

# FMCの未処理イベントのドレインとイベントの頻繁なドレインのトラブルシューティング Health Monitorアラート

## 内容

### [概要](#)

#### [問題の概要](#)

#### [一般的なトラブルシューティングシナリオ](#)

#### [事例1\)過剰なログイン](#)

#### [推奨処置](#)

#### [事例2\)センサとFMC間の通信チャネルのボトルネック](#)

#### [推奨処置](#)

#### [ケース3. SFDataCorrelatorプロセスのボトルネック](#)

#### [推奨処置](#)

#### [Cisco Technical Assistance Center\(TAC\)に連絡する前に収集すべき項目](#)

#### [分析 \[英語\]](#)

#### [イベント処理](#)

#### [ディスクマネージャ](#)

#### [サイロを手動で削除する](#)

#### [ヘルスマニタ](#)

#### [RAMディスクにログインします。](#)

#### [よく寄せられる質問 \(FAQ\)](#)

#### [既知の問題](#)

## 概要

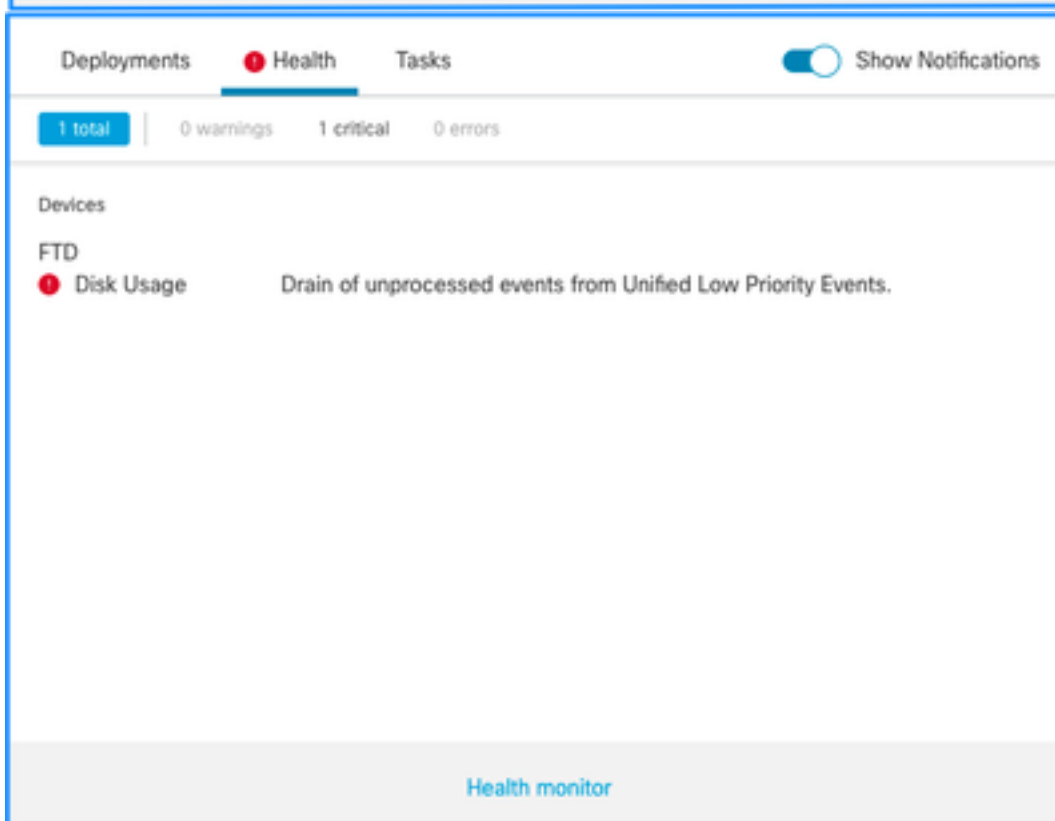
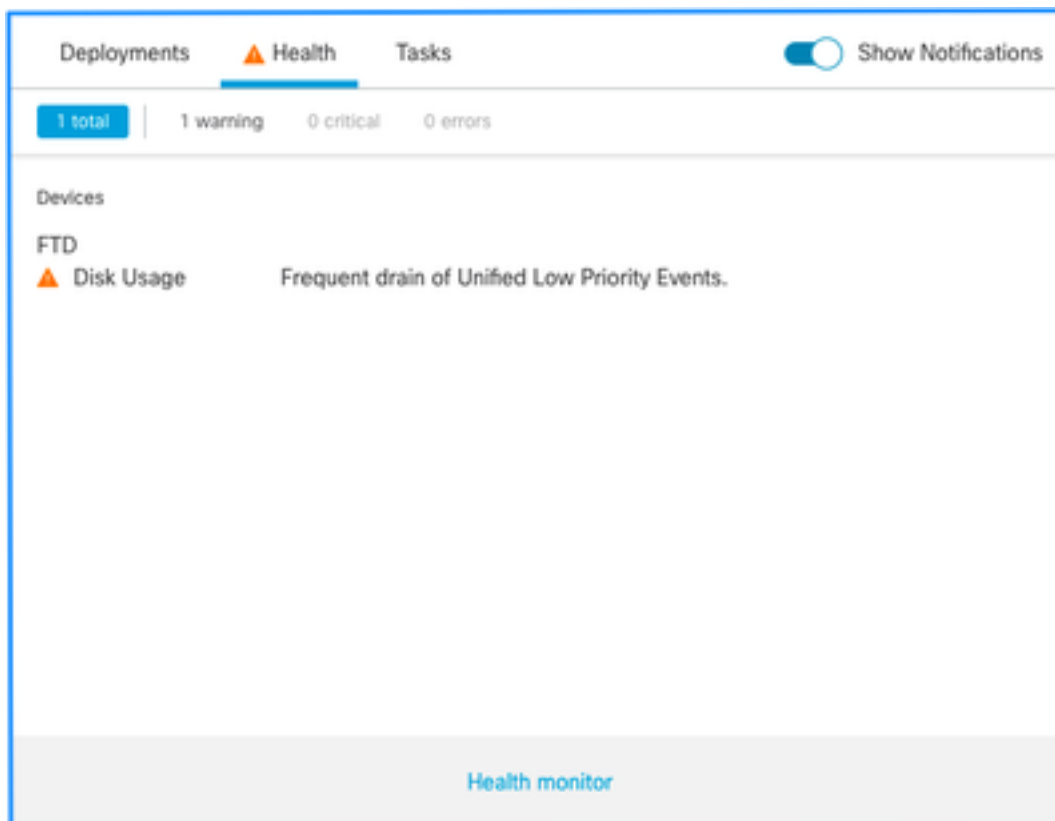
このドキュメントでは、Firepower Management Center(FMC)の未処理イベントのドレインおよびイベントの頻繁なドレインのヘルスアラートをトラブルシューティングする方法について説明します。

