排出FMC未處理事件和頻繁排出事件故障運行狀況監視器警報

目錄

簡介

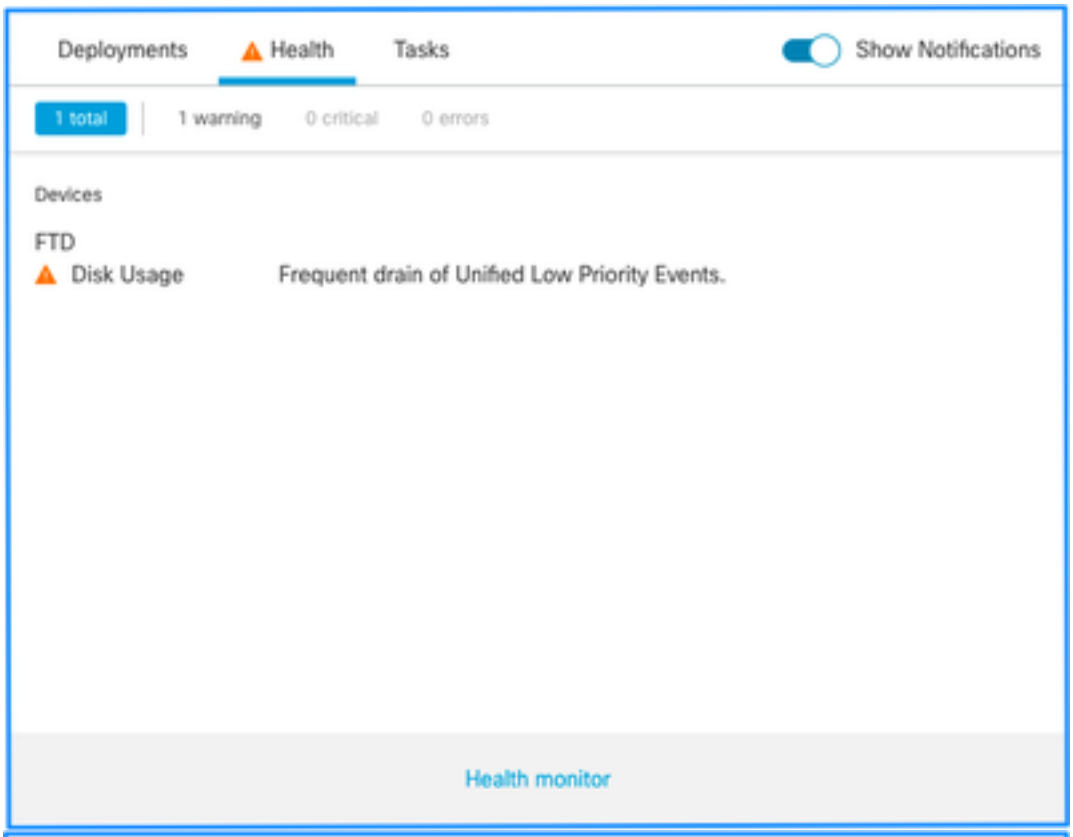
本文描述如何對Firepower Management Center(FMC)**上的未處理事**件排出**和頻繁排出**事件運行狀況警報進行故障排除。

