أستكشاف أخطاء عملية إستنزاف أحداث FMC التي لم تتم معالجتها والاستنزاف المتكرر لأحداث تنبيهات Health Monitor

المحتويات

المقدمة

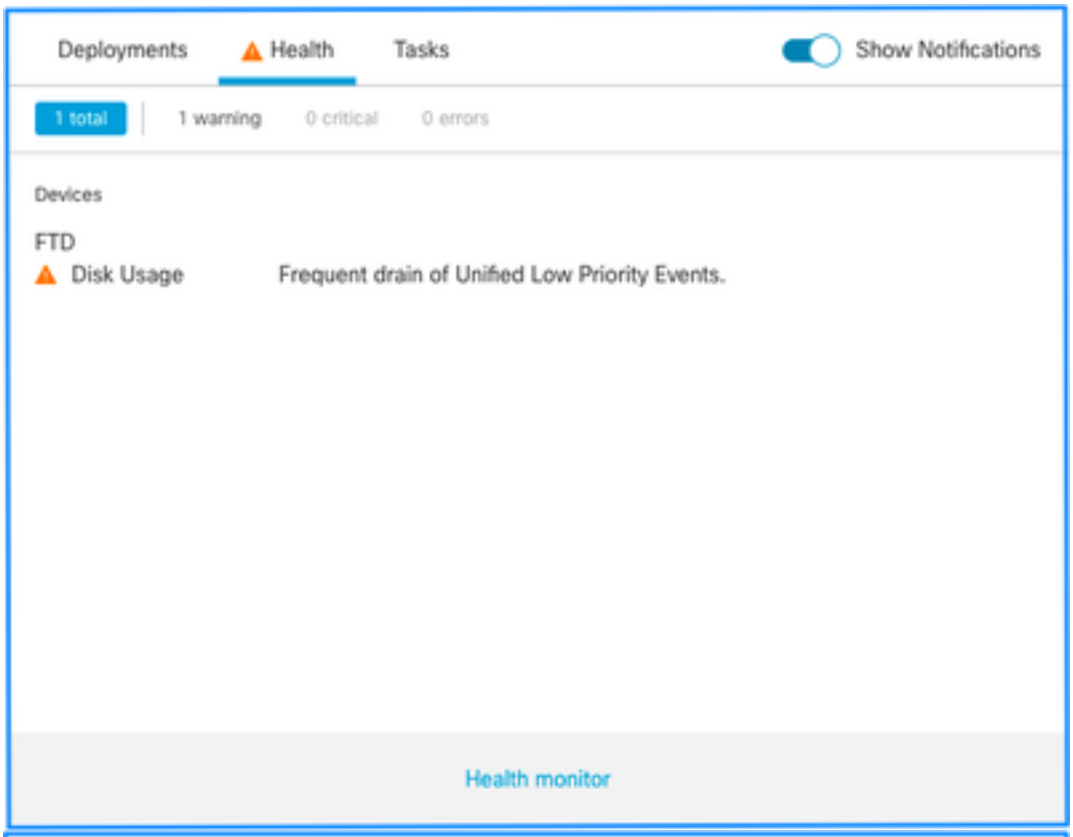
يوضح هذا المستند كيفية أستكشاف أخطاء **إستنزاف الأحداث غير المعالجة** و**التنبيهات** الصحية **المتكررة للأحداث** في مركز إدارة FirePOWER (FMC) وإصلاحها.

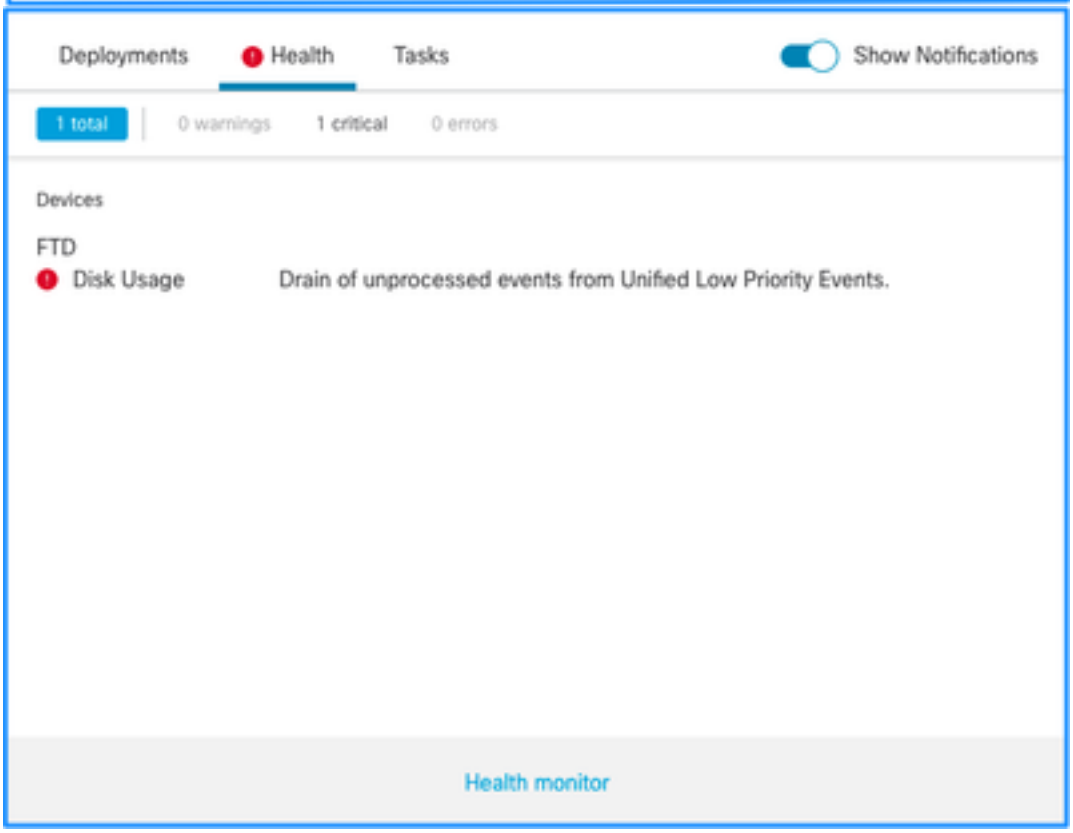
نظرة عامة على المشكلة

تقوم FMC بإنشاء أحد هذه التنبيهات الصحية:

- الإستنزاف المتكرر للأحداث الموحدة ذات الأولوية المنخفضة
  و/أو
- إستبعاد الأحداث غير المعالجة من الأحداث الموحدة ذات الأولوية المنخفضة

على الرغم من إنشاء هذه الأحداث وإظهارها على وحدة التحكم في إدارة الأجهزة (FMC)، إلا أنها تتعلق بمستشعر جهاز مدار سواء كان جهاز دفاع ضد تهديد الطاقة النارية (FTD) أو جهاز من الجيل التالي لنظام منع التسلل (NGIPS). بالنسبة لبقية هذا المستند، يشير مصطلح مستشعر إلى كل من أجهزة FTD و NGIPS على حد سواء ما لم يتم تحديد خلاف ذلك.





هذا هو هيكل التنبيه الصحيح:

- إستنزاف متكرر لـ <SILO Name>
- إستنزاف الأحداث التي لم تتم معالجتها من <اسم المخزن المؤقت>

في هذا المثال، يكون اسم المجال **أحداث موحدة ذات أولوية منخفضة**. هذا أحد خيارات إدارة الأقراص (راجع قسم "معلومات الخلفية" للحصول على شرح أكثر شمولا).