## 問題の概要

FMCは、次のいずれかのヘルスアラートを生成します。

- 優先順位の低い統合イベントの頻繁な枯渇  
または
- 優先順位の低い統合イベントからの未処理イベントの排出

これらのイベントはFMCで生成および表示されますが、Firepower Threat Defense(FTD)デバイスまたはNext-Generation Intrusion Prevention System(NGIPS)デバイスのいずれであっても、管理対象デバイスセンサーに関連します。このドキュメントの残りの部分では、特に指定がない限り、センサーという用語はFTDデバイスとNGIPSデバイスの両方を指しています。



ヘルスアラートの構造は次のとおりです。

- <SILO NAME>の頻繁なドレイン
- <SILO NAME>からの未処理イベントのドレイン

この例では、SILO NAMEは**Unified Low Priority Events**です。これは、ディスクマネージャのサイロの1つです（より包括的な説明については、「背景説明」セクションを参照してください）。

さらに：

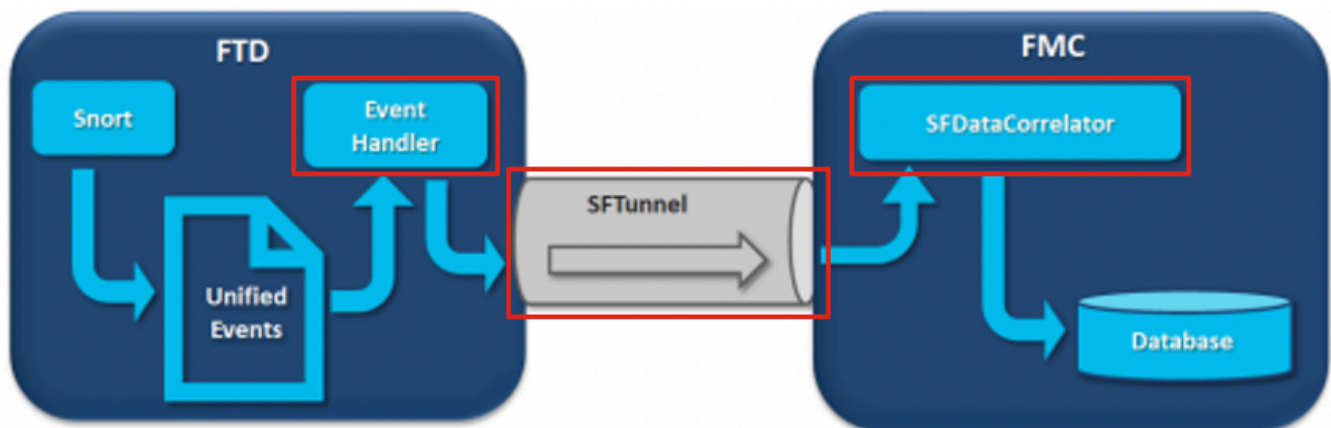
- どのサイロも技術的にはFrequent drain of <SILO NAME> ヘルスアラートを生成できますが、最も一般的に見られるのはイベントに関連するイベントで、その中でも優先度の低いイベントです。これは、単にこれらがセンサーによって頻繁に生成されるタイプのイベントであるためです。
- 「Frequent drain of <SILO NAME>」イベントは、イベント関連のサイロの場合はWarningの重大度になります。これは、このイベントが処理された場合（未処理のイベントを構成する説明が次に示されます）、FMCデータベースに存在するためです。
- 「Backups」サイロなどのイベントに関連しないサイロでは、この情報が失われるため、アラートはCriticalです。
- イベント・タイプ・サイロのみが、<SILO NAME>のヘルス・アラートから未処理のイベントのドレインを生成します。このアラートの重大度は常にCriticalです。

その他の症状としては以下のものがあります。

- FMC UIの速度低下
- イベントの損失

## 一般的なトラブルシューティングシナリオ

<SILO NAME>イベントの頻繁なドレインは、そのサイズに対してサイロへの入力が多すぎるために発生します。この場合、ディスクマネージャは、最後の5分インターバルの間に少なくとも2回そのファイルを排出（パージ）します。イベントタイプサイロでは、これは通常、そのイベントタイプの過剰なロギングによって発生します。Drain of unprocessed events of <SILO NAME> healthアラートの場合、イベント処理パスのボトルネックが原因で発生することもあります。



この図では、3つの潜在的なボトルネックがあります。

- FTDのEventHandlerプロセスがオーバーサブスクライブされている（読み取りがSnortの書き込みより遅い）
- イベントインターフェイスがオーバーサブスクライブされています
- FMCのSFDataCorrelatorプロセスがオーバーサブスクライブされている