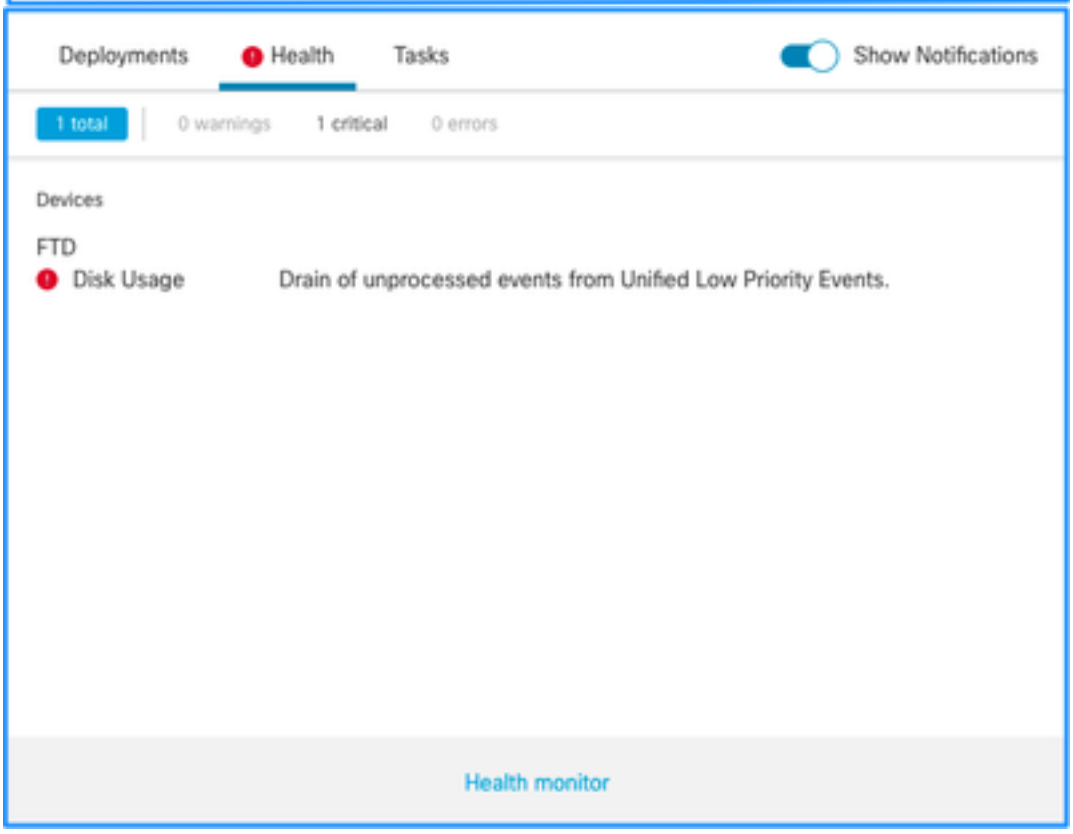
問題概述

FMC會生成以下健康警報之一：

- 統一低優先順序事件的頻繁流失
  和/或
- 從統一低優先順序事件中排出未處理的事件

雖然這些事件在FMC中生成並顯示，但它們與受管裝置感測器相關，無論它是Firepower威脅防禦(FTD)裝置還是下一代入侵防禦系統(NGIPS)裝置。在本文檔的其餘部分，除非另有說明，術語sensor同時指FTD和NGIPS裝置。





以下是健康警報結構：

- 頻繁耗盡<SILO NAME>
- 從<SILO NAME>中排出未處理的事件

在本示例中，思洛儲存器名稱為**統一低優先順序事件**。這是磁碟管理器小倉庫之一（有關更全面的說明，請參見「背景資訊」部分）。

此外：

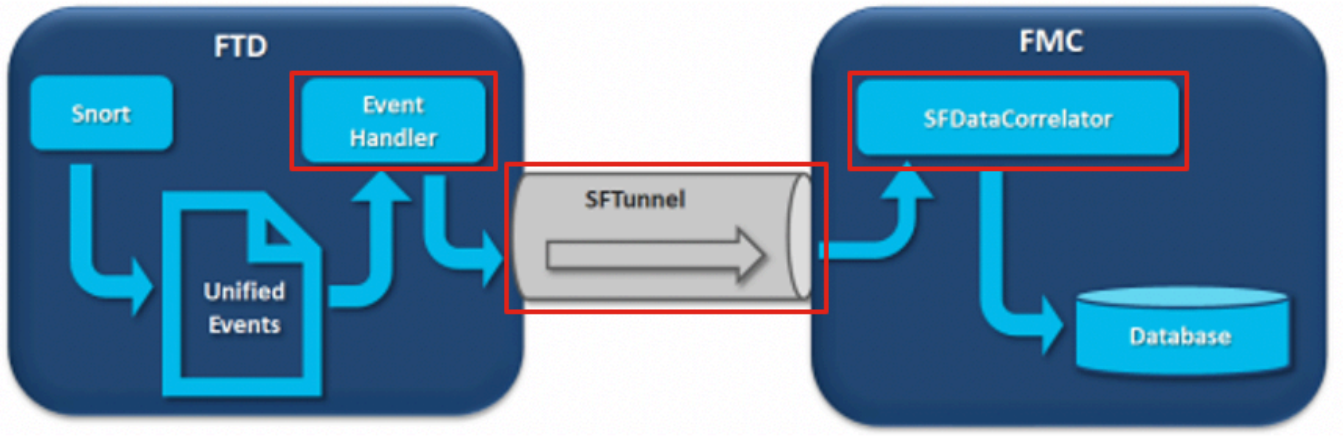
- 儘管任何思洛儲存器從技術上講都可以生成Frequent drain <SILO NAME> health警報，但最常見的是與事件相關的警報，其中低優先順序事件只是因為這些事件型別更常由感測器生成。
- 如果是「<SILO NAME>」事件相關的思洛儲存器，則頻繁排出「<SILO NAME>」事件的嚴重性為「警告」，因為如果處理了此事件（下面將說明未處理事件的構成），則它們位於FMC資料庫中。
- 對於非事件相關的思洛儲存器（如「備份」思洛儲存器），警報是嚴重的，因為此資訊已丟失。
- 只有事件型別孤島會從<SILO NAME>運行狀況警報中生成未處理事件的排出。此警報始終具有嚴重嚴重性。

其他症狀可能包括：

- FMC UI速度緩慢
- 事件丟失

常見故障排除場景

頻繁地耗盡<SILO NAME>事件是由於輸入到思洛儲存器中的資訊量與其大小相匹配造成的。在這種情況下，磁碟管理器將在最後5分鐘間隔內至少兩次清空（清除）該檔案。在事件型別思洛儲存器中，這通常是由該事件型別的過多記錄引起的。如果<SILO NAME>運行狀況警報的未處理事件排出，這也可能是由於事件處理路徑中存在瓶頸所致。



圖中存在3個潛在的瓶頸：

- FTD上的EventHandler進程超額使用（其讀取速度比Snort寫入的速度慢）
- 事件介面超額訂閱
- FMC上的SFDataCorrelator進程超額訂閱

要更深入地瞭解事件處理體系結構，請參閱各自的深入探討部分。

案例1.過度記錄

如上一節所述，導致此類運行狀況警報的最常見原因之一是輸入過多。

從**show disk-manager** CLISH命令收集的低水位標籤(LWM)和高水位標籤(HWM)之間的差異顯示了從LWM（新排出）到HWM值需要佔用該思洛儲存器多少空間。如果頻繁地消耗事件（無論有沒有未經處理的事件），首先必須檢查日誌記錄配置。

