eStreamerの理解とコア統合のトラブルシューティング

内容

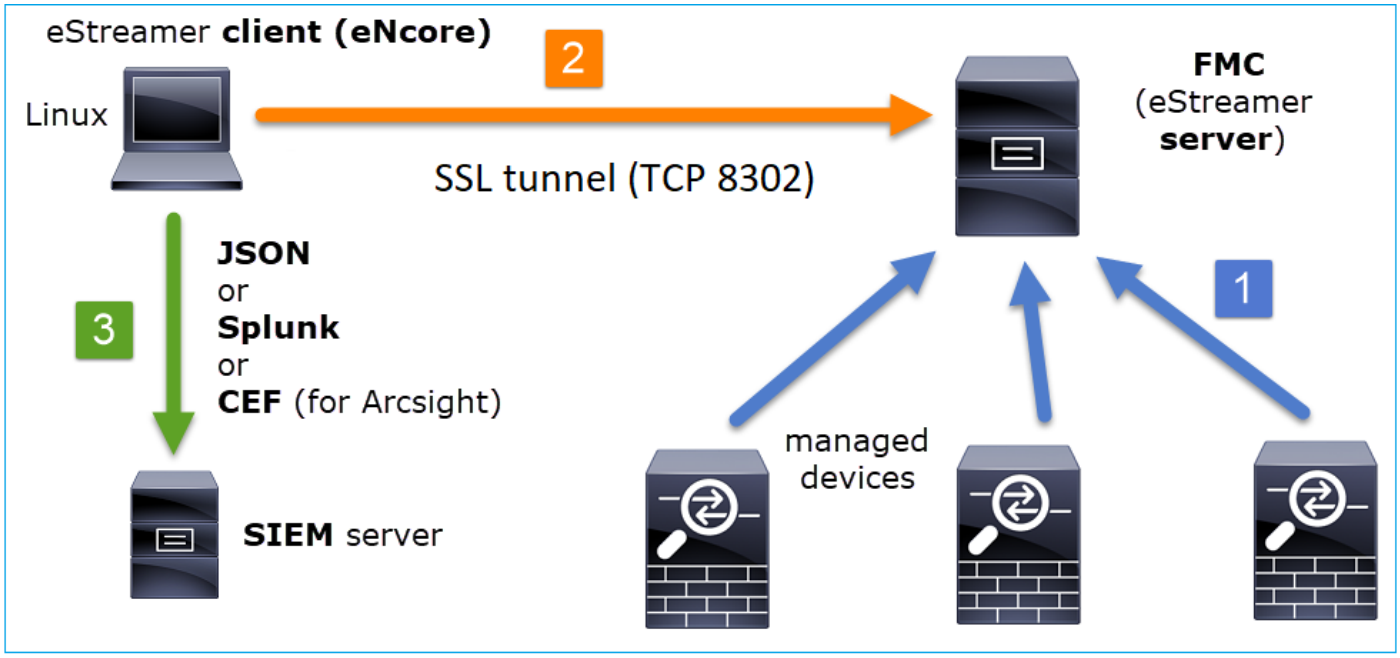
概要

このドキュメントでは、Cisco Event Streamer（eStreamerとも呼ばれる）Ncore CLIクライアントについて説明します。具体的には、動作を説明し、トラブルシューティング情報を提供します。また、Cisco Technical Assistance Center(TAC)で見られる一般的な問題とFAQについても説明します。

著者：Cisco TACエンジニア、David Torres Rivas、Mikis Zafeirodis

概要

Ncoreは、eStreamerサーバ(FMC)に可能なすべてのイベントを要求し、バイナリコンテンツを解析し、他のセキュリティ情報およびイベント管理ツール(SIEM)をサポートするためにさまざまな形式でイベントを出力する汎用クライアントです。



eStreamer接続の確立

クライアント(Ncore)は、SSLハンドシェイクが実行されるFMC TCPポート8302への接続を開始します。

```
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は接続を受け入れ、同じポートでSSLハンドシェイクを実行し、クライアントの共通名(CN)を確認します。

