فهم برنامج eStreamer واستكشاف أخطاء الاتصال وإصلاحها

المحتويات

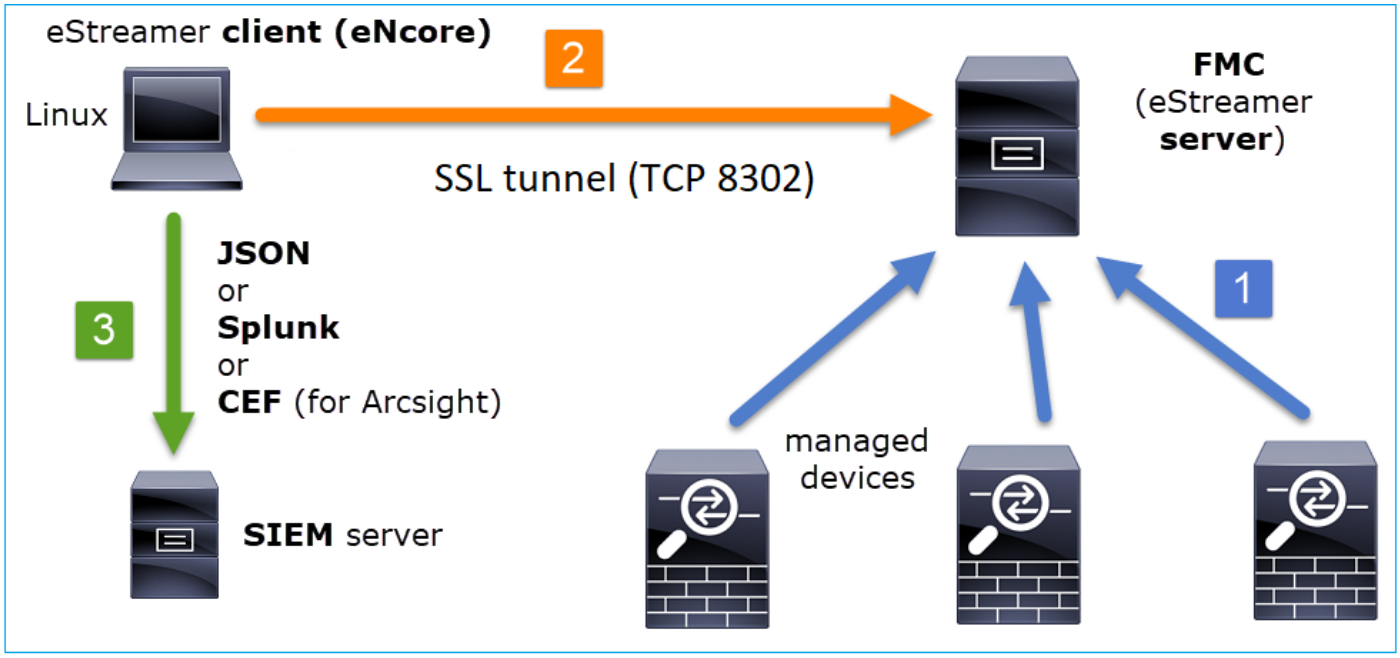
المقدمة

يصف هذا المستند عميل واجهة سطر الأوامر (CLI) الأساسي Cisco Event Streamer (المعروف أيضا باسم eStreamer). وعلى وجه التحديد، فإنه يصف العملية ويقدم معلومات أستكشاف الأخطاء وإصلاحها. وبالإضافة إلى ذلك، يغطي هذا المستند القضايا الشائعة التي يطلع عليها مركز المساعدة التقنية (TAC) من Cisco بالإضافة إلى الأسئلة المتداولة (FAQ).

تمت المساهمة من قبل ديفيد توريس ريفاس، ميكيس زافيرودييس، مهندسي TAC من Cisco.

نظرة عامة

إن eCore عبارة عن عميل متعدد الأغراض، يطلب جميع الأحداث المحتملة من خادم Streamer (FMC)، ويحلل المحتوى الثنائي، ويخرج الأحداث بتنسيقات مختلفة لدعم معلومات الأمان وأدوات إدارة الأحداث (SIEM) الأخرى.



مؤسسة اتصال Streamer

يقوم العميل (eNcore) ببدء اتصال بمنفذ TCP FMC 8302 حيث يتم إجراء مصافحة SSL:

```
1: 11:34:02.901091 192.168.27.100.46538 > 10.48.26.49.8302: S 1607291631:1607291631(0) win 29200
<mss 1460,sackOK,timestamp 2350959 0,nop,wscale 10>
2: 11:34:02.902220 10.48.26.49.8302 > 192.168.27.100.46538: S 2529774236:2529774236(0) ack
1607291632 win 28960 <mss 1380,sackOK,timestamp 940036669 2350959,nop,wscale 7>
3: 11:34:02.902739 192.168.27.100.46538 > 10.48.26.49.8302: . ack 2529774237 win 29
<nop,nop,timestamp 2350959 940036669>
```

تقبل FMC الاتصال، وتجري مصافحة SSL على نفس المنفذ، وتتحقق من الاسم الشائع للعميل (CN):

```
Mar  2 11:45:06 FMC SF-IMS[22601]: [22601] Event Streamer:ConnectionHandler [INFO] Accepted IPv4
connection from 10.48.26.47:46538/tcp
Mar  2 11:45:06 FMC SF-IMS[22601]: [22601] Event Streamer:ConnectionHandler [INFO] Added
10.48.26.47 to host table
Mar  2 11:45:06 FMC SF-IMS[22601]: [22601] Event Streamer:ConnectionHandler [INFO] Added
10.48.26.47(23935) to host table
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):ConnectionHandler
[INFO] Resolved CN 10.48.26.47 to 10.48.26.47
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):ConnectionHandler
[INFO] Matched Certificate CN:10.48.26.47 to 10.48.26.47 (IPv4)
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):sfestreamer [INFO]
Got EVENT_STREAM_REQUEST length 8
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):sfestreamer [INFO]
Publishing service INFO total data size 48
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):sfestreamer [INFO]
Publishing service id:5001 - length size 8
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):sfestreamer [INFO]
Publishing service id:5000 - length size 8
Mar  2 11:45:06 FMC SF-IMS[23935]: [23935] EventStreamer child(10.48.26.47):sfestreamer [INFO]
Publishing service id:6667 - length size 8
```

