了解eStreamer并排除eCore集成故障

目录

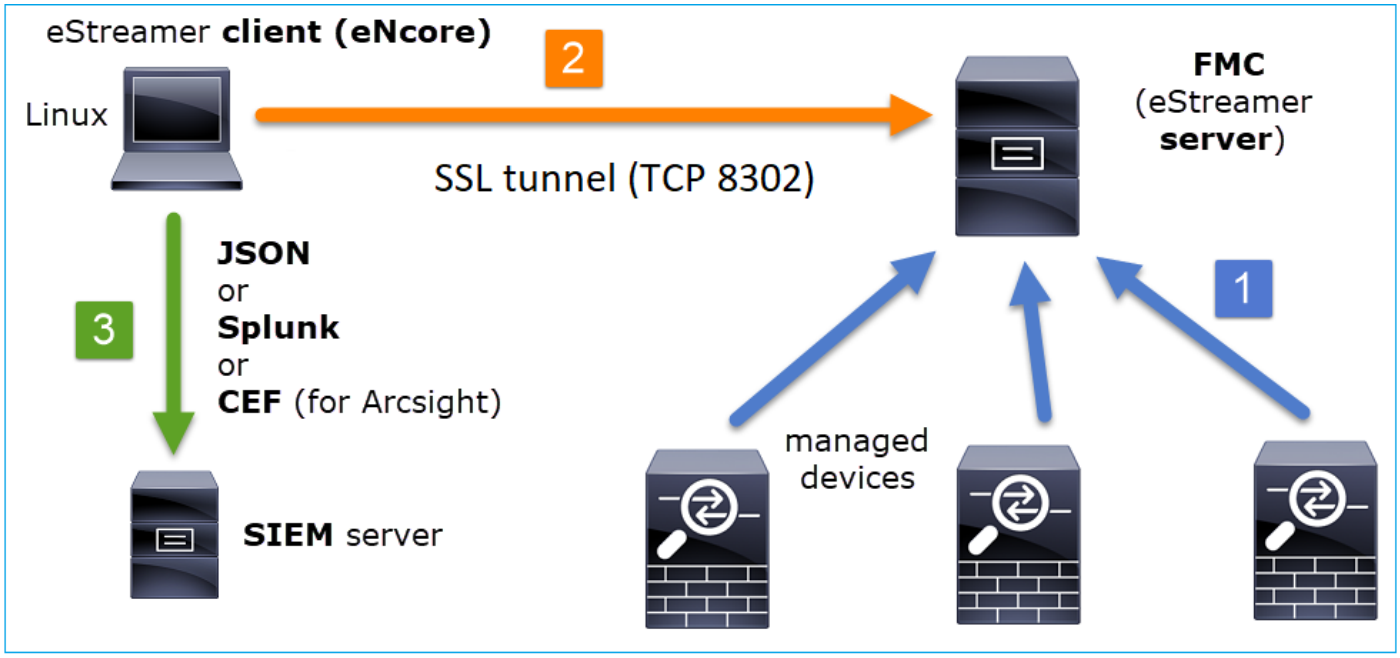
简介

本文档介绍Cisco Event Streamer（也称为eStreamer）eNcore CLI客户端。具体来说，它描述了操作并提供故障排除信息。此外，它还涵盖思科技术支持中心(TAC)发现的常见问题以及常见问题(FAQ)。

作者：David Torres Rivas、Mikis Zafeiroudis，Cisco TAC工程师。

概述

eNcore是一个多用途客户端，它从eStreamer服务器(FMC)请求所有可能的事件，解析二进制内容，并以各种格式输出事件，以支持其他安全信息和事件管理工具(SIEM)。



