Dépannage du drainage des événements non traités FMC et du drainage fréquent des événements Alertes du moniteur d'état

Contenu

Introduction

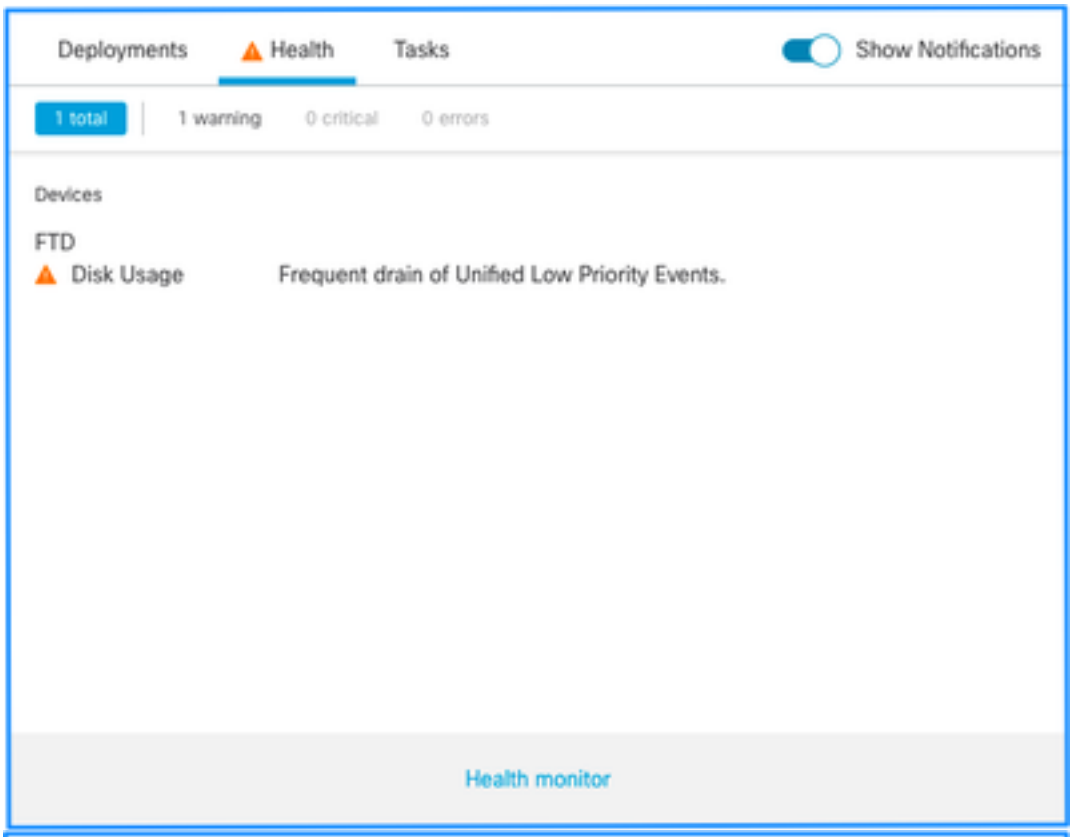
Ce document décrit comment dépanner les alertes **d'état Drain of Unprocessing Events** et **Frequent Drain of Events** sur Firepower Management Center (FMC).

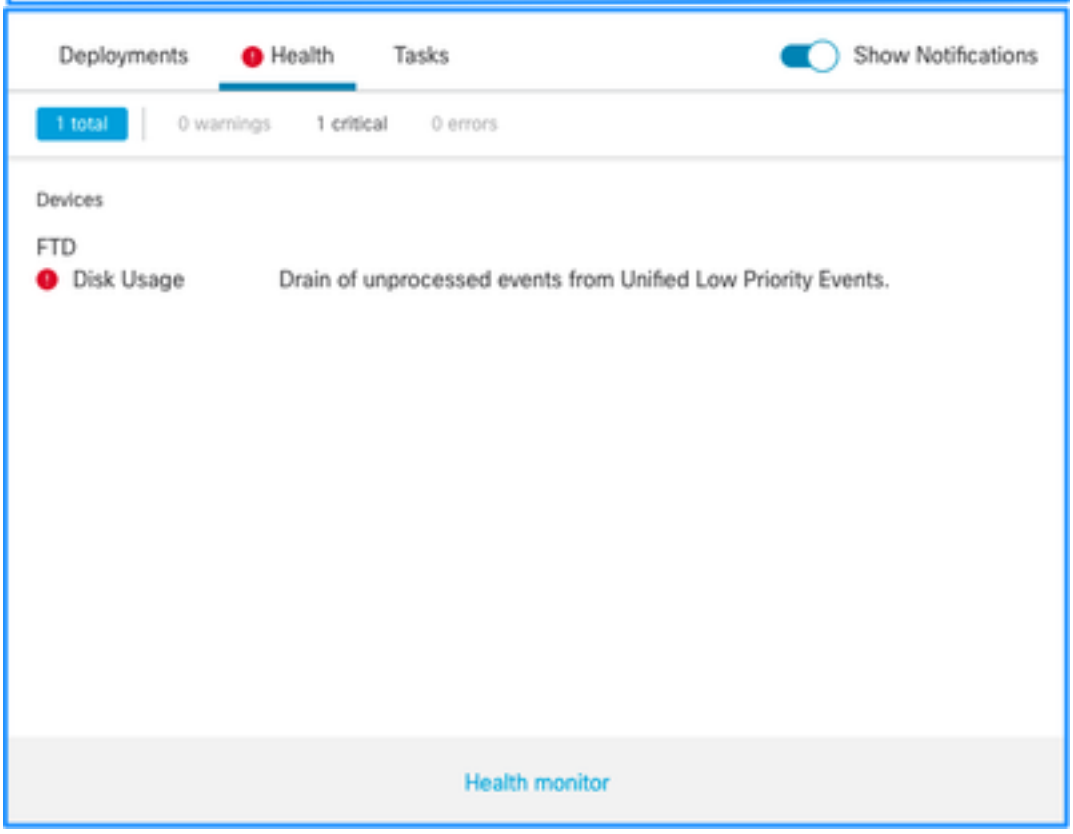
Présentation du problème

Le FMC génère l'une des alertes d'intégrité suivantes :

- Drainage fréquent des événements Unified de faible priorité
  et/ou
- Drainage des événements non traités des événements Unified de faible priorité

Bien que ces événements soient générés et affichés sur le FMC, ils concernent un capteur de périphérique géré, qu'il s'agisse d'un périphérique Firepower Threat Defense (FTD) ou d'un périphérique NGIPS (Next-Generation Intrusion Prevention System). Pour le reste de ce document, le terme capteur fait référence aux périphériques FTD et NGIPS, sauf indication contraire.





