Kenntnis der eStreamer- und Fehlerbehebung bei Integration der Netzwerkkerne

Inhalt

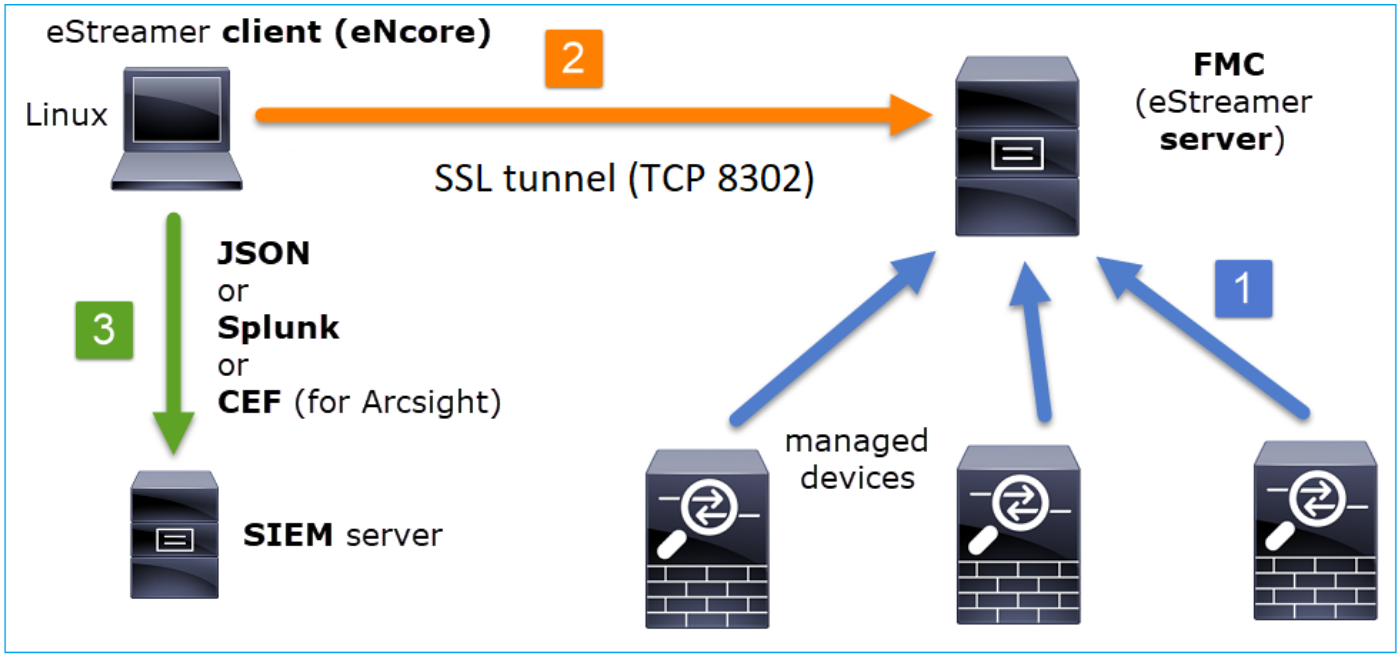
Einführung

Dieses Dokument beschreibt den Cisco Event Streamer (auch bekannt als eStreamer) Ncore CLI-Client. Insbesondere wird der Vorgang beschrieben, und es werden Informationen zur Fehlerbehebung bereitgestellt. Darüber hinaus werden häufig auftretende Probleme des Cisco Technical Assistance Center (TAC) sowie häufig gestellte Fragen (Frequently Asked Questions, FAQ) behandelt.

Mitarbeiter: David Torres Rivas, Mikis Zafeiroudis, Cisco TAC Engineers.

Übersicht

NetCore ist ein Allzweck-Client, der alle möglichen Ereignisse vom eStreamer-Server (FMC) anfordert, den binären Inhalt analysiert und Ereignisse in verschiedenen Formaten ausgibt, um andere Security Information and Event Management Tools (SIEMs) zu unterstützen.



eStreamer-Verbindungsaufbau

Der Client (Core) initiiert eine Verbindung zum FMC-TCP-Port 8302, wobei SSL-Handshake ausgeführt wird:

```
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>
```

Das FMC akzeptiert die Verbindung, führt SSL-Handshake am gleichen Port durch und verifiziert den gemeinsamen Client-Namen (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
```

Der eStreamer-Client überprüft dann die Konfiguration und die Lesezeichendatei, um zu

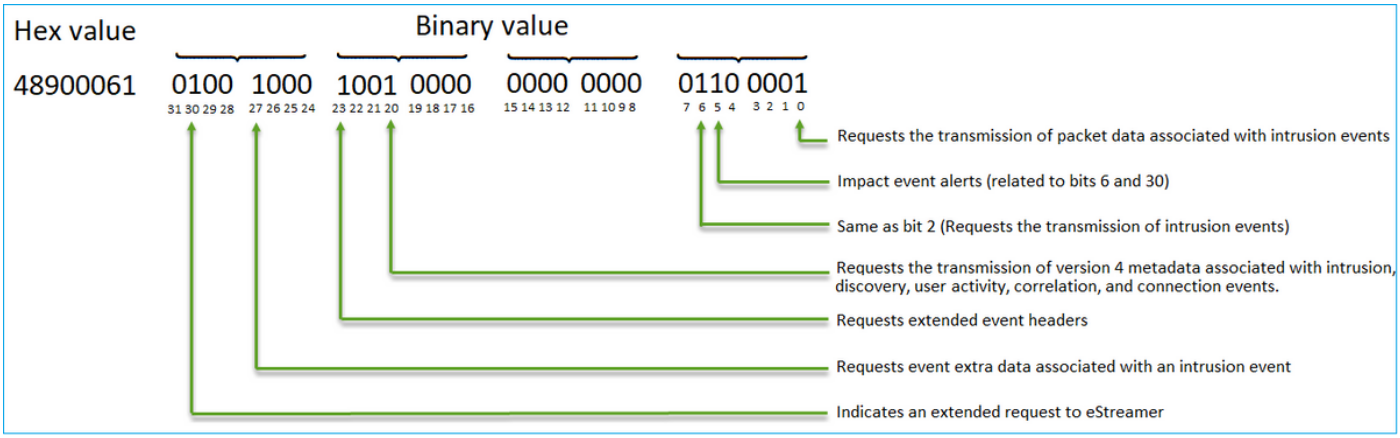
bestimmen, welche Ereignisse angefordert werden sollen und wie lange der Start dauert:

