



시스템 문제 해결

다음 주제에서는 Firepower System에서 발생할 수 있는 문제를 진단하는 방법을 설명합니다.

- 문제 해결의 첫 번째 단계, 1 페이지
- 시스템 메시지, 2 페이지
- 기본 시스템 정보 보기, 4 페이지
- 시스템 메시지 관리, 5 페이지
- 상태 모니터 알람의 메모리 사용량 임계값, 8 페이지
- 이벤트 상태 모니터 알람의 디스크 사용량 및 소모, 9 페이지
- 문제 해결을 위한 상태 모니터 보고서, 13 페이지
- 일반 문제 해결, 15 페이지
- 연결 기반 문제 해결, 15 페이지
- Firepower Threat Defense 디바이스의 고급 문제 해결, 16 페이지
- 기능별 문제 해결, 17 페이지

문제 해결의 첫 번째 단계

- 문제 해결을 위해 변경을 수행하기 전에 원래 문제를 캡처하기 위한 문제 해결 파일을 생성합니다. [문제 해결을 위한 상태 모니터 보고서, 13 페이지](#) 및 그 하위 섹션을 참조하십시오.

Cisco TAC에 지원 문의를 하는 경우 이 문제 해결 파일이 필요한 경우가 있습니다.

- 메시지 센터에서 오류 및 경고 메시지를 확인하여 검사를 시작합니다. [시스템 메시지](#)의 내용을 참조하십시오.
- 제품의 제품 문서 중 "문제 해결 및 알람"에 수록된 관련 기술 노트 및 다른 문제 해결 자료를 참고하십시오. [FMC 구축에 대한 최상위 문서 목록 페이지](#)의 내용을 참조하십시오.

시스템 메시지

Firepower System에서 발생한 문제를 추적하려면 메시지 센터에서 조사를 시작하십시오. 이 기능을 사용하면 Firepower System에서 지속적으로 생성하는 시스템 활동 및 상태에 대한 메시지를 볼 수 있습니다.

메시지 센터를 열려면 메인 메뉴의 Deploy(구축) 메뉴 옆에 있는 시스템 상태 아이콘을 클릭합니다. 이 아이콘은 시스템 상태에 따라 다음 중 하나의 형태를 취합니다.

- **Indicates One or More Errors**(오류가 하나 이상임을 표시) — 시스템에 하나 이상의 오류 및 경고가 발생했음을 나타냅니다.
- **Indicates One or More Warnings**(경고가 하나 이상임을 표시) — 시스템에 오류 없이 하나 이상의 경고가 발생했음을 나타냅니다.
- **Indicates No Warnings**(경고 없음 표시) — 시스템에 발생한 오류 및 경고가 없음을 나타냅니다.

아이콘에 표시된 숫자는 전체 오류 및 경고 메시지의 수를 나타냅니다.

메시지 센터를 닫으려면 Firepower System 웹 인터페이스에서 메시지 센터의 범위를 벗어난 아무 곳이나 클릭합니다.

메시지 센터 외에도 웹 인터페이스는 사용자 활동 및 현재 진행 중인 시스템 활동에 대해 즉시 팝업 알림을 표시합니다. 일부 팝업 알림은 5초 후 자동으로 사라지지만 "스티커" 알림은 해제 (X)을 클릭해 취소하기 전까지 표시됩니다. 모든 알림을 취소하려면 알림 목록 상단의 취소 링크를 클릭합니다.



팁 비 스티커 팝업 알림 위에 커서를 올려 놓으면 알림이 고정됩니다.

시스템은 라이선스, 도메인, 액세스 역할에 따라 사용자에게 팝업 알림과 메시지 센터 중 하나를 선택하여 메시지를 표시합니다.

메시지 유형

메시지 센터의 시스템 활동 및 상태를 보고하는 메시지는 세 가지 탭으로 구성됩니다.

구축

이 탭에는 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 설정 구축과 관련된 현재 상태가 표시됩니다. 이 탭에서 Firepower System은 다음 구축 상태 값을 보고합니다.

- 실행 중(회전 중인) - 설정이 구축 중입니다.
- 성공 - 설정이 성공적으로 구축되었습니다.
- 경고(⚠) - 경고 구축 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

- 실패 - 설정 구축에 실패했습니다. **만료된 정책**의 내용을 참조하시기 바랍니다. 구축 실패는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태

이 탭은 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 현재 상태 정보가 표시됩니다. 상태는 **상태 모니터링 정보**에서 설명한 상태 모듈에 의해 생성됩니다. 이 탭에서 Firepower System은 다음 상태 값을 보고합니다.