eStreamer连接建立

客户端(eNcore)启动到FMC TCP端口8302的连接，在该端口上执行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接受连接，在同一端口上执行SSL握手并验证客户端公用名(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
```

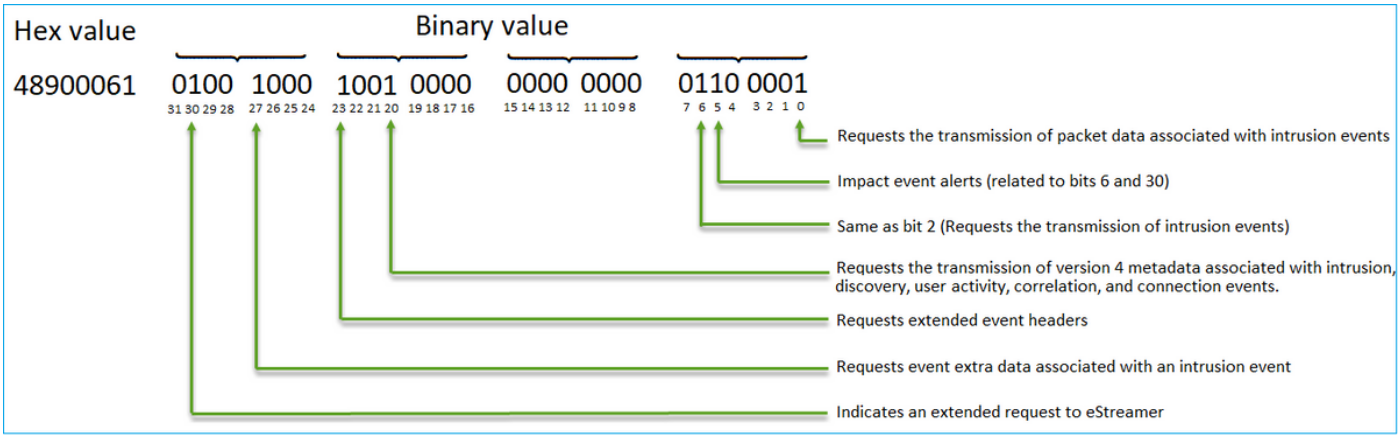
然后，eStreamer客户端会检查其配置和书签文件，以确定要请求的事件和开始时间：

