FMC 미처리 이벤트의 드레이닝(Drain) 문제 해결 및 이벤트 자주 드레이닝(Drain) 상태 모니터 알림

목차

소개

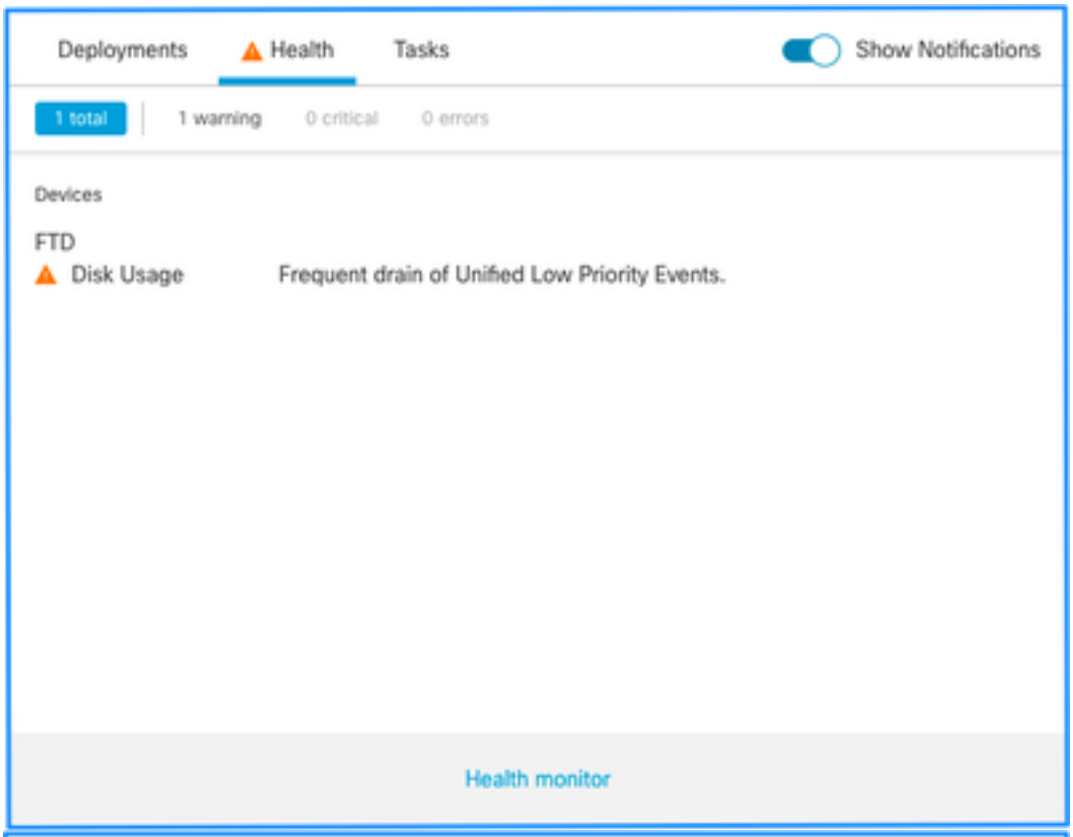
이 문서에서는 FMC(Firepower Management Center)**에서 처리되지 않은 이벤트**의 **드레이닝(Drain)** 및 **이벤트** 상태 알림의 빈번한 드레이닝을 트러블슈팅하는 방법에 대해 설명합니다.

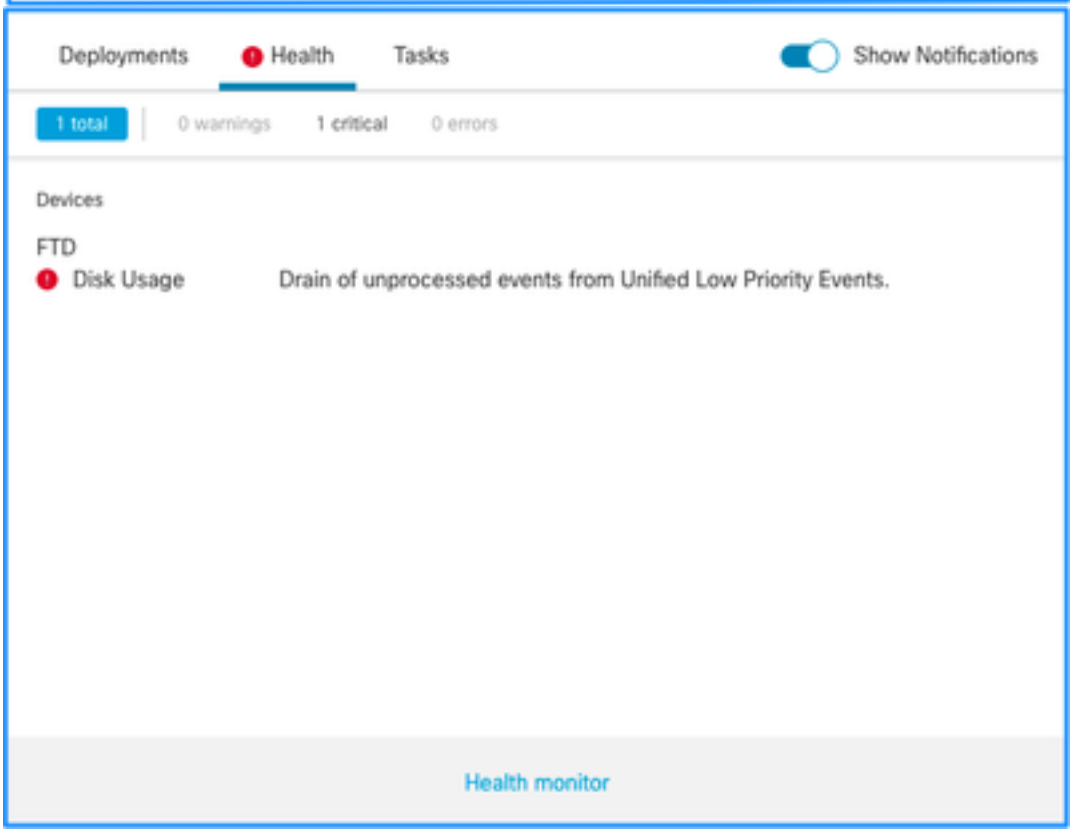
문제 개요

FMC는 다음 상태 알림 중 하나를 생성합니다.

- Unified Low Priority 이벤트의 잦은 삭제
  및/또는
- Unified Low Priority Events에서 처리되지 않은 이벤트 드레이닝

이러한 이벤트는 FMC에서 생성되고 표시되지만 FTD(Firepower Threat Defense) 디바이스인지 NGIPS(Next-Generation Intrusion Prevention System) 디바이스인지 여부에 관계없이 관리되는 디바이스 센서와 관련됩니다. 본 문서의 나머지 부분에서, 센서라는 용어는 달리 명시되지 않는 한 FTD 및 NGIPS 장치를 모두 나타냅니다.





상태 알림 구조입니다.

- <SILO NAME>의 빈번한 드레인
- <SILO NAME>에서 처리되지 않은 이벤트 제거

이 예에서 SILO NAME은 **Unified Low Priority Events입니다**. 디스크 관리자 사일로 중 하나입니다 (자세한 설명은 배경 정보 섹션 참조).

또한

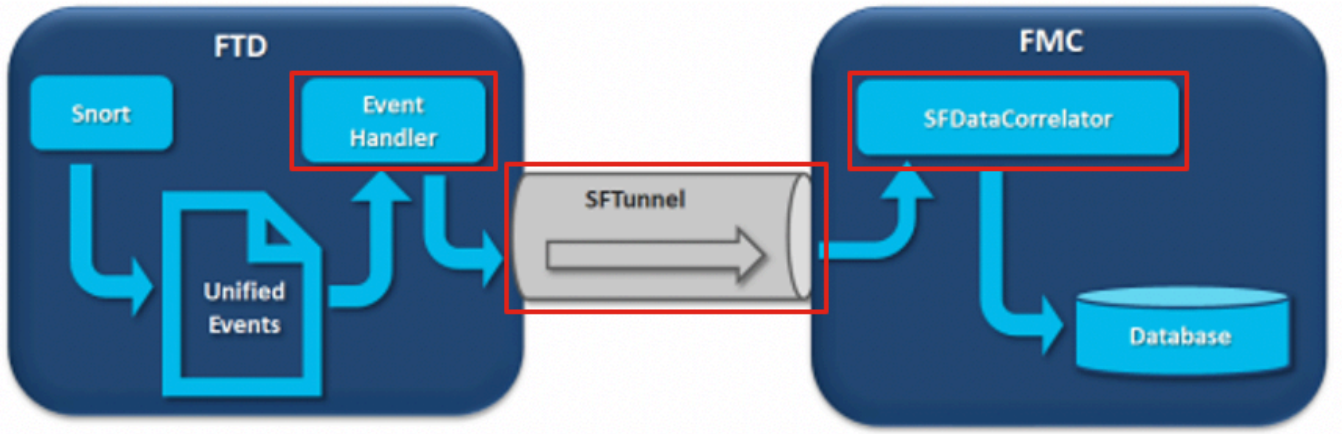
- 기술적으로 모든 사일로가 <SILO NAME> 상태 알림의 Frequent drain을 생성할 수 있지만, 가장 일반적으로 나타나는 이벤트는 이벤트와 관련된 이벤트이며, 그 중에서도 Low Priority Events는 센서에서 더 자주 생성되는 이벤트 유형이기 때문입니다.
- "Frequent drain of <SILO NAME>" 이벤트는 이벤트 관련 사일로인 경우 경고 심각도가 있습니다. 이 이벤트가 처리된 경우(처리되지 않은 이벤트를 구성하는 내용에 대한 설명이 다음에 제공됨) FMC 데이터베이스에 있기 때문입니다.
- "백업" 사일로와 같은 비이벤트 관련 사일로의 경우 이 정보가 손실되므로 알림은 Critical입니다.
- 이벤트 유형 사일로만 <SILO NAME> 상태 알림에서 처리되지 않은 이벤트의 Drain을 생성합니다. 이 경고에는 항상 Critical 심각도가 있습니다.