Voici la structure des alertes d'intégrité :

- Drainage fréquent de <NOM DU SILO>
- Drainage des événements non traités de <NOM DU SILO>

Dans cet exemple, le NOM du SILO est **Unified Low Priority Events**. Il s'agit de l'un des silos du gestionnaire de disques (voir la section Informations générales pour une explication plus complète).

En outre :

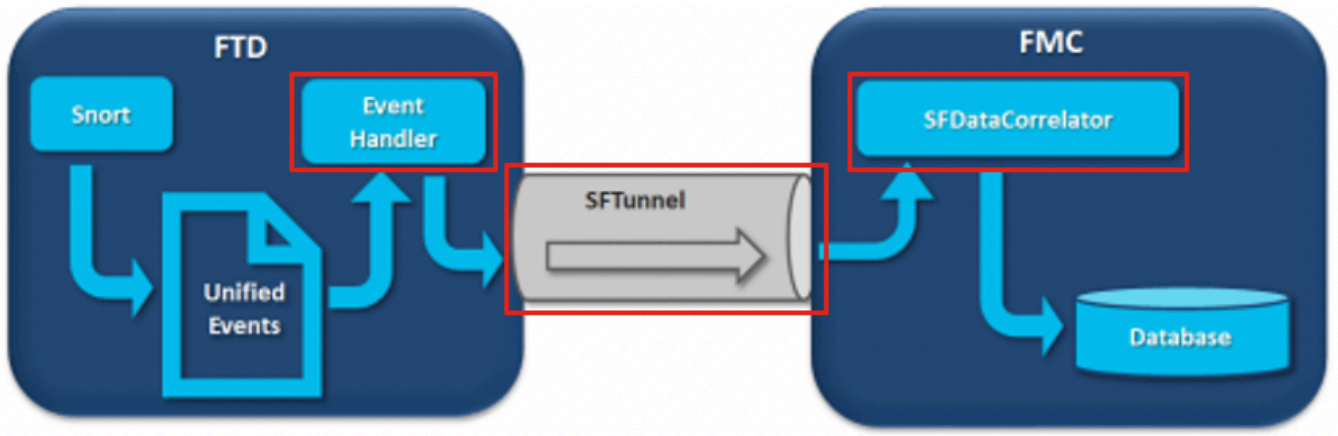
- Bien que n'importe quel silo puisse techniquement générer un drainage fréquent d'alerte d'état de santé de <NOM DU SILO>, les événements les plus courants sont ceux liés aux événements et, parmi eux, les événements de faible priorité simplement parce qu'il s'agit du type d'événements le plus souvent générés par les capteurs.
- Un événement « Fréquent drain of <NOM DU SILO> » a un niveau de gravité Avertissement dans le cas où il s'agit d'un silo lié à un événement puisque, si celui-ci a été traité (une explication sur ce qui constitue un événement non traité est donnée ensuite), ils sont dans la base de données FMC.
- Dans le cas d'un silo non lié à un événement, tel que le silo « Sauvegardes », l'alerte est critique car ces informations sont perdues.
- Seuls les silos de type d'événement génèrent une alerte d'intégrité Drain of unprocessing events from <SILO NAME>. Cette alerte a toujours un niveau de gravité Critique.

Les symptômes supplémentaires peuvent inclure :

- Lenteur sur l'interface utilisateur FMC
- Perte d'événements

Scénarios de dépannage courants

Un drainage fréquent de l'événement <NOM DU SILO> est provoqué par un trop grand nombre d'entrées dans le silo pour sa taille. Dans ce cas, le gestionnaire de disques purge ce fichier au moins deux fois au cours du dernier intervalle de 5 minutes. Dans un silo de type d'événement, cela est généralement dû à une journalisation excessive de ce type d'événement. Dans le cas d'un drainage d'événements non traités de l'alerte d'intégrité de <SILO NAME>, cela peut également être causé par un goulot d'étranglement dans le chemin de traitement des événements.



Le schéma présente 3 goulots d'étranglement potentiels :

- Le processus EventHandler sur FTD est surabonné (il lit plus lentement que ce que Snort écrit)
- L'interface d'événement est surabonnée
- Le processus SFDataCorrelator sur FMC est en sursouscription

Pour mieux comprendre l'architecture Event Processing, reportez-vous à la section Deep Dive

correspondante.

Cas 1. Journalisation excessive

Comme indiqué dans la section précédente, l'une des causes les plus courantes de ce type d'alertes est la saisie excessive.

La différence entre les valeurs Low Water Mark (LWM) et High Water Mark (HWM) collectées à partir de la commande **show disk-manager** CLISH montre l'espace nécessaire pour prendre ce silo pour passer de LWM (fraîchement drainé) à la valeur HWM. S'il y a un drainage fréquent des événements (avec ou sans événements non traités), la première chose que vous devez revoir est la configuration de journalisation.

Pour obtenir une explication détaillée du processus Gestionnaire de disques, reportez-vous à la section Enfoncement correspondante.

Qu'il s'agisse d'une double journalisation ou simplement d'un taux élevé d'événements sur l'écosystème global de gestionnaires-capteurs, un examen des paramètres de journalisation doit être effectué.

Actions recommandées

Étape 1. Vérification de la double journalisation

Les scénarios de double journalisation peuvent être identifiés si vous regardez les **perfstats** du corrélateur sur le FMC comme indiqué dans ce résultat :

```
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
```

Dans ce cas, un taux élevé de flux dupliqués peut être vu dans la sortie.

Étape 2 : vérification des paramètres de journalisation de l'ACP

Vous devez commencer par revoir les paramètres de journalisation de la stratégie de contrôle d'accès (ACP). Veillez à suivre les meilleures pratiques décrites dans ce document Bonnes pratiques pour la consignation des connexions

Il est conseillé de revoir les paramètres de journalisation dans toutes les situations, car les recommandations répertoriées ne couvrent pas uniquement les scénarios de double journalisation.

Étape 3. Vérifier si la consignation excessive est attendue ou non

Vous devez vérifier si la consignation excessive a une cause attendue ou non. Si la journalisation excessive est due à une attaque DOS/DDoS ou à une boucle de routage ou à une application/hôte spécifique qui effectue un grand nombre de connexions, vous devez vérifier et atténuer/arrêter les connexions provenant des sources de connexion excessives inattendues.