```
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可以在FMC上关联：

```
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是请求标志上描述的请求标志的十六进制表示形式，必须转换为二进制才能了解客户端是否请求了所需的数据。示例如下：



注意：如果启动扩展请求，某些标志位可能会更改提供的信息。

根据请求位，FMC将数据推送到eStreamer客户端。

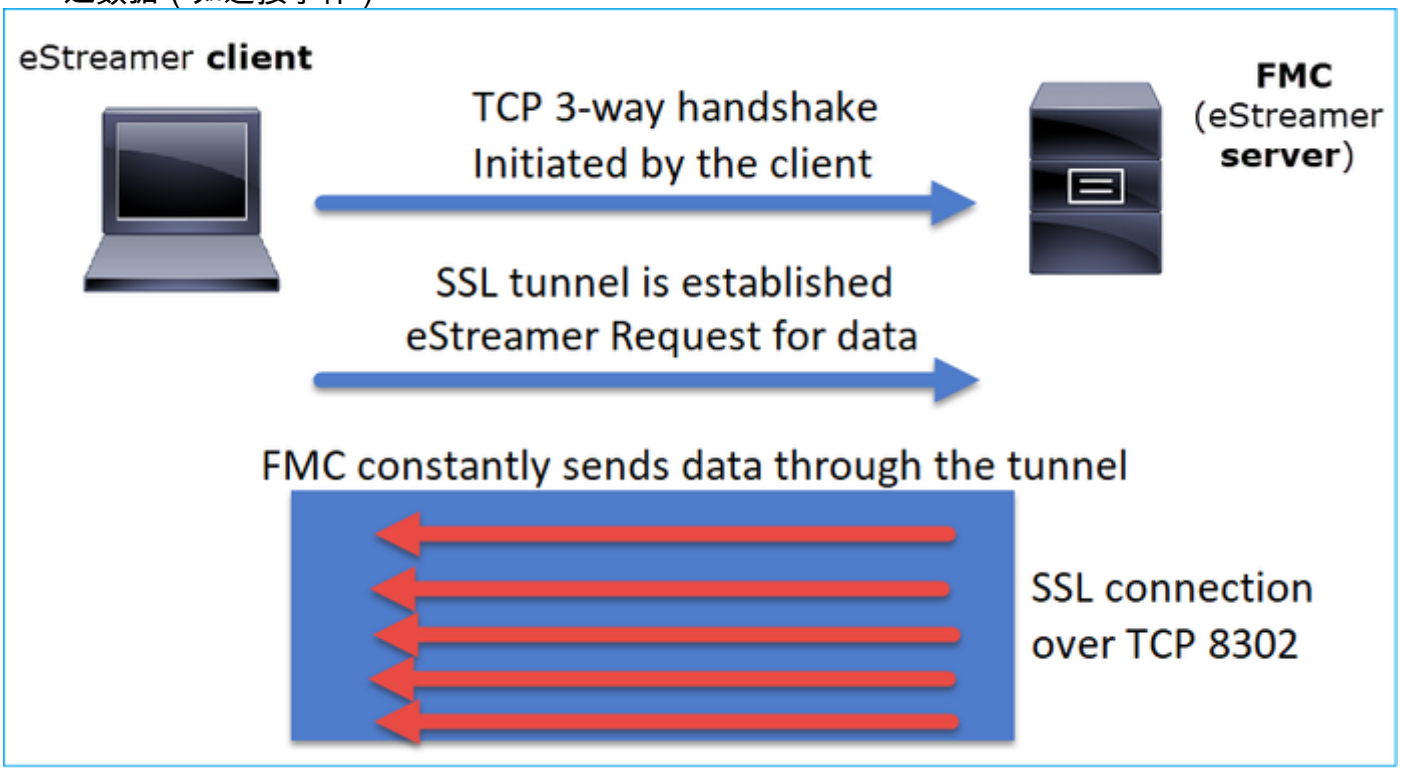
谁发起eStreamer连接和数据传输？

eStreamer客户端。具体而言，客户端建立TCP连接（三次握手），然后与客户端进行SSL协商（相互）身份验证。最后，只要有数据要发送，FMC就会通过建立的隧道发送数据：

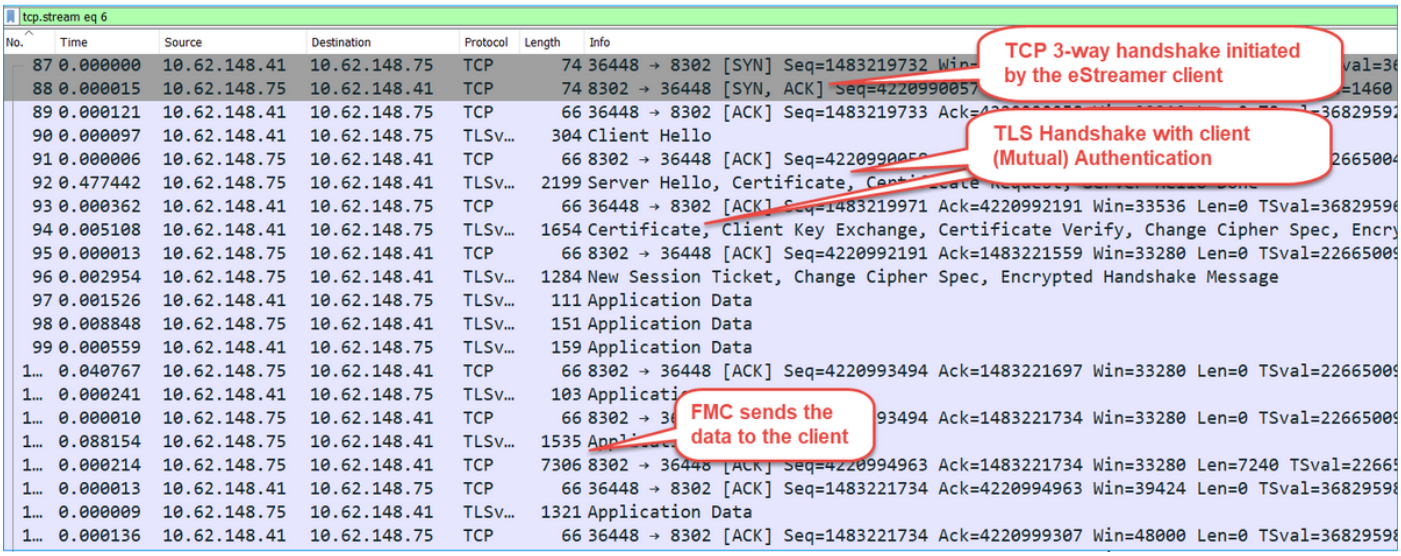
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100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

小结：

- 客户端启动SSL隧道以请求数据（拉）
- 隧道建立后，无论何时从受管设备获取数据（如连接事件），隧道都保持UP状态，FMC都会推送数据（如连接事件）



在本例中，IP 10.62.148.41是eStreamer客户端(eNcore)，而IP 10.62.148.75是FMC:



配置

有关eNcore CLI客户端的详细信息，请参阅eStreamer eNcore CLI操作指南v3.5。

《Event Streamer集成指南》中介绍了eStreamer应用的详细信息以及FMC配置步骤。

estreamer.conf文件调整

本节介绍可以或必须在estreamer.conf上修改什么才能使解决方案正常工作。estreamer.conf文件位于*path* /eStreamer-eNcore目录中。以下是文件内容的示例：