```
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
```

次に、eStreamerクライアントは設定ファイルとブックマークファイルをチェックして、要求す

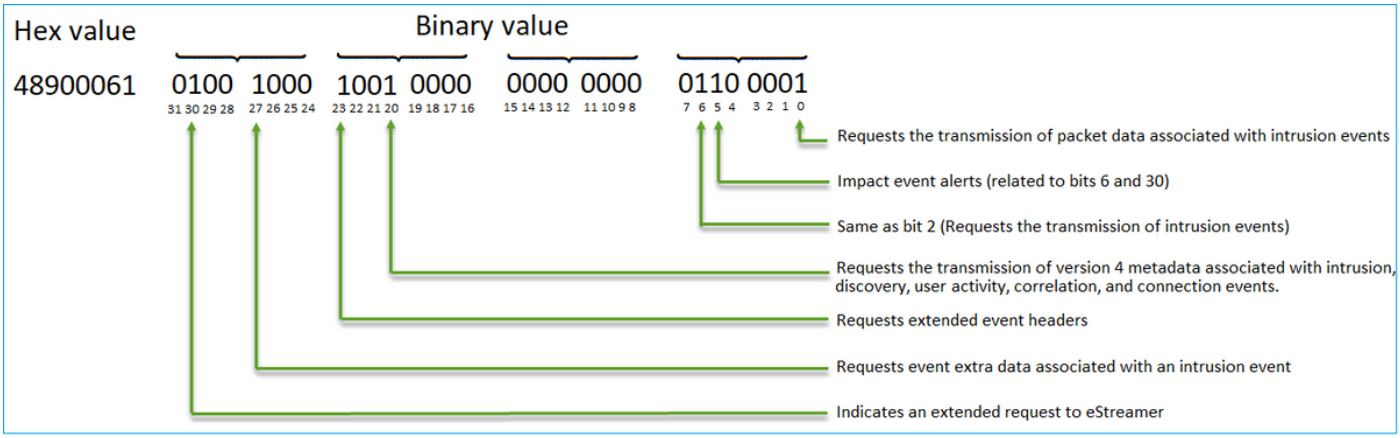
るイベントと開始時刻を判別します。

```
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
```

EventStreamRequestはFMCに関連付けることができます。

```
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は、要求フラグに記述された要求フラグを16進数で表したもので、クライアントが必要なデータを要求したかどうかを理解するため、バイナリに変換する必要があります。次に例を示します。



