상태

다음 항목에서는 Firepower System에서 상태 모니터링을 사용하는 방법에 대해 설명합니다.

상태 모니터링 요구 사항 및 사전 요건

모델 지원

Any(모든)

지원되는 도메인

모든

사용자 역할

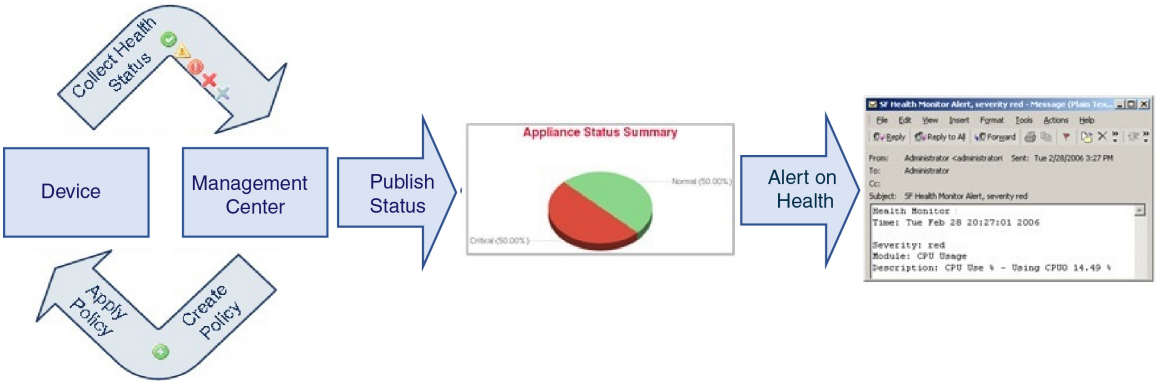
관리자

유지 보수 사용자

상태 모니터링 정보

management center에서 상태 모니터는 다양한 상태 표시기를 추적하고 시스템의 하드웨어 및 소프트웨어가 올바르게 작동하는지 확인합니다. 상태 모니터를 사용하여 구축에서 중요한 기능의 상태를 확인할 수 있습니다.

알림을 위해 상태 모듈을 실행하는 빈도를 구성할 수 있습니다. Management Center는 시계열 데이터 수집도 지원합니다. 디바이스와 디바이스 상태 모듈에서 시계열 데이터를 수집하는 빈도를 구성할 수 있습니다. 디바이스 모니터는 기본적으로 여러 미리 정의된 상태 모니터 대시보드에서 이러한 메트릭을 보고합니다. 메트릭 데이터는 분석을 위해 수집되므로 경고가 연결되지 않습니다.



상태 모니터를 사용하여 *health policy(*상태 정책*)*라고 하는 테스트 집합을 생성하고 하나 이상의 어플라이언스에 상태 정책을 적용할 수 있습니다. *health modules(*상태 모듈*)*라고도 하는 테스트는 지정한 기준을 테스트하는 스크립트입니다. 테스트를 활성화 또는 비활성화하거나 테스트 설정을 변경하여 상태 정책을 수정할 수 있으며, 더 이상 필요하지 않은 상태 정책을 삭제할 수 있습니다. 선택한 어플라이언스를 제외하여 해당 메시지를 억제할 수도 있습니다.

상태 정책의 테스트는 구성한 간격으로 자동 실행됩니다. 필요에 따라 모든 테스트 또는 특정 테스트를 실행할 수 있습니다. 상태 모니터는 구성한 테스트 조건을 기반으로 상태 이벤트를 수집합니다.

참고 모든 어플라이언스는 하드웨어 알람 상태 모듈을 통해 하드웨어 상태를 자동으로 보고합니다. management center도 기본 상태 정책에 구성된 모듈을 사용하여 상태를 자동으로 보고합니다. Appliance Heartbeat 모듈과 같은 일부 상태 모듈은 management center에서 실행되어 management center의 매니지드 디바이스의 상태를 보고합니다. 상태 모듈에서 매니지드 디바이스 상태를 제공하려면 모든 상태 정책을 디바이스에 구축해야 합니다.

상태 모니터를 사용하여 전체 시스템, 특정 어플라이언스 또는 다중 도메인 구축에서 특정 도메인의 상태 정보에 액세스할 수 있습니다. Health Monitor(상태 모니터) 페이지의 육각 차트 및 상태 테이블은 management center를 포함해 네트워크의 모든 어플라이언스 상태를 시각적으로 요약하여 보여줍니다. 개별 어플라이언스 상태 모니터에서는 특정 어플라이언스의 상태로 드릴다운할 수 있습니다.

완전히 사용자 지정 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 이러한 이벤트 보기에서는 이벤트 데이터를 검색하고 볼 수 있으며, 조사 중인 이벤트와 관련이 있을 수 있는 다른 정보에 액세스할 수 있습니다. 예를 들어 CPU 사용량이 특정 비율에 도달한 모든 경우를 보려면 CPU 사용량 모듈을 검색하고 비율 값을 입력합니다.

상태 이벤트에 대한 응답으로 이메일, SNMP 또는 syslog 알림을 구성할 수도 있습니다. *health alert(*상태 알림*)*는 표준 알림과 상태 레벨을 연결한 것입니다. 예를 들어, 하드웨어 과부하 때문에 어플라이언스가 실패하지 않도록 하려면 이메일 알림을 설정할 수 있습니다. 그런 다음 CPU, 디스크 또는 메모리 사용량이 어플라이언스에 적용된 상태 정책에서 구성한 경고(Warning) 레벨에 도달할 때마다

이메일 알림을 트리거하는 상태 알림을 생성할 수 있습니다. 반복해서 알림을 수신하는 횟수를 최소화하려면 알림 임계값을 설정할 수 있습니다.

참고 상태 모니터링은 상태 이벤트 발생 후 상태 알림을 생성하는 데 5~6분 정도 걸릴 수 있습니다.

또한 고객 지원에서 요청할 경우 어플라이언스에 대한 문제 해결 파일을 생성할 수도 있습니다.

상태 모니터링은 관리 활동이므로 관리자 사용자 역할 권한이 있는 사용자만 시스템 상태 데이터에 액세스할 수 있습니다.

상태 모듈

*Health modules(*상태 모듈*)* 또는 *health tests(*상태 테스트*)*는 상태 정책에서 지정한 기준을 테스트합니다.

표 ***1:*** 상태 모듈*(*모든 어플라이언스*)*

모듈	설명
CPU 사용량(코어당)	이 모듈은 모든 코어의 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
디스크 상태	이 모듈은 하드 디스크의 성능과 어플라이언스의 악성코드 스토리지 팩(설치된 경우)을 점검합니다. 이 모듈에서는 하드 디스크와 RAID 컨트롤러(설치된 경우)가 실패할 위험이 있을 때 또는 악성코드 스토리지 팩이 아닌 추가 하드 드라이브가 설치된 경우 Warning(노란색) 상태 알림을 생성합니다. 설치된 악성코드 스토리지 팩을 탐지할 수 없는 경우에는 Alert(빨간색) 상태 알림이 생성됩니다.
디스크 사용	이 모듈은 어플라이언스 하드 드라이브 및 악성코드 스토리지 팩의 디스크 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 또한 시스템이 모니터링되는 디스크 사용량 카테고리에서 과도하게 파일을 삭제하는 경우 또는 모듈 임계값을 기반으로 그러한 카테고리 외의 디스크 사용량이 과도한 수준에 도달하는 경우에도 알림을 전송합니다. 디스크 사용량 상태 모듈을 사용 하 여 기기에서 /및/ 또는 볼륨 파티션의 디스크 사용량을 모니터링 하 고 배수 빈도를 추적 합니다. 디스크 사용 모듈은 /boot 파티션을 모니터링되는 파티션으로 나열하지만 파티션의 크기는 정적이므로 모듈은 부팅 파티션에서 경고를 보내지 않습니다. 주의 파티션/볼륨에 대한 관리되지 않는 디스크 사용량이 높음에 대한 알림이 상태 정책에 지정된 위험 또는 경고 임계값보다 낮더라도 시스템에서 수동으로 삭제해야 하는 파일이 있음을 나타낼 수 있습니다. 이러한 알림을 받으면 TAC에 문의하십시오.

모듈	설명
파일 시스템 무결성 확인	이 모듈은 시스템에서 CC 모드 또는 UCAPL 모드가 활성화되어 있거나 시스템이 DEV 키로 서명된 이미지를 실행하는 경우 파일 시스템 무결성 검사를 수행하고 실행합니다. 이 모듈은 기본적으로 활성화되어 있습니다.
상태 모니터 프로세스	이 모듈은 상태 모니터 자체의 상태를 모니터링하고, management center에서 마지막으로 상태 이벤트를 수신한 후 시간(분 단위)이 Warning(경고) 또는 Critical(심각) 한도를 초과하면 알림을 전송합니다.
상태 모니터 프로세스	이 모듈은 상태 모니터 자체의 상태를 모니터링하고, management center에서 마지막으로 상태 이벤트를 수신한 후 시간(분 단위)이 Warning(경고) 또는 Critical(심각) 한도를 초과하면 알림을 전송합니다.
인터페이스 상태	이 모듈은 디바이스가 현재 트래픽을 수집하는지 확인하고, 물리적 인터페이스와 집계 인터페이스의 트래픽 상태를 기준으로 알림을 제공합니다. 물리적 인터페이스의 경우 정보에 인터페이스 이름, 링크 상태 및 대역폭이 포함됩니다. 집계 인터페이스의 경우 정보에 인터페이스 이름, 활성 링크의 수, 총 집계 대역폭이 포함됩니다. 참고 이 모듈은 HA 스탠바이 디바이스 트래픽 흐름도 모니터링합니다. 스탠바이 디바이스는 트래픽을 수신하지 않는 것으로 알려져 있지만, management center는 인터페이스에서 트래픽을 수신하고 있지 않음을 알립니다. 포트 채널의 일부 하위 인터페이스에서 트래픽을 수신하지 않는 경우에도 동일한 알림 원칙이 적용됩니다. **show interface** CLI 명령을 사용하여 디바이스의 인터페이스 통계를 확인하는 경우 CLI 명령 결과의 입력 및 출력 속도는 인터페이스 모듈에 표시되는 트래픽 속도와 다를 수 있습니다. 이 모듈은 Snort 성능 모니터링의 값에 따라 트래픽 속도를 표시합니다. Snort 성능 모니터링 및 management center 인터페이스 통계의 샘플링 간격은 서로 다릅니다. 샘플링 간격의 차이로 인해 management center GUI의 처리량 값은 threat defense CLI 결과에 표시되는 처리량 값과 다를 수 있습니다.
로컬 악성코드 분석	이 모듈은 로컬 악성코드 분석에 대한 ClamAV 업데이트를 모니터링합니다.

모듈	설명
메모리 사용	이 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 레벨을 초과하면 알림을 전송합니다. 메모리가 4GB를 넘는 어플라이언스의 경우 프리셋 알림 임계값은 시스템 문제를 일으킬 수 있는 사용 가능한 메모리의 비율을 고려하는 공식을 기반으로 합니다. 4GB를 넘는 어플라이언스에서는 Warning 임계값과 Critical 임계값 사이의 간격이 매우 좁기 때문에 Cisco에서는 **Warning Threshold %(**경고 임계값 **%)** 값을 50으로 수동으로 설정할 것을 권장합니다. 이렇게 하면 문제를 해결할 수 있도록 적시에 어플라이언스에 대한 메모리 알림을 받을 수 있습니다. 버전 6.6.0부터 management center virtual를 버전 6.6.0 이상으로 업그레이드하는 데 필요한 최소 RAM은 28GB이며, management center virtual 구축에 권장되는 RAM은 32GB입니다. 기본 설정을 줄이지 않는 것이 좋습니다. 대부분의 management center virtual 인스턴스의 경우 32GB RAM, management center virtual 300의 경우 64GB가 필요합니다(VMware만 해당). 주의 RAM이 부족하여 management center virtual 구축에 할당되면 상태 모니터에서 중요 알림이 생성됩니다. 복잡한 액세스 제어 정책 및 규칙을 적용할 경우 상당한 리소스가 소모되어 성능이 저하될 수 있습니다.
프로세스 상태	이 모듈은 어플라이언스의 프로세스가 프로세스 관리자 외부에서 종료되는지를 확인합니다. 프로세스가 프로세스 관리자 외부에서 고의로 종료되면 모듈 상태가 Warning으로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다. 프로세스가 프로세스 관리자 외부에서 비정상적으로 종료되거나 충돌되면 모듈 상태가 Critical로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다.