```
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
```

订用部分

要修改指向服务器(FMC)的Event Streamer请求，请修改eStreamer.conf订用部分。例如，将扩展请求设置为false时，它会更改FMC上的EventStream请求：

```
"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
        },
```

使用扩展请求=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
```

使用扩展请求= 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
```

日志记录部分

要在eNcore CLI上启用调试，请编辑estreamer.conf文件并更改日志级别：

```
 "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
    },
```

监视器部分

要查看已处理事件/秒数和当前书签的数量，请编辑estreamer.conf上的监控器部分：

```
  "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)
  },
```

其他相关顶级键：

```
"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.
```

此值可以从2到12设置。更多流程旨在提高性能，但每个流程都有开销成本。结果表明，将“进程数”与主机处理能力正确结合，可获得最佳性能。可用的最佳准则包括：

- 对于2个内核："workerProcesses":4
- 对于4个或更多内核："workerProcesses":12

故障排除

有关通用eStreamer故障排除步骤，请参阅本文档“FireSIGHT系统与eStreamer客户端(SIEM)之间的问题故障排除”

为了进行测试，您可以启用eNcore作为前台进程并验证与FMC的通信

```
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;
```

同时，在FMC上，当Necore流处理器客户端建立连接时，您可以看到这些日志。请注意，FMC后端时区始终为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
```

在联系思科技术支持中心(TAC)之前要收集的项目

强烈建议您在联系思科TAC之前收集以下项目：

- eStreamer eNcore的版本
- Python的版本
- 主机操作系统的版本
- 您看到FMC上的活动吗？共享事件+ FMC eStreamer配置的屏幕截图
- 在eNcore CLI上启用调试（如“logging section”中所述）
- 从FMC生成故障排除文件

- 从eNcore提供以下文件：
  estreamer.conf
  estreamer.log

常见问题

TCP端口8302上无连接

从eStreamer客户端Telnet至FMC端口8302，并检验连接是否已建立。

此外，您还可以使用eNcore测试选项测试连接：

```
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
```

这是成功的连接尝试，如Wireshark中所示（10.62.148.41是eCore IP，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

证书CN与远程主机不匹配

如果eStreamer客户端在NAT后，则必须使用上游IP地址生成证书，否则会出现以下错误：

```
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客户端的FMC DNS解析不正确

如果FMC为eStreamer客户端提供了错误的DNS条目，则事件无法到达客户端。要确定这是否是问题，请捕获FMC。在本示例中，FMC从流处理器客户端主机ksec-sfvm-win7-3.cisco.com接收TCP SYN数据包：

```
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
```

可以使用**-n标**志查看已解析的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，您可以从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
```

由于SSL证书错误导致eStreamer通信问题

确保eStreamer客户端使用正确的FMC SSL证书。如果FMC /var/log/message文件上的证书不正确，您会看到以下事件：

```
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
```

您可以删除FMC上的eStreamer客户端并重新配置它。这将重新生成SSL证书。将新证书导入eStreamer客户端。

为ASA SFR模块集成在eStreamer上配置的IP地址错误

在eStreamer客户端上，必须使用SFR模块IP。在ASA上，运行命令**show sfr module details**查看模块IP。

ArcSight常见事件格式(CEF)

Arcsight公共事件格式标准定义必须从Necore CLI发送的密钥值对。如果Arcisght上收到的数据不一致，例如：缺少字段、顺序混乱或某些数据在Arcsight客户端上未正确解析，通过设置将配置修改为写入日志文件非常有用。这有助于确定问题所在。

```
    "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事件以一行形式写入，每个字段用管道“|”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客户端不显示所有日志

这通常是由于eStreamer客户端超订用（FMC发送的事件太多）。 在eStreamer客户端上运行此命令，并检查Recv-Q计数器是否高。这是连接到此套接字的用户程序未复制的字节数。在本示例中，客户端上有143143个待处理字节：

