Solucionar problemas de drenagem de eventos não processados do FMC e drenagem frequente de alertas do monitor de integridade de eventos

Contents

Introduction

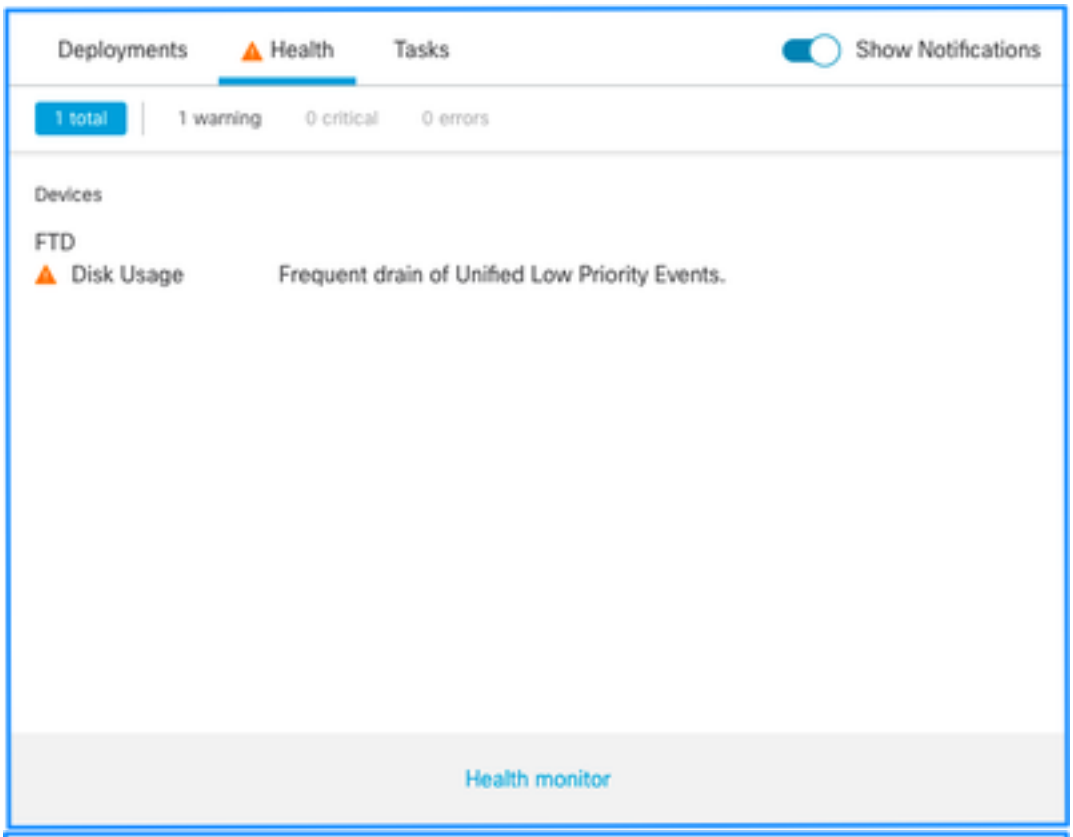
Este documento descreve como solucionar problemas de **drenagem de eventos não processados** e **drenagem frequente de eventos** em alertas de integridade do Firepower Management Center (FMC).

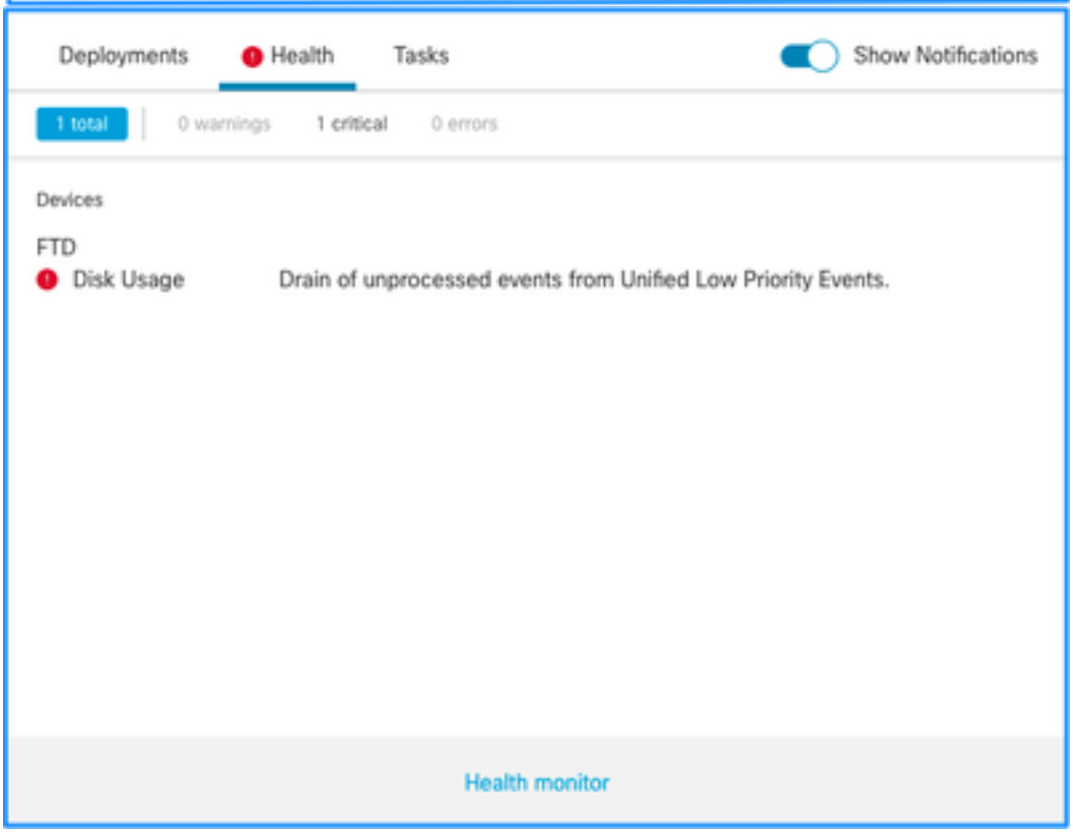
Visão geral do problema

O FMC gera um destes alertas de saúde:

- Esgotamento frequente de eventos de baixa prioridade unificados
  e/ou
- Drenagem de eventos não processados de eventos de baixa prioridade unificados

Embora esses eventos sejam gerados e exibidos no FMC, eles se relacionam a um sensor de dispositivo gerenciado, seja um dispositivo Firepower Threat Defense (FTD) ou um dispositivo NGIPS (Next-Generation Intrusion Prevention System). Para o restante deste documento, o termo sensor refere-se a dispositivos FTD e NGIPS, a menos que especificado de outra forma.