모듈	설명
디바이스에서 위협 데이터 업데이트	디바이스가 위협을 탐지하는 데 사용하는 특정 인텔리전스 데이터 및 구성은 30분마다 클라우드의 management center에서 업데이트됩니다. 이 모듈은 사용자가 지정한 기간 내에 해당 정보가 디바이스에 업데이트 되지 않은 경우 경고를 보냅니다. 모니터링되는 업데이트는 다음을 포함합니다. • 로컬 URL 카테고리 및 평판 데이터 • 보안 인텔리전스 URL 목록 및 피드. Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 URL이 포함됩니다. • 보안 인텔리전스 네트워크 목록 및 피드(IP 주소). Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 IP 주소가 포함됩니다. • 보안 인텔리전스 DNS 목록 및 피드. Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 도메인이 포함됩니다. • 에서 로컬 악성코드 분석 서명(ClamAV) • Threat Intelligence Director의 SHA 목록. **Objects(**개체**) > Object Management(**개체 관리**) > Security Intelligence(**보안 인텔리전스**) > Network Lists and Feeds(**네트워크 목록 및 피드**)** 페이지에 나와 있습니다. • 동적 분석 설정. **Integration(**통합**) > AMP > Dynamic Analysis Connections(**동적 분석 연결**)** 페이지에 구성되어 있습니다. • 캐시된 URL 만료와 관련한 Threat Configuration 설정. **System(**시스템**) > Integration(**통합**) >** 클라우드 서비스페이지의 Cached URLs Expire 설정을 포함합니다. (URL 캐시에 대한 업데이트는 이 모듈에서 모니터링하지 않습니다.) • 이벤트 전송에서의 Cisco Cloud와의 통신 이슈 **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)** 페이지의 **Cisco Cloud** 상자를 참조하십시오. 참고 Threat Intelligence Director 업데이트는 TID가 시스템에 구성되어 있고 피드가 있는 경우에만 포함됩니다. 기본적으로 이 모듈은 1시간 후에 warning(경고) 알림을 보내고 24시간 후에 critical(심각) 알림을 보냅니다. 이 모듈에서 management center 또는 어떠한 디바이스에 실패가 표시되는 경우, management center가 디바이스에 연결되는지 확인합니다.

표 *2: Management Center* 상태 모듈

모듈	설명
AMP for Endpoints 상태	이 모듈은 management center가 초기 연결에 성공한 후 AMP 클라우드 또는 Cisco AMP 프라이빗 클라우드에 연결할 수 없거나 프라이빗 클라우드가 공용 AMP 클라우드에 연결할 수 없는 경우에 경고를 보냅니다. 또한 Secure Endpoint 관리 콘솔을 사용하여 AMP 클라우드 연결을 등록 취소하면 경고를 보냅니다.
Firepower용 AMP 상태	이 모듈은 다음의 경우에 경고를 보냅니다. • management center은 AMP 클라우드(퍼블릭 또는 프라이빗) 또는 Secure Malware Analytics 클라우드 또는 어플라이언스에 연결할 수 없으며 또는 AMP 프라이빗 클라우드는 퍼블릭 AMP 클라우드에 연결할 수 없습니다. • 연결에 사용되는 암호화 키가 유효하지 않습니다. • 디바이스는 Secure Malware Analytics 클라우드 또는 Secure Malware Analytics 어플라이언스에 연결하여 동적 분석을 위한 파일을 제출할 수 없습니다. • 파일 정책 구성을 기반으로 네트워크 트래픽에서 과도한 수의 파일이 검색됩니다. management center에서 인터넷 연결이 끊어지는 경우, 시스템이 상태 알림을 생성하는 데 최대 30분이 걸릴 수 있습니다.
어플라이언스 하트비트	이 모듈은 어플라이언스에서 어플라이언스 하트비트가 전송되는지 확인하고, 어플라이언스 하트비트 상태를 기반으로 알림을 전송합니다.
데이터베이스 크기	이 모듈은 구성 데이터베이스 크기를 확인하고, 크기가 모듈에 대해 구성된 값(기가바이트)을 초과하면 알림을 보냅니다.
검색 호스트 한도	이 모듈은 management center가 모니터할 수있는 호스트의 수가 한계에 가까워지고 모듈에 구성된 경고 수준에 따라 경고를 할지 결정합니다. 자세한 내용은 Firepower System 호스트 제한의 내용을 참고하십시오.
이벤트 백로그 상태	이 모듈은 디바이스에서 management center로의 전송을 기다리는 이벤트 데이터의 백로그가 30분 이상 지속적으로 증가한 경우 알림을 표시합니다. 백로그를 줄이려면 대역폭을 평가하고 이벤트 기록을 줄이는 것이 좋습니다.
이벤트 모니터	이 모듈은 management center에 대한 전체 수신 이벤트 비율을 모니터링합니다.
이벤트 스트림 상태	이 모듈은 management center에서 Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을 모니터링합니다.
ISE 연결 모니터	이 모듈은 Cisco ISE(Identity Services Engine)와 management center간의 서버 연결 상태를 모니터링 합니다. ISE는 추가 사용자 데이터, 디바이스 유형 데이터, 디바이스 위치 데이터, SGT(Security Group Tags) 및 SXP(Security Exchange Protocol) 서비스를 제공합니다.
라이선스 모니터	이 모듈은 라이선스 만료를 모니터링합니다.

모듈	설명
Management Center 액세스 구성 변경	이 모듈은 **configure network management-data-interface** 명령을 사용하여 management center에서 직접 수행한 액세스 구성 변경을 모니터링합니다.
Management Center HA 상태	이 모듈은 management center의 고가용성 상태를 모니터링하고 경고합니다. management center 고가용성이 설정되지 않은 경우, HA 상태는 `Not in HA(HA가 아님)` 입니다. 참고 이 모듈은 이전에 management center의 HA 상태를 제공했던 HA 상태 모듈을 대체합니다. 버전 7.0에서는 매니지드 디바이스에 대한 HA 상태를 추가했습니다.
MySQL 통계	이 모듈은 데이터베이스 크기, 활성 연결 수 및 메모리 사용을 포함하여 MySQL 데이터베이스의 상태를 모니터링합니다. 기본적으로 비활성화되어 있습니다.
전력 공급 장치	이 모듈은 어플라이언스의 전력 공급 장치를 교체해야 하는지 여부를 확인하고, 전력 공급 장치 상태를 기반으로 알림을 전송합니다.
RabbitMQ 상태	이 모듈은 RabbitMQ에 대한 다양한 통계를 수집합니다.
RRD 서버 프로세스	이 모듈은 시계열 데이터를 저장하는 라운드 로빈 데이터 서버가 제대로 실행되고 있는지 확인합니다. 마지막으로 업데이트된 이후 RRD 서버가 다시 시작되면 알림이 전송됩니다. RRD 서버 다시 시작의 연속 업데이트 수가 모듈 컨피그레이션에 지정된 수에 도달하면 Critical 또는 Warning 상태로 들어가게 됩니다.
보안 인텔리전스	이 모듈은 보안 인텔리전스를 사용 중이고 management center가 피드를 업데이트할 수 없거나 피드 데이터가 손상되었거나 인식할 수 없는 IP 주소를 포함하는 경우 알림을 표시합니다. 디바이스의 위협 데이터 업데이트 모듈도 참조하십시오.
스마트 라이선스 모니터	이 모듈은 스마트 라이선싱 상태를 모니터링합니다.
스마트 라이선스 모니터	이 모듈은 다음의 경우에 경고를 보냅니다. • 스마트 라이선싱 에이전트(Smart Agent)와 스마트 소프트웨어 매니저 간에 통신 오류가 있습니다. • 제품 인스턴스 등록 토큰이 만료되었습니다. • 스마트 라이선스 사용량이 미준수 상태입니다. • 스마트 라이선스 권한 부여 또는 평가 모드 만료 되었습니다.
Sybase 통계	이 모듈은 데이터베이스 크기, 활성 연결 수 및 메모리 사용을 포함하여 management center에서 Sybase 데이터베이스의 상태를 모니터링합니다.
시계열 데이터(RRD) 모니터링	이 모듈은 시계열 데이터(예: 상관관계 이벤트 카운트)가 저장된 디렉토리에 손상된 파일이 있는지를 추적하고, 손상되어 제거된 것으로 파일에 플래그가 표시되는 경우 알림을 전송합니다.

모듈	설명
동기화 상태	이 모듈은 NTP를 사용하여 시간을 가져오는 디바이스 시계와 NTP 서버에 있는 시계의 동기화를 추적하고, 두 시계 간 차이가 10초를 넘으면 알림을 전송합니다.
확인할 수 없는 그룹 모니터	정책에 사용된 확인되지 않은 그룹을 모니터링합니다.
URL 필터링 모니터	management center가 다음에 실패하는 경우 이 모듈이 경고를 보냅니다. • Cisco Cloud에 등록 • Cisco Cloud에서 URL 위협 데이터 업데이트 다운로드 • 완전한 URL 조회 이러한 경고에 대해 시간 임계값을 구성할 수 있습니다. 디바이스의 위협 데이터 업데이트 모듈도 참조하십시오.
VPN 통계	이 모듈은 Firepower 디바이스 간의 사이트 대 사이트 및 RA VPN 터널을 모니터링합니다.
VPN 상태	이 모듈은 Firepower 디바이스 간에 하나 이상의 VPN 터널이 다운되면 알림을 보냅니다. 이 모듈을 다음을 추적합니다. • Site-to-Site VPN Secure Firewall Threat Defense • 원격 액세스 VPN Secure Firewall Threat Defense

표 ***3:*** 디바이스 상태 모듈

모듈	설명
AMP 연결 상태	이 모듈은 threat defense가 초기 연결에 성공한 후 AMP 클라우드 또는 Cisco AMP 프라이빗 클라우드에 연결할 수 없거나 프라이빗 클라우드가 공용 AMP 클라우드에 연결할 수 없는 경우에 경고를 보냅니다. 기본적으로 비활성화되어 있습니다.
AMP Threat Grid 연결성	모듈은 초기 연결에 성공한 후 threat defense이 AMP Threat Grid 클라우드에 연결할 수 없는 경우 경고를 표시합니다.
ASP 삭제	이 모듈은 데이터 플레인 가속화된 보안 경로에 의해 삭제된 연결을 모니터링합니다.
AAB(Automatic Application Bypass)	이 모듈은 우회된 탐지 애플리케이션을 모니터링합니다.

모듈	설명
클러스터/HA 페일오버 상태	이 모듈은 디바이스 클러스터의 상태를 모니터링합니다. 이 모듈은 다음의 경우 경고를 보냅니다. • 새 기본 유닛이 클러스터에 선택됩니다. • 새 보조 유닛에서 클러스터에 가입합니다. • 기본 또는 보조 유닛이 클러스터를 떠납니다.
설정 리소스 사용률	이 모듈은 구축된 구성의 크기로 인해 디바이스에서 메모리가 부족해질 위험이 있는지를 알려줍니다. 알림에는 구성에 필요한 메모리의 양과 사용 가능한 메모리를 초과하는 양이 표시됩니다. 이 경우 구성을 재평가하십시오. 종종 액세스 제어 규칙 또는 침입 정책의 수 또는 복잡성을 줄일 수 있습니다. **Snort** 메모리 할당 • *Total Snort Memory(*총 *Snort* 메모리*)*는 threat defense 디바이스에서 실행 중인 Snort 2 인스턴스에 할당된 메모리를 나타냅니다. • *Available Memory(*사용 가능한 메모리*)*는 시스템에서 Snort 2 인스턴스에 할당한 메모리를 나타냅니다. 이 값은 총 *Snort* 메모리와 다른 모듈용으로 예약된 통합 메모리 간의 차이가 아닙니다. 이 값은 몇 가지 다른 계산 후에 파생된 다음 Snort 2 프로세스의 수로 나뉩니다. *Available Memory(*사용 가능한 메모리*)* 값이 음수이면 Snort 2 인스턴스에 구축된 구성에 대한 메모리가 충분하지 않음을 나타냅니다. 지원은 Cisco Technical Assistance Center (TAC)에 문의하십시오.
연결 통계	이 모듈은 연결 통계 및 NAT 변환 수를 모니터링합니다.
CPU 사용 데이터 플레인	이 모듈은 디바이스에 있는 모든 데이터 플레인의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용량 Snort	이 모듈은 디바이스에 있는 Snort 프로세스의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용량 시스템	이 모듈은 디바이스에 있는 모든 시스템의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
중요한 프로세스 통계	이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다.