- 경고(⚠️) - 어플라이언스의 상태 모듈에 대한 경고 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 노란색 삼각형(⚠️)을 사용하여 이 상태를 표시합니다. 경고 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 중요(!) - 어플라이언스의 상태 모듈에 대한 위험 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 중요(!) 아이콘을 사용하여 이 상태를 표시합니다. 위험 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 오류(❌) - 어플라이언스에서 상태 모니터링 모듈의 오류가 발생했으며 오류 발생 이후 성공적으로 다시 실행되지 않았음을 나타냅니다. 상태 모니터링 페이지는 오류 아이콘을 사용하여 이 상태를 표시합니다. 오류 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태 모니터링 페이지에서 관련 상세정보를 보려면 상태 탭의 링크를 클릭하십시오. 현재 상태 조건이 없는 경우 상태 탭은 메시지를 표시하지 않습니다.

작업

Firepower System에서 일부 작업(구성 백업 또는 업데이트 설치)을 완료하는 데 시간이 걸릴 수 있습니다. 이 탭은 이러한 장기 작업 및 사용자 또는 적절한 액세스가 가능한 시스템의 다른 사용자가 시작한 작업 상태를 표시합니다. 이 탭은 각 메시지의 최신 업데이트를 기준으로 시간 반대로 메시지를 표시합니다. 일부 작업 상태 메시지는 문제의 작업에 대한 자세한 정보를 안내하는 링크를 포함합니다. 이 탭에서 Firepower System은 다음 작업 상태 값을 보고합니다.

- 대기() - 실행 중인 다른 작업이 완료될 때까지 작업이 실행 대기 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 실행 중 - 작업이 실행 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 재시도() - 작업이 자동으로 재시도함을 나타냅니다. 모든 작업의 재시도가 허용되는 것은 아니라는 점에 유의하십시오. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 성공() - 작업이 성공적으로 완료됨을 나타냅니다.
- 실패() - 작업이 성공적으로 완료되지 않음을 나타냅니다. 오류 작업은 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

- 중단 또는 정지() - 작업이 시스템 업데이트 때문에 중단됨을 나타냅니다. 중단된 작업은 다시 시작할 수 없습니다. 정상 작업이 복구되면 작업을 다시 시작합니다.
- 건너뛴 - 진행 중인 프로세스 때문에 작업을 시작할 수 없었습니다. 다시 시도해 작업을 시작하십시오.

새 작업이 시작되면 이 탭에 새 메시지가 표시됩니다. 작업이 완료(상태 성공, 실패, 중단)되면 이 탭은 사용자가 제거할 때까지 최종 상태 메시지를 표시합니다. 작업 탭 및 메시지 데이터베이스가 불필요하게 복잡해지지 않도록 메시지를 제거하는 것이 좋습니다.

메시지 관리

메시지 센터에서 다음을 수행할 수 있습니다.

- 팝업 알림 동작을 설정합니다(표시할 것인지 선택).
- 시스템 데이터베이스에서 추가 작업 상태 메시지를 표시합니다(제거되지 않아 사용 가능한 경우).
- 작업 상태 메시지를 하나씩 제거합니다.(제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)
- 작업 상태 메시지를 한꺼번에 제거합니다.(제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)



팁 데이터베이스 및 표시가 불필요하게 복잡해지지 않도록 작업 탭에서 누적된 작업 상태 메시지를 정기적으로 제거하는 것이 좋습니다. 데이터베이스의 메시지 수가 100,000개에 근접하면 시스템이 자동으로 제거한 작업 상태 메시지를 삭제합니다.

기본 시스템 정보 보기

About(정보) 페이지에는 Firepower System의 모델, 일련 번호, 다양한 구성 요소에 대한 버전 정보 등 어플라이언스에 대한 정보가 표시됩니다. 또한 Cisco 저작권 정보도 포함되어 있습니다.

프로시저

단계 1 페이지 상단에 있는 툴바에서 **Help**(도움말)를 클릭합니다.

단계 2 **About**(정보)를 선택합니다.

어플라이언스 정보 보기

프로시저

System(시스템) > **Configuration**(구성)을 선택합니다.

시스템 메시지 관리

프로시저

단계 1 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 구성 구축과 관련된 메시지를 보려면 배포를 클릭합니다. [구축 메시지 보기](#)의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 구성 구축 권한이 있어야 합니다.
- **Firepower Management Center** 및 등록된 디바이스의 상태와 관련된 메시지를 보려면 상태를 클릭합니다. [상태 메시지 보기](#)의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.
- 장기 작업과 관련된 메시지를 보려면 작업을 클릭합니다. [작업 메시지 보기](#) 또는 [작업 메시지 관리](#)를 참조하십시오. 누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks**(다른 사용자의 작업 보기) 권한이 있어야 합니다.
- 팝업 알림 동작을 설정하려면 메시지 센터의 오른쪽 상단 모서리의 톱니바퀴(⚙️)를 클릭합니다. [알림 동작 설정](#)의 내용을 참조하십시오.