Esta é a estrutura de alerta de integridade:

- Esgotamento frequente de <NOME DO SILO>
- Esgotamento de eventos não processados de <NOME DO SILO>

Neste exemplo, SILO NAME é **Unified Low Priority Events**. Este é um dos silos do gerenciador de disco (consulte a seção Informações de fundo para obter uma explicação mais abrangente).

Além disso:

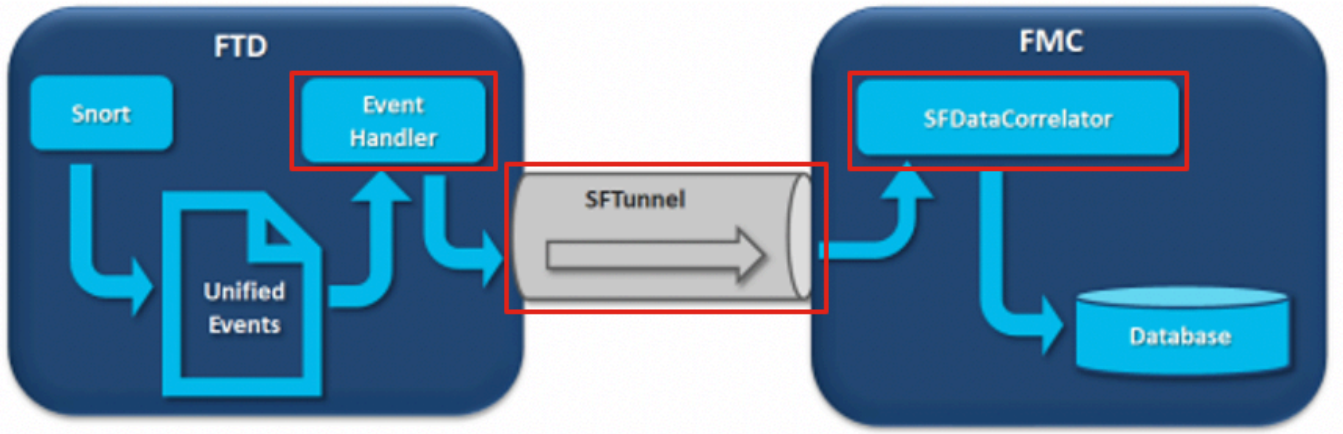
- Embora qualquer silo possa gerar tecnicamente um alerta de saúde de dreno frequente de <NOME DO SILO>, os mais comumente vistos são os relacionados aos eventos e, entre eles, os eventos de baixa prioridade simplesmente porque esses são os tipos de eventos mais frequentemente gerados pelos sensores.
- Um evento de "drenagem frequente de <NOME DO SILO>" tem uma severidade de Aviso no caso de um silo relacionado a eventos, pois, se ele for processado (a explicação sobre o que constitui um evento não processado é fornecida em seguida), ele estará no banco de dados do FMC.
- Para um silo não relacionado a eventos, como o silo "Backups", o Alerta é Crítico, pois essas informações são perdidas.
- Somente silos de tipo de evento geram um Esgotamento de eventos não processados do alerta de integridade da . Este alerta sempre tem severidade Crítica.

Os sintomas adicionais podem incluir:

- Lentidão na interface do usuário do FMC
- Perda de eventos

Cenários comuns de solução de problemas

Um dreno frequente do evento <NOME DO SILO> é causado por muita entrada no silo para seu tamanho. Nesse caso, o gerenciador de disco drena (limpa) esse arquivo pelo menos duas vezes no último intervalo de 5 minutos. Em um silo de tipo de evento, isso é normalmente causado pelo registro excessivo desse tipo de evento. No caso de um Esgotamento de eventos não processados do alerta de integridade da , isso também pode ser causado por um gargalo no caminho de processamento de eventos.



No diagrama há 3 gargalos potenciais:

- O processo EventHandler no FTD está com excesso de assinaturas (a leitura é mais lenta do que o que o Snort escreve)
- A interface Eventing tem excesso de assinaturas
- O processo SFDataCorrelator no FMC está com excesso de assinaturas

Para compreender melhor a arquitetura do processamento de eventos, consulte a respectiva seção Mergulho profundo.

Caso 1. Registro Excessivo

Como mencionado na seção anterior, uma das causas mais comuns dos alertas de integridade desse tipo é a entrada excessiva.

A diferença entre a Marca d'água inferior (LWM) e a Marca d'água superior (HWM) coletadas a partir do comando **show disk-manager** CLISH mostra quanto espaço é necessário para ocupar esse silo e passar do LWM (recentemente drenado) para o valor HWM. Se houver um esgotamento frequente de eventos (com ou sem eventos não processados), a primeira coisa que você deve revisar é a configuração de registro.

Para obter uma explicação detalhada do processo do Gerenciador de Discos, consulte a respectiva seção Mergulho profundo.

Seja um registro duplo ou apenas uma alta taxa de eventos no ecossistema geral do gerenciador-sensores, uma revisão das configurações de registro deve ser feita.

Ações recomendadas

Etapa 1. Verificar se há registro duplo

Cenários de registro duplo podem ser identificados se você olhar o correlator **perfstats** no FMC como mostrado nesta saída:

```
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
```

Neste caso, uma taxa elevada de fluxos duplicados pode ser vista na saída.

Etapa 2. Revisar as definições de log do ACP

Você deve começar com uma revisão das configurações de log da Política de Controle de Acesso (ACP). Certifique-se de seguir as melhores práticas descritas neste documento Melhores Práticas para Registro de Conexão

Érecomendável revisar as configurações de registro em todas as situações, já que as recomendações listadas não cobrem apenas cenários de registro duplo.