```
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
```

检查eStreamer客户端每秒收到的事件数。这为您提供了每秒事件数的指示：

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

尝试降低eStreamer客户端请求的数据量或FMC发送的事件类型。或者，您可以尝试增加在eStreamer客户端上分配的资源量。

常见问题(FAQ)

从何处获取eNcore-cli软件包？

- 检查FMC软件下载页、Firepower系**统工具和API - eCore for CEF**
- 或者，您可以从https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets获取最新的Ncore文件

当正在进行FMC完全备份时，eStreamer不生成事件。这是否正常？

是的，这是预期行为。从FMC配置指南何时备份：

当系统收集备份数据时，数据关联中可能会暂停（仅限FMC），并且可能会阻止您更改与备份相关的配置。

FMC与eStreamer客户端（如Qradar）集成是否需要任何特殊许可证？

无

eStreamer活动从何处获得？

FMC。具体而言，FMC从受管设备(FTD)获取事件，并将其转发到eStreamer客户端，如eNcore、ArcSight、Splunk、QRadar、LogRhythm等。

Splunk和eNcore之间是否有兼容矩阵？

检查Splunk文档以了解兼容性信息。例如，要查看哪些Splunk版本与eNcore版本3.6.8兼容，请选中https://splunkbase.splunk.com/app/3662/

eStreamer eNcore是否能使用来自多个FMC的数据？

在撰写本文时，否。检查增强请求CSCvq14351

为FMC高可用性(HA)设置配置eStreamer的推荐选项是什么？

