排除FMC未处理事件的排放和频繁事件排放运行状况监视器警报

目录

简介

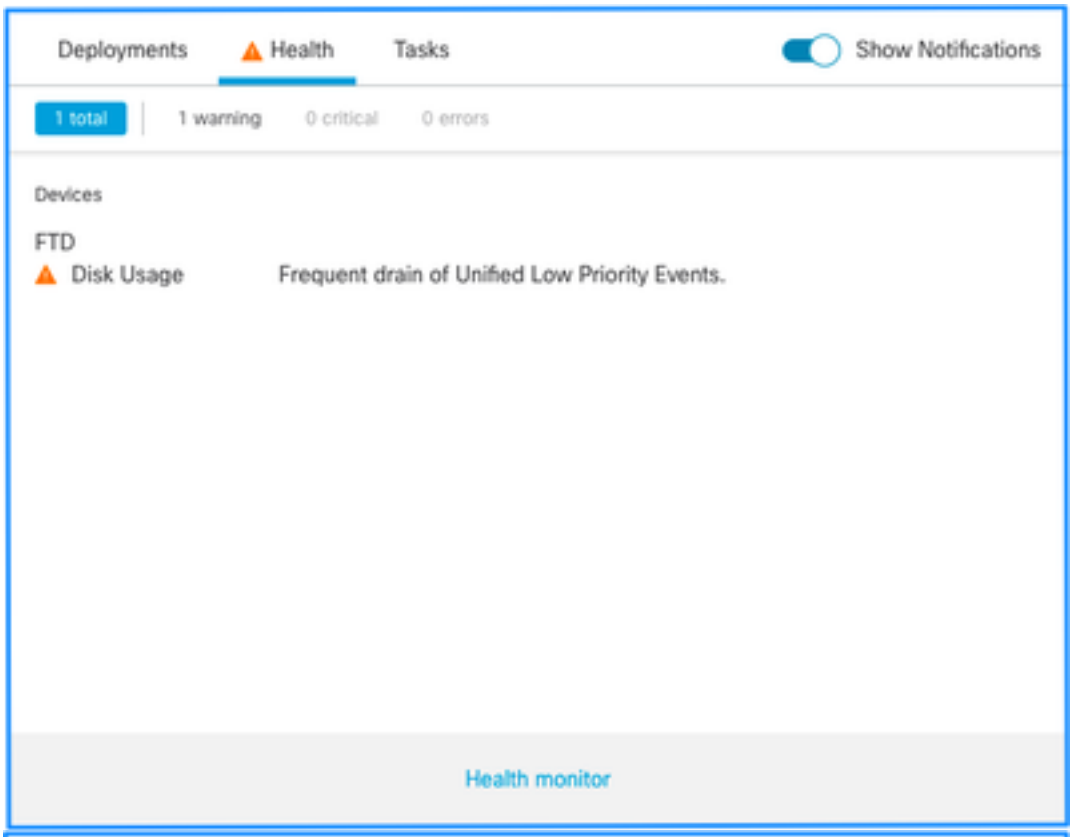
本文档介绍如何对Firepower管理中心(FMC)上的**Drain of Unprocessed Events**和**Frequent Drain of Events**运行状况警报进行故障排除。

