# Resolución de problemas de drenaje de eventos no procesados de FMC y de alertas frecuentes de monitor de estado de drenaje de eventos

## Contenido



## Introducción

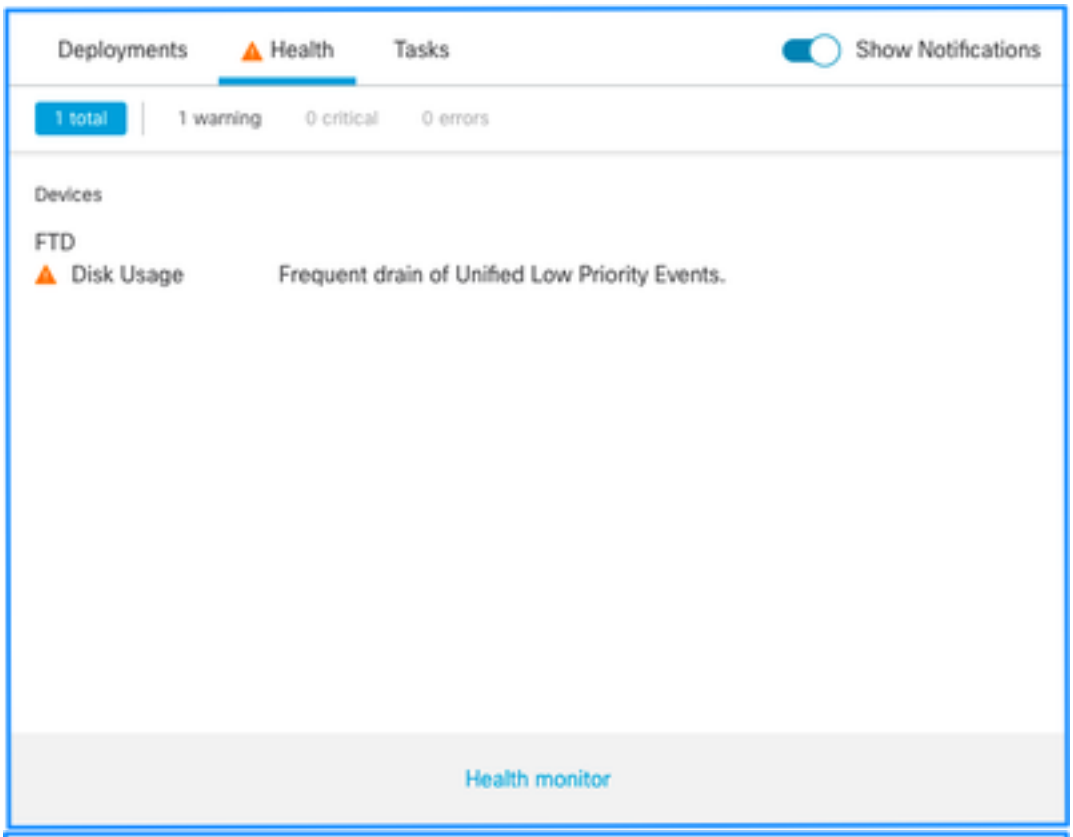
Este documento describe cómo resolver problemas de alertas de estado **Drenaje de eventos sin procesar** y **Drenaje frecuente de eventos** en Firepower Management Center (FMC).

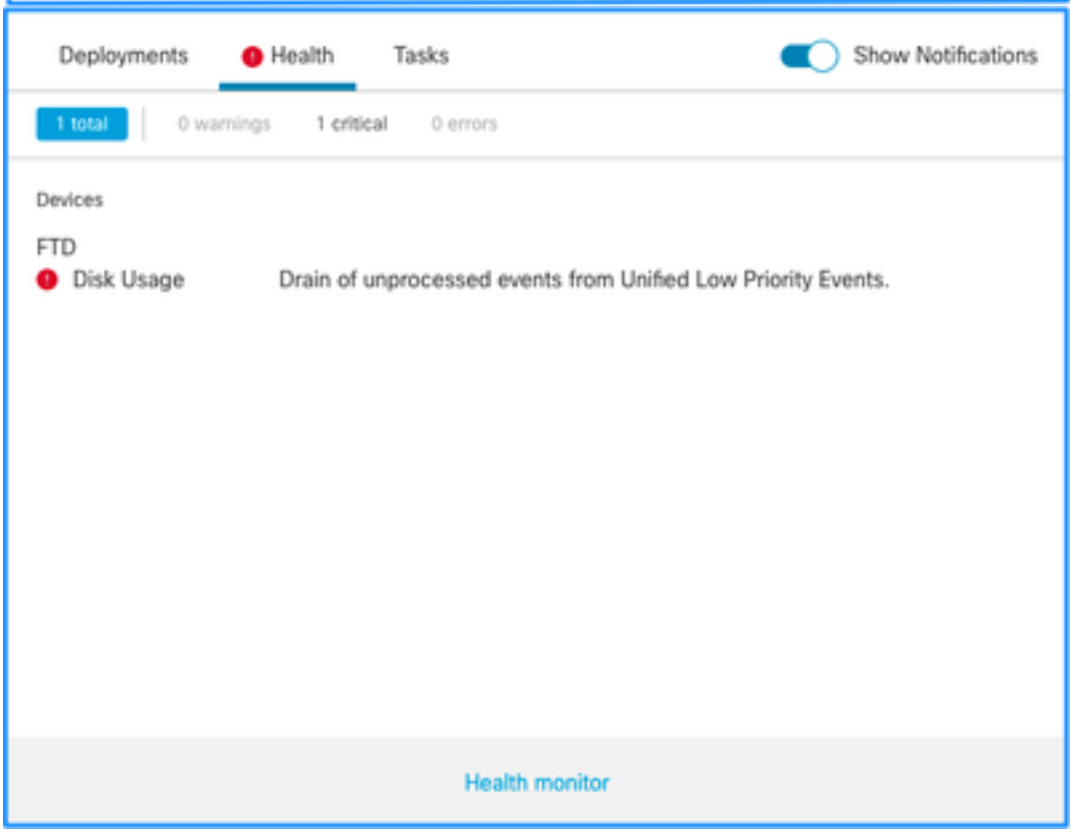
## Descripción general del problema

El FMC genera una de estas alertas sanitarias:

- Drenaje frecuente de eventos de baja prioridad de Unified
  y/o
- Drenaje de eventos sin procesar de eventos de baja prioridad de Unified

Aunque estos eventos se generan y se muestran en el FMC, están relacionados con un sensor de dispositivos gestionados, ya sea un dispositivo Firepower Threat Defence (FTD) o un dispositivo NGIPS (Sistema de prevención de intrusiones de última generación). Para el resto de este documento, el término sensor se refiere tanto a los dispositivos FTD como a los NGIPS, a menos que se especifique lo contrario.




