Risoluzione dei problemi relativi allo svuotamento degli eventi non elaborati di FMC e allo svuotamento frequente degli eventi Avvisi di Health Monitor

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di svuotamento degli eventi non elaborati e degli avvisi di integrità Svuotamento frequente degli eventi in Firepower Management Center.

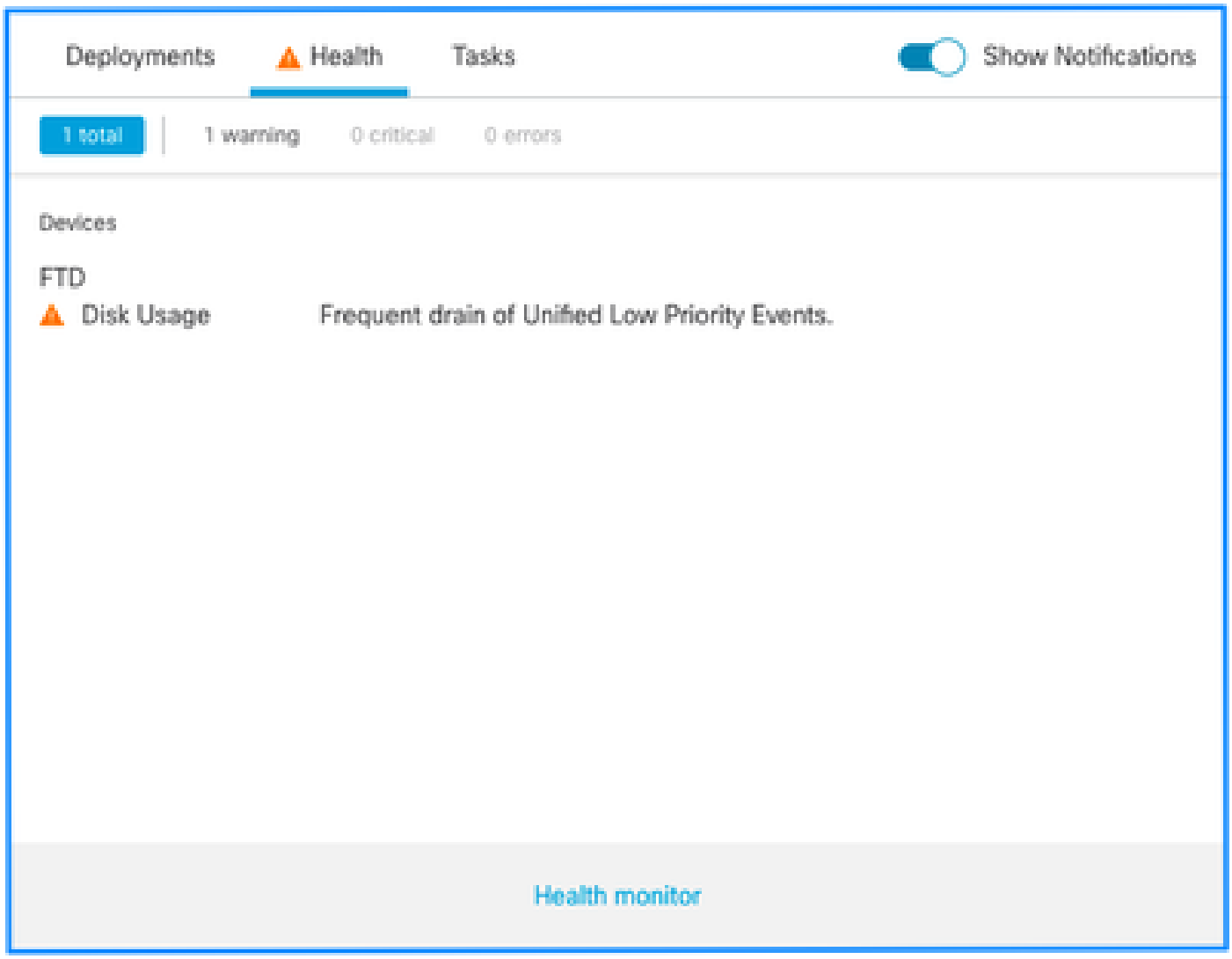
Panoramica del problema

Firepower Management Center (FMC) genera uno dei seguenti avvisi di stato:

- Eventi unificati a bassa priorità eliminati di frequente
- Svuotamento di eventi non elaborati da eventi unificati a bassa priorità

Sebbene questi eventi vengano generati e visualizzati sul FMC, sono correlati a un sensore di dispositivo gestito, sia che si tratti di un dispositivo Firepower Threat Defense (FTD) o di un

dispositivo Next-Generation Intrusion Prevention System (NGIPS). Nel prosieguo di questo documento, il termine sensore si riferisce sia a FTD che a NGIPS, a meno che non sia specificato diversamente.



Questa è la struttura degli avvisi sull'integrità:

- Scarico frequente di <NOME SILO>
- Svuotamento degli eventi non elaborati da <NOME SILO>

Nell'esempio, il nome del SILO è Unified Low Priority Events. Questo è uno degli archivi di Gestione dischi (per una spiegazione più dettagliata, vedere la sezione Informazioni di base).

Inoltre:

- Sebbene ogni silo possa generare tecnicamente un Frequent drain di allarme sanitario di <SILO NAME>, i più comunemente visti sono quelli relativi agli eventi e, tra questi, gli eventi a bassa priorità semplicemente perché sono il tipo di eventi più spesso generati dai sensori.
- Un evento Frequent drain of <SILO NAME> ha un livello di gravità Warning nel caso si tratti di un silo correlato a un evento poiché, se questo è stato elaborato (la spiegazione su cosa costituisce un evento non elaborato viene fornita successivamente), si trova nel database

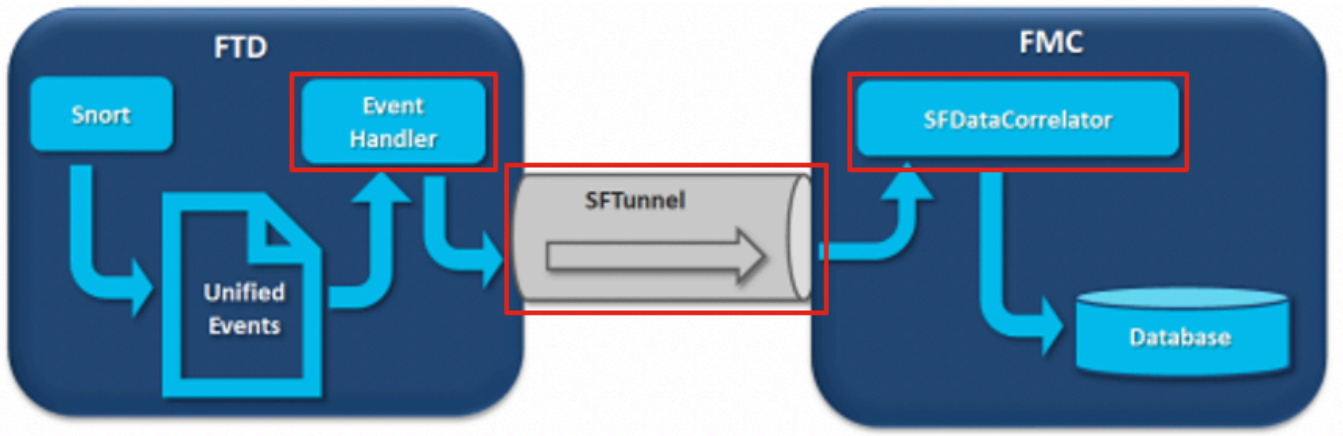
FMC.
- Per un silo non correlato a eventi, ad esempio il silo Backup, l'avviso è di tipo Critico in quanto tali informazioni vengono perse.
- Solo i silos dei tipi di eventi generano uno svuotamento degli eventi non elaborati dall'avviso di integrità <SILO NAME>. L'avviso ha sempre un livello di gravità Critico.