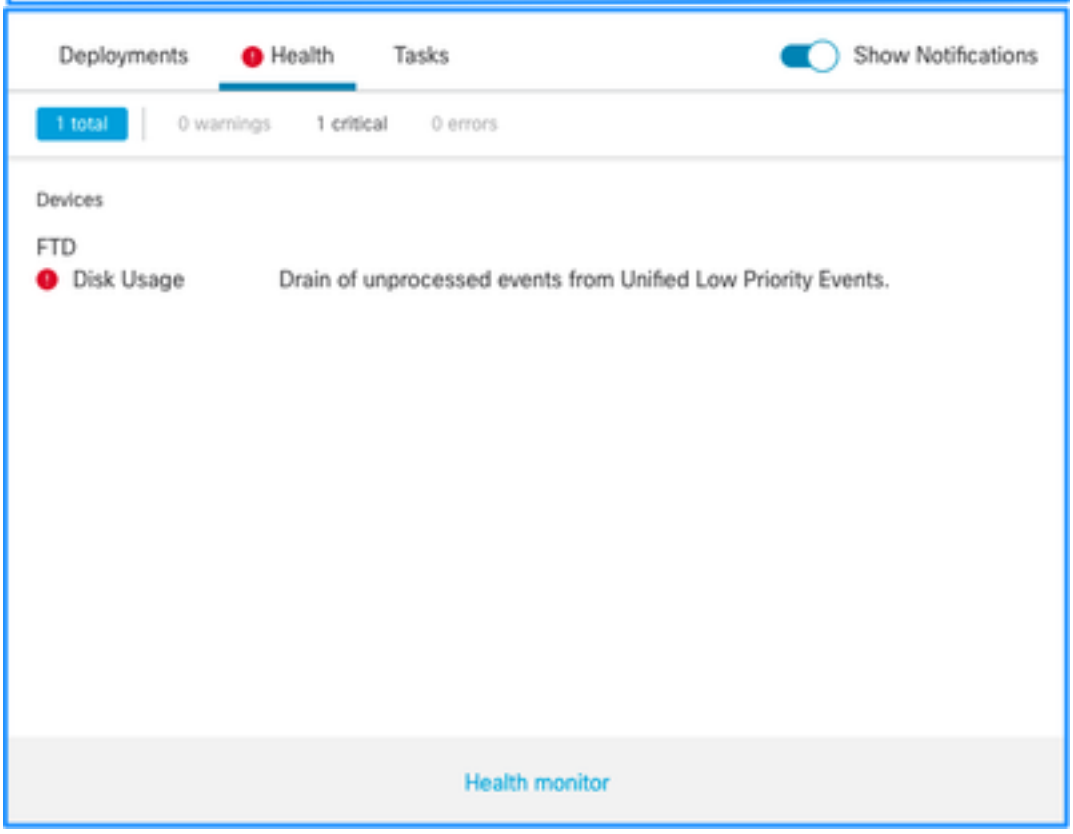
问题概述

FMC生成以下运行状况警报之一：

- 统一低优先级事件的频繁流失
  和/或
- 从统一低优先级事件中排出未处理的事件

虽然这些事件在FMC中生成并显示，但它们与受管设备传感器(无论是Firepower威胁防御(FTD)设备还是下一代入侵防御系统(NGIPS)设备)相关。在本文档的其余部分，除非另有说明，术语“传感器”同样指FTD和NGIPS设备。





这是运行状况警报结构：

- 频繁耗尽<SILO NAME>
- 从<SILO NAME>中排出未处理的事件

在本示例中，思洛存储器名称为**Unified Low Priority Events**。这是其中一个磁盘管理器孤岛（有关更全面的说明，请参见“背景信息”部分）。

此外：

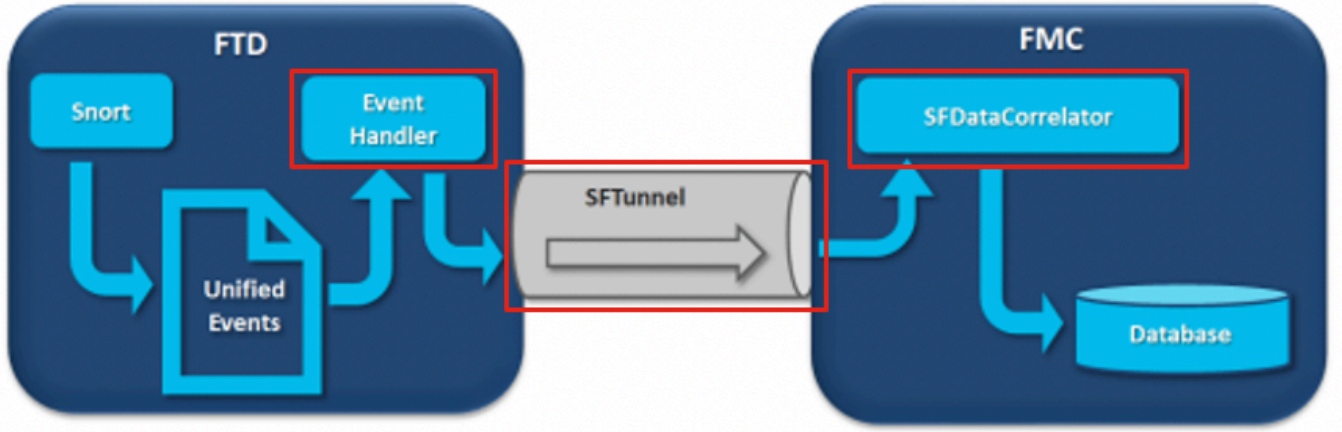
- 尽管任何思洛存储器从技术上讲都可以生成Frequent drain of <SILO NAME> health警报，但最常见的是与事件相关的警报，其中低优先级事件只是因为这些事件类型更常由传感器生成。
- “频繁排出<SILO NAME>”事件具有警告严重性（如果它是与事件相关的思洛存储器），因为如果处理了此事件（接下来说明了什么构成未处理事件），则它们在FMC数据库中。
- 对于非事件相关的思洛存储器（如“备份”思洛存储器），警报是严重的，因为此信息已丢失。
- 只有事件类型孤岛会从<SILO NAME>运行状况警报中生成未处理事件的排出。此警报始终具有“严重”严重性。

其他症状可能包括：

- FMC UI缓慢
- 事件丢失

常见故障排除场景

频繁地耗尽<SILO NAME>事件是因为向思洛存储器输入的数据过多，超过其大小。在这种情况下，磁盘管理器将在最后5分钟间隔内至少两次清空（清除）该文件。在事件类型接收器中，这通常是由该事件类型记录过多造成的。如果<SILO NAME>运行状况警报的未处理事件排出，这也可能是事件处理路径中的瓶颈所导致的。



图中存在3个潜在的瓶颈：

- FTD上的EventHandler进程超订用（其读取速度比Snort写入的慢）
- 事件接口超订用
- FMC上的SFDataCorrelator进程超订用

要深入了解事件处理架构，请参阅各自的深入探讨部分。

案例1.过度记录

如上一节所述，此类型运行状况警报的最常见原因之一是输入过多。

从**show disk-manager** CLISH命令收集的低水位标记(LWM)和高水位标记(HWM)之间的差异显示了需要占用多少空间才能从LWM（新排出）到HWM值。如果频繁地耗尽事件（无论有无未经处理的事件），您必须首先检查日志记录配置。