Esta es la estructura de alertas de estado:

- Drenaje frecuente de <SILO NAME>
- Drenaje de eventos sin procesar de <SILO NAME>

En este ejemplo, el NOMBRE DE SILO es **Eventos de Baja Prioridad Unificados**. Éste es uno de los silos del administrador de discos (consulte la sección Información general para obtener una explicación más completa).

Además:

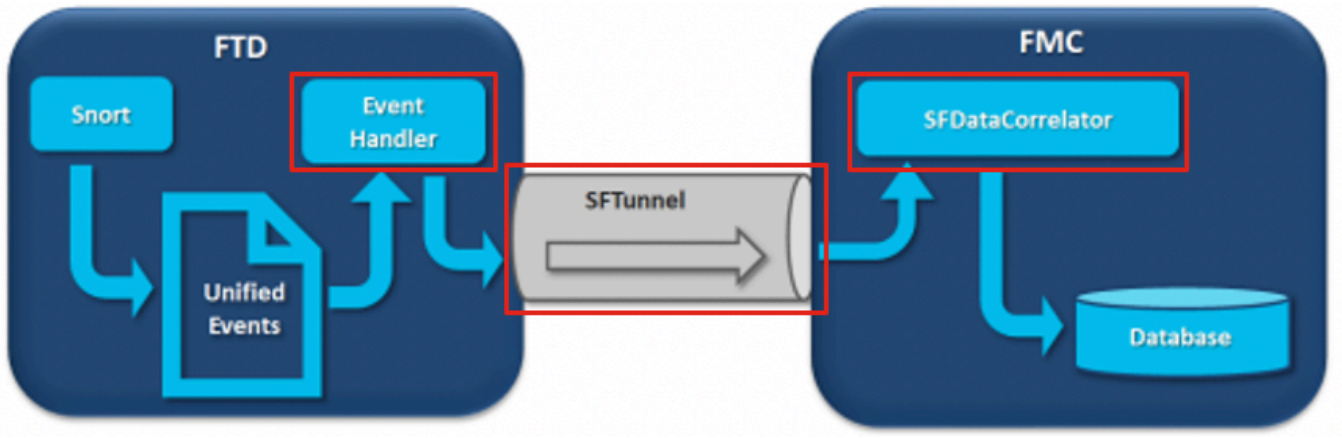
- Aunque cualquier silo puede generar técnicamente una alerta de drenaje frecuente de salud <SILO NAME>, las más frecuentes son las relacionadas con eventos y, entre ellas, las de baja prioridad simplemente porque son el tipo de eventos generados con más frecuencia por los sensores.
- Un evento de "fuga frecuente de <SILO NAME>" tiene una gravedad de advertencia en el caso de que se trate de un silo relacionado con un evento, ya que, si se procesó (a continuación se ofrece una explicación sobre lo que constituye un evento no procesado), se encuentra en la base de datos de FMC.
- Para un silo no relacionado con eventos, como el silo "Copias de seguridad", la alerta es crítica, ya que se pierde esta información.
- Sólo los silos de tipo de evento generan una fuga de eventos no procesados de la alerta de estado <SILO NAME>. Esta alerta siempre tiene gravedad crítica.

Los síntomas adicionales pueden incluir:

- Lentitud en la interfaz de usuario de FMC
- Pérdida de eventos

## Escenarios comunes de Troubleshooting

Un drenaje frecuente del evento <SILO NAME> se debe a una entrada excesiva en el silo para su tamaño. En este caso, el administrador de discos purga (purga) ese archivo al menos dos veces en el último intervalo de 5 minutos. En un silo de tipo de evento, esto suele deberse a un registro excesivo de ese tipo de evento. En el caso de un drenaje de eventos no procesados de la alerta de estado <SILO NAME>, esto también puede deberse a un cuello de botella en la ruta de procesamiento de eventos.




En el diagrama hay 3 cuellos de botella potenciales:

- El proceso EventHandler en FTD está sobresuscrito (se lee más lentamente de lo que escribe Snort)
- La interfaz de eventos está sobresuscrita
- El proceso SFDataCorrelator en FMC está sobresuscrito

Para entender más a fondo la arquitectura Event Processing, consulte la sección Deep Dive

correspondiente.

## Caso 1. Registro excesivo

Como se ha indicado en la sección anterior, una de las causas más comunes de las alertas sanitarias de este tipo es la entrada excesiva.

La diferencia entre la Marca de agua baja (LWM) y la Marca de agua alta (HWM) recopiladas del comando **show disk-manager** CLISH muestra cuánto espacio hay que ocupar en ese silo para pasar de LWM (recién drenado) al valor de HWM. Si se producen fugas frecuentes de eventos (con o sin eventos sin procesar), lo primero que debe revisar es la configuración de registro.

Para obtener una explicación detallada del proceso del Administrador de discos, consulte la sección Perspectiva en profundidad correspondiente.

Tanto si se trata de un registro doble como de una tasa alta de eventos en el ecosistema general de sensores-administradores, se debe realizar una revisión de la configuración de registro.

### Acciones recomendadas

### Paso 1. Compruebe si hay doble registro

Los escenarios de doble registro se pueden identificar si observa el correlator **perfstats** en el FMC como se muestra en esta salida:

```
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
```

En este caso, se puede ver una alta tasa de flujos duplicados en la salida.

### Paso 2. Revise la configuración de registro del ACP

Debe comenzar con una revisión de la configuración de registro de la política de control de acceso (ACP). Asegúrese de seguir las prácticas recomendadas descritas en este documento Prácticas recomendadas para el registro de conexiones

Se recomienda revisar la configuración de registro en todas las situaciones, ya que las

recomendaciones que se enumeran no solo cubren los escenarios de registro doble.