بالإضافة إلى ذلك:

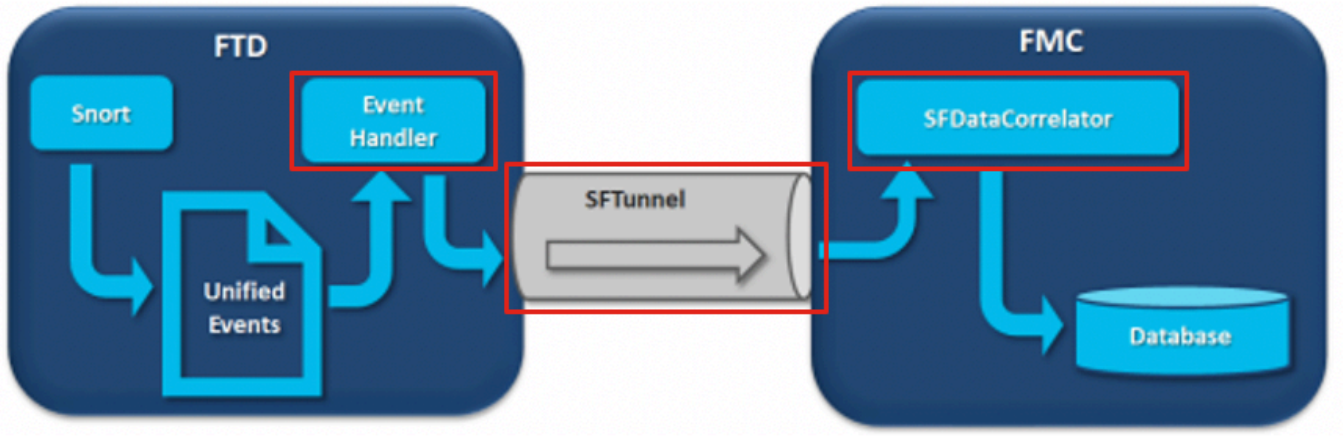
- على الرغم من أن أي مخزن يمكنه من الناحية التقنية توليد إستنزاف متكرر للتنبيه الصحي <SILO Name> فإن أكثر التنبيهات شيوعا هي تلك المتعلقة بالأحداث، ومن بينها، الأحداث ذات الأولوية المنخفضة بسبب أن هذه هي نوع الأحداث التي تولدها أجهزة الاستشعار في كثير من الأحيان.
- ينطوي حدث "إستنزاف متكرر ل <SILO NAME>" على خطورة التحذير في الحالة التي يكون فيها صوامع مرتبطة بالحدث لأنه، إذا تم معالجة ذلك (يتم بعد ذلك تقديم شرح حول ما يشكل حدثا لم تتم معالجته)، فإنه يكون في قاعدة بيانات FMC.
- بالنسبة لوحدة صوامع غير مرتبطة بالأحداث، مثل صوامع "النسخ الاحتياطية"، يكون التنبيه حيويا نظرا لفقدان هذه المعلومات.
- تقوم صوامع نوع الحدث فقط بإنشاء إستنزاف للأحداث التي لم تتم معالجتها من تنبيه صحة <SILO NAME>. يكون لهذا التنبيه دوما خطورة حرجة.

الأعراض الإضافية يمكن أن تشمل:

- بطء واجهة مستخدم FMC
- الخسائر في الأحداث

سيناريوهات أستكشاف الأخطاء وإصلاحها الشائعة

ينتج إستنزاف متكرر لحدث <SILO NAME> عن إدخال كمية كبيرة جدا من المخزن لحجمه. في هذه الحالة، تقوم إدارة الأقراص بتصفية (عمليات إزالة) الملف مرتين على الأقل في آخر 5 دقائق من الفاصل الزمني. في مخازن نوع الحدث، يحدث ذلك عادة بسبب التسجيل المفرط لنوع الحدث هذا. في حالة إستنزاف الأحداث غير المعالجة الخاصة بالتنبيه الصحي ل <SILO NAME>، يمكن أن يحدث ذلك أيضا بسبب حدوث إزدحام في مسار معالجة الحدث.



في الرسم البياني هناك 3 إختناقات محتملة:

- تم زيادة الاشتراك في عملية EventHandler على FTD (يتم قراءتها بشكل أبطأ من ما يكتبه Snort)
- تم زيادة الاشتراك في واجهة Eventing
- تم زيادة الاشتراك في عملية SFDataCorrelator على FMC

لفهم بنية معالجة الحدث بشكل أعمق، راجع قسم الغوص العميق الخاص.

القضية 1. التسجيل المفرط

وكما ذكر في القسم السابق، فإن أحد أكثر الأسباب شيوعا للتنبيهات الصحية من هذا

النوع وه الإدخال المفرط.

الفرق بين عالمة العامل المنخفضة (LWM) وعالمة العامل المرتفعة (HWM) التي تم تجميعها من أمر CLISH **show** لإدارة **الأرشيف** يوضح مقدار المساحة التي يلزم أخذها على ذلك الصوامع للانتقال من LWM (المصروف حديثا) إلى قيمة HWM. إذا كانت هناك أحداث كثيرة غير معالجة (بأحداث غير معالجة أو بدونها) فإن أول شيء يجب مراجعته وه تكوين التسجيل.

للحصول على شرح متعمق لعملية إدارة الأرشيف، ارجع إلى قسم الغوص العميق الخاص بها.

سواء كان التسجيل المزدوج أو مجرد معدل مرتفع للأحداث على نظام الإدارة - الاستشعار البيئي العام يجب القيام بمراجعة إعدادات التسجيل.

الإجراءات الموصى بها

الخطوة 1. التحقق من التسجيل المزدوج

يمكن تحديد سيناريوهات التسجيل المزدوج إذا قمت بالنظر إلى **معجزات** الموصلات على FMC كما وه موضح في هذا الإخراج:

```
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
```

في هذه الحالة، يمكن رؤية معدل مرتفع من التدفقات المكررة في المخرجات.

الخطوة 2. مراجعة إعدادات التسجيل لـ ACP

يجب أن تبدأ بمراجعة إعدادات التسجيل لنهج التحكم في الوصول (ACP). تأكد من اتباع أفضل الممارسات الموضحة في هذا المستند وهي أفضل ممارسات تسجيل الاتصال

من المستحسن مراجعة إعدادات التسجيل في جميع الحالات لأن التوصيات المدرجة لا تغطي سيناريوهات التسجيل المزدوج فقط.

الخطوة 3. التحقق مما إذا كان التسجيل المفرط متوقعا أم لا

يجب مراجعة ما إذا كان التسجيل المفرط له سبب متوقع أم لا. إذا كان التسجيل الزائد بسبب هجوم DoS/DDoS أو حلقة توجيه أو تطبيق/مضيف معين يقوم بعدد كبير من الاتصالات، فيجب التحقق من الاتصالات وتخفيفها/إيقافها من مصدر الاتصال الزائدة غير المتوقعة.

الخطوة 4. نموذج الترقية

ترقية جهاز FTD إلى طراز أداء أعلى (على سبيل المثال FPR2100 —> FPR4100)، وسيزداد مصدر المخزن المؤقت.

الخطوة 5. ضع في الاعتبار ما إذا كان يمكنك تعطيل تسجيل الدخول إلى Ramdisk

في حالة وجود مخزن ألحاث الموحد ذي الأولوية المنخفضة، يمكنك تعطيل تسجيل الدخول إلى Ramdisk لزيادة حجم الصوامع ظهور العيوب التي تمت مناقشتها في قسم إلغوص العميق الخاص.

