瞭解eStreamer並排除eCore整合故障

目錄

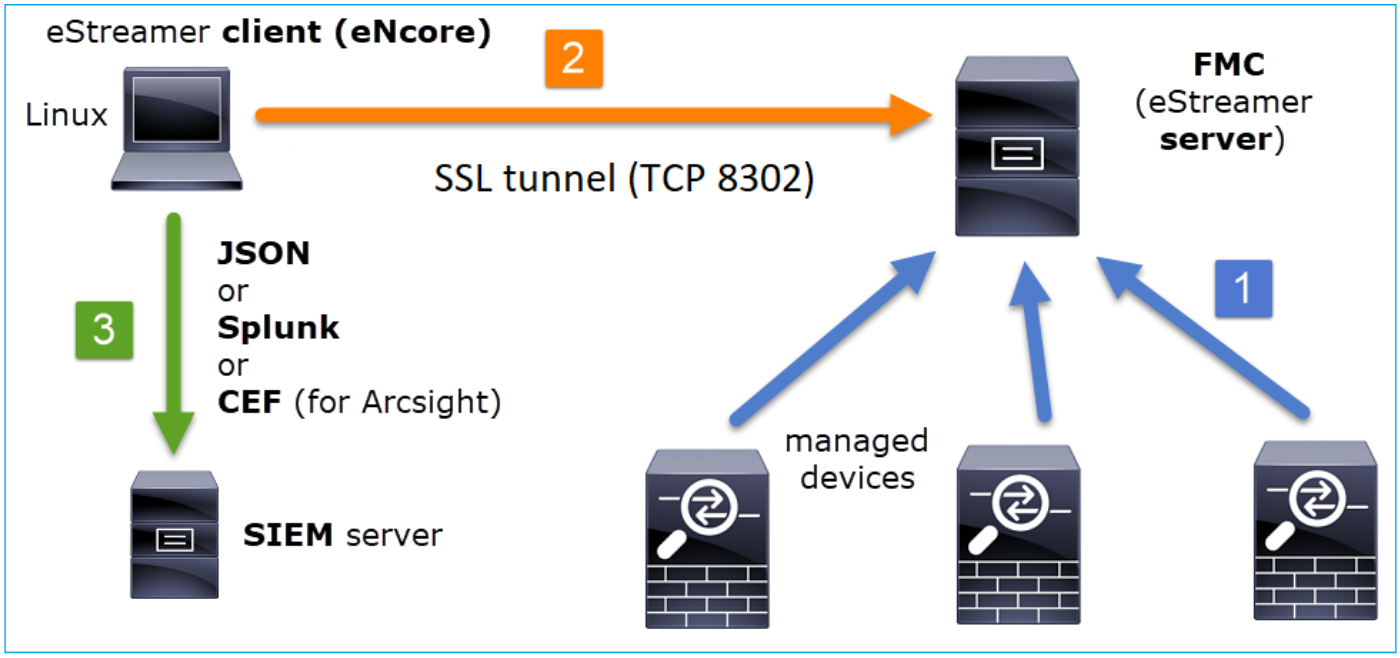
簡介

本檔案將介紹Cisco Event Streamer（也稱為eStreamer）Ncore CLI客戶端。具體而言，介紹該操作並提供故障排除資訊。此外，它還涵蓋思科技術支援中心(TAC)發現的常見問題以及常見問題(FAQ)。

作者：David Torres Rivas、Mikis Zafiroudis、思科TAC工程師。

概觀

eCore是一個通用客戶端，它從eStreamer伺服器(FMC)請求所有可能的事件，分析二進位制內容，並以各種格式輸出事件以支援其他安全資訊和事件管理工具(SIEM)。



eStreamer連線建立

客戶端(eNcore)發起與FMC TCP埠8302的連線，在此執行SSL握手：

```
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>
```

