프를 다운로드합니까? 아니면 위젯이었나요?

A: 구축 오버레이 아이콘과 관련하여 아이콘 오버레이 구축 작업을 클릭하여 선택한 그래프에서 시간을 트리거합니다.

내부 추적 정보

CSC.content-security > sfims > ftd-plug-telemetry, fmc_hm

- ftd-plug-telemetry를 사용하여 FTD API 및 텔레그래프와 관련된 결함을 기록합니다.
- fmc_hm을 사용하여 FMC UI 및 FMC 백엔드 문제 기록
- FTD REST API => CSC.content-security > sfims > ftd-api-telemetry
- EDCS 18385961

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.