القضية 2. نقطة إختناق في قناة الاتصال بين المستشعر و FMC

سبب آخر مشترك لهذا النوع من التنبيه هو مشاكل الاتصال و/أو عدم الاستقرار في قناة الاتصال (sftunnel) بين المستشعر و FMC. يمكن أن تكون مشكلة الاتصال بسبب:

- SFtunnel معطل أو غير مستقر (FLAPS).
- تم تجاوز الاشتراك في SFtunnel.

بالنسبة إلى مشكلة اتصال SFTUNNEL، تأكد من أن وحدة التحكم في الإدارة الأساسية (FMC) والمستشعر يمكن الوصول إليهما بين واجهات الإدارة الخاصة بهما على منفذ TCP 8305.

على FTD أنت يستطيع بحث عن **sftunneld** خيط في ال **[/ngfw]/var/log/messages** مبرد. تتسبب مشاكل الاتصال في إنشاء رسائل مثل هذه:

```
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
```

يمكن أن يكون الاشتراك الزائد لواجهة إدارة FMCs طفرة في حركة مرور الإدارة أو اشتراك زائد لذاكرة الوصول العشوائي. وتشكل البيانات التاريخية المستمدة من تقرير هيث مونيتور مؤشرا جيدا لهذا.

الشيء الأول الذي تجدر الإشارة إليه هو أنه في معظم الحالات يتم نشر وحدة التحكم في إدارة الوحدة الأساسية (FMC) باستخدام بطاقة واجهة شبكة (NIC) واحدة للإدارة. يتم إستخدام هذه الواجهة ل:

- إدارة FMC.
- إدارة مستشعر FMC.
- مجموعة أحداث FMC من أجهزة الاستشعار.
- تحديث موجز ويب المعلومات الإستخباراتية.
- تنزيل تحديثات SRU و Software و VDB و GeoDB من موقع تنزيل البرامج.
- الاستعلام عن سمعات URL وفئاته (إن أمكن).
- الاستعلام الخاص بعمليات توزيع الملفات (إن أمكن).

الإجراءات الموصى بها

يمكنك نشر بطاقة واجهة شبكة (NIC) ثانية على وحدة التحكم في إدارة الوحدة الأساسية (FMC) من أجل واجهة مخصصة للحدث. يمكن أن تعتمد عمليات التنفيذ على حالة الاستخدام.

يمكن العثور على إرشادات عامة في دليل أجهزة FMC الذي يتم نشره على شبكة الإدارة

القضية 3. خلل في عملية SFDataCorrelator

السيناريو الأخير الذي يجب تغطيته هو عند حدوث الاختناق على جانب SFDataCorrelator (FMC).

تتمثل الخطوة الأولى في النظر في ملف diskmanager.log نظرا لوجود معلومات مهمة يتعين تجميعها مثل:

- تردد عملية إستنزاف المياه.
- عدد الملفات ذات الأحداث التي لم تتم معالجتها التي تم تسريبها.
- حدوث عملية إستنزاف مع أحداث لم تتم معالجتها.

للحصول على معلومات حول ملف diskmanager.log وكيفية تفسيره، يمكنك الرجوع إلى قسم إدارة الأقراص. يمكن إستخدام المعلومات التي تم تجميعها من diskmanager.log للمساعدة على تقليل الخطوات التالية.

وبالإضافة إلى ذلك، تحتاج إلى الاطلاع على إحصائيات أداء المشرف:

```
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
```

لاحظ أن هذه الإحصائيات خاصة بوحدة إدارة الاتصالات الفيدرالية (FMC) وهي تتوافق مع تجميع كل أجهزة الاستشعار التي تديرها. في حالة الأحداث الموحدة المنخفضة الأولوية التي تبحث عنها بشكل رئيسي:

- إجمالي التدفقات في الثانية من أي نوع حدث لتقييم الاشتراك الزائد المحتمل لعملية SFDataCorrelator.
- الصفان المبرزان في المخرج السابق: **تدفقات الرنا/الثانية** - يشير إلى معدل الأحداث ذات الأولوية المنخفضة التي تمت معالجتها بواسطة SFDataCorrelator.**تدفقات RNA dup/الثانية** - يشير إلى معدل الأحداث المكررة ذات الأولوية المنخفضة التي تمت معالجتها بواسطة SFDataCorrelator. يتم إنشاء ذلك عن طريق التسجيل المزدوج كما هو موضح في السيناريو السابق.

استنادا إلى النتائج، يمكن الاستنتاج بما يلي:

- لا يوجد تسجيل متكرر كما هو موضح بواسطة تدفقات RNA الإضافية/الصف الثاني.
- في تدفقات الرنا/الصف الثاني، تكون القيمة القصوى أعلى بكثير من القيمة المتوسطة لذلك كان هناك إرتفاع في معدل الأحداث التي تمت معالجتها بواسطة عملية SFDataCorrelator. قد يكون هذا متوقعا إذا ما نظرت إلى هذا الصباح الباكر عندما يكون يوم عمل المستخدمين قد بدأ للتو، ولكنه بشكل عام، علم أحمر ويتطلب مزيدا من البحث.

يمكن العثور على مزيد من المعلومات حول عملية SFDataCorrelator ضمن قسم [معالجة الأحداث](#).

الإجراءات الموصى بها

الوا، يلزمكم ان تحددوا متى حدث المسمار. للقيام بذلك، تحتاج إلى النظر في إحصائيات المشرف لكل عينة فاصل زمني مدته 5 دقائق. يمكن أن تساعدك المعلومات التي تم جمعها من diskmanager.log على الوصول مباشرة إلى الإطار الزمني المهم.

تلميح: انقل الإخراج إلى جهاز الندا **من** ليونكس بحيث يمكنك البحث بسهولة.

```
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
```