有关Disk Manager过程的详细说明，请参阅相应的Deep Dive部分。

无论是双日志记录还是整个manager-sensors生态系统上的事件率较高，都必须检查日志记录设置。

推荐的操作

步骤1.检查双重日志记录

如果您查看FMC上的相关器**perfstats**，可以识别双重日志记录场景，如以下输出所示：

```
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
```

在这种情况下，输出中可以看到较高的重复流率。

步骤2.检查ACP的日志记录设置

您必须首先检查访问控制策略(ACP)的日志记录设置。 确保遵循本文档连接日志记录的最佳实践中描述的最佳实践

建议在所有情况下都检查日志记录设置，因为列出的建议不仅包括双重日志记录方案。

步骤3.检查是否应进行过多的日志记录

您必须检查过多的日志记录是否有预期的原因。如果过多的日志记录是由DOS/DDoS攻击、路由环路或产生大量连接的特定应用/主机导致的，您必须检查并减少/停止来自意外过多连接源的连接。

步骤4.升级模式

将FTD硬件设备升级到更高性能的型号（例如FPR2100 —> FPR4100），思洛存储器源将会增加。

步骤5.考虑是否可以禁用Log to Ramdisk

对于Unified Low Priority Events思洛存储器，您可以禁用Log to Ramdisk，以增大思洛存储器大小，其缺点在各自的深入分析部分中讨论。

案例2.传感器与FMC之间通信通道的一个瓶颈

此类警报的另一个常见原因是传感器和FMC之间的通信信道(sftunnel)存在连接问题和/或不稳定性。通信问题可能是由于：

- sftunnel关闭或不稳定（摆动）。
- sftunnel超订用。

对于sftunnel连接问题，请确保FMC和传感器在TCP端口8305上的管理接口之间具有可达性。

在FTD上，您可以在[/ngfw]/**var/log/messages**文件中搜索**sftunneld**字符串。连接问题会导致生成如下消息：

```
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管理接口的超订用可能是管理流量激增或持续超订用。健康监测仪的历史数据就是很好的指标。

首先需要注意的是，在大多数情况下，FMC都部署了单个网卡用于管理。此接口用于：

- FMC管理。
- FMC传感器管理。
- 从传感器收集FMC事件。
- 更新情报源。
- 从软件下载站点下载SRU、软件、VDB和GeoDB更新。
- 查询URL信誉和类别（如果适用）。
- 文件性质查询（如果适用）。

推荐的操作

您可以在FMC上为事件专用接口部署第二个NIC。实施可能取决于使用案例。

有关一般指南，请参阅FMC硬件指南在管理网络上部署

案例3. SFDataCorrelator流程的一个瓶颈

最后要介绍的场景是SFDataCorrelator端(FMC)出现瓶颈时。

第一步是查看diskmanager.log文件，因为需要收集以下重要信息：

- 排水管的频率。
- 已耗尽未处理事件的文件数。
- 具有未处理事件的排出发生。

有关diskmanager.log文件及其解释方法的信息，请参阅磁盘管理器部分。从diskmanager.log中收集的信息可用于帮助缩小后续步骤。

此外，您需要查看相关器性能统计信息：

```
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
```

请注意，这些统计信息用于FMC，并且它们对应于由其管理的所有传感器的集合。对于Unified低优先级事件，您主要寻找：

- 任何事件类型的每秒总流数，用于评估SFDataCorrelator进程的可能超订用。
- 上一输出中突出显示的两行： **rna flows/second** — 表示SFDataCorrelator处理的低优先级事件的速率。**rna dup flows/second** — 表示SFDataCorrelator处理的重复低优先级事件的速率。如前一个场景所述，这是通过双重日志记录生成的。

根据输出可以得出结论：

- 没有重复日志记录，如rna dup flows/second row所示。
- 在rna flows/second行中，“最大值”远高于“平均值”，因此SFDataCorrelator进程处理的事件速率出现峰值。如果您查看今天清晨的用户工作日刚开始的工作时间，这是可以预计的，但是总的来说，这是一个危险信号，需要进一步调查。

有关SFDataCorrelator进程的更多信息，请参阅事件处理部分。

推荐的操作

首先，您需要确定峰值发生的时间。为此，您需要查看每5分钟采样间隔的相关器统计信息。从diskmanager.log中收集的信息可帮助您直接了解重要的时间范围。

提示：减少输出到Linux页传呼机的管道，以便您轻松搜索。