Altri sintomi possono includere:

- Lentezza nell'interfaccia utente del CCP
- Perdita di eventi

Scenari comuni di risoluzione dei problemi

Un evento Frequent drain of <SILO NAME> è causato da un input eccessivo nel silo per le sue dimensioni. In questo caso, il gestore del disco scarica (elimina) il file almeno due volte nell'ultimo intervallo di 5 minuti. In un silo di tipi di eventi, questo problema è in genere causato da un numero eccessivo di registrazioni di quel tipo di eventi. Nel caso di uno svuotamento di eventi non elaborati di un avviso di integrità <SILO NAME>, ciò può anche essere causato da un collo di bottiglia nel percorso di elaborazione degli eventi.



Nel diagramma sono illustrati tre potenziali colli di bottiglia:

- Il processo EventHandler su FTD è sovrascritto (legge più lentamente di quanto scrive Snort).
- Sottoscrizione eccessiva dell'interfaccia di gestione eventi.
- Il processo SFDataCorrelator su FMC è sovrascritto.

Per informazioni più dettagliate sull'architettura di elaborazione degli eventi, fare riferimento alla rispettiva sezione Deep Dive.

Caso 1. Registrazione eccessiva

Come accennato nella sezione precedente, una delle cause più comuni per questo tipo di allarmi sull'integrità è l'input eccessivo.

La differenza tra il valore LWM (Low Water Mark) e il valore HWM (High Water Mark) raccolti dal comando show disk-manager CLISH mostra lo spazio necessario per occupare quel silo e passare da LWM (appena prosciugato) al valore HWM. Se si verificano frequenti svuotamenti di eventi (con o senza eventi non elaborati), la prima cosa da esaminare è la configurazione di registrazione.

Per una spiegazione dettagliata del processo di Gestione dischi, consultare la sezione Deep Dive corrispondente.

Che si tratti di una doppia registrazione o di un'alta percentuale di eventi nell'ecosistema generale dei manager-sensori, è necessario rivedere le impostazioni di registrazione.

Azioni consigliate

Passaggio 1. Verificare la presenza di una doppia registrazione.

È possibile identificare scenari di doppia registrazione se si considerano le prestazioni dei correlatori nel FMC, come mostrato nell'output seguente:

<#root>

```
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
```

In questo caso, nell'output è possibile vedere un'alta percentuale di flussi duplicati.

Passaggio 2. Esaminare le impostazioni di registrazione del punto di accesso.

È necessario iniziare con una revisione delle impostazioni di registrazione dei criteri di controllo di accesso. Assicurarsi di utilizzare le procedure consigliate descritte in questo documento [Procedure consigliate per la registrazione delle connessioni]

Si consiglia di rivedere le impostazioni di registrazione in tutte le situazioni, in quanto i consigli elencati non riguardano solo gli scenari di doppia registrazione.

Per verificare la frequenza degli eventi generati su FTD, controllare questo file e concentrarsi sulle colonne TotalEvents e PerSec:

<#root>

```
admin@firepower:/ngfw/var/log$

sudo more EventHandlerStats.2023-08-13 | grep Total | more


{"Time": "2023-08-13T00:03:37Z",

"TotalEvents": 298

,

"PerSec": 0

, "UserCPUSec": 0.995, "SysCPUSec": 4.598, "%CPU": 1.9, "MemoryKB": 33676}
{"Time": "2023-08-13T00:08:37Z", "TotalEvents": 298, "PerSec": 0, "UserCPUSec": 1.156, "SysCPUSec": 4.2
{"Time": "2023-08-13T00:13:37Z", "TotalEvents": 320, "PerSec": 1, "UserCPUSec": 1.238, "SysCPUSec": 4.2
{"Time": "2023-08-13T00:18:37Z", "TotalEvents": 312, "PerSec": 1, "UserCPUSec": 1.008, "SysCPUSec": 4.4
{"Time": "2023-08-13T00:23:37Z", "TotalEvents": 320, "PerSec": 1, "UserCPUSec": 0.977, "SysCPUSec": 4.4
{"Time": "2023-08-13T00:28:37Z", "TotalEvents": 299, "PerSec": 0, "UserCPUSec": 1.066, "SysCPUSec": 4.3
```

Passaggio 3. Verificare se è prevista o meno la registrazione eccessiva.

È necessario verificare se la causa della registrazione in eccesso è prevista o meno. Se la registrazione eccessiva è causata da un attacco DOS/DDoS o da un ciclo di routing o da un'applicazione/host specifico che crea un numero elevato di connessioni, è necessario controllare e mitigare/interrompere le connessioni dalle origini di connessione eccessive impreviste.

Passaggio 4. Verificare se il file diskmanager.log è danneggiato.

In genere, una voce può avere 12 valori separati da virgole. Per verificare la presenza di righe danneggiate con un numero diverso di campi:

<#root>

```
admin@firepower:/ngfw/var/log$

sudo cat diskmanager.log | awk -F',' 'NF != 12 {print}'
```

```
admin@firepower:/ngfw/var/log$
```

Se è presente una linea danneggiata con diversi da 12 campi, vengono visualizzati.

Passaggio 5. Aggiorna modello.

Aggiornare il dispositivo hardware FTD a un modello con prestazioni più elevate (ad esempio FPR2100 —> FPR4100), l'origine del silo aumenterebbe.

Passaggio 6. Valutare se è possibile disabilitare Log to Ramdisk.

Nel caso del silo Unified Low Priority Events, è possibile disabilitare Log to Ramdisk per aumentare le dimensioni del silo con gli svantaggi illustrati nella rispettiva sezione Deep Dive.

Caso 2. Un collo di bottiglia nel canale di comunicazione tra il sensore e il CCP

Un'altra causa comune di questo tipo di allarme è costituita da problemi di connettività e/o instabilità nel canale di comunicazione (sftunnel) tra il sensore e la console centrale di gestione. Il problema di comunicazione può essere dovuto a:

- sftunnel è inattivo o instabile (flap).
- sottoscrizione eccessiva di sftunnel.

Per il problema di connettività del tunnel sicuro, verificare che FMC e il sensore abbiano raggiungibilità tra le loro interfacce di gestione sulla porta TCP 8305.

Con FTD è possibile cercare la stringa sftunneld nel file [/ngfw]/var/log/messages. I problemi di connettività provocano la generazione di messaggi di questo tipo:

<#root>

```
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. drop

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

Sep  9 15:41:35 firepower SF-IMS[5458]: [27602]

sftunneld:sf_channel [INFO] >> ChannelState freeChannel peer 10.62.148.75 / channelB / DROPPED [ msgSock

Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_connections [INFO] Need to send SW version
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_peers [INFO] Confirm RPC service in CONTRO
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState do_dataio_f
Sep  9 15:41:48 firepower SF-IMS[5458]: [5464] sftunneld:tunnsockets [INFO] Started listening on port 8
Sep  9 15:41:51 firepower SF-IMS[5458]: [27602] sftunneld:control_services [INFO] Successfully Send Int
Sep  9 15:41:53 firepower SF-IMS[5458]: [5465] sftunneld:sf_connections [INFO] Start connection to : 10
```

```
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_peers [INFO] Peer 10.62.148.75 needs the s
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Interface management0 is config
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Connect to 10.62.148.75 on port
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Initiate IPv4 connection to 10.
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Initiating IPv4 connection to 1
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Wait to connect to 8305 (IPv6):
```

La sottoscrizione in eccesso dell'interfaccia di gestione FMC può essere un picco nel traffico di gestione o una sovrassegnazione costante. I dati storici del Health Monitor ne sono un buon indicatore.

La prima cosa da notare è che nella maggior parte dei casi il FMC viene implementato con una singola scheda NIC per la gestione. Questa interfaccia viene utilizzata per:

- Gestione FMC
- Gestione dei sensori FMC
- Raccolta eventi FMC dai sensori
- Aggiornamento dei feed di intelligence
- Download di SRU, software, VDB e aggiornamenti GeoDB dal sito di download del software
- Query per reputazione e categorie URL (se applicabile)
- La query per le disposizioni file (se applicabile)

Azioni consigliate

È possibile distribuire una seconda scheda NIC nel FMC per un'interfaccia dedicata agli eventi. Le implementazioni possono dipendere dallo Use Case.

Le linee guida generali sono disponibili nella Guida hardware di FMC Distribuzione in una rete di gestione

Caso 3. Un collo di bottiglia nel processo SFDataCorrelator

L'ultimo scenario da considerare è quando si verifica il collo di bottiglia sul lato SFDataCorrelator (FMC).