有關「磁碟管理器」過程的詳細說明，請參閱相應的「深入分析」部分。

無論是雙日誌記錄，還是僅是整個manager-sensors生態系統中的高事件率，都必須檢查日誌記錄設定。

建議的操作

步驟1.檢查雙重日誌記錄

如果您檢視FMC上的相關器**perfstats**，可以識別雙重日誌記錄方案，如下輸出所示：

```
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
```

在這種情況下，輸出中可以看到較高的重複流率。

步驟2.檢查ACP的日誌記錄設定

您必須從檢視訪問控制策略(ACP)的日誌記錄設定開始。 確保遵循本文檔連線日誌記錄的最佳實踐中描述的最佳實踐

建議在所有情況下都檢查日誌記錄設定，因為列出的建議不僅包括雙重日誌記錄方案。

步驟3.檢查日誌記錄是否過量

您必須檢查過度日誌記錄是否有預期的原因。如果DOS/DDoS攻擊或路由環路或特定應用程式/主機造成大量連線導致日誌記錄過多，則必須檢查並緩解/停止來自意外過度連線源的連線。

步驟4.升級模式

將FTD硬體裝置升級為更高效能的型號（例如FPR2100 —> FPR4100），思洛儲存器的來源會增加。

步驟5.考慮是否可以禁用「記錄到Ramdisk」

對於統一低優先順序事件思洛儲存器，您可以禁用Log to Ramdisk，以增大思洛儲存器大小，其缺點在各自的深入分析一節中討論。

案例2.感測器與FMC之間的通訊通道瓶頸

此型別的警報的另一個常見原因是感測器和FMC之間的通訊通道(sftunnel)中的連線問題和/或不穩定性。通訊問題可能是由於：

- sftunnel關閉或不穩定（擺動）。
- sftunnel超額訂閱。

對於sftunnel連線問題，請確保FMC和感測器在TCP埠8305上的管理介面之間具有可達性。

在FTD上，您可以在[/ngfw]/**var/log/messages**檔案中搜尋**sftunneld**字串。連線問題會導致生成如下消息：

```
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管理介面的超訂用可能是管理流量的激增或持續的超訂用。健康監測的歷史資料就是很好的指標。

首先要注意的是，在大多數情況下，FMC使用單個NIC進行部署以供管理。此介面用於：

- FMC管理。
- FMC感測器管理。
- 從感測器收集FMC事件。
- 情報源的更新。
- 從軟體下載站點下載SRU、軟體、VDB和GeoDB更新。
- 查詢URL信譽和類別（如果適用）。

- 檔案處置查詢（如果適用）。

建議的操作

您可以在FMC上為事件專用介面部署第二個NIC。實現方式可取決於使用案例。

有關一般准則，請參閱FMC硬體指南在管理網路上部署

案例3. SFDataCorrelator流程的一個瓶頸

要覆蓋的最後一個場景是SFDataCorrelator端(FMC)出現瓶頸時。

第一步是檢視diskmanager.log檔案，因為需要收集一些重要資訊，例如：

- 排水器的頻率。
- 已耗盡未處理事件的檔案數。
- 具有未處理事件的排出發生。

有關diskmanager.log檔案及其解釋方法的資訊，請參閱磁碟管理器部分。從diskmanager.log收集的資訊可用於幫助縮小後續步驟。

此外，您需要檢視相關器效能統計資訊：

```
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
```

請注意，這些統計資訊是用於FMC的，它們對應於由其管理的所有感測器的集合。在統一低優先順序事件的情況下，您主要查詢：

- 用於評估SFDataCorrelator進程可能超訂用的任何事件型別的每秒總流數。
- 在上一輸出中突出顯示的兩行： **rna flows/second** — 表示SFDataCorrelator處理的低優先順序事件的速率。**rna dup flows/second** — 指示SFDataCorrelator處理的重複低優先順序事件的速率。如前一個場景所述，這是通過雙重日誌記錄生成的。

根據輸出可得出結論：

- 沒有重複記錄，如rna dup flows/second row所示。
- 在rna flow/second行中，Maximum值遠遠高於Average值，因此SFDataCorrelator進程處理事件的速率會激增。如果您檢視使用者工作日剛開始的今天凌晨，這可能會是正常的，但一般來說，這是一個危險訊號，需要做進一步調查。

有關SFDataCorrelator進程的更多資訊，請參閱事件處理部分。

建議的操作

首先，你需要確定何時出現尖峰。為此，您需要檢視每5分鐘取樣間隔的相關器統計資訊。從diskmanager.log中收集的資訊可幫助您直接進入重要的時間範圍。

> **提示：**將輸出傳輸到Linux分頁器**較少**，以便您輕鬆搜尋。