> **注**：一部のフラグビットは、拡張要求が開始されると、提供される情報を変更する可能性があります。

要求ビットに基づいて、FMCはデータをeStreamerクライアントにプッシュします。

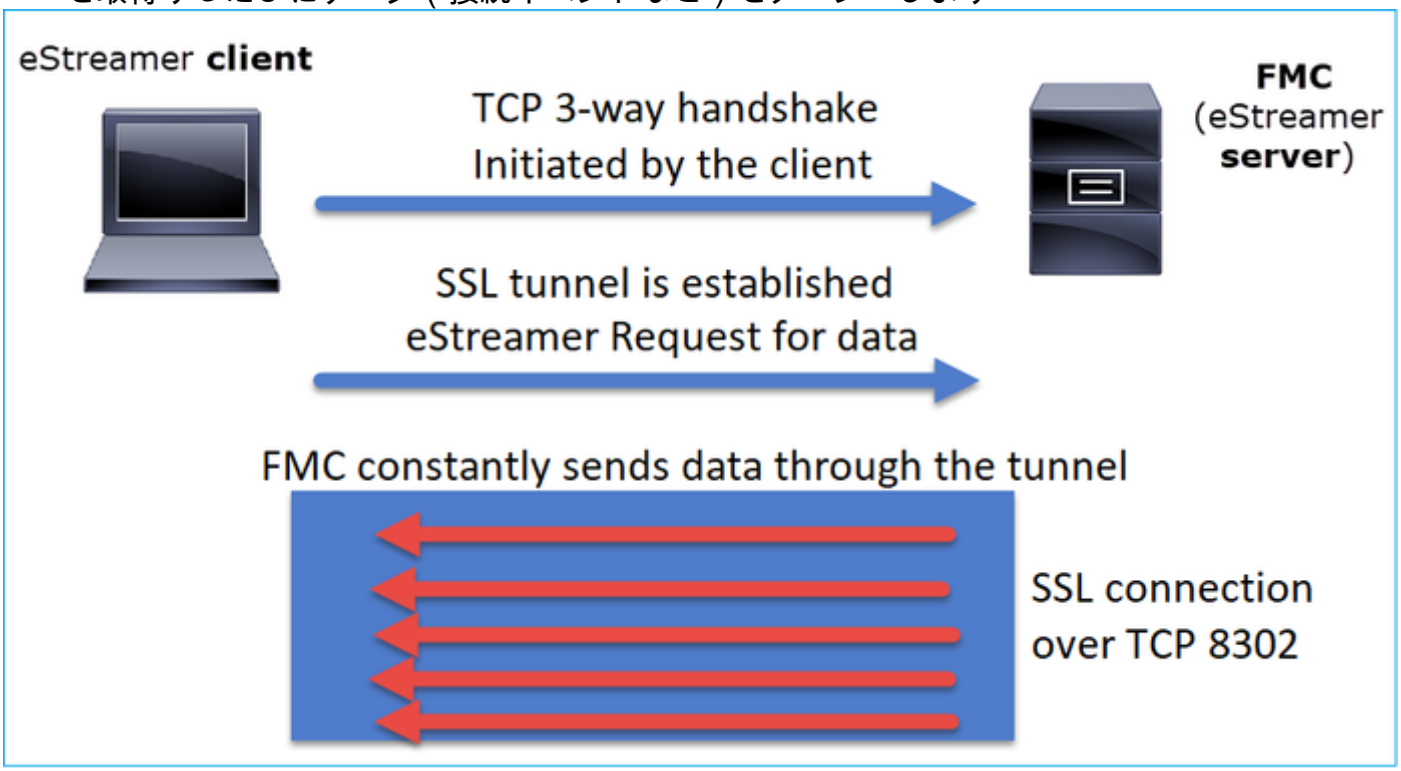
eStreamer接続とデータ転送を開始するのは誰ですか。

eStreamerクライアント。具体的には、クライアントがTCP接続（3ウェイハンドシェイク）を確立し、クライアント（相互）認証とのSSLネゴシエーションがあります。最後に、確立されたトンネルを介して、送信するデータがあるたびにFMCがデータを送信します。

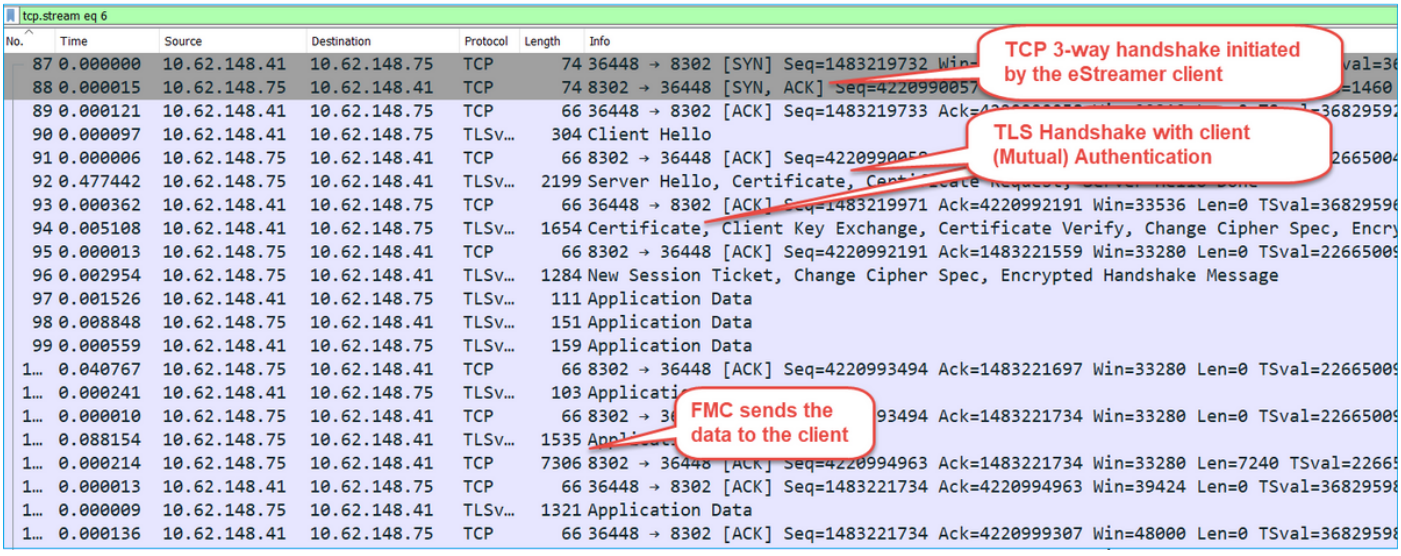
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor       INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor       INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor       INFO     Running.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