Etapa 3. Verificar se o log excessivo é esperado ou não

Você deve verificar se o log excessivo tem uma causa esperada ou não. Se o registro excessivo for causado por um ataque de DOS/DDoS ou loop de roteamento ou por um aplicativo/host específico que faz um grande número de conexões, você deverá verificar e mitigar/interromper as conexões das fontes de conexão excessivas inesperadas.

Etapa 4. Atualizar o modelo

Atualize o dispositivo de hardware FTD para um modelo de desempenho mais alto (por exemplo, FPR2100 —> FPR4100), a origem do silo aumentaria.

Etapa 5. Considere se você pode desativar o registro no Ramdisk

No caso do silo de eventos de baixa prioridade unificados, você pode desabilitar Log to Ramdisk para aumentar o tamanho do silo com as desvantagens discutidas na respectiva seção Mergulho profundo.

Caso 2. Gargalo no canal de comunicação entre o sensor e o CVP

Outra causa comum para esse tipo de alerta são problemas de conectividade e/ou instabilidade no canal de comunicação (sftunnel) entre o sensor e o FMC. O problema de comunicação pode ocorrer devido a:

- o sftunnel está inoperante ou é instável (flaps).
- sftunnel está com excesso de assinaturas.

Para o problema de conectividade de sftunnel, certifique-se de que o FMC e o sensor tenham acessibilidade entre suas interfaces de gerenciamento na porta TCP 8305.

No FTD, você pode procurar a string **sftunneld** no **arquivo [/ngfw]/var/log/messages**. Problemas de conectividade fazem com que mensagens como estas sejam geradas:

```
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
```

O excesso de assinaturas da interface de gestão dos CVP pode ser um pico no tráfego de gestão ou um excesso constante de assinaturas. Os dados históricos do Monitor de integridade são um bom indicador disso.

A primeira coisa a observar é que, na maioria dos casos, o FMC é implantado com uma única placa de rede para gerenciamento. Essa interface é usada para:

- Gestão dos CVP.
- Gerenciamento de sensores FMC.
- Coleta de eventos do FMC dos sensores.
- Atualização de Feeds de Inteligência.
- O download de atualizações de SRU, Software, VDB e GeoDB do site de download de software.
- A consulta para Reputações e Categorias de URL (se aplicável).
- A consulta para Disposições do arquivo (se aplicável).

Ações recomendadas

Você pode implantar uma segunda NIC no FMC para uma interface dedicada a eventos. As implementações podem depender do caso de uso.

As diretrizes gerais podem ser encontradas no guia de hardware do FMC Deploying on a Management Network

Caso 3. Um Gargalo no Processo SFDataCorrelator

O último cenário a ser abordado é quando ocorre o gargalo no lado do SFDataCorrelator (FMC).

A primeira etapa é examinar o arquivo diskmanager.log à medida que há informações importantes a serem reunidas, como:

- A frequência do dreno.
- O número de arquivos com eventos não processados drenados.
- A ocorrência do esvaziamento com Eventos Não Processados.

Para obter informações sobre o arquivo diskmanager.log e como interpretá-lo, consulte a seção Gerenciador de Discos. As informações coletadas do diskmanager.log podem ser usadas para ajudar a restringir as etapas subsequentes.

Além disso, é necessário examinar as estatísticas de desempenho do correlator:

```
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
```

Observe que essas estatísticas são para o FMC e correspondem ao conjunto de todos os sensores gerenciados por ele. No caso de eventos de baixa prioridade do Unified, você procura principalmente:

- Total de fluxos por segundo de qualquer tipo de evento para avaliar uma possível sobreassinatura do processo SFDataCorrelator.
- As duas linhas destacadas na saída anterior: **rna flows/second** - Indica a taxa de eventos de baixa prioridade processados pelo SFDataCorrelator.**rna dup flows/second** - Indica a taxa de eventos de baixa prioridade duplicados processados pelo SFDataCorrelator. Isso é gerado pelo registro duplo, conforme discutido no cenário anterior.

Com base na produção, pode concluir-se que:

- Não há registro duplicado conforme indicado pela linha rna dup flows/second.
- Na linha fluxos de rna/segundo, o valor Máximo é muito maior que o valor Médio, portanto houve um pico na taxa de eventos processados pelo processo SFDataCorrelator. Isso pode ser esperado se você olhar para esta manhã cedo, quando o dia de trabalho dos usuários acabou de começar, mas, em geral, é um sinalizador vermelho e requer mais investigação.

Mais informações sobre o processo SFDataCorrelator podem ser encontradas na seção Processamento de Eventos.

Ações recomendadas

Primeiro, você precisa determinar quando o pico ocorreu. Para fazer isso, é necessário examinar as estatísticas do correlator para cada intervalo de amostra de 5 minutos. As informações reunidas a partir do diskmanager.log podem ajudá-lo a ir diretamente para o período de tempo importante.

> **Tip**: Faça o pipe de saída para o pager do Linux **menos** para que você possa facilmente pesquisar.

```
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
```