[イベント処理](#)アーキテクチャの詳細については、それぞれの「[詳細](#)」セクションを参照してください。

### 事例1)過剰なロギング

前のセクションで説明したように、このタイプのヘルスアラートの最も一般的な原因の1つは過剰な入力です。

**show disk-manager** CLISHコマンドから収集されたLow Water Mark(LWM)とHigh Water Mark(HWM)の違いは、LWM (新たに排出) からHWM値に移行するために、そのサイロでどのくらいのスペースを確保する必要があるかを示しています。イベントが頻繁に排出される場合 (未処理のイベントの有無は問いません)、まず確認する必要があるのはロギング設定です。

[ディスクマネージャ](#)プロセスの詳細については、それぞれの「[ディープダイブ](#)」セクションを参照してください。

二重ロギングであるか、全体的なマネージャセンサーエコシステム上のイベントの割合が高いだけでも、ロギング設定を見直す必要があります。

## 推奨処置

### ステップ1: 二重ロギングの確認

次の出力に示すように、FMCの相関器perfstatsを調べると、二重ロギングシナリオを特定できます。

```
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
```

この場合、重複したフローの高いレートが出力に表示されます。

### ステップ2: ACPのロギング設定を確認する

まず、アクセスコントロールポリシー(ACP)のロギング設定を確認する必要があります。このドキュメント『[接続ロギングのベストプラクティス](#)』で説明されているベストプラクティスに従っていることを確認します

リストされている推奨事項は単に二重ロギングのシナリオをカバーするものではないため、ロギング設定のレビューはすべての状況で推奨されます。

### ステップ3: 過剰なロギングが予想されているかどうかを確認する

過剰なロギングに予想される原因があるかどうかを確認する必要があります。過剰なロギングが

DOS/DDoS攻撃やルーティングループ、または膨大な数の接続を行う特定のアプリケーションやホストによって引き起こされている場合は、予期しない過剰な接続ソースからの接続をチェックし、緩和または停止する必要があります。

#### ステップ4：モデルのアップグレード

FTDハードウェアデバイスを高性能モデル（たとえば、FPR2100 → FPR4100）にアップグレードすると、サイロのソースが増加します。

#### ステップ5:[Log to Ramdisk]を無効にできるかどうかを検討します

Unified Low Priority Eventsサイロの場合は、「[Log to Ramdisk](#)」を無効にしてサイロサイズを増やすことができます。これについては、それぞれの「[詳細な説明](#)」セクションで説明しています。

#### 事例2)センサとFMC間の通信チャンネルのボトルネック

このタイプのアラートのもう1つの一般的な原因は、接続の問題や、センサーとFMC間の通信チャンネル(sftunnel)の不安定性です。通信の問題は、次の原因によって発生する可能性があります。

- sftunnelがダウンしているか、不安定である（フラップ）。
- sftunnelはオーバーサブスクライブされています。

sftunnel接続の問題については、FMCとセンサーがTCPポート8305の管理インターフェイス間で到達可能であることを確認します。

FTDでは、`[ngfw]/var/log/messages`ファイルでsftunneld文字列を検索できます。接続の問題により、次のようなメッセージが生成されます。

```
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] sftunnelid:sf_ssl [INFO] Initiating IPv4
connection to 10.62.148.75:8305/tcp
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunnelid:sf_ssl [INFO] Wait to connect to 8305
(IPv6): 10.62.148.75
```

FMC管理インターフェイスのオーバーサブスクリプションは、管理トラフィックの急増または継続的なオーバーサブスクリプションの可能性があります。ヒースモニターからの履歴データは、この良い指標です。

最初に注意すべき点は、ほとんどの場合、FMCは管理用に単一のNICを使用して導入されていることです。このインターフェイスは次の目的で使用されます。

- FMC管理。
- FMCセンサー管理。
- センサーからのFMCイベントコレクション。
- インテリジェンスフィードの更新。
- ソフトウェアダウンロードサイトからSRU、ソフトウェア、VDB、およびGeoDBのアップデートをダウンロードします。
- URLレピュテーションとカテゴリのクエリ ( 該当する場合 ) 。
- ファイルディスポジションのクエリ ( 該当する場合 ) 。

## 推奨処置

イベント専用インターフェイス用の2つ目のNICをFMCに導入できます。実装はユースケースによって異なります。

一般的なガイドラインについては、『FMC Hardware Guide [Deploying on a Management Network](#)』を参照してください。

## ケース3. SFDataCorrelatorプロセスのボトルネック

最後に、SFDataCorrelator側(FMC)でボトルネックが発生する場合について説明します。

最初の手順では、次のような重要な情報が収集されるため、diskmanager.logファイルを調べます。

- ドレインの周波数。
- 未処理イベントが排出されたファイルの数です。
- 未処理イベントを含むドレインの発生。

diskmanager.logファイルとその解釈方法については、「[ディスクマネージャ](#)」の項を参照してください。diskmanager.logから収集した情報を使用して、以降の手順を絞り込むことができます。

さらに、相関器のパフォーマンス統計情報を確認する必要があります。

```
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

これらの統計情報はFMC用であり、FMCによって管理されるすべてのセンサーの集約に対応することに注意してください。優先順位の低い統合イベントの場合、主に次の項目を検索します。

- SFDataCorrelatorプロセスのオーバーサブスクリプションの可能性を評価するための、任意のイベントタイプの1秒あたりのフローの合計。
- 前の出力で強調表示されている2つの行は次のとおりです。 **rna flows/second**:SFDataCorrelatorによって処理される優先度の低いイベントの割合を示します。  
**rna dup flows/second**:SFDataCorrelatorによって処理される、重複した優先順位の低いイベントの割合を示します。これは、前のシナリオで説明した二重ロギングによって生成されます。

出力から、次のように結論付けられます。

- rna dup flows/second行で示される重複ロギングはありません。
- rna flows/second行のMaximum値はAverage値よりもはるかに高いため、SFDataCorrelatorプロセスによって処理されるイベントのレートが急上昇しました。これは、ユーザの勤務時間が始まったばかりの早朝を見れば予想できますが、一般的には赤旗であり、さらに調査する必要があります。

SFDataCorrelatorプロセスの詳細については、「[イベント処理](#)」セクションを参照してください。

## 推奨処置

まず、スパイクが発生した時期を判別する必要があります。これを行うには、各5分のサンプル間隔ごとの相関統計を調べる必要があります。diskmanager.logから収集した情報は、重要な期間に直接移動するのに役立ちます。

**ヒント**：簡単に検索できるように、出力をLinuxのポケットベルにより少ないパイプで送ります。