Étape 4. Mise à niveau du modèle

Mettre à niveau le périphérique matériel FTD vers un modèle de performances plus élevées (par exemple FPR2100 —> FPR4100), la source du silo augmenterait.

Étape 5. Déterminez si vous pouvez désactiver Log to Ramdisk

Dans le cas du silo d'événements Unified Low Priority, vous pouvez désactiver Log to Ramdisk pour augmenter la taille du silo avec les inconvénients décrits dans la section Deep Dive correspondante.

Cas 2. Goulot d'étranglement dans le canal de communication entre le capteur et le FMC

Ce type d'alerte est également souvent dû à des problèmes de connectivité et/ou à une instabilité du canal de communication (sftunnel) entre le capteur et le FMC. Le problème de communication peut être dû à :

- sftunnel est désactivé ou instable (volets).
- sftunnel est surabonné.

Pour le problème de connectivité sftunnel, assurez-vous que le FMC et le capteur sont accessibles entre leurs interfaces de gestion sur le port TCP 8305.

Sur FTD, vous pouvez rechercher la chaîne **sftunneld** dans le fichier **[/ngfw]/var/log/messages**. Des problèmes de connectivité entraînent la génération de messages de ce type :

```
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
```

Le surabonnement de l'interface de gestion des FMC peut être une pointe dans le trafic de gestion ou un surabonnement constant. Les données historiques du Moniteur d'intégrité en sont un bon indicateur.

La première chose à noter est que dans la plupart des cas, le FMC est déployé avec une seule carte réseau pour la gestion. Cette interface est utilisée pour :

- Gestion FMC.
- Gestion des capteurs FMC.
- Collecte d'événements FMC à partir des capteurs.
- Mise à jour des flux de renseignements.
- Téléchargement des mises à jour SRU, Software, VDB et GeoDB à partir du site de téléchargement de logiciels.
- Requête de réputation et de catégories d'URL (le cas échéant).
- Requête relative aux dispositions de fichiers (le cas échéant).

Actions recommandées

Vous pouvez déployer une deuxième carte réseau sur le FMC pour une interface dédiée aux événements. Les implémentations peuvent dépendre du cas d'utilisation.

Des instructions générales sont disponibles dans le Guide matériel FMC Déploiement sur un réseau de gestion

Cas 3. Un goulot d'étranglement dans le processus SFDataCorrelator

Le dernier scénario à couvrir est lorsque le goulot d'étranglement se produit du côté du SFDataCorrelator (FMC).

La première étape consiste à examiner le fichier diskmanager.log car il contient des informations importantes à collecter, telles que :

- La fréquence du drain.
- Nombre de fichiers avec des événements non traités drainés.
- Occurrence du drainage avec des événements non traités.

Pour plus d'informations sur le fichier diskmanager.log et comment l'interpréter, vous pouvez vous référer à la section Gestionnaire de disques. Les informations collectées à partir du fichier

diskmanager.log peuvent être utilisées pour affiner les étapes suivantes.

En outre, vous devez examiner les statistiques de performances du corrélateur :

```
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
```

Notez que ces statistiques concernent le FMC et correspondent à l'ensemble de tous les capteurs qu'il gère. Dans le cas d'événements Unified de faible priorité, vous recherchez principalement :

- Nombre total de flux par seconde de tout type d'événement pour évaluer un éventuel surabonnement du processus SFDataCorrelator.
- Les deux lignes mises en surbrillance dans le résultat précédent : **Flux d'exécution/seconde** - Indique le taux d'événements de faible priorité traités par SFDataCorrelator.**rna dup flows/second** - Indique le taux d'événements de faible priorité dupliqués traités par SFDataCorrelator. Cette opération est générée par la double journalisation, comme indiqué dans le scénario précédent.

Sur la base des résultats, on peut conclure que :

- Il n'y a pas de journalisation dupliquée comme indiqué par les flux d'exécution de sauvegarde/seconde ligne.
- Dans la ligne Flux d'exécution/seconde, la valeur Maximum est beaucoup plus élevée que la valeur Moyenne. Il y a donc eu un pic dans le taux d'événements traités par le processus SFDataCorrelator. Cela pourrait être prévu si vous regardez ce matin tôt quand vos utilisateurs journée de travail vient de commencer, mais en général, il est un drapeau rouge et nécessite une enquête plus approfondie.

Pour plus d'informations sur le processus SFDataCorrelator, consultez la section Traitement des événements.

Actions recommandées

Tout d'abord, vous devez déterminer quand la pointe s'est produite. Pour ce faire, vous devez examiner les statistiques du corrélateur pour chaque intervalle d'échantillonnage de 5 minutes. Les informations collectées à partir du fichier diskmanager.log peuvent vous aider à passer directement à la période importante.

> **Astuce** : Dirigez la sortie vers le pager Linux **moins** afin que vous puissiez facilement

