Probleemoplossing Afvoer van onverwerkte gebeurtenissen en frequente afvoer van gebeurtenissen Waarschuwingen voor gezondheidsmonitor

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen bij **Afvoer van onverwerkte gebeurtenissen** en **Frequent Drain of Events -** gezondheidswaarschuwingen op Firepower Management Center (FMC).

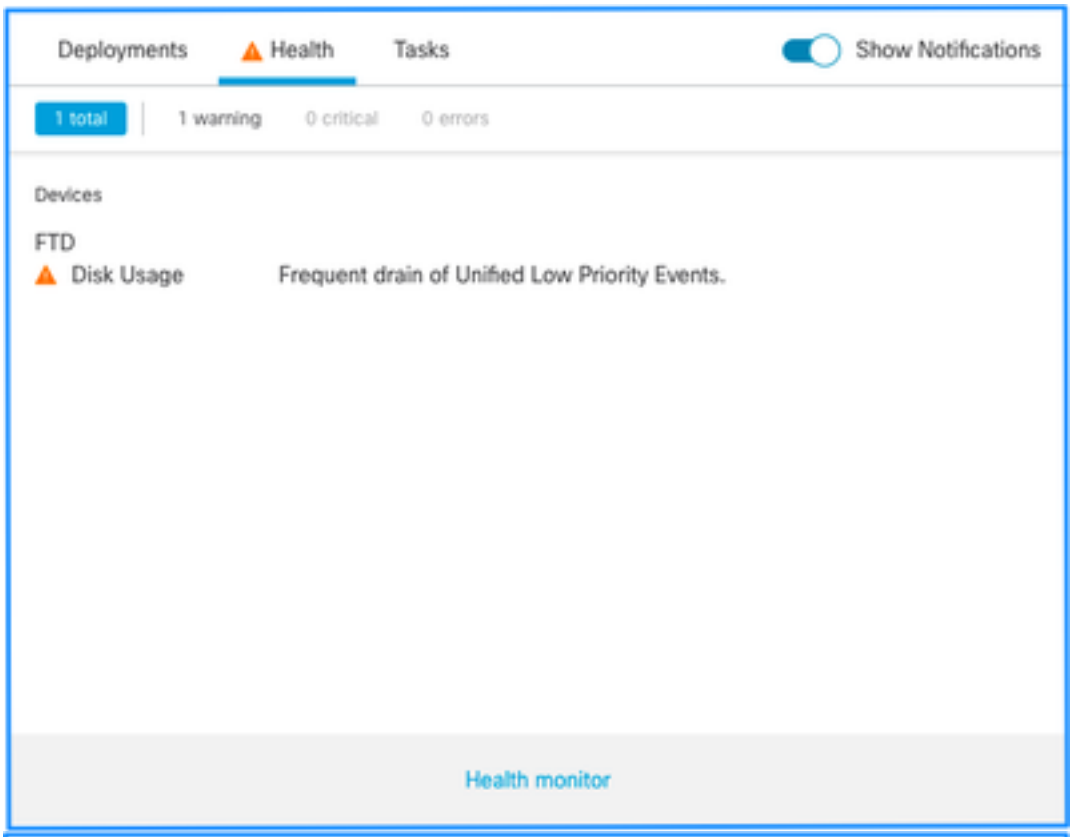
Probleemoverzicht

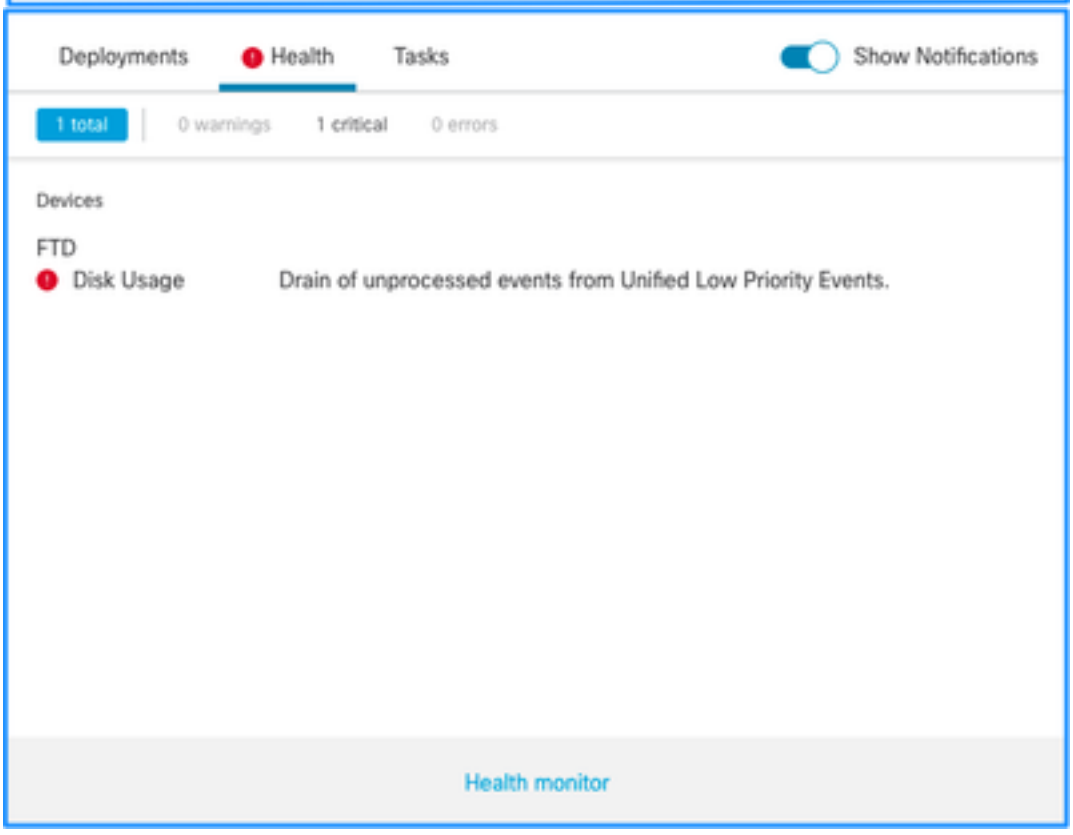
Het VCC genereert een van deze gezondheidswaarschuwingen:

- Frequente afvoer van Unified Low Priority Events
  en/of
- Afvoer van onverwerkte gebeurtenissen van Unified Low Priority Events

Hoewel deze gebeurtenissen worden gegenereerd en getoond op het VCC, hebben ze betrekking op een geleide apparatensensor of het nu gaat om een Firepower Threat Defence (FTD) of een Next-generation inbraakpreventiesysteem (NGIPS). Voor de rest van dit document verwijst de

term sensor naar zowel FTD- als NGIPS-apparaten, tenzij anders vermeld.