```
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
```

出力の情報を使用して、次のことを行います。

- イベントの通常/ベースライン率を決定します。
- スパイクが発生した5分インターバルを判別します。

前の例では、16:06:39以降に受信したイベントのレートに明らかなスパイクがあります。これらは5分間の平均値であるため、増加は示されている(バースト)よりも急激ですが、この5分間の間隔の終わりのほうから始まった場合は薄くなります。

この結果、このイベントのスパイクが未処理のイベントのドレインを引き起こしたという結論が導き出されますが、このスパイク内のFTDボックスを通過した接続のタイプを理解するために、適切なタイムウィンドウを使用してFMCのグラフィカルユーザインターフェイス(GUI)から接続イベントを調べることができます。

The screenshot displays the 'Events Time Window' configuration interface. At the top, there are tabs for 'Events Time Window' and 'Preferences'. Below the tabs, a dropdown menu is set to 'Static Time Window'. Underneath, there are two main sections: 'Start Time' and 'End Time'. The 'Start Time' is configured to '2020-09-09 17:06' and the 'End Time' is '2020-09-09 17:16'. Both sections include a calendar view for September 2020, with the 9th of the month highlighted. To the right of these sections is a 'Presets' list with two columns: 'Last' and 'Current'. The 'Last' column lists '1 hour', '6 hours', '1 day', '1 week', '2 weeks', and '1 month'. The 'Current' column lists 'Day', 'Week', 'Month', 'Synchronize with', 'Audit Log Time Window', and 'Health Monitoring Time Window'. At the bottom of the interface, it indicates a '10 minutes' interval.

このタイムウィンドウを適用して、フィルタリングされた接続イベントを取得します。タイムゾーンを忘れずに設定してください。この例では、センサーはUTCとFMCのUTC+1を使用します。テーブルビューを使用してイベントの過負荷を引き起こしたイベントを確認し、それに応じたア

クシヨンを実行します。

First Packet	Last Packet	Action	Initiator IP	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Policy	Access Control Rule	Device	Initiator Packets	Responder Packets
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	252.100.225.71	192.168.1.10	Inside	Protected	35300 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	44.183.125.50	192.168.1.10	Inside	Protected	35299 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	113.95.212.110	192.168.1.10	Inside	Protected	35303 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	199.189.50.240	192.168.1.10	Inside	Protected	35312 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	190.100.218.132	192.168.1.10	Inside	Protected	35316 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	202.144.82.61	192.168.1.10	Inside	Protected	35317 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	58.210.173.312	192.168.1.10	Inside	Protected	35335 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	100.24.73.141	192.168.1.10	Inside	Protected	35302 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	174.116.39.135	192.168.1.10	Inside	Protected	35301 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	160.243.31.20	192.168.1.10	Inside	Protected	35309 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	118.43.215.125	192.168.1.10	Inside	Protected	35341 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	61.119.209.152	192.168.1.10	Inside	Protected	35306 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	144.228.255.110	192.168.1.10	Inside	Protected	35310 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	114.70.178.151	192.168.1.10	Inside	Protected	35325 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	206.186.109.246	192.168.1.10	Inside	Protected	35350 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	80.73.62.183	192.168.1.10	Inside	Protected	35311 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	78.0.160.78	192.168.1.10	Inside	Protected	35382 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	132.234.204.95	192.168.1.10	Inside	Protected	35351 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	155.233.203.202	192.168.1.10	Inside	Protected	35357 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	121.509.228.67	192.168.1.10	Inside	Protected	35385 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	115.139.55.41	192.168.1.10	Inside	Protected	35363 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	144.192.9	192.168.1.10	Inside	Protected	35386 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	215.216.177.95	192.168.1.10	Inside	Protected	35387 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	186.208.5.119	192.168.1.10	Inside	Protected	35391 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1
2020-09-09 17:16:00	2020-09-09 17:16:31	Allow	202.95.36.125	192.168.1.10	Inside	Protected	35395 / tcp	80 (http) / tcp	FTD_Router_Policy	Default Inspection	FTD	1	1

タイムスタンプ (最初と最後のパケットの時間) に基づくと、これらは短命な接続であることがわかります。さらに、[Initiator Packets]列と[Responder Packets]列は、各方向で交換されたパケットが1つだけであることを示しています。これにより、接続が短時間で終われ、データがほとんど交換されなかったことが確認されます。

また、これらのフローがすべて同じレスポンスIPとポートをターゲットとしていることも確認できます。また、これらはすべて同じセンサーによって報告されます (入力と出力のインターフェイス情報とともに、このフローの場所と方向に通信できます)。追加アクション:

- 宛先エンドポイントのSyslogを確認します。
- DOS/DDOS保護の実装、またはその他の予防措置を講じる。

注: この記事の目的は、未処理イベントのドレインアラートをトラブルシューティングするためのガイドラインを提供することです。この例では、ping3を使用して宛先サーバへのTCP SYNフラッドを生成しています。FTDデバイスを強化するためのガイドラインについては、『[Cisco Firepower Threat Defense強化ガイド](#)』を参照してください

## Cisco Technical Assistance Center(TAC)に連絡する前に収集すべき項目

Cisco TACに連絡する前に、次の項目を収集することを強く推奨します。

- 表示されたヘルスアラートのスクリーンショット。
- FMCから生成されたファイルをトラブルシューティングします。
- 該当するセンサーから生成されたファイルをトラブルシューティングします。
- 問題が最初に発生した日時。
- ポリシーに対する最近の変更に関する情報 (該当する場合)。
- 「[イベント処理](#)」セクションで説明されているstats\_unified.plコマンドの出力と、影響を受けるセンサーの説明。

## 分析 [英語]

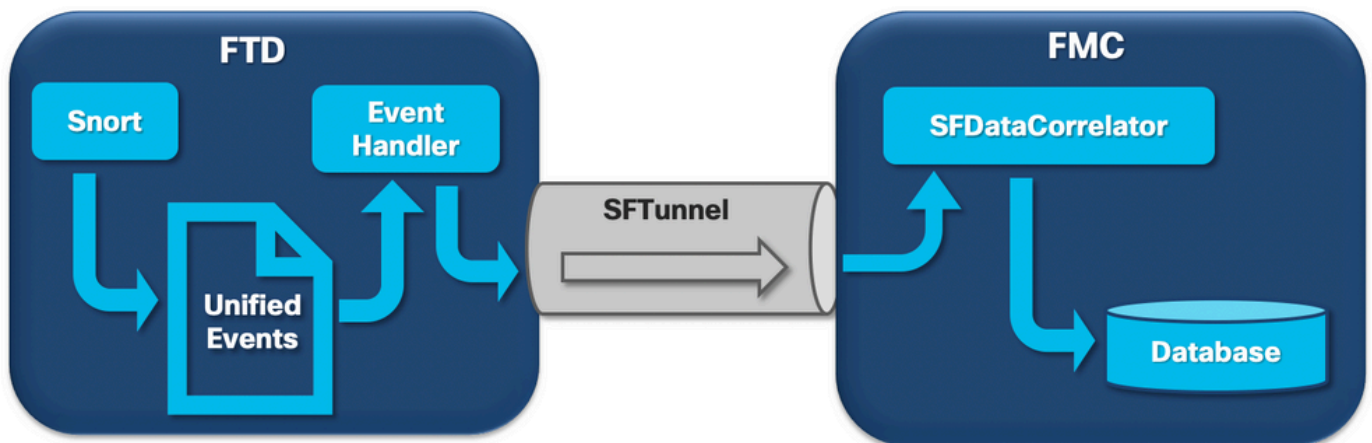
このセクションでは、このタイプのヘルスアラートに關与する可能性があるさまざまなコンポーネントについて詳しく説明します。これには、次のような特徴があります。

- イベント処理：センサーデバイスとFMCの両方で発生するパスイベントをカバーします。これは主に、ヘルスアラートがイベントタイプサイロを参照する場合に役立ちます。
- ディスク・マネージャ：ディスク・マネージャのプロセス、サイロ、それらの排出の方法について説明します。
- ヘルスモニタ：ヘルスマニタモジュールを使用してヘルスアラートを生成する方法を示します。
- Log to Ramdisk:Ramdiskへのロギング機能と、ヘルスアラートへの潜在的な影響について説明します。

イベントの枯渇に関するヘルスアラートを理解し、潜在的な障害ポイントを特定するには、これらのコンポーネントがどのように動作し、相互に作用するかを調べる必要があります。

## イベント処理

Frequent Drainタイプのヘルスアラートは、イベントに関連しないサイロによってトリガーされる可能性があります。Cisco TACで確認されるケースの大部分は、イベント関連情報の枯渇に関連しています。また、未処理のイベントの流出を構成するものを理解するには、イベント処理アーキテクチャとそれを構成するコンポーネントを確認する必要があります。



Firepowerセンサーが新しい接続からパケットを受信すると、snortプロセスはイベントをunified2形式で生成します。これは、より高速な読み取り/書き込みと軽いイベントを可能にするバイナリ形式です。

この出力は、新しい接続が作成されたことを確認できるFTDコマンドsystem support traceを示しています。重要な部分を強調表示して説明します。