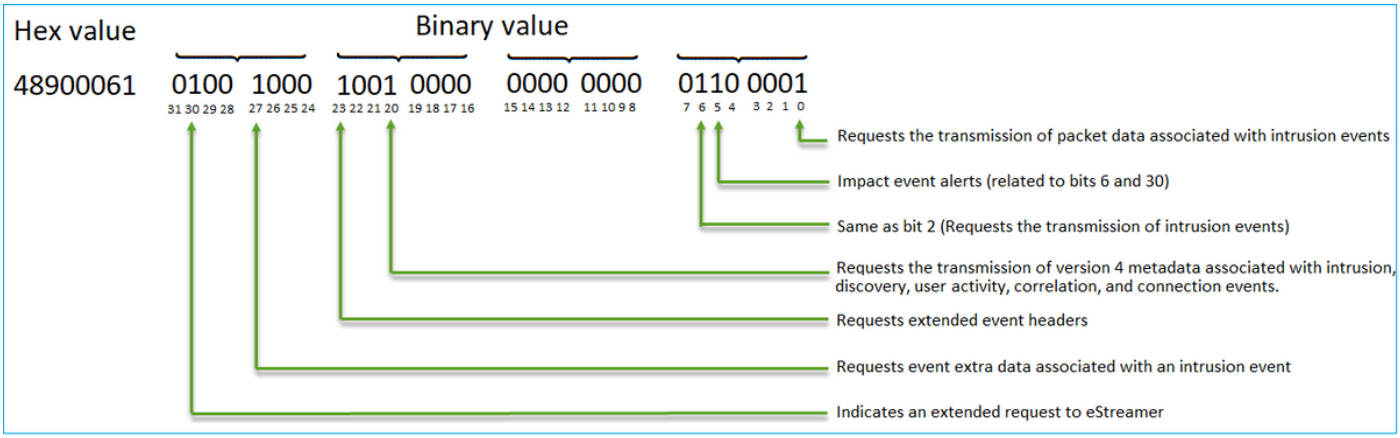
ثم يتحقق عميل eStreamer من التكوين الخاص به وملف الإشارة المرجعية لتحديد الأحداث التي يجب طلبها ووقت البدء:

```
2020-03-02 07:18:11,500 Connection   INFO     Connecting to 10.48.26.49:8302
2020-03-02 07:18:11,500 Connection   INFO     Using TLS v1.2
2020-03-02 07:18:11,500 Monitor      INFO     Starting Monitor.
2020-03-02 07:18:11,500 Monitor      INFO     Starting. 0 handled; average rate 0 ev/sec;
2020-03-02 07:18:11,501 Writer       INFO     Starting process.
2020-03-02 07:18:11,506 Transformer  INFO     Starting process.
2020-03-02 07:18:11,985 Bookmark     INFO     Bookmark file /root/eStreamer-eNcore/10.48.26.49-
8302_bookmark.dat does not exist.
2020-03-02 07:18:11,986 Settings     INFO     Timestamp: Start = 2 (Bookmark = 0)
2020-03-02 07:18:11,986 Receiver     INFO     EventStreamRequestMessage:
00010002000000080000000048900061
2020-03-02 07:18:11,986 SubscriberParser INFO     Starting process.
2020-03-02 07:18:11,996 Bookmark     INFO     Bookmark file /root/eStreamer-eNcore/10.48.26.49-
8302_bookmark.dat does not exist.
2020-03-02 07:18:11,996 Settings     INFO     Timestamp: Start = 2 (Bookmark = 0)
2020-03-02 07:18:11,997 Receiver     INFO     StreamingRequestMessage:
000108010000003800001a0b0000003848900061000000000009000c000400150009001f000b003d000e00470004005b
0007006500060060f0002008300000000
```

يمكن ربط EventStreamRequest على FMC:

```
Mar  2 12:29:16 FMC SF-IMS[6671]: [6671] EventStreamer child(10.48.26.47):sfestreamer [INFO]
EventStream Request (0x48900061): Since 0 w/ NS Events w/ NS 6.0 Events
w/ Packets w/ Extra IDS Event data w/ Metadata v4 w/ RUA 5.2 Events w/ Impact Alerts w/ 5.3
Impact Alerts w/ Impact Flags w/ RNA 5.3 Events w/ RNA 6.0 Flow w/ Policy 5.4 Events
w/ FireAMP 6.0 Events w/ Filelog 6.0 Events w/ Send archive timestamp w/ Send Detail Request
```

EventStreamRequest هو التمثيل السداسي العشري لعلامات الطلب الموضحة في [علامات الطلب](#) ويجب تحويلها إلى علامات ثنائية لمعرفة ما إذا كان العميل يطلب البيانات المطلوبة. وفيما يلي مثال على هذا:



ملاحظة: قد تغير بعض وحدات البت العلامة المعلومات المقدمة في حالة بدء الطلبات الموسعة.

استنادا إلى وحدات البت الطلب، تقوم وحدة التحكم في إدارة الملفات (FMC) بإرسال البيانات إلى عميل Streamer.

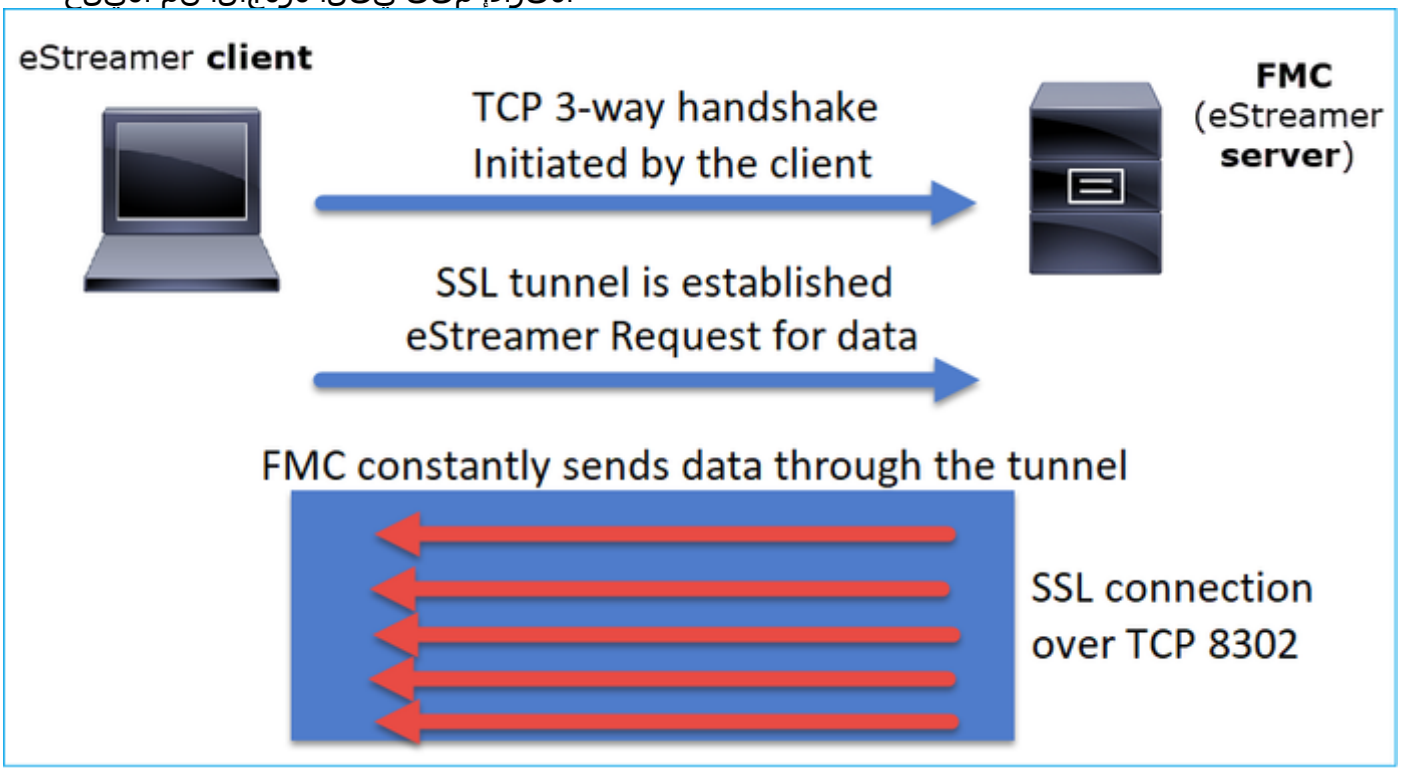
من يبدأ اتصال eStreamer ونقل البيانات؟

عميل eStreamer. وعلى وجه الخصوص، يقوم العميل بإنشاء اتصال TCP (مصافحة ثلاثية الإتجاه)، ثم يكون هناك تفاوض SSL مع مصادقة العميل (المتبادلة). وأخيرا، من خلال النفق القائم ترسل FMC البيانات كلما كانت هناك بيانات ليتم إرسالها:

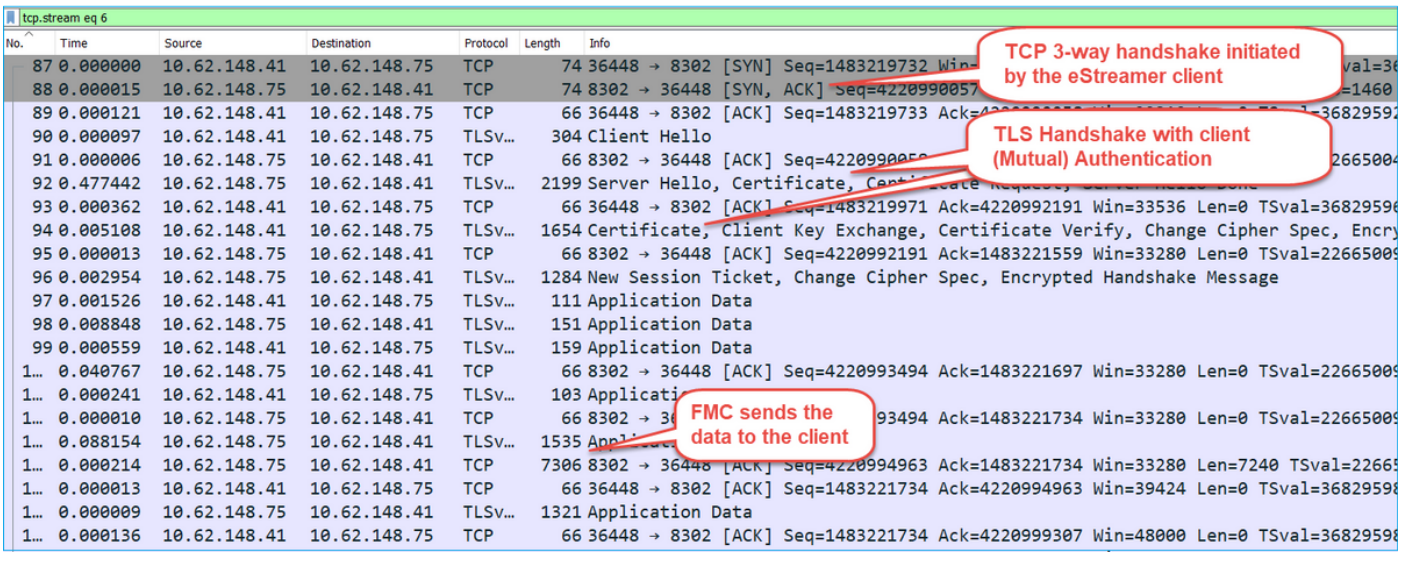
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100 handled; average rate 0.21 ev/sec;
2020-06-03 20:56:53,725 Monitor      INFO     Running. 100 handled; average rate 0.17 ev/sec;
```

باختصار:

- يقوم العميل ببدء نفق SSL لطلب البيانات (السحب)
- وبمجرد إنشاء النفق، يبقى النفق قيد التشغيل وتقوم وحدة التحكم في إدارة اللوحة الأساسية (FMC) بدفع البيانات (على سبيل المثال أحداث الاتصال) كلما تم الحصول عليها من الأجهزة التي تتم إدارتها



في هذا المثال، يمثل IP 10.62.148.41 هو عميل Streamer (eCore) بينما يمثل IP 10.62.148.75 وحدة التحكم FMC:



التكوين

للحصول على تفاصيل حول عميل واجهة سطر الأوامر (CLI) من Intel، ارجع إلى دليل عمليات واجهة سطر الأوامر (CLI) من EStreamer الإصدار 3.5.

يتم تغطية تفاصيل تطبيق eStreamer مع خطوات تكوين FMC في دليل دمج Event Streamer.

تعيين ملف.conf توليف

يصف هذا القسم ما يمكن أو يجب تعديله على estreamer.conf حتى يعمل الحل بشكل صحيح. يوجد ملف estreamer.conf داخل دليل *path*/eStreamer-eNcore. هنا عينة من محتويات الملف:

```
root@kali:~/eStreamer-eNcore# cat estreamer.conf
{
    "connectTimeout": 10,
    "enabled": true,
    "handler": {
        "output@comment": "If you disable all outputters it behaves as a sink",
        "outputters": [
            {
                "adapter": "json",
                "enabled": true,
                "stream": {
                    "options": {
                        "maxLogs": 10000,
                        "rotate": true
                    },
                    "uri": "relfile:///data/json/encore.{0}.json"
                }
            }
        ],
        "records": {
            "connections": true,
            "core": true,
            "excl@comment": [
                "These records will be excluded regardless of above (overrides 'include')",
                "e.g. to exclude flow and IPS events use [ 71, 400 ]"
            ],
            "exclude": [],
            "inc@comment": "These records will be included regardless of above",
            "include": [],
            "intrusion": true,
            "metadata": true,
            "packets": true,
            "rna": true,
            "rua": true
        }
    },
    "logging": {
        "filepath": "estreamer.log",
        "format": "%(asctime)s %(name)-12s %(levelname)-8s %(message)s",
        "lev@comment": "Levels include FATAL, ERROR, WARNING, INFO, DEBUG, VERBOSE and TRACE",
        "level": "INFO",
        "stdOut": true
    },
    "monitor": {
        "bookmark": false,
        "handled": true,
        "period": 120,
```

```
        "subscribed": true,
        "velocity": false
    },
    "responseTimeout": 2,
    "star@comment": "0 for genesis, 1 for now, 2 for bookmark",
    "start": 2,
    "subscription": {
        "records": {
            "@comment": [
                "Just because we subscribe doesn't mean the server is sending. Nor does it
mean",
                "we are writing the records either. See handler.records[]"
            ],
            "archiveTimestamps": true,
            "eventExtraData": true,
            "extended": true,
            "impactEventAlerts": true,
            "intrusion": true,
            "metadata": true,
            "packetData": true
        },
        "servers": [
            {
                "host": "10.62.148.75",
                "pkcs12Filepath": "client.pkcs12",
                "port": 8302,
                "tls@comment": "Valid values are 1.0 and 1.2",
                "tlsVersion": 1.2
            }
        ]
    },
    "workerProcesses": 4
```

قسم الاشتراك

لتعديل طلب Event Streamer باتجاه الخادم (FMC)، قم بتعديل قسم اشتراكات eStreamer.conf. على سبيل المثال، عند تعيين طلبات موسعة إلى false، يوقوم هذه الإجراء بتغيير طلب EventStream على FMC:

```
"subscription": {
        "records": {
            "@comment": [
                "Just because we subscribe doesn't mean the server is sending. Nor does it
mean",
                "we are writing the records either. See handler.records[]"
            ],
            "archiveTimestamps": true,
            "connection": true,
            "eventExtraData": true,
            "extended": false,
            "impactEventAlerts": true,
            "intrusion": true,
            "metadata": true,
            "packetData": true
        },
```

مع الطلبات الموسعة = false:

```
Jun 3 13:48:24 firepower SF-IMS[16084]: [16084] EventStreamer child(10.48.26.47):sfestreamer
```

```
[INFO]
EventStream Request (0x08900061): Since 4294967295 w/ NS Events w/ Packets w/ Extra IDS Event
data w/
Metadata v4 w/ Impact Alerts w/ Impact Flags w/ Send archive timestamp
```

مع الطلبات الموسعة = true:

```
Jun 3 13:50:52 firepower SF-IMS[17167]: [17167] EventStreamer child(10.48.26.47):sfestreamer
[INFO]
EventStream Request (0x48900061): Since 1590497346 w/ NS Events w/ NS 6.0 Events w/ Packets w/
Extra IDS Event data w/ Metadata
v4 w/ RUA 5.2 Events w/ Impact Alerts w/ 5.3 Impact Alerts w/ Impact Flags w/ RNA 5.3 Events w/
RNA 6.0 Flow w/ Policy 5.4 Events
v w/ FireAMP 6.0 Events w/ Filelog 6.0 Events w/ Send archive timestamp w/ Send Detail Request
```

قسم التسجيل

لتمكين تصحيح الأخطاء على واجهة سطر الأوامر (CLI) من خلال eCore، قم بتحرير ملف estreamer.conf وقم بتغيير مستوى السجل:

```
 "logging": {
        "filepath": "estreamer.log",
        "format": "%(asctime)s %(name)-12s %(levelname)-8s %(message)s",
        "lev@comment": "Levels include FATAL, ERROR, WARNING, INFO, DEBUG, VERBOSE and TRACE",
        "level": "DEBUG",
        "stdOut": true
    },
```

قسم الشاشات

لترى عدد الأحداث/الإشارة المرجعية الثانية التي تمت معالجتها والإشارة المرجعية الحالية، قم بتحرير قسم المراقبة على estreamer.conf:

```
  "monitor": {
    "bookmark": true,         #If true, adds date/timestamp (see above)
    "handled": true,           #Number of records processed
    "period": 120,             #How often (in seconds) monitor writes to the log
    "subscribed": true,        #Number of records received
    "velocity": false          #A measure of whether eNcore is keeping up (>=1 is good)
  },
```

مفاتيح أخرى ذات صلة من المستوى الأعلى:

```
"connectTimeout": 10,     <- The number of seconds to wait for a response when establishing a
connection to the FMC.

"workerProcesses": 4,     <- The number of processes that eNcore spawns.
```

يمكن تعيين هذه القيمة من 2-12. والغرض من مزيد من العمليات هو تحسين الأداء ولكن "عدد العمليات" مع قدرة الآلة المضيفة على المعالجة. أفضل الإرشادات المتوفرة هي:

- بالنسبة لنقطتين: "WorkerOperations": 4
- لـ 4 أو أكثر: "WorkerOperations": 12

استكشاف الأخطاء وإصلاحها

بالنسبة لإجراءات أستكشاف أخطاء Streamer العامة وإصلاحها، ارجع إلى هذا المستند [لاستكشاف أخطاء هذا المستند وإصلاحها بين FireSIGHT System و eStreamer Client (SIEM)]

لأغراض الاختبار، يمكنك تمكين eCore كعملية أمامية والتحقق من الاتصال ب FMC

```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-04 11:48:00,048 Controller   INFO     eNcore version: 3.5.4
2020-06-04 11:48:00,049 Controller   INFO     Python version: 2.7.13 (default, Jan 19 2017,
14:48:08) \n[GCC 6.3.0 20170118]
2020-06-04 11:48:00,051 Controller   INFO     Platform version: Linux-4.13.0-kali1-amd64-x86_64-
with-Kali-kali-rolling-kali-rolling
2020-06-04 11:48:00,052 Controller   INFO     Starting client (pid=12374).
2020-06-04 11:48:00,052 Controller   INFO     Sha256:
77ac7e72d0b96e0a4b9c1c4f9a16c2de0b2b5ccf2929dd2857cf94ed96b295e3
2020-06-04 11:48:00,052 Controller   INFO     Processes: 4
2020-06-04 11:48:00,053 Controller   INFO     Settings:
 …
2020-06-04 11:48:00,053 Diagnostics  INFO     Check certificate
2020-06-04 11:48:00,054 Diagnostics  INFO     Creating connection
2020-06-04 11:48:00,054 Connection   INFO     Connecting to 10.62.148.75:8302
2020-06-04 11:48:00,054 Connection   INFO     Using TLS v1.2
2020-06-04 11:48:00,136 Diagnostics  INFO     Creating request message
2020-06-04 11:48:00,137 Diagnostics  INFO     Request message=00010002000000008ffffffff48900061
2020-06-04 11:48:00,137 Diagnostics  INFO     Sending request message
2020-06-04 11:48:00,137 Diagnostics  INFO     Receiving response message
2020-06-04 11:48:00,229 Diagnostics  INFO     Response
message=KGRwMApTJ2xlbmd0aCcKcDEKSTQ4CnNTJ3ZlcnNpb24nCnAyCkkxCnNTJ2RhdGEnCnAzClMnXHgwMFx4MDBceDEz
XHg4OVx4MDBceDAwXHgwMFx4MDhceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgxM1x4ODhceDAw
XHgwMFx4MDBceDA4XHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MWFceDBiXHgwMFx4MDBceDAw
XHgwOFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwJwpwNApzUydtZXNzYWdlVHlwZScKcDUKSTIwNTEKcy4=
2020-06-04 11:48:00,229 Diagnostics  INFO     Streaming info response
2020-06-04 11:48:00,230 Diagnostics  INFO     Connection successful
2020-06-04 11:48:00,230 Monitor      INFO     Starting Monitor.
2020-06-04 11:48:00,236 Decorator    INFO     Starting process.
2020-06-04 11:48:00,236 Transformer  INFO     Starting process.
2020-06-04 11:48:00,237 Connection   INFO     Connecting to 10.62.148.75:8302
2020-06-04 11:48:00,237 Connection   INFO     Using TLS v1.2
2020-06-04 11:48:00,238 Writer       INFO     Starting process.
2020-06-04 11:48:00,639 Bookmark     INFO     Opening bookmark file /root/eStreamer-
eNcore/10.62.148.75-8302_bookmark.dat.
2020-06-04 11:48:00,640 Settings     INFO     Timestamp: Start = 2 (Bookmark = 1591210934)
2020-06-04 11:48:00,640 Receiver     INFO     EventStreamRequestMessage:
00010002000000085ed7f3b648900061
2020-06-04 11:48:00,640 SubscriberParser INFO     Starting process.
2020-06-04 11:48:00,640 Bookmark     INFO     Opening bookmark file /root/eStreamer-
eNcore/10.62.148.75-8302_bookmark.dat.
2020-06-04 11:48:00,646 Bookmark     INFO     Opening bookmark file /root/eStreamer-
eNcore/10.62.148.75-8302_bookmark.dat.
2020-06-04 11:48:00,646 Settings     INFO     Timestamp: Start = 2 (Bookmark = 1591210934)
2020-06-04 11:48:00,647 Receiver     INFO     StreamingRequestMessage:
000108010000003800001a0b0000003848900061 5ed7f3b60009000c000400150009001f000b003d000e00470004005b
0007006500060060f0002008300000000
2020-06-04 11:48:00,653 Monitor      INFO     Running. 0 handled; average rate 1.2 ev/sec;
```

هذه سجلات مثل رؤية (FMC) لمحرك الكيان في إدارة الجهاز، يمكنك في وحدة التحكم في الوقت نفسه. لاحظ أن المنطقة الزمنية لسجلات عندما يعمل eCore Streamer بإنشاء الاتصال. هي دائما UTC: للخلفية لوحدة التحكم في إدارة اللوحة الأساسية (FMC)