rechercher.

```
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
```

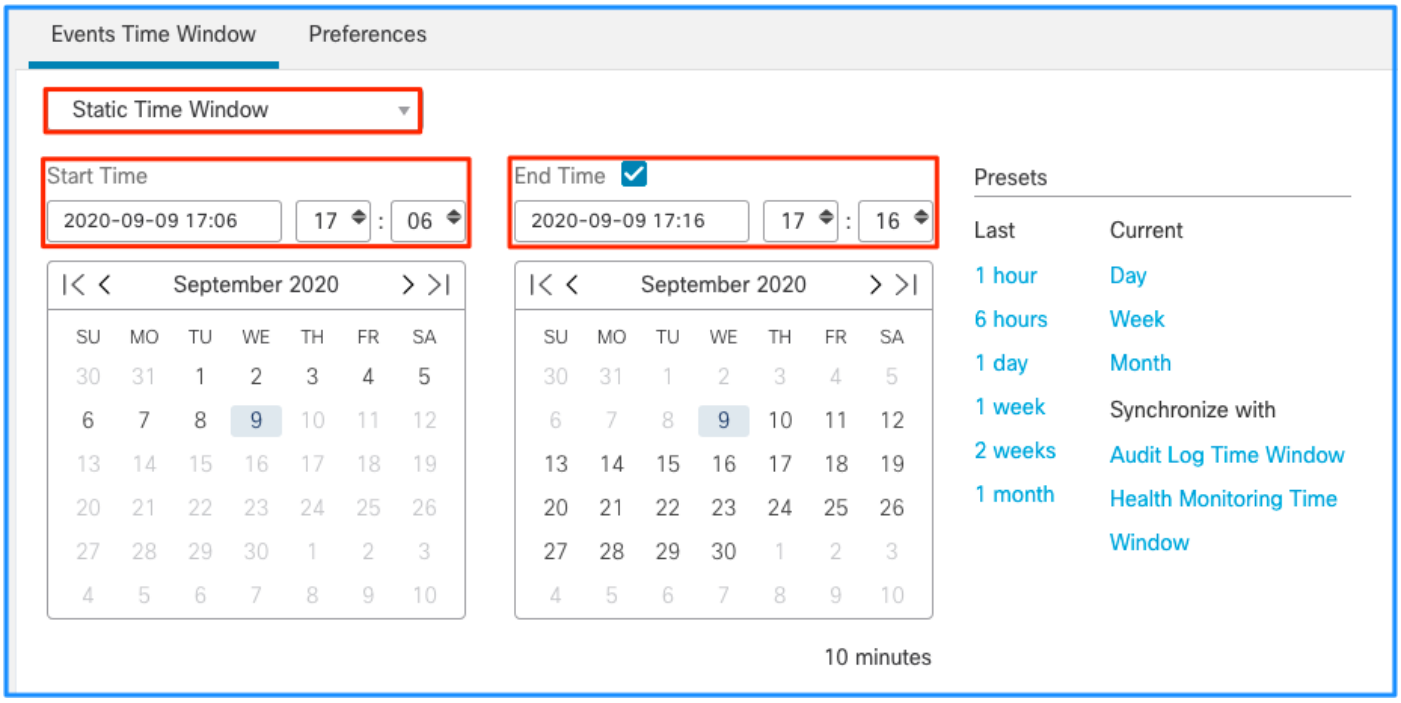
```
pcnt host limit in use:        100.00
rna events/second:             8.57
user cpu time:                 58.20
system cpu time:               41.13
memory usage:                  5007832
resident memory usage:         837732
rna flows/second:              3388.23
rna dup flows/second:          0.00
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
```

Utilisez les informations du résultat pour :

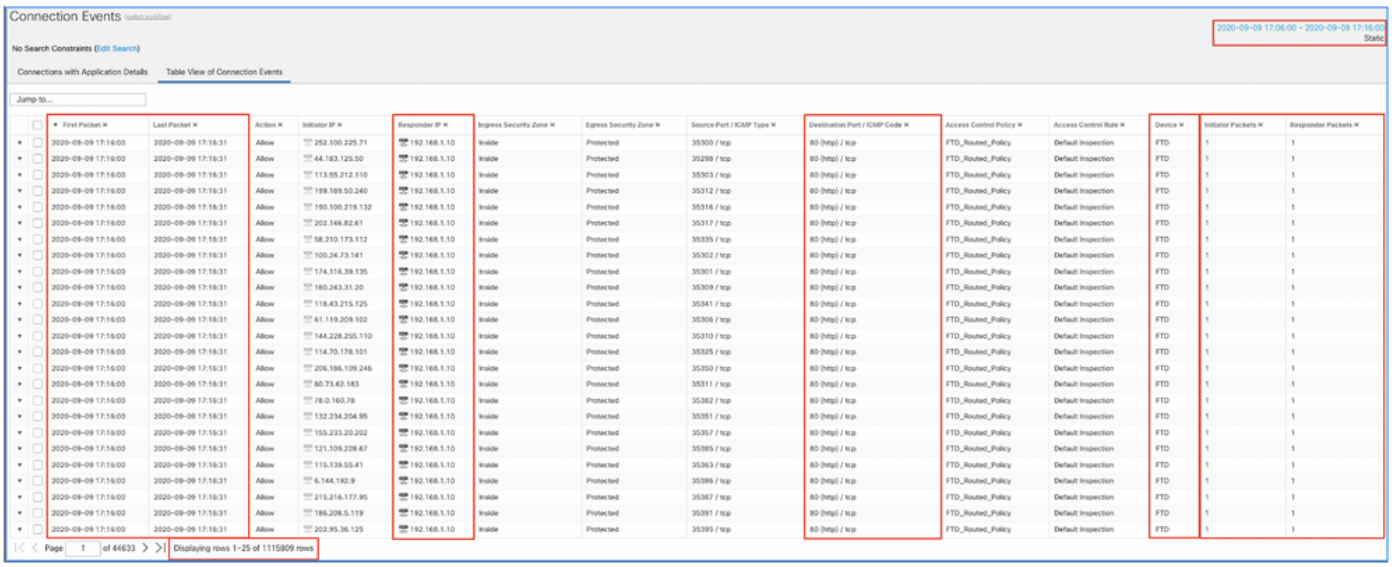
- Déterminer le taux normal/de base des événements.
- Déterminez l'intervalle de 5 minutes entre chaque pic.

Dans l'exemple précédent, il y a un pic évident dans le taux d'événements reçus à 16:06:39 et au-delà. Notez qu'il s'agit de moyennes sur 5 minutes, de sorte que l'augmentation peut être plus abrupte que celle indiquée (rafale), mais diluée dans cet intervalle de 5 minutes si elle a commencé vers la fin.

Bien que cela mène à la conclusion que ce pic d'événements a causé le drainage des événements non traités, vous pouvez jeter un oeil aux événements de connexion de l'interface utilisateur graphique (GUI) de FMC avec la fenêtre de temps appropriée pour comprendre quel type de connexions a traversé la boîte FTD dans ce pic :



Appliquez cette fenêtre de temps pour obtenir les événements de connexion filtrés, n'oubliez pas de prendre en compte le fuseau horaire. Dans cet exemple, le capteur utilise UTC et le FMC UTC+1. Utilisez la vue Tableau pour afficher les événements qui ont déclenché la surcharge d'événements et prendre les mesures appropriées :



En se basant sur les horodatages (heure du premier et du dernier paquet), on peut voir qu'il s'agit de connexions de courte durée. En outre, les colonnes Paquets initiateur et répondeur indiquent qu'il n'y a eu qu'un seul paquet échangé dans chaque direction. Cela confirme que les connexions ont été de courte durée et ont échangé très peu de données.

Vous pouvez également constater que tous ces flux ciblent les mêmes adresses IP et ports de répondeur. En outre, ils sont tous signalés par le même capteur (qui, avec les informations d'interface d'entrée et de sortie, peut indiquer l'emplacement et la direction de ces flux). Actions supplémentaires :

- Vérifiez les journaux système sur le point d'extrémité de destination.
- Mettez en oeuvre la protection DOS/DDOS ou prenez d'autres mesures préventives.