추가 증상은 다음과 같습니다.

- FMC UI의 느림
- 이벤트 손실

일반적인 문제 해결 시나리오

<SILO NAME> 이벤트의 잦은 삭제는 해당 크기에 비해 사일로에 너무 많은 입력이 입력되었기 때문입니다. 이 경우 디스크 관리자는 최근 5분 간격 동안 해당 파일을 두 번 이상 드레이닝(제거)합니다. 이벤트 유형 사일로에서는 일반적으로 해당 이벤트 유형의 과도한 로깅이 원인입니다. <SILO NAME> 상태 알림의 처리되지 않은 이벤트 드레이닝의 경우 이벤트 처리 경로의 병목 현상 때문일 수도 있습니다.



다이어그램에는 3가지 잠재적 병목 현상이 있습니다.

- FTD의 EventHandler 프로세스가 오버서브스크립션됩니다(Snort가 기록하는 것보다 느리게 읽음).
- 이벤트 인터페이스가 오버서브스크립션되었습니다.
- FMC의 SFDataCorrelator 프로세스가 오버서브스크립션되었습니다.

이벤트 처리 아키텍처에 대해 자세히 알아보려면 해당 Deep Dive 섹션을 참조하십시오.

사례 1. 과도한 로깅

앞 절에서 언급했듯이, 이러한 유형의 상태 알림에 대한 가장 일반적인 원인 중 하나는 과도한 입력이다.

show disk-manager CLISH 명령에서 수집한 LWM(Low Water Mark)과 HWM(High Water Mark)의 차이는 사일로에서 LWM(새로 배출됨)에서 HWM 값으로 이동하기 위해 필요한 공간의 양을 보여줍니다. 처리되지 않은 이벤트가 있거나 없는 이벤트가 자주 발생하는 경우 먼저 로깅 컨피그레이션을 검토해야 합니다.

디스크 관리자 프로세스에 대한 자세한 설명은 해당 Deep Dive 섹션을 참조하십시오.

이중 로깅이든 전체 관리자-센서 에코시스템에서 높은 이벤트 비율이든 로깅 설정에 대한 검토가 이루어져야 합니다.

권장 작업

1단계. 이중 로깅 확인

이 출력에 표시된 대로 FMC의 상관기 성능을 보면 이중 로깅 시나리오를 식별할 수 있습니다.

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
129 statistics lines read
                host limit:                     50000           0               50000
                pcnt host limit in use:         0.01            0.01            0.01
                rna events/second:              0.00            0.00            0.06
                user cpu time:                  0.48            0.21            10.09
                system cpu time:                0.47            0.00            8.83
                memory usage:                   2547304         0               2547304
                resident memory usage:          28201           0               49736
                 rna flows/second:               126.41          0.00            3844.16
                 rna dup flows/second:           69.71           0.00            2181.81
                 ids alerts/second:              0.00            0.00            0.00
                ids packets/second:             0.00            0.00            0.00
                ids comm records/second:        0.02            0.01            0.03
                ids extras/second:              0.00            0.00            0.00
                fw_stats/second:                0.00            0.00            0.03
                user logins/second:             0.00            0.00            0.00
                file events/second:             0.00            0.00            0.00
                malware events/second:          0.00            0.00            0.00
                fireamp events/second:          0.00            0.00            0.00
```

이 경우, 높은 비율의 중복 흐름을 출력에서 볼 수 있다.

2단계. ACP의 로깅 설정 검토

ACP(액세스 제어 정책)의 로깅 설정 검토부터 시작해야 합니다. 이 문서에 설명된 연결 로깅 모범 사례에 따른 모범 사례를 따르십시오

나열된 권장 사항은 이중 로깅 시나리오만 다루지 않으므로 모든 상황에서 로깅 설정을 검토하는 것이 좋습니다.

3단계. 과도한 로깅이 예상되는지 확인합니다.

과도한 로깅에 예상 원인이 있는지 여부를 검토해야 합니다. 과도한 로깅이 DOS/DDoS 공격 또는 라우팅 루프 또는 엄청난 수의 연결을 만드는 특정 애플리케이션/호스트에 의해 발생하는 경우 예기치 않은 과도한 연결 소스에서 연결을 확인하고 차단/중지해야 합니다.

4단계. 모델 업그레이드

FTD 하드웨어 디바이스를 고성능 모델(예: FPR2100 —> FPR4100)로 업그레이드하면 사일로의

소스가 증가합니다.

5단계. Log to Ramdisk(Ramdisk에 대한 로그)를 비활성화할 수 있는지 고려하십시오.

Unified Low Priority Events 사일로의 경우 Log to Ramdisk를 비활성화하여 해당 Deep Dive 섹션에서 설명한 단점으로 사일로 크기를 늘릴 수 있습니다.

사례 2. 센서와 FMC 간 통신 채널의 병목 현상

이러한 유형의 알림의 또 다른 일반적인 원인은 센서와 FMC 간의 통신 채널(sftunnel)에 연결 문제 및/또는 불안정성이 원인입니다. 커뮤니케이션 문제는 다음 때문일 수 있습니다.

- sftunnel이 다운되었거나 불안정합니다(flaps).
- sftunnel이 오버서브스크립션되었습니다.

sftunnel 연결 문제의 경우 FMC와 센서가 TCP 포트 8305의 관리 인터페이스 간에 연결할 수 있어야 합니다.

FTD에서 **[/ngfw]**/var/**log/messages 파일**에서 **sftunneled 문자열을** 검색할 수 있습니다. 연결 문제로 인해 다음과 같은 메시지가 생성됩니다.

```
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_ch_util [INFO] Delay for heartbeat
reply on channel from 10.62.148.75 for 609 seconds. dropChannel...
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_connections [INFO] Ping Event
Channel for 10.62.148.75 failed
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState
dropChannel peer 10.62.148.75 / channelB / EVENT [ msgSock2 & ssl_context2 ] <<
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState
freeChannel peer 10.62.148.75 / channelB / DROPPED [ msgSock2 & ssl_context2 ] <<
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_connections [INFO] Need to send SW
version and Published Services to 10.62.148.75
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_peers [INFO] Confirm RPC service in
CONTROL channel
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState
do_dataio_for_heartbeat peer 10.62.148.75 / channelA / CONTROL [ msgSock & ssl_context ] <<
Sep  9 15:41:48 firepower SF-IMS[5458]: [5464] sftunneld:tunnsockets [INFO] Started listening on
port 8305 IPv4(10.62.148.180) management0
Sep  9 15:41:51 firepower SF-IMS[5458]: [27602] sftunneld:control_services [INFO] Successfully
Send Interfaces info to peer 10.62.148.75 over managemen
Sep  9 15:41:53 firepower SF-IMS[5458]: [5465] sftunneld:sf_connections [INFO] Start connection
to : 10.62.148.75 (wait 10 seconds is up)
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_peers [INFO] Peer 10.62.148.75
needs the second connection
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Interface management0 is
configured for events on this Device
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Connect to 10.62.148.75
on port 8305 - management0
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Initiate IPv4 connection
to 10.62.148.75 (via management0)
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Initiating IPv4
connection to 10.62.148.75:8305/tcp
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Wait to connect to 8305
(IPv6): 10.62.148.75
```

FMC 관리 인터페이스의 초과 서브스크립션은 관리 트래픽의 급증이거나 지속적인 초과 서브스크립션일 수 있습니다. Health Monitor의 기록 데이터는 이를 나타내는 좋은 지표입니다.

가장 먼저 주의할 점은 대부분의 경우 FMC는 관리를 위해 단일 NIC를 사용하여 구축된다는 것입니다. 이 인터페이스는 다음에 사용됩니다.

- FMC 관리.
- FMC 센서 관리.
- 센서에서 FMC 이벤트 수집.
- 인텔리전스 피드 업데이트
- 소프트웨어 다운로드 사이트에서 SRU, 소프트웨어, VDB 및 GeoDB 업데이트를 다운로드합니다.
- URL 평판 및 카테고리에 대한 쿼리(해당되는 경우).
- 파일 속성 쿼리(해당되는 경우)

권장 작업

이벤트 전용 인터페이스에 대해 FMC에 두 번째 NIC를 구축할 수 있습니다. 구현은 활용 사례에 따라 달라질 수 있습니다.

일반 지침은 FMC Hardware Guide Deploying on a Management Network(FMC 하드웨어 가이드 관리 네트워크에서 구축)에서 확인할 수 있습니다

사례 3. SFDataCorrelator 프로세스의 병목 현상

마지막으로 다룰 시나리오는 SFDataCorrelator측(FMC)에서 병목 현상이 발생하는 경우입니다.

첫 번째 단계는 다음과 같이 중요한 정보를 수집할 때 diskmanager.log 파일을 살펴보는 것입니다.

- 배수 빈도입니다.
- 처리되지 않은 이벤트가 제거된 파일 수입니다.
- 처리되지 않은 이벤트의 드레인 발생.

diskmanager.log 파일 및 파일 해석 방법에 대한 자세한 내용은 디스크 관리자 섹션을 참조하십시오. diskmanager.log에서 수집한 정보를 사용하여 후속 단계를 좁힐 수 있습니다.

또한 correlator 성능 통계를 확인해야 합니다.

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
129 statistics lines read
host limit: 50000 0 50000 pcnt host limit in use: 100.01 100.00 100.55 rna events/second: 1.78
0.00 48.65 user cpu time: 2.14 0.11 58.20 system cpu time: 1.74 0.00 41.13 memory usage: 5010148
0 5138904 resident memory usage: 757165 0 900792                    rna flows/second:
101.90           0.00             3388.23
                 rna dup flows/second:               0.00             0.00             0.00
                 ids alerts/second:                  0.00             0.00             0.00
                 ids packets/second:                 0.00             0.00             0.00
                 ids comm records/second:            0.02             0.01             0.03
                 ids extras/second:                  0.00             0.00             0.00
                 fw_stats/second:                    0.01             0.00             0.08
                 user logins/second:                 0.00             0.00             0.00
                 file events/second:                 0.00             0.00             0.00
                 malware events/second:              0.00             0.00             0.00
                 fireamp events/second:              0.00             0.00             0.01
```