FMC接受連線，在同一埠上執行SSL握手，並驗證客戶端公用名(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
```

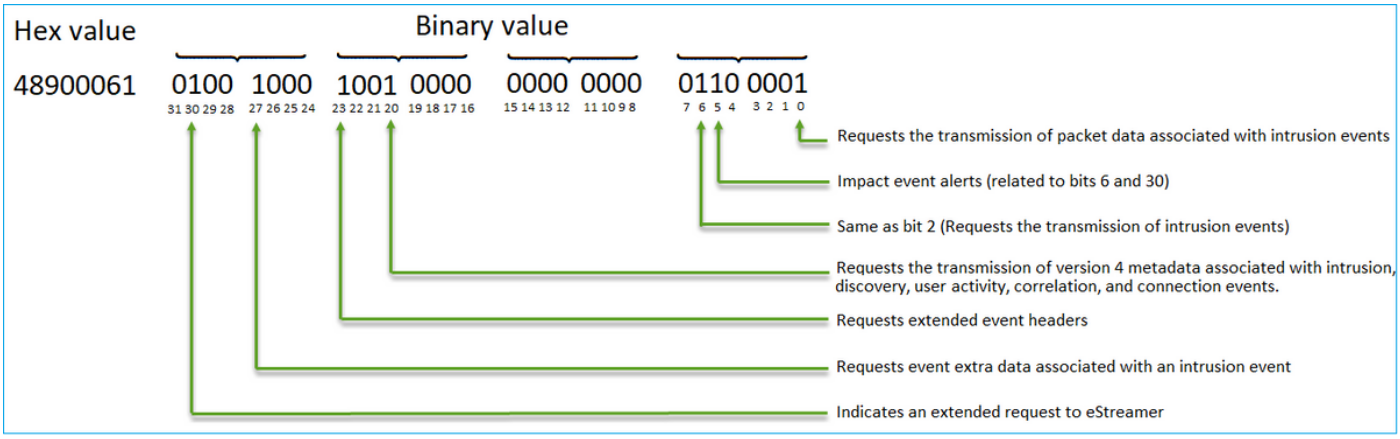
然後，eStreamer客戶端檢查其配置和書籤檔案，以確定請求哪些事件和開始時間：

```
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
000700650006006f0002008300000000
```

EventStreamRequest可在FMC上關聯：

```
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是Request Flags中描述的請求標誌的十六進位制表示形式，必須轉換為二進位制才能瞭解客戶端是否請求了所需的資料。範例如下：