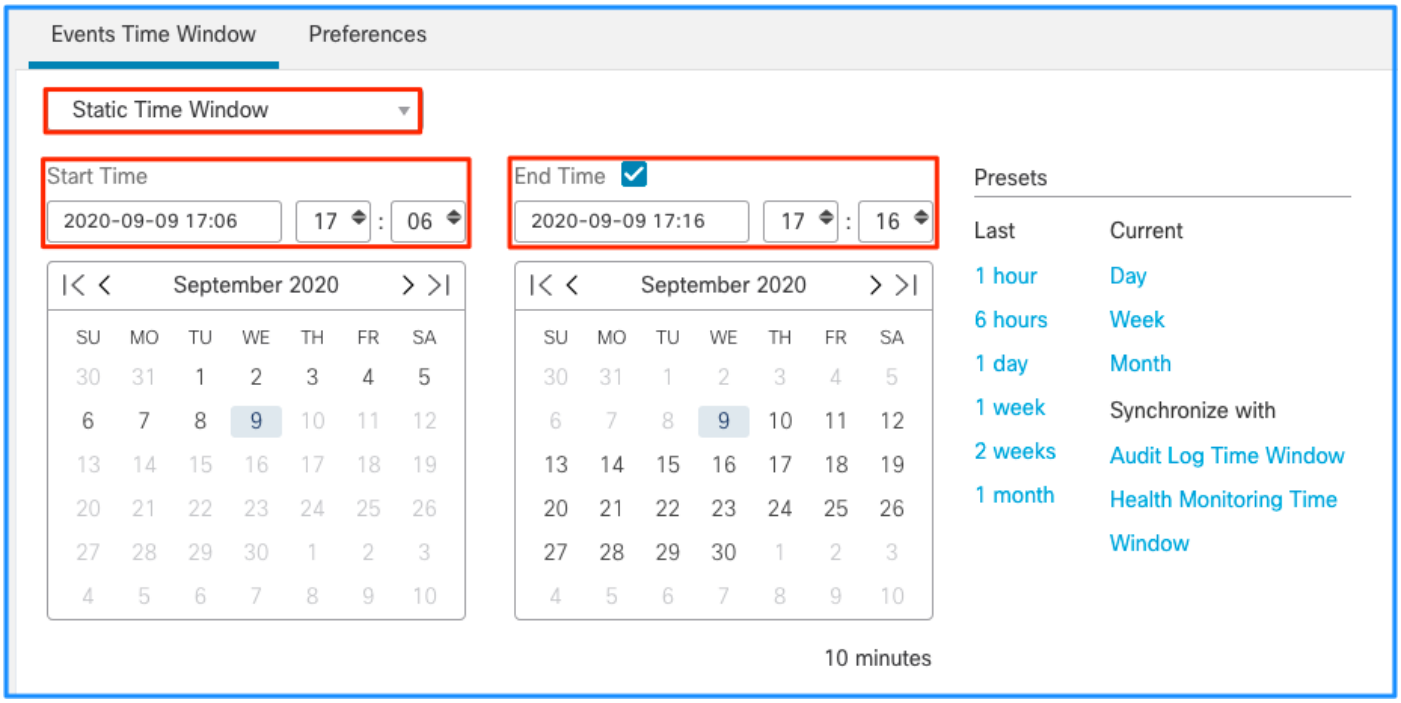
```
host limit:                     50000           0               50000
pcnt host limit in use:         100.01          100.00          100.55
rna events/second:              1.78            0.00            48.65
user cpu time:                  2.14            0.11            58.20
system cpu time:                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
```

أستخدم المعلومات الموجودة في الإخراج إلى:

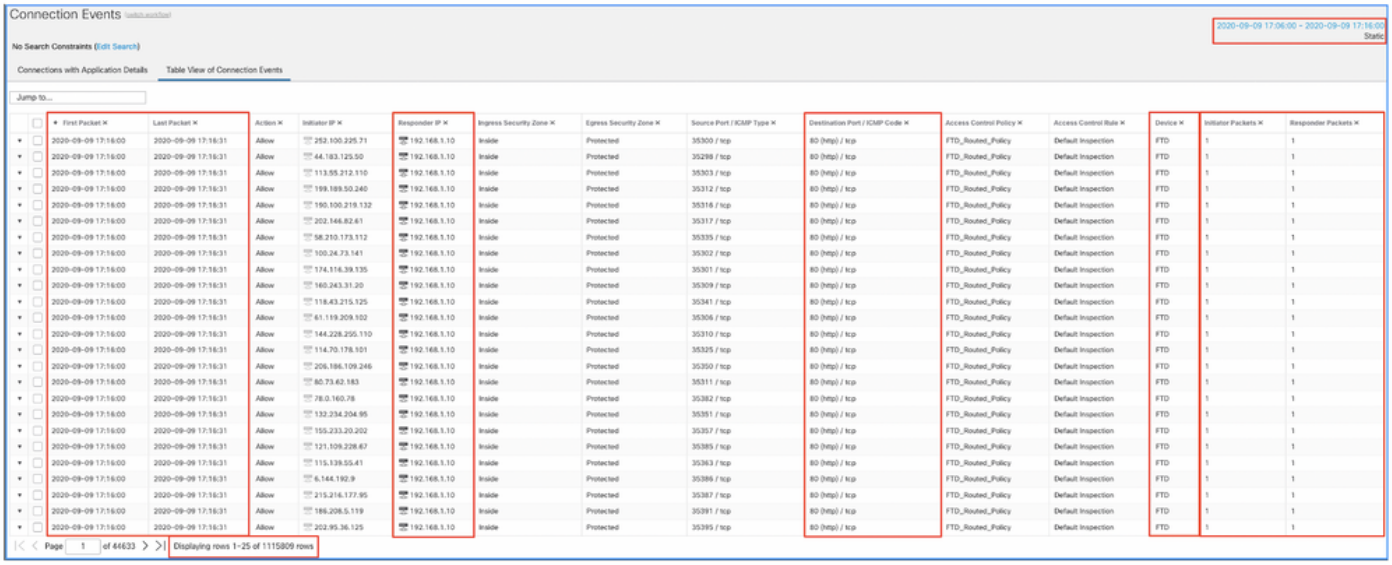
- تحديد المعدل العادي/الأساسي للأحداث.
- حدد فترة الخمس دقائق التي حدث فيها الارتفاع.

في المثال السابق، هناك إرتفاع واضح في معدل الأحداث التي تم تلقيها في الساعة 16:06:39 وما بعدها. لاحظ أن هذه المعدلات تبلغ 5 دقائق بحيث يمكن أن تكون الزيادة أكثر فجائية مما هو موضح (انفجار) ولكن أقل خلال فترة الخمس دقائق هذه إذا بدأت مع نهاية الفترة.

على الرغم من أن هذا يؤدي إلى الاستنتاج بأن هذا الارتفاع الحاد في الأحداث تسبب في إستنزاف الأحداث غير المعالجة، يمكنك إلقاء نظرة على أحداث الاتصال من واجهة المستخدم الرسومية (GUI) الخاصة ب FMC باستخدام الإطار الزمني المناسب لفهم نوع الاتصالات التي مرت عبر مربع FTD في هذا الارتفاع الحاد:



تطبيق هذا الإطار الزمني للحصول على أحداث الاتصال التي تمت تصفيتها، لا تنس حساب المنطقة الزمنية. في هذا المثال، يستخدم المستشعر تقنية UTC و FMC UTC+1. أستخدم "طريقة عرض الجدول" لعرض الأحداث التي أدت إلى الحمل الزائد للأحداث واتخاذ الإجراء وفقا لذلك:



استنادا إلى الطوابع الزمنية (وقت الحزمة الأولى والأخيرة) يمكن ملاحظة أن هذه هي إتصالات قصيرة العمر. علاوة على ذلك، تظهر أعمدة حزم البادئ والمستجيب أنه كان هناك حزمة واحدة فقط يتم تبادلها في كل إتجاه. وهذا يؤكد أن الوصلات كانت قصيرة الأجل ولم تتبادل سوى بيانات قليلة جدا.

أنت يستطيع أيضا رأيت أن كل هذا دفق يستهدف نفس مستجيب IPs ومنفذ. أيضا، يتم الإبلاغ عنها كلها من قبل نفس المستشعر (الذي يجانب معلومات واجهة الدخول والخروج يمكن أن تتحدث إلى مكان واتجاه هذه التدفقات). إجراءات إضافية:

- تحقق من Syslogs على نقطة نهاية الوجهة.
- تنفيذ الحماية ضد رفض الخدمة (DoS)/رفض الخدمة (DoS)، أو إتخاذ تدابير وقائية أخرى.