```
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
```

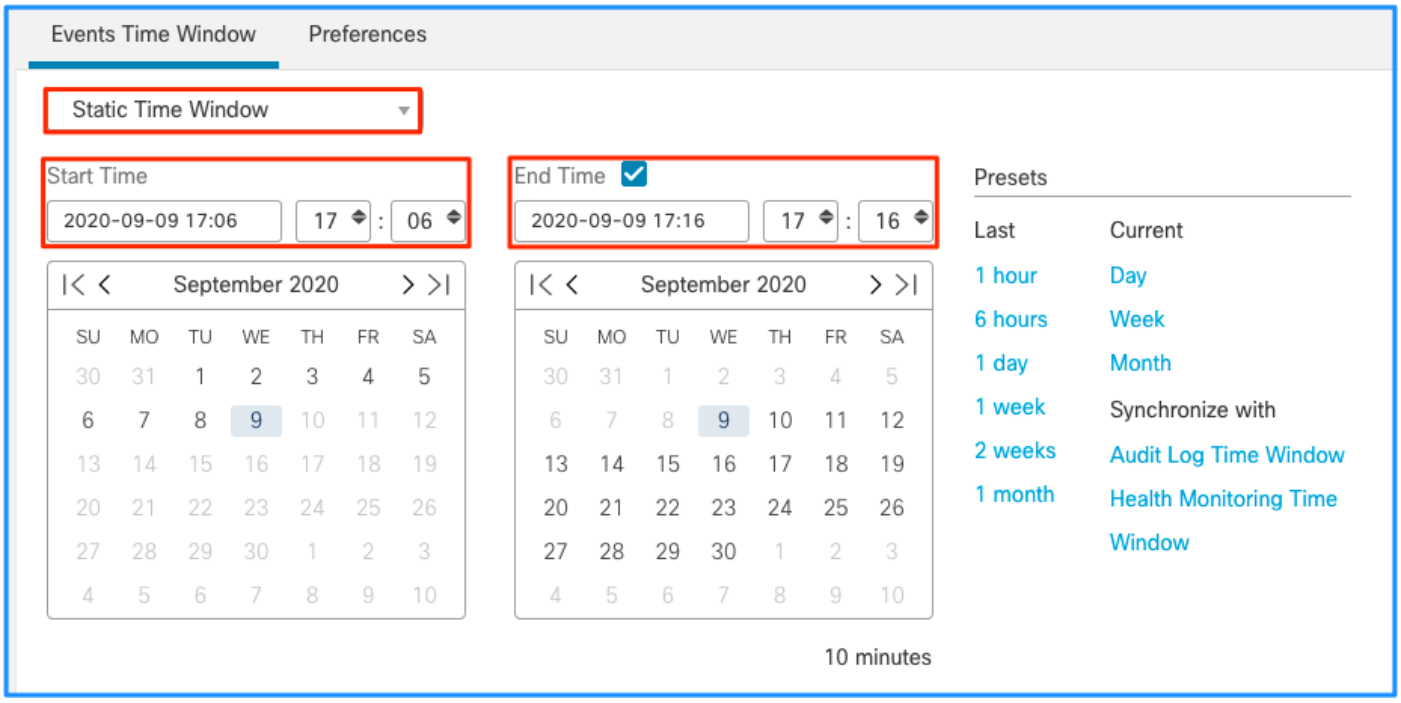
```
                fw stats/second:              0.01
                user logins/second:           0.00
                file events/second:           0.00
                malware events/second:        0.00
                fireAMP events/second:        0.00