```

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ファイルは、インスタンスごとにパス

```



Rule ID: 268437505  
Tunnel Rule ID: 0  
Monitor Rule ID: <none>  
Rule Action: 2

すべてのunified\_eventsファイルの横に、2つの重要な値を含むブックマークファイルがあります。

1. そのインスタンスと優先順位の現在のunified\_eventsファイルに対応するタイムスタンプ。
2. unified\_eventファイルの最後の読み取りイベントのバイト単位の位置。

値は、次の例に示すように、カンマで区切られた順序で並んでいます。

```
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-68e7af9190591599862498, 18754115
```

これにより、ディスクマネージャプロセスは、どのイベントがすでに処理され ( FMCに送信され )、どのイベントがまだ処理されていないかを知ることができます。

ディスクマネージャがイベントサイロを削除すると、ユニファイドイベントファイルが削除されることに注意してください。サイロの排除の詳細については、「[ディスクマネージャ](#)」の項を参照してください。

ドレインされた統合ファイルは、次のいずれかが当てはまる場合、未処理のイベントを持つとみなされます。

1. ブックマークのタイムスタンプがファイルの作成時刻より小さい。
2. ブックマークのタイムスタンプはファイルの作成時刻と同じであり、ファイル内のバイト単位の位置はそのサイズよりも小さくなります。

EventHandlerプロセスは、統合されたファイルからイベントを読み取り、それらをセンサーとFMC間の暗号化通信を行うプロセスであるsftunnel経由で ( メタデータとして ) FMCにストリームします。これはTCPベースの接続であるため、イベントストリーミングはFMCによって確認応答されます。

[/ngfw]/var/log/messagesファイルで次のメッセージを確認できます。