Note: L'objectif de cet article est de fournir des directives pour dépanner l'alerte Drain of

Unprocessing Events. Cet exemple a utilisé hping3 pour générer une inondation TCP SYN vers le serveur de destination. Pour obtenir des instructions sur le durcissement de votre périphérique FTD, consultez le Guide de durcissement de Cisco Firepower Threat Defense

Éléments à collecter avant de contacter le centre d'assistance technique Cisco (TAC)

Il est vivement recommandé de collecter ces éléments avant de contacter le TAC Cisco :

- Capture d'écran des alertes d'intégrité détectées.
- Dépannez le fichier généré à partir du FMC.
- Dépannez le fichier généré à partir du capteur affecté.
- Date et heure de la première apparition du problème.
- Informations sur les modifications apportées récemment aux politiques (le cas échéant).
- Le résultat de la commande stats_unified.pl comme décrit dans la section Event Processing avec une mention des capteurs affectés.

Présentation détaillée

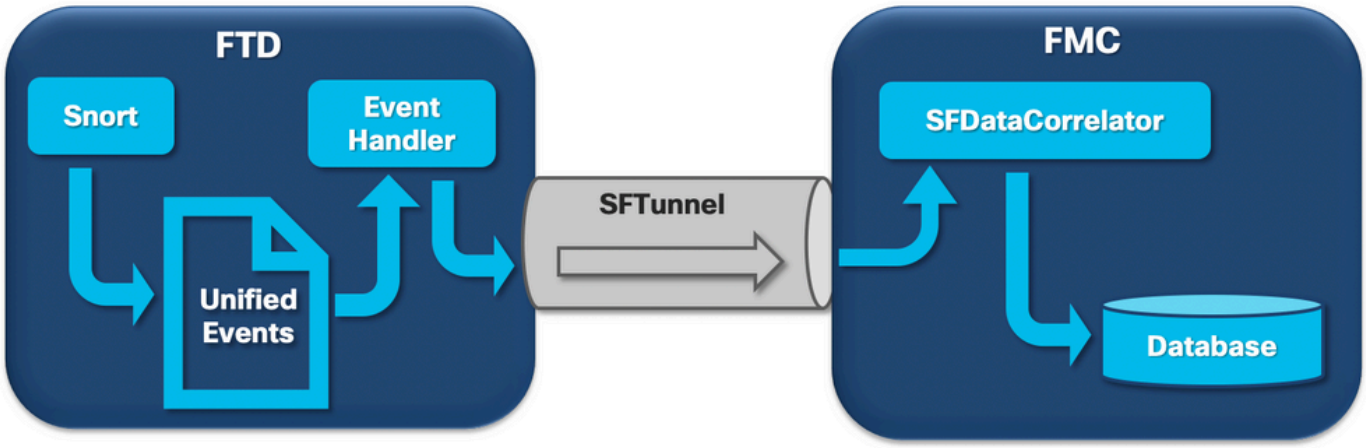
Cette section couvre une explication détaillée des divers composants qui peuvent participer à ce type d'alertes d'intégrité. Cela inclut :

- Event Processing (Traitement des événements) : couvre le chemin emprunté par les événements sur les capteurs et le FMC. Ceci est principalement utile lorsque l'alerte d'intégrité fait référence à un silo de type événement.
- Gestionnaire de disques : couvre le processus du gestionnaire de disques, les silos et leur mode de vidange.
- Health Monitor - couvre la manière dont les modules Health Monitor sont utilisés pour générer des alertes d'intégrité.
- Log to Ramdisk : couvre la fonctionnalité de journalisation sur Ramdisk et son impact potentiel sur les alertes d'intégrité.

Pour comprendre les alertes d'état Drain of Events et être en mesure d'identifier les points de défaillance potentiels, il est nécessaire d'examiner comment ces composants fonctionnent et interagissent les uns avec les autres.

Traitement des événements

Même si le type d'alerte de santé Drain fréquent peut être déclenché par des silos qui ne sont pas liés à un événement, la grande majorité des cas observés par le TAC Cisco sont liés à un drainage des informations liées à un événement. En outre, pour comprendre ce qui constitue un drain d'événements non traités, il est nécessaire de jeter un oeil à l'architecture de traitement des événements et aux composants qui la constituent.



Lorsqu'un capteur Firepower reçoit un paquet d'une nouvelle connexion, le processus snort génère un événement au format unified2, qui est un format binaire permettant une lecture/écriture plus rapide ainsi que des événements plus légers.

Le résultat montre la commande FTD **system support trace** où vous pouvez voir une nouvelle connexion créée. Les parties importantes sont mises en évidence et expliquées :

```
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
```

Les fichiers Snort unified_events sont générés par instance sous le chemin **[/ngfw]var/sf/detection_engine/*/instance-N/**, où :

- ***** est l'UUID Snort. Il s'agit d'une valeur unique par appliance.
- **N** est l'ID d'instance Snort qui peut être calculé comme l'ID d'instance de la sortie précédente (le 0 mis en surbrillance dans l'exemple) + 1

Il peut y avoir 2 types de fichiers unified_events dans n'importe quel dossier d'instance Snort donné :

- unified_events-1 (qui contient des événements de haute priorité).
- unified_events-2 (qui contient des événements de faible priorité).

Un événement hautement prioritaire est un événement qui correspond à une connexion potentiellement malveillante.

Types d'événements et leur priorité :

Priorité élevée (1)	Priorité faible (2)
Intrusion	Connexion
Programme malveillant	Découverte
Renseignements De Sécurité	Fichier

Événements de connexion associés	Statistiques

Le résultat suivant montre un événement qui appartient à la nouvelle connexion tracée dans l'exemple précédent. Le format est unified2 et provient de la sortie du journal des événements unifié respectif situé sous [/ngfw]/var/sf/detection_engine/*/instance-**1**/ où 1 est l'ID d'instance snort en gras dans la sortie précédente +1. Le nom du format du journal des événements unifié suit la syntaxe unified_events-**2**.log.**1599654750** où 2 représente la priorité des événements comme indiqué dans le tableau et la dernière partie en gras (**1596547) 0**) est l'horodatage (heure Unix) de la création du fichier.