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
```

使用输出中的信息可以：

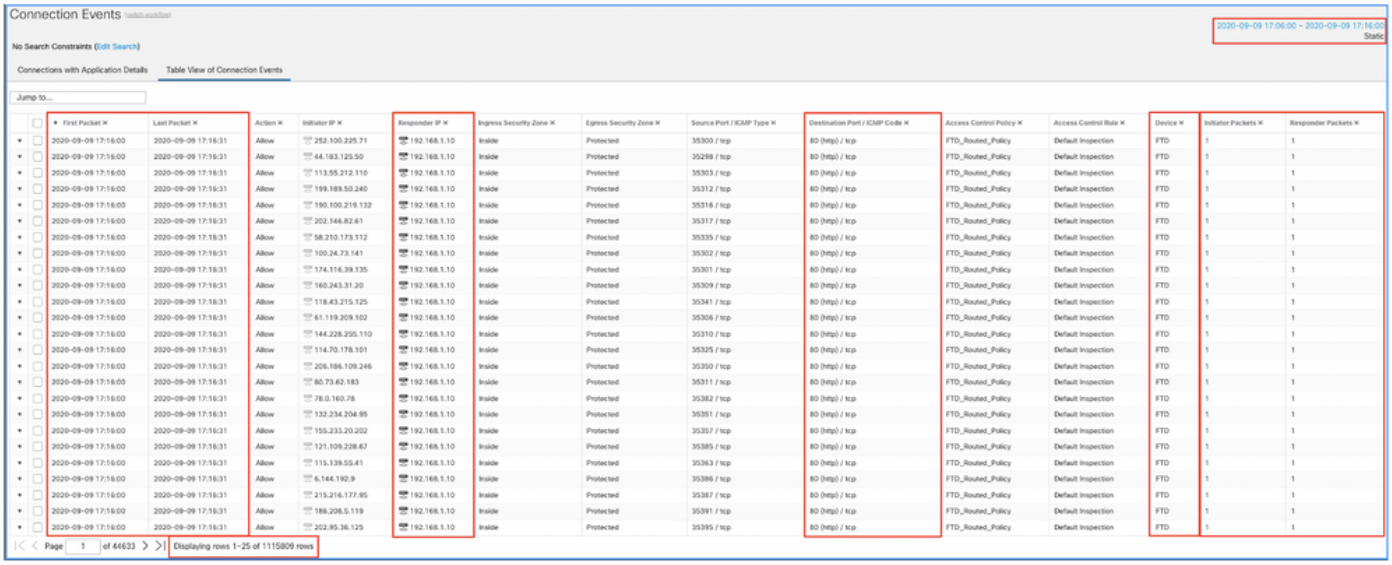
- 确定事件的正常/基线速率。
- 确定发生峰值的5分钟间隔。

在上一个示例中，在16:06:39及更长时间接收事件的速率出现明显峰值。请注意，这些是5分钟平均值，因此如果增量开始接近末尾，则此增量可能比所示的增量（突发）更突然，但在此5分钟间隔内稀释。

虽然由此可以得出这样的结论：此事件峰值导致未处理事件的耗尽，但您可以使用适当的时间窗口从FMC图形用户界面(GUI)查看连接事件，以了解此峰值中穿越FTD框的连接类型：



应用此时间段以获取过滤的连接事件，不要忘记考虑时区。在本示例中，传感器使用UTC和FMC UTC+1。使用表视图可查看触发事件过载的事件，并相应采取措施：



根据时间戳（第一个和最后一个数据包的时间），可以看出这些是短暂的连接。此外，Initiator和Responder Packets列显示每个方向只交换1个数据包。这证实了连接是短暂的，交换的数据很少。

您还可以看到所有这些流量针对相同的响应方IP和端口。此外，它们都由同一传感器报告（与入口和出口接口信息一起，可以指示此流量的位置和方向）。 其他操作：

- 检查目标终端上的系统日志。
- 实施DOS/DDOS保护或采取其他预防措施。

注意：本文的目的是提供用于排除“未处理事件排出”警报故障的准则。此示例使用hping3生成到目标服务器的TCP SYN泛洪。有关强化FTD设备的准则，请查看Cisco Firepower威胁防御强化指南

在联系思科技术支持中心(TAC)之前收集的项目

强烈建议您在联系Cisco TAC之前收集以下项目：

- 看到的运行状况警报的截图。
- 排除从FMC生成的文件故障。
- 对从受影响的传感器生成的文件进行故障排除。
- 首次发现问题的日期和时间。
- 有关最近对策略所做的任何更改的信息（如果适用）。
- stats_unified.pl命令的输出，如事件处理部分所述，其中提到了受影响的传感器。

深入了解

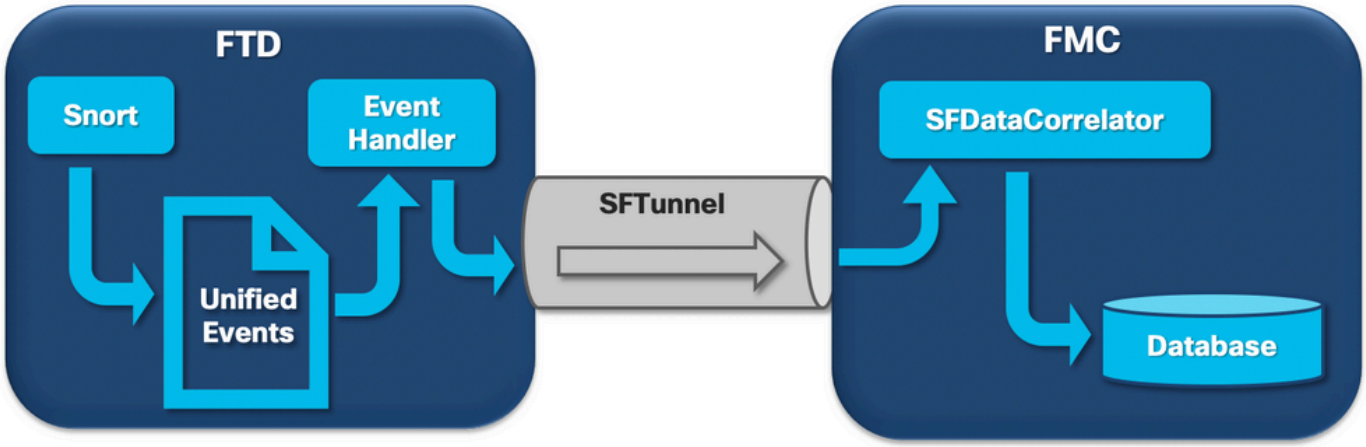
本节详细说明了可以参与此类运行状况警报的各种组件。包括：

- 事件处理 — 涵盖传感器设备和FMC上事件所采用的路径。当运行状况警报是指事件类型的思洛存储器时，这主要有用。
- 磁盘管理器 — 涵盖磁盘管理器流程、孤岛及其耗尽方式。
- 运行状况监视器 — 介绍如何使用运行状况监视器模块生成运行状况警报。
- Log to Ramdisk — 介绍ramdisk功能的日志记录及其对运行状况警报的潜在影响。

要了解“事件排出”运行状况警报并能够识别潜在的故障点，需要研究这些组件如何工作以及它们如何相互交互。

事件处理

尽管频繁漏电类型的运行状况警报可能由与事件无关的孤岛触发，但Cisco TAC看到的绝大多数案例都与漏电事件相关信息有关。此外，要了解什么会耗尽未处理的事件，需要了解事件处理体系结构及其组成部分。



当Firepower传感器收到来自新连接的数据包时，snort进程会以unified2格式生成事件，该格式是一种二进制格式，允许更快的读/写以及更轻的事件。

输出显示FTD命令**system support trace**，您可以在其中看到已创建的新连接。重点介绍并解释以下重要部分：