```
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
```

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

次の出力は、次の情報を提供します。

- Snortは出力用に ( 書き込み用に ) unified\_eventsファイルを開きました。
- イベントハンドラは、同じunified\_eventsファイルを開きました ( このファイルから読み取るため )。
- sftunnelは、そのunified\_eventsファイルから処理されたイベントの数を報告しました。

その後、ブックマークファイルが更新されます。sftunnelは、高優先度イベントと低優先度イベントにそれぞれUnified Events(UE)Channel 0と1という2つの異なるチャンネルを使用します。

FTDでsfunnel\_status CLIコマンドを使用すると、ストリームされたイベントの数を確認できます

。

```
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
```

FMCでは、イベントはSFDataCorrelatorプロセスによって受信されます。

各センサーから処理されたイベントのステータスは、stats\_unified.plコマンドで確認できます。

```
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

このコマンドは、チャンネルごとに特定のデバイスのイベントのバックログのステータスを表示します。使用されるチャンネルIDはsftunnelと同じです。

Bytes Behind値は、ユニファイドイベントブックマークファイルに表示される位置とユニファイドイベントファイルのサイズの差、およびブックマークファイルよりもタイムスタンプの高い後続ファイルの差として計算できます。

SFDataCorrelatorプロセスは、パフォーマンス統計情報も保存します。パフォーマンス統計情報は/var/sf/rna/correlator-stats/に保存されます。1日に1つのファイルが作成され、その日のパフォーマンス統計情報がCSV形式で保存されます。ファイル名は「YYYY-MM-DD」の形式を使用し、現在の日付に対応するファイルはnowと呼ばれます。

統計情報は5分ごとに収集されます (5分インターバルごとに1つの行があります)。

このファイルの出力は、perfstatsコマンドで読み取ることができます。このisコマンドは、snortパフォーマンス統計情報ファイルの読み取りにも使用されるため、適切なフラグを使用する必要があります。

-C:perfstatsに、入力が相関統計ファイルであることを指示します (このフラグを指定しない場合、perfstatsは入力がSnortパフォーマンス統計ファイルであると仮定します)。

-q:Quietモードでは、ファイルの概要だけが出力されます。

```
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

```

サマリーの各口ーには、次の順序で3つの値があります。平均、最小、最大。

-qフラグを付けずに出力すると、5分インターバルの値も表示されます。最後にサマリーを示します。

各FMCには、データシートに記載されている最大フローレートがあります。次の表に、各データシートから取得したモジュールごとの値を示します。

モデル	FMC 750	FMC 1000	FMC 1600	FMC 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMC
最大流量(fps)	2000	5000	5000	12000	12000	12000	20,000	20,000	20,000	可変	12

これらの値は、SFDataCorrelatorの統計出力に太字で示されているすべてのイベントタイプの集約に使用されます。

出力を見て、最悪のシナリオ(すべての最大値が同時に発生する場合)に備えた方法でFMCのサイズを設定すると、FMCが認識するイベントのレートは  $48.65 + 348.15 + 4.63 + 3.25 + 0.06 = 404.74$  fpsになります。

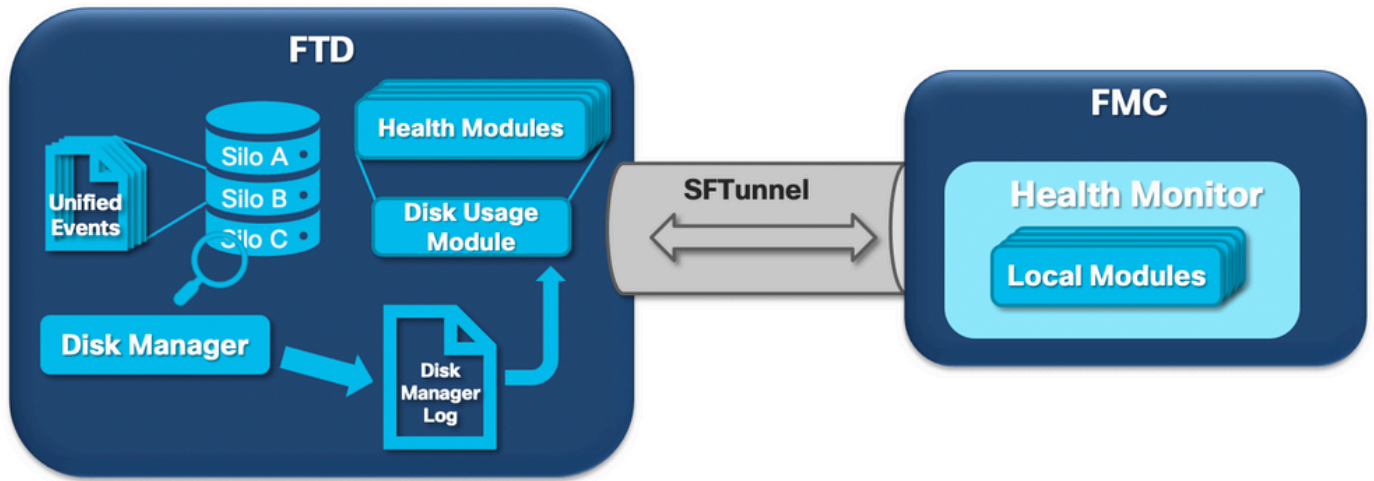
この合計値は、各モデルのデータシートの値と比較できます。

また、SFDataCorrelatorは受信したイベントに加えて(相関規則など)追加の作業を行い、それらをデータベースに格納します。データベースは、ダッシュボードやイベントビューなど、FMCのグラフィカルユーザインターフェイス(GUI)でさまざまな情報を入力するために照会されます。