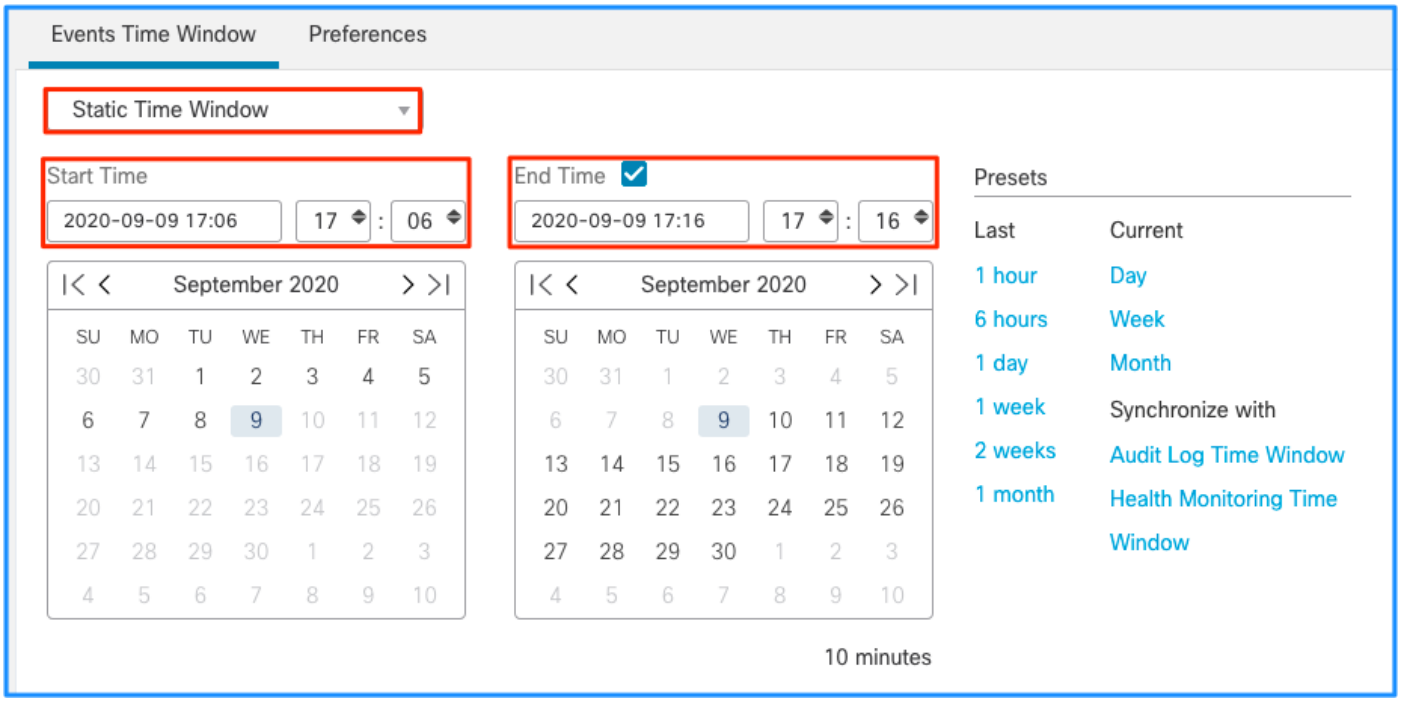
```
                ids comm records/second:       0.01
                ids extras/second:             0.00
                fw stats/second:               0.03
                user logins/second:            0.00
                file events/second:            0.00
                malware events/second:         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
```

Use as informações na saída para:

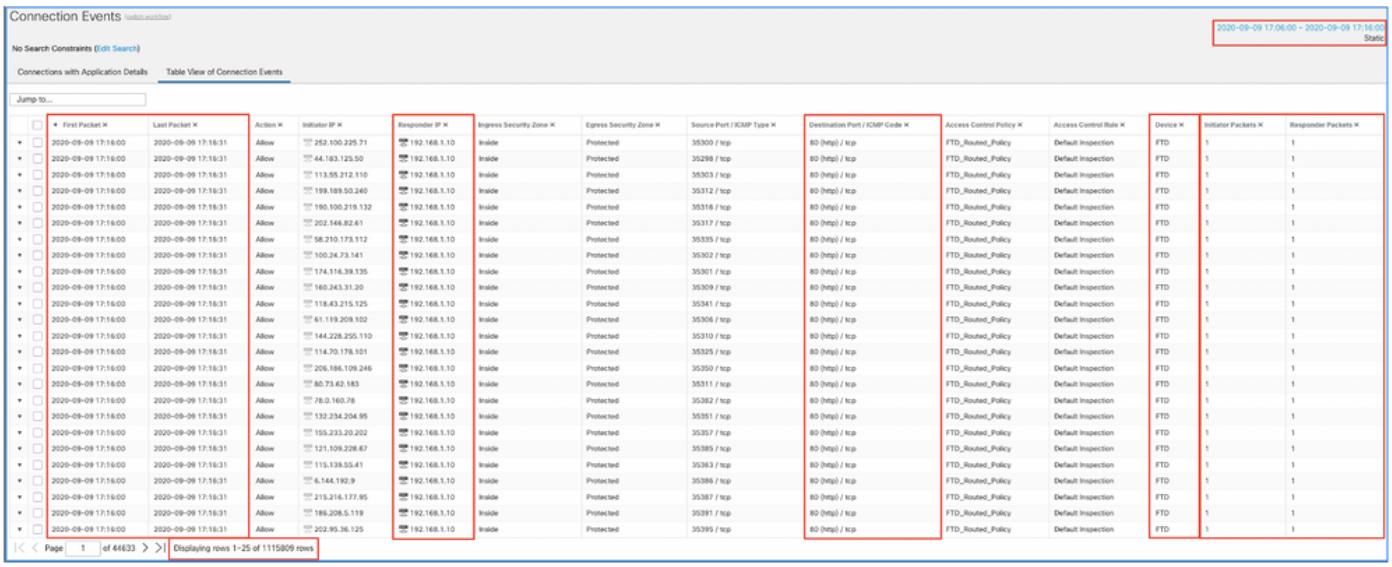
- Determine a taxa normal/linha de base dos eventos.
- Determine o intervalo de 5 minutos quando o pico ocorreu.

No exemplo anterior, há um pico óbvio na taxa de eventos recebidos às 16:06:39 e além. Observe que essas são médias de 5 minutos para que o aumento possa ser mais abrupto do que o mostrado (intermitência), mas diluído nesse intervalo de 5 minutos se ele tiver começado no final.

Embora isso leve à conclusão de que esse pico de eventos causou o esgotamento de eventos não processados, você pode dar uma olhada nos eventos de conexão da interface gráfica do usuário (GUI) do FMC com a janela de tempo apropriada para entender que tipo de conexões atravessaram a caixa FTD nesse pico:



Aplique esta janela de tempo para obter os eventos de conexão filtrados, não se esqueça de considerar o fuso horário. Neste exemplo, o sensor usa o UTC e o FMC UTC+1. Use a Exibição de Tabela para ver os eventos que dispararam a sobrecarga de eventos e tomar as medidas necessárias:



Com base nos carimbos de data/hora (hora do primeiro e do último pacote), pode-se ver que essas são conexões de curta duração. Além disso, as colunas de Pacotes do Iniciador e do Respondente mostram que havia apenas 1 pacote trocado em cada direção. Isso confirma que as conexões tiveram vida curta e trocaram muito poucos dados.