Dit is de alarmstructuur voor de gezondheid:

- Frequente afvoer van <SILO NAME>
- Afvoer van onverwerkte gebeurtenissen van <SILO NAME>

In dit voorbeeld is de SILO NAME **Unified Low Priority Events**. Dit is een van de silo's van de diskbeheerder (zie het gedeelte Achtergrondinformatie voor een uitgebreidere uitleg).

Daarnaast:

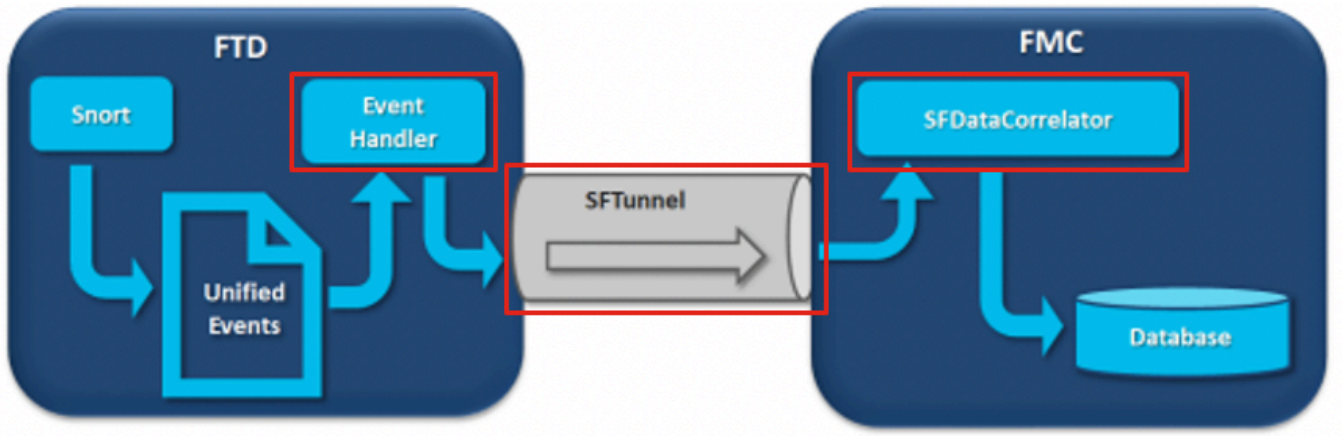
- Hoewel elke silo technisch gezien een Frequent afvoersignaal van de gezondheidswaarschuwing van <SILO NAME> kan genereren, zijn de meest geziene degene die gerelateerd zijn aan gebeurtenissen en, onder hen, de Low Priority Events gewoon omdat dit het type gebeurtenissen zijn die vaker door de sensoren worden gegenereerd.
- Een "Frequent drain of <SILO NAME>" gebeurtenis heeft een Waarschuwing ernst in het geval dat het een gebeurtenis-gerelateerde silo is, omdat, als dit werd verwerkt (hierna wordt uitgelegd wat een onverwerkte gebeurtenis is), ze in de FMC-database staan.
- Voor een niet-gebeurtenisgerelateerde silo, zoals de "Back-ups" silo, is de Waarschuwing kritisch omdat deze informatie verloren gaat.
- Alleen silo's van het type gebeurtenis genereren een afvoer van onverwerkte gebeurtenissen uit de gezondheidswaarschuwing van <SILO NAME>. Deze waarschuwing heeft altijd Kritische strengheid.

Extra symptomen kunnen zijn:

- Laagheid op de FMC UI
- Verlies van gebeurtenissen

Gemeenschappelijke probleemoplossingsscenario's

Een frequente afvoer van de gebeurtenis <SILO NAME> wordt veroorzaakt door te veel invoer in de silo voor de grootte ervan. In dit geval laat de diskbeheerder de gegevens ten minste tweemaal weglopen in het laatste 5 minuten-interval. In een silo van het gebeurtenistype, wordt dit typisch veroorzaakt door bovenmatige vastlegging van dat gebeurtenistype. In het geval van een afvoer van onverwerkte gebeurtenissen met een gezondheidswaarschuwing van <SILO NAME> kan dit ook worden veroorzaakt door een knelpunt in het gebeurtenisverwerkingstraject.



In het diagram zijn er 3 mogelijke knelpunten:

- Het EventHandler proces op FTD is oversubscribed (het leest langzamer dan wat Snort schrijft)
- De interface Event is oversubscribed
- Het SFDataCorrelator-proces op het VCC is overtekend

Om de architectuur van Event Processing dieper te begrijpen, raadpleegt u de betreffende sectie

Deep Dive.

Zaak 1: Buitensporige houtkap

Zoals in de vorige paragraaf is aangegeven, is een van de meest voorkomende oorzaken van de gezondheidswaarschuwingen van dit type excessieve input.

Het verschil tussen de LWM (Low Water Mark) en de High Water Mark (HWM), verzameld uit de opdracht **show disk-manager** CLISH, laat zien hoeveel ruimte er nodig is om op die silo te gaan van LWM (vers gedraineerd) naar de HWM-waarde. Als er vaak afvoer van gebeurtenissen (met of zonder onverwerkte gebeurtenissen) is het eerste wat je moet bekijken de logboekconfiguratie.

Raadpleeg voor een uitgebreide uitleg van het Disk Manager-proces het betreffende gedeelte Deep Dive.

Of het nu gaat om dubbele vastlegging of alleen een hoog aantal gebeurtenissen op het gehele ecosysteem van de manager-sensoren moet een overzicht van de loginstellingen worden uitgevoerd.

Aanbevolen acties

Stap 1. Controleer op dubbele vastlegging

Dubbele registratiescenario's kunnen worden geïdentificeerd als u kijkt naar de correlator **presteert** op het VCC zoals getoond in deze output:

```
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 dit geval kan een hoog percentage gedupliceerde stromen in de output worden gezien.

Stap 2. Herzie de logboekinstellingen van de ACS

U moet beginnen met een beoordeling van de loginstellingen van het toegangscontrolebeleid (ACS). Zorg ervoor dat u de beste praktijken volgt die in dit document worden beschreven Best Practices for Connection Logging

Een beoordeling van de logboekinstellingen is raadzaam in alle situaties, aangezien de genoemde aanbevelingen niet alleen betrekking hebben op dubbele logboekscenario's.

Stap 3. Controleer of de buitensporige vastlegging al dan niet wordt verwacht

Je moet bekijken of de excessieve vastlegging een verwachte oorzaak heeft of niet. Als de buitensporige vastlegging wordt veroorzaakt door DOS/DDoS-aanval of routinglus of een specifieke toepassing/host die een groot aantal verbindingen maakt, moet u verbindingen uit de onverwachte buitensporige verbindingsbronnen controleren en beperken/stoppen.

Stap 4. Upgrademodel

Upgrade FTD hardwareapparaat naar een beter prestatiemodel (bijvoorbeeld FPR2100 —> FPR4100), de bron van silo zou toenemen.

Stap 5. Overweeg of u Log in Ramdisk kunt uitschakelen

In het geval van de Unified Low Priority Events silo kunt u Log to Ramdisk uitschakelen om de silo-grootte te vergroten met de nadelen die in de betreffende Deep Dive-sectie worden besproken.

Zaak 2: Knelpunt in het communicatiekanaal tussen de sensor en het VCC

Een andere veel voorkomende oorzaak van dit soort waarschuwing zijn connectiviteitsproblemen en/of instabiliteit in het communicatiekanaal (sftunnel) tussen de sensor en het VCC. De communicatie kwestie kan worden veroorzaakt door:

- sftunnel is down of is instabiel (flaps).
- sftunnel is oversubscribed.

Voor de kwestie van de sftunnelconnectiviteit zorg ervoor dat het VCC en de sensor bereikbaarheid tussen hun beheersinterfaces op TCP-poort 8305 hebben.

Op FTD kunt u zoeken naar een **sftunnelstring** in het bestand **[/ngfw]/var/log/message**. Problemen met de connectiviteit zorgen ervoor dat dergelijke berichten worden gegenereerd:

```
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
```

Overinschrijving op de beheerinterface van VCC's kan een piek in het beheerverkeer of een constante overinschrijving betekenen. Historische gegevens van de gezondheidsmonitor zijn hier een goede indicator van.

Het eerste wat opvalt is dat in de meeste gevallen het VCC wordt ingezet met één NIC voor beheer. Deze interface wordt gebruikt voor:

- beheer van het VCC.
- FMC-sensorbeheer.
- VCC-eventverzameling uit de sensoren.
- Update van inlichtingenfeeds.
- De download van SRU, Software, VDB en GeoDB updates van de Software Download Site.
- De query voor URL-reputaties en -categorieën (indien van toepassing).
- De query voor bestandsdisponeringen (indien van toepassing).

Aanbevolen acties

U kunt een tweede NIC op het VCC implementeren voor een speciale interface voor gebeurtenissen. De implementatie kan afhankelijk zijn van het gebruik.

Algemene richtlijnen zijn te vinden in de FMC Hardware Guide implementeren op een beheernetwerk

Zaak 3: Knelpunt in het SFDataCorrelator-proces

Het laatste scenario dat moet worden behandeld, is wanneer het knelpunt zich voordoet aan de kant van de SFDataCorrelator (FMC).

De eerste stap is om te kijken in het diskmanager.log bestand als er belangrijke informatie te verzamelen is zoals:

- De frequentie van de afvoer.
- Het aantal bestanden met onverwerkte gebeurtenissen is weggelopen.
- Het optreden van de afvoer met onverwerkte gebeurtenissen.

Raadpleeg het gedeelte Disk Manager voor meer informatie over het bestand diskmanager.log en hoe u het kunt interpreteren. De informatie die wordt verzameld via diskmanager.log kan worden gebruikt om de volgende stappen te versmallen.

Daarnaast dient u de prestatiestatistieken van de correlator te bekijken:

```
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
```

Opgemerkt zij dat deze statistieken betrekking hebben op het VCC en overeenstemmen met het totaal van alle door het VCC beheerde sensoren. In het geval van Unified lage prioriteit evenementen zoekt u vooral:

- Totale stromen per seconde van elk type gebeurtenis om mogelijke overinschrijving op het SFDataCorrelator-proces te evalueren.
- De twee rijen die in de vorige uitvoer zijn gemarkeerd: **rna-stromen/seconde** - Geeft het aantal gebeurtenissen met een lage prioriteit aan dat door de SFDataCorrelator is verwerkt.**rna dup flows/seconde** - Geeft het aantal gedupliceerde lage prioriteit gebeurtenissen aan dat door de SFDataCorrelator is verwerkt. Dit wordt gegenereerd door dubbel vastleggen zoals besproken in het vorige scenario.

Op basis van de output kan worden geconcludeerd dat:

- Er is geen dubbele vastlegging zoals aangegeven door de rna dup flows/tweede rij.
- In de rna-stromen/tweede rij is de maximumwaarde veel hoger dan de gemiddelde waarde, zodat er een piek in de snelheid van gebeurtenissen door het SFDataCorrelator-proces verwerkt was. Dit kan worden verwacht als u kijkt naar deze vroege ochtend, toen uw gebruikers werkdag net is begonnen, maar over het algemeen is het een rode vlag en vereist verder onderzoek.

Meer informatie over het SFDataCorrelator-proces vindt u onder de sectie Event Processing.

Aanbevolen acties

Eerst moet u bepalen wanneer de piek is opgetreden. Om dit te doen moet u kijken naar de correlator statistieken per 5-minuten steekproefinterval. De informatie die wordt verzameld via diskmanager.log kan u helpen om direct naar het belangrijke tijdsbestek te gaan.

> **Tip**: Pijp de uitvoer **minder** naar de Linux pager zodat u gemakkelijk kunt zoeken.