모듈	설명
구축된 컨피그레이션 통계	이 모듈은 구축된 설정에 대한 통계(예: ACE 수 및 IPS 규칙)를 모니터링합니다.
Firepower Platform 결함	이 모듈은 Firepower 1000, 2100 및 3000 Series 디바이스의 플랫폼 결함에 대한 알림을 생성합니다. 결함은 management center에서 관리하는 변경 가능한 개체입니다. 각 결함은 Firepower 1000, 2100 및 3000 인스턴스의 장애 또는 경고 임계값 증가를 나타냅니다. 결함의 라이프사이클 중에 상태 또는 심각도가 서로 변경될 수 있습니다. 각 결함에는 결함이 제기된 시점에 영향을 받은 개체의 운영 상태에 대한 정보가 포함됩니다. 결함이 과도적이고 실패가 해결될 경우, 개체가 기능적 상태로 전환됩니다. 자세한 내용은*Cisco Firepower 1000 /2100 FXOS* 결함 및 오류 메시지 가이드를 참조하십시오.
플로우 오프로드 통계	이 모듈은 관리되는 디바이스에 대한 하드웨어 플로우 오프로드 통계를 모니터링합니다.
하드웨어 경보	이 모듈은 하드웨어의 교체가 필요한지 여부를 판단하고, 하드웨어 상태를 기반으로 알림을 전송합니다. 이 모듈은 하드웨어 관련 데몬의 상태도 보고합니다.
인라인 링크 불일치 경보	이 모듈은 인라인 집합과 관련된 포트를 모니터링하고, 인라인 쌍의 두 인터페이스가 서로 다른 속도를 협상하는 경우 알림을 전송합니다.
침입 및 파일 이벤트 비율	이 모듈은 초당 침입 이벤트 수를 모듈에 대해 구성된 제한과 비교하고, 제한을 초과하는 경우 알림을 전송합니다. 침입 및 파일 이벤트 비율이 0이면 침입 프로세스가 다운되거나 매니지드 디바이스가 이벤트를 전송하지 못할 수 있습니다. **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을 선택하고 이벤트가 디바이스에서 수신되는지 확인합니다. 일반적으로 네트워크 세그먼트의 이벤트 속도는 초당 이벤트 20개입니다. 이 평균 속도의 네트워크 세그먼트에서 Events per second(Critical)는 `50`, Events per second (Warning)는 `30`으로 설정해야 합니다. 시스템에 대한 제한을 확인하려면 디바이스의 Statistics(통계) 페이지에서 Events/Sec 값을 찾고(시스템 (⚙) > **Monitoring(**모니터링**)** > **Statistics(**통계**)**), 다음 공식을 사용하여 제한을 계산합니다. • Events per second (Critical) = Events/Sec * 2.5 • Events per second (Warning) = Events/Sec * 1.5 두 가지 제한 중 하나에 대해 설정할 수 있는 최대 이벤트 수는 999이며, Critical 제한이 Warning 제한보다 높아야 합니다.
링크 상태 전파	ISA 3000에만 해당. 페어링된 인라인 집합의 링크가 실패하는 경우를 확인하고 링크 상태 전파 모드를 트리거합니다. 링크 상태가 쌍으로 전파되면 해당 모듈에 대한 상태 분류가 Critical로 변경되고 다음과 같은 메시지가 나타납니다. `Module Link State Propagation: ethx_ethy is Triggered` 여기서 `x`및 `y`는 쌍을 이룬 인터페이스 번호입니다.

모듈	설명
메모리 사용량 데이터 플레인	이 모듈은 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 확인하고 메모리 사용량이 모듈에 대해 설정된 백분율을 초과할 때 경고를 표시합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
메모리 사용량 Snort	이 모듈은 Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 확인하고 메모리 사용량이 모듈에 대해 설정된 백분율을 초과할 때 경고를 표시합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
네트워크 카드 재설정	이 모듈은 하드웨어 장애 때문에 다시 시작된 네트워크 카드를 확인하고, 재설정이 발생하면 알림을 전송합니다.
NTP 통계	이 모듈은 매니지드 디바이스의 NTP 클럭 동기화 상태를 모니터링합니다. 기본적으로 비활성화되어 있습니다.
영역	영역 또는 사용자 불일치에 대한 경고 임계값을 설정할 수 있습니다. • 사용자 불일치: 사용자가 다운로드되지 않고 management center에 보고됩니다. 사용자 불일치가 발생하는 일반적인 이유는 사용자가 management center 다운로드에서 제외된 그룹에 속하기 때문입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 논의된 정보를 검토합니다. • 영역 불일치: 사용자가 management center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다. 자세한 내용은Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오. 이 모듈은 또한 영역당 지원되는 다운로드된 사용자의 최대 수보다 많은 사용자를 다운로드하려고 할 때 상태 알림을 표시합니다. 단일 영역에 대해 다운로드되는 최대 사용자 수는 관리 센터 모델에 따라 다릅니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 제한을 참조하십시오.
라우팅 통계	이 모듈은 라우팅 테이블의 현재 상태를 모니터링합니다.
Snort3 통계	이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort3 통계를 수집하고 모니터링합니다.

모듈	설명
Snort ID 메모리 사용량	메모리 사용량이 모듈에 대해 설정된 레벨을 초과할 때 Snort ID 처리 및 알림에 대한 경고 임계값을 설정할 수 있습니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 `80`입니다. 이 상태 모듈은 Snort에서 사용자 ID 정보에 사용된 총 공간을 추적합니다. 여기에는 현재 메모리 사용량 세부 정보, 총 사용자-IP 바인딩 수 및 사용자-그룹 매핑 세부 정보가 표시됩니다. Snort는 이러한 세부 정보를 파일에 기록합니다. 메모리 사용량 파일을 사용할 수 없는 경우 이 모듈에 대한 Health Alert(상태 알림)에 *Waiting for data(*데이터 대기 중*)*가 표시됩니다. 이는 신규 설치 또는 주요 업데이트, Snort2에서 Snort3 또는 그 반대로의 전환 또는 주요 정책 구축으로 인해 Snort 재시작 중에 발생할 수 있습니다. 상태 모니터링 주기에 따라 그리고 파일을 사용할 수 있는 경우 경고가 사라지고 상태 모니터에 이 모듈의 상세정보가 녹색으로 표시됩니다.
Snort 재구성 탐지	이 모듈은 디바이스 재구성이 실패한 경우 경고를 보냅니다.
Snort 통계	이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다.
SSE 연결 상태	모듈은 초기 연결에 성공한 후 threat defense이 SSE 클라우드에 연결할 수 없는 경우 경고를 표시합니다. 기본적으로 비활성화되어 있습니다.
Threat Defense HA(스플릿 브레인 검사)	이 모듈은 threat defense의 고가용성 상태를 모니터링하고 경고하며 분할 브레인 시나리오에 대한 상태 경고를 제공합니다. threat defense 고가용성이 설정되지 않은 경우, HA 상태는 `Not in HA(HA가 아님)` 입니다.
XTLS 카운터	이 모듈은 XTLS/SSL 플로우, 메모리 및 캐시 효율성을 모니터링합니다. 기본적으로 비활성화되어 있습니다.

상태 모니터링 구성

프로시저

단계 **1** 상태 모듈, 3 페이지에 설명된 대로 모니터링 하려는 상태 모듈을 결정합니다.

Firepower System에 있는 각 어플라이언스 종류에 대해 특정 정책을 설정하고 해당 어플라이언스에 맞는 테스트만 활성화할 수 있습니다.

팁 모니터링 동작을 사용자 지정하지 않고 빠르게 상태 모니터링을 활성화하려면 이 용도로 제공되는 기본 정책을 적용할 수 있습니다.

단계 **2** 상태 정책 생성, 14 페이지에 설명된 대로 상태를 추적하려는 각 어플라이언스에 상태 정책을 적용합니다.

단계 **3** (선택 사항). 상태 모니터 알림 생성, 21 페이지에 설명된 대로 상태 모니터 알림을 구성합니다.

상태 레벨이 특정 상태 모듈에 대해 특정 심각도에 도달할 때 트리거되는 이메일, syslog 또는 SNMP 알림을 설정할 수 있습니다.

상태 정책

상태 정책에는 여러 모듈용으로 구성된 상태 테스트 기준이 포함되어 있습니다. 각 어플라이언스에 대해 어떤 상태 모듈을 실행할지 제어할 수 있으며, 각 모듈에 의해 실행되는 테스트에서 사용할 특정 제한을 구성할 수 있습니다.

상태 정책을 구성할 때에는 해당 정책에 대해 각 상태 모듈을 활성화할지 여부를 결정합니다. 또한 각 사용 가능 모듈에서 프로세스의 상태를 평가 하는 때마다 보고할 상태를 제어 하는 조건을 선택합니다.

시스템의 모든 어플라이언스에 적용할 수 있는 하나의 상태 정책을 생성하거나, 특정 어플라이언스에 적용하고자 하는 각 상태 정책을 사용자 지정하거나, 제공되는 기본 상태 정책을 사용할 수 있습니다. 다중 도메인 구축에서, 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

기본 상태 정책

management center설정 프로세스에서는 초기 상태 정책을 생성하고 적용하며, 모든 상태 모듈이 아닌 대부분의 사용 가능한 상태 모듈이 활성화됩니다. 시스템은 management center에 추가된 디바이스에도 이 초기 정책을 적용합니다.

이 초기 상태 정책은 기본 상태 정책을 기반으로 합니다. 이 정책은 보거나 편집할 수 없지만 맞춤형 상태 정책을 생성할 때 복사할 수 있습니다.

업그레이드 및 기본 상태 정책

management center을 업그레이드할 때 모든 새 상태 모듈이 초기 상태 정책, 기본 상태 정책 및 기타 사용자 지정 상태 정책을 포함하여 모든 상태 정책에 추가됩니다. 일반적으로 새 상태 모듈은 활성화된 상태로 추가됩니다.

참고 새 상태 모듈에서 모니터링 및 알림을 시작하려면 업그레이드 후 상태 정책을 다시 적용합니다.

상태 정책 생성

어플라이언스와 함께 사용할 상태 정책을 사용자 지정하려면 새 정책을 생성할 수 있습니다. 초기에는 정책의 설정이 새 정책의 기반으로 선택한 상태 정책에서 오는 설정으로 채워집니다. 정책을 수정하여 정책 내에서 모듈 활성화 또는 비활성화와 같은 환경 설정을 지정하고, 필요에 따라 각 모듈에 대한 알림 기준을 변경하고, 실행 시간 간격을 지정할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** 정책의 이름을 입력합니다.

단계 **4** 새 정책의 기본으로 사용할 기존 정책을 **Base Policy(**기본 정책**)** 드롭다운 목록에서 선택합니다.

단계 **5** 이 정책에 대한 설명을 입력합니다.

단계 **6** **Save(**저장**)**를 선택합니다.

다음에 수행할 작업

- 상태 정책 적용, 15 페이지에 설명된 대로 디바이스에 상태 정책을 적용합니다.
- 상태 정책 수정, 16 페이지에 설명된 대로 정책을 편집하여 모듈 레벨 정책 설정을 지정합니다.

상태 정책 적용

어플라이언스에 상태 정책을 적용하면, 정책에서 활성화한 모든 모듈에 대한 상태 테스트가 어플라이언스의 프로세스 및 하드웨어의 상태를 모니터링합니다. 상태 테스트는 정책에 구성된 간격으로 계속 실행되면서 어플라이언스에 대한 상태 데이터를 수집한 다음 management center로 전달합니다.

상태 정책에서 모듈을 활성화한 다음 상태 테스트가 필요하지 않은 어플라이언스에 정책을 적용하면, 상태 모니터는 해당 상태 모듈의 상태를 비활성으로 보고합니다.

모든 모듈이 비활성화된 정책을 어플라이언스에 적용하면, 적용된 모든 상태 정책이 어플라이언스에서 제거됩니다.

정책이 이미 적용된 어플라이언스에 다른 정책을 적용하면, 새로 적용된 테스트를 기반으로 새 데이터의 표시에 약간의 레이턴시가 발생합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** 적용하려는 정책 옆에 있는 상태 정책 구축( )를 클릭합니다.

단계 **3** 상태 정책을 적용할 어플라이언스를 선택합니다.

참고 구축한 후에는 어플라이언스에서 정책을 제거할 수 없습니다. 어플라이언스에 대한 상태 모니터링을 중지하려면 모든 모듈이 비활성화된 상태 정책을 생성하여 어플라이언스에 적용합니다.

단계 **4** **Apply(**적용**)**를 클릭하고 선택한 어플라이언스에 정책을 적용합니다.

다음에 수행할 작업

- 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기를 참조하십시오.

정책이 성공적으로 적용됨과 동시에 어플라이언스의 모니터링이 시작됩니다.

상태 정책 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** 수정하려는 NAT 정책 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 정책 이름 및 설명을 편집하려면 정책 이름 옆에 있는 **Edit(**수정**)** ( ) 아이콘을 클릭합니다.

단계 **4** **Health Modules(**상태 모듈**)** 탭에는 모든 디바이스 모듈 및 해당 속성이 표시됩니다. 모듈 및 해당 속성에 대해 제공되는 토글 버튼을 클릭합니다. 켜거나 ( ) 끄면 ( ) 각각 상태 테스트를 활성화하거나 비활성화합니다. 상태 모듈에서 대량 활성화 또는 비활성화 테스트를 실행하려면 **Select All(**모두 선택**)** 토글 버튼을 클릭합니다. 모듈에 대한 자세한 내용은 상태 모듈, 3 페이지을(를) 참조하십시오.

참고
- 모듈 및 속성은 지원 어플라이언스(threat defense, management center 또는 둘 다)로 플래그가 지정됩니다.
- CPU 및 메모리 모듈의 개별 속성을 포함하거나 제외하도록 선택할 수 없습니다.

단계 **5** 해당되는 경우, **Critical(**심각**)**및 **Warning(**경고**)** 임계값 백분율을 설정합니다.

단계 **6** **Run Time Intervals(**실행 시간 간격**)** 탭에서 필드에 관련 값을 입력합니다.

- **Health Module Run Interval(**상태 모듈 실행 간격**)** - 상태 모듈을 실행할 빈도입니다. 최소 간격은 5분입니다.
- **Metric Collection Interval(**메트릭 수집 간격**)** - 디바이스 및 해당 상태 모듈에서 시계열 데이터를 수집하는 빈도입니다. 디바이스 모니터는 기본적으로 여러 미리 정의된 상태 모니터 대시보드에서 이러한 메트릭을 보고합니다. 대시보드에 대한 자세한 내용은 대시보드 정보의 내용을 참조하십시오. 메트릭 데이터는 분석을 위해 수집되므로 경고가 연결되지 않습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 상태 정책 적용, 15 페이지에 설명된 대로 각 어플라이언스에 상태 정책을 적용합니다. 이 옵션을 사용하면 변경 사항이 적용되고 영향을 받는 모든 정책에 대한 정책 상태를 업데이트할 수 있습니다.