Il primo passaggio consiste nell'esaminare il file diskmanager.log in quanto è necessario raccogliere informazioni importanti quali:

- Frequenza dello scarico.
- Numero di file con eventi non elaborati eliminati.
- Occorrenza dell'eliminazione con eventi non elaborati.

Per informazioni sul file diskmanager.log e su come interpretarlo, consultare la sezione Gestione dischi. Le informazioni raccolte da diskmanager.log possono essere utilizzate per restringere i passaggi successivi.

Inoltre, è necessario esaminare le statistiche sulle prestazioni dei correlatori:

<#root>

```
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
```

Queste statistiche sono destinate al CCP e corrispondono all'aggregato di tutti i sensori da esso gestiti. Nel caso di eventi unificati a bassa priorità, si cercano principalmente:

- Flussi totali al secondo di qualsiasi tipo di evento per valutare eventuali sottoscrizioni in eccesso del processo SFDataCorrelator.
- Le due righe evidenziate nell'output precedente:
  - flussi rna/secondo: indica la frequenza di eventi a bassa priorità elaborati da SFDataCorrelator.
  - flussi dup rna/secondo: indica la frequenza di eventi di bassa priorità duplicati elaborati da SFDataCorrelator. Questo viene generato dalla registrazione doppia come descritto nello scenario precedente.

Sulla base dei risultati ottenuti si può concludere che:

- Non sono presenti registrazioni duplicate come indicato dai flussi di dup RNA al secondo.
- Nella riga Flussi rna/secondo, il valore Massimo è molto più alto del valore Medio, pertanto si è verificato un picco nella frequenza degli eventi elaborati dal processo SFDataCorrelator. Questo è probabile se si considera questa mattina presto quando la giornata di lavoro degli utenti è appena iniziata, ma in generale si tratta di un segnale d'allarme che richiede ulteriori indagini.

Ulteriori informazioni sul processo SFDataCorrelator sono disponibili nella sezione Elaborazione eventi.

Azioni consigliate

Innanzitutto, dovete determinare quando si è verificato il picco. A tale scopo, è necessario esaminare le statistiche del correlatore per ogni intervallo di campionamento di 5 minuti. Le informazioni raccolte dal file diskmanager.log consentono di passare direttamente all'intervallo temporale importante.

Suggerimento: reindirizzare l'output al cercapersone Linux in modo da semplificare le ricerche.

<#root>

```
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
```

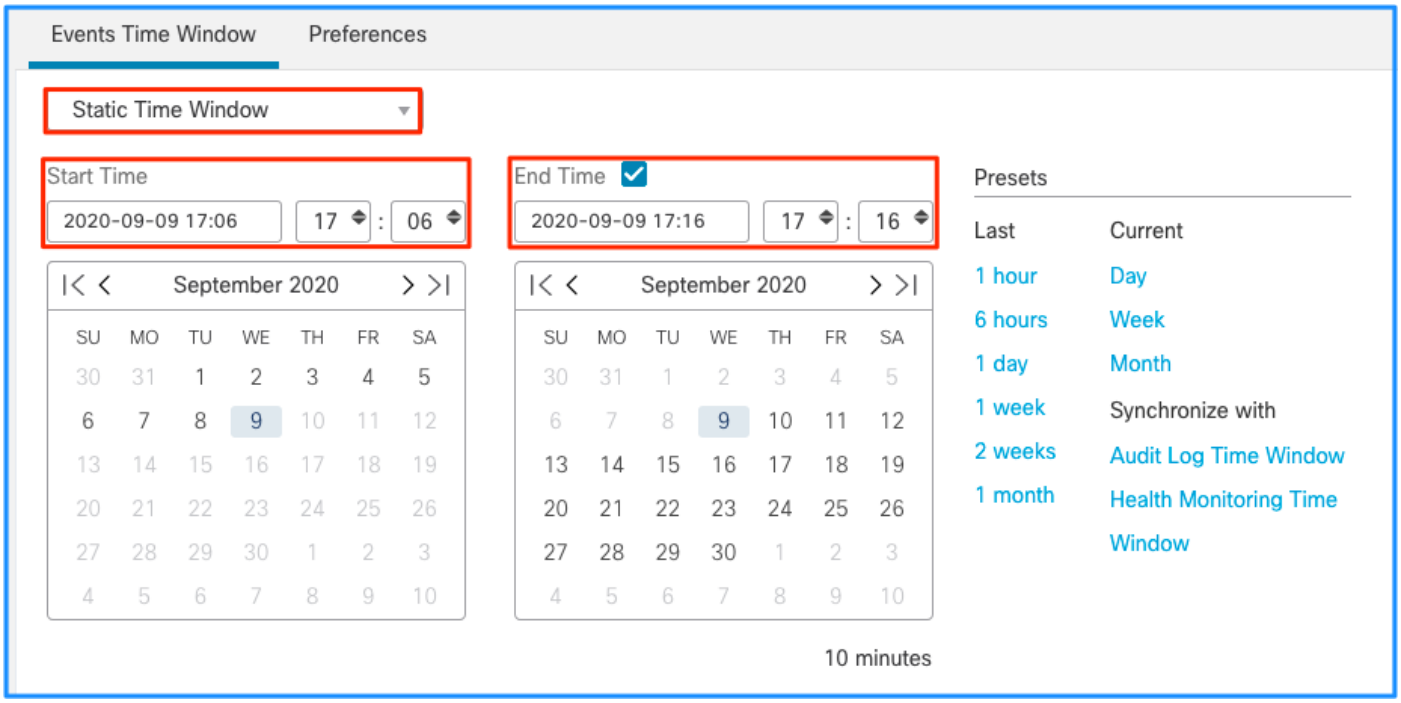
```
memory usage:                   5010148         0               5138904
resident memory usage:          757165          0               900792

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
```

Utilizzate le informazioni nell'output per:

- Determinare la frequenza normale/di base degli eventi.
- Determinare l'intervallo di 5 minuti in cui si è verificato il picco.

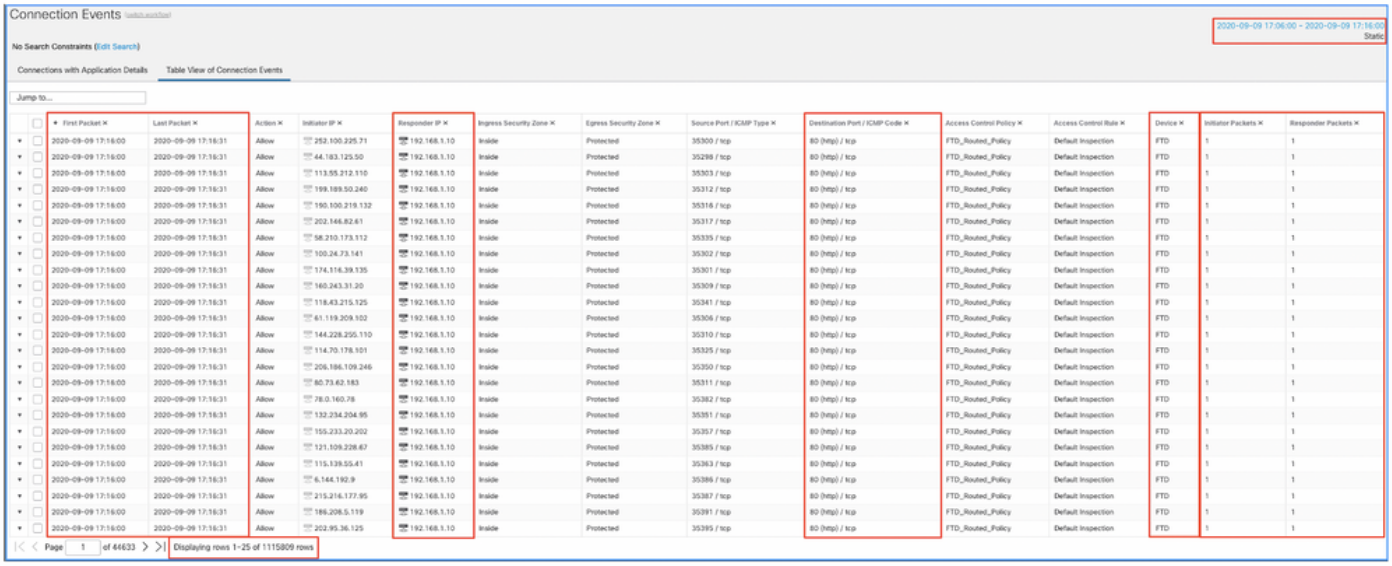
Nell'esempio precedente, è presente un evidente picco nella frequenza degli eventi ricevuti alle 16:06:39 e oltre. Si tratta di medie di 5 minuti, quindi l'aumento può essere più brusco di quanto mostrato (burst) ma diluito in questo intervallo di 5 minuti se inizia verso la fine.