附註：如果啟動擴展請求，某些標誌位可能會更改提供的資訊。

根據請求位，FMC將資料推送到eStreamer客戶端。

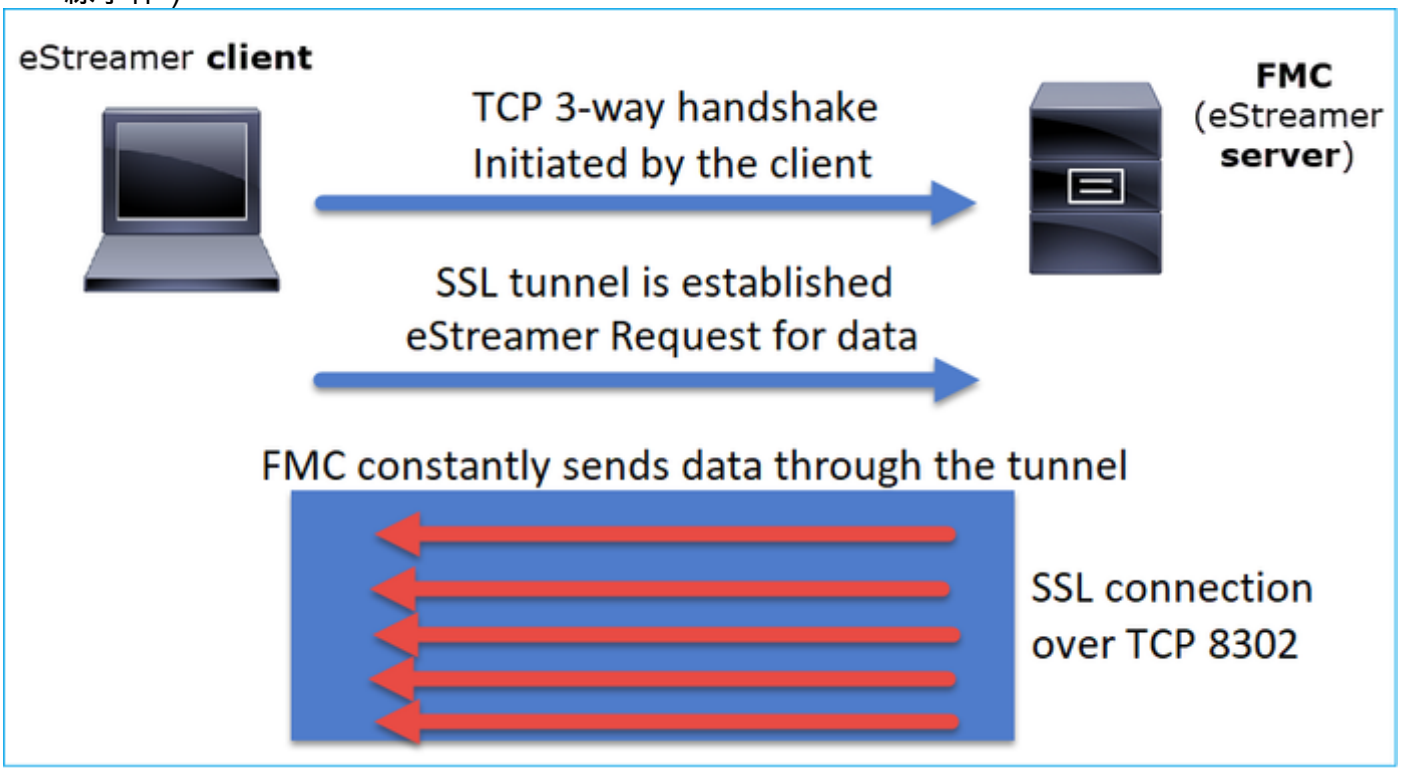
誰啟動eStreamer連線和資料傳輸？

eStreamer客戶端。具體而言，客戶端建立TCP連線（三次握手），然後與客戶端進行SSL協商（雙向）身份驗證。最後，無論何時有資料要傳送，FMC都會通過建立的隧道傳送資料：

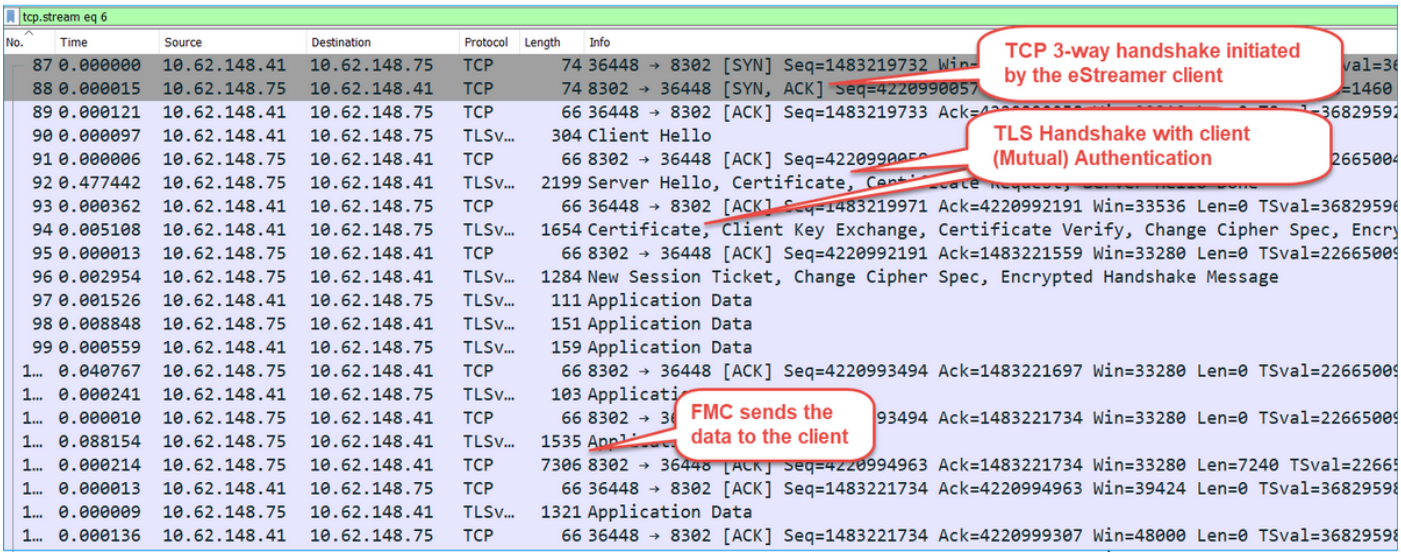
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100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