ملاحظة: الغرض من هذه المقالة هو توفير مبادئ توجيهية لاستكشاف أخطاء إستنفار الأحداث غير المعالجة وإصلاحها. أستخدم هذا المثال hping3 لإنشاء تدفق TCP SYN إلى الخادم الوجهة. للحصول على إرشادات لتعزيز جهاز FTD الخاص بك تحقق من دليل توقيع الدفاع ضد تهديد تهديد FirePOWER من Cisco

العناصر التي سيتم تجميعها قبل الاتصال بمركز المساعدة التقنية (TAC) ل Cisco

ينصح بشدة بجمع هذه العناصر قبل الاتصال ب Cisco TAC:

- لقطة شاشة للتنبيهات الصحية التي تم رؤيتها.
- أستكشاف أخطاء الملف الذي تم إنشاؤه من وحدة التحكم في إدارة الوحة الأساسية (FMC) وإصلاحها.
- أستكشاف أخطاء الملف الذي تم إنشاؤه من أداة الاستشعار المتأثرة وإصلاحها.
- تاريخ ووقت رؤية المشكلة لأول مرة.
- معلومات حول أي تغييرات تم إجراؤها مؤخرا على السياسات (إن أمكن).
- مخرجات الأمر stats_unified.pl كما هو موضح في قسم معالجة الأحداث مع ذكر أجهزة الاستشعار المتأثرة.

التعمّق

يغطي هذا القسم شرحا متعمقا لمختلف المكونات التي يمكن أن تشارك في هذا النوع من

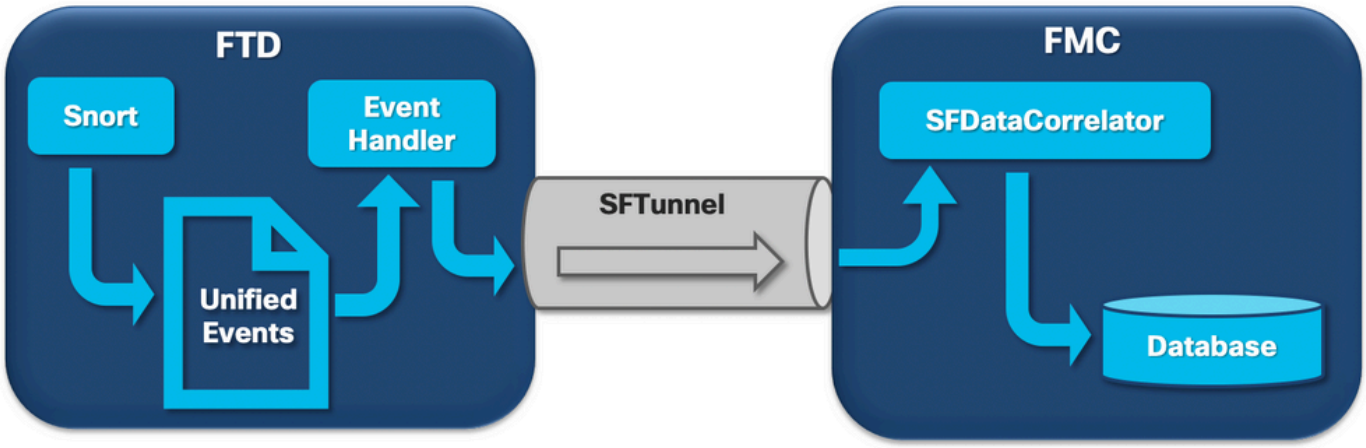
تنبيهات الصحة. ويشمل ذلك ما يلي:

- معالجة الحدث - يغطي أحداث المسار التي يتم تنفيذها على كل من أجهزة الاستشعار ووحدة التحكم في إدارة اللوحة الأساسية (FMC). ويكون هذا مفيدا بشكل رئيسي عندما يشير تنبيه الصحة إلى مخزن نوع الحدث.
- Disk Manager (إدارة الأقراص) - يغطي عملية إدارة الأقراص والصوامع وكيفية تصفيتها.
- Health Monitor - يغطي كيفية إستخدام وحدات Health Monitor لإنشاء تنبيهات الحماية.
- تسجيل إلى RamDisk - يغطي ميزة التسجيل إلى RamDisk وتأثيرها المحتمل على تنبيهات الحماية.

لفهم تنبيهات الحماية الخاصة باستنزاف الأحداث والقدرة على تحديد نقاط الفشل المحتملة، هناك حاجة للنظر في كيفية عمل هذه المكونات والتفاعل فيما بينها.

معالجة الحدث

على الرغم من أنه يمكن تشغيل نوع التنبيهات الصحية "التنزيل المتكرر" بواسطة صوامع غير مرتبطة بالأحداث، إلا أن الغالبية العظمى من الحالات التي تراها Cisco TAC تتعلق بنزوح المعلومات المتعلقة بالحدث. إضافة إلى ذلك، لفهم ما يشكل إنهيارا للأحداث غير المعالجة، هناك حاجة إلى إلقاء نظرة على بنية معالجة الحدث والمكونات التي تتألف منها.



عندما يستقبل مستشعر FirePOWER حزمة من اتصال جديد، تولد عملية الشرخ حدثا بتنسيق Unified2 وهو تنسيق ثنائي يسمح بالقراءة/الكتابة بشكل أسرع بالإضافة إلى الأحداث الأخف.

يعرض الإخراج **تتبع دعم نظام** أوامر FTD حيث يمكنك رؤية اتصال جديد تم إنشاؤه. وتسلط الأضواء على الأجزاء الهامة وتشرح:

```
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
```

يتم إنشاء ملفات snort unified_events لكل مثيل ضمن المسار **[/ngfw]var/sf/detection_engine/*/instance-N/**، حيث:

- ***** هو Snort uid. هذا فريد لكل جهاز.
- **N** هو معرف مثيل Snort الذي يمكن حسابه على أنه معرف المثيل من الإخراج السابق (الذي تم تمييزه بمقدار 0 في المثال) + 1

يمكن أن يكون هناك نوعان من ملفات unified_events في أي مجلد مثيل Snort محدد:

- unified_events-1 (الذي يحتوي على أحداث ذات أولوية عالية).
- unified_events-2 (الذي يحتوي على أحداث ذات أولوية منخفضة).

الحدث ذو الأولوية العالية هو حدث يتوافق مع اتصال ضار محتمل.

أنواع الأحداث وأولوياتها:

أولوية عالية (1)	**أولوية منخفضة (2)**
اقتحام	الاتصال
برمجيات خبيثة	اكتشاف
الاستخبارات الأمنية	FILE
أحداث الاتصال المقترنة	إحصائيات

يعرض الإخراج التالي حدث ينتمي إلى الاتصال الجديد الذي تم تتبعه في المثال السابق. التنسيق موحد 2 وهو مأخوذ من مخرجات سجل الأحداث الموحد الخاص بكل واحد الموجود تحت [/ngfw]/var/sf/detection_engine/*/instance-1/ حيث يكون 1 معرف مثيل الشخير بالخط الداكن في الإخراج السابق +1. يتبع اسم تنسيق سجل الأحداث الموحد بناء الجملة unified_events-**2**.log.1599654750 حيث يمثل إثنان أولوية الأحداث كما هو موضح في الجدول والجزء الأخير بالخط الغامق (**1599654750**) هو الطابع الزمني (وقت Unix) لوقت إنشاء الملف.