ここまでの内容をまとめます。

- クライアントがSSLトンネルを開始してデータを要求（プル）
- トンネルが確立されると、トンネルはUPのままになり、FMCは管理対象デバイスからデータを取得するたびにデータ（接続イベントなど）をプッシュします



この例では、IP 10.62.148.41がeStreamerクライアント(eNcore)で、IP 10.62.148.75がFMCです。



設定

Ncore CLIクライアントの詳細については、『eStreamer eNcore CLI Operations Guide v3.5』を

参照してください。

eStreamerアプリケーションとFMC設定手順の詳細については、『Event Streamer Integration Guide』を参照してください。

estreamer.confファイルの調整

このセクションでは、ソリューションが正常に動作するためにestreamer.confで変更できる内容と変更する必要がある内容について説明します。estreamer.confファイルは、*path*/eStreamer-eNcoreディレクトリ内にあります。ファイルの内容の例を次に示します。

```
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
```

定期購読セクション

サーバ(FMC)へのEvent Streamer Requestを変更するには、eStreamer.conf subscriptionsセクションを変更します。たとえば、拡張要求をfalseに設定すると、FMCのEventStream Requestが変更されます。

```
"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
        },
```

拡張要求の場合= 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
```

拡張要求= 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
```

ロギングセクション

Ncore CLIでデバッグを有効にするには、estreamer.confファイルを編集し、ログレベルを変更します。

```
 "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
    },
```

モニタセクション

処理されたイベント/秒および現在のブックマークの数を表示するには、estreamer.confのmonitorセクションを編集します。

```
  "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)
  },
```

関連するその他のトップレベルのキー：

```
"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.
```

この値は2 ~ 12の範囲で設定できます。パフォーマンス向上を目的としたプロセスが増えますが、各プロセスにはオーバーヘッドのコストがかかります。その結果、「プロセス数」とホストマシンの処理能力を適切に組み合わせることで、最適なパフォーマンスを実現できます。使用できる最適なガイドラインは次のとおりです。

- 2コア：「workerProcesses」:4
- 4コア以上：「workerProcesses」:12

トラブルシュート

一般的なeStreamerのトラブルシューティング手順については、このドキュメントの「FireSIGHTシステムとeStreamerクライアント(SIEM)間の問題のトラブルシューティング」を参照してください

テスト目的で、フォアグラウンドプロセスとしてNcoreを有効にし、FMCとの通信を確認できます

```
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;
```

同時に、FMCでは、eNcore streamerクライアントが接続を確立したときに、次のような口グが表示されます。FMCバックエンドタイムゾーンは常にUTCであることに注意してください。

```
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
```

Cisco Technical Assistance Center(TAC)に連絡する前に収集すべき項目

Cisco TACに連絡する前に、次の項目を収集することを強く推奨します。

- eStreamer eNcoreのバージョン
- Pythonのバージョン
- ホストOSのバージョン
- FMCのイベントは見えますか。イベント+ FMC eStreamer設定のスクリーンショットを共有する
- Ncore CLIでデバッグを有効にします（「logging」セクションで説明されています）。
- FMCからのトラブルシューティングファイルの生成
- Ncoreから次のファイルを提供します。
  estreamer.conf
  estreamer.log