이러한 통계는 FMC에 대한 것이며 FMC에서 관리하는 모든 센서의 집계에 해당합니다. Unified low priority 이벤트의 경우 주로 다음을 찾습니다.

- SFDataCorrelator 프로세스의 가능한 오버서브스크립션을 평가하기 위한 이벤트 유형의 초당 총 플로우 수입니다.
- 이전 출력에서 강조 표시된 두 행: **rna flows/second** - SFDataCorrelator에서 처리한 낮은 우선순위 이벤트의 비율을 나타냅니다.**rna dup flows/second** - SFDataCorrelator에서 처리한 중복 낮은 우선순위 이벤트의 비율을 나타냅니다. 이는 이전 시나리오에서 설명한 것처럼 이중 로깅에 의해 생성됩니다.

결과에 따라 다음과 같은 결론을 내릴 수 있습니다.

- rna 중복 플로우/두 번째 행에 표시된 것과 같은 중복 로깅은 없습니다.
- rna 흐름/두 번째 행에서 Maximum 값은 Average 값보다 훨씬 높으므로 SFDataCorrelator 프로세스에서 처리하는 이벤트 속도가 급증했습니다. 사용자 근무가 막 시작된 오늘 이른 아침의 모습을 보면 예상할 수 있는 일이지만, 대체로 적기이며 추가 조사가 필요하다.

SFDataCorrelator 프로세스에 대한 자세한 내용은 Event Processing(이벤트 처리) 섹션에서 확인할 수 있습니다.

권장 작업

우선, 언제 스파이크가 발생했는지 확인해야 한다. 이렇게 하려면 각 5분 샘플 간격당 상관기 통계를 확인해야 합니다. diskmanager.log에서 수집한 정보를 사용하여 중요한 기간으로 바로 이동할 수 있습니다.

> **팁:** 쉽게 검색할 수 있도록 출력을 Linux 호출기에 **적게** 파이프합니다.

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

<OUTPUT OMITTED FOR READABILITY>
Wed Sep 9 16:01:35 2020 host limit: 50000 pcnt host limit in use: 100.14 rna events/second:
24.33 user cpu time: 7.34 system cpu time: 5.66 memory usage: 5007832 resident memory usage:
797168  rna flows/second:              638.55
                rna dup flows/second:          0.00
                ids alerts/second:             0.00
                ids pkts/second:               0.00
                ids comm records/second:       0.02
                ids extras/second:             0.00
                fw stats/second:               0.00
                user logins/second:            0.00
                file events/second:            0.00
                malware events/second:         0.00
                fireAMP events/second:         0.00


Wed Sep  9 16:06:39 2020
                host limit:                    50000
                pcnt host limit in use:        100.03
                rna events/second:             28.69
                user cpu time:                 16.04
                system cpu time:               11.52
                memory usage:                  5007832
                resident memory usage:         801476
                rna flows/second:              685.65
                rna dup flows/second:          0.00
                ids alerts/second:             0.00
```

```
                ids pkts/second:              0.00
                ids comm records/second:      0.01
                ids extras/second:            0.00
                fw stats/second:              0.00
                user logins/second:           0.00
                file events/second:           0.00
                malware events/second:        0.00
                fireAMP events/second:        0.00

Wed Sep  9 16:11:42 2020
                host limit:                   50000
                pcnt host limit in use:       100.01
                rna events/second:            47.51
                user cpu time:                16.33
                system cpu time:              12.64
                memory usage:                 5007832
                resident memory usage:        809528
                rna flows/second:             1488.17
                rna dup flows/second:         0.00
                ids alerts/second:            0.00
                ids pkts/second:              0.00
                ids comm records/second:      0.02
                ids extras/second:            0.00
                fw stats/second:              0.01
                user logins/second:           0.00
                file events/second:           0.00
                malware events/second:        0.00
                fireAMP events/second:        0.00

Wed Sep  9 16:16:42 2020
                host limit:                   50000
                pcnt host limit in use:       100.00
                rna events/second:            8.57
                user cpu time:                58.20
                system cpu time:              41.13
                memory usage:                 5007832
                resident memory usage:        837732
                rna flows/second:             3388.23
                rna dup flows/second:         0.00
                ids alerts/second:            0.00
                ids pkts/second:              0.00
                ids comm records/second:      0.01
                ids extras/second:            0.00
                fw stats/second:              0.03
                user logins/second:           0.00
                file events/second:           0.00
                malware events/second:        0.00
                fireAMP events/second:        0.00