Anche se questo porta alla conclusione che questo picco di eventi ha causato lo svuotamento di eventi non elaborati, è possibile esaminare gli eventi di connessione dall'interfaccia grafica dell'utente (GUI) di FMC con la finestra temporale appropriata per comprendere quale tipo di connessioni ha attraversato la casella FTD in questo picco:



Applica questa finestra temporale per ottenere gli eventi di connessione filtrati. Non dimenticare di tenere conto del fuso orario. In questo esempio, il sensore utilizza UTC e FMC UTC+1. Utilizzare la Vista tabella per visualizzare gli eventi che hanno attivato il sovraccarico degli eventi e adottare

le misure appropriate:



In base all'indicatore di data e ora del primo e dell'ultimo pacchetto, si può verificare che si tratta di connessioni di breve durata. Inoltre, le colonne Initiator e Responder Packets mostrano che è stato scambiato solo un pacchetto in ciascuna direzione. Ciò conferma che le connessioni erano di breve durata e scambiavano pochissimi dati.

È inoltre possibile notare che tutti questi flussi hanno come destinazione gli stessi IP e la stessa porta dei responder. Inoltre, sono tutti segnalati dallo stesso sensore (che insieme alle informazioni dell'interfaccia Ingress ed Egress può parlare al luogo e alla direzione di questi flussi). Azioni aggiuntive:

- Controllare i syslog sull'endpoint di destinazione.
- Implementare la protezione DOS/DDOS o adottare altre misure preventive.

Nota: in questo articolo vengono fornite linee guida per la risoluzione dei problemi relativi all'avviso Svuotamento degli eventi non elaborati. In questo esempio viene usato il comando hping3 per generare un flusso SYN di TCP verso il server di destinazione. Per le linee guida per fortificare il dispositivo FTD, consultare la Cisco Firepower Threat Defense Hardening Guide

---

Elementi da raccogliere prima di contattare il Cisco Technical Assistance Center (TAC)

Si consiglia di raccogliere questi elementi prima di contattare Cisco TAC:

- Screenshot degli allarmi rilevati.
- Risolvere i problemi relativi al file generato dal CCP.
- Risolvere i problemi relativi al file generato dal sensore interessato.
- Data e ora in cui il problema è stato rilevato per la prima volta.
- Informazioni su eventuali modifiche recenti apportate ai criteri (se applicabile).
- L'output del comando stats_unified.pl come descritto nella sezione Elaborazione degli eventi

con una menzione dei sensori interessati.

Analisi approfondita

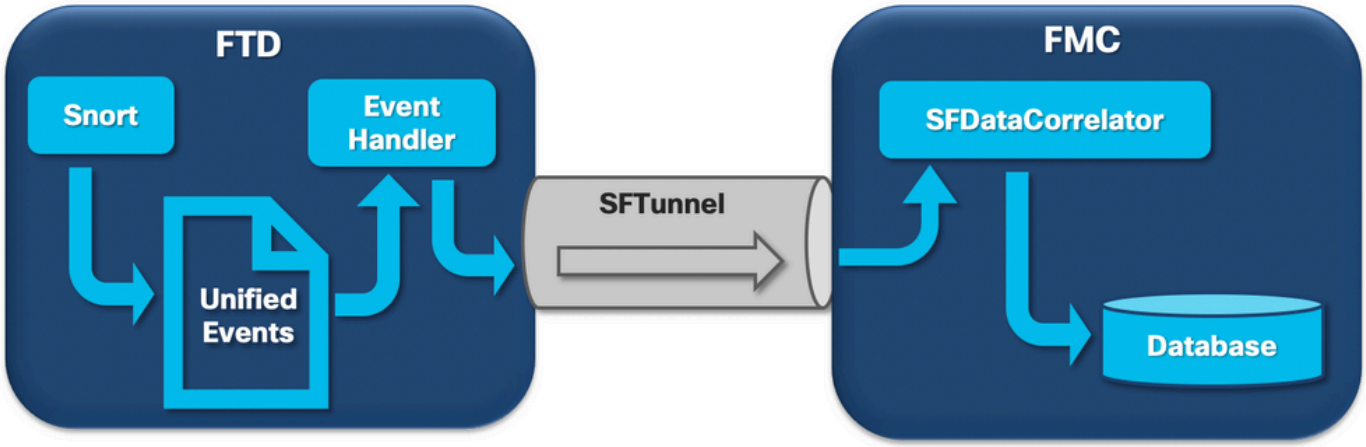
In questa sezione viene fornita una spiegazione dettagliata dei vari componenti che possono prendere parte a questo tipo di avvisi sullo stato di salute. Ciò include:

- Event Processing (Elaborazione eventi) - Copre il percorso degli eventi rilevati sia sui dispositivi sensore che sul FMC. Ciò è utile principalmente quando l'avviso di integrità fa riferimento a un silo di tipo evento.
- Disk Manager: descrive il processo di gestione dei dischi, gli archivi e il modo in cui vengono eliminati.
- Health Monitor - Illustra come i moduli di Health Monitor vengono utilizzati per generare avvisi di stato.
- Log to Ramdisk - Descrive la funzione di log su ramdisk e il suo impatto potenziale sugli avvisi relativi allo stato di salute.

Per comprendere gli avvisi di integrità relativi allo svuotamento degli eventi ed essere in grado di identificare i potenziali punti di errore, è necessario esaminare il funzionamento e l'interazione tra questi componenti.

Elaborazione degli eventi

Anche se il tipo di avviso sulla salute Frequent Drain può essere attivato da silos non correlati a eventi, la grande maggioranza dei casi rilevati da Cisco TAC è correlata allo svuotamento di informazioni relative a eventi. Inoltre, per comprendere che cosa costituisce un drenaggio di eventi non elaborati, è necessario esaminare l'architettura di elaborazione degli eventi e i componenti che la costituiscono.



Quando un sensore Firepower riceve un pacchetto da una nuova connessione, il processo snort genera un evento in formato unified2, che è un formato binario che consente letture/scritture più rapide ed eventi più leggeri.

L'output mostra la traccia di supporto del comando FTD dove è possibile vedere la creazione di

una nuova connessione. Le parti importanti sono evidenziate e spiegate:

<#root>

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

I file Snort unified_events vengono generati per istanza nel percorso [/ngfw]var/sf/detection_engine/*/instance-N/, dove:

- * è l'UUID dell'ugello. Questa caratteristica è unica per ogni accessorio.
- N è l'ID istanza Snort che può essere calcolato come ID istanza dall'output precedente (lo 0 evidenziato nell'esempio) + 1

In una cartella di istanze Snort possono essere presenti due tipi di file unified_events:

- unified_events-1 (che contiene eventi ad alta priorità).
- unified_events-2 (che contiene eventi a bassa priorità).

Un evento con priorità alta è un evento che corrisponde a una connessione potenzialmente dannosa.

Tipi di eventi e relativa priorità:

Priorità alta (1)	Priorità bassa (2)
Intrusione	Connessione
Malware	Individuazione
Security Intelligence	File
Eventi di connessione associati	Statistiche

Nell'output successivo viene mostrato un evento appartenente alla nuova connessione tracciata nell'esempio precedente. Il formato è unificato2 e viene ricavato dall'output del rispettivo registro eventi unificato situato in [/ngfw]/var/sf/detection_engine/*/instance-1/ dove 1 è l'ID istanza snort in grassetto nell'output precedente +1. Il nome del formato del registro eventi unificato utilizza la sintassi unified_events-2.log.1599654750, dove 2 indica la priorità degli eventi come mostrato nella tabella e l'ultima parte in grassetto (1599654750) è il timestamp (ora Unix) del momento in cui è stato creato il file.