Você também pode ver que todos esses fluxos têm como destino os mesmos IPs e a mesma porta do respondente. Além disso, todos são relatados pelo mesmo sensor (que, juntamente com as informações de interface de entrada e saída, pode falar com o local e a direção desse fluxo). Ações adicionais:

- Verifique os Syslogs no ponto final de destino.
- Implemente a proteção DOS/DDOS ou tome outras medidas preventivas.

Note: O objetivo deste artigo é fornecer diretrizes para solucionar problemas do alerta Dreno

de Eventos Não Processados. Este exemplo usou o hping3 para gerar uma inundação TCP SYN para o servidor de destino. Para obter diretrizes para fortalecer seu dispositivo FTD, consulte o Guia de Fortalecimento do Cisco Firepower Threat Defense

Itens a serem coletados antes de entrar em contato com o Cisco Technical Assistance Center (TAC)

Éaltamente recomendável coletar esses itens antes de entrar em contato com o TAC da Cisco:

- Captura de tela dos alertas de integridade vistos.
- Arquivo de solução de problemas gerado do FMC.
- Solução de problemas de arquivo gerado a partir do sensor afetado.
- Data e Hora em que o problema foi visto pela primeira vez.
- Informações sobre alterações recentes feitas nas políticas (se aplicável).
- A saída do comando stats_unified.pl como descrito na seção Processamento de eventos com uma menção dos sensores afetados.

Análise detalhada

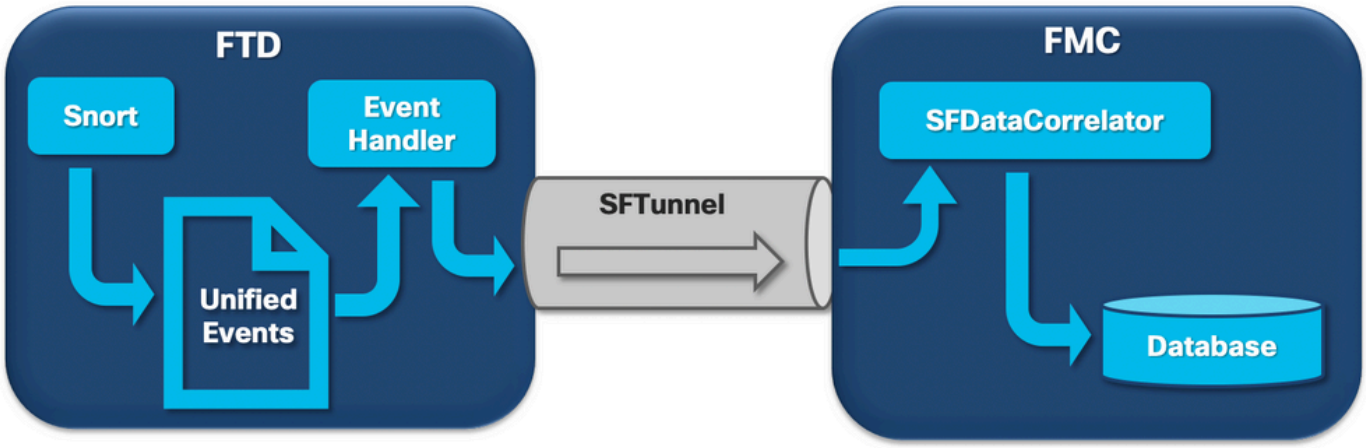
Esta seção aborda uma explicação detalhada dos vários componentes que podem participar deste tipo de alertas de integridade. Isso inclui:

- Processamento de eventos - Abrange o caminho que os eventos tomam nos dispositivos do sensor e no FMC. Isso é útil principalmente quando o alerta de integridade se refere a um Silo do tipo evento.
- Gerenciador de discos - Abrange o processo do gerenciador de discos, os silos e como eles são drenados.
- Monitor de integridade - Abrange como os módulos do Monitor de integridade são usados para gerar alertas de integridade.
- Log no Ramdisk - Abrange o recurso de log no ramdisk e seu impacto potencial nos alertas de integridade.

Para entender os alertas de integridade de Drenagem de Eventos e ser capaz de identificar pontos de falha potenciais, é necessário examinar como esses componentes funcionam e interagem entre si.

Processamento de eventos

Mesmo que o tipo de alerta de saúde Drenagem Frequente possa ser disparado por silos que não estão relacionados a eventos, a grande maioria dos casos vistos pelo Cisco TAC está relacionada à drenagem de informações relacionadas a eventos. Além disso, para entender o que constitui um dreno de eventos não processados, é necessário examinar a arquitetura de processamento de eventos e os componentes que a constituem.



Quando um sensor Firepower recebe um pacote de uma nova conexão, o processo de snort gera um evento no formato unified2, que é um formato binário que permite leituras/gravações mais rápidas, bem como eventos mais leves.

A saída mostra o **rastreamento de suporte do sistema de** comandos FTD onde você pode ver uma nova conexão criada. As partes importantes são destacadas e explicadas:

```
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
```

Os arquivos de eventos unificados do Snort são gerados por instância no caminho **[/ngfw]var/sf/detection_engine/*/instance-N/**, onde:

- ***** é o UUID do Snort. Isso é exclusivo por dispositivo.
- **N** é o ID da instância do Snort que pode ser calculado como o ID da instância da saída anterior (o 0 realçado no exemplo) + 1

Pode haver 2 tipos de arquivos unified_events em qualquer pasta de instância do Snort:

- unified_events-1 (que contém eventos de alta prioridade).
- unified_events-2 (que contém eventos de baixa prioridade).

Um evento de alta prioridade corresponde a uma conexão potencialmente mal-intencionada.

Tipos de eventos e suas prioridades:

Alta prioridade (1)	Baixa prioridade (2)
Intrusão	Conexão
Malware	Descoberta
Inteligência de segurança	Arquivo
Eventos de Conexão Associada	Estatísticas

A próxima saída mostra um evento que pertence à nova conexão rastreada no exemplo anterior. O formato é unified2 e é tirado da saída do respectivo log de eventos unificado localizado em [/ngfw]/var/sf/detection_engine/*/instance-**1**/ onde 1 é o id da instância do snort em negrito na saída anterior +1. O nome do formato do log de eventos unificado segue a sintaxe unified_events-**2**.log.**1599654750** onde 2 representa a prioridade dos eventos como mostrado na tabela e a última parte em negrito (**159 9654750**) é o carimbo de data/hora (hora Unix) de quando o arquivo foi criado.