197 statistics lines read

                host limit:                   50000           0               50000
                pcnt host limit in use:       100.01          100.00          100.55
                rna events/second:            1.78            0.00            48.65
                user cpu time:                2.14            0.11            58.20
                system cpu time:              1.74            0.00            41.13
                memory usage:                 5010148         0               5138904
                resident memory usage:        757165          0               900792
                rna flows/second:             101.90          0.00            3388.23
                rna dup flows/second:         0.00            0.00            0.00
                ids alerts/second:            0.00            0.00            0.00
                ids packets/second:           0.00            0.00            0.00
                ids comm records/second:      0.02            0.01            0.03
                ids extras/second:            0.00            0.00            0.00
```

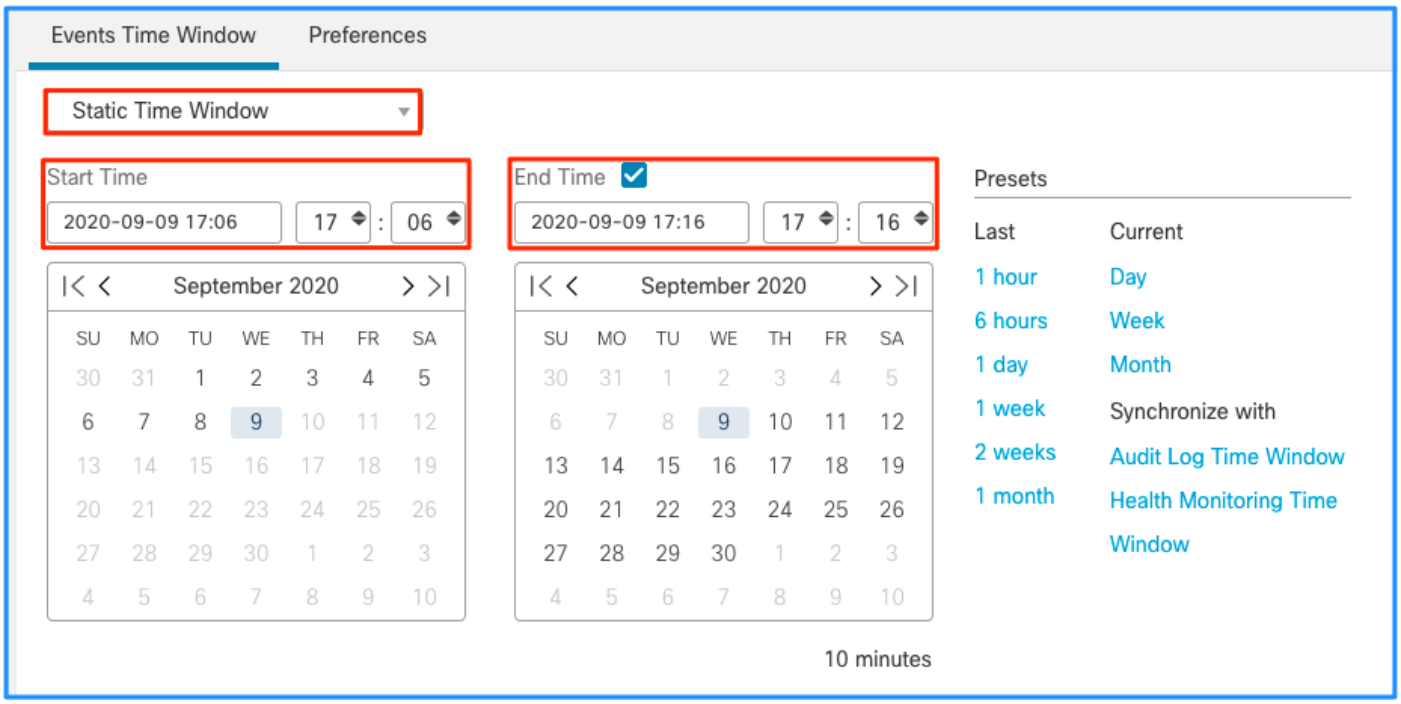
```
fw_stats/second:                0.01            0.00            0.08
user logins/second:             0.00            0.00            0.00
file events/second:             0.00            0.00            0.00
malware events/second:          0.00            0.00            0.00
fireamp events/second:          0.00            0.00            0.01
```

출력의 정보를 사용하여 다음을 수행할 수 있습니다.

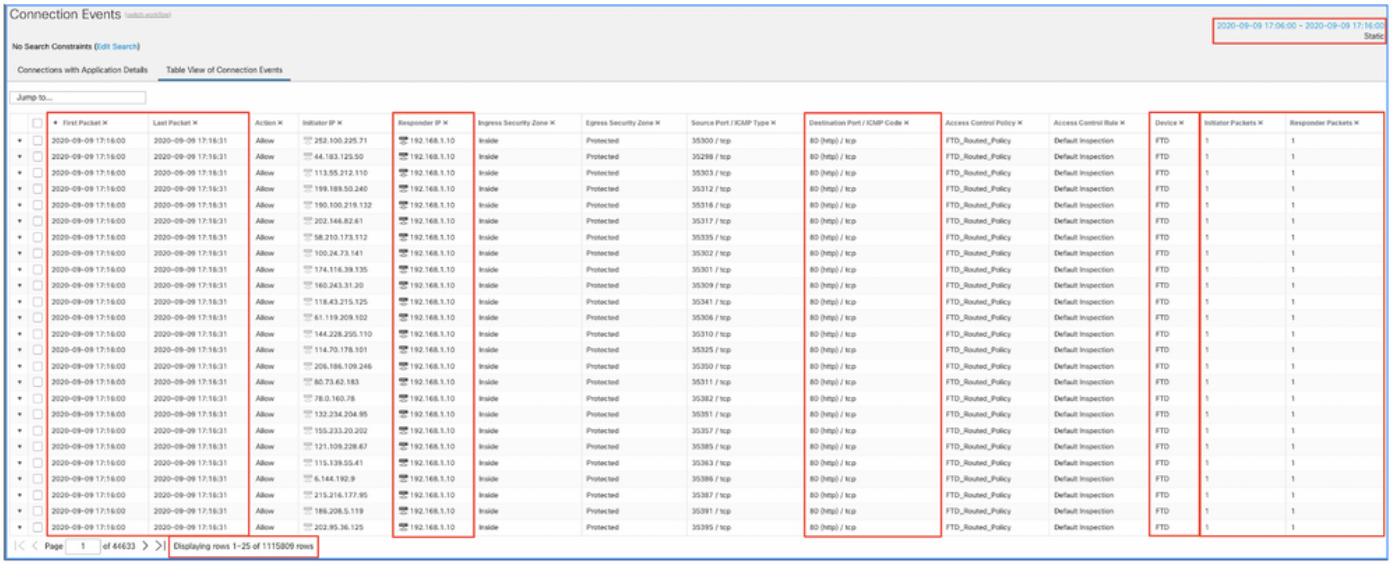
- 이벤트의 정상/기본 비율을 결정합니다.
- 스파이크가 발생한 5분 간격을 확인합니다.

이전 예에서는 16:06:39 이상에서 수신된 이벤트의 속도가 현저히 증가했습니다. 이 값은 5분 평균이므로 표시된 것보다 더 급격하게 증가할 수 있지만(버스트), 이 5분 간격에서 감소합니다(이 기간이 끝날 때까지 시작된 경우).

이로 인해 이벤트 급증으로 인해 처리되지 않은 이벤트가 Drain되었다는 결론이 내려지지만, 적절한 시간 창을 사용하여 FMC GUI(그래픽 사용자 인터페이스)에서 연결 이벤트를 확인하여 이 급증 시 FTD 상자를 통과한 연결의 유형을 파악할 수 있습니다.



필터링된 연결 이벤트를 가져오려면 이 시간 창을 적용하십시오. 시간대를 고려하십시오. 이 예에서는 센서가 UTC 및 FMC UTC+1을 사용합니다. 테이블 보기를 사용하여 이벤트 오버로드를 트리거한 이벤트를 보고 그에 따라 작업을 수행합니다.



타임스탬프(첫 번째 및 마지막 패킷의 시간)를 기반으로 이러한 연결은 수명이 짧은 연결임을 알 수 있습니다. 또한 Initiator 및 Responder Packets 열은 각 방향에서 교환된 패킷이 1개만 있음을 보여줍니다. 이는 연결이 단명하고 매우 적은 양의 데이터를 교환했음을 확인합니다.

또한 이러한 모든 플로우가 동일한 responder IP 및 포트를 대상으로 한다는 것도 확인할 수 있습니다. 또한 이러한 정보는 모두 동일한 센서에 의해 보고됩니다(인그레스 및 이그레스 인터페이스 정보와 함께 이 흐름의 위치와 방향을 말할 수 있음). 추가 작업:

- 대상 엔드포인트의 Syslog를 확인합니다.
- DOS/DDOS 보호를 구현하거나 기타 예방 조치를 취하십시오.

참고: 이 문서의 목적은 처리되지 않은 이벤트 드레이닝의 문제를 해결하기 위한 지침을 제공하는 것입니다. 이 예에서는 hping3을 사용하여 대상 서버에 대한 TCP SYN 플러드를 생성했습니다. FTD 디바이스 강화에 대한 지침은 Cisco Firepower Threat Defense 강화 가이드를 참조하십시오

Cisco TAC(Technical Assistance Center)에 문의하기 전에 수집할 항목

Cisco TAC에 문의하기 전에 이러한 항목을 수집하는 것이 좋습니다.

- 상태 알림의 스크린샷입니다.
- FMC에서 생성된 파일의 문제를 해결합니다.
- 영향을 받는 센서에서 생성된 파일의 문제를 해결합니다.
- 문제가 처음 발견된 날짜 및 시간입니다.
- 최근 정책 변경 사항 정보(해당되는 경우).
- 영향을 받는 센서에 대한 설명과 함께 이벤트 처리 섹션에 설명된 stats_unified.pl 명령의 출력.

심층 분석

이 섹션에서는 이러한 유형의 상태 알림에 참여할 수 있는 다양한 구성 요소에 대한 자세한 설명을 제공합니다. 여기에는 다음이 포함됩니다.

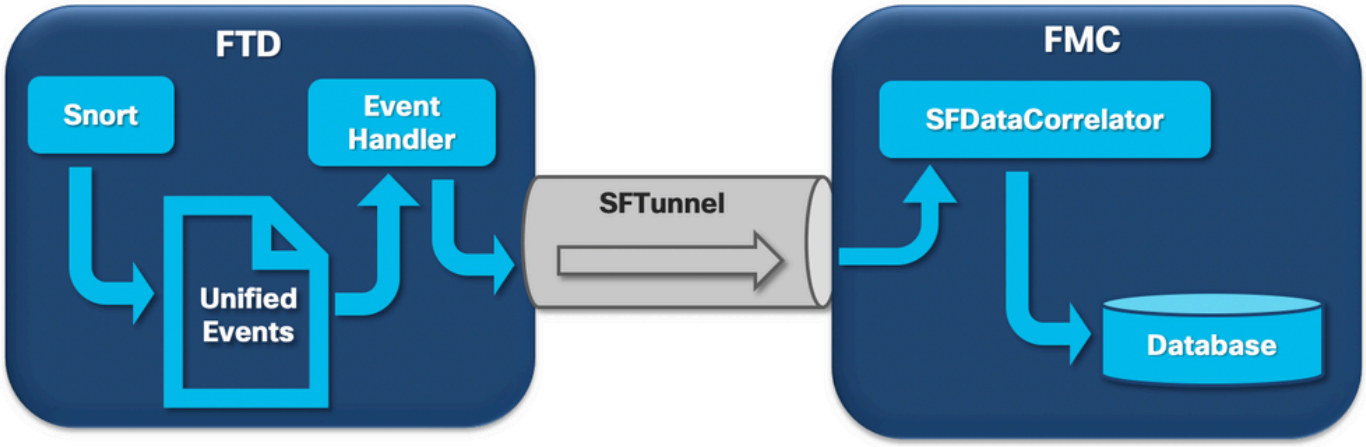
- Event Processing(이벤트 처리) - 센서 디바이스와 FMC 모두에서 발생하는 경로를 다룹니다. 이는 상태 알림이 이벤트 유형 사일로를 참조할 때 주로 유용합니다.

- Disk Manager - 디스크 관리자 프로세스, 사일로 및 해당 사일로 제거 방식을 다룹니다.
- Health Monitor - Health Monitor 모듈을 사용하여 상태 알림을 생성하는 방법을 다룹니다.
- Log to Ramdisk(Ramdisk에 로그 기록) - ramdisk에 대한 로깅 기능 및 상태 알림에 대한 잠재적 영향을 다룹니다.

Drain of Events 상태 알림을 이해하고 잠재적인 장애 지점을 파악하려면 이러한 구성 요소가 어떻게 작동하고 상호 작용하는지 살펴봐야 합니다.

이벤트 처리

Frequent Drain 유형의 상태 알림은 이벤트와 관련이 없는 사일로(silo)에 의해 트리거될 수 있지만, Cisco TAC에서 확인한 대부분의 케이스는 이벤트 관련 정보의 유출과 관련이 있습니다. 또한 처리되지 않은 이벤트의 소진을 구성하는 요소를 파악하려면 이벤트 처리 아키텍처와 이를 구성하는 구성 요소를 살펴보아야 합니다.



Firepower 센서가 새 연결에서 패킷을 수신하면 snort 프로세스는 이벤트를 더 빠르게 읽기/쓰기와 더 가벼운 이벤트를 허용하는 이진 형식인 unified2 형식으로 생성합니다.

출력에 FTD 명령 **시스템 지원 추적이 표시되며**, 여기에서 생성된 새 연결을 확인할 수 있습니다. 주요 부분은 강조 표시되어 설명합니다.