Suggerimento: è possibile utilizzare il comando date di Linux per convertire l'ora di Unix in una data leggibile:
admin@FP1120-2:~$ data sudo -d@1599654750
mer 9 set 14:32:30 CEST 2020

<#root>

```
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
```

Accanto a ogni file unified_events è disponibile un file di segnalibri contenente due valori importanti:

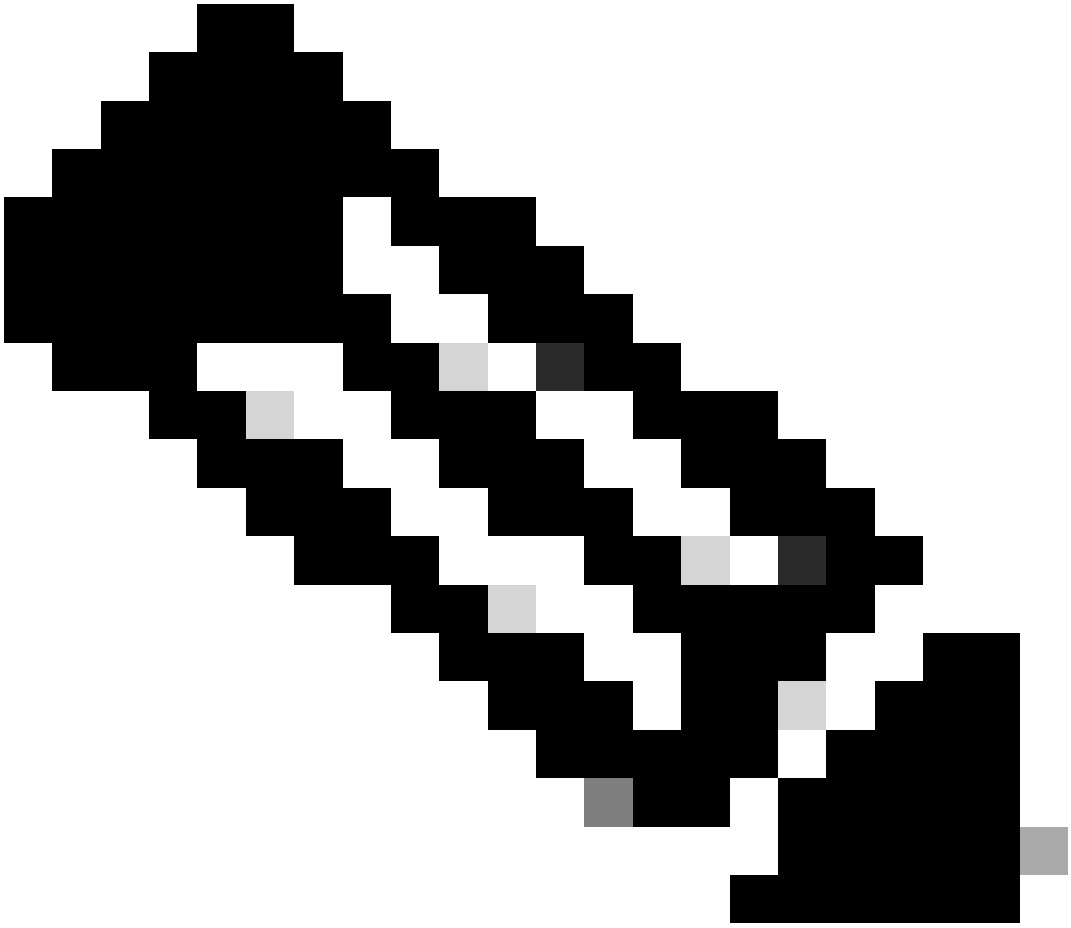
1. Timestamp corrispondente al file unified_events corrente per tale istanza e priorità.
2. Posizione in byte per l'ultimo evento di lettura nel file unified_event.

I valori sono ordinati e separati da una virgola, come mostrato nell'esempio:

<#root>

```
root@FTD:/home/admin#

cat /var/sf/detection_engines/d5a4d5d0-6ddf-11ea-b364-2ac815c16717/instance-1/unified_events-2.log.bookm


1599862498

,

18754115
```

In questo modo il processo di gestione dei dischi può sapere quali eventi sono già stati elaborati (inviati a FMC) e quali no.



Nota: quando Gestione disco svuota un silo di eventi, rimuove i file di eventi unificati.

Per ulteriori informazioni sullo svuotamento dei silos, consultare la sezione Disk Manager.

Un file unificato svuotato può avere eventi non elaborati quando si verifica una delle seguenti condizioni:

1. Il timestamp del segnalibro è inferiore all'ora di creazione del file.
2. Il timestamp del segnalibro corrisponde all'ora di creazione del file e la posizione in Byte nel file è inferiore alle dimensioni.

Il processo EventHandler legge gli eventi dai file unificati e li invia in streaming al FMC (come metadati) tramite sftunnel, che è il processo responsabile della comunicazione crittografata tra il sensore e il FMC. Si tratta di una connessione basata su TCP in modo che il flusso di eventi venga riconosciuto da FMC

È possibile visualizzare questi messaggi nel file [/ngfw]/var/log/messages:

<#root>

sfpreproc

:OutputFile [INFO] ***

Opening

/ngfw/var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.15

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.15978104

sftunneld

:FileUtils [INFO]

Processed 10334 events from log file

var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.159781047

Questo output fornisce le seguenti informazioni:

- Snort ha aperto il file unified_events per l'output (per scrivervi).
- Il gestore eventi ha aperto lo stesso file unified_events (per leggerlo).
- sftunnel ha riportato il numero di eventi elaborati dal file unified_events.

Il file del segnalibro viene quindi aggiornato di conseguenza. Il sftunnel utilizza due diversi canali denominati Unified Events (UE), rispettivamente il canale 0 e il canale 1 per gli eventi ad alta e bassa priorità.

Con il comando sfunnel_status CLI sull'FTD, è possibile visualizzare il numero di eventi trasmessi.

<#root>

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

Nell'FMC, gli eventi sono ricevuti dal processo SFDataCorrelator.

Lo stato degli eventi elaborati da ciascun sensore può essere visualizzato con il comando stats_unified.pl:

<#root>

```
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
```

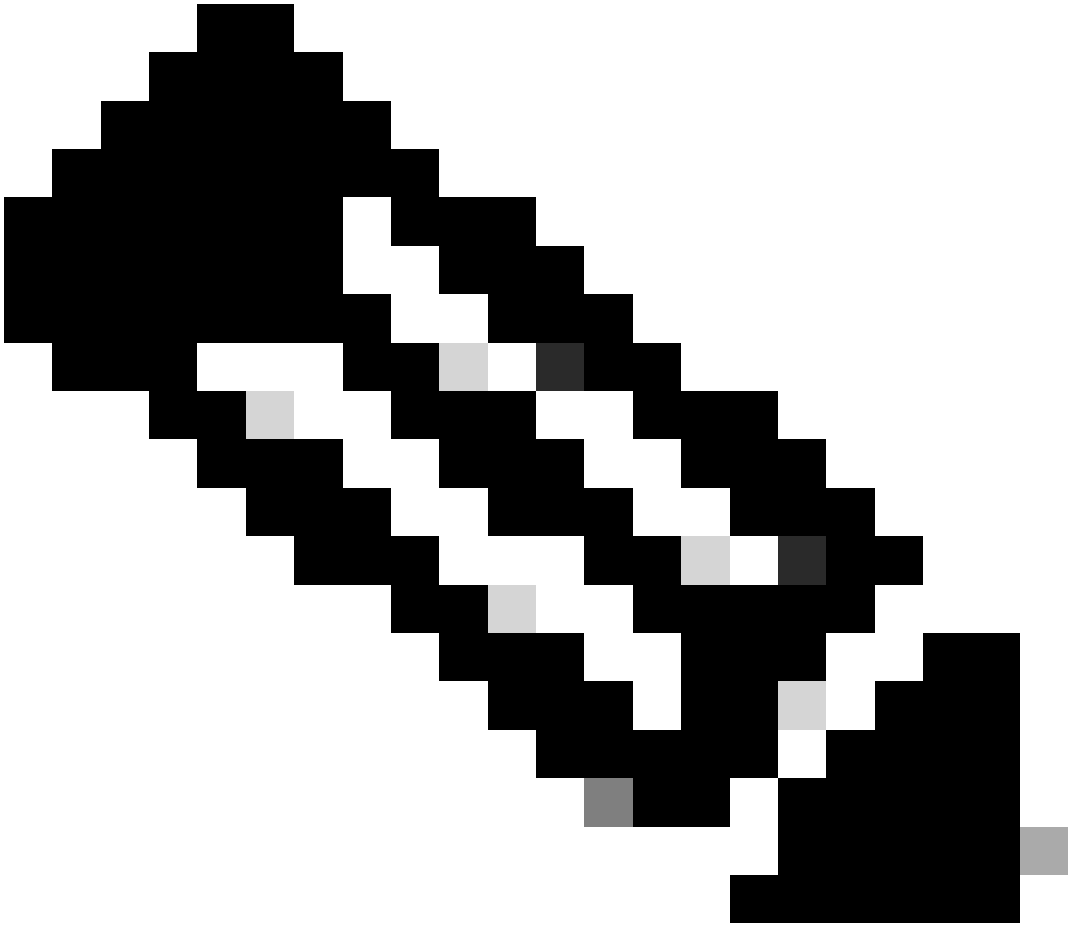
Con questo comando viene mostrato lo stato del backlog di eventi per un determinato dispositivo per canale. L'ID di canale utilizzato è lo stesso di sftunnel.