```
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
```

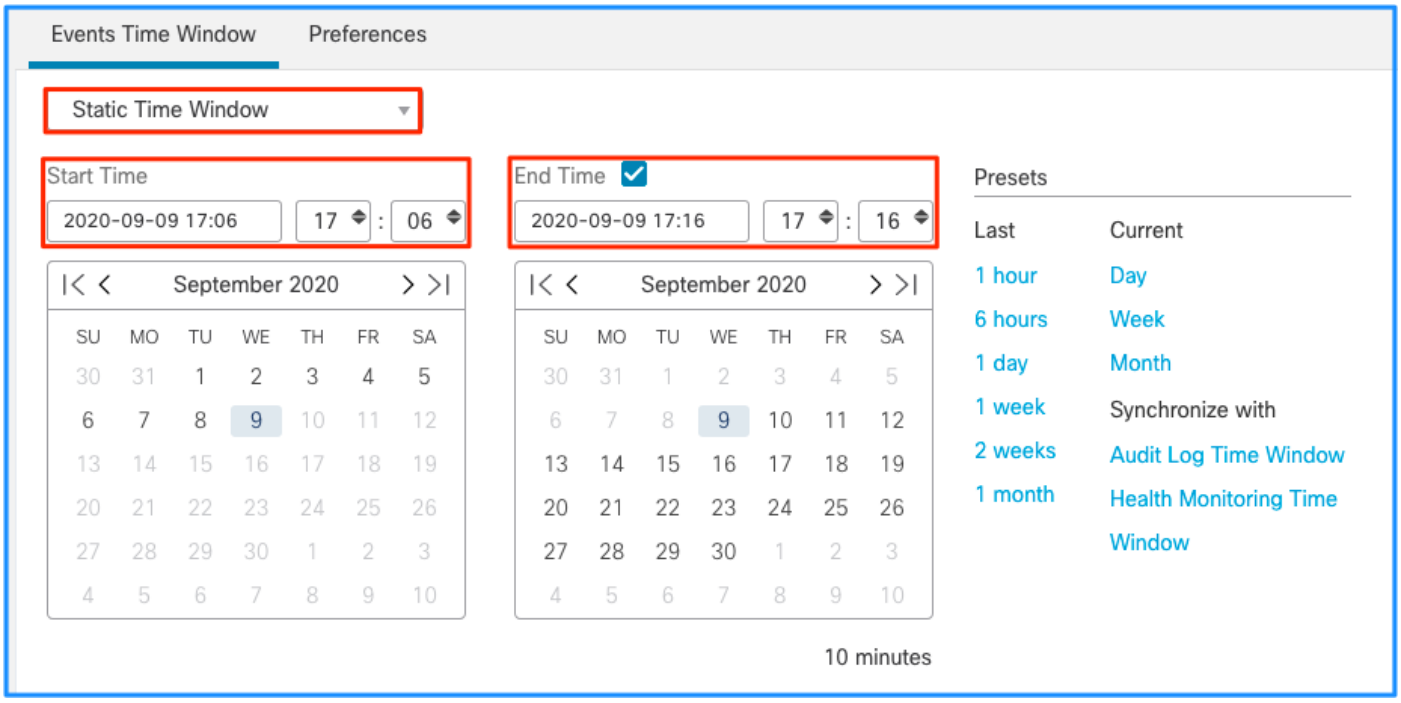
```
                ids alerts/second:              0.00
                ids pkts/second:                0.00
                ids comm records/second:        0.01
                ids extras/second:              0.00
                fw stats/second:                0.03
                user logins/second:             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
```

Gebruik de informatie in het uitvoerdocument om:

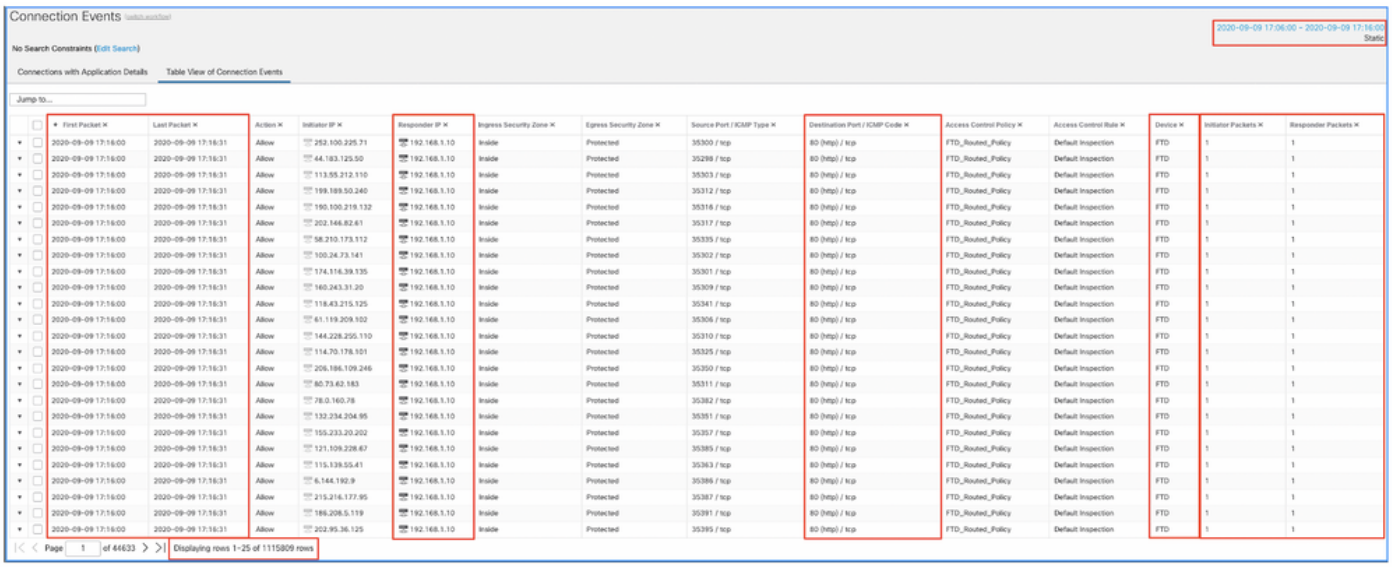
- Bepaal het normale/baseline aantal gebeurtenissen.
- Bepaal het interval van 5 minuten wanneer de pin is opgetreden.

In het vorige voorbeeld is er een duidelijke piek in het aantal gebeurtenissen dat wordt ontvangen op 16:06:39 en daarna. Merk op dat dit 5-minuten gemiddelden zijn zodat de toename abrupter kan zijn dan getoond (barst) maar verdund in deze 5-minuten interval als het begon tegen het einde van het.

Hoewel dit leidt tot de conclusie dat deze piek van gebeurtenissen de afvoer van onverwerkte gebeurtenissen veroorzaakt, kunt u een blik op de verbindingsgebeurtenissen van de grafische gebruikersinterface van het VCC (GUI) met het aangewezen tijdvenster nemen om te begrijpen welk type verbindingen de FTD-doos in deze piek overstaken:



Pas dit tijdvenster toe om de gefilterde verbinding gebeurtenissen, vergeet niet om rekening te houden met de tijdzone. In dit voorbeeld gebruikt de sensor UTC en het VCC UTC+1. Gebruik de Tabelweergave om de gebeurtenissen te zien die tot de overbelasting van gebeurtenissen hebben geleid en onderneem dienovereenkomstig actie:



Op basis van de tijdstempels (tijd van het eerste en laatste pakket) kan worden gezien dat dit kortstondige verbindingen zijn. Bovendien tonen de kolommen Initiator- en Responder-pakketten aan dat er slechts 1 pakket is uitgewisseld in elke richting. Dit bevestigt dat de verbindingen van korte duur waren en zeer weinig gegevens uitwisselden.

Je kunt ook zien dat al deze stromen zich richten op dezelfde responder IP's en poort. Ook worden ze allemaal gerapporteerd door dezelfde sensor (die naast Ingress en Egress interface informatie kan spreken over de plaats en richting van deze stromen). Aanvullende acties:

- Controleer Syslogs op het eindpunt van de bestemming.
- Voer DOS/DDOS-bescherming uit of neem andere preventieve maatregelen.

Opmerking: De bedoeling van dit artikel is om richtlijnen te geven voor probleemoplossing in de waarschuwing 'Leegpompen van onverwerkte gebeurtenissen'. Dit voorbeeld gebruikte

hping3 om een TCP SYN-overstroming naar de doelserver te genereren. Raadpleeg de Cisco Firepower Threat Defence Hardening Guide voor richtlijnen voor het harden van uw FTD-apparaat

Te verzamelen items voordat u contact opneemt met het Cisco Technical Assistance Center (TAC)

Het is sterk aanbevolen om deze items te verzamelen voordat u contact opneemt met Cisco TAC:

- Screenshot van de gesignaleerde gezondheidswaarschuwingen.
- Probleemoplossing voor bestanden die door het VCC zijn gegenereerd.
- Probleemoplossing voor bestanden die door de betreffende sensor zijn gegenereerd.
- Datum en tijd waarop het probleem voor het eerst is gezien.
- Informatie over recente wijzigingen van het beleid (indien van toepassing).
- De output van de opdracht stats_unified.pl zoals beschreven in de sectie Event Processing met een vermelding van de getroffen sensoren.

Diepduiken

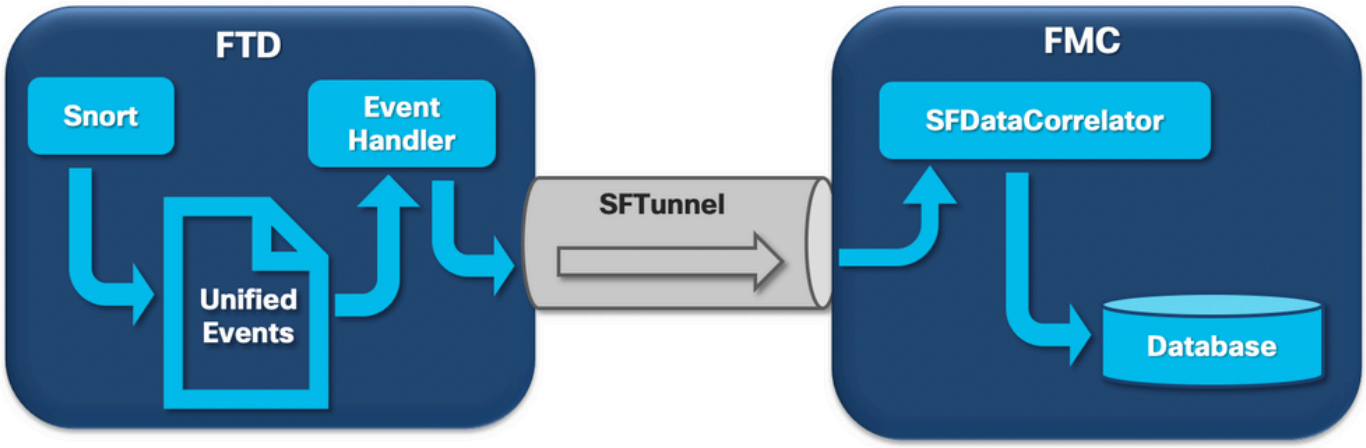
In dit deel wordt een uitvoerige toelichting gegeven op de verschillende onderdelen die aan dit soort gezondheidswaarschuwingen kunnen deelnemen. Dit omvat:

- Event Processing - Omvat de baangebeurtenissen die zowel op de sensorapparaten als op het VCC plaatsvinden. Dit is vooral nuttig wanneer de gezondheidswaarschuwing verwijst naar een gebeurtenis-type Silo.
- Disk Manager - dekt het schijfbeheerproces, silo's en hoe deze worden afgevoerd.
- Health Monitor - Omvat hoe de Health Monitor modules worden gebruikt om gezondheidswaarschuwingen te genereren.
- Log in op Ramdisk - Beschrijft de functie vastlegging op ramdisk en de mogelijke gevolgen voor gezondheidswaarschuwingen.

Om inzicht te krijgen in de 'Drain of Events'-gezondheidswaarschuwingen en om mogelijke storingen te kunnen identificeren is het nodig om te kijken hoe deze componenten werken en met elkaar interageren.

Verwerking van gebeurtenissen

Hoewel het type frequente afvoer van gezondheidswaarschuwingen kan worden geactiveerd door silo's die niet gebeurtenisgerelateerd zijn, is de overgrote meerderheid van de gevallen die worden gezien door Cisco TAC gerelateerd aan de afvoer van gebeurtenisgerelateerde informatie. Bovendien, om te begrijpen wat een afvoerkanaal van onverwerkte gebeurtenissen vormt, is er een behoefte om een blik te nemen op de architectuur van de gebeurtenisverwerking en de componenten die het vormen.



Wanneer een FirePOWER-sensor een pakket van een nieuwe verbinding ontvangt, genereert het snortproces een gebeurtenis in unified2-formaat dat een binair formaat is dat snellere lees-/schrijfbewerkingen en lichtere gebeurtenissen mogelijk maakt.

De output laat het **ondersteuningsspoor van het** FTD-opdrachtsysteem zien waar een nieuwe verbinding tot stand kan worden gebracht. De belangrijkste onderdelen worden belicht en toegelicht:

```
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3310981951
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Session: new snort session
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 new firewall session
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Inspection', action Allow and prefilter rule 0
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 HitCount data sent for rule id: 268437505,
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 allow action
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Default Inspection',
allow
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Snort id 0, NAP id 1, IPS id 0, Verdict PASS
```

Snort unified_events-bestanden worden gegenereerd per instantie onder het pad **[/ngfw]var/sf/detectie_engine/*/instance-N/**, waarbij:

- ***** is de gekleurde UUID. Dit is per apparaat uniek.
- **N** is de gescande instantie-ID die kan worden berekend als de instantie-ID van de vorige uitvoer (de gemarkeerde 0 in het voorbeeld) + 1

Er kunnen 2 types van unified_events files zijn in een gegeven Snort instantie map:

- unified_events-1 (bevat gebeurtenissen met hoge prioriteit).
- unified_events-2 (bevat gebeurtenissen met een lage prioriteit).

Een gebeurtenis met hoge prioriteit is een gebeurtenis die overeenkomt met een potentieel schadelijke verbinding.

Soorten gebeurtenissen en hun prioriteit:

Hoge prioriteit (1)	Lage prioriteit (2)
Inbraak	Connection
Malware	Detectie
Beveiligingsinformatie	Bestand

Gerelateerde verbindingsgebeurtenissen | Statistieken

De volgende output toont een gebeurtenis die tot de nieuwe verbinding behoort die in het vorige voorbeeld wordt gevonden. Het formaat is unified2 en is afkomstig van de output van het respectieve unified event log dat zich bevindt onder [/ngfw]/var/sf/detectie_engine/*/instance-**1**/ waarbij 1 de snort instance id is in de vorige output +1. De naam van het unified event log format volgt de syntaxis unified_events-**2**.log.**1599654750** waarbij 2 staat voor de prioriteit van de gebeurtenissen zoals getoond in de tabel en het laatste gedeelte in vet (**15996 4750**) is de tijdstempel (Unix-tijd) van het moment waarop het bestand is gemaakt.

> **Tip**: U kunt de Linux **date** opdracht gebruiken om de Unix tijd om te zetten naar een leesbare datum:
> admin@FP1120-2:~$ **sudo date -d@1599654750**
> Wed Sep 9 14:32:30 CEST 2020

```
Unified2 Record at offset 2190389
Type: 210(0x000000d2)
Timestamp: 0
Length: 765 bytes
Forward to DC: Yes
FlowStats:
Sensor ID: 0
Service: 676
NetBIOS Domain: <none>
Client App: 909, Version: 1.20.3 (linux-gnu)
Protocol: TCP
Initiator Port: 42310
Responder Port: 80
First Packet: (1599662092) Tue Sep 9 14:34:52 2020
Last Packet: (1599662092) Tue Sep 9 14:34:52 2020