상태 정책 삭제

더 이상 필요 없는 상태 정책을 삭제할 수 있습니다. 어플라이언스에 여전히 적용된 정책을 삭제하면, 다른 정책을 적용할 때까지 정책 설정이 그대로 유지됩니다. 또한 장치에 적용 되는 상태 정책을 삭제 하면 기본 연결 된 알림 응답을 비활성화할 때까지 장치에 적용 되는 모든 상태 모니터링 경고가 활성 상태로 유지 됩니다.

다중 도메인 구축에서는 현재 도메인에서 만든 상태 정책만 삭제할 수 있습니다.

팁 어플라이언스에 대한 상태 모니터링을 중지하려면 모든 모듈이 비활성화된 상태 정책을 생성하여 어플라이언스에 적용합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** 삭제할 정책 옆의 **Delete(**삭제**)** ( )을 클릭한 다음 **Delete health policy (**상태 정책 삭제**)**를 클릭하여 삭제합니다.
성공적으로 삭제했음을 알리는 메시지가 나타납니다.

상태 모니터링에서 디바이스 제외

일반적인 네트워크 유지 보수 과정에서 어플라이언스를 비활성화하거나 일시적으로 사용할 수 없도록 만들 수 있습니다. 이러한 중단은 고의적인 것이므로 해당 어플라이언스의 상태가 management center의 요약 상태에 영향을 미치지 않도록 할 수 있습니다.

어플라이언스나 모듈에 대한 상태 모니터링 상태 보고를 비활성화하려면 상태 모니터 제외 기능을 사용할 수 있습니다. 예를 들어, 네트워크의 한 세그먼트를 사용할 수 없게 될 것임을 알고 있는 경우 해당 세그먼트의 매니지드 디바이스에 대한 상태 모니터링을 일시적으로 비활성화할 수 있습니다. 그러면 디바이스에 대한 연결이 무효화되므로 management center의 상태가 Warning 또는 Critical 상태로 표시되지 않습니다.

상태 모니터링 상태를 비활성화하면 상태 이벤트는 여전히 생성되지만 비활성화된 상태를 갖게 되어 상태 모니터의 상태에 영향을 미치지 않습니다. 어플라이언스나 모듈을 제외 목록에서 제거하면 제외에 있는 동안 생성된 이벤트는 계속해서 비활성 상태를 표시합니다.

어플라이언스에서 일시적으로 상태 이벤트를 비활성화하려면 제외 구성 페이지로 이동하고 디바이스 제외 목록에 어플라이언스를 추가합니다. 설정이 적용되면 시스템은 전체적인 상태를 계산할 때 제외된 어플라이언스를 더 이상 고려하지 않습니다. Health Monitor Appliance Status Summary(상태 모니터 어플라이언스 상태 요약)에는 어플라이언스가 비활성 상태로 나열됩니다.

개별 상태 모듈을 비활성화할 수도 있습니다. 예를 들어 management center에서 호스트 제한에 도달하는 경우, 호스트 제한 상태 메시지를 비활성화할 수 있습니다.

기본 Health Monitor 페이지에서, 특정 상태 행의 화살표를 클릭하여 해당 상태의 어플라이언스 목록을 볼 수 있도록 확장하면 제외된 여러 어플라이언스를 구분할 수 있습니다.

참고 management center에서 Health Monitor 제외 설정은 로컬 구성 설정입니다. 따라서 디바이스를 제외한 다음, 삭제 후 management center에서 다시 등록하는 경우 제외 설정이 계속 유지됩니다. 새롭게 다시 등록한 디바이스는 계속 제외 상태를 유지합니다.

다중 도메인 구축에서 상위 도메인의 관리자는 하위 도메인의 어플라이언스 또는 상태 모듈을 제외할 수 있습니다. 그러나 하위 도메인의 관리자는 상위 구성을 무시하고 해당 도메인의 디바이스에 대한 제외를 지울 수 있습니다.

상태 모니터링에서 어플라이언스 제외

어플라이언스를 개별적으로 또는 그룹, 모델 또는 관련 상태 정책별로 제외할 수 있습니다.

개별 어플라이언스의 이벤트 및 상태를 비활성으로 설정하려면 어플라이언스를 제외할 수 있습니다. 제외 설정이 적용되면 어플라이언스가 Health Monitor Appliance Module Summary(상태 모니터 어플라이언스 모듈 요약)에서 Disabled(비활성)로 표시되고, 어플라이언스에 대한 상태 이벤트에 상태가 Disabled(비활성)로 표시됩니다.

다중 도메인 구축에서 상위 도메인의 어플라이언스를 제외하면 모든 하위 도메인에 대해 어플라이언스가 제외됩니다. 하위 도메인은 이 상속된 구성을 무시하고 제외를 지울 수 있습니다. 전역 수준에서 management center만 제외할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Exclude(**제외**)**을(를) 선택합니다.

단계 **2** **Add Device(**디바이스 추가**)**를 클릭합니다.

단계 **3** **Device Exclusion(**디바이스 제외**)**대화 상자의 **Available Devices(**사용 가능한 디바이스**)** 아래에서 상태 모니터링에서 제외할 디바이스의 **Add(**추가**)** ( )를 클릭합니다.

단계 **4** **Exclude(**제외**)**를 클릭합니다. 선택한 디바이스가 제외 기본 페이지에 표시됩니다.

단계 **5** 제외 목록에서 디바이스를 제거하려면 **Delete(**삭제**)** ( )를 클릭합니다.

단계 **6** **Apply(**적용**)**를 클릭합니다.

다음에 수행할 작업

어플라이언스에서 개별 상태 정책 모듈을 제외하려면 상태 정책 모듈 제외, 19 페이지의 내용을 참조하십시오.

상태 정책 모듈 제외

어플라이언스에서 개별 상태 정책 모듈을 제외할 수 있습니다. 모듈의 이벤트가 어플라이언스의 상태를 Warning(경고) 또는 Critical(심각)로 변경하지 못하게 하려면 이 기능을 사용할 수 있습니다.

제외 설정이 적용되면 어플라이언스는 상태 모니터링에서 디바이스에서 제외되는 모듈의 수를 표시합니다.

팁 개별적으로 제외한 모듈은 필요 시 다시 활성화할 수 있도록 계속 추적해야 합니다. 실수로 모듈을 비활성 상태로 남겨 두면 필요한 Warning(경고) 또는 Critical(심각) 메시지를 놓칠 수 있습니다.

다중 도메인 구축에서 상위 도메인의 관리자는 하위 도메인의 상태 모듈을 제외할 수 있습니다. 그러나 하위 도메인의 관리자는 이러한 상위 구성을 무시하고 해당 도메인의 디바이스에 대한 제외를 지울 수 있습니다. 전역 수준에서 management center 상태 모듈만 제외할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Exclude(**제외**)**를 선택합니다.

단계 **2** 수정하려는 어플라이언스 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에서는 기본적으로 디바이스의 모든 모듈이 상태 모니터링에서 제외됩니다. 특정 모듈은 특정 디바이스만 적용됩니다. 자세한 내용은 상태 모듈, 3 페이지을 참조 하십시오.

단계 **4** 디바이스의 제외 기간을 지정하려면 **Exclude Period(**제외 기간**)** 드롭다운 목록에서 기간을 선택합니다.

단계 **5** 상태 모니터링에서 제외할 모듈을 선택하려면 **Enable Module Level Exclusion(**모듈 레벨 제외 활성화**)** 링크를 클릭합니다. **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에 디바이스의 모든 모듈이 표시됩니다. 연결된 상태 정책에 적용할 수 없는 모듈은 기본적으로 비활성화되어 있습니다. 모듈을 제외하려면 다음을 수행합니다.

1. 원하는 모듈 옆에 있는 **Slider(**슬라이더**)**( ) 버튼을 클릭합니다.
2. 선택한 모듈의 제외 기간을 지정하려면 **Exclude Period(**제외 기간**)** 드롭다운 목록에서 기간을 선택합니다.

단계 **6** 제외 구성에 대해 **Permanent(**영구**)** 이외의 **Exclude Period(**제외 기간**)**를 선택하는 경우 구성이 만료될 때 자동으로 삭제하도록 선택할 수 있습니다. 이 설정을 활성화하려면 **Auto-delete expire Configurings(**만료된 구성 자동 삭제**)** 확인란을 선택합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** 디바이스 제외 기본 페이지에서 **Apply(**적용**)**를 클릭합니다.

만료된 상태 모니터 제외

디바이스 또는 모듈에 대한 제외 기간이 경과하면 제외를 지우거나 갱신할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Exclude(**제외**)**을(를) 선택합니다.

디바이스 또는 모듈이 알림에서 제외되는 기간의 만료를 나타내는 **Warning(**경고**)** ( ) 아이콘이 디바이스에 표시됩니다.

단계 **2** 디바이스의 제외를 갱신하려면 어플라이언스 옆에 있는 **Edit(**수정**)**( )을 클릭합니다. **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에서 **Renew(**갱신**)** 링크를 클릭합니다. 디바이스의 제외 기간이 현재 값으로 연장됩니다.

단계 **3** 디바이스를 제외에서 지우려면 어플라이언스 옆에 있는 **Delete(**삭제**)** ( )를 클릭하고 **Remove the device from exclusion(**제외에서 디바이스 제거**)**을 클릭한 다음 **Apply(**적용**)**를 클릭합니다.

단계 **4** 모듈을 갱신하거나 제외에서 지우려면 어플라이언스 옆에 있는 **Edit(**수정**)**( )을 클릭합니다. **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에서 **Enable Module Level Exclusion(**모듈 레벨 제외 활성화**)** 링크를 클릭한 다음 모듈에 대해 **Renew(**갱신**)** 또는 **Clear(**지우기**)** 링크를 클릭합니다. **Renew(**갱신**)**를 클릭하면 현재 값으로 모듈에서 제외 기간이 연장됩니다.

상태 모니터 알림

상태 정책에서 모듈에 대한 상태가 변경될 때 이메일, SNMP 또는 시스템 로그를 통해 알리도록 알림을 설정할 수 있습니다. 기존 알림 응답을 트리거할 상태 이벤트 레벨과 연결하고, 특별한 레벨의 상태 이벤트가 발생할 때 알릴 수 있습니다.

예를 들어 어플라이언스의 하드 디스크 공간이 부족해질 것이 우려되면, 남은 디스크 공간이 Warning(경고) 수준에 도달할 때 시스템 관리자에게 이메일을 자동으로 전송할 수 있습니다. 하드 디스크가 계속 채워지면 하드 드라이브가 Critical(심각) 수준에 도달할 때 두 번째 이메일을 전송할 수 있습니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

상태 모니터 알림 정보

상태 모니터에 의해 생성되는 알림에는 다음 정보가 포함됩니다.

- Severity(심각도) - 알림의 심각도를 나타냅니다.
- Module(모듈) - 테스트 결과가 알림을 트리거한 상태 모듈을 지정합니다.
- Description(설명) - 테스트 결과가 알림을 트리거한 상태 테스트를 포함합니다.

아래 표는 이러한 심각도 수준을 설명합니다.

표 *4:* 알림 심각도

심각도	설명
중대	상태 테스트 결과가 Critical(심각) 알림 상태를 트리거하는 기준을 충족함.
경고	상태 테스트 결과가 Warning(경고) 알림 상태를 트리거하는 기준을 충족함.
정상	상태 테스트 결과가 Normal(정상) 알림 상태를 트리거하는 기준을 충족함.
오류	상태 테스트가 실행되지 않음.
복원됨	상태 테스트 결과가 Critical(심각) 또는 Warning(경고) 알림 상태에 이어 Normal(정상) 알림 상태로 전환되는 기준을 충족함.

상태 모니터 알림 생성

이 절차를 수행하려면 관리자 사용자여야 합니다.

상태 모니터 알림을 생성할 때 심각도, 상태 모듈 및 알림 응답 간에 연결을 생성합니다. 기존 알림을 사용할 수도 있고 특별히 시스템 상태에 대해 보고하도록 새 알림을 구성할 수도 있습니다. 선택한 모듈에 대해 심각도가 발생하면 알림이 트리거됩니다.

기존 임계값을 복제하는 방식으로 임계값을 생성하거나 업데이트하는 경우 충돌이 발생합니다. 중복된 임계값이 존재하면 상태 모니터는 가장 적은 알림을 생성하는 임계값을 사용하고 나머지는 무시합니다. 임계값의 시간 제한 값은 범위가 5~4,294,967,295분이어야 합니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

시작하기 전에

- 상태 경고를 보내는 SNMP, syslog 또는 이메일 서버와 management center의 통신을 제어하는 알림 응답을 구성합니다. Secure Firewall Management Center 알림 응답를 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Add Health Alert(**상태 알림 추가**)** 대화 상자의 **Health Alert Name(**상태 알림 이름**)** 필드에 상태 알림 이름을 입력합니다.