구축 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 컨피그레이션 구축 권한이 있어야 합니다.

프로시저

단계 1 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 2 **Deployments**(구축)를 클릭합니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- **total**(전체)을 클릭하여 모든 현재 구축 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 구축 상태의 메시지만 확인합니다.

- 경과된 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **1m 5s(1분 5초)**)에서 구축의 경과된 시간과 시작 및 중지 시간을 확인합니다.

관련 항목

[컨피그레이션 변경 사항 구축](#)

상태 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.

프로시저

단계 1 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 2 **Health(상태)**를 클릭합니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- 모든 현재 상태를 확인하려면 **total(전체)**을 클릭합니다.
- 특정 상태 메시지만을 확인하려면 상태 메시지를 클릭합니다.
- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3일 전)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 특정 메시지에 대한 자세한 상태 정보를 보려면 메시지를 클릭합니다.
- 상태 모니터링 페이지에서 전체 상태를 보려면 상태 모니터를 클릭합니다.

관련 항목

[상태 모니터링 정보](#)

작업 메시지 보기

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(다른 사용자의 작업 보기)** 권한이 있어야 합니다.

프로시저

단계 1 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 2 **Tasks(작업)**를 클릭합니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- **total(전체)**을 클릭하여 모든 현재 작업 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 상태의 작업에 대한 메시지만 확인합니다.

참고 중지된 작업에 대한 메시지는 작업 상태 메시지의 전체 목록에만 표시됩니다. 중지된 작업을 필터링할 수는 없습니다.

- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3일 전)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 메시지 내의 링크를 클릭하여 작업에 대한 자세한 정보를 확인합니다.
- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(메시지 더 가져오기)**를 클릭하여 해당 메시지를 검색합니다.

작업 메시지 관리


누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자인거나 **View Other Users' Tasks(다른 사용자의 작업 보기)** 권한이 있어야 합니다.

프로시저

단계 1 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 2 **Tasks(작업)**를 클릭합니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(메시지 더 가져오기)**를 클릭하여 해당 메시지를 검색합니다.
- 완료된 작업(상태 중단, 성공, 실패)에 대한 단일 메시지를 제거하려면 메시지 옆의 제거()를 클릭합니다.
- 모든 완료된 작업(상태 중단, 성공, 실패)에 대한 전체 메시지를 제거하려면 **Total(전체)**에서 메시지를 필터링하고 **Remove all completed tasks(모든 완료된 작업 제거)**를 클릭합니다.
- 성공적으로 완료된 모든 작업에 대한 전체 메시지를 제거하려면 **Success(성공)** 메시지를 필터링하고 **Remove all completed tasks(모든 성공적인 작업 제거)**를 클릭합니다.
- 실패한 모든 작업에 대한 전체 메시지를 제거하려면 **Failure(실패)** 메시지를 필터링하고 **Remove all failed tasks(모든 실패한 작업 제거)**를 클릭합니다.

알림 동작 설정



참고 이 설정은 모든 팝업 알림에 영향을 주고 로그인 세션 동안 유지됩니다.

프로시저

- 단계 1 시스템 상태를 클릭하여 메시지 센터를 표시합니다.
- 단계 2 메시지 센터 오른쪽 상단 구석의 톱니바퀴(⚙️)를 클릭합니다.
- 단계 3 팝업 알람 표시를 활성화 또는 비활성화하려면 알람 표시 슬라이더를 클릭 합니다.
- 단계 4 슬라이더를 다시 숨기려면 톱니바퀴(⚙️)를 클릭합니다.
- 단계 5 메시지 센터를 닫으려면 시스템 상태를 다시 클릭합니다.

상태 모니터 알람의 메모리 사용량 임계값

Memory Usage 상태 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 설정된 제한과 비교하고, 사용량이 레벨을 초과하면 알람을 전송합니다. 모듈은 매니지드 디바이스 및 FMC 자체의 데이터를 모니터링합니다.

메모리 사용에 대해 설정 가능한 두 가지 임계값인 Critical(심각) 및 Warning(경고)을 사용된 메모리의 백분율로 설정할 수 있습니다. 이러한 임계값을 초과하면 심각도 레벨이 지정된 상태 알람이 생성됩니다. 그러나 상태 정보 시스템은 이러한 임계 값을 정확한 방식으로 계산하지 않습니다.

높은 메모리 디바이스를 사용하는 경우 특정 프로세스에서는 낮은 메모리 공간 디바이스에서보다 전체 시스템 메모리의 비율이 더 많이 사용됩니다. 이 설계에서는 보조 프로세스에 사용할 수 있는 작은 메모리 값을 남겨 두면서 최대한 많은 물리적 메모리를 사용합니다.