```
root@FMC2000-2:~# tail -f /var/log/messages
Jun  4 09:48:00 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Accepted
IPv4 connection from 10.62.148.41:36528/tcp
Jun  4 09:48:00 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Added
10.62.148.41(8512) to host table
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):SFUtil [INFO] Found IPv4 address 10.62.148.41 for ksec-sfvm-win7-3.cisco.com
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Resolved CN ksec-sfvm-win7-3.cisco.com to 10.62.148.41
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Matched Certificate CN:ksec-sfvm-win7-3.cisco.com to
10.62.148.41 (IPv4)
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Got EVENT_STREAM_REQUEST length 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service INFO total data size 48
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service id:5001 - length size 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service id:5000 - length size 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service id:6667 - length size 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Got UEC_STREAM_REQUEST length 56
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] requested service [6667] timestamp [1591210934]
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 12, version 9
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 21, version 4
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 31, version 9
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 61, version 11
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 71, version 14
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 91, version 4
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 101, version 7
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 111, version 6
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 131, version 2
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] EventStream Request (0x48900061): Since 1591210934 w/ NS Events
w/ NS 6.0 Events w/ Packets w/ Extra IDS Event data w/ Metadata v4 w/ RUA 5.2 Events w/ Impact
Alerts w/ 5.3 Impact Alerts w/ Impact Flags w/ RNA 5.3 Events w/ RNA 6.0
Flow w/ Policy 5.4 Events w/ FireAMP 6.0 Events w/ Filelog 6.0 Events w/ Send archive timestamp
w/ Send Detail Request
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] creating iterator for service [6667] prefix [unified2.]
timestamp [1591210934]
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):Unified2Iterator [INFO] Opened /var/sf/archive/netmap_2/unified2.1591210800
Jun  4 09:48:02 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Child
with pid 8510 exited with status 5120
Jun  4 09:48:02 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Removed
host entry for pid: 8510
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
URLFiltering: 310f4c00-a415-11ea-bf5b-a2d6028849fe
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
```

```
URLFiltering: d637b6f0-a414-11ea-ad97-cc17b6ea4c03
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
URLFiltering: 873709b8-78b6-11ea-ae87-b82f93835447
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
URLFiltering: c7c0217c-78b6-11ea-a719-b7f0a277eb86
```

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

ينصح بشدة بجمع هذه العناصر قبل الاتصال ب Cisco TAC:

- إصدار eStreamer eCore
- نسخة باي ثون
- إصدار نظام التشغيل المضيف
- هل ترى أحداث على FMC؟ مشاركة لقطة شاشة من الأحداث + تكوين FMC eStreamer
- قم بتمكين تصحيح الأخطاء على واجهة سطر الأوامر (كما هو موضح في 'قسم التسجيل')
- إنشاء ملف أستكشاف الأخطاء وإصلاحها من FMC
- قم بتوفير هذه الملفات من خلال eCore:
  estreamer.conf
  سجل المعلومات

المشكلات الشائعة

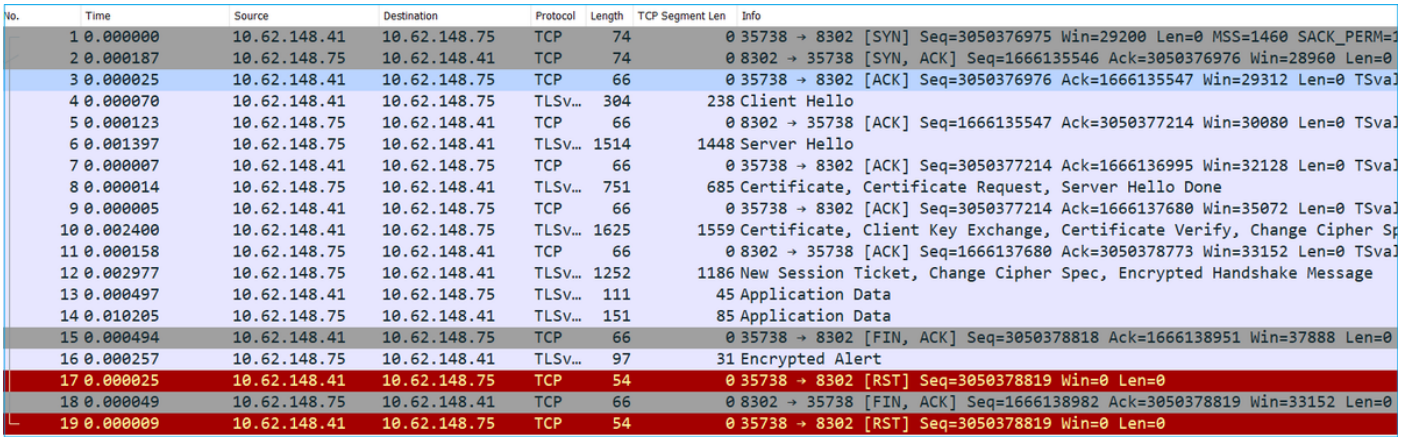
لا يوجد اتصال على منفذ TCP 8302

برنامج Telnet من عميل Streamer إلى منفذ FMC 8302 والتحقق من إنشاء الاتصال.

بالإضافة إلى ذلك، يمكنك إستخدام خيار الخاتم الإلكتروني الخاتم الاتصال:

```
root@kali:~/eStreamer-eNcore# ./encore.sh test
2020-05-28T16:02:56.931919 Diagnostics  INFO    Checking that configFilepath (estreamer.conf)
exists
2020-05-28 16:02:56,935 Diagnostics  INFO     Check certificate
2020-05-28 16:02:56,936 Diagnostics  INFO     Creating connection
2020-05-28 16:02:56,936 Connection   INFO     Connecting to 10.62.148.75:8302
2020-05-28 16:02:56,936 Connection   INFO     Using TLS v1.2
2020-05-28 16:02:56,946 Diagnostics  INFO     Creating request message
2020-05-28 16:02:56,946 Diagnostics  INFO     Request message=00010002000000008ffffffff48900061
2020-05-28 16:02:56,946 Diagnostics  INFO     Sending request message
2020-05-28 16:02:56,946 Diagnostics  INFO     Receiving response message
2020-05-28 16:02:56,957 Diagnostics  INFO     Response
message=KGRwMApTJ2xlbmd0aCcKcDEKSTQ4CnNTJ3ZlcnNpb24nCnAyCkkxCnNTJ2RhdGEnCnAzClMnXHgwMFx4MDBceDEz
XHg4OVx4MDBceDAwXHgwMFx4MDhceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgxM1x4ODhceDAw
XHgwMFx4MDBceDA4XHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MWFceDBiXHgwMFx4MDBceDAw
XHgwOFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwJwpwNApzUydtZXNzYWdlVHlwZScKcDUKSTIwNTEKcy4=
2020-05-28 16:02:56,957 Diagnostics  INFO     Streaming info response
2020-05-28 16:02:56,957 Diagnostics  INFO     Connection successful
```

هذه لقطة شاشة من حركة المرور التي تظهر اتصال ناجح (10.62.148.41 هو كمبيوتر المختبر الذي يعمل بنظام التشغيل Wireshark وهو 10.62.148.75 هو FMC):



No.	Time	Source	Destination	Protocol	Length	TCP Segment Len	Info
1	0.000000	10.62.148.41	10.62.148.75	TCP	74	0	35738 → 8302 [SYN] Seq=3050376975 Win=29200 Len=0 MSS=1460 SACK_PERM=1
2	0.000187	10.62.148.75	10.62.148.41	TCP	74	0	8302 → 35738 [SYN, ACK] Seq=1666135546 Ack=3050376976 Win=28960 Len=0
3	0.000025	10.62.148.41	10.62.148.75	TCP	66	0	35738 → 8302 [ACK] Seq=3050376976 Ack=1666135547 Win=29312 Len=0 TSval
4	0.000070	10.62.148.41	10.62.148.75	TLSv…	304	238	Client Hello
5	0.000123	10.62.148.75	10.62.148.41	TCP	66	0	8302 → 35738 [ACK] Seq=1666135547 Ack=3050377214 Win=30080 Len=0 TSval
6	0.001397	10.62.148.75	10.62.148.41	TLSv…	1514	1448	Server Hello
7	0.000007	10.62.148.41	10.62.148.75	TCP	66	0	35738 → 8302 [ACK] Seq=3050377214 Ack=1666136995 Win=32128 Len=0 TSval
8	0.000014	10.62.148.75	10.62.148.41	TLSv…	751	685	Certificate, Certificate Request, Server Hello Done
9	0.000005	10.62.148.41	10.62.148.75	TCP	66	0	35738 → 8302 [ACK] Seq=3050377214 Ack=1666137680 Win=35072 Len=0 TSval
10	0.002400	10.62.148.41	10.62.148.75	TLSv…	1625	1559	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Sp
11	0.000158	10.62.148.75	10.62.148.41	TCP	66	0	8302 → 35738 [ACK] Seq=1666137680 Ack=3050378773 Win=33152 Len=0 TSval
12	0.002977	10.62.148.75	10.62.148.41	TLSv…	1252	1186	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
13	0.000497	10.62.148.41	10.62.148.75	TLSv…	111	45	Application Data
14	0.010205	10.62.148.75	10.62.148.41	TLSv…	151	85	Application Data
15	0.000494	10.62.148.41	10.62.148.75	TCP	66	0	35738 → 8302 [FIN, ACK] Seq=3050378818 Ack=1666138951 Win=37888 Len=0
16	0.000257	10.62.148.75	10.62.148.41	TLSv…	97	31	Encrypted Alert
17	0.000025	10.62.148.41	10.62.148.75	TCP	54	0	35738 → 8302 [RST] Seq=3050378819 Win=0 Len=0
18	0.000049	10.62.148.75	10.62.148.41	TCP	66	0	8302 → 35738 [FIN, ACK] Seq=1666138982 Ack=3050378819 Win=33152 Len=0
19	0.000009	10.62.148.41	10.62.148.75	TCP	54	0	35738 → 8302 [RST] Seq=3050378819 Win=0 Len=0

لا تتطابق الشهادة CN مع المضيف البعيد

إذا كان عميل eStreamer خلف NAT، فيجب إنشاء الشهادة باستخدام عنوان IP للتدفق أو ظهور أخطاء مثل هذه:

```
Mar  2 11:30:01 FMC SF-IMS[16921]: [16921] Event Streamer:ConnectionHandler [INFO] Accepted IPv4
connection from 10.48.26.47:46529/tcp
Mar  2 11:30:01 FMC SF-IMS[16921]: [16921] Event Streamer:ConnectionHandler [INFO] Added
10.48.26.47 to host table
Mar  2 11:30:01 FMC SF-IMS[16921]: [16921] Event Streamer:ConnectionHandler [INFO] Added
10.48.26.47(17659) to host table
Mar  2 11:30:01 FMC SF-IMS[17659]: [17659] EventStreamer child(192.168.27.100):ConnectionHandler
[INFO] Resolved CN 192.168.27.100 to 192.168.27.100
Mar  2 11:30:01 FMC SF-IMS[17659]: [17659] EventStreamer child(192.168.27.100):ConnectionHandler
[ERROR] Certificate Common Name 192.168.27.100 does not match remote host: 10.48.26.47. It was
issued to a different client.
Mar  2 11:30:02 FMC SF-IMS[16921]: [16921] Event Streamer:ConnectionHandler [INFO] Child with
pid 17659 exited with status 0
Mar  2 11:30:02 FMC SF-IMS[16921]: [16921] Event Streamer:ConnectionHandler [INFO] Removed host
entry for pid: 17659
```

دقة FMC DNS لعميل eStreamer غير صحيحة

في حالة وجود إدخالات DNS خاطئة في FMC لعميل eStreamer، لا تصل الأحداث إلى العميل. لتحديد ما إذا كانت هذه هي المشكلة، التقط صور على FMC. في هذا المثال، تستلم FMC حزمة TCP SYN من مضيف عميل Streamer ksec-sfvm-win7-3.cisco.com:

```
root@FMC2000-2:/var/sf/archive/netmap_2# tcpdump -i eth0 port 8302
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:32:45.453401 IP ksec-sfvm-win7-3.cisco.com.36428 > FMC2000-2.8302: Flags [S], seq 2427598184,
win 29200, options [mss 1460,sackOK,TS val 3681355935 ecr 0,nop,wscale 7], length 0
18:32:45.453425 IP FMC2000-2.8302 > ksec-sfvm-win7-3.cisco.com.36428: Flags [S.], seq
1996800475, ack 2427598185, win 28960, options [mss 1460,sackOK,TS val 2264897265 ecr
3681355935,nop,wscale 7], length 0
18:32:45.453539 IP ksec-sfvm-win7-3.cisco.com.36428 > FMC2000-2.8302: Flags [.], ack 1, win 229,
options [nop,nop,TS val 3681355935 ecr 2264897265], length 0
```

يمكنك إستخدام علامة -N لرؤية IP الذي تم تحليله:

```
root@FMC2000-2:/var/sf/archive/netmap_2# tcpdump -i eth0 port 8302 -n
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:34:58.015971 IP 10.62.148.41.36434 > 10.62.148.75.8302: Flags [S], seq 713101140, win 29200,
options [mss 1460,sackOK,TS val 3681488496 ecr 0,nop,wscale 7], length 0
```

بدل من ذلك، يمكنك إستخدام أداة الأمر **nslookup** من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم FMC:

```
root@FMC2000-2:/var/sf/archive/netmap_2# nslookup ksec-sfvm-win7-3.cisco.com
Server:         1.2.3.4
Address:        1.2.3.4#53

Name: ksec-sfvm-win7-3.cisco.com Address: 10.62.148.41
```

مشكلة في اتصال eStreamer بسبب خطأ في شهادة SSL

تأكد من أن عميل eStreamer يستخدم شهادة FMC SSL الصحيحة. إذا كانت الشهادة غير صحيحة في ملفات FMC /var/log/message، سترى الأحداث التالية:

```
Jun 11 14:15:33 FMC SF-IMS[14211]: [14211] Event Streamer:ConnectionHandler [INFO]
estreamer.c:2149:AcceptConnections(): Accepted IPv4 connection from 192.0.2.100:42143/tcp
Jun 11 14:15:33 FMC SF-IMS[14211]: [14211] Event Streamer:ConnectionHandler [INFO]
estreamer.c:389:allowConnection(): Added 192.0.2.100 to host table
Jun 11 14:15:33 FMC SF-IMS[14211]: [14211] Event Streamer:ConnectionHandler [INFO]
estreamer.c:334:rememberPid(): Added 192.0.2.100(13687) to host table
Jun 11 14:15:33 FMC SF-IMS[14211]: [14211] Event Streamer:ConnectionHandler [DEBUG]
estreamer.c:1347:AcceptConnection(): Created new estreamer child with src 192.0.2.100 : pid
13615
Jun 11 14:15:34 FMC SF-IMS[13687]: [13615] Event Streamer:ConnectionHandler [ERROR]
estreamer.c:1116:AcceptConnection(): SSL_accept failed, SSL_get_error reports SSL_ERROR_SYSCALL
```

يمكنك ذف عميل eStreamer على FMC وإعادة تكوينه. يؤدي هذا إلى إعادة إنشاء شهادة SSL. إستيراد الشهادة الجديدة إلى عميل eStreamer.

عنوان IP غير صحيح تم تكوينه على eStreamer لتكامل وحدة ASA SFR

على عميل Streamer، يجب إستخدام وحدة SFR النمطية IP. على ASA قم بتشغيل الأمر **show sfr module detail** لعرض الوحدة النمطية IP.

تنسيق الحدث الشائع ArcSight (CEF)

يحدد معيار [تنسيق الحدث المشترك ArcSight](#) أزواج القيم الأساسية التي يجب إرسالها من واجهة سطر الأوامر (CLI) من eCore. إذا كان هناك عدم تناسق في البيانات المتلقاة على ArcGht، أي: الحقول المفقودة، خارج الترتيب، أو بعض البيانات لم يتم تحليلها بشكل صحيح على عميل ArcSight، فمن المفيد تعديل التكوين للكتابة إلى ملف سجل عن طريق الإعداد. وهذا يساعد على تحديد مكان المشكلة.

```
    "handler": {
        "output@comment": "If you disable all outputters it behaves as a sink",
        "outputters": [
```

```
            {
                "adapter": "cef",
                "enabled": true,
                "stream": {
                    "uri": "relfile:///data/data.{0}.cef"
                }
            }
        ],
```

تتم كتابة أحداث CEF الخام في سطر مع كل حقل يفصل بينهما ممرر البيانات "|":

```
<13>May 26 09:31:39 kali2 CEF:0|Cisco|Firepower|6.0|RNA:1003:1|CONNECTION STATISTICS|3|act=Allow
app=STUN bytesOut=820 cs1=test cs1Label=fwPolicy
cs2=Default Action cs2Label=fwRule cs3=INSIDE cs3Label=ingressZone cs4=OUTSIDE
cs4Label=egressZone cs5Label=secIntelCategory deviceExternalId=1
deviceInboundInterface=inside deviceOutboundInterface=outside dpt=9000 dst=216.151.129.103
dvchost=10.48.26.45 dvcpid=2 end=1590497212000 externalId=50850
proto=17 reason=N/A requestClientApplicatio
```

لا يعرض عميل eStreamer جميع السجلات

غالبا ما يرجع ذلك إلى الإفراط في الاشتراك في عميل eStreamer (عدد كبير للغاية من الأحداث التي تم إرسالها بواسطة FMC). قم بتشغيل هذا الأمر على جانب عميل Streamer وتحقق مما إذا كان عداد Rev-Q مرتفعا. هذا هو عدد وحدات البايت التي لم يتم نسخها بواسطة برنامج المستخدم المتصل بهذا المقبس. في هذا المثال، هناك 143143 بايت معلقة على جانب العميل:

```
root@kali:~# netstat -an | egrep "8302|Recv-Q"
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp   143143  0 10.62.148.41:36732      10.62.148.75:8302       ESTABLISHED
```

تحقق من الأحداث في الثانية التي يتلقاها عميل eStreamer. يوفر لك هذا مؤشرا للأحداث في الثانية كمعدل:

```
root@kali:~/eStreamer-eNcore# cat estreamer.log | grep "ev/sec"
```

حاول تقليل كمية البيانات المطلوبة من قبل عميل eStreamer، أو أنواع الأحداث المرسلة من قبل FMC. بدلا من ذلك، يمكنك محاولة زيادة مقدار الموارد المخصصة على جانب عميل eStreamer.

الأسئلة المتداولة (FAQ)

أين يمكن الحصول على حزمة واجهة سطر الأوامر (CLI) من خلال تقنية eNcore؟

- تحقق من صفحة تنزيل برنامج FMC، **أو أدوات نظام FirePOWER، وواجهات برمجة التطبيقات (API) - ECore لـ CEF**
- بدلا من ذلك، يمكنك الحصول على أحدث ملف إلكتروني من https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets

عند وجود نسخة احتياطية كاملة من FMC قيد التقدم، لا يقوم eStreamer بإنشاء أحداث. هل هذا طبيعي؟

نعم، انه سلوك متوقع. من دليل تكوين FMC متى يمكن اجراء نسخ احتياطي:

بينما يقوم النظام بتجميع بيانات النسخ الاحتياطي، قد يكون هناك توقف مؤقت في ارتباط البيانات (FMC فقط)، وقد يتم منعك من تغيير التكوينات المتعلقة بالنسخ الاحتياطي.

هل هناك أي ترخيص خاصة مطلوبة لدمج وحدة التحكم الإدارية الموحدة مع عميل Streamer (على سبيل المثال، QRADAR)؟

ال

من أين يتم الحصول على مصدر أحداث eStreamer؟

وحدة إدارة الاتصالات الفيدرالية. وعلى وجه التحديد، تقوم وحدة التحكم في إدارة اللوحة الأساسية (FTD) بنقل الأحداث من الأجهزة المدارة (FTD) وإعادة توجيهها إلى عميل (عملاء) eStreamer مثل eNcore و ArcSight و Splunk و QRadar و LogRhythm وما إلى ذلك.

هل هناك أي مصفوفة توافق بين Splunk و eCore؟

تحقق من مستندات Splunk للحصول على معلومات التوافق. على سبيل المثال، للاطلاع على إصدارات Splunk المتوافقة مع الإصدار 3.6.8 من البرنامج الإلكتروني، راجع https://splunkbase.splunk.com/app/3662/

هل بإمكان الطرازان eStreamer Core استهلاك البيانات من العديد من وحدات التحكم في إدارة اللوحة الأساسية (FMC)؟

في وقت كتابة هذا التقرير، لا. فحص طلب التحسين CSCvq14351

ما هي الخيارات الموصى بها لتكوين eStreamer لإعداد التوفر العالي (HA) من FMC؟

تتمثل التوصية في تكوين وحدة FMC النشطة فقط لـ eStreamer. إذا قمت بتكوين كل وحدتي FMC لـ eStreamer، فإن SIEM يستلم أحداث تكرار لأن FMC في وضع الاستعداد يستجيب لطلب eStreamer. طلب التعزيز ذي الصلة: CSCvi95944

هل تتطلب ترقية FMC إنشاء شهادات eStreamer جديدة يدويا؟

ال

هل يتم إرسال أحداث إستخبارات الأمان إلى عميل Streamer؟ هل من الممكن تحديد أحداث إستخبارات الأمان كفئة منفصلة وإرسالها إلى عميل eStreamer؟

يتم تضمين أحداث إستخبارات الأمان (SI) في فئة أحداث الاتصال وليس كفئة منفصلة. ولهذا السبب، ال يوجد حدث SI منفصل يتم إرساله إلى جهاز التحكم في الشبكة. طلب التعزيز ذي الصلة: CSCva39052

هل من الممكن تحديد أجهزة الاستشعار/الأجهزة المدارة على FMC التي تم إرسال أحداث eStreamer الخاصة بها إلى عميل eStreamer؟

ال يمكن إستخدام مجال FMC واحد حاليا. طلب التحسين ذو الصلة CSCvt31270. بدال من ذلك، تقوم بتكوين مجالين مختلفين على FMC. في المجال الأول، تقوم بإضافة جميع الأجهزة المدارة التي تريد تمكين eStreamer لها وتكوين عميل eStreamer. للمجال الثاني، تقوم بإضافة بقية الأجهزة وال تقوم بتكوين eStreamer.

ما هو إصدار eStreamer على FirePOWER؟ أحتاج إلى هذه المعلومات لتكوين SIEM (مثل LogRhythm)

للتحقق من إصدار FirePOWER (FMC) من واجهة مستخدم FMC، انتقل إلى **تعليمات** (الزاوية العلوية اليمنى) > **حول** > **إصدار البرنامج**

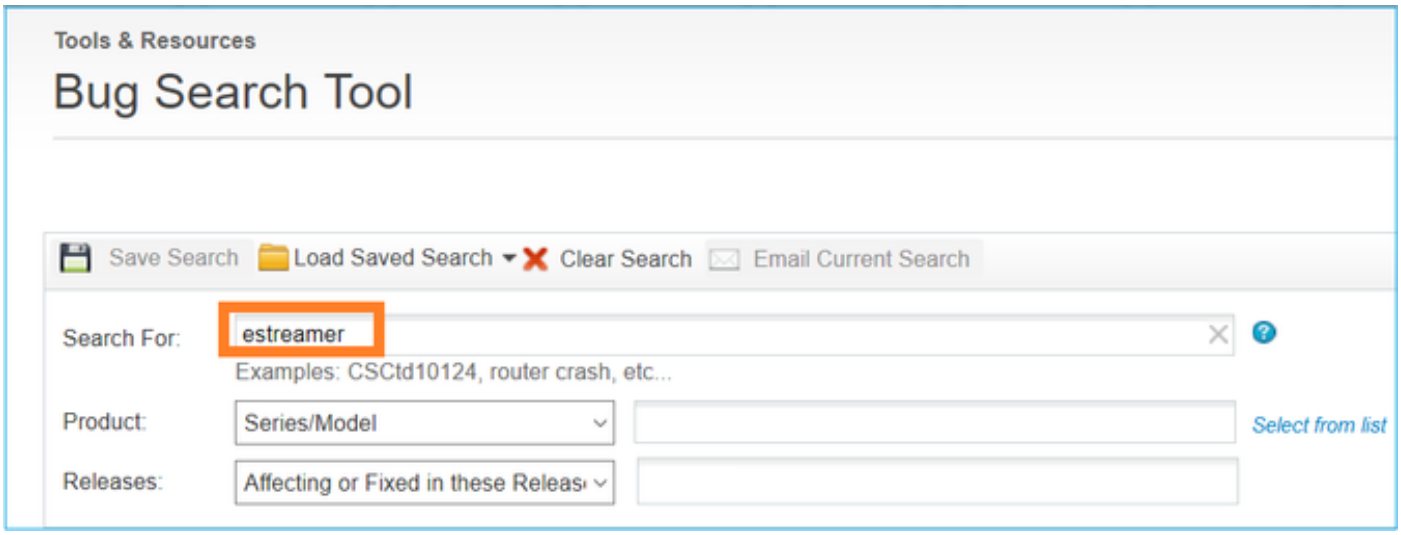
عند تكوين FMC باستخدام المجالات كيف يمكن رؤية معلومات المجال في بيانات eStreamer الخاصة ب FMC؟

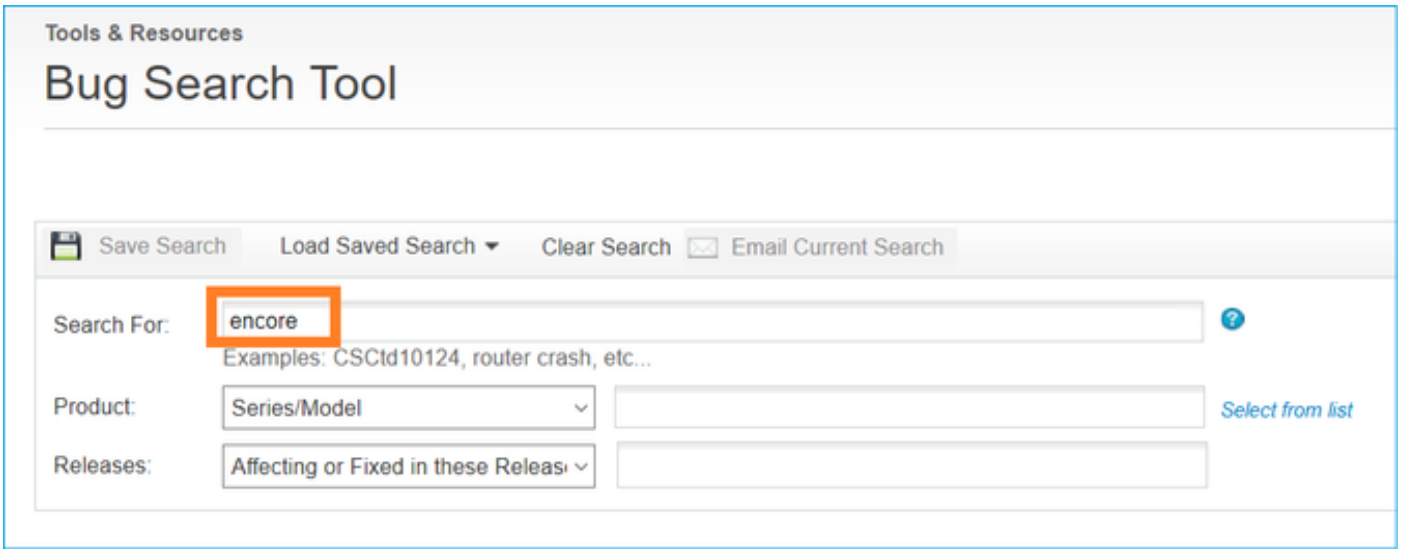
في دليل كامل eStreamer تحقق من رقم **معرف NetMap** بجوار عنوان السجل في قسم الرأس الخاص بالعديد من أنواع السجالت المختلفة. يمكن تحويل رقم معرف NetMap إلى اسم مجال باستخدام جهاز **بيانات تعريف مجال NetMap** (نوع السجل 350) و**بيانات تعريف سجل الأجهزة المدارة** (نوع السجل 123)، على التوالي.

يجب أن يقوم تطبيق العميل بتفسير البيانات الثنائية وبيانات التعريف وفقا للمعلومات الواردة في دليل تكامل eStreamer.

مشكلات معروفة

افتح أداة البحث عن الأخطاء وابحث عن مشاكل الشوارع والأشرطة، على سبيل المثال.





معلومات ذات صلة

- تطوير خادم eStreamer

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).