### Paso 3. Compruebe si se espera o no el registro excesivo

Debe revisar si el registro excesivo tiene una causa esperada o no. Si el registro excesivo se debe a un ataque de DOS/DDoS o a un loop de ruteo o a una aplicación/host específica que realiza una gran cantidad de conexiones, debe verificar y mitigar/detener las conexiones de los orígenes de conexión excesivos inesperados.

### Paso 4. Modelo de actualización

Actualice el dispositivo de hardware FTD a un modelo de mayor rendimiento (por ejemplo, FPR2100 —> FPR4100); la fuente de silos aumentaría.

### Paso 5. Considere si puede inhabilitar Log to Ramdisk

En el caso del silo de eventos de baja prioridad de Unified, puede deshabilitar Log to Ramdisk para aumentar el tamaño del silo con los inconvenientes descritos en la sección Perspectiva en profundidad respectiva.

## Caso 2. Un cuello de botella en el canal de comunicación entre el sensor y el FMC

Otra causa común de este tipo de alerta son los problemas de conectividad y/o la inestabilidad en el canal de comunicación (sftunnel) entre el sensor y el FMC. El problema de comunicación puede deberse a:

- sftunnel está inactivo o es inestable (flaps).
- sftunnel está sobresuscrito.

Para el problema de conectividad de sftunnel, asegúrese de que FMC y el sensor tengan disponibilidad entre sus interfaces de administración en el puerto TCP 8305.

En FTD puede buscar la cadena **sftunneld** en el archivo **[/ngfw]/var/log/messages**. Los problemas de conectividad hacen que se generen mensajes como estos:

```
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
```

La sobresuscripción de la interfaz de gestión de los CSP puede ser un pico en el tráfico de gestión o una sobresuscripción constante. Los datos históricos del Health Monitor son un buen indicador de esto.

Lo primero que hay que tener en cuenta es que, en la mayoría de los casos, el FMC se implementa con una única NIC para la gestión. Esta interfaz se utiliza para:

- Gestión de CSP.
- Gestión del sensor FMC.
- Recogida de eventos FMC de los sensores.
- Actualización de fuentes de inteligencia.
- La descarga de actualizaciones de SRU, Software, VDB y GeoDB desde el sitio de descarga de software.
- Consulta de reputación y categorías de URL (si procede).
- Consulta de Disposiciones de archivo (si procede).

#### Acciones recomendadas

Puede implementar una segunda NIC en el FMC para una interfaz dedicada a eventos. Las implementaciones pueden depender del caso práctico.

Las directrices generales se pueden encontrar en la Guía de Hardware de FMC Implementación en una Red de Administración

## Caso 3. Un cuello de botella en el proceso SFDataCorrelator

El último escenario que se tratará es cuando se produzca un cuello de botella en el lado del Correlador de datos de la SDF (FMC).

El primer paso es buscar en el archivo diskmanager.log, ya que hay información importante que se debe recopilar, como:

- La frecuencia del drenaje.
- Número de archivos con eventos no procesados purgados.
- La ocurrencia del drenaje con Eventos sin procesar.

Para obtener información sobre el archivo diskmanager.log y cómo interpretarlo, puede consultar la sección Administrador de discos. La información recopilada del archivo diskmanager.log se puede utilizar para limitar los pasos siguientes.

Además, debe consultar las estadísticas de rendimiento del correlacionador:

```
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
```

Téngase en cuenta que estas estadísticas corresponden al CSP y al conjunto de todos los sensores que gestiona. En el caso de los eventos de baja prioridad de Unified, busca principalmente:

- Flujos totales por segundo de cualquier tipo de evento para evaluar una posible sobresuscripción del proceso SFDataCorrelator.
- Las dos filas resaltadas en el resultado anterior: **flujos ARN/segundo**: indica la velocidad de eventos de baja prioridad procesados por SFDataCorrelator.**flujos rna dup/second** - Indica la tasa de eventos duplicados de baja prioridad procesados por SFDataCorrelator. Esto se genera por el registro doble como se discutió en el escenario anterior.

Sobre la base de los resultados, se puede concluir que:

- No hay registros duplicados, como indica la segunda fila/flujos de duplicación de arn.
- En los flujos de arn/segunda fila, el valor Máximo es mucho mayor que el valor Promedio, por lo que hubo un pico en la tasa de eventos procesados por el proceso SFDataCorrelator. Esto podría esperarse si nos fijamos en esta mañana temprano cuando la jornada laboral de sus usuarios acaba de comenzar, pero en general, es una bandera roja y requiere una investigación adicional.

Puede encontrar más información sobre el proceso SFDataCorrelator en la sección Procesamiento de eventos.

### Acciones recomendadas

En primer lugar, debe determinar cuándo se produjo el pico. Para ello, debe observar las estadísticas del correlacionador por cada intervalo de muestra de 5 minutos. La información recopilada de diskmanager.log puede ayudarle a ir directamente al período de tiempo importante.