```
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文件在路径[/ngfw]**var/sf/detection_engine/*/instance-N/下按实例生成，**其中：

- ***是Snort UUID。每台设备都具有唯一性。
- **N**是Snort实例ID，可以按照上一个输出（示例中突出显示的0）+ 1的实例ID进行计算

任何给定的Snort实例文件夹中都可以有2种类型的unified_events文件：

- unified_events-1（包含高优先级事件）。
- unified_events-2（包含低优先级事件）。

高优先级事件是对应于潜在恶意连接的事件。

事件类型及其优先级：

高优先级(1)	**低优先级(2)**
入侵	连接
恶意软件	发现
安全情报	文件
关联的连接事件	统计信息

下一个输出显示属于上一个示例中跟踪的新连接的事件。该格式为unified2，取自位于[/ngfw]/var/sf/detection_engine/*/instance-**1/下方的各自统一事件日志的输**出，其中1是上一个输出+1中以粗体表示的snort实例id。统一事件日志的格式名称遵循unified_events-**2.**log.**159654750**语法，其中2表示表中显示的事件优先级，而最后一部分以粗体表示(**159654750)是unix时间戳(Unix)时间)。**

> **提示：**您可以使用Linux **date**命令将Unix时间转换为可读日期：
> admin@FP1120-2:~$ sudo**日期-d@1599654750**
> 2020年9月9日（星期三）：14:32:30

```
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
```

每个unified_events文件旁边都有一个书签文件，其中包含两个重要值：

1. 对应于该实例和优先级的当前unified_events文件的时间戳。
2. 在unified_event文件中最后一次读取事件的位置（以字节为单位）。

这些值按逗号分隔的顺序排列，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
```

这样，磁盘管理器进程就可以知道哪些事件已处理（发送到FMC），哪些事件未处理。

请注意，当磁盘管理器清空事件思洛存储器时，它会删除统一事件文件。有关释放孤岛的更多信息，请阅读磁盘管理器部分。

当以下情况之一为真时，已耗尽的统一文件被视为具有未处理的事件：

1. 书签时间戳低于文件创建时间。
2. 书签时间戳与文件创建时间相同，并且文件中的字节位置低于其大小。

EventHandler进程从统一文件中读取事件，并通过sftunnel（负责传感器与FMC之间加密通信的进程）将其流式传输到FMC（作为元数据）。这是基于TCP的连接，因此事件流由FMC确认

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

```
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
```

此输出提供以下信息：

- Snort打开了unified_events文件以供输出（在其中写入）。
- 事件处理程序打开了同一个unified_events文件（从中读取）。
- sftunnel报告从该unified_events文件处理的事件数。

然后相应地更新书签文件。Sftunnel为高优先级事件和低优先级事件分别使用2个不同的信道，称为统一事件(UE)信道0和1。

在FTD上使用**sfunnel_status** CLI命令，您可以看到流传输的事件数。

```
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进程接收。

使用**stats_unified.pl**命令可以查看从每个传感器处理的事件的状态：

```
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
```

此命令显示每个通道特定设备的事件积压的状态，使用的通道ID与sftunnel相同。

Bytes Behind值可以计算为统一事件书签文件中显示的位置与统一事件文件大小之间的差值，加上时间戳高于书签文件中的时间戳的任何后续文件。

SFDataCorrelator进程还存储性能统计信息，这些统计信息保存在**/var/sf/rna/correlator-stats/**中。每天创建一个文件，以CSV格式存储该天的性能统计信息。文件名称采用**"YYYY-MM-DD"**格式，当前日期对应的文件称为**now**。