一般的な問題

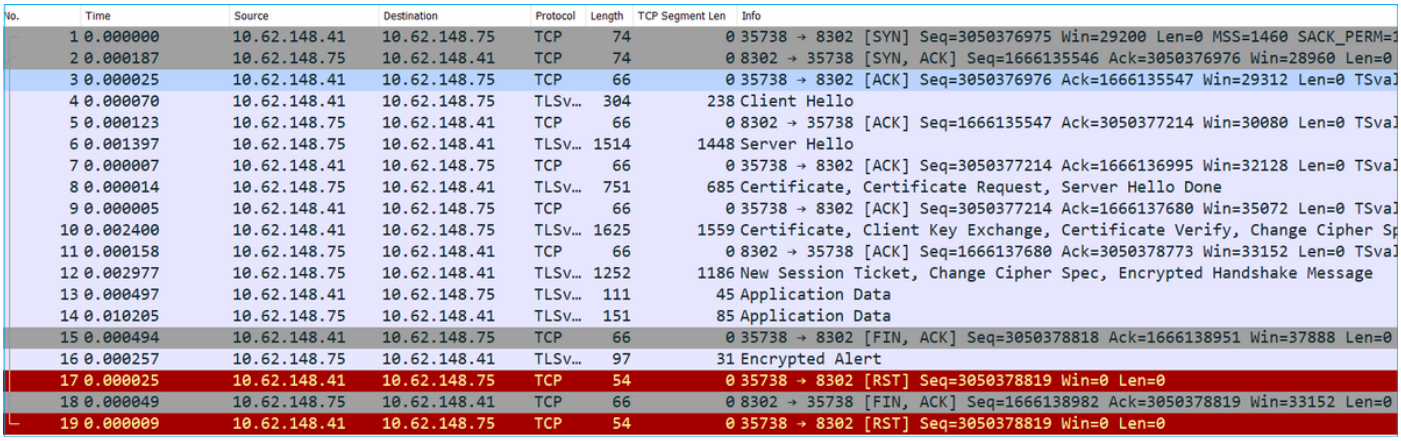
TCPポート8302に接続できない

eStreamerクライアントからFMCポート8302にTelnetで接続が確立されていることを確認します。

さらに、Ncoreテストオプションを使用して接続をテストできます。

```
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
```

これは、Wiresharkで確認できる正常な接続の試みです(10.62.148.41がNcore IPで、10.62.148.75がFMCです)。



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

証明書CNがリモートホストと一致しない

eStreamerクライアントがNATの背後にある場合、証明書はアップストリームのIPアドレスで生成される必要があります。そうでないと、次のような工ラーが表示されます。

```
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クライアントのFMC DNS解決が正しくない

FMCにeStreamerクライアントの誤ったDNSエントリがある場合、イベントはクライアントに到達しません。これが問題であるかどうかを確認するには、FMCでキャプチャを行います。この例では、FMCがストリーマクライアントホストksec-sfvm-win7-3.cisco.comからTCP SYNパケットを受信します。

```
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
```

-nフラグを使用して、解決されたIPを確認できます。

```
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
```

または、FMC CLIからnslookupコマンドツールを使用できます。

```
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
```

SSL証明書エラーによるeStreamer通信の問題

eStreamerクライアントが正しいFMC SSL証明書を使用していることを確認します。FMC /var/log/messageファイルの証明書が正しくない場合、次のイベントが表示されます。

```
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
```

FMC上のeStreamerクライアントを削除し、再設定できます。これにより、SSL証明書が再生成されます。新しい証明書をeStreamerクライアントにインポートします。

ASA SFRモジュール統合のeStreamerに誤ったIPアドレスが設定されている

eStreamerクライアントでは、SFRモジュールのIPを使用する必要があります。ASAでコマンド**show sfr module detailsを実行し**て、モジュールIPを表示します。

ArcSight Common Event Format(CEF)

Arcsight Common Event Format Standardは、eNcore CLIから送信する必要があるキーと値のペアを定義します。Arcisghtで受信されたデータに矛盾がある場合は、次のようになります。フィールドが不足している、順序が正しくない、または一部のデータがArcsightクライアントで正しく解析されない場合は、設定によって口グファイルに書き込むように設定を変更すると便利です。これにより、問題の所在を特定できます。

```
    "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イベントは、各フィールドがパイプ「|」で区切られた行で記述されます。

```
<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クライアントにすべてのログが表示されない

これは、eStreamerクライアントのオーバーサブスクリプション（FMCによって送信されるイベントが多すぎる）が原因で発生することがよくあります。 eStreamerクライアント側でこのコマンドを実行し、Recv-Qカウンタが高いかどうかを確認します。これは、このソケットに接続されたユーザプログラムによってコピーされなかったバイト数です。この例では、クライアント側で143143バイトが保留中です。