```
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
```

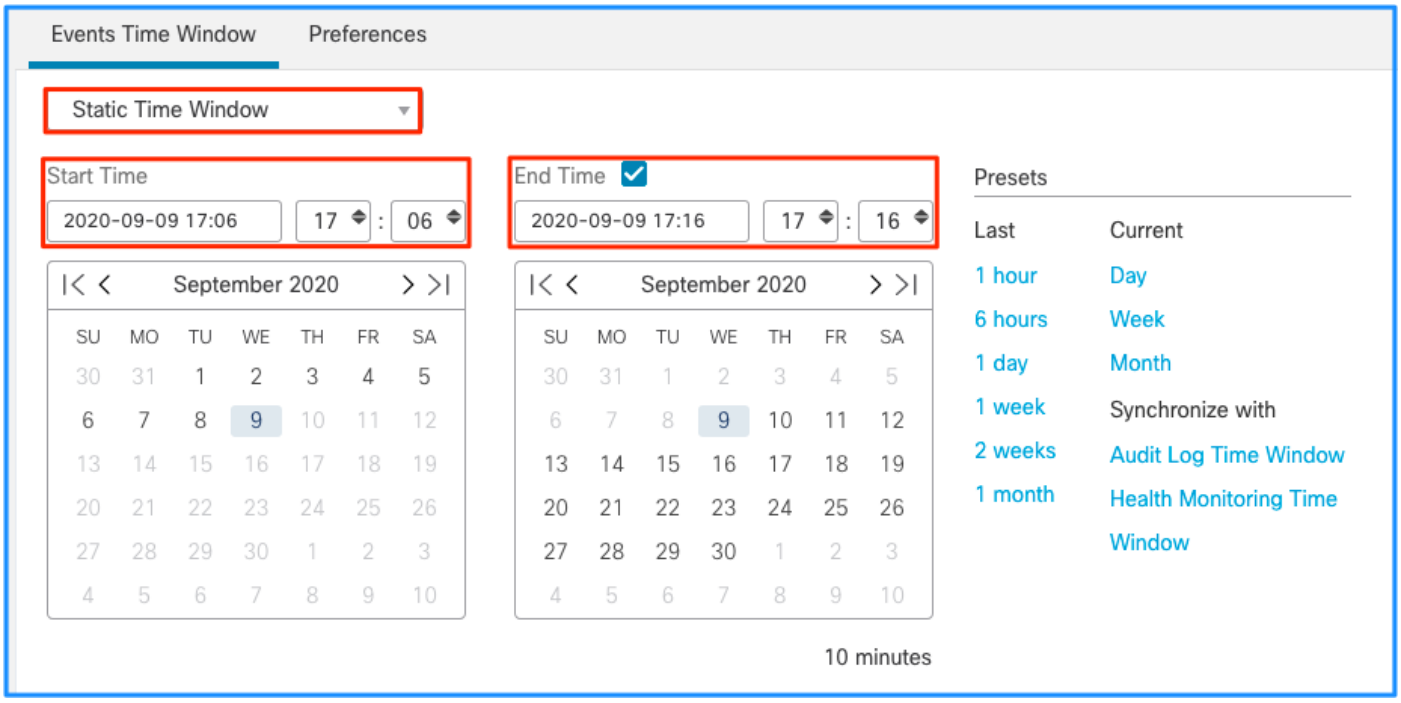
```
                ids pkts/second:              0.00
                ids comm records/second:      0.02
                ids extras/second:            0.00
                fw stats/second:              0.01
                user logins/second:           0.00
                file events/second:           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
```

使用輸出中的資訊可以：

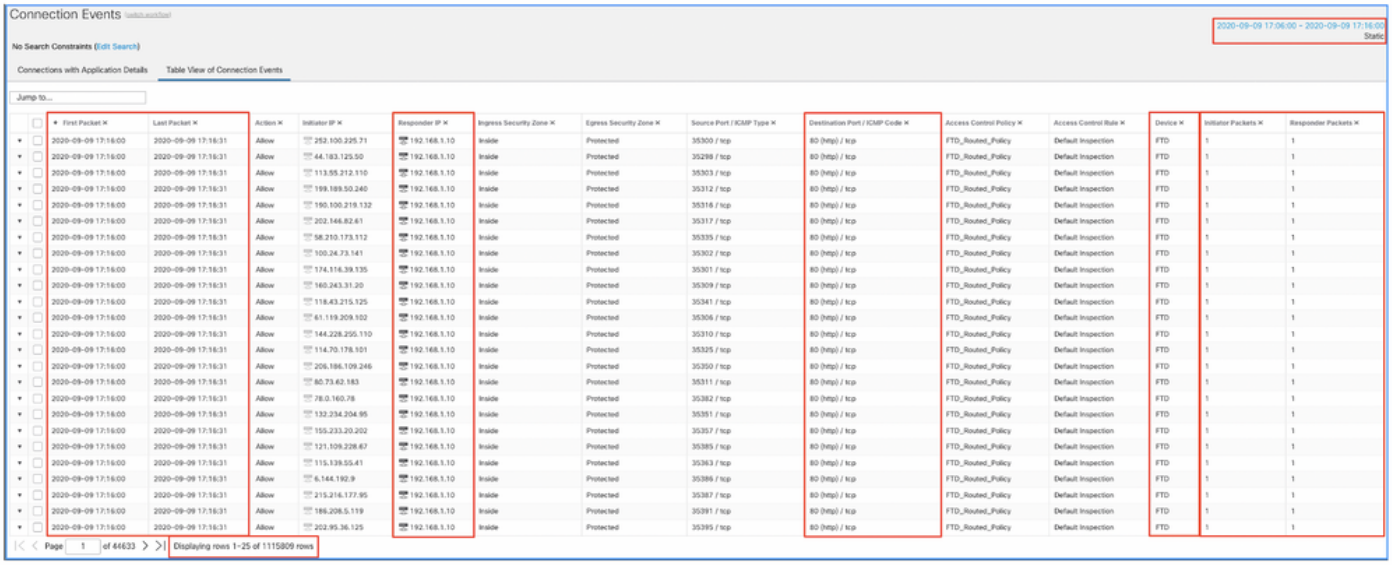
- 確定事件的正常/基線速率。
- 確定發生峰值的5分鐘時間間隔。

在上一個示例中，在16:06:39及以後收到的事件率明顯激增。請注意，這些是5分鐘的平均值，因此如果增量開始接近末尾，則增加值可能比所示的（突發）更突然，但在5分鐘間隔內稀釋。

雖然由此可以得出結論，此事件高峰已導致未處理事件的耗盡，但您可以檢視具有適當時間視窗的FMC圖形使用者介面(GUI)中的連線事件，瞭解此高峰中穿越FTD框的連線型別：



應用此時間視窗以獲取篩選的連線事件，不要忘記考慮時區。在本示例中，感測器使用UTC和FMC UTC+1。使用表檢視可檢視觸發事件過載的事件，並相應地採取措施：



根據時間戳（第一個和最後一個資料包的時間），可以看到這些連線是短暫的。此外，Initiator和Responder Packets列顯示每個方向只交換了一個資料包。這證明連線是短暫的，交換的資料很少。