總而言之：

- 客戶端發起SSL隧道以請求資料（拉入）
- 一旦通道建立，通道就會一直運作，每當從受管裝置取得資料時，FMC都會推送資料（例如連線事件）



在本示例中，IP 10.62.148.41是eStreamer客戶端(eNcore)，而IP 10.62.148.75是FMC:



設定

有關eCore CLI客戶端的詳細資訊，請參閱eStreamer eCore CLI操作指南3.5版。

Event Streamer Integration Guide中介紹了eStreamer應用程式的詳細資訊以及FMC配置步驟。

estreamer.conf檔案調整

本節介紹為了讓解決方案正常工作，可以或者必須在estreamer.conf上修改哪些內容。estreamer.conf檔案位於*path/*eStreamer-eNcore目錄中。以下是檔案內容的範例：

```
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
```

預訂部分

要修改對伺服器(FMC)的事件流處理器請求，請修改eStreamer.conf訂閱部分。例如，將擴展請求設定為false時，會更改FMC上的EventStream請求：

```
"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
        },
```

擴展請求= 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
```

使用擴展請求= 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
```

日誌記錄部分

要在eCore CLI上啟用調試，請編輯estreamer.conf檔案並更改日誌級別：

```
 "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
    },
```

Monitor部分

要檢視每秒處理的事件的數量和當前書籤，請編輯estreamer.conf上的monitor部分：

```
  "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)
  },
```

其他相關頂級金鑰：

```
"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.
```

此值可以設定為2-12。更多進程旨在改進效能，但每個進程都會產生開銷成本。結果表明，在主機處理能力與「處理次數」的正確組合下，可以獲得最優的效能。現有的最佳准則包括：

- 對於2個核心："workerProcesses":4
- 對於4個或更多核心："workerProcesses":12

疑難排解

有關一般eStreamer故障排除過程，請參閱文檔FireSIGHT系統和eStreamer客戶端(SIEM)之間的故障排除問題

出於測試目的，您可以啟用eNcore作為前台進程並驗證與FMC的通訊

```
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
000700650006006f0002008300000000
2020-06-04 11:48:00,653 Monitor      INFO     Running. 0 handled; average rate 1.2 ev/sec;
```

同時，在FMC上，當eNcore流處理器客戶端建立連線時，您可以看到類似這些日誌。請注意，FMC後端時區始終為UTC:

```
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
```

在聯絡思科技術協助中心(TAC)之前收集的專案

強烈建議您在聯絡Cisco TAC之前收集以下專案：

- eStreamer eCore的版本
- Python版本
- 主機作業系統的版本
- 您看到FMC上的事件嗎？共用來自事件+ FMC eStreamer配置的螢幕截圖
- 在eCore CLI上啟用調試（如「logging section」中所述）
- 從FMC生成故障排除檔案