```
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
```

eStreamerクライアントが受信した1秒あたりのイベント数を確認します。これにより、1秒あたりのイベント数が表示されます。

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

eStreamerクライアントから要求されるデータ量、またはFMCから送信されるイベントのタイプを減らしてみてください。または、eStreamerクライアント側に割り当てられるリソースの量を増やしてみてください。

よく寄せられる質問（FAQ）

Ncore-cliパッケージの入手先

- FMCソフトウェアのダウンロードページ、**Firepower System Tools and APIs - eCore for CEFを確認します。**
- または、https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assetsから最新のNcoreファイルを取得できます

FMCの完全バックアップが進行中の場合、eStreamerはイベントを生成しません。これは正常な状態ですか。

はい、これは予期された動作です。FMC構成ガイドからバックアップするタイミング：

システムがバックアップデータを収集している間は、データの関連付けに一時的な一時停止が発生する可能性があります（FMCのみ）。バックアップに関連する設定の変更を防止できます。

eStreamerクライアント（Qradarなど）とのFMC統合に必要な特別なライセンスはありますか。

No

eStreamerイベントの送信元はどこですか。

FMC具体的には、FMCは管理対象デバイス(FTD)からイベントを取得し、eNcore、ArcSight、Splunk、QRadar、LogRismなどのeStreamerクライアントに転送します。

SplunkとNcoreの間に互換性マトリクスはありますか。

互換性の情報については、Splunkのドキュメントを参照してください。たとえば、どのSplunkバージョンがeNcoreバージョン3.6.8と互換性があるかを確認するには、https://splunkbase.splunk.com/app/3662/をチェックします

eStreamer eNcoreは複数のFMCからのデータを消費できますか。

このドキュメントの執筆時点では、いいえ。チェック拡張機能の要求CSCvq14351

FMCハイアベイラビリティ(HA)セットアップ用にeStreamerを設定するための推奨オプションは何ですか。

eStreamerのアクティブなFMCユニットだけを設定することを推奨します。eStreamerに両方の