统计信息每5分钟收集一次（每5分钟间隔有一行）。

可以使用**perfstats**命令读取此文件的输出。请注意，此is命令也用于读取snort性能统计信息文件，因此必须使用相应的标志：

-C:指示perfstats输入是相关器统计文件（如果没有此标志perfstats，则假设输入是snort性能统计文件）。

-q:安静模式，仅打印文件的摘要。

```
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
```

摘要中的每一行按此顺序有3个值：平均值，最小值，最大值。

如果打印时不带 — q标志，您还会看到5分钟间隔值。总结在末尾显示。

请注意，每个FMC在其数据表中都有描述的最大流量。下表包含各个数据表中每个模块的值：

型号	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	变量	12

请注意，这些值用于SFDataCorrelator统计信息输出中以粗体显示的所有事件类型的聚合。

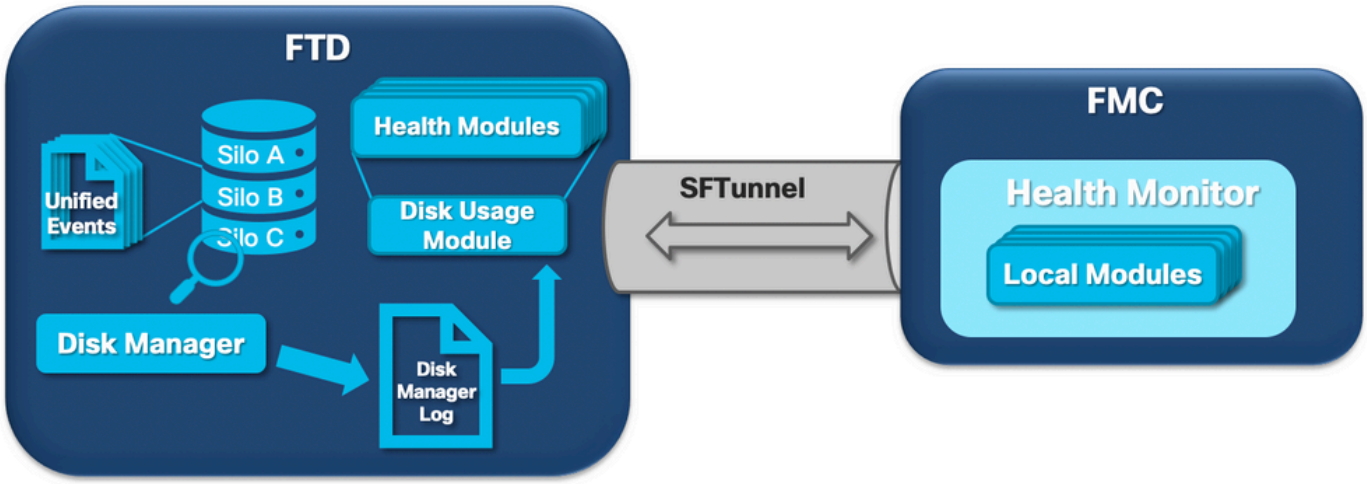
如果您查看输出，并且我们按照我们为最坏情况（所有最大值同时发生时）做好准备的方式来调整我们的FMC，则此FMC看到的事件速率是48.65 + 348.15 + 4.63 + 3.25 + 0.06 = **404.74 fps**。

此总值与相应模型数据表中的值进行比较。

SFDataCorrelator还可以对收到的事件（例如关联规则）进行其他工作，然后将其存储到数据库中，查询该数据库以填充FMC图形用户界面(GUI)中的各种信息，例如控制面板和事件视图。

磁盘管理器

下一个逻辑图显示了**运行状况监视器**和**磁盘管理器**进程的逻辑组件，因为它们相互交织以生成与磁盘相关的运行状况警报。



简而言之，磁盘管理器进程管理该盒的磁盘使用率，其配置文件位于[/ngfw]/etc/sf/文件夹中。在某些情况下可以使用磁盘管理器进程的多个配置文件：

- diskmanager.conf — 标准配置文件。
- diskmanager_2hd.conf — 当包装盒中安装了2个硬盘时使用。第二个硬盘驱动器与恶意软件扩展相关，用于存储文件策略中定义的文件。

- ramdisk-diskmanager.conf — 在启用记录到Ramdisk时使用。有关详细信息，请查看Log to Ramdisk部分。

磁盘管理器监控的每种文件类型都分配有一个思洛存储器。根据系统上可用的磁盘空间量，磁盘管理器会为每个思洛存储器计算高水位标记(HWM)和低水位标记(LWM)。

当磁盘管理器进程耗尽思洛存储器时，它会一直耗尽，直到到达LWM点。由于每个文件都排除了事件，因此可以超过此阈值。

要检查传感器设备上孤岛的状态，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
```

满足以下条件之一时，磁盘管理器进程将运行：

- 进程开始（或重新启动）
- 思洛存储器到达HWM
- 思洛存储器已手动排空
- 每小时一次

每次运行磁盘管理器进程时，它都会在其日志文件中为每个不同的孤岛生成一个条目，该日志文件位于[/ngfw]/var/log/diskmanager.log下，并且具有CSV格式的数据。

接下来，显示来自diskmanager.log文件的示例行，该示例行取自触发从Unified Low Priority Events运行状况警报中排出未处理事件的传感器，以及相应列的细分：

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

列	价值
思洛存储器标签	priority_2_events
排出时间（纪元时间）	1599668981
已耗尽的文件数	221
已耗尽的字节	4587929508
排出后数据的当前大小（字节）	1132501868
已耗尽的最大文件（字节）	20972020

已耗尽的最小文件（字节）	4596
最旧的文件已耗尽（纪元时间）	1586044534
高水印（字节）	5710966962
低水印（字节）	1142193392
未处理事件已耗尽的文件数	110
Diskmanager状态标志	0

然后，相应的运行状况监视器模块读取此信息，以触发相关的运行状况警报。

手动清空思洛存储器

在某些情况下，可能需要手动清空思洛存储器。例如，使用手动释放思洛存储器来清除磁盘空间而不是手动删除文件，有利于磁盘管理器决定保留和删除哪些文件。磁盘管理器保留该思洛存储器的最新文件。

任何思洛存储器都可以被耗尽，并且如前所述那样工作（磁盘管理器会耗尽数据，直到数据量低于LWM阈值）。 命令**system support silo-drain**在FTD CLISH模式下可用，它提供可用思洛存储器（名称+数字ID）的列表。

下面是手动清空统一低优先级事件孤岛的示例：