您還可以看到所有這些流都以相同的響應方IP和埠為目標。此外，它們都由同一感測器報告（該感測器與Ingress和Egress介面資訊一起可指示此流的位置和方向）。 其他操作：

- 檢查目標端點上的系統日誌。
- 實施DOS/DDOS保護或採取其他預防措施。

附註：本文的目的是提供用於排除「未處理事件排出」警報故障的准則。此示例使用hping3生成到目標伺服器的TCP SYN泛洪。有關強化FTD裝置的准則，請檢視Cisco Firepower威脅防禦強化指南

在聯絡思科技術協助中心(TAC)之前收集的專案

強烈建議您在聯絡Cisco TAC之前收集以下專案：

- 檢視的運行狀況警報的螢幕快照。
- 對從FMC生成的檔案進行故障排除。
- 對從受影響的感測器生成的檔案進行故障排除。
- 首次發現問題的日期和時間。
- 有關最近對策略所做的任何更改的資訊（如果適用）。
- 事件處理部分中所述的stats_unified.pl命令的輸出及受影響的感測器的說明。

深入探討

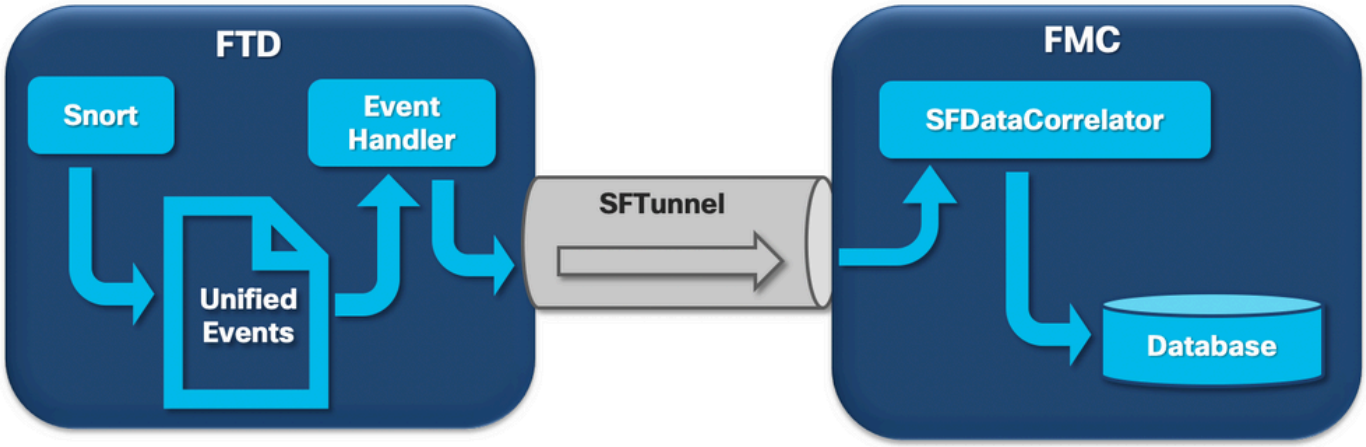
本節詳細說明了可以參與此型別運行狀況警報的各種元件。其中包括：

- 事件處理 — 說明感測器裝置和FMC上發生的事件路徑。當運行狀況警報涉及事件型別思洛儲存器時，這很有用。
- Disk Manager — 介紹磁碟管理器流程、孤島及其耗盡方式。
- 運行狀況監視器 — 介紹如何使用運行狀況監視器模組生成運行狀況警報。
- Log to Ramdisk — 介紹ramdisk功能的日誌記錄及其對健康警報的潛在影響。

要瞭解「事件引出」運行狀況警報，並能夠識別潛在的故障點，需要研究這些元件如何工作以及彼此之間的互動。

事件處理

即使頻繁漏出型別的健康警報可能由與事件無關的孤島觸發，Cisco TAC看到的絕大多數案例都與事件相關資訊的漏出有關。此外，要瞭解什麼構成未處理事件的消耗，需要檢視事件處理體系結構及其組成元件。



當Firepower感測器從新連線收到資料包時，snort進程會生成統一的2格式的事件，該格式是一種二進位制格式，允許更快的讀/寫以及更輕的事件。

輸出顯示FTD命令**system support trace**，您可以在其中看到已建立的新連線。重點介紹和解釋以下重要部分：