두 개의 디바이스(하나는 32GB 메모리, 다른 하나는 4GB 메모리)를 비교합니다. 32GB의 메모리가 있는 디바이스에서 메모리의 5%(1.6GB)는 4GB의 메모리가 있는 디바이스(4GB의 5% = 200MB)보다 보조 프로세스에서 남겨야 할 메모리 값이 훨씬 더 큼니다.

특정 프로세스에서 시스템 메모리를 더 많이 사용하는 비율을 고려하기 위해 FMC는 총 물리적 메모리와 총 스왑 메모리를 모두 포함하도록 총 메모리를 계산합니다. 따라서 사용자가 설정한 임계값 입력에 대해 시행된 메모리 임계값은 이벤트의 "Value(값)" 열이 초과된 임계값을 결정하기 위해 입력한 값과 일치하지 않는 상태 이벤트를 초래할 수 있습니다.

다음 표에는 설치된 시스템 메모리에 따라 사용자 입력 임계값 및 시행된 임계값의 예가 나와 있습니다.



참고 이 표의 값은 예시입니다. 이 정보를 사용하여 여기에 표시된 설치된 RAM과 일치하지 않는 디바이스에 대한 임계값을 추정할 수 있습니다. 또는 더 정확한 임계값 계산을 위해 Cisco TAC에 문의할 수 있습니다.

표 1: 설치된 RAM 기반 메모리 사용량 임계값

사용자 입력 임계값	설치된 메모리당 시행된 임계값(RAM)			
	4GB	6 GB	32GB	48GB
10%	10%	34%	72%	81%
20%	20%	41%	75%	83%
30%	30%	48%	78%	85%
40%	40%	56%	81%	88%
50%	50%	63%	84%	90%
60%	60%	70%	88%	92%
70%	70%	78%	91%	94%
80%	80%	85%	94%	96%
90%	90%	93%	97%	98%
100%	100%	100%	100%	100%

이벤트 상태 모니터 알림의 디스크 사용량 및 소모

디스크 사용량 상태 모듈은 매니지드 디바이스의 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.

이 주제에서는 디스크 사용량 상태 모듈에서 생성되는 두 가지 상태 경고에 대한 증상 및 문제 해결 지침에 대해 설명합니다.

- 이벤트의 빈번한 드레인
- 처리되지 않은 이벤트의 드레인

디스크 관리자 프로세스는 디바이스의 디스크 사용량을 관리합니다. 디스크 관리자가 모니터링하는 각 파일 유형에는 사일로가 할당됩니다. 시스템에서 사용 가능한 디스크 공간의 양에 따라 디스크 관리자는 각 사일로에 대해 HWM(상위 워터마크) 및 LWM(하위 워터마크)을 계산합니다.

시스템의 각 부분(silo, LWM 및 HWM 등)에 대한 자세한 디스크 사용량 정보를 표시하려면 **show disk-manager** 명령을 사용합니다.

예

다음은 디스크 관리자 정보의 예입니다.

```
> show disk-manager
Silo                               Used           Minimum       Maximum
Temporary Files                    0 KB           499.197 MB   1.950 GB
Action Queue Results                0 KB           499.197 MB   1.950 GB
User Identity Events                0 KB           499.197 MB   1.950 GB
UI Caches                           4 KB           1.462 GB     2.925 GB
Backups                             0 KB           3.900 GB     9.750 GB
Updates                             0 KB           5.850 GB     14.625 GB
Other Detection Engine              0 KB           2.925 GB     5.850 GB
Performance Statistics              33 KB          998.395 MB   11.700 GB
Other Events                        0 KB           1.950 GB     3.900 GB
IP Reputation & URL Filtering        0 KB           2.437 GB     4.875 GB
Archives & Cores & File Logs        0 KB           3.900 GB     19.500 GB
Unified Low Priority Events          1.329 MB       4.875 GB     24.375 GB
RNA Events                          0 KB           3.900 GB     15.600 GB
File Capture                        0 KB           9.750 GB     19.500 GB
Unified High Priority Events         0 KB           14.625 GB    34.125 GB
IPS Events                          0 KB           11.700 GB    29.250 GB
```

상태 알림 형식

FMC의 상태 모니터 프로세스가 실행되면(5분마다 또는 수동 실행이 트리거될 때) 디스크 사용량 모음이 `diskmanager.log` 파일을 살펴보고 올바른 조건이 충족되면 해당 상태 알림이 트리거됩니다.

이러한 상태 알림의 구조는 다음과 같습니다.

- <사일로 이름>의 빈번한 드레인
- <사일로 이름>에서 처리되지 않은 이벤트의 드레인

예를 들면 다음과 같습니다.