建议仅为eStreamer配置活动FMC设备。如果为eStreamer配置两个FMC设备，则SIEM会收到重复事件，因为备用FMC会响应eStreamer请求。相关增强请求：CSCvi95944

FMC升级是否需要手动生成新的eStreamer证书？

无

安全情报事件是否被发送到eStreamer客户端？是否可以将安全情报事件选择为单独的类别，并将其发送到eStreamer客户端？

安全情报(SI)事件包含在连接事件类别中，而不是单独的类别。因此，没有单独的SI事件发送到流处理器。相关增强请求：CSCva39052

能否在FMC上指定将其eStreamer事件发送到eStreamer客户端的传感器/受管设备？

当前只有一个FMC域时，这是不可能的。相关增强请求CSCvt31270。或者，在FMC上配置两个不同的域。在第一个域中，添加要为eStreamer客户端启用和配置eStreamer的所有受管设备。对于第二个域，添加其余设备，但不配置eStreamer。

Firepower上的eStreamer版本是什么？我需要此信息用于SIEM配置（例如LogRhythm）

要从FMC UI中检查Firepower(FMC)版本，请导航至“帮助”(**右上角**)>“关于”**>“软件版本”**

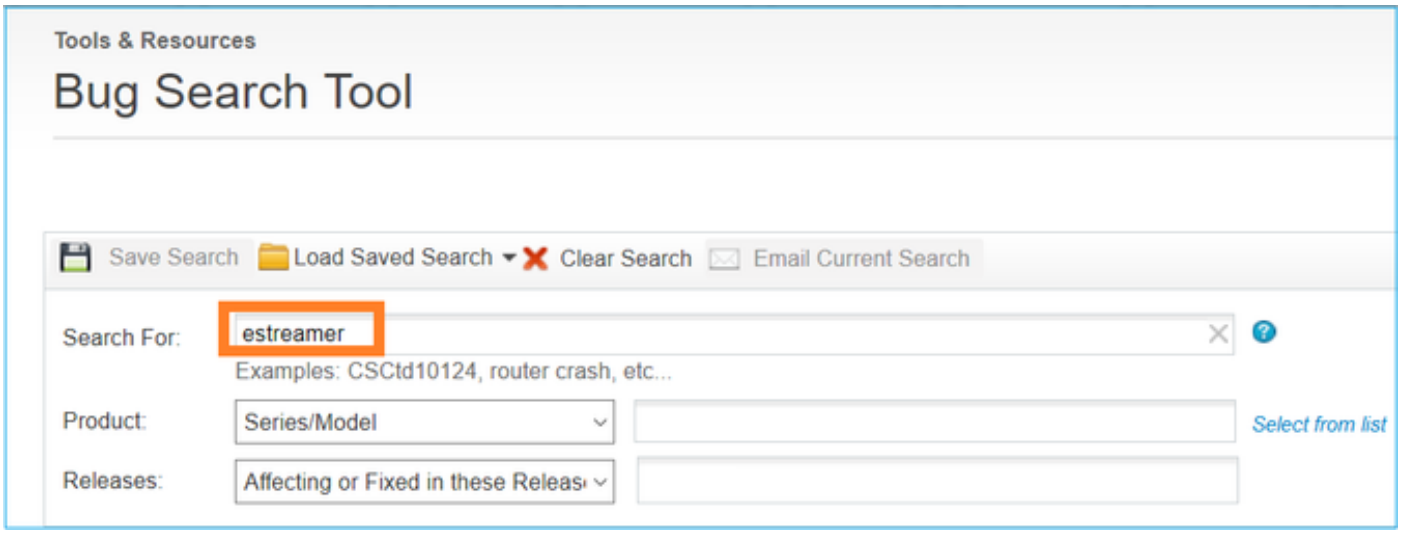
当FMC配置了域时，如何在FMC eStreamer数据中查看域信息？

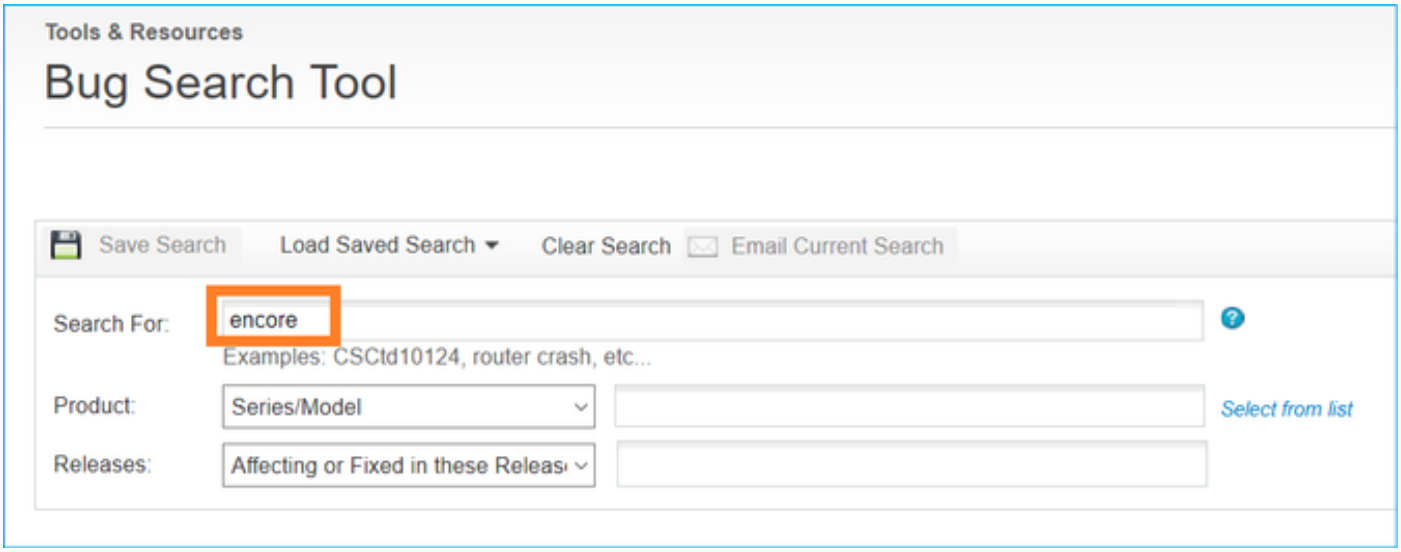
在eStreamer集成指南中，检查**Netmap ID** 编号，该编号位于许多不同记录类型的报头部分的“记录类型”旁。Netmap ID号可以分别使用**Netmap域元数据**（记录类型350）和**受管设备**记录元数据（记录类型123）转换为域或设备名称。

客户端应用程序必须根据《eStreamer集成指南》中提供的信息解释二进制数据和元数据。

已知问题

打开Bug搜索工具并搜索流处理器和核心问题，例如





相关信息

- eStreamer服务器流