- 從eCore提供以下檔案：
  estreamer.conf
  estreamer.log

常見問題

TCP埠8302無連線

從eStreamer客戶端Telnet至FMC埠8302，並驗證是否已建立連線。

此外，您還可以使用eNcore測試選項來測試連線：

```
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
XHgwMFx4MDBceDA4XHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MWFceDBiXHgwMFx4MDBceDAw
XHgwOFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwJwpwNApzUydtZXNzYWdlVHlwZScKcDUKSTIwNTEKcy4=
2020-05-28 16:02:56,957 Diagnostics  INFO     Streaming info response
2020-05-28 16:02:56,957 Diagnostics  INFO     Connection successful
```

這是一次成功的連線嘗試，如在Wireshark中所見（10.62.148.41是eCore IP，而10.62.148.75是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

證書CN與遠端主機不匹配

如果eStreamer客戶端位於NAT之後，必須使用上游IP地址生成證書，或者出現以下錯誤：

```
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
```

eStreamer客戶端的FMC DNS解析不正確

如果FMC的eStreamer客戶端的DNS條目有誤，則事件不會到達客戶端。要確定問題是否存在，請捕獲有關FMC的資訊。在此範例中，FMC收到來自串流器使用者端主機ksec-sfvm-win7-3.cisco.com的TCP SYN封包：

```
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
```

您可以使用**-n**標誌檢視已解析的IP:

```
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
```

或者，您可以從FMC CLI使用**nslookup**命令工具：

```
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
```

由於SSL證書錯誤而導致的電子流處理器通訊問題

確保eStreamer客戶端使用正確的FMC SSL證書。如果FMC /var/log/message檔案中的證書不正確，您將看到以下事件：

```
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
```

您可以刪除FMC上的eStreamer客戶端並重新配置。這會重新生成SSL證書。將新證書匯入到eStreamer客戶端。

在eStreamer上為ASA SFR模組整合配置的IP地址錯誤

在eStreamer客戶端上，必須使用SFR模組IP。在ASA上，運行命令**show sfr module details**以檢視模組IP。

ArcSight公共事件格式(CEF)

Arcsight公共事件格式標準定義了必須從Core CLI傳送的鍵值對。如果Arcisght上收到的資料不一致，即：缺少欄位、順序錯誤或某些資料在Arcsight客戶端上未正確分析，通過設定來修改配置以寫入日誌檔案非常有用。這有助於確定問題所在。

```
    "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"
                }
            }
        ],
```

RAW CEF事件以線條書寫，每個欄位用管道「|」分隔：

```
<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
```

eStreamer客戶端不顯示所有日誌

這通常是由於eStreamer客戶端超訂用（FMC傳送的事件太多）。 在eStreamer客戶端運行此命令，並檢查Recv-Q計數器是否高。這是連線到此套接字的使用者程式未複製的位元組數。在本示例中，客戶端有143143個待處理的位元組：

```
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
```

檢查eStreamer客戶端每秒接收的事件。這為您提供了每秒事件數的指示：

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

嘗試減少eStreamer客戶端請求的資料量或FMC傳送的事件的型別。或者，您可以嘗試增加在eStreamer客戶端上分配的資源量。

常見問題 (FAQ)

從何處獲取eCore-cli軟體包？

- 檢查FMC軟體下載頁面、**Firepower System Tools and APIs** - eNcore for CEF
- 或者，您可以從https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets獲取最新的eNcore檔案

進行FMC完全備份時，eStreamer不會生成事件。這正常嗎？

是的，這是預期行為。在FMC配置指南的備份時間：

當系統收集備份資料時，資料關聯中可能會出現臨時暫停（僅限FMC），並且可能會阻止您更改與備份相關的配置。

FMC與eStreamer客戶端（例如Qradar）整合是否需要任何特殊許可證？

否

eStreamer事件的來源是什麼？

FMC。具體而言，FMC從受管裝置(FTD)取得事件，並將其轉送到eStreamer使用者端，例如eNcore、ArcSight、Splunk、QRadar、LogRhythm等。