- 낮은 우선순위 이벤트의 빈번한 드레인
- 낮은 우선순위 이벤트에서 처리되지 않은 이벤트의 드레인

사일로에서 <사일로 이름>의 빈번한 드레인 상태 알림을 생성할 수 있습니다. 그러나 이벤트와 관련된 알림이 가장 일반적으로 표시됩니다. 이벤트 사일로 중에는 이러한 유형의 이벤트가 디바이스에서 더욱 빈번하게 생성되므로 낮은 우선순위 이벤트가 자주 표시됩니다.

<사일로 이름>의 빈번한 드레인 이벤트는 이벤트가 FMC로 전송되도록 대기하기 때문에 이벤트 관련 사일로에 대해서 표시할 때 **Warning**(경고) 심각도 레벨을 갖습니다. 백업 사일로와 같이 이벤트와 관련이 없는 사일로의 경우, 이 정보가 손실되므로 경고의 심각도는 **Critical**(중대)입니다.



중요 이벤트 사일로만이 <사일로 이름>에서 처리되지 않은 이벤트의 드레인 상태 알림을 생성합니다. 이 알림의 심각도 레벨은 항상 **Critical**(중대)입니다.

알림 외에 추가 증상은 다음과 같습니다.

- FMC 사용자 인터페이스의 속도 저하
- 이벤트 손실

일반적인 문제 해결 시나리오

<사일로 이름>의 빈번한 드레인 이벤트가 그 크기로 인해 사일로에 너무 많이 입력되어 발생합니다. 이 경우, 디스크 관리자는 마지막 5분 간격으로 해당 파일을 두 번 이상 비우거나 제거합니다. 이벤트 유형 사일로에서 이는 일반적으로 해당 이벤트 유형의 과도한 로깅으로 인해 발생합니다.

<사일로 이름>의 처리되지 않은 이벤트의 드레인 상태 알림의 경우, 이벤트 처리 경로의 병목 현상으로 인해 발생할 수도 있습니다.

이러한 디스크 사용량 알림과 관련하여 발생 가능한 세 가지 병목 현상이 있습니다.

- 과도한 로깅 - FTD의 EventHandler 프로세스가 초과 서브스크립션됩니다(Snort가 쓰는 것보다 느리게 읽음).
- Sftunnel 병목 현상 - Eventing 인터페이스가 불안정하거나 초과 서브스크립션됩니다.
- SFDataCorrelator 병목 현상 - FMC와 매니지드 디바이스 간의 데이터 전송 채널이 초과 서브스크립션됩니다.

과도한 로깅

이 유형의 상태 알림의 가장 일반적인 원인 중 하나는 과도한 입력입니다. **show disk-manager** 명령에서 수집한 LWM(하위 워터마크)과 HWM(상위 워터마크)의 차이점은 LWM(새로 드레인됨)에서 HWM 값으로 이동하기 위해 해당 사일로에서 사용할 수 있는 공간의 양을 나타냅니다. 처리되지 않은 이벤트의 유무에 관계없이 이벤트가 자주 비워지는 경우, 로깅 설정을 가장 먼저 검토해야 합니다.

- 이중 로깅 확인 - FMC에서 상관기 *perfstats*를 보면 이중 로깅 시나리오를 확인할 수 있습니다.