```
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3310981951
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Session: new snort session
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 new firewall session
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Inspection', action Allow and prefilter rule 0
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 HitCount data sent for rule id: 268437505,
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 allow action
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Default Inspection',
allow
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Snort id 0, NAP id 1, IPS id 0, Verdict PASS
```

Snort unified_events 파일은 **[/ngfw]var/sf/detection_engine/*/instance-N/경로**에서 인스턴스별로 생성됩니다. 여기서는 다음과 같습니다.

- *는 Snort UUID입니다. 이는 어플라이언스별로 고유합니다.
- N은 이전 출력에서 인스턴스 ID로 계산할 수 있는 Snort 인스턴스 ID입니다(예에서 강조 표시된 0) + 1

지정된 Snort 인스턴스 폴더에는 2가지 유형의 unified_events 파일이 있을 수 있습니다.

- unified_events-1(높은 우선순위 이벤트 포함).
- unified_events-2(낮은 우선순위 이벤트 포함).

우선순위가 높은 이벤트는 악성 연결에 해당하는 이벤트입니다.

이벤트 유형 및 우선 순위:

높은 우선 순위(1)	낮은 우선 순위 (2)
침입	연결
악성코드	검색
보안 인텔리전스	파일
관련 연결 이벤트	통계

다음 출력에서는 이전 예에서 추적한 새 연결에 속하는 이벤트를 보여 줍니다. 형식은 unified2이며 [/ngfw]/var/sf/detection_engine/*/instance-**1**/ 아래에 있는 각 통합 이벤트 로그의 출력에서 가져옵니다. 여기서 1은 이전 출력 +1에서 굵게 표시된 snort 인스턴스 id입니다. 통합 이벤트 로그 형식 이름은 unified_events-**2**.log.**159654750 구문을 따릅니다.** 여기서 2는 테이블에 표시된 이벤트 우선 순위를 나타내고 굵게 표시된 마지막 부분(**1599654750**)은 파일을 만든 시점의 타임스탬프(Unix 시간)입니다.

> **팁:** Linux **date** 명령을 사용하여 **Unix** 시간을 읽을 수 있는 날짜로 변환할 수 있습니다.
> admin@FP1120-2:~$ **sudo 날짜 -d@1599654750**
> 2020년 9월 9일 수요일 14:32:30 CEST

```
Unified2 Record at offset 2190389
Type: 210(0x000000d2)
Timestamp: 0
Length: 765 bytes
Forward to DC: Yes
FlowStats:
Sensor ID: 0
Service: 676
NetBIOS Domain: <none>
Client App: 909, Version: 1.20.3 (linux-gnu)
Protocol: TCP
Initiator Port: 42310
Responder Port: 80
First Packet: (1599662092) Tue Sep 9 14:34:52 2020
Last Packet: (1599662092) Tue Sep 9 14:34:52 2020

<OUTPUT OMITTED FOR READABILITY>

Initiator: 192.168.0.2
Responder: 192.168.1.10
Original Client: ::
Policy Revision: 00000000-0000-0000-0000-00005f502a92
Rule ID: 268437505
Tunnel Rule ID: 0
Monitor Rule ID: <none>
Rule Action: 2
```

모든 unified_events 파일과 함께 책갈피 파일이 있습니다. 여기에는 두 가지 중요한 값이 포함됩니다.

1. 해당 인스턴스 및 우선순위에 대한 현재 unified_events 파일의 타임스탬프 대응자입니다.
2. unified_event 파일에서 마지막 읽기 이벤트의 위치를 바이트 단위로 지정합니다.

값은 다음 예제와 같이 순서대로 쉼표로 구분됩니다.

```
root@FTD:/home/admin# cat /var/sf/detection_engines/d5a4d5d0-6ddf-11ea-b364-
2ac815c16717/instance-1/unified_events-2.log.bookmark.1a3d52e6-3e09-11ea-838f-68e7af919059
1599862498,   18754115
```

그러면 디스크 관리자 프로세스에서 어떤 이벤트가 이미 처리(FMC로 전송)되었고 어떤 이벤트가 처리되지 않았는지 알 수 있습니다.

디스크 관리자가 이벤트 사일로를 제거하면 통합 이벤트 파일이 제거됩니다. 사일로 방전에 대한 자세한 내용은 디스크 관리자 섹션을 참조하십시오.

다음 중 하나가 참인 경우 제거된 통합 파일에 처리되지 않은 이벤트가 있는 것으로 간주됩니다.

1. 책갈피 타임스탬프가 파일 생성 시간보다 낮습니다.
2. 책갈피 타임스탬프는 파일 생성 시간과 동일하며 파일에서 바이트 단위의 위치가 크기보다 작습니다.

EventHandler 프로세스는 통합 파일에서 이벤트를 읽고 sftunnel을 통해 메타데이터로 FMC에 스트리밍합니다. sftunnel은 센서와 FMC 간의 암호화된 통신을 담당하는 프로세스입니다. 이는 TCP 기반 연결이므로 FMC에서 이벤트 스트리밍을 승인합니다

[/ngfw]/var/log/messages 파일에서 다음 메시지를 볼 수 있습니다.

```
sfpreproc:OutputFile [INFO] *** Opening /ngfw/var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-
d428d53ed3ae/instance-1/unified_events-2.log.1597810478 for output" in /var/log/messages

EventHandler:SpoolIterator [INFO] Opened unified event file /var/sf/detection_engines/77d31ce2-
c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478

sftunneld:FileUtils [INFO] Processed 10334 events from log file
var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-
2.log.1597810478
```

이 출력은 다음 정보를 제공합니다.

- Snort가 출력을 위해 unified_events 파일을 열어 여기에 기록했습니다.
- 이벤트 처리기가 동일한 unified_events 파일을 열어 읽었습니다.
- sftunnel에서 해당 unified_events 파일에서 처리된 이벤트 수를 보고했습니다.

그런 다음 책갈피 파일이 그에 따라 업데이트됩니다. sftunnel은 우선 순위가 높은 이벤트와 낮은 이벤트에 각각 UE(Unified Events) Channel 0 및 1이라는 서로 다른 2개의 채널을 사용합니다.

FTD의 **sfunnel_status** CLI 명령을 사용하면 스트리밍된 이벤트의 수를 확인할 수 있습니다.