단계 **4** **Severity(**심각도**)** 드롭다운 목록에서 알림을 트리거하기 위해 사용하려는 심각도 수준을 선택합니다.

단계 **5** **Alert(**알림**)** 드롭다운 목록에서 지정된 심각도 수준에 도달할 때 트리거하려는 알림 응답을 선택합니다. 알림 응답을 아직 구성하지 않은 경우 **Alerts(**알림**)**를 클릭하여 **Alerts(**알림**)** 페이지로 이동하여 설정합니다.

단계 **6** **Health Modules(**상태 모듈**)** 목록에서 경고를 적용하려는 상태 정책 모듈을 선택합니다.

단계 **7** 경우에 따라 각 임계값 기간이 끝나고 임계값 카운트가 재설정되기까지의 시간(분 단위)을 **Threshold Timeout(**임계값 시간 초과**)** 필드에 입력합니다.

정책 실행 시간 간격 값이 임계값 시간 초과 값보다 작은 경우에도 지정된 모듈에서 보고된 두 가지 상태 이벤트 사이의 간격은 항상 더 큽니다. 예를 들어 임계값 시간 초과를 8 분으로 변경하고 정책 실행 시간 간격을 5분으로 설정하는 경우, 보고된 이벤트 사이의 간격은 10분(5 x 2)입니다.

단계 **8** **Save(**저장**)**를 클릭하고 상태 알림을 저장합니다.

상태 모니터 알림 수정

이 절차를 수행하려면 관리자 사용자여야 합니다.

상태 모니터 알림과 관련된 심각도, 상태 모듈 또는 알림 응답을 변경하려면 기존의 상태 모니터 알림을 수정할 수 있습니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** 수정하려는 필수 상태 알림에 대해 제공된 **Edit(**수정**)** ( ) 아이콘을 클릭합니다.

단계 **3** **Edit Health Alert(**상태 알림 편집**)** 대화 상자의 **Alert(**알림**)** 드롭다운 목록에서 필요한 알림 항목을 선택하거나 **Alerts(**알림**)** 링크를 클릭하여 새 알림 항목을 구성합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

상태 모니터 알림 삭제

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** 삭제할 상태 알림 옆의 **Delete(**삭제**)** ( )을 클릭한 다음 **Delete health alert(**상태 알림 삭제**)**를 클릭하여 삭제합니다.

다음에 수행할 작업

- 알림이 계속 전송되지 않도록 하려면 기본 알림 응답을 비활성화하거나 삭제해야 합니다. Secure Firewall Management Center 알림 응답을 참조하십시오.

상태 모니터 정보

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모니터는 management center뿐만 아니라 management center에서 관리하는 모든 디바이스에 대한 편집된 상태를 제공합니다. 상태 모니터는 다음으로 구성됩니다.

- Health Status(상태) 요약 페이지 - management center에서 관리하는 모든 디바이스 및 management center의 상태를 한눈에 볼 수 있습니다. 디바이스는 해당하는 경우 지리위치, 고가용성 또는 클러스터 상태에 따라 개별적으로 나열되거나 그룹화됩니다.
  - 디바이스 상태를 나타내는 육각형 위에 마우스를 올려놓으면 management center 및 디바이스의 상태 요약을 확인할 수 있습니다.
  - 디바이스의 왼쪽에 있는 점은 해당 상태를 나타냅니다.
    - 녹색 - 알람 없음
    - 주황색 - 하나 이상의 상태 경고가 표시됨
    - 빨간색 - 하나 이상의 중대 상태 알람

- Monitoring(모니터링) 탐색창 - 디바이스 계층 구조를 탐색할 수 있습니다. 탐색창에서 개별 디바이스에 대한 상태 모니터를 볼 수 있습니다.

다중 도메인 구축에서 상위 도메인의 상태 모니터는 모든 하위 도메인의 데이터를 표시합니다. 하위 도메인에서 상태 모니터는 현재 도메인의 데이터만 표시합니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** **Health Status(**상태**)** 랜딩 페이지에서 management center 및 매니지드 디바이스의 상태를 확인합니다.

a) 디바이스의 상태 요약을 보려면 육각형 위로 마우스 포인터를 올려놓습니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

b) 디바이스 목록에서 **Expand(**확장**)** (>) 및 **Collapse(**축소**)** (⌄)를 클릭하여 디바이스의 상태 알림 목록을 확장하고 축소합니다.

행을 확장하면 상태, 제목 및 상세 정보를 포함한 모든 상태 알림이 나열됩니다.

참고 상태 알림은 심각도 레벨을 기준으로 정렬됩니다.

단계 **3** Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다. Monitoring(모니터링) 탐색창을 사용하는 경우, 다음을 수행합니다.

a) **Home(**홈**)**을 클릭하여 Health Status(상태) 요약 페이지로 돌아갑니다.

b) **Firewall Management Center**를 클릭하여 Secure Firewall Management Center 자체에 대한 상태 모니터를 봅니다.

c) 디바이스 목록에서 **Expand(**확장**)** (>) 및 **Collapse(**축소**)** (⌄)를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

행을 확장하면 모든 디바이스가 나열됩니다.

d) 디바이스별 상태 모니터를 보려면 디바이스를 클릭합니다.

다음에 수행할 작업

- management center에서 관리하는 모든 디바이스의 편집된 상태 및 메트릭에 대한 자세한 내용은 디바이스 상태 모니터, 27 페이지의 내용을 참조하십시오.
- management center의 상태에 대한 자세한 내용은 Management Center 상태 모니터 사용, 25 페이지의 내용을 참조하십시오.

언제든지 **Home(**홈**)**을 클릭하여 Health Status(상태) 랜딩 페이지로 돌아갈 수 있습니다.

Management Center 상태 모니터 사용

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

management center 모니터는 management center의 상태에 대한 자세한 보기를 제공합니다. 상태 모니터는 다음으로 구성됩니다.

- 고가용성(구성된 경우) - HA(고가용성) 패널에는 액티브 및 스탠바이 유닛의 상태, 마지막 동기화 시간, 전체 디바이스 상태를 비롯한 현재 HA 상태가 표시됩니다.
- Event Rate(이벤트 속도) - Event Rate(이벤트 속도) 패널에는 management center에서 수신한 전체 이벤트 속도 및 최대 이벤트 속도가 기준선으로 표시됩니다.
- Event Capacity(이벤트 용량) - Event Capacity(이벤트 용량) 패널은 이벤트 보유 시간, 현재 및 최대 이벤트 용량, 이벤트가 management center의 구성된 최대 용량을 초과하여 저장될 때 알림을 받는 용량 오버플로 메커니즘 등을 포함하여 이벤트 범주별 현재 사용량을 보여줍니다. .
- Process Health(프로세스 상태) - Process Health(프로세스 상태) 패널에는 중요 프로세스를 한눈에 볼 수 있는 보기와 각 프로세스의 CPU 및 메모리 사용량을 포함하여 처리된 모든 프로세스의 상태를 볼 수 있는 탭이 있습니다.
- CPU - CPU 패널에서는 평균 CPU 사용량(기본값)과 모든 코어의 CPU 사용량 간에 전환할 수 있습니다.
- Memory(메모리) - Memory(메모리) 패널에는 management center의 전체 메모리 사용량이 표시됩니다.
- Interface(인터페이스) - Interface(인터페이스) 패널에는 모든 인터페이스의 평균 입력 및 출력 속도가 표시됩니다.
- Disk Usage(디스크 사용량) - Disk Usage(디스크 사용량) 패널에는 전체 디스크의 사용량과 management center 데이터가 저장된 중요 파티션의 사용량이 표시됩니다.

팁 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 상태를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** **Monitoring(**모니터링**)** 탐색 창을 사용하여 management center 및 디바이스별 상태 모니터에 액세스합니다.

- 독립형 management center은 단일 노드로 표시됩니다. 고가용성 management center은 노드 쌍으로 표시됩니다.
- 상태 모니터는 HA 쌍의 액티브 및 스탠바이 management center 모두에서 사용할 수 있습니다.

단계 **3** management center 대시보드를 탐색합니다.

management center 대시보드에는 management center의 HA 상태에 대한 요약 보기(구성된 경우)뿐만 아니라 management center 프로세스 및 디바이스 메트릭(예: CPU, 메모리, 디스크 사용량)을 한눈에 볼 수 있는 보기가 포함되어 있습니다.

어플라이언스에 대해 모든 모듈 실행

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 어플라이언스에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 모든 상태 모듈 테스트를 실행할 수도 있습니다.

다중 도메인 구축에서 현재 도메인 및 모든 하위 도메인의 어플라이언스에 대한 상태 모듈 테스트를 실행할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다.의 내용을 참조하십시오.

단계 **2** **Run All Modules(**모든 모듈 실행**)**를 클릭합니다. 상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance(상태 모니터 어플라이언스) 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

특정 상태 모듈 실행

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 모듈에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 해당 상태 모듈 테스트를 실행할 수도 있습니다.

다중 도메인 구축에서 현재 도메인 및 모든 하위 도메인의 어플라이언스에 대한 상태 모듈 테스트를 실행할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다.의 내용을 참조하십시오.

단계 **2** **Module Status Summary(**모듈 상태 요약**)** 그래프에서 확인하려는 상태 알림 카테고리의 색상을 클릭합니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)**열에서 **Run(**실행**)**을 클릭합니다.

상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance(상태 모니터 어플라이언스) 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

상태 모듈 알림 그래프 생성

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

특정 어플라이언스에 대한 특별한 상태 테스트 기간 중에 발생한 결과를 그래프로 표시할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다의 내용을 참조하십시오.

단계 **2** Health Monitor Appliance(상태 모니터 어플라이언스) 페이지의 **Module Status Summary** 그래프에서 확인하려는 상태 알림 상태 카테고리의 색상을 클릭합니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)**열에서 **Graph(**그래프**)**를 클릭합니다.

팁 이벤트가 나타나지 않으면 시간 범위를 조정해야 합니다.

디바이스 상태 모니터

디바이스 상태 모니터는 management center에서 관리하는 모든 디바이스에 대한 편집된 상태를 제공합니다. 디바이스 상태 모니터는 Firepower 디바이스에 대한 상태 메트릭을 수집하여 시스템 이벤트를 예측하고 이에 응답합니다. 디바이스 상태 모니터는 다음 구성 요소로 이루어집니다.

- System Details(시스템 세부 사항) - 설치된 Firepower 버전 및 기타 구축 세부 사항을 포함하여 매니지드 디바이스에 대한 정보를 표시합니다.
- Troubleshooting & Links(문제 해결 및 링크) - 자주 사용하는 문제 해결 주제 및 절차에 대한 편리한 링크를 제공합니다.
- Health Alerts(상태 알림) - 상태 알림 모니터에서 디바이스의 상태를 한눈에 볼 수 있습니다.

- Time Range(시간 범위) - 다양한 디바이스 메트릭 창에 표시되는 정보를 제한하도록 조정할 수 있는 시간 창입니다.
- Device Metrics(디바이스 메트릭) - 다음을 포함하여 사전 정의된 대시보드에서 범주화된 주요 Firepower 디바이스 상태 메트릭의 어레이입니다.
  - CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
  - 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
  - Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
  - Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.
  - Snort - Snort 프로세스와 관련된 통계
  - Disk Usage(디스크 사용량) - 파티션별 디스크 크기 및 디스크 사용률을 포함한 디바이스 디스크 사용량
  - Critical Processes(중요 프로세스) - 프로세스 재시작과 CPU 및 메모리 사용률과 같이 기타 선택된 상태 모니터를 포함하여 관리 프로세스와 관련된 통계

시스템 세부 사항 및 문제 해결 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

System Details(시스템 세부 사항) 섹션에서는 선택한 디바이스에 대한 일반 시스템 정보를 제공합니다. 해당 디바이스에 대한 문제 해결 작업을 시작할 수도 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 **Expand(**확장**)** (>) 및 **Collapse(**축소**)** (⌄)를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 디바이스별 상태 모니터를 보려면 디바이스를 클릭합니다.

단계 **4** **View System & Troubleshoot Details** ⋯**(**시스템 및 문제 해결 세부 사항 보기**...)** 링크를 클릭합니다.

이 패널은 기본적으로 축소되어 있습니다. 링크를 클릭하면 축소된 섹션이 확장되어 디바이스의 **System Details(**시스템 세부 사항**)** 및 **Troubleshooting & Links(**문제 해결 및 링크**)**가 표시됩니다. 시스템 세부 사항은 다음으로 구성됩니다.

- **Version(**버전**):** Firepower 소프트웨어 버전
- **Model(**모델**):** 디바이스 모델

- **Mode(모드):** 방화벽 모드 Firepower Threat Defense 디바이스는 일반 방화벽 인터페이스에 대해 라우팅 방화벽 모드 및 투명 방화벽 모드의 두 가지 방화벽 모드를 지원합니다.
- **VDB:** Cisco VDB(취약성 데이터베이스) 버전
- **SRU:** 침입 규칙 집합 버전
- **Snort:** Snort 버전

단계 **5** 다음 문제 해결 옵션을 이용할 수 있습니다.