## ディスクマネージャ

次の論理ダイアグラムは、Health MonitorプロセスとDisk Managerプロセスの両方の論理コンポーネントを示しています。これらは、ディスク関連のヘルスアラートを生成するために相互に絡み合っています。





簡単に言うと、ディスクマネージャプロセスはボックスのディスク使用量を管理し、設定ファイルは[/ngfw]/etc/sf/フォルダにあります。ディスクマネージャプロセスには、特定の状況で使用される複数のコンフィギュレーションファイルがあります。

- diskmanager.conf : 標準構成ファイル。
- diskmanager\_2hd.conf – ボックスに2つのハードドライブがインストールされている場合に使用します。2番目のハードドライブは、ファイルポリシーで定義されているようにファイルを保存するために使用されるマルウェア拡張に関連するものです。
- ramdisk-diskmanager.conf - Log to Ramdiskが有効な場合に使用します。詳細については、「[RAMディスクへのログ](#)」セクションを参照してください。

ディスク・マネージャによって監視される各タイプのファイルには、サイロが割り当てられます。システムで使用可能なディスク容量に基づいて、ディスクマネージャは各サイロのHigh Water Mark(HWM)とLow Water Mark(LWM)を計算します。

ディスク・マネージャ・プロセスがサイロを排出する場合、LWMに到達するまで処理が行われません。イベントはファイルごとに排出されるため、このしきい値を超える可能性があります。

センサーデバイスのサイロのステータスを確認するには、次のコマンドを使用できます。

```
> 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
```

次のいずれかの条件が満たされると、ディスクマネージャプロセスが実行されます。

- プロセスが開始 ( または再起動 ) します
- サイロがHWMに到達する
- サイロが手動でドレインされる
- 1時間に1回

ディスクマネージャプロセスを実行するたびに、独自のログファイルに異なるサイロのエントリが生成されます。このログファイルは[/ngfw]/var/log/diskmanager.logの下にあり、CSV形式のデータを持ちます。

次に、Unified Low Priority Eventsヘルスアラートからの未処理イベントの削除をトリガーしたセンサーからのdiskmanager.logファイルのサンプル行と、それぞれの列の内訳を示します。

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

カラム	値
サイロラベル	priority_2_events
排液時間 ( エポック時間 )	1599668981
排出されたファイルの数	221
排出バイト数	4587929508
ドレイン後のデータの現在のサイズ ( バイト )	1132501868
排出される最大ファイル ( バイト )	20972020
排出される最小ファイル ( バイト )	4596
排出された最も古いファイル ( エポック時間 )	1586044534
高水準点 ( バイト )	5710966962
ロー・ウォーターマーク ( バイト )	1142193392
未処理のイベントが排出されたファイルの数	110
Diskmanager状態フラグ	0

この情報は、それぞれのヘルスマニタモジュールによって読み取られ、関連するヘルスアラートがトリガーされます。

## サイロを手動で削除する

特定のシナリオでは、サイロを手動で削除できます。たとえば、手動でファイルを削除する代わりに手動でサイロドレインを使用してディスク領域をクリアするには、ディスクマネージャが保持するファイルと削除するファイルを決定する利点があります。ディスクマネージャは、そのサイロの最新のファイルを保持します。

どのサイロもドレイン可能で、すでに説明したように動作します ( データ量がLWMしきい値を下回るまで、ディスクマネージャがデータをドレインします )。 **system support silo-drain** コマンドはFTD CLISHモードで使用でき、使用可能なサイロ ( 名前+数値ID ) のリストを提供します。

次に、Unified Low Priority Eventsサイロの手動ドレインの例を示します。

> 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
<b>Unified Low Priority Events</b>	<b>2.397 GB</b>	<b>1.061 GB</b>	<b>5.307 GB</b>
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
<b>Unified Low Priority Events</b>	<b>1.046 GB</b>	<b>1.061 GB</b>	<b>5.307 GB</b>
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

## ヘルスマニタ

主なポイントは次のとおりです。

- FMCの[Health Monitor]メニューまたは[Message Center]の[Health]タブに表示されるヘルスアラートは、Health Monitorプロセスによって生成されます。
- このプロセスは、FMCと管理対象センサーの両方についてシステムの状態を監視し、多数の異なるモジュールで構成されます。
- ヘルスアラートモジュールは、デバイスごとにアタッチできる[ヘルスポリシー](#)で定義されます。
- ヘルスアラートは、Disk Usageモジュールによって生成されます。このモジュールは、FMCによって管理される各センサーで実行できます。
- FMC上でヘルスマニタプロセスが（5分に1回または手動実行がトリガーされたときに）実行されると、ディスク使用状況モジュールはdiskmanager.logファイルを調べ、正しい条件が満たされると、それぞれのヘルスアラートがトリガーされます。

**Drain of Unprocessed events**ヘルスアラートをトリガーするには、次の条件をすべて満たす必要があります。

1. Bytes drainedフィールドが0より大きい（このサイロのデータが排出されたことを示す）。
2. 未処理のイベントが0より多く排出されたファイルの数（これは、排出されたデータ内に未処理のイベントがあったことを示します）。
3. ドレインの時間は過去1時間以内です。

**Frequent Drain of events**ヘルスアラートをトリガーするには、次の条件が満たされている必要があります。

1. diskmanager.logファイルの最後の2つのエントリは、次の操作を行う必要があります。  
Have Bytes drained field greater than 0（これは、このサイロからのデータが排出されたことを示します）。5分未満の間隔を空けてください。
2. このサイロの最後のエントリのドレイン時間は、過去1時間以内です。

ディスク使用モジュールから収集された結果（および他のモジュールで収集された結果）は、sftunnel経由でFMCに送信されます。sftunnel\_statusコマンドを使用すると、sftunnelを介して交換されるヘルスイベントのカウンタを確認できます。

```
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
```