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
```

- ACP에 대한 로깅 설정 확인 - ACP(Access Control Policy, 액세스 제어 정책)의 로깅 설정을 검토합니다. 연결의 "시작" 및 "종료"를 모두 로깅하는 경우, 시작을 기록할 때 포함된 모든 항목을 포함하고 이벤트의 양을 줄이므로 종료만 기록합니다.

[연결 로깅 모범 사례](#)에 설명된 모범 사례를 따라야 합니다.

통신 병목 현상 - Sftunnel

sftunnel은 FMC와 매니지드 디바이스 간의 암호화된 통신을 담당합니다. 이벤트는 터널을 통해 FMC로 전송됩니다. 매니지드 디바이스와 FMC 간의 통신 채널(sftunnel)에서 연결 문제 및/또는 불안정은 다음과 같은 원인으로 발생할 수 있습니다.

- sftunnel이 다운되었거나 불안정합니다(플랩).

FMC와 매니지드 디바이스가 TCP 포트 8305의 관리 인터페이스 간에 연결 가능한지 확인합니다.

sftunnel 프로세스는 안정적이어야 하며 예기치 않게 재시작되지 않아야 합니다. `/var/log/message` 파일을 점검하여 이를 확인하고 *sftunneld* 문자열이 포함된 메시지를 검색합니다.

- sftunnel이 초과 서브스크립션되었습니다.

상태 모니터에서 추세 데이터를 검토하고 관리 트래픽이 급증하거나 지속적인 초과 서브스크립션이 될 수 있는 FMC 관리 인터페이스의 초과 서브스크립션 징후를 확인합니다.

Firepower 이벤트를 위한 보조 관리 인터페이스로 사용합니다. 이 인터페이스를 사용하려면 **configure network management-interface** 명령을 사용하여 FTD CLI에서 해당 IP 주소 및 기타 매개변수를 구성해야 합니다.

통신 병목 현상 - SFDataCorrelator

SFDataCorrelator는 FMC와 매니지드 디바이스 간의 데이터 전송을 관리합니다. FMC는 시스템에서 생성된 이진 파일을 분석하여 이벤트, 연결 데이터 및 네트워크 맵을 생성합니다. 첫 번째 단계는 **diskmanager.log** 파일에서 다음과 같이 수집할 중요한 정보를 검토하는 것입니다.

- 드레인의 빈도
- 처리되지 않은 이벤트가 드레인된 파일의 수
- 처리되지 않은 이벤트가 있는 드레인의 발생

디스크 관리자 프로세스가 실행될 때마다 `[/ngfw]/var/log/diskmanager.log`에 있는 자체 로그 파일에서 각기 다른 사일로에 대한 항목을 생성합니다. `diskmanager.log`에서 수집한 정보(CSV 형식)를 사용하면 원인을 찾는 범위를 좁힐 수 있습니다.

추가 문제 해결 단계:

- **stats_unified.pl** 명령을 사용하면 매니지드 디바이스에 FMC로 전송해야 하는 데이터가 있는지 확인할 수 있습니다. 이 상태는 매니지드 디바이스와 FMC에 연결 문제가 있을 때 발생할 수 있습니다. 매니지드 디바이스는 로그 데이터를 하드 드라이브에 저장합니다.

```
admin@FMC:~$ sudo stats_unified.pl
```

- **manage_proc.pl** 명령은 FMC 측의 상관기를 재설정할 수 있습니다.