```
> 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
```

运行状况监视器

以下是要点：

- 在FMC上“运行状况监视器”(Health Monitor)菜单或“消息中心”(Message Center)的“运行状况”(Health)选项卡下看到的所有运行状况警报均由运行状况监视器进程生成。
- 此过程可监控系统的运行状况，包括FMC和受管传感器，并且由多个不同的模块组成。
- 运行状况警报模块在运行状况策略中定义，可以按设备连接这些模块。
- 运行状况警报由磁盘使用量模块生成，该模块可在FMC管理的每个传感器上运行。
- 当FMC上的运行状况监控进程运行时（每5分钟一次或触发手动运行时），磁盘使用模块会查看diskmanager.log文件，如果满足正确的条件，则会触发相应的运行状况警报。

要触发Drain of Unprocessed events运行状况警报，必须满足以下所有条件：

1. 已耗尽的字节数字段大于0（这表示此思洛存储器中的数据已耗尽）。
2. 排出未处理事件的文件数大于0（这表示排出数据中存在未处理事件）。
3. 下水的时间是在最近1小时内。

要触发**频繁排出事**件运行状况警报，以下条件必须为true:

1. diskmanager.log文件中的最后两个条目需要： Have Bytes drawed字段大于0（这表示此思洛存储器中的数据已用尽）。间距应小于5分钟。
2. 此思洛存储器最后一个条目的耗尽时间是在过去1小时内。

从磁盘使用模块收集的结果（以及其他模块收集的结果）通过sftunnel发送到FMC。您可以使用**sftunnel_status**命令查看通过sftunnel交换的运行状况事件的计数器：

```
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
```

记录到Ramdisk

即使大多数事件存储在磁盘中，设备也会默认配置为记录到ramdisk，以防止不断向磁盘写入和删除事件导致SSD逐渐损坏。

在此方案中，事件不存储在**[/ngfw]/var/sf/detection_engine/*/instance-N/** 下，但它们位于**[/ngfw]/var/sf/detection_engines/*/instance-N/connection/**中，后者是指向**/dev/shm/instance-N/connection的符号链接。**在这种情况下，事件驻留在虚拟内存中，而不是物理内存中。

```
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
```

要验证设备当前配置为执行的操作，请从FTD CLISH运行**show log-events-to-ramdisk**命令。如果使用**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**：当执行“configure log-events-to-ramdisk disable”命令时，需要在FTD上完成两个部署，以便snort不会陷入“D”状态（不间断睡眠），这将导致流量中断。
> 此行为在缺陷中记录为Cisco Bug ID CSCvz5372。在首次部署中，将跳过Snort内存阶段的重新评估，导致Snort进入“D”状态，解决方法是使用任何虚拟更改执行其他部署。

当您登录到磁盘时，主要缺点是各个思洛存储器分配了较小的空间，因此在相同的情况下会更频繁地耗尽它们。下一个输出是FPR 4140的磁盘管理器，其中启用了日志事件到ramdisk以供比较。

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“记录到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
```

思洛存储器尺寸越小，访问事件并将其流式传输到FMC的速度就越快。虽然在适当的条件下这是更好的选择，但是必须考虑它的缺点。

常见问题解答 (FAQ)

Drain of Events运行状况警报是否仅由Connection Events生成？

不能。

- 任何磁盘管理器孤岛都可以生成频繁耗尽警报。
- 任何与事件相关的思洛存储器都可以生成未处理事件排出的警报。

连接事件是最常见的罪魁祸首。

当出现Frequent Drain运行状况警报时，是否始终建议禁用Log to Ramdisk?

否。仅在除DOS/DDOS之外的过多日志记录情况下，当受影响的思洛存储器是连接事件思洛存储器时，且仅在无法进一步调整日志记录设置的情况下。

如果DOS/DDOS导致过多的日志记录，解决方案是实施DOS/DDOS保护或消除DOS/DDOS攻击的来源。

默认功能“Log to Ramdisk”可减少SSD磨损，因此强烈建议使用它。

什么是未处理的事件？

事件不会单独标记为未处理。在以下情况下，文件具有未处理的事件：

其创建时间戳高于相应书签文件中的时间戳字段。

或

其创建时间戳等于相应书签文件中的时间戳字段，并且其大小高于相应书签文件上的字节字段中的位置。

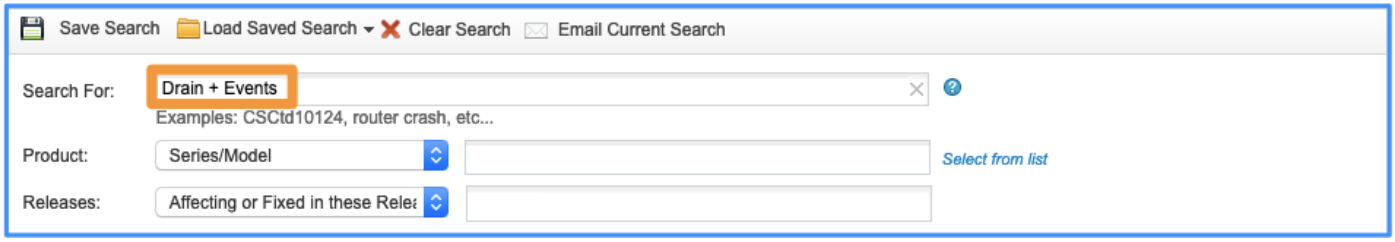
FMC如何知道特定传感器的字节数？

传感器发送有关unified_events文件名和大小的元数据，以及书签文件上的信息，为FMC提供计算后面的字节所需的足够信息，如下所示：

当前unified_events文件大小 — 来自书签文件的**Position in Bytes**"字段+所有unified_events文件的大小，其时间戳高于相应书签文件中的时间戳。

已知问题

打开Bug Search Tool并使用此查询：



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。