> **Astuce** : Vous pouvez utiliser la commande Linux **date** pour convertir l'heure Unix en une date lisible :
> admin@FP1120-2:~$ **sudo date -d@1599654750**
> mer 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
```

Àcôté de chaque fichier unified_events se trouve un fichier de signets, qui contient 2 valeurs importantes :

1. Horodatage correspondant au fichier unified_events actuel pour cette instance et cette priorité.
2. Position en octets du dernier événement de lecture dans le fichier unified_event.

Les valeurs sont dans l'ordre, séparées par une virgule, comme indiqué dans cet exemple :

```
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
```

Cela permet au processus du gestionnaire de disques de savoir quels événements ont déjà été

traités (envoyés à FMC) et lesquels n'ont pas été traités.

Notez que lorsque le gestionnaire de disques draine un silo d'événements, il supprime les fichiers d'événements unifiés. Pour plus d'informations sur la purge des silos, consultez la section Gestionnaire de disques.

Un fichier unifié drainé est considéré comme ayant des événements non traités lorsque l'un de ces événements est vrai :

1. L'horodatage du signet est inférieur à l'heure de création du fichier.
2. L'horodatage du signet est identique à l'heure de création du fichier et la position en octets du fichier est inférieure à sa taille.

Le processus EventHandler lit les événements des fichiers unifiés et les transmet au FMC (sous forme de métadonnées) via sftunnel, qui est le processus responsable de la communication cryptée entre le capteur et le FMC. Il s'agit d'une connexion TCP, de sorte que le FMC accuse réception de la transmission des événements

Vous pouvez voir ces messages dans le fichier [/ngfw]/var/log/messages :

```
sfpreproc:OutputFile [INFO] *** Opening /ngfw/var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478 for output" in /var/log/messages

EventHandler:SpoolIterator [INFO] Opened unified event file /var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478

sftunneld:FileUtils [INFO] Processed 10334 events from log file var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478
```

Cette sortie fournit les informations suivantes :

- Snort a ouvert le fichier unified_events pour la sortie (pour y écrire).
- Le gestionnaire d'événements a ouvert le même fichier unified_events (pour le lire).
- sftunnel a signalé le nombre d'événements traités à partir de ce fichier unified_events.

Le fichier de signet est alors mis à jour en conséquence. Le sftunnel utilise 2 canaux différents appelés Unified Events (UE) Channel 0 et 1 pour les événements de priorité haute et basse respectivement.

Avec la commande CLI **sfunnel_status** sur le FTD, vous pouvez voir le nombre d'événements qui ont été diffusés.

```
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
```

Dans le FMC, les événements sont reçus par le processus SFDataCorrelator.

L'état des événements qui ont été traités à partir de chaque capteur peut être vu avec la commande **stats_unified.pl** :

```
admin@FMC:~$ sudo stats_unified.pl
Current Time - Fri Sep 9 23:00:47 UTC 2020

********************************************************************************
* FTD - 60a0526e-6ddf-11ea-99fa-89a415c16717, version 6.6.0.1
********************************************************************************
 Channel Backlog Statistics (unified_event_backlog)
   Chan    Last Time              Bookmark Time          Bytes Behind
      0    2020-09-09 23:00:30    2020-09-07 10:41:50               0
      1    2020-09-09 23:00:30    2020-09-09 22:14:58            6960
```

Cette commande montre l'état du journal des événements pour un certain périphérique par canal, l'ID de canal utilisé est le même que le sftunnel.

La valeur Bytes Behind peut être calculée comme la différence entre la position affichée dans le fichier de signet d'événement unifié et la taille du fichier d'événement unifié, plus tout fichier suivant dont l'horodatage est supérieur à celui du fichier de signet.

Le processus SFDataCorrelator stocke également des statistiques de performances, qui sont enregistrées dans **/var/sf/rna/correlator-stats/**. Un fichier est créé par jour pour stocker les statistiques de performances de cette journée au format CSV. Le nom du fichier utilise le format « **AAAA-MM-JJ** » et le fichier correspondant au jour actuel est appelé **maintenant**.

Les statistiques sont collectées toutes les 5 minutes (il y a une ligne par intervalle de 5 minutes).

La sortie de ce fichier peut être lue avec la commande **perfstats**. Notez que cette commande est également utilisée pour lire les fichiers de statistiques de performances de snort, de sorte que les indicateurs appropriés doivent être utilisés :

-C : Indique perfstats que l'entrée est un fichier correlator-stats (sans cet indicateur perfstats suppose que l'entrée est un fichier de statistiques de performances Snort).

-q : Mode silencieux, imprime uniquement le résumé du fichier.