> **تلميح**: يمكنك إستخدام **أمر** Linux **date** لتحويل وقت Unix إلى تاريخ يمكن قراءته:
> admin@FP1120-2:~$ **sudo date -d@1599654750**
> سبتمبر المتزوج 9:32:30 ص 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
```

بجانب كل ملف Unified_events، هناك ملف إشارة مرجعية، والذي يحتوي على قيمتين مهمتين:

1. مراسل الطابع الزمني لملف unified_events الحالي لذلك المثيل والأولوية.
2. الموضع بالبايت لحدث القراءة الأخير في ملف unified_event.

يتم فصل القيم بفاصلة كما هو موضح في هذا المثال:

```
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
```

وهذا يسمح لعملية إدارة الأقراص بمعرفة الأحداث التي تمت معالجتها بالفعل (والتي تم إرسالها إلى FMC) والأحداث التي لم تتم معالجتها.

لاحظ أنه عند قيام "إدارة الأقراص" بمسح مخزن الأحداث، فإنها تقوم بإزالة ملفات الأحداث الموحدة. للحصول على مزيد من المعلومات حول عملية تصفية وحدات التخزين، أقرأ قسم "إدارة الأقراص".

يعد الملف الموحد الذي تم إستنزافه يحتوي على أحداث لم تتم معالجتها عندما يكون أحد هذه الأحداث صحيحا:

1. الطابع الزمني للإشارة المرجعية أقل من وقت إنشاء الملف.
2. يكون الطابع الزمني للإشارة المرجعية هو نفس وقت إنشاء الملف والموضع بالبايت في الملف أقل من حجمه.

تقرأ عملية EventHandler الأحداث من الملفات الموحدة وتدفقها إلى FMC (على هيئة بيانات وصفية) عبر SFTUNNEL، وهي العملية المسؤولة عن الاتصال المشفر بين المستشعر و FMC. هذا الاتصال يستند إلى TCP، لذلك يتم التعرف على دفق الحدث بواسطة FMC.

أنت يستطيع رأيت هذا رسالة في ال [/ngfw]/var/log/رسالة مبرد:

```
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
```

يوفر هذا الإخراج المعلومات التالية:

- فتح snort ملف unified_events للمخرجات (للكتابة فيه).
- قام "معالج الأحداث" بفتح الملف unified_events نفسه (للقراءة منه).
- قام sftunnel بالإعلام عن عدد الأحداث التي تمت معالجتها من ملف unified_events هذا.

يتم بعد ذلك تحديث ملف الإشارة المرجعية وفقا لذلك. يستخدم SFtunnel قناتين مختلفتين تدعيان قناة الأحداث الموحدة (UE) 0 و 1 للأحداث ذات الأولوية العالية والمنخفضة على التوالي.

باستخدام أمر واجهة سطر الأوامر (CLI) **sfunnel_status** على FTD، يمكنك رؤية عدد الأحداث التي تم تدفقها.

```
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
```

في FMC يتم إستلام الأحداث بواسطة عملية SFDataCorrelator.

يمكن رؤية حالة الأحداث التي تمت معالجتها من كل مستشعر باستخدام الأمر **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
```

يبدي هذا الأمر الحالة من تراكم أحداث لجهاز معين لكل قناة، القناة id يستعمل لا نفسه بما أن ال sftunnel.

يمكن حساب قيمة وحدات البايت الخلف كفرق بين الموضع الظاهر في ملف الإشارة المرجعية للحدث الموحد وحجم ملف الحدث الموحد، بالإضافة إلى أي ملف تالي ذو طابع زمني أعلى من الملف الموجود في ملف الإشارة المرجعية.

تقوم عملية SFDataCorrelator أيضا بتخزين إحصائيات الأداء، والتي يتم حفظها في **/var/sf/rna/correlator-stats/**. يتم إنشاء ملف واحد في اليوم لتخزين إحصائيات الأداء لذلك اليوم بتنسيق CSV. يستخدم اسم الملف التنسيق **YYYY-MM-DD** ويتم إستدعاء **الآن** مرسل الملف الحالي.

وتجمع الإحصاءات كل 5 دقائق (هناك خط واحد لكل فترة خمس دقائق).

يمكن قراءة مخرجات هذا الملف باستخدام أمر **الأداءات**. الحظ أن هذا الأمر يتم إستخدامه أيضا لقراءة ملفات إحصائيات أداء الشيخ، لذا يجب إستخدام العلامات المناسبة:

-C: يشير المؤشر إلى أن الإدخال هو ملف حالة-إرتباط (بدون هذه العلامة يفترض المؤشر أن الإدخال هو ملف إحصائيات أداء snort).

-Q: وضع الهدوء، يطبع فقط الملخص للملف.

```
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
```

يحتوي كل صف في الملخص على 3 قيم بهذا الترتيب: المتوسط، الحد الأدنى، الحد الأقصى.

إذا قمت بالطباعة بدون علامة -q ستر أيضا قيم الفاصل الزمني لمدة 5 دقائق. يتم عرض الملخص في النهاية.

لاحظ أن كل وحدة تحكم في إدارة الهيكل (FMC) تحتوي على الحد الأقصى لمعدل التدفق الموضح في ورقة البيانات الخاصة بها. يحتوي الجدول التالي على القيم لكل وحدة نمطية مأخوذة من ورقة البيانات ذات الصلة:

الطراز	FMC 750	FMC 1000	FMC 1600	FMC 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMC
الحد الأقصى لمعدل التدفق (FPS)	2000	5000	5000	12000	12000	12000	20000	20000	20000	متغير	12

لاحظ أن هذه القيم خاصة بتجميع جميع أنواع الأحداث الموضحة بالأسود في إخراج إحصائيات SFDataCorrelator.

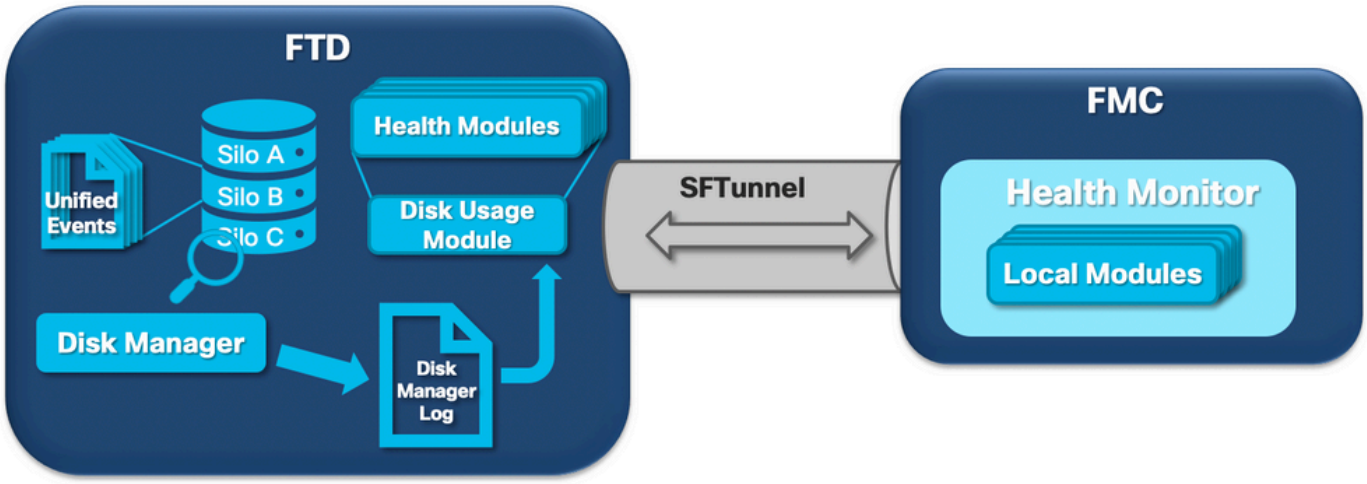
إذا نظرت إلى المخرجات وجمعت FMC لديك طريقة ما حيث أنك مستعدون لسيناريو أسوأ (عندما تحدث كل القيم القصوى في نفس الوقت)، عندئذ فإن معدل الأحداث الذي تراه FMC هو 48.65 + 348.15 + 4.63 + 3.25 + 0.06 = **404.74 إطار في الثانية**.