<OUTPUT OMITTED FOR READABILITY>

Initiator: 192.168.0.2
Responder: 192.168.1.10
Original Client: ::
Policy Revision: 00000000-0000-0000-0000-00005f502a92
Rule ID: 268437505
Tunnel Rule ID: 0
Monitor Rule ID: <none>
Rule Action: 2
```

Naast elk unified_events bestand is er een bookmark bestand, dat 2 belangrijke waarden bevat:

1. Tijdstempel komt overeen met het huidige bestand unified_events voor die instantie en prioriteit.
2. Positie in bytes voor de laatste gelezen gebeurtenis in het bestand unified_event.

De waarden worden in volgorde van elkaar gescheiden door een komma zoals in dit voorbeeld:

```
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
```

Hierdoor kan de diskbeheerder weten welke gebeurtenissen al zijn verwerkt (naar het VCC gestuurd) en welke niet.

Merk op dat wanneer de disk manager een gebeurtenissilo afvoert het Unified event bestanden verwijdert. Voor meer informatie over de afvoer van silo's leest u het gedeelte Disk Manager.

Een uitgelekt uniform bestand wordt geacht onverwerkte gebeurtenissen te hebben wanneer een van deze gebeurtenissen waar is:

1. De tijdstempel voor de bladwijzer is lager dan de tijd voor het maken van bestanden.
2. De bladwijzertijdstempel is hetzelfde als de tijd voor het maken van bestanden en de positie in bytes in het bestand is kleiner dan de grootte ervan.

Het EventHandler-proces leest gebeurtenissen uit de geünificeerde bestanden en stroomt ze naar het FMC (als metagegevens) via sftunnel, het proces dat verantwoordelijk is voor versleutelde communicatie tussen de sensor en het FMC. Dit is een op TCP gebaseerde verbinding, zodat de gebeurtenisstreaming wordt bevestigd door de FMC

U kunt deze berichten zien in het bestand [/ngfw]/var/log/message:

```
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
```

Deze output verstrekt deze informatie:

- Snort heeft het bestand unified_events geopend voor uitvoer (om erin te schrijven).
- Event Handler opende hetzelfde bestand unified_events (om ervan te lezen).
- sftunnel meldde het aantal gebeurtenissen die van dat unified_events bestand verwerkt zijn.

Het bladwijzerbestand wordt vervolgens aangepast. De sftunnel gebruikt 2 verschillende kanalen genaamd Unified Events (UE) Channel 0 en 1 voor gebeurtenissen met hoge en lage prioriteit.

Met de opdracht **sfunnel_status** CLI op de FTD, kunt u het aantal gebeurtenissen zien dat is gestreamd.

```
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
```

In het VCC worden de gebeurtenissen ontvangen via het SFDataCorrelator-proces.

De status van gebeurtenissen die van elke sensor werden verwerkt kan met de opdracht **stats_unified.pl** worden gezien:

```
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
```

Deze opdracht toont de status van de achterstand van gebeurtenissen voor een bepaald apparaat per kanaal, de gebruikte Channel-id is hetzelfde als de sftunnelbuis.

De Bytes Behind waarde kan worden berekend als het verschil tussen de positie die wordt weergegeven in het bestand met de unified event bookmark en de grootte van het Unified event bestand, plus elk volgend bestand met een hogere timestamp dan die in het bookmark bestand.

In het SFDataCorrelator-proces worden ook prestatiestatistieken opgeslagen, die worden opgeslagen in **/var/sf/rna/correlator-stats/**. Er wordt per dag één bestand gemaakt om de prestatiestatistieken voor die dag in CSV-indeling op te slaan. De naam van het bestand gebruikt het formaat "**JJJJ-MM-DD**" en het bestand dat overeenkomt met de huidige dag wordt **nu** aangeroepen.

De statistieken worden om de 5 minuten verzameld (er is één regel per 5-minuten interval).

De output van dit bestand kan worden gelezen met de opdracht **perfstats**. Merk op dat deze opdracht ook wordt gebruikt om bestanden met snortprestatiestatistieken te lezen, dus de juiste vlaggen moeten worden gebruikt:

-C: Draagt perfstats op dat de input een correlator-stats bestand is (zonder deze vlag perfstats veronderstelt de input is een snort performance statistics bestand).

-q: In de stille modus wordt alleen de samenvatting van het bestand afgedrukt.