```
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
```

Chaque ligne du résumé comporte 3 valeurs dans l'ordre suivant : Moyenne, Minimum, Maximum.

Si vous imprimez sans l'indicateur -q, vous voyez également les valeurs de l'intervalle de 5 minutes. Le résumé est affiché à la fin.

Notez que chaque FMC a un débit maximal décrit dans sa fiche technique. La table suivante contient les valeurs par module tirées de la feuille de données correspondante :

Modèle	FMC 750	FMC 1000	FMC 1600	FMC 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMC
Débit maximal (ips)	2000	5000	5000	12000	12000	12000	20000	20000	20000	Variable	12

Notez que ces valeurs concernent l'agrégation de tous les types d'événements indiqués en gras dans le résultat des statistiques SFDataCorrelator.

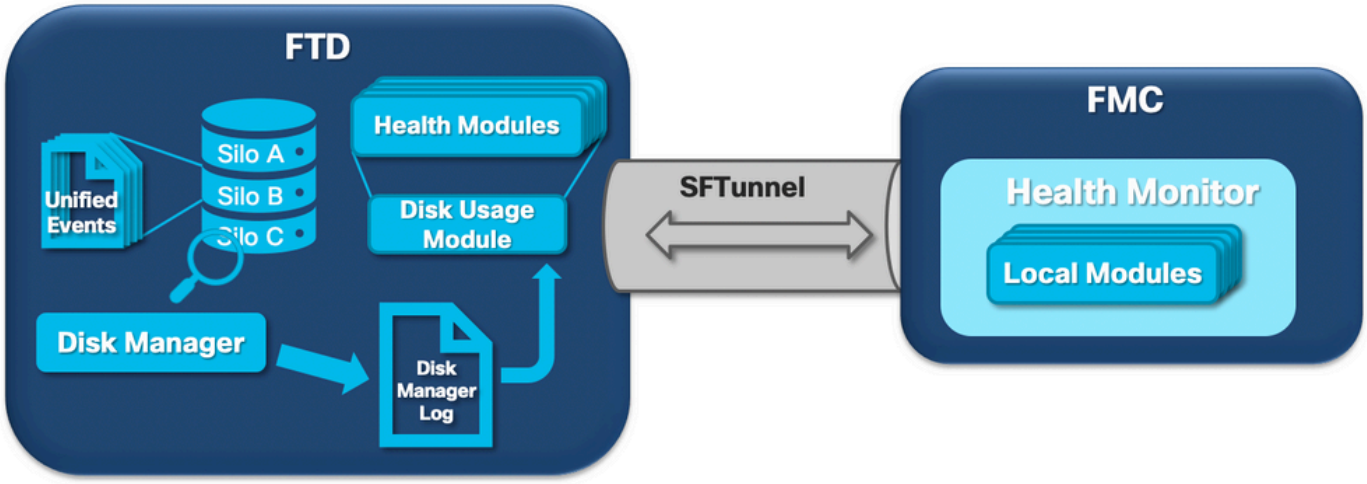
Si vous regardez le résultat et que nous dimensionnons notre FMC de telle manière que nous sommes préparés au pire scénario (lorsque toutes les valeurs maximales se produisent en même temps), alors le taux d'événements que ce FMC voit est de 48,65 + 348,15 + 4,63 + 3,25 + 0,06 = **404,74 ips**.

Cette valeur totale peut être comparée à la valeur de la feuille de données du modèle correspondant.

Le SFDataCorrelator peut également effectuer un travail supplémentaire sur les événements reçus (comme pour les règles de corrélation), puis les stocke dans la base de données qui est interrogée pour remplir diverses informations dans l'interface utilisateur graphique (GUI) de FMC, telles que les tableaux de bord et les vues d'événements.

Gestionnaire de disques

Le schéma logique suivant présente les composants logiques des processus **Health Monitor** et **Disk Manager** car ils sont interconnectés pour la génération d'alertes d'intégrité liées au disque.



En bref, le gestionnaire de disque gère l'utilisation du disque de la boîte et ses fichiers de configuration se trouvent dans le dossier [/ngfw]/etc/sf/. Il existe plusieurs fichiers de configuration

pour le processus du gestionnaire de disques qui sont utilisés dans certaines circonstances :

- diskmanager.conf - Fichier de configuration standard.
- diskmanager_2hd.conf : utilisé lorsque le boîtier comporte 2 disques durs installés. Le deuxième disque dur est celui associé à l'extension Malware, utilisée pour stocker les fichiers tels que définis dans la politique de fichiers.
- ramdisk-diskmanager.conf : utilisé lorsque l'option Log to Ramdisk est activée. Pour plus d'informations, consultez la section Log to Ramdisk.

Un silo est attribué à chaque type de fichier surveillé par le gestionnaire de disques. En fonction de la quantité d'espace disque disponible sur le système, le gestionnaire de disques calcule un seuil supérieur (HWM) et un seuil inférieur (LWM) pour chaque silo.

Lorsque le processus du gestionnaire de disques draine un silo, il le fait jusqu'au point où le LWM est atteint. Comme les événements sont drainés par fichier, ce seuil peut être franchi.

Pour vérifier l'état des silos sur un périphérique capteur, vous pouvez utiliser cette commande :

```
> 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
```

Le processus du gestionnaire de disques s'exécute lorsque l'une des conditions suivantes est remplie :

- Le processus démarre (ou redémarre)
- Un silo atteint le HWM
- Un silo est drainé manuellement
- Une fois par heure

Chaque fois que le processus du gestionnaire de disques s'exécute, il génère une entrée pour chacun des différents silos sur son propre fichier journal qui se trouve sous [/ngfw]/var/log/diskmanager.log et contient des données au format CSV.

Ensuite, une ligne d'exemple du fichier diskmanager.log, tirée d'un capteur qui a déclenché le drainage des événements non traités de l'alerte d'intégrité des événements de priorité faible unifiée, ainsi que la répartition des colonnes respectives :

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

93392,110,0

Colonne	Valeur
Étiquette Silo	priority_2_events
Heure de drainage (Heure d'époque)	1599668981
Nombre de fichiers drainés	221
Octets drainés	4587929508
Taille actuelle des données après le drainage (octets)	1132501868
Fichier le plus volumineux drainé (octets)	20972020
Plus petit fichier drainé (octets)	4596
Fichier le plus ancien drainé (époque)	1586044534
Filigrane supérieur (octets)	5710966962
Filigrane bas (octets)	1142193392
Nombre de fichiers avec des événements non traités drainés	110
Indicateur d'état Diskmanager	0

Ces informations sont ensuite lues par le module Health Monitor correspondant pour déclencher l'alerte d'état correspondante.

Égoutter manuellement un silo

Dans certains scénarios, vous pouvez drainer manuellement un silo. Par exemple, pour libérer de l'espace disque avec une vidange manuelle du silo au lieu de la suppression manuelle des fichiers, le gestionnaire de disques a l'avantage de décider quels fichiers conserver et quels fichiers supprimer. Le gestionnaire de disques conserve les fichiers les plus récents pour ce silo.

N'importe quel silo peut être vidé et cela fonctionne comme décrit précédemment (le gestionnaire de disques vidange les données jusqu'à ce que la quantité de données passe sous le seuil LWM). La commande **system support silo-drain** est disponible en mode FTD CLISH et fournit une liste des silos disponibles (nom + id numérique).

Voici un exemple de drainage manuel du silo d'événements Unified de faible priorité :

```
> 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

Voici les principaux points :

- Toute alerte d'intégrité vue sur le FMC dans le menu Health Monitor ou sous l'onglet Health du centre de messages est générée par le processus Health Monitor.
- Ce processus surveille l'état du système, à la fois pour le FMC et les capteurs gérés, et il est composé d'un certain nombre de modules différents.
- Les modules d'alerte d'intégrité sont définis dans la politique d'intégrité qui peut être attachée

par périphérique.
- Les alertes d'intégrité sont générées par le module d'utilisation des disques qui peut s'exécuter sur chacun des capteurs gérés par le FMC.
- Lorsque le processus Health Monitor sur le FMC s'exécute (une fois toutes les 5 minutes ou lorsqu'une exécution manuelle est déclenchée), le module d'utilisation des disques examine le fichier diskmanager.log et, si les conditions correctes sont remplies, l'alerte d'intégrité correspondante est déclenchée.