```
Priority UE Channel 1 service

TOTAL TRANSMITTED MESSAGES <530541> for UE Channel service
RECEIVED MESSAGES <424712> for UE Channel service
SEND MESSAGES <105829> for UE Channel service
FAILED MESSAGES <0> for UE Channel service
HALT REQUEST SEND COUNTER <17332> for UE Channel service
STORED MESSAGES for UE Channel service (service 0/peer 0)
STATE <Process messages> for UE Channel service
```

```
REQUESTED FOR REMOTE <Process messages> for UE Channel service
REQUESTED FROM REMOTE <Process messages> for UE Channel service
```

FMC에서 이벤트는 SFDataCorrelator 프로세스에 의해 수신됩니다.

각 센서에서 처리된 이벤트의 상태는 stats_unified.**pl 명령**으로 확인할 수 있습니다.

```
admin@FMC:~$ sudo stats_unified.pl
Current Time - Fri Sep 9 23:00:47 UTC 2020

******************************************************************************
* FTD - 60a0526e-6ddf-11ea-99fa-89a415c16717, version 6.6.0.1
******************************************************************************
 Channel Backlog Statistics (unified_event_backlog)
   Chan    Last Time              Bookmark Time          Bytes Behind
      0    2020-09-09 23:00:30    2020-09-07 10:41:50               0
      1    2020-09-09 23:00:30    2020-09-09 22:14:58            6960
```

이 명령은 채널당 특정 디바이스에 대한 이벤트 백로그의 상태를 표시합니다. 사용된 채널 ID는 sftunnel과 동일합니다.

Bytes Behind 값은 유니파이드 이벤트 북마크 파일에 표시된 위치와 유니파이드 이벤트 파일의 크기 및 북마크 파일보다 타임스탬프가 높은 후속 파일의 차이로서 계산될 수 있습니다.

SFDataCorrelator 프로세스는 성능 통계도 저장합니다. **/var/sf/rna/correlator-stats/에 저장됩니다**. 해당 날짜의 성능 통계를 CSV 형식으로 저장하기 위해 매일 파일 하나가 생성됩니다. 파일 이름은 "YYYY-MM-DD" 형식을 사용하며 현재 날짜에 해당하는 파일 Responder를 **now**라고 합니다.

통계는 5분마다 수집됩니다(5분 간격마다 한 줄이 있음).

이 파일의 출력은 perfstats 명령으로 읽을 **수** 있습니다. 이 명령은 snort 성능 통계 파일을 읽는 데에도 사용되므로 적절한 플래그를 사용해야 합니다.

-C: 입력이 correlator-stats 파일임을 perfstats에 지시합니다(이 플래그 perfstats가 없으면 입력이 snort 성능 통계 파일인 것으로 가정).

-q: 자동 모드 - 파일의 요약만 인쇄합니다.

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

               host limit:                         50000           0               50000
               pcnt host limit in use:             100.01          100.00          100.55
               rna events/second:                  1.22            0.00            48.65
               user cpu time:                      1.56            0.11            58.20
               system cpu time:                    1.31            0.00            41.13
               memory usage:                       5050384         0               5138904
               resident memory usage:              801920          0               901424
               rna flows/second:                   64.06           0.00            348.15
      rna dup flows/second:               0.00            0.00            37.05
               ids alerts/second:                  1.49            0.00            4.63
               ids packets/second:                 1.71            0.00            10.10
               ids comm records/second:            3.24            0.00            12.63
               ids extras/second:                  0.01            0.00            0.07
               fw_stats/second:                    1.78            0.00            5.72
               user logins/second:                 0.00            0.00            0.00
               file events/second:                 0.00            0.00            3.25
               malware events/second:              0.00            0.00            0.06
```

```
fireamp events/second:              0.00            0.00            0.00
```

요약의 각 행은 다음 순서로 3개의 값을 가집니다. 평균, 최소, 최대

-q 플래그 없이 인쇄할 경우 5분 간격 값도 표시됩니다. 요약은 마지막에 표시됩니다.

각 FMC는 데이터시트에 설명된 Maximum flow rate(최대 플로우 속도)를 갖습니다. 다음 표에는 각 데이터시트에서 가져온 모듈당 값이 포함되어 있습니다.

모델	FMC 750	FMC 1000	FMC 1600	FMC 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FM
최대 플로우 속도(fps)	2000	5000	5000	12000	12000	12000	20000	20000	20000	변수	12

이 값은 SFDataCorrelator 통계 출력에 굵게 표시된 모든 이벤트 유형의 집계에 사용됩니다.

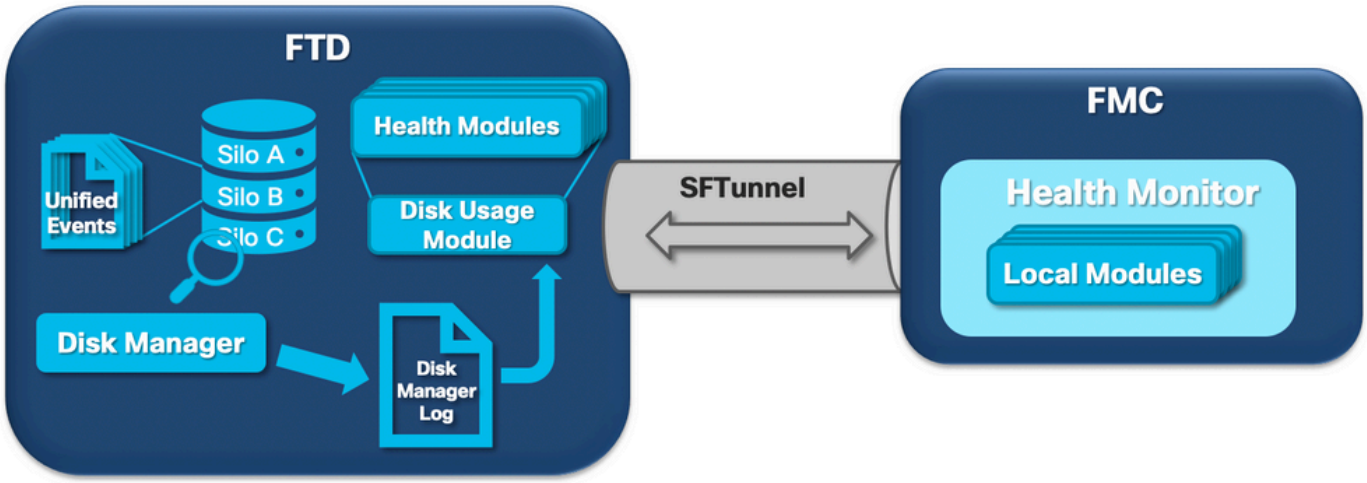
출력을 살펴보면 최악의 경우(모든 최대값이 동시에 발생할 때) 대비하는 방식으로 FMC의 크기를 조정하면 이 FMC에서 확인하는 이벤트의 속도는 48.65 + 348.15 + 4.63 + 3.25 + 0.06 = **404.74fps입니다**.

이 총 값은 각 모델의 데이터시트에 있는 값과 비교할 수 있습니다.

또한 SFDataCorrelator는 수신된 이벤트(예: 상관관계 규칙의 경우)를 기반으로 추가 작업을 수행한 다음 이를 데이터베이스에 저장하여 대시보드 및 이벤트 보기와 같은 FMC GUI(Graphical User Interface)에 다양한 정보를 채우도록 쿼리합니다.

디스크 관리자

다음 논리 다이어그램은 **상태 모니터** 및 **디스크 관리자 프로세스**가 디스크 관련 상태 알림 생성을 위해 서로 얽혀 있을 때의 논리 구성 요소를 보여줍니다.



간단히 말해, 디스크 관리자 프로세스는 상자의 디스크 사용을 관리하고 [/ngfw]/etc/sf/ 폴더에 해당 구성 파일을 포함합니다. 디스크 관리자 프로세스에 대한 여러 구성 파일이 특정 상황에서 사용됩니다.

- diskmanager.conf - 표준 구성 파일입니다.
- diskmanager_2hd.conf - 2개의 하드 드라이브가 설치된 경우 사용합니다. 두 번째 하드 드라이브는 파일 정책에 정의된 대로 파일을 저장하는 데 사용되는 악성코드 확장과 관련된 드라이브입니다.

- ramdisk-diskmanager.conf - Log to Ramdisk가 활성화된 경우 사용됩니다. 자세한 내용은 Log to Ramdisk 섹션을 참조하십시오.

디스크 관리자에서 모니터링하는 각 파일 유형에는 사일로가 할당됩니다. 디스크 관리자는 시스템에서 사용할 수 있는 디스크 공간을 기준으로 각 사일로에 대해 HWM(High Water Mark) 및 LWM(Low Water Mark)을 계산합니다.

디스크 관리자 프로세스에서 사일로를 제거하면 LWM에 도달하는 지점까지 처리됩니다. 파일당 이벤트가 소모되므로 이 임계값을 초과할 수 있습니다.