> **Consejo:** Canalice el resultado al localizador de Linux **menos** para que pueda buscar fácilmente.

```
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** |

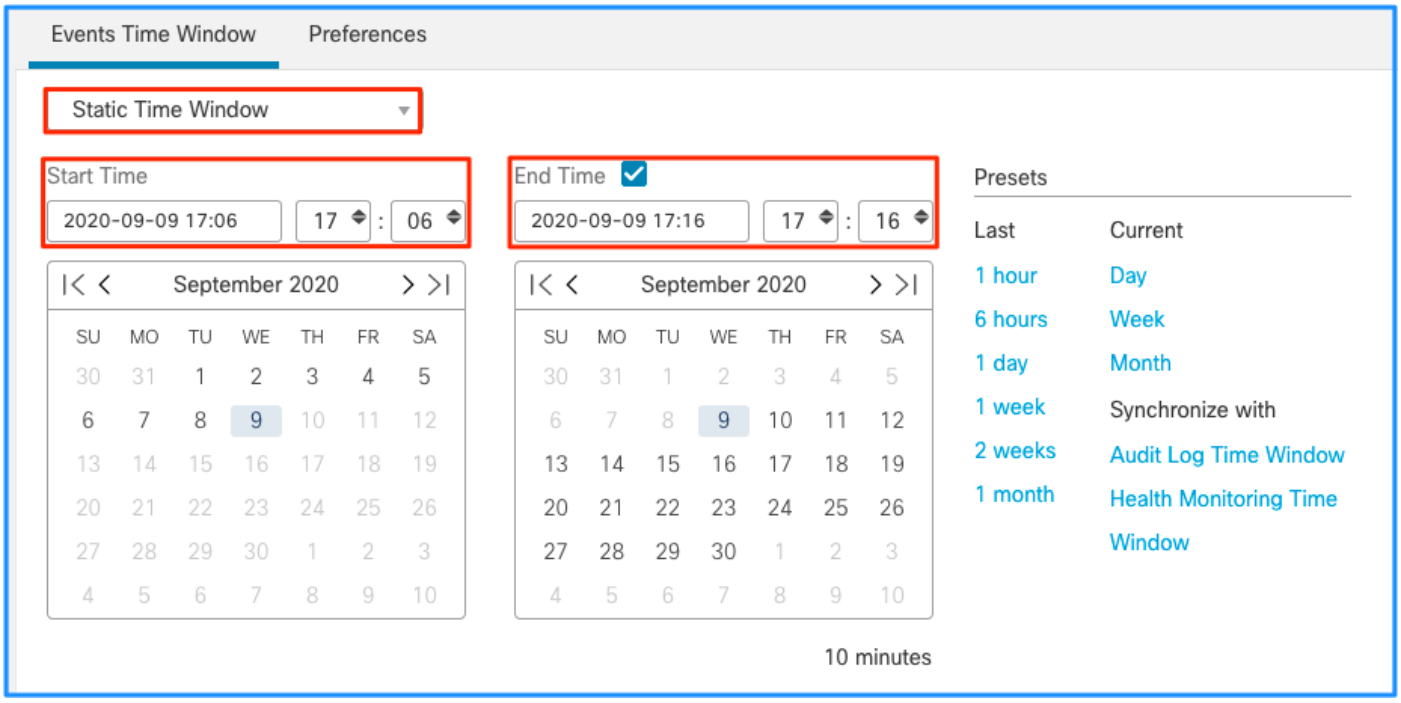
```
                rna dup flows/second:          0.00
                ids alerts/second:             0.00
                ids pkts/second:               0.00
                ids comm records/second:       0.01
                ids extras/second:             0.00
                fw stats/second:               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
```

Utilice la información de la salida para:

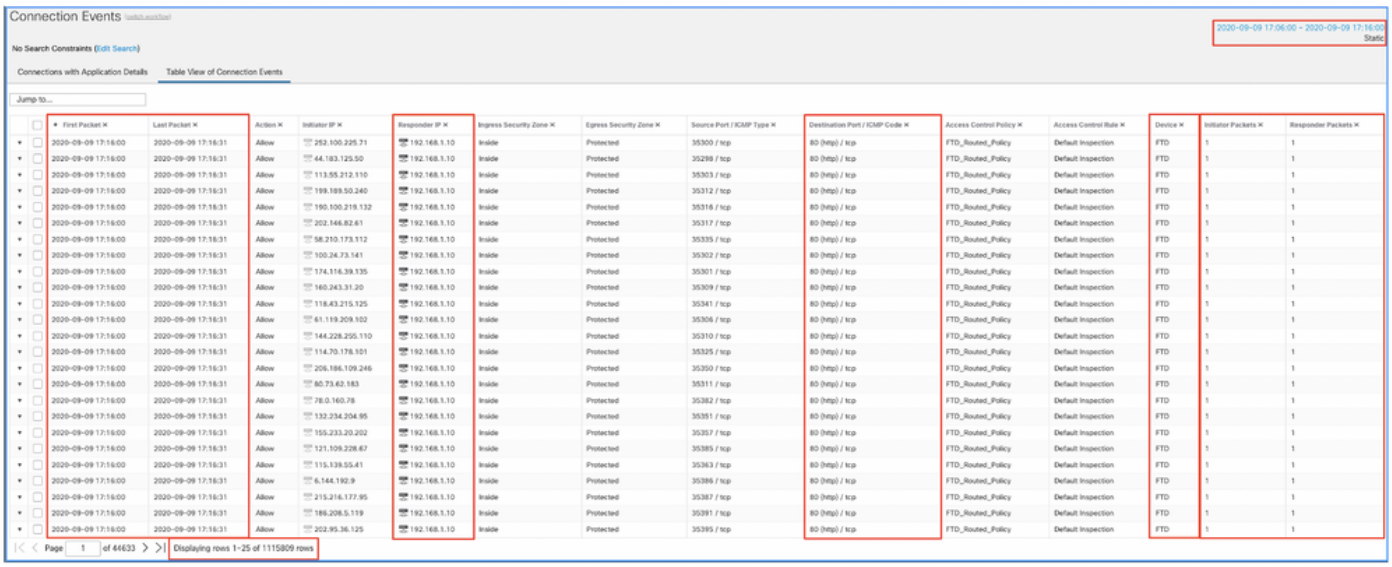
- Determinar la tasa de eventos normal/basal.
- Determine el intervalo de 5 minutos en que se produjo el pico.

En el ejemplo anterior, hay un pico obvio en la tasa de eventos recibidos a las 16:06:39 y más allá. Tenga en cuenta que se trata de promedios de 5 minutos, por lo que el aumento puede ser más brusco de lo que se muestra (ráfaga), pero diluido en este intervalo de 5 minutos si comenzó hacia el final de la misma.

Aunque esto lleva a la conclusión de que este pico de eventos provocó el drenaje de eventos sin procesar, puede echar un vistazo a los eventos de conexión de la interfaz gráfica de usuario (GUI) de FMC con la ventana de tiempo adecuada para entender qué tipo de conexiones atravesaron el cuadro de FTD en este pico:




Aplique esta ventana de tiempo para obtener los eventos de conexión filtrados, no olvide dar cuenta de la zona horaria. En este ejemplo, el sensor utiliza UTC y el FMC UTC+1. Utilice la vista de tabla para ver los eventos que desencadenaron la sobrecarga de eventos y realizar las acciones correspondientes:




Según las marcas de tiempo (hora del primer y último paquete), se puede ver que se trata de conexiones de corta duración. Además, las columnas Paquetes del iniciador y del respondedor muestran que sólo se intercambió 1 paquete en cada dirección. Esto confirma que las conexiones duraron poco e intercambiaron muy pocos datos.

También puede ver que todos estos flujos tienen como objetivo las mismas IP y el mismo puerto de respuesta. Además, todos ellos son reportados por el mismo sensor (que junto con la información de la interfaz de ingreso y egreso puede hablar con el lugar y la dirección de estos flujos). Acciones adicionales:

- Verifique los registros del sistema en el punto final de destino.
- Implementar la protección DOS/DDOS o tomar otras medidas preventivas.

**Nota:** El objetivo de este artículo es proporcionar pautas para resolver problemas de la

alerta de drenaje de eventos no procesados. En este ejemplo se utilizó hping3 para generar una inundación SYN TCP al servidor de destino. Para obtener directrices para reforzar su dispositivo FTD, consulte la Guía de refuerzo de Cisco Firepower Threat Defence

### Elementos que debe recopilar antes de ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC)

Se recomienda encarecidamente recopilar estos elementos antes de ponerse en contacto con el TAC de Cisco:

- Captura de pantalla de las alertas de estado vistas.
- Solucione los problemas de archivo generados desde el FMC.
- Solucione el archivo generado desde el sensor afectado.
- Fecha y hora en que se detectó el problema por primera vez.
- Información sobre cualquier cambio reciente realizado en las políticas (si procede).
- La salida del comando stats_unified.pl como se describe en la sección Procesamiento de Eventos con una mención de los sensores afectados.

## Profundización

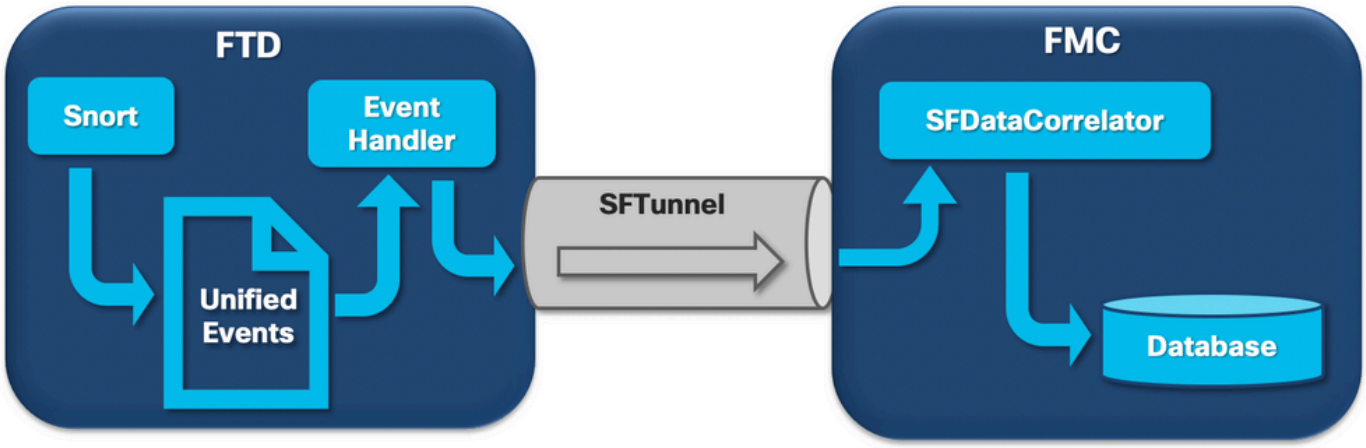
En esta sección se ofrece una explicación detallada de los diversos componentes que pueden participar en este tipo de alertas sanitarias. Esto incluye:

- Procesamiento de eventos: cubre la ruta que toman los eventos tanto en los dispositivos del sensor como en el FMC. Esto es principalmente útil cuando la alerta de estado se refiere a un tipo de evento Silo.
- Administrador de discos: cubre el proceso del administrador de discos, los silos y cómo se drenan.
- Health Monitor: trata sobre cómo se utilizan los módulos Health Monitor para generar alertas de estado.
- Log to Ramdisk - Cubre el registro a la función ramdisk y su posible impacto en las alertas de salud.

Para comprender las alertas de estado de drenaje de eventos y poder identificar puntos de fallo potenciales, es necesario analizar cómo funcionan estos componentes e interactúan entre sí.

### Procesamiento de eventos

Aunque los silos que no están relacionados con eventos pueden activar el tipo de alertas de estado de Drenaje frecuente, la gran mayoría de los casos que ha detectado el Cisco TAC están relacionados con el drenaje de información relacionada con eventos. Además, para comprender lo que constituye una fuga de eventos sin procesar, es necesario echar un vistazo a la arquitectura de procesamiento de eventos y a los componentes que la constituyen.




Cuando un sensor de Firepower recibe un paquete de una nueva conexión, el proceso snort genera un evento en formato unified2, que es un formato binario que permite una lectura/escritura más rápida, así como eventos más ligeros.

El resultado muestra el comando FTD **system support trace** donde puede ver una nueva conexión creada. Se destacan y explican las partes importantes:

```
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
```

Los archivos de Snort unified_events se generan por instancia en la ruta **[/ngfw]var/sf/detection_engine/*/instance-N/**, donde:

- ***** es el UUID de Snort. Se trata de un valor único por dispositivo.
- **N** es el ID de instancia de Snort que se puede calcular como el ID de instancia de la salida anterior (el 0 resaltado en el ejemplo) + 1

Puede haber 2 tipos de archivos unified_events en cualquier carpeta de instancia de Snort:

- unified_events-1 (que contiene eventos de alta prioridad).
- unified_events-2 (que contiene eventos de baja prioridad).

Un evento de alta prioridad es un evento que corresponde a una conexión potencialmente malintencionada.

Tipos de eventos y su prioridad:

| Prioridad alta (1) | Prioridad baja (2) |
|---|---|
| Intrusión | Conexión |
| Malware | Descubrimiento |
| Inteligencia de seguridad | Archivo |

Eventos de conexión asociados  Estadísticas

El siguiente resultado muestra un evento que pertenece a la nueva conexión rastreada en el ejemplo anterior. El formato es unified2 y se toma de la salida del registro de eventos unificado respectivo ubicado en [/ngfw]/var/sf/detection_engine/*/instance-**1**/ donde 1 es el id. de la instancia de snort en negrita en la salida anterior +1. El nombre del formato del registro de eventos unificado sigue la sintaxis unified_events-**2**.log.**1599654750**, donde 2 representa la prioridad de los eventos como se muestra en la tabla y la última parte en negrita (**159999 654750**) es la marca de tiempo (hora Unix) de cuando se creó el archivo.

> **Consejo:** Puede utilizar el comando Linux **date** para convertir la hora Unix en una fecha legible:
> admin@FP1120-2:~$ **sudo date -d@1599654750**
> Miércoles 9 de septiembre 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 a cada archivo unified_events hay un archivo de marcador, que contiene 2 valores importantes:

1. Marca de tiempo correspondiente al archivo unified_events actual para esa instancia y prioridad.
2. Posición en bytes para el último evento leído en el archivo unified_event.

Los valores están en orden separados por una coma como se muestra en este ejemplo:

```
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
```

Esto permite al proceso del administrador de discos saber qué eventos ya se han procesado (enviado a FMC) y cuáles no.

Tenga en cuenta que cuando el administrador de discos vacía un silo de eventos, elimina los archivos de eventos unificados. Para obtener más información sobre la fuga de silos, lea la sección Administrador de discos.

Se considera que un archivo unificado purgado tiene eventos sin procesar cuando uno de estos es verdadero:

1. La marca de tiempo del marcador es inferior a la hora de creación del archivo.
2. La marca de tiempo del marcador coincide con la hora de creación del archivo y la posición en Bytes del archivo es inferior a su tamaño.

El proceso EventHandler lee los eventos de los archivos unificados y los transmite al FMC (como metadatos) a través de sftunnel, que es el proceso responsable de la comunicación cifrada entre el sensor y el FMC. Se trata de una conexión basada en TCP, por lo que el FMC reconoce la transmisión del evento

Puede ver estos mensajes en el archivo [/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
```

Este resultado proporciona esta información:

- Snort abrió el archivo unified_events para obtener la salida (para escribir en él).
- El controlador de eventos abrió el mismo archivo unified_events (para leerlo).
- sftunnel informó el número de eventos procesados desde ese archivo unified_events.

El archivo de marcador se actualiza en consecuencia. El sftunnel utiliza 2 canales diferentes llamados Unified Events (UE) Channel 0 y 1 para eventos de alta y baja prioridad respectivamente.

Con el comando CLI **sfunnel_status** en el FTD, puede ver el número de eventos que se transmitieron.

```
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
```

En el FMC, los eventos se reciben mediante el proceso SFDataCorrelator.

El estado de los eventos que se procesaron desde cada sensor se puede ver con el 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
```

Este comando muestra el estado de la acumulación de eventos para un dispositivo determinado por canal, el ID de canal utilizado es el mismo que el sftunnel.

El valor Bytes detrás se puede calcular como la diferencia entre la posición mostrada en el archivo de marcador de eventos unificado y el tamaño del archivo de eventos unificado, más cualquier archivo subsiguiente con una marca de tiempo superior a la del archivo de marcador.

El proceso SFDataCorrelator también almacena estadísticas de rendimiento, que se guardan en **/var/sf/rna/correlator-stats/**. Se crea un archivo al día para almacenar las estadísticas de rendimiento de ese día en formato CSV. El nombre del archivo utiliza el formato "**AAAA-MM-DD**" y el archivo correspondiente al día actual se llama **now**.

Las estadísticas se recopilan cada 5 minutos (hay una línea por cada intervalo de 5 minutos).

La salida de este archivo se puede leer con el comando **perfstats**. Tenga en cuenta que este comando is también se utiliza para leer archivos de estadísticas de rendimiento de snort, por lo que se deben utilizar los indicadores adecuados:

**-c:** Indica a perfstats que la entrada es un archivo correlator-stats (sin este indicador perfstats supone que la entrada es un archivo de estadísticas de rendimiento de snort).

**-q:** Modo silencioso, imprime sólo el resumen del archivo.

```
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 fila del resumen tiene 3 valores en este orden: Promedio, Mínimo, Máximo.

Si imprime sin el indicador -q, también verá los valores del intervalo de 5 minutos. El resumen se muestra al final.

Tenga en cuenta que cada CSP tiene un caudal máximo descrito en su ficha técnica. La siguiente tabla contiene los valores por módulo tomados de la hoja de datos respectiva:

| Modelo | FMC 750 | FMC 1000 | FMC 1600 | FMC 2000 | FMC 2500 | FMC 2600 | FMC 4000 | FMC 4500 | FMC 4600 | FMCv | FMC |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Velocidad de flujo máxima (fps) | 2000 | 5000 | 5000 | 12000 | 12000 | 12000 | 20000 | 20000 | 20000 | Variable | 12 |

Tenga en cuenta que estos valores son para la suma de todos los tipos de eventos que se muestran en negrita en la salida de las estadísticas de SFDataCorrelator.

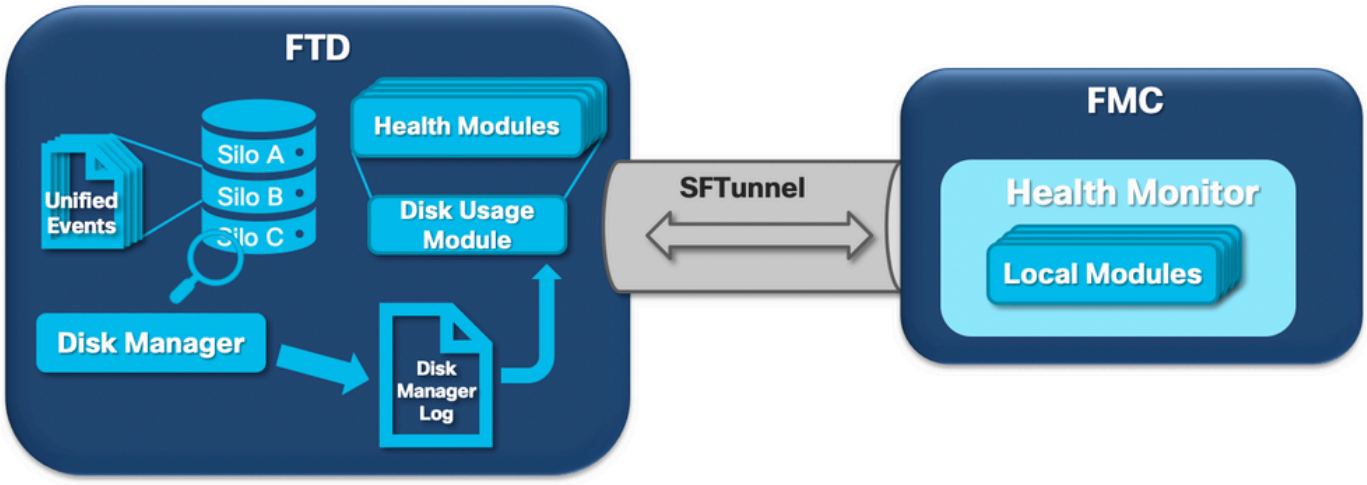
Si observa el resultado y dimensionamos nuestro FMC de tal manera que estamos preparados para el peor escenario posible (cuando todos los valores máximos ocurren al mismo tiempo), entonces la tasa de eventos que este FMC ve es 48.65 + 348.15 + 4.63 + 3.25 + 0.06 = **404.74 fps**.