## RAMディスクにログインします。

ほとんどのイベントはディスクに保存されますが、イベントの定期的な書き込みと削除によってSSDが徐々に損傷を受けないように、デバイスはデフォルトでRAMディスクにログを記録するように設定されています。

このシナリオでは、イベントは[/ngfw]/var/sf/detection\_engine/\*/instance-Nの下に保存されていませんが、[/ngfw]/var/sf/detection\_engines/\*/instance-N/connection/に配置されています。これは/dev/shm/instance-N/connectionへのシンボリックリンクです。この場合、イベントは物理メモリではなく仮想メモリに存在します。

```
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
```

デバイスで現在実行するように設定されていることを確認するには、FTD CLISHからshow log-events-to-ramdiskコマンドを実行します。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：**「configure log-events-to-ramdisk disable」コマンドを実行すると、Snortが「D」状態(Uninterruptible Sleep)でスタックし、トラフィックが停止しないようにするために、FTDで2つの展開を行う必要があります。

この動作は、Cisco Bug ID [CSCvz53372](#)の不具合に記載されています。最初の導入では、snortのメモリ段階の再評価がスキップされ、snortが「D」状態になります。回避策は、タミーの変更を含む別の導入を行うことです。

ramdiskにログを記録する際の主な欠点は、それぞれのサイロに割り当てられるスペースが小さいため、同じ状況で頻繁に排出されることです。次の出力は、FPR 4140からのディスクマネージャで、比較のためにramdiskへのログイベントが有効になっているものと無効になっているものです。

## RAMディスクへのログが有効

```
> show disk-manager
```

	Used	Minimum	Maximum
Silo			
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
<b>Connection Events</b>	<b>0 KB</b>	<b>451.698 MB</b>	<b>903.396 MB</b>
IPS Events	0 KB	12.357 GB	26.479 GB

## RAMディスクへのログが無効

```

> 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

```

サイロのサイズが小さいほど、イベントにアクセスしてFMCにストリームする速度が速くなります。これは適切な条件下では優れたオプションですが、欠点を考慮する必要があります。

## よく寄せられる質問 (FAQ)

Drain of EventsヘルスアラートはConnection Eventsによってのみ生成されますか。

No.

- Frequent Drainのアラートは、どのディスク・マネージャ・サイロでも生成できます。
  - 未処理イベントのドレインのアラートは、イベント関連の任意のサイロで生成できます。
- 最も一般的な原因は接続イベントです。

Frequent Drainヘルスアラートが表示されたら、Log to Ramdiskをディセーブルにすることをお勧めします。

いいえ。DOS/DDOSを除く過剰なロギングのシナリオでのみ、影響を受けるサイロが接続イベントサイロである場合、およびロギング設定をさらに調整できない場合にのみ使用します。

DOS/DDOSが過度のロギングを引き起こす場合の解決策は、DOS/DDOS保護を実装するか、DOS/DDOS攻撃の原因を排除することです。

デフォルトの機能「Log to Ramdisk」はSSDの消費を減らすため、使用することを強くお勧めします。

未処理のイベントを構成するものはどれか？

イベントは個別に未処理としてマークされません。次の場合、ファイルに未処理のイベントがあります。

その作成タイムスタンプは、それぞれのブックマークファイル内のタイムスタンプフィールドよりも大きくなります。

または

その作成タイムスタンプは、各ブックマークファイルのtimestampフィールドと同じで、サイズ

は各ブックマークファイルのposition in Bytesフィールドよりも大きくなります。

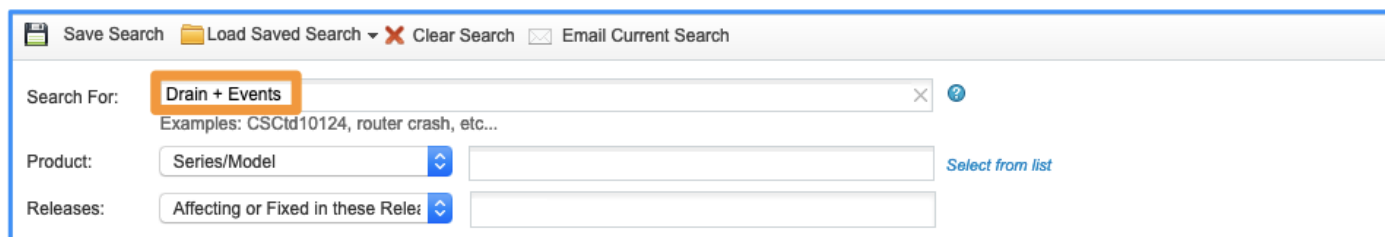
FMCは特定のセンサーの後ろのバイト数をどのように知りますか。

センサーは、unified\_eventsファイルの名前とサイズ、およびブックマークファイルの情報に関するメタデータを送信します。これにより、FMCは次のようにバイト数を計算するのに十分な情報を取得できます。

Current unified\_events file size - Position in Bytes」フィールド (ブックマークファイルからのバイト数) +各ブックマークファイル内のタイムスタンプよりも高いタイムスタンプを持つすべてのunified\_eventsファイルのサイズ。

## 既知の問題

[Bug Search Tool](#)を開き、次のクエリを使用します。



The screenshot shows the Bug Search Tool interface. At the top, there are buttons for 'Save Search', 'Load Saved Search', 'Clear Search', and 'Email Current Search'. The 'Search For:' field contains the query 'Drain + Events' and has a help icon. Below it, examples are listed: 'Examples: CSCtd10124, router crash, etc...'. The 'Product:' field has a dropdown menu with 'Series/Model' selected and a 'Select from list' link. The 'Releases:' field has a dropdown menu with 'Affecting or Fixed in these Rele:' selected.



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。