```
root@FMC:~# manage_procs.pl
```

Cisco TAC(Technical Assistance Center)에 연락하기 전에

Cisco TAC에 연락하기 전에 다음 항목을 수집하는 것이 좋습니다.

- 표시되는 상태 알림의 스크린샷
- FMC에서 생성된 문제 해결 파일
- 영향을 받는 매니지드 디바이스에서 생성된 문제 해결 파일
문제가 처음 확인된 날짜 및 시간
- 정책에 적용된 최근 변경 사항에 대한 정보(해당되는 경우)

통신 병목 현상 - SFDataCorrelator, 12 페이지에 설명된 `stats_unified.pl` 명령의 출력

문제 해결을 위한 상태 모니터 보고서

경우에 따라 어플라이언스에 문제가 발생하면 support(지원팀)가 문제 진단에 도움이 될 수 있도록 문제 해결 파일을 생성하도록 요청할 수 있습니다. 아래 표에 나열된 옵션 중 하나를 선택하여 상태 모니터가 보고하는 문제 해결 데이터를 맞춤화할 수 있습니다.

일부 옵션은 보고하는 데이터의 측면에서 겹치지만, 문제 해결 파일은 선택하는 옵션에 관계없이 중복된 사본을 포함하지 않는다는 점에 유의하십시오.

표 2: 선택 가능한 문제 해결 옵션

옵션	보고 내용
Snort 성능 및 구성	어플라이언스의 Snort에 관련된 데이터 및 구성 설정
하드웨어 성능 및 로그	어플라이언스 하드웨어의 성능에 관련된 데이터 및 로그
시스템 구성, 정책 및 로그	어플라이언스의 현재 시스템 구성에 관련된 구성 설정, 데이터 및 로그
탐지 구성, 정책 및 로그	어플라이언스의 탐지에 관련된 구성 설정, 데이터 및 로그
인터페이스 및 네트워크 관련 데이터	어플라이언스의 인라인 집합 및 네트워크 구성에 관련된 구성 설정, 데이터 및 로그
검색, 인식, VDB 데이터 및 로그	어플라이언스의 현재 검색 및 인식 구성에 관련된 구성 설정, 데이터 및 로그
데이터 및 로그 업그레이드	어플라이언스의 이전 업그레이드와 관련된 데이터 및 로그
모든 데이터베이스 데이터	문제 해결 보고서에 포함된 모든 데이터베이스 관련 데이터
모든 로그 데이터	어플라이언스 데이터베이스에 의해 수집된 모든 로그
네트워크 맵 정보	현재 네트워크 토폴로지 데이터

특정 시스템 기능에 대한 문제 해결 파일 생성

지원 시 전송할 수 있는 맞춤 문제 해결 파일을 생성 및 다운로드할 수 있습니다.

다중 도메인을 구축한 경우, 하위 도메인의 디바이스에서 문제 해결 파일을 생성하고 다운로드할 수 있습니다.



주의 메모리가 적은 디바이스에서 문제 해결 파일을 생성하는 경우 자동 애플리케이션 우회(AAB)가 활성화되어 있는 경우 AAB가 발생할 수 있습니다. 적어도 AAB가 작동하면 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 [Snort® 재시작 트래픽 동작](#)을 참고하십시오. 일부 경우에는 AAB가 작동하여 디바이스가 일시적으로 동작하지 않을 수 있습니다. 만약 동작 정지 상태가 지속되면 Cisco TAC(Technical Assistance Center)에 문의할 경우 구축 시 적절한 솔루션을 제시할 것입니다. 영향을 받기 쉬운 디바이스에는 Firepower 7010, 7020 및 7030, 5508-X, 5516-X NGIPSv가 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 유지 보수, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자여야 합니다.

프로시저

단계 1 [디바이스 상태 모니터 보기](#)의 단계를 수행합니다.

단계 2 **Generate Troubleshooting Files**(문제 해결 파일 생성)를 클릭합니다.

단계 3 모든 생성 가능한 문제 해결 날짜의 파일을 생성하려면 모든 데이터를 선택하거나 [작업 메시지 보기](#)의 설명에 따라 개별 상자를 체크합니다.

단계 4 **OK**(확인)를 클릭합니다.

단계 5 Message Center에서 작업 메시지를 확인하려면 [작업 메시지 보기](#)를 참고하십시오.

단계 6 사용자가 생성한 문제 해결 파일에 해당하는 작업을 찾습니다.

단계 7 어플라이언스가 문제 해결 파일을 생성하고 작업 상태가 Completed(완료)로 변경된 후 **Click to retrieve generated files**(생성된 파일을 검색하려면 클릭)를 클릭합니다.

단계 8 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다.(문제 해결 파일은 단일 .tar.gz 파일에 다운로드 됩니다.)

단계 9 Cisco에 문제 해결 파일을 보내려면 Support(지원팀)의 지시에 따르십시오.

고급 문제 해결 파일 다운로드

다중 도메인을 구축한 경우, 하위 도메인의 디바이스에서 문제 해결 파일을 생성하고 다운로드할 수 있습니다. 파일의 다운로드 는 글로벌 도메인의 Firepower Management Center에서만 할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 유지 보수, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자여야 합니다.

프로시저

단계 1 어플라이언스의 상태 모니터를 보려면 [디바이스 상태 모니터 보기](#)을 참고하십시오.

단계 2 **Advanced Troubleshooting**(고급 문제 해결)을 클릭하십시오.

단계 3 **File Download**(파일 다운로드)에서 지원팀이 제공한 파일 이름을 입력합니다.

단계 4 **Download**(다운로드)를 클릭합니다.

단계 5 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다.

참고 매니지드 디바이스의 경우, 시스템 이름 앞에 장치 이름을 추가하여 파일의 이름을 바꿉니다.

단계 6 Cisco에 문제 해결 파일을 보내려면 **Support**(지원팀)의 지시에 따르십시오.

일반 문제 해결

내부 전원 장애(하드웨어 장애, 전원 서지) 또는 외부 전원 장애(플러그 뽑힘)로 인해 예기치 않은 시스템 셧다운 또는 재부팅이 발생할 수 있습니다. 이러한 경우 결국 데이터 손상이 발생할 수 있습니다.

연결 기반 문제 해결

연결 기반 문제 해결 또는 디버깅은 특정 연결에 대한 적절한 로그를 수집하기 위해 모듈에 균일한 디버깅을 제공합니다. 또한 최대 레벨 7까지 레벨 기반 디버깅을 지원하고 액세스 모듈에 대한 균일한 로그 수집 메커니즘을 활성화합니다. 연결 기반 디버깅은 다음을 지원합니다.

- Firepower Threat Defense에서 문제를 해결하는 공통 연결 기반 디버깅 하위 시스템
- 모듈에서 일관된 디버그 메시지 형식
- 재부팅에서 지속적인 디버그 메시지
- 모듈에서 기존 연결 기반 엔드 투 엔드 디버깅
- 진행 중인 연결 디버깅



참고 연결 기반 디버깅은 Firepower 2100 시리즈 디바이스에서는 지원되지 않습니다.

문제 해결 연결에 대한 자세한 내용은 [연결 문제 해결](#), 16 페이지를 참조하십시오.

연결 문제 해결

프로시저

단계 1 **debug packet-condition** 명령을 사용하여 연결을 식별하는 필터를 구성합니다.

예:

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

단계 2 관심 있는 모듈 및 해당 레벨에 대한 디버그를 활성화합니다. **debug packet** 명령을 사용합니다.

예:

```
Debug packet acl 5
```

단계 3 다음 명령을 사용하여 패킷 디버깅을 시작합니다.