```
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檔案在每個例項的path**[/ngfw]var/sf/detection_engine/*/instance-N/下生成，**其中：

- ***是Snort UUID。每個裝置都是唯一的。
- **N**是Snort例項ID，其計算方式可為來自上一個輸出（示例中突出顯示的為0）+ 1的例項ID

任何給定的Snort例項資料夾中都可以有2種型別的unified_events檔案：

- unified_events-1（包含高優先順序事件）。
- unified_events-2（包含低優先順序事件）。

高優先順序事件是與潛在惡意連線相對應的事件。

事件型別及其優先順序：

高優先順序(1)	**低優先順序(2)**
入侵	連線
惡意軟體	發現
安全情報	檔案
關聯的連線事件	統計

下一個輸出顯示屬於上一個示例中跟蹤的新連線的事件。該格式為unified2，取自位於[/ngfw]/var/sf/detection_engine/*/instance-**1**/(其中1是前面輸出+1中粗體的snort例項id。統一事件日誌格式名稱使用語法unified_events-**2**.log.**1599654750**，其中2表示表中顯示的事件優先順序，而粗體的最後部分(**1599654750)是時間戳(Unix)建立檔案的時間)。**

> **提示：**您可以使用Linux **date**命令將Unix時間轉換為可讀日期：
> admin@FP1120-2:~$ sudo **日期-d@1599654750**
> 2020年9月9日週三14:32:30 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
```

每個unified_events檔案旁邊都有一個書籤檔案，其中包含兩個重要值：

1. 該例項和優先順序的當前unified_events檔案的對應時間戳。
2. Unified_event檔案中最後一個讀取事件的位置（以位元組為單位）。

這些值按逗號分隔的順序排列，如下例所示：

```
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
```

這樣，磁碟管理器進程就可以知道哪些事件已經處理（傳送到FMC），哪些還沒有處理。

請注意，當磁碟管理器釋放事件思洛儲存器時，它會刪除統一事件檔案。有關釋放孤島的更多資訊，請參閱磁碟管理器部分。

當以下情況之一為真時，已耗盡的統一檔案被視為具有未處理的事件：

1. 書籤時間戳低於檔案建立時間。
2. 書籤時間戳與檔案建立時間相同，並且檔案中的「位元組」位置低於其大小。

EventHandler進程從統一檔案中讀取事件，並通過sftunnel（負責感測器與FMC之間加密通訊的進程）將其流式處理到FMC（作為後設資料）。這是一個基於TCP的連線，因此事件流由FMC確認

您可以在[/ngfw]/var/log/messages檔案中看到以下消息：

```
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
```

此輸出提供以下資訊：

- Snort開啟了unified_events檔案以便輸出（在其中寫入）。
- 事件處理程式開啟了同一個unified_events檔案（從中讀取）。
- sftunnel報告從該unified_events檔案處理的事件數。

然後，相應地更新書籤檔案。Sftunnel為高優先順序事件和低優先順序事件分別使用2個稱為統一事件(UE)通道0和1的不同通道。

在FTD上使用**funnel_status** CLI指令，您可以看到串流的事件的數量。

```
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
```

在FMC中，事件由SFDataCorrelator進程接收。

使用**stats_unified.pl**命令可檢視每個感測器處理的事件狀態：

```
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
```

此命令顯示每個通道中特定裝置的事件積壓的狀態，使用的通道ID與sftunnel相同。

Bytes Behind值可以計算為統一事件書籤檔案中顯示的位置與統一事件檔案大小之間的差值，加上任何時間戳高於書籤檔案中的時間戳的後續檔案。

SFDataCorrelator進程還儲存效能統計資訊，這些統計資訊儲存在**/var/sf/rna/correlator-stats/**中。每天建立一個檔案，以CSV格式儲存該天的效能統計資訊。檔名稱使用「**YYYY-MM-DD**」格式，當前日期對應的檔案現在稱**為**。

統計資訊每5分鐘收集一次（每5分鐘間隔有一行）。

可以使用**perfstats**命令讀取此檔案的輸出。請注意，此is命令還用於讀取snort效能統計資訊檔案，因此必須使用相應的標誌：

-C:指示perfstats輸入為correlator-stats檔案（不帶此標誌perfstats假定輸入為snort效能統計資訊檔案）。

-q:安靜模式，只列印檔案的摘要。