> **Tip**: Você pode usar o comando Linux **date** para converter a hora Unix em uma data legível:
> admin@FP1120-2:~$ **sudo date -d@1599654750**
> Qua Set 9 14:32:30 CEST 2020

```
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
```

Junto com cada arquivo unified_events há um arquivo de marcadores, que contém 2 valores importantes:

1. Carimbo de data/hora correspondente ao arquivo unified_events atual para essa instância e prioridade.
2. Posição em Bytes para o último evento de leitura no arquivo unified_event.

Os valores estão em ordem, separados por vírgula, como mostrado neste exemplo:

```
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
```

Isso permite que o processo do gerenciador de disco saiba quais eventos já foram processados (enviados ao FMC) e quais não foram.

Observe que quando o gerenciador de disco drena um silo de eventos, ele remove arquivos de eventos unificados. Para obter mais informações sobre a drenagem de silos, leia a [seção]

Gerenciador de disco.

Um arquivo unificado drenado é considerado como tendo eventos não processados quando um destes é verdadeiro:

1. O carimbo de data/hora do indicador é inferior à hora de criação do arquivo.
2. O carimbo de data/hora do indicador é o mesmo da hora de criação do arquivo e a posição em Bytes no arquivo é menor que seu tamanho.

O processo EventHandler lê os eventos dos arquivos unificados e transmite-os para o FMC (como metadados) através do sftunnel, que é o processo responsável pela comunicação criptografada entre o sensor e o FMC. Esta é uma conexão baseada em TCP, de modo que a transmissão do evento é confirmada pelo FMC

Você pode ver estas mensagens no arquivo [/ngfw]/var/log/messages:

```
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
```

Esta saída fornece estas informações:

- O Snort abriu o arquivo unified_events para saída (para gravar nele).
- O Manipulador de eventos abriu o mesmo arquivo unified_events (para ler a partir dele).
- sftunnel relatou o número de eventos processados desse arquivo unified_events.

O arquivo de favoritos é atualizado de acordo. O sftunnel usa 2 canais diferentes chamados Unified Events (UE) Canal 0 e 1 para eventos de alta e baixa prioridade, respectivamente.

Com o comando CLI **sfunnel_status** no FTD, você pode ver o número de eventos que foram transmitidos.

```
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
```

No CVP, os eventos são recebidos pelo processo SFDataCorrelator.

O status dos eventos que foram processados de cada sensor pode ser visto com o comando **stats_unified.pl**:

```
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
```

Esse comando mostra o status da lista de pendências de eventos para um determinado dispositivo por canal, o ID do canal usado é o mesmo que o sftunnel.

O valor de Bytes Atrás pode ser calculado como a diferença entre a posição mostrada no arquivo de marcador de evento unificado e o tamanho do arquivo de evento unificado, mais qualquer arquivo subsequente com um carimbo de data/hora maior do que aquele no arquivo de marcador.

O processo SFDataCorrelator também armazena estatísticas de desempenho, que são salvas em **/var/sf/rna/correlator-stats/**. Um arquivo é criado por dia para armazenar as estatísticas de desempenho desse dia no formato CSV. O nome do arquivo usa o formato "**AAAA-MM-DD**" e o correspondente do arquivo para o dia atual é chamado **agora**.

As estatísticas são coletadas a cada 5 minutos (há uma linha para cada intervalo de 5 minutos).

A saída desse arquivo pode ser lida com o comando **perfstats**. Observe que esse comando também é usado para ler arquivos de estatísticas de desempenho do snort, portanto, os sinalizadores apropriados devem ser usados:

-c: Instrui perfstats de que a entrada é um arquivo correlator-stats (sem esta flag perfstats assume que a entrada é um arquivo de estatísticas de desempenho de snort).

q: Modo silencioso, imprime somente o resumo do arquivo.

```
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
```

Cada linha no resumo tem 3 valores nesta ordem: Média, Mínimo, Máximo.

Se você imprimir sem o sinalizador -q, também verá os valores do intervalo de 5 minutos. O resumo é mostrado no final.

Note-se que cada CVP tem um caudal máximo descrito na sua ficha técnica. A tabela a seguir contém os valores por módulo obtidos da respectiva folha de dados:

Modelo	FMC 750	CVP 1000	FMC 1600	CVP 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMC
Caudal máximo (qps)	2000	5000	5000	12000	12000	12000	20000	20000	20000	Variável	12

Observe que esses valores são para o agregado de todos os tipos de eventos mostrados em negrito na saída de estatísticas SFDataCorrelator.

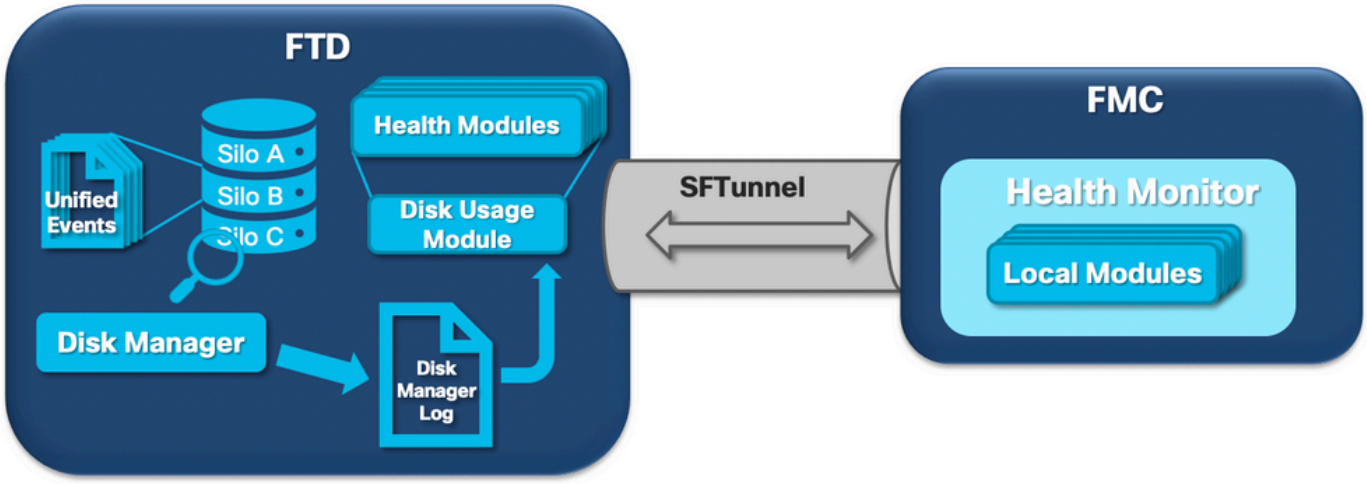
Se você olhar para a saída e dimensionarmos nosso FMC de forma que estejamos preparados para o pior cenário (quando todos os valores máximos acontecem ao mesmo tempo), a taxa de eventos que este FMC vê é 48,65 + 348,15 + 4,63 + 3,25 + 0,06 = **404,74 fps**.