```
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
```

Elke rij in de samenvatting heeft 3 waarden in deze volgorde: Gemiddeld, Minimaal, Maximaal.

Als u afdrukt zonder de markering -q, ziet u ook de intervalwaarden van 5 minuten. De samenvatting wordt aan het eind getoond.

Merk op dat elk VCC een maximumdebiet heeft zoals beschreven in zijn gegevensblad. De volgende tabel bevat de waarden per module uit de desbetreffende datasheet:

Model	VCC 750	VCC 1000	VCC 1600	VCC 2000	VCC 2500	VCC 2600	VCC 4000	VCC 4500	VCC 4600	VCCv	V
Max. stroomsnelheid (fps)	2000	5000	5000	12000	12000	12000	20000	20000	20000	Variabel	1

Merk op dat deze waarden gelden voor het totaal van alle soorten gebeurtenissen die in vet worden weergegeven op de SFDataCorrelator statistiek output.

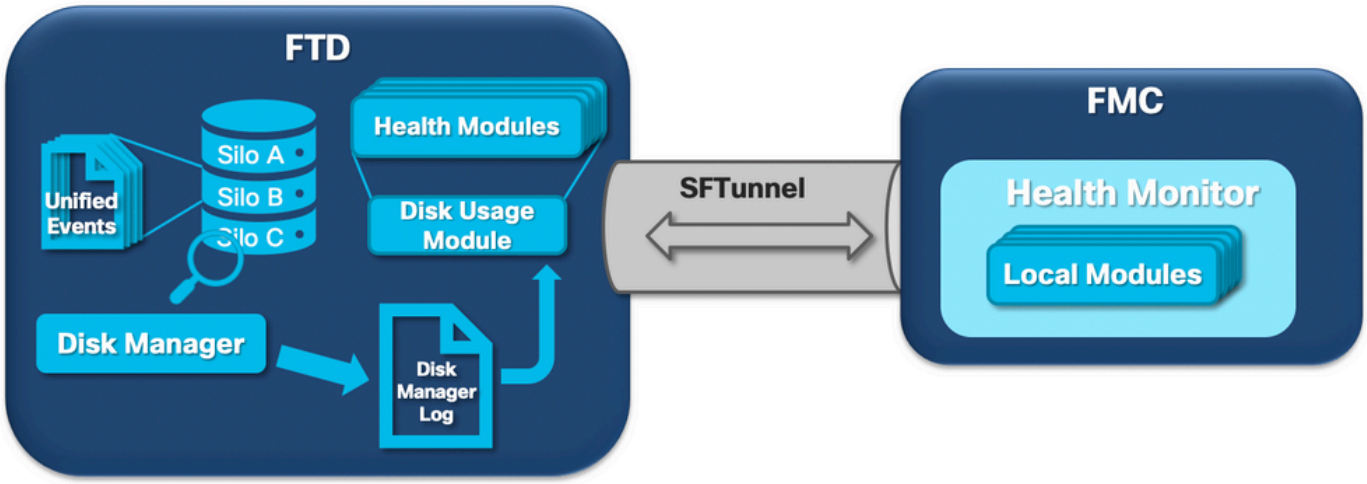
Als je kijkt naar de output en we de grootte van ons VCC zo inschatten dat we voorbereid zijn op het slechtst denkbare scenario (wanneer alle maximumwaarden tegelijkertijd gebeuren), dan is het aantal gebeurtenissen dat dit VCC ziet 48,65 + 348,15 + 4,63 + 3,25 + 0,06 = **404,74 fps**.

Deze totale waarde kan worden vergeleken met de waarde uit het gegevensblad van het betreffende model.

De SFDataCorrelator kan ook extra werk maken bovenop de ontvangen gebeurtenissen (zoals voor Correlatieregels), het slaat ze dan op in de database die wordt gevraagd om verschillende informatie te vullen in de grafische gebruikersinterface van het FMC (GUI) zoals Dashboards en Event Views.

Disk Manager

Het volgende logische diagram toont de logische componenten voor zowel de **Health Monitor** als de processen van de **Disk Manager** aangezien zij voor de generatie van schijf-gerelateerde gezondheidswaarschuwingen worden verweven.



In een notendop beheert het disk manager proces het schijfgebruik van het vak en het heeft zijn configuratiebestanden in de map [/ngfw]/etc/sf/. Er zijn meerdere configuratiebestanden voor het schijfbeheerproces die onder bepaalde omstandigheden worden gebruikt:

- diskmanager.conf - Standaard configuratiebestand.

- diskmanager_2hd.conf - Gebruikt wanneer de doos 2 harde schijven heeft geïnstalleerd. De tweede harde schijf is die welke gerelateerd is aan de Malware Expansion, gebruikt om bestanden op te slaan zoals gedefinieerd in het bestandsbeleid.
- ramdisk-diskmanager.conf - Wordt gebruikt wanneer Log in Ramdisk is ingeschakeld. Kijk voor meer informatie in het gedeelte Log in op Ramdisk.

Elk type bestand dat door de disk manager wordt gevolgd krijgt een Silo toegewezen. Op basis van de hoeveelheid beschikbare schijfruimte op het systeem berekent de diskbeheerder een HWM (High Water Mark) en een LWM (Low Water Mark) voor elke silo.

Wanneer een silo wordt afgevoerd door het Disk Manager-proces, gebeurt dit totdat de LWM is bereikt. Aangezien gebeurtenissen per bestand worden afgevoerd, kan deze drempelwaarde worden overschreden.

Om de status van de silo's op een sensorapparaat te controleren, kunt u deze opdracht gebruiken:

```
> 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
```

Het Disk Manager-proces wordt uitgevoerd als aan een van deze voorwaarden is voldaan:

- Het proces wordt gestart of opnieuw gestart
- Een Silo bereikt de HWM
- Een Silo is handmatig gedraineerd
- Eén keer per uur

Elke keer dat het Disk Manager-proces wordt uitgevoerd, genereert het een vermelding voor elk van de verschillende silo's op zijn eigen logbestand dat zich onder [/ngfw]/var/log/diskmanager.log bevindt en gegevens in CSV-formaat heeft.

Vervolgens wordt een voorbeeldlijn getoond uit het bestand diskmanager.log, genomen van een sensor die de afvoer van onverwerkte gebeurtenissen heeft geactiveerd uit de gezondheidswaarschuwing Unified Low Priority Events, evenals de uitsplitsing van de respectievelijke kolommen:

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

Kolom	Waarde

Silo Label	prioriteit_2_gebeurtenissen
Tijd van afvoer (Epochtijd)	1599668981
Aantal afgevoerde bestanden	221
Afgelopen bytes	4587929508
Huidige grootte van gegevens na afvoer (bytes)	1132501868
Grootste bestand leeg (bytes)	20972020
Kleinste bestand leeg (bytes)	4596
Oudste bestand gedraineerd (Epoch-tijd)	1586044534
Hoog watermerk (bytes)	5710966962
Laag watermerk (bytes)	1142193392
Aantal bestanden met uitlekken van onverwerkte gebeurtenissen	110
Vlag Diskmanager	0

Deze informatie wordt vervolgens gelezen door de betreffende Health Monitor module om de gerelateerde gezondheidswaarschuwing te activeren.

Handmatig een Silo afvoeren

In bepaalde scenario's, kunt u een silo handmatig willen afvoeren. Bijvoorbeeld, om schijfruimte met handmatige silo drain in plaats van handmatige verwijdering van bestanden te wissen heeft het voordeel van de disk manager om te beslissen welke bestanden te houden en welke te verwijderen. De disk manager houdt de meest recente bestanden voor die silo.

Alle silo's kunnen worden afgevoerd en dit werkt zoals reeds beschreven (de diskbeheerder voert gegevens af tot de hoeveelheid gegevens onder de LWM-drempel valt). Het opdrachtsysteem **ondersteunt silo-drain** is beschikbaar in de FTD CLISH-modus en geeft een lijst van de beschikbare silo's (naam + numerieke id).

Dit is een voorbeeld van een handmatige afvoer van de Unified Low Priority Events-silo:

```
> 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

Dat zijn de belangrijkste punten:

- Alle gezondheidswaarschuwingen die worden weergegeven op het VCC in het menu Gezondheidsmonitor of onder het tabblad Gezondheid in het Berichtencentrum, worden gegenereerd door het proces voor Gezondheidsmonitor.
- Dit proces bewaakt de gezondheid van het systeem, zowel voor het VCC als voor de beheerde sensoren, en bestaat uit een aantal verschillende modules.
- In het gezondheidsbeleid worden alarmmodules voor de gezondheid gedefinieerd die per apparaat kunnen worden aangesloten.

- Gezondheidswaarschuwingen worden gegenereerd door de Disk Usage-module die kan draaien op elk van de sensoren die door het VCC worden beheerd.
- Wanneer het Health Monitor-proces op het VCC wordt uitgevoerd (eenmaal om de 5 minuten of wanneer een handmatige run wordt geactiveerd) kijkt de Disk Usage-module in het diskmanager.log-bestand en, als aan de juiste voorwaarden is voldaan, wordt de respectieve gezondheidswaarschuwing geactiveerd.

Om een **drain van onverwerkte gebeurtenissen** gezondheidswaarschuwing te activeren Al deze voorwaarden moeten waar zijn:

1. Het afvoerveld bytes is groter dan 0 (dit geeft aan dat gegevens van deze silo zijn afgevoerd).
2. Het aantal bestanden met gebeurtenissen die niet verwerkt zijn, is groter dan 0 (dit geeft aan dat er gebeurtenissen die niet verwerkt zijn in de uitgelekte gegevens).
3. De tijd van de afvoer is minder dan 1 uur.