센서 디바이스에서 사일로의 상태를 확인하려면 다음 명령을 사용할 수 있습니다.

```
> show disk-manager
Silo                                Used        Minimum     Maximum
misc_fdm_logs                       0 KB        65.208 MB   130.417 MB
Temporary Files                     0 KB        108.681 MB  434.726 MB
Action Queue Results                0 KB        108.681 MB  434.726 MB
User Identity Events                0 KB        108.681 MB  434.726 MB
UI Caches                           4 KB        326.044 MB  652.089 MB
Backups                             0 KB        869.452 MB  2.123 GB
Updates                             304.367 MB  1.274 GB    3.184 GB
Other Detection Engine              0 KB        652.089 MB  1.274 GB
Performance Statistics              45.985 MB   217.362 MB  2.547 GB
Other Events                        0 KB        434.726 MB  869.452 MB
IP Reputation & URL Filtering       0 KB        543.407 MB  1.061 GB
arch_debug_file                     0 KB        2.123 GB    12.736 GB
Archives & Cores & File Logs        0 KB        869.452 MB  4.245 GB
Unified Low Priority Events         974.109 MB  1.061 GB    5.307 GB
RNA Events                          879 KB      869.452 MB  3.396 GB
File Capture                        0 KB        2.123 GB    4.245 GB
Unified High Priority Events        252 KB      3.184 GB    7.429 GB
IPS Events                          3.023 MB    2.547 GB    6.368 GB
```

다음 조건 중 하나가 충족되면 디스크 관리자 프로세스가 실행됩니다.

- 프로세스가 시작되거나 다시 시작됩니다.
- 사일로가 HWM에 도달함
- 사일로가 수동으로 배출됩니다.
- 매시간에 한 번

디스크 관리자 프로세스가 실행될 때마다 [/ngfw]/var/log/diskmanager.log에 있으며 CSV 형식의 데이터가 있는 자체 로그 파일에 있는 서로 다른 각 사일로에 대한 항목을 생성합니다.

다음은 Unified Low Priority Events 상태 알림에서 처리되지 않은 이벤트의 Drain을 트리거한 센서에서 가져온 diskmanager.log 파일의 샘플 행과 각 열의 분석입니다.

```
priority_2_events,1599668981,221,4587929508,1132501868,20972020,4596,1586044534,5710966962,1142193392,110,0
```

열	가치
사일로 레이블	priority_2_events
배출 시간(Epoch 시간)	1599668981
제거된 파일 수	221
소모된 바이트	4587929508
드레이닝 후의 현재 데이터 크기(바이트)	1132501868

가장 많이 제거된 파일(바이트)	20972020
가장 작은 파일 손실(바이트)	4596
가장 오래된 파일이 드레이닝됨(에포크 시간)	1586044534
하이 워터마크(바이트)	5710966962
로우 워터마크(바이트)	1142193392
처리되지 않은 이벤트가 제거된 파일 수	110
Diskmanager 상태 플래그	0

그런 다음 관련 상태 알림을 트리거하기 위해 각 상태 모니터 모듈에서 이 정보를 읽습니다.

수동으로 사일로 제거

특정 시나리오에서 사일로를 수동으로 제거할 수 있습니다. 예를 들어, 수동 파일 제거 대신 수동 사일로 드레인으로 디스크 공간을 지우려면 디스크 관리자가 보관할 파일과 삭제할 파일을 결정하는 것이 좋습니다. 디스크 관리자는 해당 사일로의 최신 파일을 보관합니다.

모든 사일로를 제거할 수 있으며 이는 이미 설명한 대로 작동합니다(디스크 관리자는 데이터 양이 LWM 임계값 아래로 갈 때까지 데이터를 드레이닝합니다). 명령 **시스템 지원 사일로-드레인**은 FTD CLISH 모드에서 사용할 수 있으며 사용 가능한 사일로 목록(이름 + 숫자 ID)을 제공합니다.

다음은 Unified Low Priority Events 사일로의 수동 배출 예입니다.

```
> show disk-manager
Silo                                Used        Minimum     Maximum
misc_fdm_logs                       0 KB        65.213 MB   130.426 MB
Temporary Files                     0 KB        108.688 MB  434.753 MB
Action Queue Results                0 KB        108.688 MB  434.753 MB
User Identity Events                0 KB        108.688 MB  434.753 MB
UI Caches                           4 KB        326.064 MB  652.130 MB
Backups                             0 KB        869.507 MB  2.123 GB
Updates                             304.367 MB  1.274 GB    3.184 GB
Other Detection Engine              0 KB        652.130 MB  1.274 GB
Performance Statistics              1.002 MB    217.376 MB  2.547 GB
Other Events                        0 KB        434.753 MB  869.507 MB
IP Reputation & URL Filtering       0 KB        543.441 MB  1.061 GB
arch_debug_file                     0 KB        2.123 GB    12.737 GB
Archives & Cores & File Logs        0 KB        869.507 MB  4.246 GB
Unified Low Priority Events         2.397 GB    1.061 GB    5.307 GB
RNA Events                          8 KB        869.507 MB  3.397 GB
File Capture                        0 KB        2.123 GB    4.246 GB
Unified High Priority Events        0 KB        3.184 GB    7.430 GB
IPS Events                          0 KB        2.547 GB    6.368 GB

> system support silo-drain
Available Silos
  1 - misc_fdm_logs
  2 - Temporary Files
  3 - Action Queue Results
  4 - User Identity Events
  5 - UI Caches
  6 - Backups
  7 - Updates
  8 - Other Detection Engine
```

```
  9 - Performance Statistics
 10 - Other Events
 11 - IP Reputation & URL Filtering
 12 - arch_debug_file
 13 - Archives & Cores & File Logs
 14 - Unified Low Priority Events
 15 - RNA Events
 16 - File Capture
 17 - Unified High Priority Events
 18 - IPS Events
  0 - Cancel and return

Select a Silo to drain: 14
Silo Unified Low Priority Events being drained.

> show disk-manager
Silo                                  Used        Minimum     Maximum
misc_fdm_logs                         0 KB        65.213 MB   130.426 MB
Temporary Files                       0 KB        108.688 MB  434.753 MB
Action Queue Results                  0 KB        108.688 MB  434.753 MB
User Identity Events                  0 KB        108.688 MB  434.753 MB
UI Caches                             4 KB        326.064 MB  652.130 MB
Backups                               0 KB        869.507 MB  2.123 GB
Updates                               304.367 MB  1.274 GB    3.184 GB
Other Detection Engine                0 KB        652.130 MB  1.274 GB
Performance Statistics                1.002 MB    217.376 MB  2.547 GB
Other Events                          0 KB        434.753 MB  869.507 MB
IP Reputation & URL Filtering         0 KB        543.441 MB  1.061 GB
arch_debug_file                       0 KB        2.123 GB    12.737 GB
Archives & Cores & File Logs          0 KB        869.507 MB  4.246 GB
Unified Low Priority Events           1.046 GB    1.061 GB    5.307 GB
RNA Events                            8 KB        869.507 MB  3.397 GB
File Capture                          0 KB        2.123 GB    4.246 GB
Unified High Priority Events          0 KB        3.184 GB    7.430 GB
IPS Events                            0 KB        2.547 GB    6.368 GB
```

상태 모니터

주요 내용은 다음과 같습니다.

- FMC의 Health Monitor 메뉴 또는 메시지 센터의 Health 탭에 표시되는 모든 상태 알림은 Health Monitor 프로세스에 의해 생성됩니다.
- 이 프로세스는 FMC 및 관리 대상 센서 모두에 대해 시스템의 상태를 모니터링하며, 다양한 모듈로 구성됩니다.
- 상태 알림 모듈은 디바이스별로 연결할 수 있는 상태 정책에 정의됩니다.
- 상태 알림은 FMC에서 관리하는 각 센서에서 실행할 수 있는 Disk Usage 모듈에 의해 생성됩니다.
- FMC에서 상태 모니터 프로세스가 실행될 때(5분마다 한 번 또는 수동 실행이 트리거될 때) Disk Usage 모듈은 diskmanager.log 파일을 확인하고, 올바른 조건이 충족되면 각 상태 알림이 트리거됩니다.

Drain **of Unprocessed events 상태 경고**가 트리거되려면 다음 조건이 모두 충족되어야 합니다.

1. Bytes drained 필드가 0보다 큽니다(이 사일로의 데이터가 제거되었음을 나타냄).
2. 처리되지 않은 이벤트가 0보다 많이 제거된 파일 수(제거된 데이터 내에 처리되지 않은 이벤트가 있음을 나타냄)
3. 배수 시간은 마지막 1시간 이내입니다.

이벤트**의 Frequent Drain** 상태 알림이 트리거되려면 다음 조건이 충족되어야 합니다.

1. diskmanager.log 파일의 마지막 2개 항목은 다음을 수행해야 합니다. Bytes drained 필드가 0보다 큽니다(이 사일로의 데이터가 드레이닝되었음을 나타냄).5분도 채 안 남았어요
2. 이 사일로에 대한 마지막 항목의 배출 시간은 지난 1시간 이내입니다.