Pour qu'une alerte d'état **Drain of Unprocessing events** soit déclenchée Toutes ces conditions doivent être vraies :

1. Le champ Octets drainés est supérieur à 0 (ce qui indique que les données de ce silo ont été drainées).
2. Nombre de fichiers avec des événements non traités drainés supérieur à 0 (cela indique qu'il y avait des événements non traités dans les données drainées).
3. L'heure du drainage se situe dans la dernière heure.

Pour qu'une alerte **d'évacuation fréquente des événements** soit déclenchée, ces conditions doivent être vraies :

1. Les 2 dernières entrées du fichier diskmanager.log doivent : Le champ Octets drainés est supérieur à 0 (ce qui indique que les données de ce silo ont été drainées).Soyez à moins de 5 minutes d'intervalle.
2. L'heure de vidange de la dernière entrée de ce silo se situe dans la dernière heure.

Le collecteur de résultats du module d'utilisation du disque (ainsi que les résultats collectés par les autres modules) sont envoyés au FMC via sftunnel. Vous pouvez voir les compteurs pour les événements d'intégrité échangés sur sftunnel avec la commande **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
```

Se connecter à Ramdisk

Même si la plupart des événements sont stockés sur le disque, le périphérique est configuré par défaut pour se connecter à ramdisk afin d'éviter des dommages graduels au disque SSD qui peuvent être causés par des écritures et des suppressions constantes d'événements sur le disque.

Dans ce scénario, les événements ne sont pas stockés sous **[/ngfw]/var/sf/detection_engine/*/instance-N/,** mais ils sont situés dans **[/ngfw]/var/sf/detection_engine**/*/**instance-N/connection/**, qui est un lien symbolique vers **/dev/shm/instance-N/connection.** Dans ce cas, les événements résident dans la mémoire virtuelle plutôt que dans la mémoire physique.

```
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
```

Pour vérifier ce que le périphérique est actuellement configuré pour faire, exécutez la commande **show log-events-to-ramdisk** à partir de FTD CLISH. Vous pouvez également modifier ce paramètre si vous utilisez la commande **configure log-events-to-ramdisk <enable/disable> :**

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

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

> **Avertissement :** Lorsque la commande « configure log-events-to-ramdisk disable » est exécutée, il est nécessaire d'effectuer deux déploiements sur le FTD pour que snort ne soit pas bloqué dans l'état « D » (Uninterruptible Sleep), ce qui provoquerait une interruption du trafic.
> Ce comportement est documenté dans le défaut avec l'ID de bogue Cisco CSCvz53372.
> Avec le premier déploiement, la réévaluation de l'étape de mémoire de snort est ignorée, ce qui entraîne le passage de snort à l'état "D", la solution de contournement est de faire un autre déploiement avec toutes les modifications factices.

Lorsque vous vous connectez à ramdisk, le principal inconvénient est que le silo respectif a un espace alloué plus petit et les draine donc plus souvent dans les mêmes circonstances. La sortie suivante est le gestionnaire de disques d'un FPR 4140 avec et sans les événements de journal à ramdisk activé pour la comparaison.

Connexion à Ramdisk activée

```
> 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 to Ramdisk désactivé

```
> 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

La plus petite taille du silo est compensée par la vitesse plus élevée pour accéder aux Événements et les diffuser au FMC. Bien qu'il s'agisse d'une meilleure option dans de bonnes conditions, l'inconvénient doit être considéré.

Foire aux questions (FAQ)

Les alertes d'intégrité Drain of Events sont-elles uniquement générées par les événements de connexion ?

No.

- Les alertes de drainage fréquent peuvent être générées par n'importe quel silo du gestionnaire de disques.
- Les alertes de drainage d'événements non traités peuvent être générées par n'importe quel silo lié à l'événement.

Les événements de connexion sont les plus courants.

Est-il toujours conseillé de désactiver Log to Ramdisk lorsqu'une alerte d'intégrité de drainage fréquent est détectée ?

Non. Uniquement dans les scénarios de consignation excessive, à l'exception de DOS/DDOS, lorsque le silo affecté est le silo Événements de connexion, et uniquement dans les cas où il n'est pas possible de régler davantage les paramètres de consignation.

Si DOS/DDOS entraîne une consignation excessive, la solution consiste à mettre en oeuvre une protection DOS/DDOS ou à éliminer la ou les sources des attaques DOS/DDOS.

La fonctionnalité par défaut "Log to Ramdisk" réduit l'usure du SSD, il est donc fortement recommandé de l'utiliser.

Que constitue un événement non traité ?

Les événements ne sont pas marqués individuellement comme non traités. Un fichier comporte des événements non traités lorsque :

Son horodatage de création est supérieur au champ d'horodatage du fichier de signet correspondant.

ou

Son horodatage de création est égal au champ d'horodatage dans le fichier de signet respectif et sa taille est supérieure à la position dans le champ d'octets sur le fichier de signet respectif.

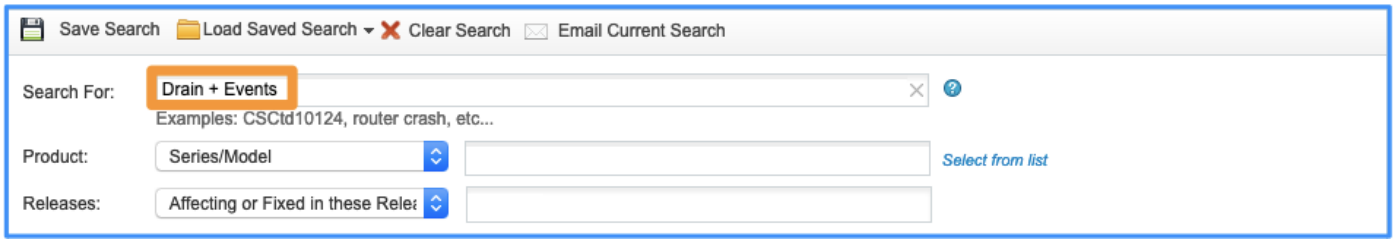
Comment le FMC connaît-il le nombre d'octets en retard pour un capteur particulier ?

Le capteur envoie des métadonnées sur le nom et la taille du fichier unified_events ainsi que sur les informations des fichiers de signets, ce qui donne au FMC suffisamment d'informations pour calculer les octets derrière comme :

Taille actuelle du fichier **unified_events** - **Position en octets"** du fichier de signet + Taille de tous les fichiers unified_events dont l'horodatage est supérieur à celui du fichier de signet correspondant.

Problèmes identifiés

Ouvrez l'[Outil de recherche de bogues] et utilisez cette requête :



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.