```
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
```

摘要中的每一行按以下順序有3個值：平均值，最小值，最大值。

如果列印時不帶 — q標誌，您還會看到5分鐘間隔值。總結將在末尾顯示。

請注意，每個FMC在其資料表中都有描述的最大流速。下表包含各個資料表中每個模組的值：

型號	FMC 750	FMC 1000	FMC 1600	FMC 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMC
最大流速(fps)	2000	5000	5000	12000	12000	12000	20000	20000	20000	變數	12

請注意，這些值用於SFDataCorrelator統計資訊輸出中以粗體顯示的所有事件型別的聚合。

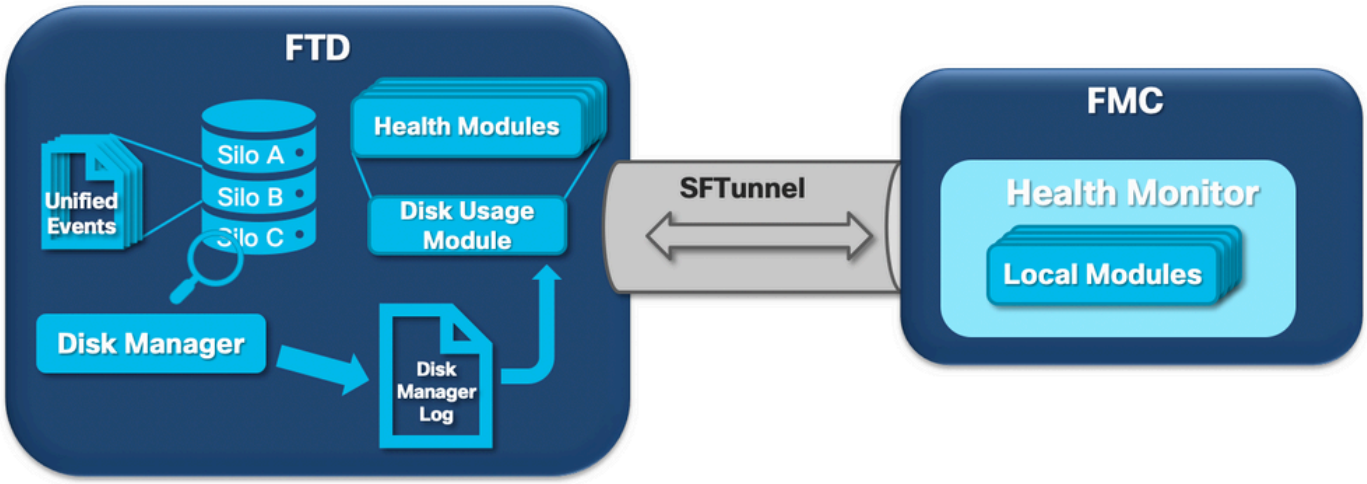
如果您檢視輸出，並且我們按照我們為最壞情況（所有最大值同時發生時）準備的方法來調整我們的FMC，則此FMC看到的事件率為48.65 + 348.15 + 4.63 + 3.25 + 0.06 = **404.74 fps**。

此總值與相應模型資料表中的值進行比較。

SFDataCorrelator還可以對接收的事件（例如關聯規則）進行其他工作，然後將它們儲存在資料庫中，該資料庫被查詢以填充FMC圖形使用者介面(GUI)中的各種資訊，例如儀表板和事件檢視。

磁碟管理器

下一個邏輯圖顯示Health Monitor和Disk Manager進程的邏輯元件，因為它們相互交織以生成與磁碟相關的運行狀況警報。



簡而言之，磁碟管理器進程管理該盒的磁碟使用情況，其配置檔案位於[/ngfw]/etc/sf/資料夾中。在特定情況下可以使用磁碟管理器進程的多個配置檔案：

- diskmanager.conf — 標準配置檔案。
- diskmanager_2hd.conf — 在機箱上安裝2個硬碟時使用。第二個硬碟驅動器與惡意軟體擴展相關，用於儲存檔案策略中定義的檔案。

- ramdisk-diskmanager.conf — 在啟用記錄到Ramdisk時使用。有關詳細資訊，請檢視Log to Ramdisk部分。

磁碟管理器監控的每種型別的檔案都分配有一個思洛儲存器。根據系統上可用的磁碟空間量，磁碟管理器會為每個思洛儲存器計算高水位標籤(HWM)和低水位標籤(LWM)。

當磁碟管理器進程耗盡思洛儲存器時，它會一直耗盡，直到到達LWM點。由於每個檔案都排出事件，因此可以超過此閾值。

要檢查感測器裝置上孤島的狀態，可以使用此命令：

```
> 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
```

滿足以下條件之一時，磁碟管理器進程將運行：

- 進程開始（或重新啟動）
- 思洛儲存器到達HWM
- 思洛儲存器已手動排空
- 每小時一次

每次運行磁碟管理器進程時，它都會在自己的日誌檔案中為每個不同的孤島生成一個條目，該日誌檔案位於[/ngfw]/var/log/diskmanager.log下，並且具有CSV格式的資料。

接下來，顯示來自diskmanager.log檔案的示例行，該示例行取自觸發從統一低優先順序事件運行狀況警報中排出未處理事件的感測器，以及相應列的細分：

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

列	價值
思洛儲存器標籤	priority_2_events
排出時間（紀元時間）	1599668981
已耗盡的檔案數	221
已耗盡的位元組	4587929508
排出後資料的當前大小（位元組）	1132501868
已耗盡的最大檔案（位元組）	20972020

已耗盡的最小檔案（位元組）	4596
最舊的檔案已耗盡（紀元時間）	1586044534
高水印（位元組）	5710966962
低水位線（位元組）	1142193392
已耗盡未處理事件的檔案數	110
Diskmanager狀態標誌	0

然後，各個運行狀況監視器模組讀取此資訊，以觸發相關的運行狀況警報。

手動清空思洛儲存器

在某些情況下，您可能希望手動清空思洛儲存器。例如，使用手動思洛儲存器清空磁碟空間，而不是手動刪除檔案，有利於磁碟管理器決定保留和刪除哪些檔案。磁碟管理器保留該思洛儲存器的最新檔案。

任何思洛儲存器都可以被清空，並且如前所述那樣工作（磁碟管理器會清空資料，直到資料量低於LWM閾值）。 **system support silo-drain**命令可在FTD CLISH模式下使用，它提供可用思洛儲存器（名稱+數字ID）的清單。

以下是手動清空統一低優先順序事件思洛儲存器的示例：