디스크 사용 모듈에서 수집한 결과 및 다른 모듈에서 수집한 결과는 sftunnel을 통해 FMC로 전송됩니다. sftunnel을 통해 교환된 상태 이벤트에 대한 카운터를 sftunnel_**status 명령**과 함께 볼 수 있습니다.

```
TOTAL TRANSMITTED MESSAGES <3544> for Health Events service
RECEIVED MESSAGES <1772> for Health Events service
SEND MESSAGES <1772> for Health Events service
FAILED MESSAGES <0> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service
```

Ramdisk에 로그인

대부분의 이벤트가 디스크에 저장되지만, 디스크에 대한 이벤트의 지속적인 쓰기 및 삭제로 인해 발생할 수 있는 SSD의 점진적인 손상을 방지하기 위해 디바이스는 기본적으로 ramdisk에 로깅하도록 구성됩니다.

이 시나리오에서 이벤트는 **[/ngfw]/var/sf/detection_engine/*/instance-N/ 아래에** 저장되지 않지만 **[/ngfw]/var/sf/detection_engines/*/instance-N/connection/**(/dev/shm/instance-N/connection으로 연결되는 심볼 링크)에 있습니다. 이 경우 이벤트는 물리적 메모리가 아닌 가상 메모리에 상주합니다.

```
admin@FTD4140:~$ ls -la /ngfw/var/sf/detection_engines/b0c4a5a4-de25-11ea-8ec3-
4df4ea7207e3/instance-1/connection
lrwxrwxrwx 1 sfsnort sfsnort 30 Sep  9 19:03 /ngfw/var/sf/detection_engines/b0c4a5a4-de25-11ea-
8ec3-4df4ea7207e3/instance-1/connection -> /dev/shm/instance-1/connection
```

디바이스가 현재 어떤 작업을 수행하도록 구성되어 있는지 확인하려면 FTD CLISH에서 **show log-events-to-ramdisk** 명령을 실행합니다. **configure log-events-to-**ramdisk <enable**/disable> 명령을 사용하는** 경우에도 이**를** 변경할 수 **있습니다.**

```
> show log-events-to-ramdisk
Logging connection events to RAM Disk.

>configure log-events-to-ramdisk
Enable or Disable  enable or disable (enable/disable)
```

> **경고:** "configure log-events-to-ramdisk disable" 명령이 실행되면 FTD에서 두 가지 구축을 수행해야 snort가 "D" 상태(Uninterruptible Sleep)에 머물지 않으므로 트래픽이 중단됩니다. 이 동작은 Cisco 버그 ID CSCvz53372의 결함에 설명되어 있습니다. 첫 번째 구축에서는 snort 메모리 단계의 재평가를 건너뛰고, 이로 인해 snort가 "D" 상태로 전환되므로 해결 방법은 더미 변경을 통해 다른 구축을 수행하는 것입니다.

ramdisk에 로그인할 때 가장 큰 단점은 각 사일로의 할당 공간이 더 작기 때문에 같은 상황에서는 더 자주 이러한 공간이 소모된다는 것입니다. 다음 출력은 비교를 위해 ramdisk에 대한 로그 이벤트가 활성화되었거나 없는 FPR 4140의 디스크 관리자입니다.

Ramdisk 사용

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        903.803 MB  3.530 GB
Action Queue Results                0 KB        903.803 MB  3.530 GB
User Identity Events                0 KB        903.803 MB  3.530 GB
UI Caches                           4 KB        2.648 GB    5.296 GB
Backups                             0 KB        7.061 GB    17.652 GB
Updates                             305.723 MB  10.591 GB   26.479 GB
Other Detection Engine              0 KB        5.296 GB    10.591 GB
Performance Statistics              19.616 MB   1.765 GB    21.183 GB
Other Events                        0 KB        3.530 GB    7.061 GB
IP Reputation & URL Filtering       0 KB        4.413 GB    8.826 GB
arch_debug_file                     0 KB        17.652 GB   105.914 GB
Archives & Cores & File Logs        0 KB        7.061 GB    35.305 GB
RNA Events                          0 KB        7.061 GB    28.244 GB
File Capture                        0 KB        17.652 GB   35.305 GB
Unified High Priority Events        0 KB        17.652 GB   30.892 GB
Connection Events                   0 KB        451.698 MB  903.396 MB
IPS Events                          0 KB        12.357 GB   26.479 GB
```

Ramdisk에 대한 로그 사용 안 함

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        976.564 MB  3.815 GB
Action Queue Results                0 KB        976.564 MB  3.815 GB
User Identity Events                0 KB        976.564 MB  3.815 GB
UI Caches                           4 KB        2.861 GB    5.722 GB
Backups                             0 KB        7.629 GB    19.074 GB
Updates                             305.723 MB  11.444 GB   28.610 GB
Other Detection Engine              0 KB        5.722 GB    11.444 GB
Performance Statistics              19.616 MB   1.907 GB    22.888 GB
Other Events                        0 KB        3.815 GB    7.629 GB
IP Reputation & URL Filtering       0 KB        4.768 GB    9.537 GB
arch_debug_file                     0 KB        19.074 GB   114.441 GB
Archives & Cores & File Logs        0 KB        7.629 GB    38.147 GB
Unified Low Priority Events         0 KB        9.537 GB    47.684 GB
RNA Events                          0 KB        7.629 GB    30.518 GB
File Capture                        0 KB        19.074 GB   38.147 GB
Unified High Priority Events        0 KB        19.074 GB   33.379 GB
IPS Events                          0 KB        13.351 GB   28.610 GB
```

더 작은 크기의 사일로는 더 빠른 속도로 보상되어 이벤트에 액세스하고 이를 FMC에 스트리밍합니다. 적절한 조건에서 이것이 더 나은 옵션이지만, 단점을 고려해야 한다.

FAQ(자주 묻는 질문)

Drain of Events 상태 알림은 Connection Events에서만 생성됩니까?

아니요.

- Disc Manager Silo를 통해 Frequent Drain(자주 드레이닝하는 경우) 경고를 생성할 수 있습니다.
- 처리되지 않은 이벤트의 삭제 경보는 이벤트 관련 사일로에 의해 생성될 수 있습니다.

연결 이벤트가 가장 일반적인 원인입니다.

Frequent Drain 상태 알림이 표시되면 Log to Ramdisk를 비활성화하는 것이 항상 바람직합니까?

아니요. DOS/DDOS를 제외한 과도한 로깅 시나리오에서만, 영향을 받는 사일로가 연결 이벤트 사일로인 경우 및 로깅 설정을 더 이상 튜닝할 수 없는 경우에만 해당됩니다.

DOS/DDOS로 인해 과도한 로깅이 발생하는 경우 해결 방법은 DOS/DDOS 보호를 구현하거나 DOS/DDOS 공격의 소스를 제거하는 것입니다.

기본 기능인 "Log to Ramdisk"는 SSD 마모를 감소시키므로 사용하는 것이 좋습니다.

미처리 이벤트를 구성하는 것은 무엇입니까?

이벤트는 개별적으로 처리되지 않은 것으로 표시되지 않습니다. 다음과 같은 경우 파일에 처리되지 않은 이벤트가 있습니다.

생성 타임스탬프가 해당 책갈피 파일의 타임스탬프 필드보다 높습니다.

또는

생성 타임스탬프는 해당 책갈피 파일의 타임스탬프 필드와 같으며 해당 크기가 해당 책갈피 파일의 Bytes 필드 위치보다 큽니다.

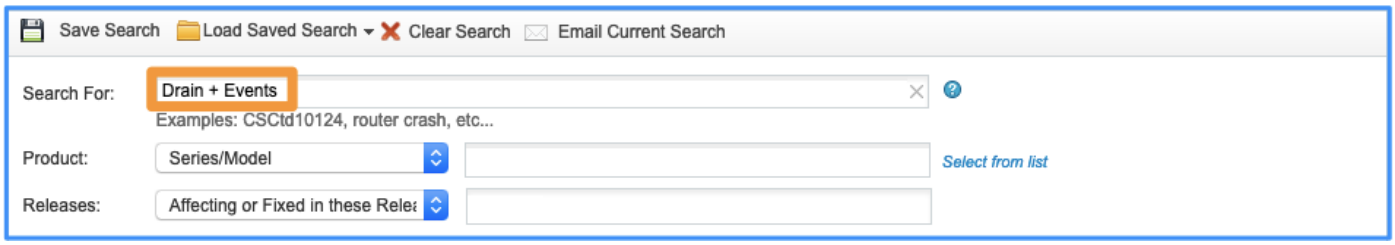
FMC는 특정 센서의 뒤에 있는 바이트 수를 어떻게 알 수 있습니까?

센서는 unified_events 파일 이름 및 크기에 대한 메타데이터와 북마크 파일에 대한 정보를 전송합니다. 이 정보는 FMC에 다음과 같이 뒤에 있는 바이트를 계산할 수 있는 충분한 정보를 제공합니다.

Current unified_events file size - **Position in Bytes"** 필드의 북마크 파일 + 해당 북마크 파일의 타임스탬프보다 타임스탬프가 높은 모든 unified_events 파일의 크기.

알려진 문제

버그 검색 도구를 열고 다음 쿼리를 사용합니다.



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.