Il valore Byte dietro può essere calcolato come la differenza tra la posizione mostrata nel file dei segnalibri degli eventi unificati e la dimensione del file degli eventi unificati, più qualsiasi file successivo con un timestamp superiore a quello del file dei segnalibri.

Il processo SFDataCorrelator memorizza anche le statistiche sulle prestazioni, che vengono salvate in /var/sf/rna/correlator-stats/. Viene creato un file al giorno per memorizzare le statistiche delle prestazioni per quel giorno in formato CSV. Il nome del file utilizza il formato AAAA-MM-GG e il file corrispondente al giorno corrente viene chiamato adesso.

Le statistiche vengono raccolte ogni 5 minuti (c'è una riga per ogni intervallo di 5 minuti).

L'output di questo file può essere letto con il comando perfstats.



Nota: questo comando viene utilizzato anche per leggere i file delle statistiche sulle prestazioni degli snort, pertanto è necessario utilizzare i flag appropriati:

-C: Indica a perfstats che l'input è un file correlator-stats (senza questo flag, perfstats presuppone che l'input sia un file di statistiche delle prestazioni snort).

-q: Modalità non interattiva, stampa solo il riepilogo per il file.

<#root>

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

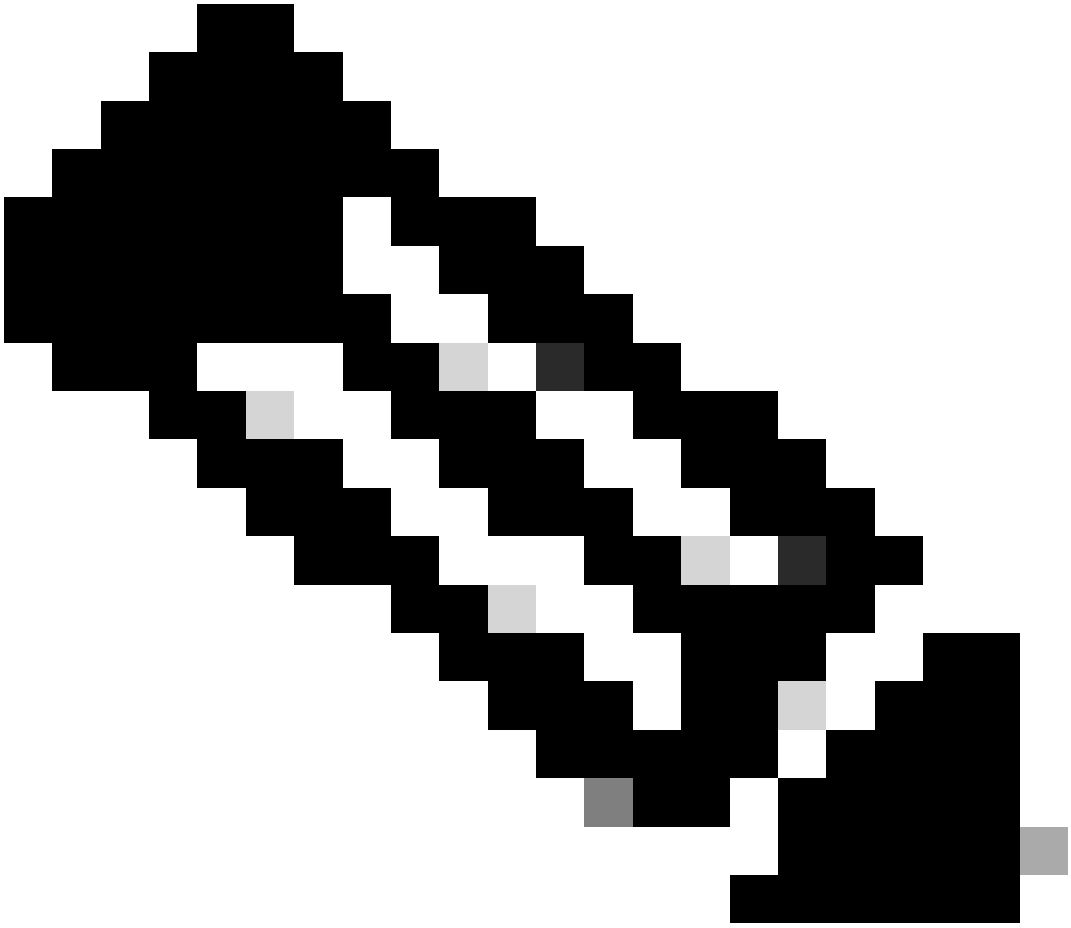
:

0.00 0.00 0.06

fireamp events/second:	0.00	0.00	0.00

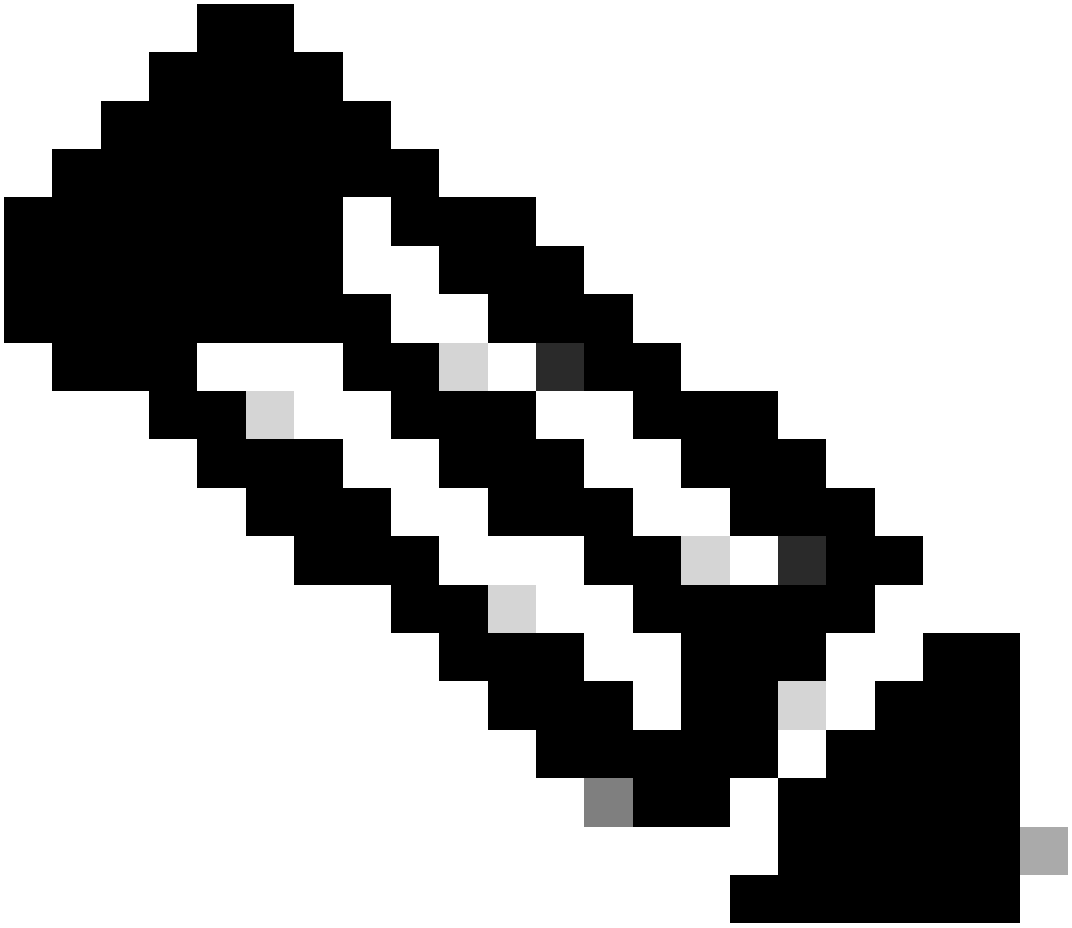
Ogni riga del riepilogo contiene 3 valori nell'ordine seguente: Media, Minimo, Massimo.