```
> 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
```

運行狀況監視器

以下是要點：

- 在FMC的「運行狀況監視器」(Health Monitor)選單或「消息中心」(Message Center)的「運行狀況」(Health)頁籤下顯示的任何運行狀況警報均由運行狀況監視器進程生成。
- 此過程可監控系統的運行狀況，包括FMC和受管感測器，並且由多個不同的模組組成。
- 健康警報模組在健康策略中定義，可以按裝置連線。
- 運行狀況警報由磁碟使用模組生成，該模組可在FMC管理的每個感測器上運行。
- 當FMC上的運行狀況監視器進程運行時（每5分鐘一次或觸發手動運行時），磁碟使用情況模組會檢視diskmanager.log檔案，如果滿足正確的條件，則會觸發相應的運行狀況警報。

要觸發Drain of Unprocessed events運行狀況警報，必須滿足以下所有條件：

1. 已耗盡的位元組數欄位大於0（這表示此思洛儲存器中的資料已耗盡）。
2. 未處理事件已耗盡大於0的檔案數（這表示已耗盡的資料中存在未處理事件）。
3. 下水的時間是在最近1小時內。

要觸發**頻繁排出事**件運行狀況警報，必須滿足以下條件：

1. diskmanager.log檔案中的最後2個條目需要： Have Bytes drawed欄位大於0（這表示來自此思洛儲存器的資料已排空）。間隔時間不超過5分鐘。
2. 此思洛儲存器最後一個條目的耗盡時間是在過去1小時內。

從磁碟使用模組收集的結果（以及其他模組收集的結果）通過sftunnel傳送到FMC。您可以使用**sftunnel_status**命令檢視通過sftunnel交換的運行狀況事件的計數器：

```
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
```

登入到Ramdisk

即使大多數事件儲存在磁碟中，裝置也會預設配置為記錄到ramdisk以防止由於不斷向磁碟寫入和刪除事件而導致的SSD逐漸損壞。

在此案例中，事件不儲存在**[/ngfw]/var/sf/detection_engine/*/instance-N/** 下，但它們位於**[/ngfw]/var/sf/detection_engine/*/instance-N/connection/**中，該連結是**/dev/shm/instance-N/connection的符號連結。**在這種情況下，事件駐留在虛擬記憶體中，而不是實體記憶體中。

```
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
```

要驗證裝置當前配置為執行什麼操作，請從FTD CLISH運行**show log-events-to-ramdisk**命令。您也可以使用命令**configure log-events-to-ramdisk <enable/disable>:**

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

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

> **警告：**執行「configure log-events-to-ramdisk disable」命令時，需要在FTD上完成兩個部署，以便snort不會陷入「D」狀態（不間斷睡眠），這將導致流量中斷。
> 此行為已記錄在Cisco錯誤ID CSCvz5372的缺陷中。在第一個部署中，將跳過對snort記憶體階段的重新評估，這導致snort進入「D」狀態，解決方法是使用任何虛擬更改執行另一個部署。

當您登入到磁碟時，主要缺點是各個思洛儲存器所分配的空間較小，因此在同一情況下會更頻繁地耗盡它們。下一個輸出是來自FPR 4140的磁碟管理器，該管理器帶有日誌事件和沒有日誌事件以啟用到ramdisk以供比較。

Log to Ramdisk enabled

```
> 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
```

已禁用登入到Ramdisk

```
> 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
```

思洛儲存器尺寸越小，訪問事件並將其流向FMC的速度就越快。雖然在適當的條件下這是一個更好的選擇，但是必須考慮到它的缺點。

常見問題 (FAQ)

事件排出健康警報是否僅由連線事件生成？

編號

- 任何磁碟管理器思洛儲存器都可以生成頻繁耗盡警報。
- 任何與事件相關的思洛儲存器都可以生成未處理事件排出的警報。

連線事件是最常見的罪魁禍首。

當出現Frequent Drain健康警報時，是否始終建議禁用Log to Ramdisk?

否。僅在除DOS/DDOS之外的「過度日誌記錄」情形中，當受影響的思洛儲存器是連線事件思洛儲存器時，且僅在無法進一步調整日誌記錄設定時。

如果DOS/DDOS導致過多的日誌記錄，解決方案是實施DOS/DDOS保護或消除DOS/DDOS攻擊的來源。

預設功能「Log to Ramdisk」可減少SSD的磨損，因此強烈建議使用它。

什麼是未處理事件？

事件不會單獨標籤為未處理。在下列情況下，檔案具有未處理的事件：

其建立時間戳高於相應書籤檔案中的時間戳欄位。

或

其建立時間戳等於各個書籤檔案中的時間戳欄位，並且其大小高於各個書籤檔案上「位元組」欄位中的位置。

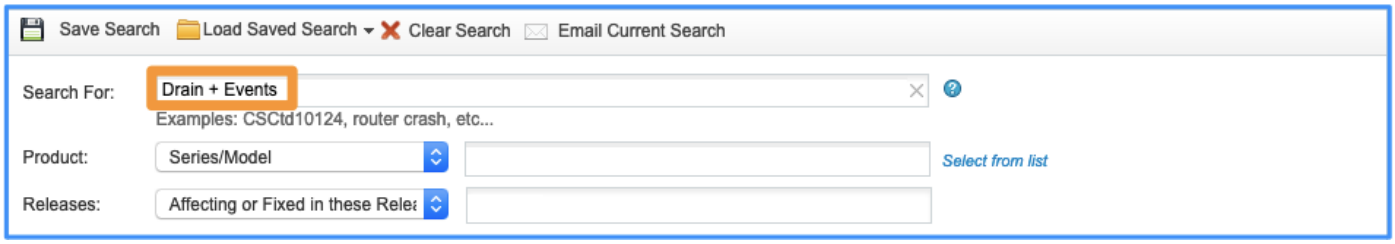
FMC如何知道特定感測器的滯後位元組數？

感測器傳送有關unified_events檔名和大小的後設資料，以及書籤檔案上的資訊，從而為FMC提供足夠的資訊以計算後面的位元組，如下所示：

Current unified_events file size - **Position in Bytes**" field from bookmark file + Size of all unified_events files with than timestamp than the timestamp in the accorrect bookmark file。

已知的問題

開啟Bug Search Tool並使用以下查詢：



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。