FMCユニットを設定すると、スタンバイFMCがeStreamer要求に応答するため、SIEMは重複イベントを受信します。関連する機能拡張要求：CSCvi95944

FMCのアップグレードでは、新しいeStreamer証明書を手動で生成する必要がありますか。

No

セキュリティインテリジェンスイベントはeStreamerクライアントに送信されますか。セキュリティインテリジェンスイベントを別のカテゴリとして選択し、eStreamerクライアントに送信することはできますか。

セキュリティインテリジェンス(SI)イベントは、接続イベントのカテゴリに含まれ、個別のカテゴリとして含まれません。このため、ストリーマに送信される別のSIイベントはありません。関連する機能拡張要求：CSCva39052

eStreamerイベントがeStreamerクライアントに送信されるセンサー/管理対象デバイスをFMCで指定できますか。

現在、FMCドメインが1つだけの場合、これは不可能です。関連する拡張要求CSCvt31270。または、FMCで2つの異なるドメインを設定します。最初のドメインでは、eStreamerクライアントのeStreamerを有効にし、設定するすべての管理対象デバイスを追加します。2番目のドメインでは、残りのデバイスを追加し、eStreamerを設定しません。

FirepowerのeStreamerのバージョンは何ですか。SIEMの設定（LogRismなど）にはこの情報が必要です

FMC UIからFirepower (FMC)のバージョンを確認するには、[ヘルプ(**Help**)](右上角)> [バージョン**情報] > [ソフトウェアのバージョン]に移動します**

FMCがドメインで設定されている場合、FMC eStreamerデータにドメイン情報を表示する方法を教えてください。

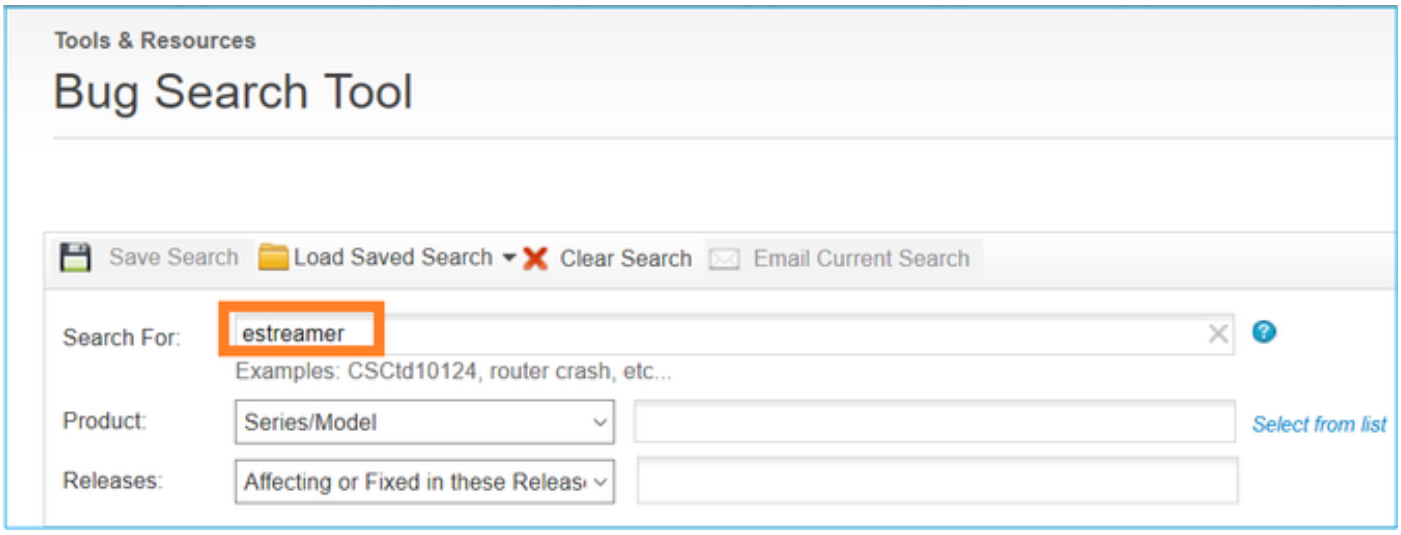
eStreamer統合ガイドで、さまざまなレコードタイプのヘッダ**セクションの[Record Type]**の横にあるNetmap ID番号を確認してください。Netmap ID番号は、**Netmap Domain Metadata**(Record Type 350)および**Managed Device Record Metadata**(Record Type 123)を使用して、それぞれドメインまたはデバイス名に変換できます。

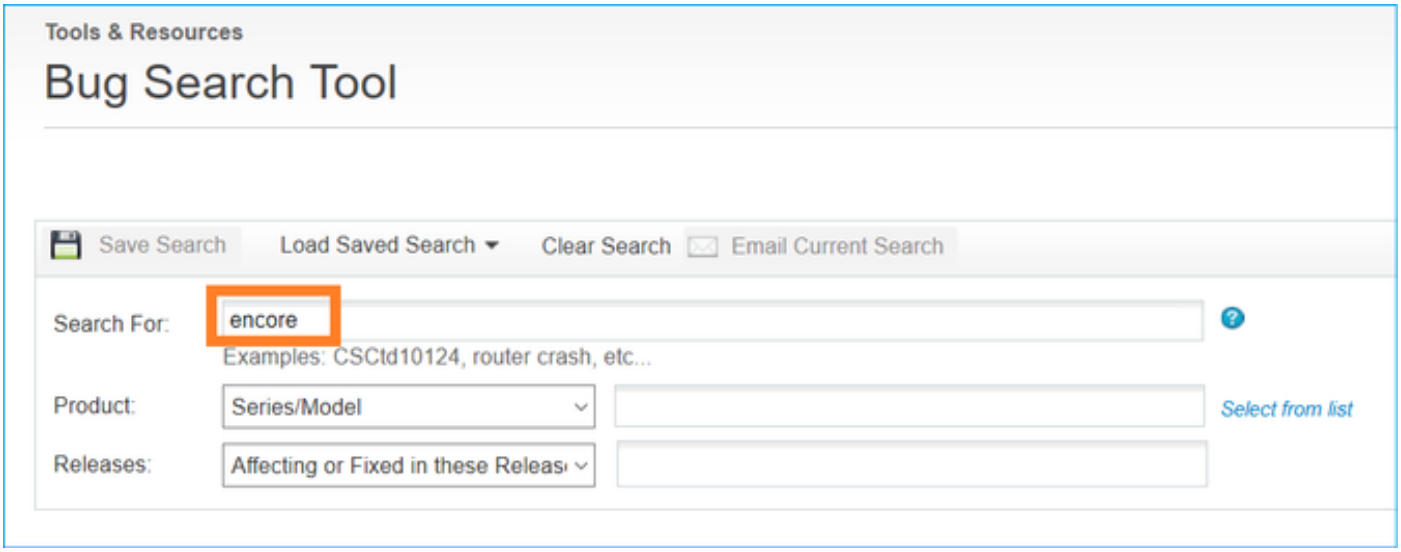
クライアントアプリケーションは、『eStreamer Integration Guide』に記載されている情報に従

って、バイナリデータとメタデータを解釈する必要があります。

既知の問題

バグ検索ツールを開き、ストリーマやencoreの問題を検索します。





関連情報

- eStreamerサーバストリーミング