Este valor total se puede comparar con el valor de la hoja de datos del modelo respectivo.

SFDataCorrelator también puede realizar trabajo adicional sobre los eventos recibidos (como las reglas de correlación) y, a continuación, los almacena en la base de datos que se consulta para rellenar información diversa en la interfaz gráfica de usuario (GUI) de FMC, como paneles y vistas de eventos.

## Administrador de discos

El siguiente diagrama lógico muestra los componentes lógicos de los procesos **Health Monitor** y **Disk Manager** a medida que se entrelazan para la generación de alertas de estado relacionadas con el disco.




En pocas palabras, el proceso del administrador de discos administra el uso del disco de la caja y tiene sus archivos de configuración en la carpeta [/ngfw]/etc/sf/. Existen varios archivos de configuración para el proceso del administrador de discos que se utilizan en determinadas circunstancias:

- diskmanager.conf - Archivo de configuración estándar.

- diskmanager_2hd.conf - Se utiliza cuando la caja tiene 2 discos duros instalados. El segundo disco duro es el relacionado con la expansión de malware, que se utiliza para almacenar archivos según se define en la política de archivos.
- ramdisk-diskmanager.conf - Se utiliza cuando se habilita Log to Ramdisk. Para obtener más información, consulte la sección Log to Ramdisk.

A cada tipo de archivo supervisado por el administrador de discos se le asigna un Silo. Según la cantidad de espacio de disco disponible en el sistema, el administrador de discos calcula una marca de agua alta (HWM) y una marca de agua baja (LWM) para cada silo.

Cuando el proceso del administrador de discos drena un silo, lo hace hasta el punto donde se alcanza el LWM. Dado que los eventos se purgan por archivo, este umbral se puede cruzar.

Para verificar el estado de los silos en un dispositivo sensor, puede utilizar 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
```

El proceso del administrador de discos se ejecuta cuando se cumple una de estas condiciones:

- El proceso se inicia (o se reinicia)
- Un Silo alcanza el HWM
- Un silo se drena manualmente
- Una vez cada hora

Cada vez que se ejecuta el proceso del administrador de discos, genera una entrada para cada uno de los diferentes silos en su propio archivo de registro, que se encuentra en [/ngfw]/var/log/diskmanager.log y tiene datos en formato CSV.

A continuación, se muestra una línea de ejemplo del archivo diskmanager.log, tomada de un sensor que activó el drenaje de eventos no procesados desde la alerta de estado de eventos de baja prioridad de Unified, así como el desglose de las columnas respectivas:

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

| Columna | Valor |
|---|---|
| Etiqueta de silo | priority_2_events |
| Tiempo de drenaje (tiempo Epoch) | 1599668981 |

| | |
|---|---|
| Número de archivos vaciados | 221 |
| Bytes vaciados | 4587929508 |
| Tamaño actual de los datos después del drenaje (bytes) | 1132501868 |
| Mayor archivo vaciado (bytes) | 20972020 |
| Archivo más pequeño vaciado (bytes) | 4596 |
| Archivo más antiguo vaciado (época) | 1586044534 |
| Límite máximo (bytes) | 5710966962 |
| Límite bajo (bytes) | 1142193392 |
| Número de archivos con eventos sin procesar purgados | 110 |
| Indicador de estado de Diskmanager | 0 |

Esta información la lee el módulo Health Monitor correspondiente para activar la alerta de estado relacionada.

### Escurrir manualmente un silo

En ciertos escenarios, es posible que desee drenar manualmente un silo. Por ejemplo, para borrar el espacio en disco con el drenaje manual de silos en lugar de la eliminación manual de archivos tiene la ventaja del administrador de discos para decidir qué archivos mantener y cuáles eliminar. El administrador de discos conserva los archivos más recientes para ese silo.

Cualquier silo se puede vaciar y esto funciona como ya se ha descrito (el administrador de discos purga los datos hasta que la cantidad de datos pasa por debajo del umbral LWM). El comando **system support silo-drain** está disponible en el modo FTD CLISH y proporciona una lista de los silos disponibles (nombre + id numérico).

Este es un ejemplo de un drenaje manual del silo de eventos de baja prioridad de Unified:

```
> 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 estado

Estos son los puntos principales:

- El proceso Health Monitor genera cualquier alerta de estado que se vea en el FMC en el menú Health Monitor o en la ficha Health del Message Center.
- Este proceso supervisa el estado del sistema, tanto para el CSP como para los sensores gestionados, y se compone de varios módulos diferentes.
- Los módulos de alerta de estado se definen en la Política de estado que se puede adjuntar por dispositivo.
- Las alertas de estado las genera el módulo Uso de discos que puede ejecutarse en cada uno de los sensores gestionados por el FMC.

- Cuando se ejecuta el proceso de supervisión de estado en FMC (una vez cada 5 minutos o cuando se activa una ejecución manual), el módulo Uso de disco busca en el archivo diskmanager.log y, si se cumplen las condiciones correctas, se activa la alerta de estado correspondiente.