Splunk和eNcore之間是否存在任何相容性矩陣？

檢查Splunk文檔以獲取相容性資訊。例如，要檢視哪些Splunk版本與eNcore 3.6.8版相容，請檢視https://splunkbase.splunk.com/app/3662/

eStreamer eNcore能否使用來自多個FMC的資料？

在撰寫本文時，否。請檢查增強請求CSCvq14351

為FMC高可用性(HA)設定配置eStreamer的建議選項是什麼？

建議只為eStreamer配置活動FMC單元。如果為eStreamer配置兩個FMC單元，則SIEM會收到重複事件，因為備用FMC會響應eStreamer請求。相關增強請求：CSCvi95944

FMC升級是否需要手動生成新的eStreamer證書？

否

是否將安全情報事件傳送到eStreamer客戶端？是否可以選擇安全情報事件作為單獨的類別並將其傳送到eStreamer客戶端？

安全情報(SI)事件包含在「連線」事件的類別下，而不是作為一個單獨的類別。因此，沒有單獨的SI事件傳送到流處理器。相關增強請求：CSCva39052

是否可以在FMC上指定將其eStreamer事件傳送到eStreamer客戶端的感測器/受管裝置？

目前只有一個FMC網域，這是不可能的。相關增強請求CSCvt31270。或者，您可以在FMC上設定兩個不同的網域。在第一個域中，新增要為eStreamer客戶端啟用eStreamer的所有受管裝置並對其進行配置。對於第二個域，您可以新增其餘裝置而不配置eStreamer。