Se si stampa senza il flag -q, verranno visualizzati anche i valori di intervallo di 5 minuti. Il riepilogo viene visualizzato alla fine.



Nota: ogni CCP ha una portata massima descritta nel proprio foglio dati. La tabella seguente contiene i valori per modulo ricavati dal rispettivo foglio dati.

Modello	FMC 750	FMC 1000	FMC 1600	CCP 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMCv300
Massima portata (fps)	2000	5000	5000	12000	12000	12000	20000	20000	20000	Variabile	12000



Nota: questi valori si riferiscono all'aggregazione di tutti i tipi di evento visualizzati in grassetto nell'output delle statistiche SFDataCorrelator.

Se si esamina l'output e si dimensiona il CCP in modo da essere preparati per lo scenario peggiore (quando tutti i valori massimi si verificano contemporaneamente), il tasso di eventi rilevato da questo CCP è 48,65 + 348,15 + 4,63 + 3,25 + 0,06 = 404,74 fps.

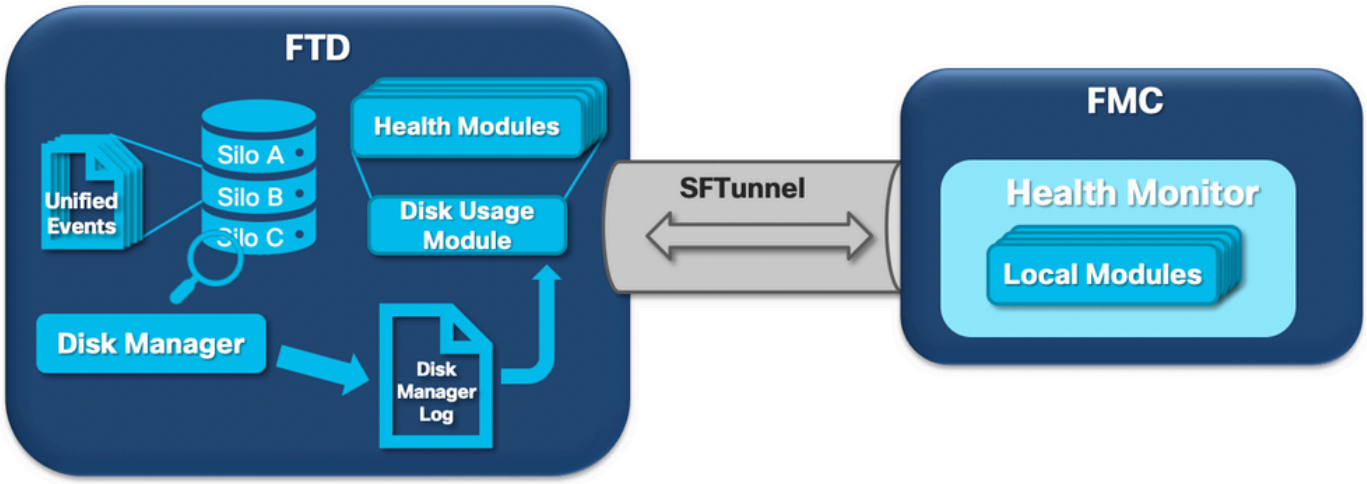
Questo valore totale può essere confrontato con il valore del foglio dati del rispettivo modello.

SFDataCorrelator consente inoltre di eseguire ulteriori operazioni sugli eventi ricevuti, ad esempio le regole di correlazione, e di memorizzarli nel database in cui viene eseguita la query per popolare varie informazioni nell'interfaccia utente grafica (GUI) di FMC, ad esempio dashboard e visualizzazioni eventi.

Gestione dischi

Nel diagramma logico successivo vengono illustrati i componenti logici per entrambi i processi

Health Monitor e Gestione disco, interconnessi per la generazione di avvisi di integrità relativi al disco.



In breve, il processo di gestione dei dischi gestisce l'utilizzo del disco della scatola e ha i suoi file di configurazione nella cartella [/ngfw]/etc/sf/. Esistono più file di configurazione per il processo di gestione dischi che vengono utilizzati in determinate circostanze:

- diskmanager.conf - File di configurazione standard.
- diskmanager_2hd.conf - Utilizzato quando nella confezione sono installati 2 dischi rigidi. Il secondo disco rigido è quello correlato all'espansione malware utilizzato per archiviare i file come definito nel criterio file.
- ramdisk-diskmanager.conf - Utilizzato quando Log to Ramdisk è abilitato. Per ulteriori informazioni, consultare la sezione Log to Ramdisk.

A ogni tipo di file monitorato da Gestione disco viene assegnato un Silo. In base alla quantità di spazio disponibile sul sistema, il gestore del disco calcola un High Water Mark (HWM) e un Low Water Mark (LWM) per ciascun silo.

Quando il processo di gestione dei dischi scarica un silo, lo fa fino al punto in cui viene raggiunto LWM. Poiché gli eventi vengono svuotati per file, questa soglia può essere superata.

Per controllare lo stato degli archivi su un dispositivo sensore, è possibile utilizzare questo comando:

<#root>

>

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
```

Il processo di Gestione dischi viene eseguito quando si verifica una delle seguenti condizioni:

- Il processo viene avviato o riavviato
- Un silo raggiunge l'HWM
- Un silo viene svuotato manualmente
- Una volta all'ora

Ogni volta che il processo di gestione dei dischi viene eseguito, genera una voce per ciascuno dei diversi archivi nel proprio file di registro, che si trova in [/ngfw]/var/log/diskmanager.log e contiene dati in formato CSV.

Viene quindi visualizzata una riga di esempio del file diskmanager.log. È stato preso da un sensore che ha attivato lo svuotamento di eventi non elaborati dall'avviso di integrità degli eventi a bassa priorità unificati, nonché la suddivisione delle rispettive colonne:

```
priority_2_events,1599668981,221,4587929508,1132501868,20972020,4596,1586044534,5710966962,1142193392,1
```

Colonna	Valore
Etichetta silo	priority_2_events
Tempo di scarico (tempo di esposizione)	1599668981
Numero di file eliminati	221
Byte eliminati	4587929508
Dimensioni correnti dei dati dopo lo svuotamento (byte)	1132501868
File di dimensioni maggiori svuotato (byte)	20972020
File più piccolo svuotato (byte)	4596
Il file meno recente è stato prosciugato (tempo di attesa)	1586044534
Limite massimo (byte)	5710966962

Limite minimo (byte)	1142193392
Numero di file con eventi non elaborati eliminati	110
Flag di stato di Diskmanager	0

Queste informazioni vengono quindi lette dal rispettivo modulo Health Monitor per attivare l'avviso di integrità correlato.

Svuotamento manuale di un silo

In alcuni scenari, è possibile svuotare manualmente un silo. Ad esempio, per liberare spazio su disco con l'eliminazione manuale dei silo anziché con la rimozione manuale dei file, il gestore del disco può decidere quali file conservare e quali eliminare. Gestione disco conserva i file più recenti per quel silo.

Qualsiasi silo può essere svuotato e funziona come già descritto (il gestore del disco svuota i dati fino a quando la quantità di dati non rientra nella soglia LWM). Il comando system support silo-drain è disponibile in modalità FTD CLISH e fornisce un elenco dei silos disponibili (nome + ID numerico).

Questo è un esempio di svuotamento manuale del silo Unified Low Priority Events:

<#root>

>

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
```

Health Monitor

Questi sono i punti principali:

- Qualsiasi avviso relativo allo stato di salute visualizzato sul CCP nel menu Health Monitor o nella scheda Stato del centro messaggi viene generato dal processo Health Monitor.
- Questo processo controlla lo stato del sistema, sia per il FMC che per i sensori gestiti, ed è

composto da diversi moduli.
- I moduli di avviso di integrità sono definiti nei criteri di integrità che possono essere collegati a ciascun dispositivo.
- Gli avvisi sull'integrità vengono generati dal modulo Utilizzo disco che può essere eseguito su ogni sensore gestito dal FMC.
- Quando il processo Health Monitor sul FMC è in esecuzione (una volta ogni 5 minuti o quando viene attivata un'esecuzione manuale), il modulo Disk Usage esamina il file diskmanager.log e, se vengono soddisfatte le condizioni corrette, viene attivato il relativo avviso di stato.