Este valor total pode ser comparado com o valor da folha de dados do respectivo modelo.

O SFDataCorrelator também pode fazer um trabalho adicional sobre os eventos recebidos (como para Regras de Correlação), em seguida, armazena-os no banco de dados que é consultado para preencher várias informações na Interface Gráfica do Usuário (GUI) do FMC, como Painéis e Visualizações de Eventos.

Gerenciador de disco

O próximo diagrama lógico mostra os componentes lógicos dos processos **Health Monitor** e **Disk Manager** à medida que são interligados para a geração de alertas de integridade relacionados ao disco.



Em poucas palavras, o processo gerenciador de disco gerencia o uso do disco da caixa e tem seus arquivos de configuração na pasta [/ngfw]/etc/sf/. Há vários arquivos de configuração para o processo do gerenciador de discos que são usados em determinadas circunstâncias:

- diskmanager.conf - Arquivo de configuração padrão.
- diskmanager_2hd.conf - Usado quando a caixa tem 2 discos rígidos instalados. O segundo disco rígido é aquele relacionado à expansão de malware, usado para armazenar arquivos conforme definido na política de arquivos.
- ramdisk-diskmanager.conf - Usado quando o Log no Ramdisk está ativado. Para obter mais

informações, verifique a seção Log to Ramdisk.

Cada tipo de arquivo monitorado pelo gerenciador de disco é atribuído a um Silo. Com base na quantidade de espaço em disco disponível no sistema, o gerenciador de disco calcula uma Marca d'água superior (HWM) e uma Marca d'água inferior (LWM) para cada silo.

Quando o processo do gerenciador de disco drena um silo, ele o faz até o ponto em que o LWM é alcançado. Como os eventos são drenados por arquivo, esse limite pode ser ultrapassado.

Para verificar o status dos silos em um dispositivo sensor, você pode usar este comando:

```
> 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
```

O processo do gerenciador de discos é executado quando uma destas condições é atendida:

- O processo é iniciado (ou reiniciado)
- Um silo alcança o HWM
- Um silo é drenado manualmente
- Uma vez a cada hora

Cada vez que o processo do gerenciador de disco é executado, ele gera uma entrada para cada um dos diferentes silos em seu próprio arquivo de log, localizado em [/ngfw]/var/log/diskmanager.log e que tem dados em formato CSV.

Em seguida, é mostrado um exemplo de linha do arquivo diskmanager.log, obtido de um sensor que acionou o Esgotamento de eventos não processados do alerta de integridade de Eventos de baixa prioridade unificados, bem como a divisão das respectivas colunas:

```
priority_2_events,1599668981,221,4587929508,1132501868,20972020,4596,1586044534,5710966962,11421
93392,110,0
```

Coluna	Valor
Rótulo do Silo	priority_2_events
Tempo de drenagem (Época)	1599668981
Número de arquivos drenados	221
Bytes drenados	4587929508

Tamanho atual dos dados após a drenagem (bytes)	1132501868
Maior arquivo esvaziado (bytes)	20972020
Menor arquivo drenado (Bytes)	4596
Arquivo mais antigo drenado (tempo Época)	1586044534
Marca d'água alta (bytes)	5710966962
Marca d'água baixa (bytes)	1142193392
Número de arquivos com eventos não processados drenados	110
Sinalizador de estado do Diskmanager	0

Essas informações são lidas pelo respectivo módulo do Health Monitor para disparar o alerta de integridade relacionado.

Drenar manualmente um silo

Em determinados cenários, talvez você queira drenar manualmente um silo. Por exemplo, para liberar espaço em disco com drenagem manual de silos em vez de remoção manual de arquivos, o gerente de disco tem a vantagem de decidir quais arquivos manter e quais excluir. O gerenciador de disco mantém os arquivos mais recentes desse silo.

Qualquer silo pode ser drenado e isso funciona como já descrito (o gerenciador de disco drena dados até que a quantidade de dados vá abaixo do limite de LWM). O comando **system support silo-drain** está disponível no modo FTD CLISH e fornece uma lista dos silos disponíveis (nome + id numérico).

Este é um exemplo de drenagem manual do silo de Eventos de Baixa Prioridade Unificados:

```
> 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
```

Monitor de integridade

Estes são os pontos principais:

- Qualquer alerta de integridade visto no FMC no menu Health Monitor ou na guia Health no Message Center é gerado pelo processo Health Monitor.
- Esse processo monitora a integridade do sistema, tanto para o FMC quanto para os sensores gerenciados, e é composto por vários módulos diferentes.
- Os módulos de alerta de integridade são definidos na Política de Integridade que pode ser anexada por dispositivo.
- Os alertas de integridade são gerados pelo módulo de utilização de disco que pode ser executado em cada um dos sensores gerenciados pelo FMC.
- Quando o processo Health Monitor no FMC é executado (uma vez a cada 5 minutos ou quando uma execução manual é acionada), o módulo Disk Usage examina o arquivo diskmanager.log e, se as condições corretas forem atendidas, o alerta de integridade respectivo é acionado.