يمكن مقارنة هذه القيمة الإجمالية مع القيمة من ورقة البيانات الخاصة بالنموذج ذي الصلة.

كما يمكن أن يقوم SFDataCorrelator بعمل إضافي على رأس الأحداث المستلمة (مثل قواعد الارتباط)، ثم يقوم بتخزينها في قاعدة البيانات التي يتم الاستعلام عنها لنشر وعرض المعلومات لمثل حالات المعلومات في واجهة المستخدم الرسومية (GUI) لـ FMC مثل المعلومات مختلفة الأحداث.

إدارة الأقراص

يوضح المخطط المنطقي التالي المكونات المنطقية لكل من عمليتي Health Monitor وDisk Manager عند تداخلها لإنشاء تنبيهات الحماية المتعلقة بالقرص.



باختصار، تقوم عملية إدارة الأقراص بإدارة إستخدام القرص الخاص بالمربع، كما أنها تحتوي على ملفات التكوين الخاصة به في المجلد [/ngfw]/etc/sf/. هناك ملفات تكوين متعددة لعملية إدارة الأقراص يتم إستخدامها في ظروف معينة:

- diskmanager.conf - ملف تكوين قياسي.
- diskmanager_2hd.conf - يتم إستخدامه عندما يتم تثبيت محرك أقراص ثابتة في العبوة. ومحرك الأقراص الصلبة الثاني وه ذلك المرتبط بتوسعة البرامج الضارة، ويتم إستخدامه لتخزين الملفات كما وه محدد في نهج الملف.
- ramDisk-diskmanager.conf - يستخدم عند تمكين التسجيل إلى RamDisk. لمزيد من المعلومات، تحقق من قسم "تسجيل الدخول إلى Ramdisk".

يتم تعيين مخزن لكل نوع من الملفات التي تتم مراقبتها بواسطة إدارة الأقراص. بناء على كمية المساحة على القرص المتوفرة على النظام، يقوم "مدير الأقراص" بحساب علامة عام مرتفعة (HWM) وعلامة عام منخفضة (LWM) لكل مخزن.

عندما تقوم عملية "إدارة الأقراص" بمسح مخزن، فإنها تفعل ذلك حتى تصل إلى النقطة التي تم الوصول إليها من خلال LWM. ونظرا لأنه يتم تصفية الأحداث لكل ملف، يمكن تجاوز هذا الحد.

للتحقق من حالة الصوامع على جهاز إستشعار يمكنك إستخدام هذا الأمر:

```
> 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
```

يتم تشغيل عملية "إدارة الأقراص" عند استيفاء أحد هذه الشروط:

- تبدأ العملية (أو تعيد تشغيلها)
- مخزن يصل إلى HWM
- يتم [تصريف](#) صومعة [يدوي](#)
- مرة كل ساعة

في كل مرة يتم فيها تشغيل عملية "إدارة الأقراص"، فإنها تقوم بإنشاء إدخال لكل وحدة تخزين مختلفة في ملف السجل الخاص بها الذي يقع ضمن [/ngfw]/var/log/diskmanager.log ويحتوي على بيانات بتنسيق CSV.

بعد ذلك، يتم عرض نموذج للسطر من ملف diskmanager.log، مأخوذ من مستشعر تسبب في إستنزاف الأحداث غير المعالجة من تنبيه صحة "الأحداث ذات الأولوية المنخفضة الموحدة"، بالإضافة إلى تصنيف الأعمدة المقابلة:

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

القيمة	عمود
priority_2_events	تسمية المخزن
1599668981	زمن التصريف (الزمن الافتراضي)
221	عدد الملفات التي تم تصفيتها
4587929508	وحدات البايت التي تم تصفيتها
1132501868	الحجم الحالي للبيانات بعد عملية السحب (بالبايت)
20972020	أكبر ملف تم تجفيره (بالبايت)
4596	أصغر ملف تم تجفيره (بالبايت)
1586044534	أقدم ملف تم تجفيره (الوقت المستغرق في epoch)
5710966962	علامة مائية عالية (بايت)
1142193392	علامة مائية منخفضة (بايت)
110	عدد الملفات ذات الأحداث التي لم تتم معالجتها التي تم تصفيتها
0	علم حالة Diskmanager

ثم تقرأ هذه المعلومات بواسطة وحدة مراقبة الصحة المعينة لتشغيل التنبيه الصحي ذي الصلة.

تصريف يدوي

في بعض السيناريوهات، قد ترغب في إستنزاف صومعة يدوي. على سبيل المثال، لمسح مساحة القرص باستخدام ميزة "تصفية المخزن المؤقت يدوي" بدلا من "إزالة الملفات يدوي"، فإنه من مصلحة إدارة الأقراص تحديد الملفات التي يجب الاحتفاظ بها والملفات التي يجب حذفها. تحتفظ إدارة الأقراص بأحدث الملفات لهذا المخزن.

يمكن إستنزاف أي مخزن وهذا يعمل كما هو موضح بالفعل (تقوم إدارة الأقراص بتصفية البيانات حتى يتم تدفق مقدار البيانات أسفل حد LWM). يتوفر الأمر **system support silo-drain** في وضع CLISH لـ FTD وهو يوفر قائمة بالوحدات المتاحة (الاسم + المعرف الرقمي).

هذا مثال على عملية إستنزاف يدوية لمكدس أحداث Unified Low Priority Events:

```
> 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
```

مرقاب صحي

هذه هي النقاط الرئيسية:

- يتم إنشاء أي تنبيه صحي يظهر على FMC في قائمة Health Monitor أو تحت علامة التبويب Health في مركز الرسائل بواسطة عملية Health Monitor.
- تراقب هذه العملية سلامة النظام، بالنسبة لكل من وحدة إدارة اللوحة الأساسية (FMC) وأجهزة الاستشعار المدارة، كما تتكون من عدد من الوحدات المختلفة.
- يتم تحديد وحدات التنبيه الصحي في نهج الصحة الذي يمكن إرفاقه لكل جهاز.
- يتم إنشاء تنبيهات الحماية بواسطة وحدة "إستخدام القرص" التي يمكن تشغيلها على كل جهاز من أجهزة الاستشعار المدارة بواسطة FMC.
- عند تشغيل عملية Health Monitor على FMC (مرة كل 5 دقائق أو عند تشغيل تشغيل يدوي)، تقوم وحدة "إستخدام القرص" بالبحث في ملف diskmanager.log، وإذا تم استيفاء الشروط الصحيحة، يتم تشغيل تنبيه الصحة الخاص.

لـ **إستنزاف الأحداث غير المعالجة** تنبيه صحة ليتم تشغيله كل هذه الشروط يجب أن تكون صحيحة:

1. حقل وحدات البايت التي تم تسريبها أكبر من 0 (يشير ذلك إلى أن البيانات من هذا المخزن قد تم تسريبه).
2. عدد الملفات ذات الأحداث التي لم تتم معالجتها التي تم استنفادها أكبر من 0 (وهذا يشير إلى وجود أحداث لم تتم معالجتها داخل البيانات التي تم استنفادها).
3. وقت النزيف في غضون الساعة الواحدة الأخيرة.