- 문제 해결 파일 생성(다음 참조) 특정 시스템 기능에 대한 문제 해결 파일 생성
- 고급 문제 해결 파일을 생성하고 다운로드합니다. 고급 문제 해결 파일 다운로드의 내용을 참조하십시오.
- 상태 정책을 생성하고 수정합니다. 상태 정책 생성, 14 페이지의 내용을 참조하십시오.
- 상태 모니터 알림을 생성하고 수정합니다. 상태 모니터 알림 생성, 21 페이지의 내용을 참조하십시오.

디바이스 상태 모니터 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

디바이스 상태 모니터는 방화벽 디바이스의 상태에 대한 자세한 보기를 제공합니다. 디바이스 상태 모니터는 디바이스 메트릭을 컴파일하고 대시보드 어레이에 있는 디바이스의 상태 및 추세를 제공합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(상태)** > **Monitor(모니터)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 **Expand(확장)** ( ) 및 **Collapse(축소)** ( )를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 페이지 상단에서 디바이스 이름의 바로 오른쪽에 있는 알림에서 디바이스의 **Health Alerts(상태 알림)**를 확인합니다.

Health Alerts(상태 알림) 위에 포인터를 올려놓으면 디바이스의 상태 요약이 표시됩니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

단계 **4** 오른쪽 상단의 드롭다운에서 시간 범위를 설정할 수 있습니다. 시간 범위는 지난 시간처럼 짧은 기간(기본값) 또는 지난 주처럼 긴 기간을 반영할 수 있습니다. 드롭다운에서 **Custom(사용자 지정)**을 선택하여 사용자 지정 시작 및 종료 날짜를 설정합니다.

새로 고침 아이콘을 클릭하여 자동 새로 고침을 5분으로 설정하거나 자동 새로 고침을 해제합니다.

단계 **5** 선택한 시간 범위와 관련하여 추세 그래프에서 구축 오버레이를 보려면 **Show Deployment Info(**구축 정보 표시**)** () 아이콘을 클릭합니다.

Show Deployment Info(구축 정보 표시**)** () 아이콘은 선택한 시간 범위 동안의 구축 수를 나타냅니다. 세로 줄은 구축 시작 및 종료 시간을 나타냅니다. 다수의 구축이 있는 경우, 여러 대역/라인이 나타납니다. 점선 위에 있는 아이콘을 클릭하여 구축 세부 사항을 확인합니다.

단계 **6** 디바이스 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.
- Snort - Snort 프로세스와 관련된 통계

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 디바이스 메트릭의 전체 목록은 Firepower 디바이스 메트릭, 32 페이지의 내용을 참조하십시오.

단계 **7** 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 지정 상관 관계 대시보드를 생성하려면 디바이스 모니터의 오른쪽 상단 모서리에 있는 더하기 기호(+)를 클릭합니다. 디바이스 메트릭 연계, 30 페이지의 내용을 참조하십시오.

디바이스 메트릭 연계

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

디바이스 상태 모니터에는 시스템 이벤트를 예측하고 응답하는 데 사용되는 주요 Firepower 디바이스 메트릭 어레이가 포함되어 있습니다. 보고된 메트릭을 통해 모든 Firepower 디바이스의 상태를 확인할 수 있습니다.

디바이스 모니터는 기본적으로 여러 미리 정의된 대시보드에서 이러한 메트릭을 보고합니다. 이러한 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.

- Snort - Snort 프로세스와 관련된 통계
- ASP 삭제 - ASP(Accelerated Security Path) 성능 및 동작과 관련된 통계입니다.

사용자 정의 대시보드를 추가하여 상호 연결된 메트릭을 상호 연결할 수 있습니다. 사전 정의된 상관 관계 그룹(예: CPU 및 Snort) 중에서 선택합니다. 또는 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 정의 상관 관계 대시보드를 생성할 수도 있습니다.

시작하기 전에

상태 모니터 대시보드에서 시계열 데이터(디바이스 메트릭)를 보고 상관 관계를 지정하려면 REST API(**Settings(**설정**)** > **Configuration(**구성**)** > **REST API Preferences(REST API** 기본 설정**)**)를 활성화합니다.

참고 디바이스 메트릭 상관은 threat defense 6.7 이상 버전에서만 사용할 수 있습니다. 따라서 threat defense 6.7 이전 버전의 경우 REST API를 활성화하더라도 상태 모니터 대시보드에 이러한 메트릭이 표시되지 않습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 **Expand(**확장**)** (>) 및 **Collapse(**축소**)** (⌄)를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 디바이스 모니터의 오른쪽 상단 모서리에 있는 더하기 기호(+)를 클릭하여 새 대시보드를 추가합니다.

단계 **4** **Select Correlation Group(**상관 관계 그룹 선택**)** 드롭다운에서 미리 정의된 상관 관계 그룹을 선택하거나 사용자 정의 그룹을 생성합니다.

단계 **5** 미리 정의된 상관 관계 그룹에서 대시보드를 생성하려면 그룹을 선택하고 **Add(**추가**)**를 클릭합니다.

- CPU – 데이터 플레인
- CPU – Snort
- CPU – 기타
- 메모리 – 데이터 플레인
- 패킷 삭제

단계 **6** 사용자 정의 상관 관계 대시보드를 생성하려면:

a) **Custom(**사용자 정의**)**을 선택합니다.

b) 필요에 따라 **Dashboard Name(**대시보드 이름**)** 필드에 고유한 이름을 입력하거나 기본값을 수락합니다.

c) 그런 다음 **Select Metric Group(**메트릭 그룹 선택**)** 드롭다운에서 그룹을 선택한 다음 **Select Metrics(**메트릭 선택**)** 드롭다운에서 해당 메트릭을 선택합니다.

- 연결; 사용 가능한 메트릭은 연결 그룹 메트릭, 34 페이지의 내용을 참조하십시오.
- CPU; 사용 가능한 메트릭은 CPU 그룹 메트릭, 32 페이지의 내용을 참조하십시오.
- 중요 프로세스; 사용 가능한 메트릭은 중요 프로세스 그룹 메트릭, 39 페이지의 내용을 참조하십시오.
- 구축된 구성; 사용 가능한 메트릭은 구축된 컨피그레이션 그룹 메트릭, 38 페이지의 내용을 참조하십시오.
- 디스크; 사용 가능한 메트릭은 디스크 그룹 메트릭, 38 페이지의 내용을 참조하십시오.
- 인터페이스; 사용 가능한 메트릭은 인터페이스 그룹 메트릭, 34 페이지의 내용을 참조하십시오.
- Snort; 사용 가능한 메트릭은 Snort 그룹 메트릭, 35 페이지의 내용을 참조하십시오.
- ASP 삭제. 사용 가능한 메트릭은 ASP 삭제 메트릭, 36 페이지을(를) 참조하십시오.

단계 **7** **Add Metrics(**메트릭 추가**)**를 클릭하여 다른 그룹에서 메트릭을 추가하고 선택합니다.

단계 **8** 개별 메트릭을 제거하려면 항목의 오른쪽에있는 **x**를 클릭합니다. 전체 그룹을 제거하려면 삭제 아이콘(휴지통)을 클릭합니다.

단계 **9** **Add(**추가**)**를 클릭하여 워크플로우를 완료하고 상태 모니터에 대시보드를 추가합니다.

단계 **10** 사용자 정의 상관 관계 대시보드를 편집하거나 삭제할 수 있습니다.

Firepower 디바이스 메트릭

다음 섹션에서는 Firepower Threat Defense 디바이스에서 사용 가능한 상태 메트릭에 대해 설명합니다.

CPU 그룹 메트릭

상태 모니터는 프로세스 및 물리적 코어별 CPU 사용률을 포함하여 CPU 이용률과 관련된 통계를 추적합니다.

표 ***5: CPU*** 그룹 메트릭

메트릭	설명	형식
컨트롤 플레인	지난 1분 동안 제어 플레인의 평균 CPU 사용률입니다.	백분율
데이터 플레인	지난 1분 동안 데이터 플레인의 평균 CPU 사용률입니다.	백분율
Snort	지난 1분 동안 Snort 프로세스의 평균 CPU 사용률입니다.	백분율
시스템	지난 1분 동안 시스템 프로세스의 평균 CPU 사용률입니다.	백분율

메트릭	설명	형식
물리적 코어	지난 1분 동안의 모든 코어에 대한 평균 CPU 사용률입니다.	백분율

메모리 그룹 메트릭

상태 모니터는 데이터 플레인 및 Snort 메모리 사용량을 포함하여 디바이스 메모리 사용률과 관련된 통계를 추적합니다.

표 ***6:*** 메모리 그룹 메트릭

메트릭	설명	형식
버퍼 캐시	버퍼 캐시입니다.	바이트
여유 공간	사용 가능한 총 메모리입니다.	바이트
최대 데이터 플레인	데이터 플레인에서 사용하는 최대 메모리입니다.	바이트
최대 Snort	Snort 프로세스에서 사용하는 최대 메모리입니다.	바이트
Snort에 대한 최대 스왑	Snort 프로세스에서 사용하는 최대 스왑 메모리입니다.	바이트
남은 메모리 블록(1550)	1550 바이트 블록의 사용 가능한 메모리입니다.	숫자
남은 메모리 블록(256)	256 바이트 블록의 사용 가능한 메모리입니다.	숫자
사용된 시스템	시스템에서 사용한 총 메모리입니다.	바이트
합계	사용 가능한 총 메모리입니다.	바이트
총 스왑	스왑에 사용 가능한 총 메모리입니다.	바이트
데이터 플레인	데이터 플레인에서 사용된 총 메모리입니다.	바이트
데이터 플레인에서 사용된 비율	데이터 플레인에 사용된 메모리의 비율입니다.	백분율
Snort에서 사용된 비율	Snort 프로세스에 사용된 메모리의 비율입니다.	백분율
스왑에서 사용된 비율	스왑에 사용된 메모리의 비율입니다.	백분율
시스템에서 사용된 비율	시스템에 사용된 메모리의 비율입니다.	백분율
시스템 및 스왑에서 사용된 비율	시스템 및 스왑에 사용된 메모리의 비율입니다.	백분율
Snort	Snort 프로세스에 사용된 총 메모리입니다.	바이트
사용된 스왑	스왑에 사용된 총 메모리입니다.	바이트
Snort에서 사용된 스왑	Snort 프로세스에 사용된 총 스왑 메모리입니다.	바이트

인터페이스 그룹 메트릭

상태 모니터는 인터페이스 상태 및 집계 트래픽 통계를 포함하여 디바이스 인터페이스와 관련된 통계를 추적합니다.

표 *7:* 인터페이스 그룹 메트릭

메트릭	설명	형식
패킷 삭제	드롭된 패킷 수입니다.	숫자
평균 입력 패킷 크기	수신 패킷의 평균 크기입니다.	바이트
입력 속도	총 수신 바이트 수입니다.	바이트
입력 패킷	총 수신 패킷 수입니다.	숫자
평균 출력 패킷 크기	발신 패킷의 평균 크기입니다.	바이트
출력 속도	총 발신 바이트 수입니다.	바이트
출력 패킷	총 발신 패킷 수입니다.	숫자
상태	인터페이스의 상태로, 1은 up(가동), 0은 down(중지)입니다.	1 또는 0

연결 그룹 메트릭

상태 모니터는 연결 및 NAT 변환 수와 관련된 통계를 추적합니다.

표 *8:* 연결 그룹 메트릭

메트릭	설명	형식
Elephant 플로우	활성 엘리펀트 플로우 수를 보여줍니다. 엘리펀트 플로우는 전체 시스템 성능에 영향을 줄 수 있을 만큼 큰 연결입니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큰 상태입니다. **system support elephant-flow-detection** 명령을 사용하여 threat defense CLI에서 엘리펀트 플로우 식별을 위한 바이트 및 시간 임계값을 조정할 수 있습니다. 참고 바이트 및 시간 임계값이 모두 초과되는 경우에만 플로우가 Elephant 플로우로 간주됩니다.	숫자
사용 중인 연결	사용 중인 연결 수를 표시합니다.	숫자
최대 연결 수	최대 동시 연결 수를 표시합니다.	숫자

메트릭	설명	형식
초당 전체 연결 수	모든 연결 유형에 대한 초당 연결 수입니다.	숫자
초당 TCP 연결 수	TCP 연결 유형의 초당 연결 수입니다.	숫자
초당 UDP 연결 수	UDP 연결 유형의 초당 연결 수입니다.	숫자
활성화된 연결 유지	Snort 프로세스가 중단될 경우 라우팅 및 투명 인터페이스에서 기존 TCP/UDP 연결을 유지합니다.	숫자
유지되는 연결	현재 유지되는 연결이 활성화된 연결 수입니다.	숫자
가장 활성화된 연결 유지	지금까지 유지되는 가장 많은 연결 수입니다.	숫자
유지되는 최대 연결 수	지금까지 유지되는 가장 많은 최대 연결 수입니다.	숫자
NAT 변환	변환 수를 표시합니다.	숫자
최대 NAT 변환	동시 변환의 기록 최대 값을 한 번에 표시합니다.	숫자

Snort 그룹 메트릭

상태 모니터는 Snort 프로세스와 관련된 통계를 추적합니다.