Para que um alerta de integridade **Drenagem de eventos não processados** seja acionado Todas

estas condições devem ser verdadeiras:

1. O campo Bytes drenados é maior que 0 (isso indica que os dados desse silo foram drenados).
2. O número de arquivos com eventos não processados drenados maior que 0 (isso indica que havia eventos não processados nos dados drenados).
3. O tempo de drenagem está dentro da última hora.

Para que um alerta de integridade **Drenagem Frequente de Eventos** seja disparado, estas condições devem ser verdadeiras:

1. As duas últimas entradas no arquivo diskmanager.log precisam: O campo Bytes drenados deve ser maior que 0 (isso indica que os dados desse silo foram drenados).Esteja a menos de 5 minutos de distância.
2. O tempo de drenagem da última entrada para este silo está dentro da última 1 hora.

O coletor de resultados do módulo de uso do disco (bem como os resultados coletados pelos outros módulos) são enviados ao FMC através do sftunnel. Você pode ver contadores para os Eventos de Integridade trocados em sftunnel com o comando **sftunnel_status**:

```
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
```

Registrar no Ramdisk

Embora a maioria dos eventos seja armazenada em disco, o dispositivo é configurado por padrão para registrar no ramdisk para evitar danos graduais ao SSD que podem ser causados por gravações e exclusões constantes de eventos no disco.

Neste cenário, os eventos não são armazenados em **[/ngfw]/var/sf/detection_engine/*/instance-N/,** mas estão localizados em **[/ngfw]/var/sf/detection_engines**/*/**instance-N/connection/**, que é um link simbólico para **/dev/shm/instance-N/connection.** Nesse caso, os eventos residem na memória virtual em vez de na física.

```
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
```

Para verificar qual dispositivo está configurado atualmente para executar o comando **show log-events-to-ramdisk** a partir do CLISH FTD. Você também pode alterar isso se usar o comando **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)
```

> **aviso:** Quando o comando "configure log-events-to-ramdisk disable" é executado, há uma necessidade de duas implantações serem feitas no FTD para que o snort não fique preso no estado "D" (Suspensão Ininterrupta), o que causaria uma interrupção de tráfego.
> Esse comportamento é documentado no defeito com a ID de bug Cisco CSCvz5372. Com a primeira implantação, a reavaliação do estágio de memória snort é ignorada, o que faz com que o snort entre no estado "D", a solução é fazer outra implantação com qualquer alteração fictícia.

Quando você faz login no ramdisk, a principal desvantagem é que o respectivo silo tem um espaço menor alocado e, portanto, os drena com mais frequência sob as mesmas circunstâncias. A próxima saída é o gerenciador de disco de um FPR 4140 com e sem os eventos de registro para o ramdisk habilitado para comparação.

Log no Ramdisk habilitado

```
> 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
```

Registro no Ramdisk desativado

```
> 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
```

O tamanho menor do silo é compensado pela velocidade mais alta para acessar os eventos e transmiti-los ao FMC. Embora esta seja uma opção melhor em condições adequadas, a desvantagem deve ser considerada.

Perguntas frequentes

Os alertas de integridade Drenagem de eventos são gerados apenas por Eventos do Connection?

No.

- Alertas de drenagem frequente podem ser gerados por qualquer silo gerenciador de disco.
- Alertas de drenagem de eventos não processados podem ser gerados por qualquer silo relacionado a eventos.

Os eventos de conexão são os culpados mais comuns.

É sempre aconselhável desativar Registrar no Ramdisk quando um alerta de funcionamento de Drenagem Frequente é visto?

Não. Somente em cenários de log excessivo, exceto para DOS/DDOS, quando o silo afetado é o silo de eventos de conexão e somente nos casos em que não é possível ajustar ainda mais as configurações de log.

Se o DOS/DDOS causar excesso de registro, a solução será implementar a proteção DOS/DDOS ou eliminar a(s) fonte(s) dos ataques DOS/DDOS.

O recurso padrão "Log to Ramdisk" reduz o desgaste da SSD, por isso é altamente recomendável usá-lo.

O que constitui um evento não processado?

Os eventos não são marcados individualmente como não processados. Um arquivo tem eventos não processados quando:

Seu carimbo de data/hora de criação é maior que o campo de carimbo de data/hora no respectivo arquivo de indicador.

or

Seu carimbo de data/hora de criação é igual ao campo de carimbo de data/hora no respectivo arquivo de indicador e seu tamanho é maior que a posição no campo Bytes no respectivo arquivo de indicador.

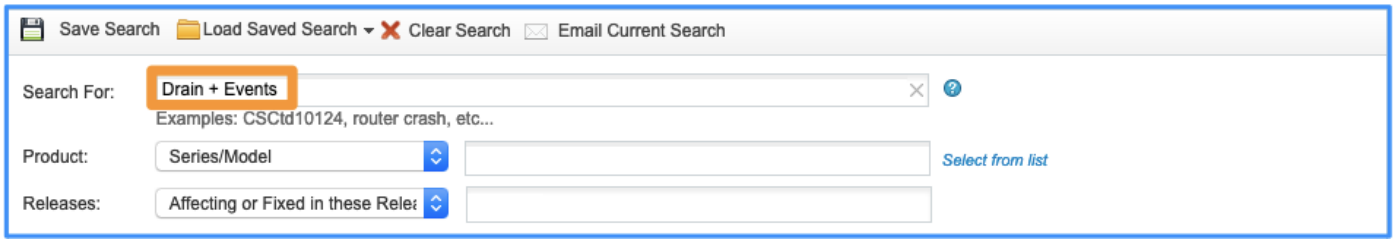
Como o FMC sabe o número de bytes de atraso de um sensor específico?

O sensor envia metadados sobre o nome e o tamanho do arquivo unified_events, bem como informações sobre os arquivos de favoritos, o que dá ao FMC informações suficientes para calcular os bytes que estão por trás como:

Tamanho **atual do** arquivo **unified_events** - **Campo Posição em Bytes**" do arquivo de marcador + Tamanho de todos os arquivos unified_events com carimbo de data/hora maior que o carimbo de data/hora no respectivo arquivo de marcador.

Problemas conhecidos

Abra a Bug Search Tool e use esta consulta:



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.