Om een **Frequent Drain of Events** gezondheidswaarschuwing te activeren moeten deze voorwaarden waar zijn:

1. De laatste 2 vermeldingen in het bestand diskmanager.log moeten: Laat Bytes een veld groter dan 0 uitlekken (dit geeft aan dat gegevens van deze silo zijn uitgelekt).Zorg dat u minder dan 5 minuten van elkaar verwijderd bent.
2. De tijd van de afvoer van de laatste vermelding voor deze silo is minder dan 1 uur.

De resultaten van de module van het schijfgebruik (evenals de resultaten die door de andere modules worden verzameld) worden via sftunnel naar het VCC gestuurd. U kunt tellers zien voor de Gezondheidsgebeurtenissen die via sftunnel worden uitgewisseld met de opdracht **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
```

Log in op Ramdisk

Hoewel de meeste gebeurtenissen in schijf worden opgeslagen, wordt het apparaat standaard geconfigureerd om aan te melden bij ramdisk om geleidelijke schade aan de SSD te voorkomen die kan worden veroorzaakt door constant schrijft en verwijdert van gebeurtenissen naar disk.

In dit scenario worden de gebeurtenissen niet opgeslagen onder **[/ngfw]/var/sf/detectie_engine/*/instance-N/,** maar ze bevinden zich in **[/ngfw]/var/sf/detectie_engines/*/instantie-N/connection/**, wat een symbolische link is naar **/dev/shm/instance-N/connection.** In dit geval, verblijven de gebeurtenissen in virtueel geheugen eerder dan fysiek.

```
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
```

Om te verifiëren wat het apparaat momenteel is geconfigureerd om de opdracht **te** laten uitvoeren, **laat log-events-to-ramdisk** van de FTD CLISH zien. U kunt dit ook wijzigen als u de opdracht **log-events-to-ramdisk configureren <in/uitschakelen>** gebruikt:

```
> show log-events-to-ramdisk
Logging connection events to RAM Disk.

>configure log-events-to-ramdisk
Enable or Disable  enable or disable (enable/disable)
```

> **Waarschuwing**: Wanneer de opdracht "log-events-to-ramdisk uitschakelen configureren" wordt uitgevoerd, moeten er twee implementaties worden uitgevoerd op de FTD zodat de snort niet vast komt te zitten in "D"-toestand (Uninterruptible Sleep), wat een verkeersstoring zou veroorzaken.
> Dit gedrag is in het defect gedocumenteerd met Cisco bug-id CSC53372. Met de eerste implementatie wordt de herbeoordeling van de fase van het snortgeheugen overgeslagen, wat ervoor zorgt dat de snort in "D"-status gaat, de tijdelijke oplossing is om een andere implementatie te doen met eventuele dummywijzigingen.

Wanneer u logt op ramdisk is het belangrijkste nadeel dat de respectievelijke silo een kleinere ruimte toegewezen heeft en deze dus vaker onder dezelfde omstandigheden afvoert. De volgende output is de diskmanager van een FPR 4140 met en zonder de loggebeurtenissen aan ramdisk die voor vergelijking wordt toegelaten.

Log in op Ramdisk ingeschakeld

```
> 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
```

Log in op Ramdisk uitgeschakeld

```
> 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

De kleinere omvang van de silo wordt gecompenseerd door de hogere snelheid om toegang te krijgen tot de Evenementen en deze te streamen naar het VCC. Hoewel dit onder goede omstandigheden een betere optie is, moet het nadeel worden overwogen.

Veelgestelde vragen (FAQ)

Wordt de afvoer van gebeurtenissen alleen gegenereerd door Connection Events?

Nee.

- Waarschuwingen voor frequente afvoer kunnen worden gegenereerd door elke disk manager silo.
- Waarschuwingen van afvoer van onverwerkte gebeurtenissen kunnen worden gegenereerd door elke eventgerelateerde silo.

Verbindingsgebeurtenissen zijn de meest voorkomende schuldige.

Is het altijd aan te raden om Log in Ramdisk uit te schakelen als er een melding voor een vaak afvoersignaal wordt weergegeven?

Nee. Alleen in scenario's voor overmatige vastlegging, met uitzondering van DOS/DDOS, wanneer de betrokken Silo de Connection Events silo is, en alleen in gevallen waarin het niet mogelijk is om de vastlegging-instellingen verder te verbeteren.

Als DOS/DDOS excessieve vastlegging veroorzaakt, is de oplossing om DOS/DDOS-bescherming te implementeren of de bron(nen) van de DOS/DDOS-aanvallen te elimineren.

De standaardfunctie "Log to Ramdisk" vermindert de slijtage van de SSD, dus het gebruik ervan wordt sterk aanbevolen.

Wat is een onverwerkte gebeurtenis?

Gebeurtenissen worden niet afzonderlijk als onverwerkt aangemerkt. Een bestand heeft onverwerkte gebeurtenissen wanneer:

De aanmaaktijdstempel is hoger dan het tijdstempelveld in het betreffende bladwijzerbestand.

of

De aanmaaktijdstempel is gelijk aan het tijdstempelveld in het betreffende bladwijzerbestand en de grootte is groter dan de positie in het veld Bytes in het betreffende bladwijzerbestand.

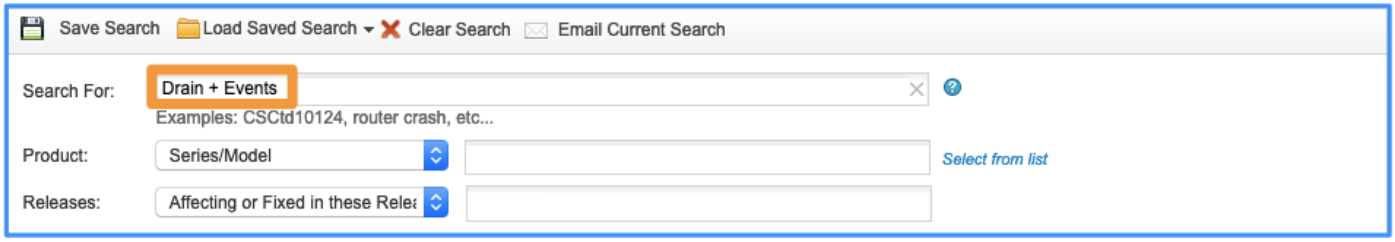
Hoe kent het VCC het aantal Bytes achter voor een bepaalde sensor?

De sensor stuurt metagegevens over de unified_events bestandsnaam en grootte en de informatie over de bladwijzerbestanden die het VCC genoeg informatie geeft om de bytes erachter te berekenen als:

Current unified_events file size - **Positie in Bytes**" veld van bladwijzerbestand + Grootte van alle unified_events bestanden met hogere tijdstempel dan de tijdstempel in de respectievelijke bladwijzerbestand.

Bekende problemen

Open de Zoekfunctie voor bugs en gebruik deze query:



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.