Affinché venga attivato un avviso di integrità Eventi non elaborati Tutte le condizioni seguenti devono essere vere:

1. Il campo Byte svuotati è maggiore di 0 (ciò indica che i dati di questo silo sono stati svuotati).
2. Il numero di file con eventi non elaborati eliminati è maggiore di 0 (ciò indica che erano presenti eventi non elaborati all'interno dei dati eliminati).
3. Il tempo di scarico è nell'ultima ora.

Affinché venga attivato un avviso di integrità relativo a uno svuotamento frequente di eventi, è necessario che le condizioni seguenti siano vere:

1. Le ultime due voci del file diskmanager.log devono:
    - Il campo Byte svuotati è maggiore di 0 (ciò indica che i dati di questo silo sono stati svuotati).
    - Distanza inferiore a 5 minuti.
2. L'ora di svuotamento dell'ultima voce di questo silo è compresa nell'ultima ora.

I risultati ottenuti dal modulo di utilizzo del disco (nonché i risultati raccolti dagli altri moduli) vengono inviati al FMC tramite sftunnel. È possibile visualizzare i contatori degli eventi sanitari scambiati tramite sftunnel con il comando sftunnel_status:

<#root>

```
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
```

Registra su disco RAM

Anche se la maggior parte degli eventi è memorizzata su disco, per impostazione predefinita il

dispositivo è configurato in modo da eseguire il log su ramdisk per impedire danni graduali all'unità SSD che possono essere causati da scritture e eliminazioni costanti di eventi su disco.

In questo scenario, gli eventi non vengono memorizzati in [/ngfw]/var/sf/detection_engine/*/instance-N/, ma si trovano in [/ngfw]/var/sf/detection_engine/*/instance-N/connection/, che è un collegamento simbolico a /dev/shm/instance-N/connection. In questo caso, gli eventi risiedono nella memoria virtuale anziché in quella fisica.

```
<#root>

admin@FTD4140:~$

ls -la /ngfw/var/sf/detection_engines/b0c4a5a4-de25-11ea-8ec3-4df4ea7207e3/instance-1/connection


l

rwxrwxrwx 1 sfsnort sfsnort 30 Sep  9 19:03 /ngfw/var/sf/detection_engines/b0c4a5a4-de25-11ea-8ec3-4df4

-> /dev/shm/instance-1/connection
```

Per verificare la configurazione corrente del dispositivo, eseguire il comando show log-events-to-ramdisk dalla schermata FTD CLISH. È possibile modificare questa impostazione anche utilizzando il comando configure log-events-to-ramdisk <enable/disable>:

```
<#root>

>

show log-events-to-ramdisk


Logging connection events to RAM Disk.

>

configure log-events-to-ramdisk


Enable or Disable  enable or disable (enable/disable)
```

Avviso: quando si esegue il comando configure log-events-to-ramdisk disable, è necessario che vengano eseguite due distribuzioni sull'FTD per evitare di rimanere bloccati in uno stato D (sospensione ininterrompibile), che provocherebbe un'interruzione del traffico. Questo comportamento è documentato nel difetto con l'ID bug Cisco CSCvz53372. Con la prima distribuzione, la rivalutazione dello stadio della memoria snort viene saltata, il che fa sì che lo snort entri nello stato D. Per ovviare al problema, è necessario eseguire un'altra distribuzione con eventuali modifiche fittizie.

Quando si accede a ramdisk, lo svantaggio principale è che il rispettivo silo ha uno spazio allocato più piccolo e quindi li scarica più spesso nelle stesse circostanze. L'output successivo è lo strumento di gestione dei dischi di un FPR 4140 con e senza gli eventi di registro su ramdisk abilitato per il confronto.

Accesso a Ramdisk abilitato.

<#root>

>

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

Accesso a Ramdisk disabilitato.

<#root>

>

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

Le dimensioni ridotte del silo sono compensate dalla velocità più elevata di accesso agli eventi e di trasmissione degli stessi al FMC. Benché si tratti di un'opzione migliore in condizioni adeguate, si deve prendere in considerazione il rimborso.

Domande frequenti (FAQ)

Gli avvisi di integrità relativi allo svuotamento degli eventi vengono generati solo dagli eventi di connessione?

No.

- Gli allarmi relativi allo svuotamento frequente possono essere generati da qualsiasi silo di gestione dei dischi.
- Gli avvisi di svuotamento degli eventi non elaborati possono essere generati da qualsiasi silo correlato agli eventi.

I motivi più comuni sono gli eventi di connessione.

È sempre consigliabile disabilitare Log to Ramdisk quando viene visualizzato un avviso relativo allo stato di salute della fuoriuscita frequente?

No. Solo in scenari di registrazione eccessivi ad eccezione di DOS/DDOS, quando il silo interessato è il silo degli eventi di connessione e solo nei casi in cui non è possibile ottimizzare ulteriormente le impostazioni di registrazione.

Se DOS/DDOS provoca una registrazione eccessiva, la soluzione è implementare la protezione DOS/DDOS o eliminare le origini degli attacchi DOS/DDOS.

La funzione predefinita Log to Ramdisk riduce l'usura dell'SSD, pertanto si consiglia vivamente di utilizzarla.

Che cosa costituisce un evento non elaborato?

Gli eventi non vengono contrassegnati singolarmente come non elaborati. Un file presenta eventi non elaborati quando:

Il timestamp di creazione è maggiore del campo timestamp nel file del segnalibro corrispondente.

o

Il timestamp di creazione è uguale al campo timestamp nel file del segnalibro corrispondente e la sua dimensione è superiore alla posizione nel campo Byte del file del segnalibro corrispondente.

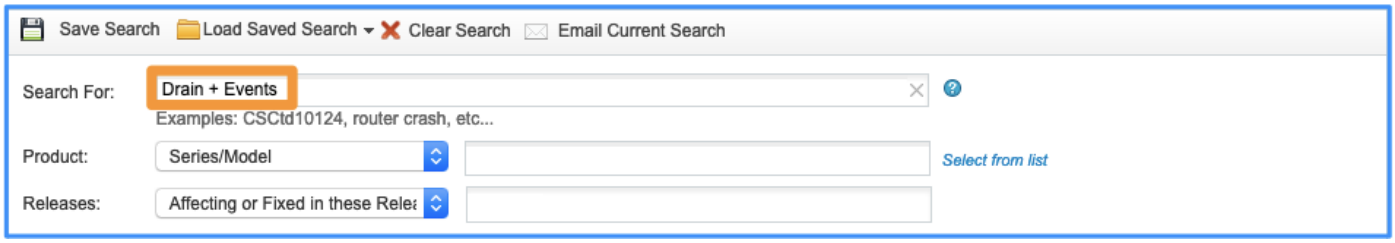
Come fa il CCP a conoscere il numero di byte arretrati per un determinato sensore?

Il sensore invia metadati relativi al nome e alle dimensioni del file unified_events, nonché informazioni sui file dei segnalibri che forniscono al FMC informazioni sufficienti per calcolare i byte arretrati come:

Dimensione file unified_events corrente: posizione nel campo Byte dal file dei segnalibri + Dimensione di tutti i file unified_events con un timestamp superiore a quello nel file dei segnalibri corrispondente.

Problemi noti

Aprire Bug Search Tool e usare la seguente query:



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).