표 ***9: Snort*** 그룹 메트릭

메트릭	설명	형식
차단된 목록 플로우	Snort에서 삭제한 정책 설정의 플로우 수입니다.	숫자
차단된 패킷	차단된 패킷 수입니다.	숫자
거부된 플로우	거부된 플로우 이벤트 수입니다. 데이터 플레인은 Snort로 전송하기 전에 플로우를 삭제하기로 결정하면 거부된 플로우 이벤트를 Snort로 전송합니다.	숫자
플로우 종료	데이터 플레인은 빠른 경로 플로우가 종료되면 Snort에 플로우 종료 이벤트를 전송합니다.	숫자
빠른 전달 플로우	정책에 의해 빨리 전달되어 검사되지 않은 플로우 수입니다.	숫자
데이터 플레인에서 전달된 삭제된 프레임	데이터 플레인에서 전달된 삭제된 프레임 수입니다.	숫자
삽입된 패킷 삭제됨	Snort가 삭제된 트래픽 스트림에 추가한 패킷 수입니다.	숫자

메트릭	설명	형식
삽입된 패킷	Snort가 생성하여 트래픽 스트림에 추가한 패킷 수입니다. 예를 들어 재설정 작업으로 파단을 구성하는 경우, Snort는 연결을 재설정할 패킷을 생성합니다.	숫자
인스턴스	Snort 인스턴스(프로세스) 수입니다.	숫자
패킷 수신 대기열 사용률	데이터 플레인 수신 대기열의 대기열 사용률입니다.	백분율
Snort가 사용 중이어서 패킷 우회됨	Snort 사용량이 너무 많아 패킷을 처리할 수 없을 때 검사를 우회한 패킷 수입니다.	숫자
Snort 다운으로 인해 패킷 우회됨	Snort가 중단되었을 때 검사를 우회한 패킷 수입니다.	숫자
RX 대기열이 꽉 차서 패킷 우회됨	수신 대기열이 꽉 차서 우회된 패킷 수입니다.	숫자
TX 대기열이 꽉 차서 패킷 우회됨	전송 대기열이 꽉 차서 우회된 패킷 수입니다.	숫자
통과된 패킷	데이터 플레인에서 Snort로 전송된 패킷 수입니다.	숫자
플로우 시작	플로우 시작 이벤트 수입니다. 이러한 이벤트는 Snort가 연결을 추적하고 연결 이벤트를 보고하는 데 도움이 됩니다.	숫자

ASP 삭제 메트릭

상태 모니터는 ASP(Accelerated Security Path) 삭제된 패킷 또는 연결과 관련된 통계를 추적합니다.

표 ***10: ASP*** 삭제 메트릭

메트릭	설명	형식
연결 제한이 초과됨	연결 제한이 초과되었을 때 닫히는 플로우 수를 계산합니다.	숫자
연결 제한에 도달함	연결 제한 또는 호스트 연결 제한을 초과했을 때 손실된 패킷 수를 계산합니다.	숫자
L2 규칙 삭제	레이어 2 ACL로 인해 거부된 패킷 수를 계산합니다.	숫자
L2 규칙 VXLAN 삭제	레이어 2 ACL 검사를 적용할 때 VXLAN out_tag를 찾지 못하여 거부된 패킷 수를 계산합니다.	숫자

메트릭	설명	형식
NAT 역방향 경로 실패	변환된 호스트의 실제 주소를 사용하여 변환된 호스트에 연결하는 거부된 시도 횟수를 계산합니다.	숫자
NAT 실패	IP 또는 전송 헤더를 변환하는 xlate를 생성하려고 시도했지만 실패한 횟수를 계산합니다.	숫자
유효한 v4 인접성 없음	보안 어플라이언스가 인접 항목을 가져오려고 했지만 다음 홉(IPv4)에 대한 MAC 주소를 가져올 수 없는 경우 손실된 패킷 수를 계산합니다.	숫자
유효한 v6 인접성 없음	보안 어플라이언스가 인접성을 가져오려고 했는데 다음 홉의 MAC 주소를 가져올 수 없으면 이 카운터의 값이 증가합니다.	숫자
Snort에 의해 차단 목록에 나열된 패킷; Snort에 의해 차단된 패킷	Snort 모듈의 요청에 따라 삭제된 패킷 수를 계산합니다.	숫자
프레임 삭제 - Snort 사용 중; 프레임 삭제 - Snort 다운; 프레임 삭제 – Snort 삭제	Snort 모듈이 사용 중이며 프레임을 처리할 수 없으므로 삭제된 프레임 수를 계산합니다. Snort 모듈이 중단되었습니다. Snort 모듈은 삭제를 요청합니다.	숫자
디스패치 대기열 제한에 도달함	디바이스의 로드 밸런싱 ASP 디스패처가 큐 제한에 도달하는 횟수를 계산합니다. 이보다 더 많은 패킷을 포함하려고 하면 tail drop이 수행되며 이 카운터의 값이 증가합니다.	숫자
대상 MAC L2 조회에 실패함	실패한 레이어 2 대상 MAC 주소 조회 수를 계산합니다. 조회 장애 시 어플라이언스는 대상 MAC 검색 프로세스를 시작하여 ARP 및/또는 ICMP 메시지를 통해 호스트 위치를 찾으려고 합니다.	숫자
검사 실패	네트워크 프로세서가 연결에 대해 수행하는 프로토콜 검사를 실행하지 못하는 횟수를 계산합니다. 메모리 할당 장애가 원인일 수도 있고, ICMP 오류 메시지의 경우에는 ICMP 오류 메시지에 임베드된 프레임과 관련하여 설정된 연결을 어플라이언스가 찾을 수 없는 것일 수도 있습니다.	숫자
NAT PAT 풀에 대한 xlate 없음	PAT 풀의 매핑된 주소와 일치하는 대상이 있는 연결에 대해 기존의 xlate를 찾을 수 없습니다.	숫자
호스트로의 경로 없음	보안 어플라이언스가 인터페이스 외부로 패킷을 전송하려고 하지만 라우팅 테이블에서 패킷을 찾을 수 없는 횟수를 계산합니다.	숫자

메트릭	설명	형식
패킷이 대기된 패킷의 수로 삭제됨	잘못된 순서 패킷 큐에 이미 포함되어 있는 재전송된 데이터 패킷을 어플라이언스가 수신할 때 삭제된 패킷 수를 계산합니다.	숫자
제한에 도달한 검사에 대기된 세그먼트 수	플로우의 경우 검사기에 대기중인 패킷 수가 제한에 도달하여 플로우가 종료됩니다.	숫자
Snort에 의해 차단되거나 차단 목록에 추가됨	Snort 모듈의 요청에 따라 패킷이 삭제된 횟수를 계산합니다.	숫자
Snort에서 패킷 묵시적 삭제	Snort 모듈의 요청에 따라 패킷이 자동으로 삭제되는 횟수를 계산합니다.	숫자
동기화되지 않은 첫 번째 TCP 패킷	비 SYN 패킷이 비가로채기/비고정 연결의 첫 번째 패킷으로 수신되는 횟수를 계산합니다.	숫자

구축된 컨피그레이션 그룹 메트릭

상태 모니터는 구축된 설정과 관련된 통계(예: IPS 규칙 수 및 ACE 수)를 추적합니다.

표 ***11:*** 구축된 설정 그룹 메트릭

메트릭	설명	형식
ACE의 수	ACE(Access Control Entry) 또는 규칙의 수입니다. ACL(액세스 제어 목록)은 하나 이상의 ACE 또는 규칙으로 구성됩니다.	숫자
규칙의 수	침입 정책에 있는 규칙의 수입니다.	숫자

디스크 그룹 메트릭

상태 모니터는 디스크 크기 및 파티션별 디스크 사용률을 포함하여 디바이스 디스크 사용과 관련된 통계를 추적합니다.

표 ***12:*** 디스크 그룹 메트릭

메트릭	설명	형식
합계	디바이스 디스크의 총 크기입니다.	바이트
사용됨	디바이스 디스크에서 사용된 총 공간입니다.	바이트
/ngfw에서 사용된 %	/ngfw 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Ngfw/Volume에서 사용된 %	/ngfw/Volume 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율

메트릭	설명	형식
/Dev/cgroups에서 사용된 %	/dev/cgroups 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Mnt/disk0에서 사용된 %	/mnt/disk0 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Var/volatile에서 사용된 %	/var/volatile 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율

중요 프로세스 그룹 메트릭

상태 모니터는 관리되는 프로세스의 프로세스 재시작과 관련된 통계를 추적합니다. 또한 각 중요 프로세스에 대해 상태 모니터는 CPU 사용률, 메모리 사용률, 업타임 및 상태를 추적합니다.

표 ***13:*** 중요 프로세스 그룹 메트릭

메트릭	설명	형식
CPU 사용률	마지막 1분 동안 제어 플레인 및 데이터 플레인의 평균 CPU 사용률입니다.	백분율
재시작 횟수	지난 1분 동안 제어 플레인의 평균 CPU 사용률입니다.	백분율
상태	지난 1분 동안 데이터 플레인의 평균 CPU 사용률입니다.	백분율
업타임	지난 1분 동안 Snort 프로세스의 평균 CPU 사용률입니다.	백분율
사용된 메모리	지난 1분 동안 시스템 프로세스의 평균 CPU 사용률입니다.	백분율

상태 모니터 상태 카테고리

사용 가능한 상태 카테고리가 아래 표에 심각도별로 나열됩니다.

표 ***14:*** 상태 표시기

상태 레벨	상태 아이콘	원 그래프의 상태 색상	설명
오류	**Error(**오류**)** (✖)	검은색	어플라이언스에서 하나 이상의 상태 모니터링 모듈이 실패했으며, 실패 이후 성공적으로 다시 실행되지 않았습니다. 상태 모니터링 모듈의 업데이트를 얻으려면 기술 지원 담당자에게 문의하십시오.

상태 레벨	상태 아이콘	원 그래프의 상태 색상	설명
중대	**Critical(중요)** ()	빨간색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Critical(심각) 한도가 초과되었으며 문제가 해결되지 않았음을 나타냅니다.
경고	**Warning(경고)** ()	노란색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Warning(경고) 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 이 상태는 또한 과도기 상태를 나타냅니다. 즉, 디바이스 구성의 변경으로 인해 필요한 데이터를 일시적으로 사용할 수 없거나 처리할 수 없습니다. 모니터링 주기에 따라 이 과도 상태는 자동으로 수정됩니다.
정상	**Normal(정상)** ()	녹색	어플라이언스의 모든 상태 모듈이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있습니다.
복원됨	**Recovered(복구됨)** ()	녹색	어플라이언스의 모든 상태 모듈(Critical(심각) 또는 Warning(경고) 상태에 있던 모듈 포함)이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있음을 나타냅니다.
Disabled(비활성화)	**Disabled(비활성화됨)** ()	파란색	어플라이언스가 비활성화되었거나 제외되었거나, 어플라이언스에 상태 정책이 적용되지 않았거나, 어플라이언스에 현재 도달할 수 없음을 나타냅니다.

상태 이벤트 보기

상태 이벤트 보기(Health Event View) 페이지에서는 management center로그 상태 이벤트의 상태 모니터가 기록한 상태 이벤트를 볼 수 있습니다. 완전하게 맞춤화가 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 조사하는 이벤트와 관련된 기타 정보에 쉽게 액세스 할 수 있도록 이벤트 데이터를 검색 할 수 있습니다. 각 상태 모듈이 테스트하는 조건을 이해하면 상태 이벤트에 대한 알림을 좀 더 효과적으로 구성할 수 있습니다.

상태 이벤트 보기 페이지에서 많은 표준 이벤트 보기 기능을 수행할 수 있습니다.

상태 이벤트 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

Health Events(상태 이벤트) 페이지의 Table View(테이블 보기)에는 지정된 어플라이언스의 모든 상태 이벤트가 나열됩니다.

management center의 Health Monitor(상태 모니터) 페이지에서 상태 이벤트에 액세스하면 모든 관리되는 어플라이언스에 대한 모든 상태 이벤트가 검색됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

팁 Health Events(상태 이벤트) 테이블이 포함된 상태 이벤트 워크플로의 페이지로 돌아가려면 이 보기에 북마크를 지정할 수 있습니다. 북마크 지정된 보기는 현재 보고 있는 시간 범위 내에서 이벤트를 검색하지만, 필요한 경우 시간 범위를 수정하여 좀 더 최신 정보로 테이블을 업데이트할 수 있습니다.

프로시저

시스템 (⚙) > **Health(**상태**)** > **Events(**이벤트**)**를 선택합니다.

팁 상태 이벤트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭하십시오. Select Workflow(워크플로 선택) 페이지에서 **Health Events(**상태 이벤트**)**를 클릭합니다.

참고 이벤트가 나타나지 않으면 시간 범위를 조정해야 합니다.

상태 이벤트 테이블 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Bookmark(즐겨찾기) — 현재 페이지에 즐겨찾기에 등록해 빠르게 돌아오려면, **Bookmark This Page(**이 페이지를 즐겨찾기에 등록**)**를 클릭하고 즐겨찾기 이름을 지정한 후 **Save(**저장**)**를 클릭합니다.
- Change Workflow(워크플로 변경) — 다른 상태 이벤트 워크플로 선택하려면, **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- Delete Events(이벤트 삭제) — 상태 이벤트를 삭제하려, 삭제하려는 이벤트 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다. 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All(**모두 삭제**)**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
- Generate Reports(보고서 생성) — 테이블 보기에서 데이터를 기반으로 보고서를 생성하고 **Report Designer(**리포트 디자이너**)**를 클릭합니다.