Firepower上的eStreamer版本是什麼？我需要SIEM配置的此資訊（例如LogRhythm）

要從FMC UI檢查Firepower(FMC)版本，請導航至**Help**（右上角）> **About** > **Software version**

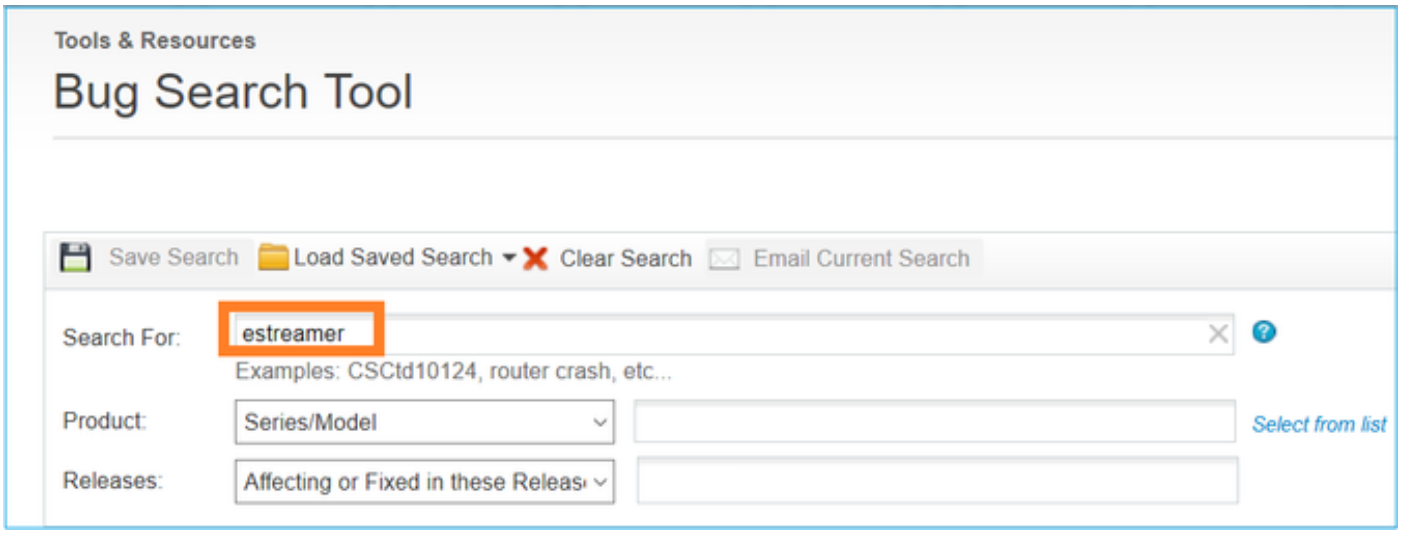
當FMC配置了域時，如何檢視FMC電子流處理器資料中的域資訊？

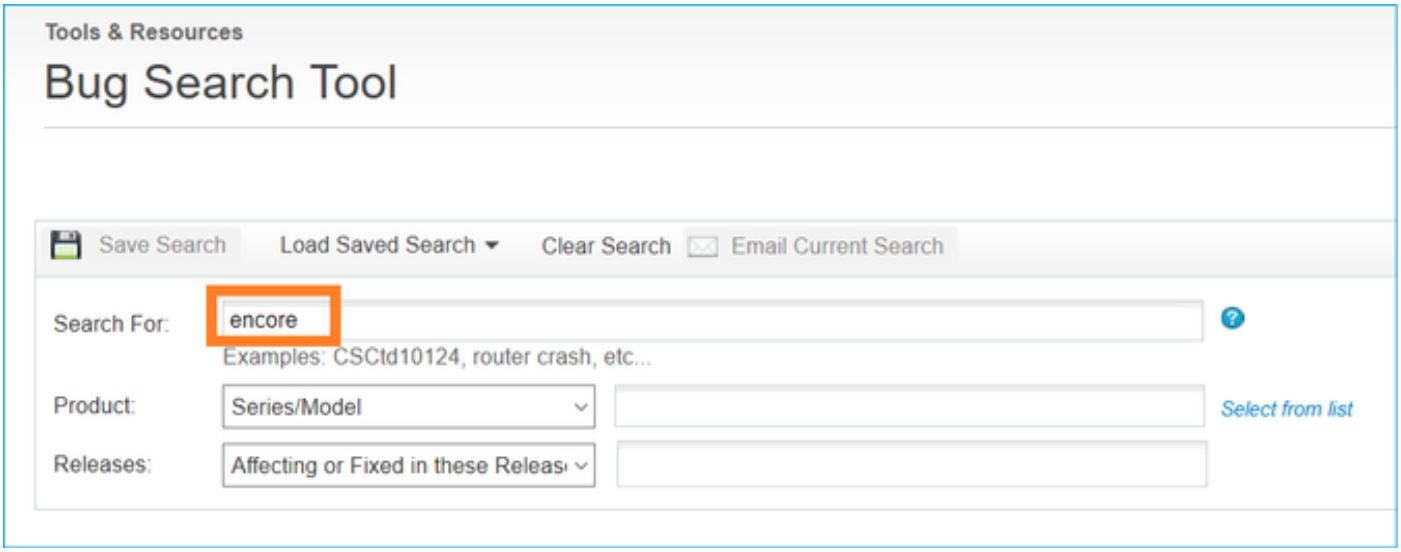
在eStreamer Integration Guide中，檢查許多不同記錄型別的標題部分中記錄型別旁邊的**Netmap ID**號。可以分別使用**Netmap Domain Metadata**（記錄型別350）和**Managed Device Record Metadata**（記錄型別123）將Netmap ID號轉換為域或裝置名稱。

客戶端應用程式必須根據《eStreamer整合指南》中提供的資訊解釋二進位制資料和後設資料。

已知的問題

開啟Bug Search Tool，並搜尋串流器和核心問題，例如





相關資訊

- eStreamer伺服器串流