يجب أن تكون هذه الشروط صحيحة لـ **إستنزاف متكرر للأحداث**:

1. يجب أن يكون الإدخالان الأخيران في ملف diskmanager.log: جعل حقل "وحدات البايت" التي تم استنفادها أكبر من 0 (يشير ذلك إلى أنه تم تصريف البيانات من هذا المخزن المؤقت).يفصل بين كل منهما أقل من 5 دقائق.
2. وقت إستنزاف آخر إدخال لهذا المخزن خلال الساعة الأخيرة.

يتم إرسال نتائج المجمع من وحدة إستخدام القرص النمطية (بالإضافة إلى النتائج المجمعة بواسطة الوحدات النمطية الأخرى) إلى FMC عبر sftunnel. يمكنك رؤية عدادات أحداث الصحة المتبادلة عبر sftunnel باستخدام الأمر **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
```

تسجيل الدخول إلى Ramdisk

على الرغم من أن معظم الأحداث يتم تخزينها في القرص، إلا أن الجهاز يتم تكوينه بشكل

افتراضي لتسجيل الدخول إلى القرص الثابت لمنع حدوث تلف تدريجي لمحركات الأقراص المزودة بذاكرة مصنوعة من مكونات صلبة (SSD) والذي يمكن أن يحدث بسبب عمليات الكتابة والحذف المستمرة للأحداث إلى القرص.

في هذا السيناريو، لا يتم تخزين الأحداث ضمن **[/ngfw]/var/sf/detection_engine/*/instance-N/،** ولكنها موجودة في **[/ngfw]/var/sf/detection_engines/*/instance-N/connection/**، وهو إرتباط رمزي إلى **/dev/shm/instance-N/connection.** في هذه الحالة، تكمن الأحداث في الذاكرة الافتراضية بدل من المادية.

```
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
```

للتحقق مما إذا تم تكوين الجهاز حاليا لتسجيل الأحداث على القرص، استخدم الأمر **show log-events-to-ramdisk** من FTD. يمكنك أيضا تغيير هذا إذا كنت تستخدم الأمر **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)
```

> **تحذير**: عند تنفيذ الأمر "configure log-events-to-ramdisk disable"، هناك حاجة إلى عمليتي نشر يتم القيام بهما على FTD لكي لا يعلق الشخير في حالة "D" (نوم غير متقطع)، مما قد يتسبب في انقطاع حركة المرور.
> وثق هذا تصرف في الخلل مع cisco بق id CSCvz53372. مع عملية النشر الأولى، يتم تخطي عملية إعادة تقييم مرحلة ذاكرة الشخر، والتي تتسبب في ظهور الشخر في حالة "D"، بينما يكون الحل البديل هو القيام بعملية نشر أخرى مع أي تغييرات وهمية.

عند تسجيل الدخول إلى ذاكرة التخزين المؤقت، يكون العائق الرئيسي هو أن مساحة المخزن المخصص له أصغر وبالتالي تستنزف بشكل أكبر في ظل نفس الظروف. الإخراج التالي هو "إدارة الأقراص" من FPR 4140 مع تمكين أحداث السجل أو بدونها على Ramdisk للمقارنة.

تم تمكين التسجيل إلى Ramdisk

```
> 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
```

تم تعطيل التسجيل إلى Ramdisk

```
> 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
```

أما الحجم الأصغر للهواتف فيتم تعويضه بسرعة أعلى للوصول إلى الأحداث وتدفقها إلى وحدة التحكم في إدارة الاتصالات الفيدرالية (FMC). وعلى الرغم من أن هذا الخيار أفضل في ظل الظروف المناسبة، فإنه يجب النظر في رد الفعل.

الأسئلة المتداولة (FAQ)

هل تنبيهات صحة "استنزاف الأحداث" تم إنشاؤها فقط بواسطة "أحداث الاتصال"؟

م

- يمكن إنشاء تنبيهات "التخلص المتكرر" بواسطة أي مخزن لإدارة الأقراص.
- يمكن إنشاء التنبيهات الخاصة باستنزاف الأحداث التي لم تتم معالجتها بواسطة أي مخزن خاص بالأحداث.

تعد "أحداث الاتصال" السبب الأكثر شيوعا.

هل من المستحسن دائما تعطيل "تسجيل الدخول إلى Ramdisk" عند ظهور تنبيه صحة "استنزاف متكرر"؟

ال. فقط في سيناريوهات التسجيل الزائدة باستثناء DoS/DDo، عندما يكون المخزن المتأثر هو مخزن أحداث الاتصال، وفقط في الحالات التي ال يمكن فيها ضبط إعدادات التسجيل بشكل إضافي.

إذا كانت رفض الخدمة (DoS)/رفض الخدمة (DoS) يؤدي إلى تسجيل مفرط، فإن الحل يكمن في تنفيذ حماية رفض الخدمة (DoS) أو القضاء على مصدر (مصادر) هجمات رفض الخدمة (DoS)/رفض الخدمة (DoS).

تعمل الميزة الافتراضية "تسجيل إلى Ramdisk" على تقليل استهلاك محرك الأقراص في الحالة الصلبة (SSD)، لذلك يوصى بشدة باستخدامه.

ما الذي يشكل حدثا لم تتم معالجته بعد؟

ال يتم تمييز الأحداث بشكل فردي كأحداث غير معالجة. يحتوي الملف على أحداث غير معالجة

عندما:

طابعها الزمني للإنشاء أعلى من حقل الطابع الزمني في ملف الإشارة المرجعية الخاص به.

أو

طابعها الزمني للإنشاء مساوٍ لحقل الطابع الزمني في ملف الإشارة المرجعية الخاص به وحجمه أعلى من الموضع في حقل وحدات البايت على ملف الإشارة المرجعية الخاص به.

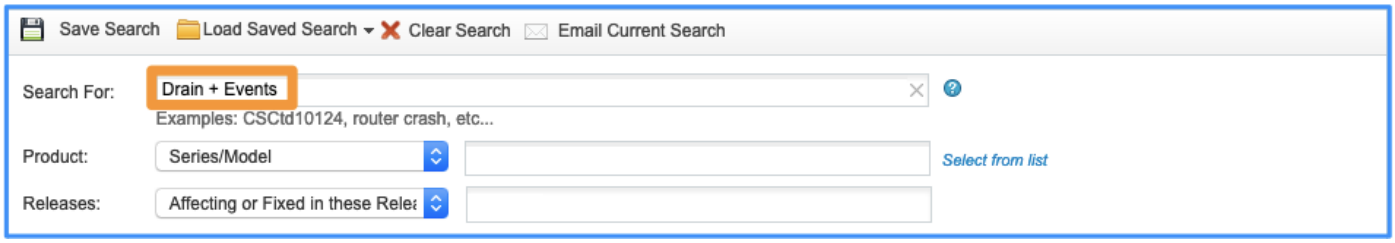
كيف تعرف FMC عدد وحدات البايت المتخلفة عن جهاز استشعار معين؟

يرسل المستشعر بيانات أولية حول اسم ملف unified_events وحجمه وكذلك المعلومات على ملفات الإشارة المرجعية التي تعطي لـ FMC معلومات كافية لحساب البايت خلفها كـ:

حجم ملف Unified_events الحالي - **موضع البايت**" من ملف الإشارة المرجعية + حجم كل ملفات Unified_events ذات ختم وقت أعلى من الطابع الزمني الموجود في ملف الإشارة المرجعية الخاص.

مشكلات معروفة

افتح أداة البحث عن الأخطاء واستخدم هذا الاستعلام:



حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).