- Modify(수정) — 상태 테이블 보기에 나열된 이벤트의 시간 및 날짜 범위를 수정합니다. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
- Navigate(탐색) — 이벤트 보기 페이지를 탐색합니다.
- Navigate Bookmark(즐겨찾기 탐색) — 즐겨찾기 관리 페이지로 이동하려면 이벤트 보기에서 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- Navigate Other(기타 탐색) — 관련 이벤트를 보기 위해 다른 이벤트 테이블로 이동합니다.
- Sort(정렬) — 표시되는 이벤트를 정렬하고, 이벤트 테이블에 표시되는 열을 변경하며, 표시되는 이벤트를 제한합니다.
- View All(모두 보기) — 보기에서 모든 이벤트에 대한 이벤트 세부 정보를 보려면, **View All(**모두 보기**)**를 클릭합니다.
- View Details(세부 정보 보기) — 단일 상태 이벤트와 관련된 세부 사항을 보려면, 이벤트의 왼쪽에 있는 아래쪽 화살표 링크를 클릭합니다.
- View Multiple(다중 보기) — 여러 상태 이벤트의 이벤트 세부 정보를 보려면, 세부 정보를 보려는 이벤트에 해당하는 행 옆의 확인란을 선택한 후 **View(**보기**)**를 클릭합니다.
- View Status(상태 보기) - 특정 상태의 모든 이벤트를 보려면 Status(상태) 열의 상태를 클릭하여 해당 상태의 이벤트를 찾습니다.

상태 이벤트 테이블

상태 정책에서 활성화하기 위해 선택하는 Health Monitor(상태 모니터) 모듈은 다양한 테스트를 실행하여 어플라이언스 상태를 결정합니다. 상태가 지정된 기준을 충족하면 상태 이벤트가 생성됩니다.

아래 표에서는 상태 이벤트 테이블에서 보고 검색 할 수 있는 필드를 설명합니다.

표 ***15:*** 상태 이벤트 필드

필드	설명
모듈 이름	보려는 상태 이벤트를 생성한 모듈의 이름을 지정합니다. 예를 들어 CPU 성능을 측정하는 이벤트를 보려면, `CPU`를 입력합니다. 그러면 해당 CPU Usage 및 CPU 온도 이벤트가 검색됩니다.
테스트 이름 (검색만 해당)	이벤트를 생성한 상태 모듈의 이름입니다.
시간 (검색만 해당)	상태 이벤트의 타임스탬프.
설명	이벤트를 생성한 상태 모듈의 설명. 예를 들어, 프로세스를 실행할 수 없을 때 생성되는 상태 이벤트에는 `Unable to Execute`라는 레이블이 지정됩니다.

필드	설명
값	이벤트를 생성한 상태 테스트에서 얻은 결과의 값(단위의 수). 예를 들어 management center에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때마다 상태 이벤트가 생성된다면 값은 80~100의 숫자가 될 수 있습니다.
단위	결과의 단위 설명자. 와일드카드 검색을 생성하려면 별표(*)를 사용할 수 있습니다. 예를 들어 management center에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때 상태 이벤트가 생성된다면 단위 설명자는 퍼센트 기호(%)입니다.
상태	어플라이언스에 대해 보고된 상태(Critical(심각), Yellow(노란색), Green(녹색) 또는 Disabled(비활성화)).
도메인	매니지드 디바이스에서 보고한 상태 이벤트의 경우, 상태 이벤트를 보고한 디바이스의 도메인. management center에서 보고한 상태 이벤트의 경우, `Global(전역)`. 이 필드는 다중 도메인 구축에서만 나타납니다.
디바이스	상태 이벤트가 보고된 어플라이언스.

상태 모니터링 기록

기능	버전	세부정보
상태 모니터 UI 수정	7.1	다음 UI 페이지는 더 나은 사용성과 데이터 표시를 위해 개선되었습니다. • 정책 • 제외 • 모니터 알림 신규/수정된 화면: **Settings(**설정**)** > **Health(**상태**)** > **Policy(**정책**)**, **Settings(**설정**)** > **Health(**상태**)** > **Exclude(**제외**)** 및 **Settings(**설정**)** > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**.
엘리펀트 플로우 탐지	7.1	상태 모니터에는 다음과 같은 향상된 기능이 포함됩니다. • 연결 통계에는 활성 엘리펀트 플로우가 포함됩니다. • Connection Group Metrics(연결 그룹 메트릭)에는 활성 엘리펀트 플로우의 수가 포함됩니다. 엘리펀트 플로우 탐지 기능은 Cisco Firewall 2100 시리즈에서 지원되지 않습니다.

기능	버전	세부정보
중단된 높은 비관리 디스크 사용량 알림.	7.0.6	디스크 사용량 상태 모듈은 더 이상 높은 비관리 디스크 사용량에 대해 알림을 전송하지 않습니다. 업그레이드 후에는 매니지드 디바이스에 상태 정책을 구축하거나(알림 표시 중지) 디바이스를 업그레이드(알림 전송 중지)할 때까지 이러한 알림이 계속 표시될 수 있습니다. 참고 버전 7.0–7.0.5, 7.1.x, 7.2.0–7.2.3 및 7.3.x는 이러한 알림을 계속 지원합니다. management center에서 이러한 버전을 실행하는 경우에도 알림이 계속 표시될 수 있습니다.

기능	버전	세부정보
새 상태 모듈	7.0	

기능	버전	세부정보
		다음 상태 모듈을 추가했습니다. • AMP Connection Status(AMP 연결 상태): threat defense에서 AMP 클라우드 연결을 모니터링합니다. • AMP Threat Grid Status(AMP Threat Grid 상태): threat defense에서 AMP Threat Grid 클라우드 연결을 모니터링합니다. • ASP Drop(ASP 삭제): 데이터 플레인 가속 보안 경로에 의해 삭제된 연결을 모니터링합니다. • Advanced Snort Statistics(고급 Snort 통계): 패킷 성능, 흐름 카운터 및 흐름 이벤트와 관련된 Snort 통계를 모니터링합니다. • Event Stream Status(이벤트 스트림 상태): Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을 모니터링합니다. • FMC Access Configuration Changes(FMC 액세스 구성 변경): management center에서 직접 수행한 액세스 구성 변경 사항을 모니터링합니다. • FMC HA Status(FMC HA 상태): 액티브 및 스탠바이 management center와 디바이스 간의 동기화 상태를 모니터링합니다. HA 상태 모듈을 교체합니다. • FTD HA Status(FTD HA 상태): 액티브 및 스탠바이 threat defense HA 쌍과 디바이스 간의 동기화 상태를 모니터링합니다. • File System Integrity Check(파일 시스템 무결성 검사): 시스템에 CC 모드 또는 UCAPL 모드가 활성화되어 있는 경우 파일 시스템 무결성 검사를 수행합니다. • Flow Offload(플로우 오프로드): Firepower 9300 및 4100 플랫폼에서 하드웨어 플로우 오프로드 통계를 모니터링합니다. • Hit Count(적중 횟수): 액세스 제어 정책에서 특정 규칙이 적중된 횟수를 모니터링합니다. • MySQL Status(MySQL 상태): MySQL 데이터베이스의 상태를 모니터링합니다. • NTP Status FTD(NTP 상태 FTD): 매니지드 디바이스의 NTP 클럭 동기화 상태를 모니터링합니다. • RabbitMQ Status(RabbitMQ 상태): RabbitMQ 메시징 브로커의 상태를 모니터링합니다. • Routing Statistics(라우팅 통계): 에서 IPv4 및 IPv6 경로 정보를 모두 모니터링합니다.threat defense • SSE Connection Status(SSE 연결 상태): threat defense에서 SSE 클라우드 연결을 모니터링합니다. • Sybase Status(Sybase 상태): Sybase 데이터베이스의 상태를 모니터링합니다. • Unresolved Groups Monitor(확인되지 않은 그룹 모니터): 액세스 제어 정책에 사용

기능	버전	세부정보
		되는 확인되지 않은 그룹을 모니터링합니다. • VPN Statistics(VPN 통계): 사이트 간 및 원격 액세스 VPN 터널 통계를 모니터링합니다. • xTLS Counters(xTLS 카운터): xTLS/SSL 플로우, 메모리 및 캐시 효율성을 모니터링합니다.
상태 모니터 개선 사항	7.0	상태 모니터에는 다음과 같은 향상된 기능이 추가되었습니다. • 다음의 요약 보기가 있는 향상된 management center 대시보드: • 고가용성 • 이벤트 비율 및 용량 • 프로세스 상태 • CPU 임계값 • 메모리 • 인터페이스 속도 • 디스크 사용 • 향상된 threat defense 대시보드: • 스플릿 브레인 시나리오에 대한 상태 알림 • 새 상태 모듈에서 사용 가능한 추가 상태 메트릭

기능	버전	세부정보
새 상태 모듈	6.7	CPU 사용 모듈은 더 이상 사용되지 않습니다. 대신 다음 CPU 사용 모듈을 참조하십시오. • CPU 사용(코어 당): 모든 코어의 CPU 사용을 모니터링합니다. • CPU 사용 데이터 플레인: 디바이스에서 모든 데이터 플레인 프로세스의 평균 CPU 사용을 모니터링합니다. • CPU 사용 데이터 Snort: 디바이스에서 Snort 프로세스의 평균 CPU 사용을 모니터링합니다. • CPU 사용량 시스템: 디바이스에 있는 모든 시스템 프로세스의 평균 CPU 사용량을 모니터링합니다. 통계를 추적하기 위해 다음 모듈이 추가되었습니다. • 연결 통계: 연결 통계 및 NAT 변환 수를 모니터링합니다. • 중요 프로세스 통계: 이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다. • 구축된 구성 통계: 구축 된 구성에 대한 통계(예: ACE 및 IPS 규칙 수)를 모니터링합니다. • Snort 통계: 이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다. 메모리 사용을 추적하기 위해 다음 모듈이 추가되었습니다. • 메모리 사용 데이터 플레인: 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다. • 메모리 사용량 Snort: Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다.

기능	버전	세부정보
상태 모니터 개선 사항	6.7	상태 모니터에는 다음과 같은 향상된 기능이 추가되었습니다. • 상태 요약 페이지는 Firepower Management Center 및 management center가 관리하는 모든 디바이스의 상태를 한눈에 볼 수 있도록 합니다. • Monitoring(모니터링) 탐색 창에서는 디바이스 계층 구조를 탐색할 수 있습니다. • 매니지드 디바이스는 개별적으로 나열되거나 해당하는 경우 지리적 위치, 고 가용성 또는 클러스터 상태에 따라 그룹화됩니다. • 탐색창에서 개별 디바이스에 대한 상태 모니터를 볼 수 있습니다. • 상호 관련된 메트릭을 상호 연결하는 맞춤형 대시 보드입니다. 사전 정의된 상관 관계 그룹(예: CPU 및 Snort) 중에서 선택합니다. 또는 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 정의 상관 관계 대시보드를 생성할 수도 있습니다.
기능이 디바이스의 위협 데이터 업데이트 모듈로 이동됨	6.7	로컬 악성 코드 분석 모듈은 더 이상 사용되지 않습니다. 대신 이 정보는 디바이스의 위협 데이터 업데이트 모듈을 참조하십시오. 이전에는 보안 인텔리전스 모듈 및 URL 필터링 모듈에서 제공한 일부 정보가 디바이스의 위협 데이터 업데이트 모듈에서 제공되었습니다.
새 상태 모듈: 구성 메모리 할당	7.0 6.6.3	버전 6.6.3에서는 디바이스 메모리 관리를 개선하고 새로운 상태 모듈인 구성 메모리 할당을 도입했습니다. 이 모듈은 구축된 구성의 크기로 인해 디바이스에서 메모리가 부족해질 위험이 있을 때 알려줍니다. 알림에는 구성에 필요한 메모리의 양과 사용 가능한 메모리를 초과하는 양이 표시됩니다. 이 경우 구성을 재평가하십시오. 종종 액세스 제어 규칙 또는 침입 정책의 수 또는 복잡성을 줄일 수 있습니다.
URL 필터링 모니터링 개선 사항	6.5	이제 URL 필터링 모니터 모듈은 management center가 Cisco Cloud에 등록하지 못하면 알림을 보냅니다.
URL 필터링 모니터링 개선 사항	6.4	이제 URL 필터링 모니터 경고에 대한 시간 임계값을 구성할 수 있습니다.
새 상태 모듈: Threat Data Updates on Devices(디바이스에서 위협 데이터 업데이트)	6.3	새 모듈 **Threat Data Updates on Devices(**디바이스에서 위협 데이터 업데이트**)**이 삭제되었습니다. 이 모듈은 디바이스가 위협 탐지에 사용하는 특정 인텔리전스 데이터 및 구성이 사용자가 지정한 기간 내에 디바이스에서 업데이트되지 않은 경우 알림을 보냅니다.