```
debug packet-start
```

단계 4 다음 명령을 사용하여 데이터베이스에서 디버그 메시지를 가져오고 디버그 메시지를 분석합니다.

```
show packet-debuggs
```

단계 5 다음 명령을 사용하여 패킷 디버깅을 중지합니다.

```
debug packet-stop
```

Firepower Threat Defense 디바이스의 고급 문제 해결

Firepower Threat Defense 디바이스의 자세한 문제 해결 분석을 수행하기 위해 패킷 트레이서 및 패킷 캡처 기능을 사용할 수 있습니다. 패킷 트레이서는 방화벽 관리자가 가상 패킷을 보안 어플라이언스에 삽입하고 인그레스에서 이그레스로의 흐름을 추적하도록 합니다. 그 과정에서 패킷은 흐름 및 경로 조회, ACL, 프로토콜 검사, NAT, 침입 탐지에 대해 평가됩니다. 유틸리티 전원은 프로토콜 및 포트 정보로 소스 및 대상 주소를 지정하여 실제 트래픽을 시뮬레이션하는 기능에서 가져옵니다. 패킷 캡처는 패킷의 성공 실패 판정을 제공하는 추적 옵션을 통해 사용 가능합니다.

문제 해결 파일에 대한 자세한 내용은 [고급 문제 해결 파일 다운로드, 14 페이지](#)의 내용을 참조하십시오.

웹 인터페이스에서 FTD CLI 사용

Firepower Management Center 웹 인터페이스에서 선택한 FTD 명령줄 인터페이스(CLI)를 실행할 수 있습니다. 이러한 명령은 **ping**, **packet-tracer**, **traceroute** 및 **show(show history** 및 **show banner** 제외)입니다.

다중 도메인 구축 시 하위 도메인에서 관리되는 디바이스를 위한 Firepower Management Center 웹 인터페이스를 통해 FTD CLI 명령을 입력할 수 있습니다.



참고 Firepower Management Center의 고가용성을 활용한 배포의 경우 이 기능은 활성화된 Firepower Management Center에서만 사용할 수 있습니다.

FTD CLI에 대한 자세한 정보는, *Firepower Threat Defense*용 명령 참조 가이드를 참조하십시오.

시작하기 전에

CLI를 사용하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 1 어플라이언스의 상태 모니터를 보려면 [디바이스 상태 모니터 보기](#)을 참고하십시오.

단계 2 **Advanced Troubleshooting**(고급 문제 해결)을 클릭하십시오.

단계 3 **Threat Defense CLI**(위협 방어 CLI)를 클릭합니다.

단계 4 **Command**(명령) 드롭다운 목록에서 명령을 선택합니다.

단계 5 선택 사항으로 매개 변수 텍스트 상자에 명령 매개 변수를 입력할 수도 있습니다.

단계 6 명령 출력을 보려면 **Execute**(실행)를 클릭합니다.

기능별 문제 해결

기능 관련 문제 해결 팁과 기술은 다음 표를 참조하십시오.

표 3: 기능 관련 문제 해결 주제

기능	관련 문제 해결 정보
애플리케이션 제어	애플리케이션 제어 규칙 문제 해결
LDAP 외부 인증	LDAP 인증 연결 문제 해결 LDAP 인증 연결 문제 해결
라이선싱	FTD 라이선싱 문제 해결 특정 라이선스 예약 문제 해결
FMC 고가용성	Firepower Management Center 고가용성 문제 해결
7000 및 8000 Series 디바이스 고가용성 상태 공유	문제 해결을 위한 디바이스 고가용성 상태 공유 통계
사용자 규칙 조건	사용자 제어 문제 해결

기능	관련 문제 해결 정보
사용자 ID 소스	ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결 캡티브 포털(captive portal) ID 소스 문제 해결 원격 액세스 VPN ID 소스 문제 해결 LDAP 인증 연결 문제 해결 LDAP 인증 연결 문제 해결
영역 및 사용자 데이터 다운로드	영역 및 사용자 다운로드 문제 해결
네트워크 검색	네트워크 검색 전략 문제 해결
SSL 규칙	TLS/SSL 규칙 문제 해결
Firepower Threat Defense syslog	시스템 로그 구성 관련 정보
침입 성능 통계	침입 성능 통계 로깅 구성
7000 및 8000 Series NGIPSv ASA 및 FirePOWER Services	generate-troubleshoot (명령줄 인터페이스(CLI)의 명령)
연결 기반 문제 해결	연결 기반 문제 해결, 15 페이지