Para que se active una alerta de estado **Drenaje de eventos no procesados**, deben cumplirse todas estas condiciones:

1. El campo Bytes vaciados es mayor que 0 (esto indica que se vaciaron los datos de este silo).
2. El número de archivos con eventos sin procesar purgados mayor que 0 (esto indica que había eventos sin procesar en los datos purgados).
3. El tiempo de drenaje es dentro de la última 1 hora.

Para que se active una alerta de estado **de** Drenaje frecuente de **eventos**, estas condiciones deben ser verdaderas:

1. Las últimas 2 entradas del archivo diskmanager.log necesitan: Haga que Bytes drenen el campo mayor que 0 (esto indica que se drenaron los datos de este silo).Estar separados menos de 5 minutos.
2. El tiempo de vaciado de la última entrada para este silo es en la última hora.

El recopilador de resultados del módulo de uso del disco (así como los resultados recopilados por los otros módulos) se envían al FMC a través de sftunnel. Puede ver los contadores para los eventos de estado intercambiados sobre sftunnel con el 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
```

## Iniciar sesión en Ramdisk

Aunque la mayoría de los eventos se almacenan en disco, el dispositivo está configurado de forma predeterminada para registrar en ramdisk para evitar daños graduales en la SSD que pueden ser causados por escrituras y eliminaciones constantes de eventos en disco.

En esta situación, los eventos no se almacenan en **[/ngfw]/var/sf/detection_engine/*/instance-N/,** sino que se encuentran en **[/ngfw]/var/sf/detection_engine**/*/**instance-N/connection/**, que es un enlace simbólico a **la conexión/dev/shm/instance-N/connection.** En este caso, los eventos residen en la memoria virtual en lugar de en la 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 lo que el dispositivo está actualmente configurado para hacer, ejecute el comando **show log-events-to-ramdisk** desde FTD CLISH. También puede cambiar esto si utiliza el 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)
```

> **Advertencia:** Cuando se ejecuta el comando "configure log-events-to-ramdisk disable", es necesario realizar dos implementaciones en el FTD para que el snort no se atasque en el estado "D" (suspensión ininterrumpible), lo que provocaría la interrupción del tráfico. Este comportamiento se documenta en el defecto con el ID de bug de Cisco CSCvz5372. Con la primera implementación, la reevaluación de la etapa de memoria del snort se salta lo que hace que el snort pase al estado "D", la solución alternativa es hacer otra implementación con cualquier cambio ficticio.

Cuando se inicia sesión en ramdisk, el principal inconveniente es que el silo respectivo tiene un espacio más pequeño asignado y, por lo tanto, los drena más a menudo en las mismas circunstancias. El siguiente resultado es el administrador de disco de un FPR 4140 con y sin los eventos de registro a ramdisk habilitados para la comparación.

### Registro en 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 en Ramdisk deshabilitado

```
> 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 |

El menor tamaño del silo se compensa con una mayor velocidad para acceder a los eventos y transmitirlos al FMC. Aunque esta es una mejor opción en condiciones adecuadas, se debe considerar el inconveniente.

# Preguntas frecuentes

### ¿Las alertas de estado de drenaje de eventos sólo las generan los eventos de conexión?

No.

- Cualquier silo del administrador de discos puede generar alertas de drenaje frecuente.
- Cualquier silo relacionado con eventos puede generar alertas de eliminación de eventos no procesados.

Los eventos de conexión son los culpables más comunes.

### ¿Es siempre recomendable inhabilitar Log to Ramdisk cuando se ve una alerta de estado de drenaje frecuente?

No. Sólo en escenarios de Registro Excesivo excepto para DOS/DDOS, cuando el Silo afectado es el silo de Eventos de Conexión, y sólo en casos en los que no es posible ajustar más la Configuración de Registro.

Si DOS/DDOS causa un registro excesivo, la solución es implementar la protección DOS/DDOS o eliminar el origen o los orígenes de los ataques DOS/DDOS.

La función predeterminada "Log to Ramdisk" (Iniciar sesión en Ramdisk) reduce el desgaste de la SSD, por lo que se recomienda encarecidamente su uso.

### ¿Qué constituye un evento sin procesar?

Los eventos no se marcan individualmente como no procesados. Un archivo tiene eventos sin procesar cuando:

Su marca de tiempo de creación es mayor que el campo de marca de tiempo del archivo de marcador correspondiente.

or

Su marca de tiempo de creación es igual al campo de marca de tiempo del archivo de marcador respectivo y su tamaño es mayor que la posición en el campo Bytes del archivo de marcador respectivo.

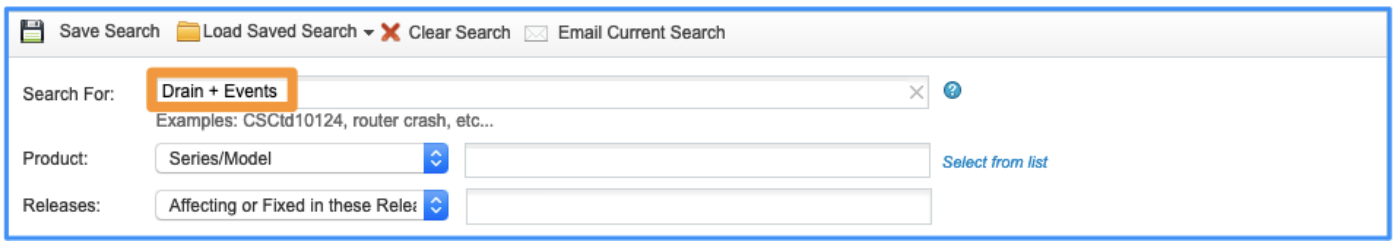
### ¿Cómo sabe el CSP el número de bytes que hay detrás de un sensor concreto?

El sensor envía metadatos sobre el nombre y el tamaño del archivo unified_events, así como la información sobre los archivos de marcadores, lo que proporciona al FMC suficiente información para calcular los bytes subyacentes como:

**Tamaño actual del** archivo **unified_events** - **Posición en bytes**" campo del archivo de marcador + Tamaño de todos los archivos unified_events con una marca de tiempo superior a la marca de tiempo en el archivo de marcador respectivo.

# Problemas conocidos

Abra la Herramienta Bug Search y utilice esta consulta:



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).