```
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:
0001080100000038000001a0b0000003848900061000000000009000c000400150009001f000b003d000e00470004005b
0007006500060060f0002008300000000
```

Die EventStreamRequest kann auf FMC korreliert werden:

```
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 ist die hexadezimale Darstellung der Anforderungsflags, die unter Request Flags beschrieben sind, und muss in binäre Dateien konvertiert werden, um zu ermitteln, ob der Client die erforderlichen Daten angefordert hat. Dies ist ein Beispiel:



> **Hinweis**: Einige Flag-Bits können die bereitgestellten Informationen ändern, wenn erweiterte Anforderungen initiiert werden.

Basierend auf den Request Bits leitet das FMC die Daten an den eStreamer-Client weiter.

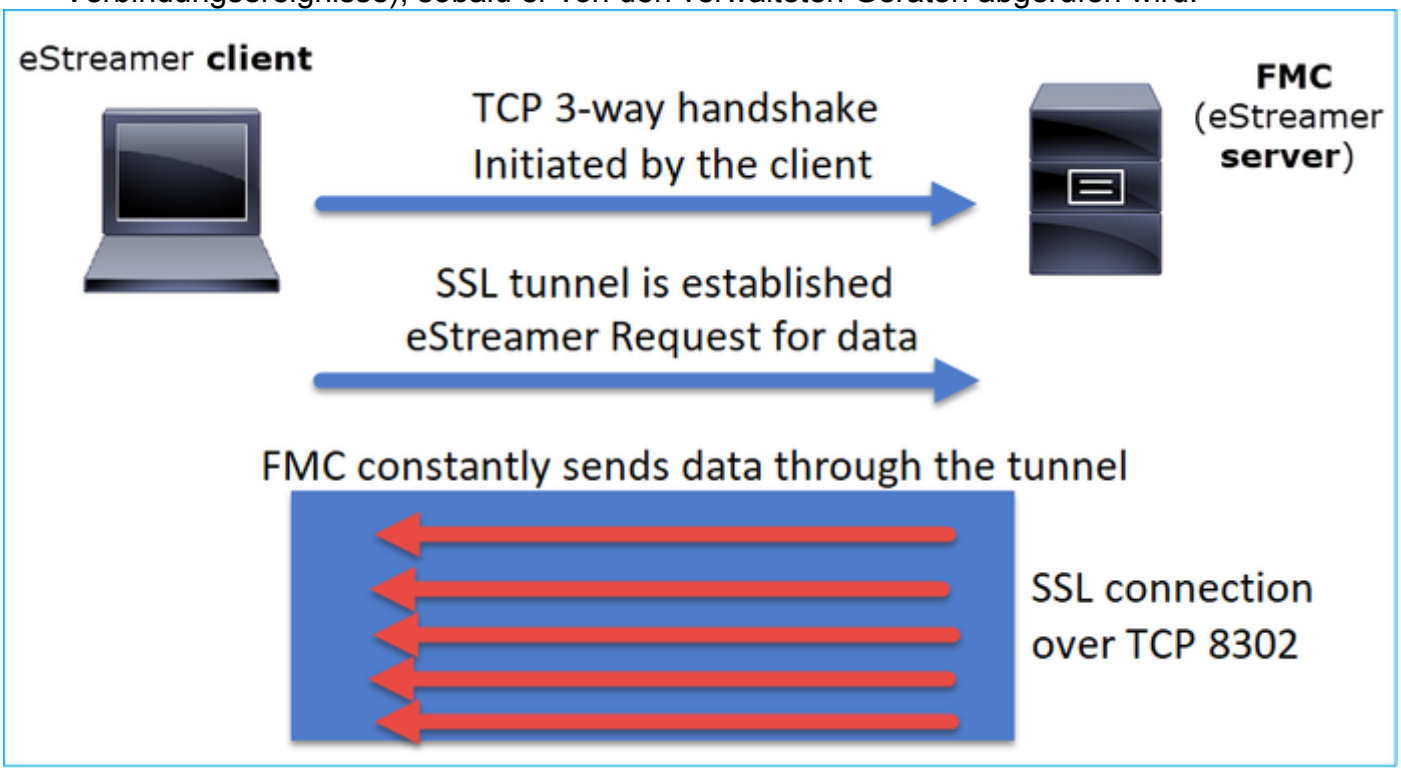
Wer initiiert die eStreamer-Verbindung und -Datenübertragung?

Der eStreamer-Client. Insbesondere stellt der Client eine TCP-Verbindung (3-Wege-Handshake) her, dann gibt es eine SSL-Verhandlung mit Client-Authentifizierung (wechselseitig). Schließlich sendet das FMC über den etablierten Tunnel die Daten, wenn Daten gesendet werden sollen:

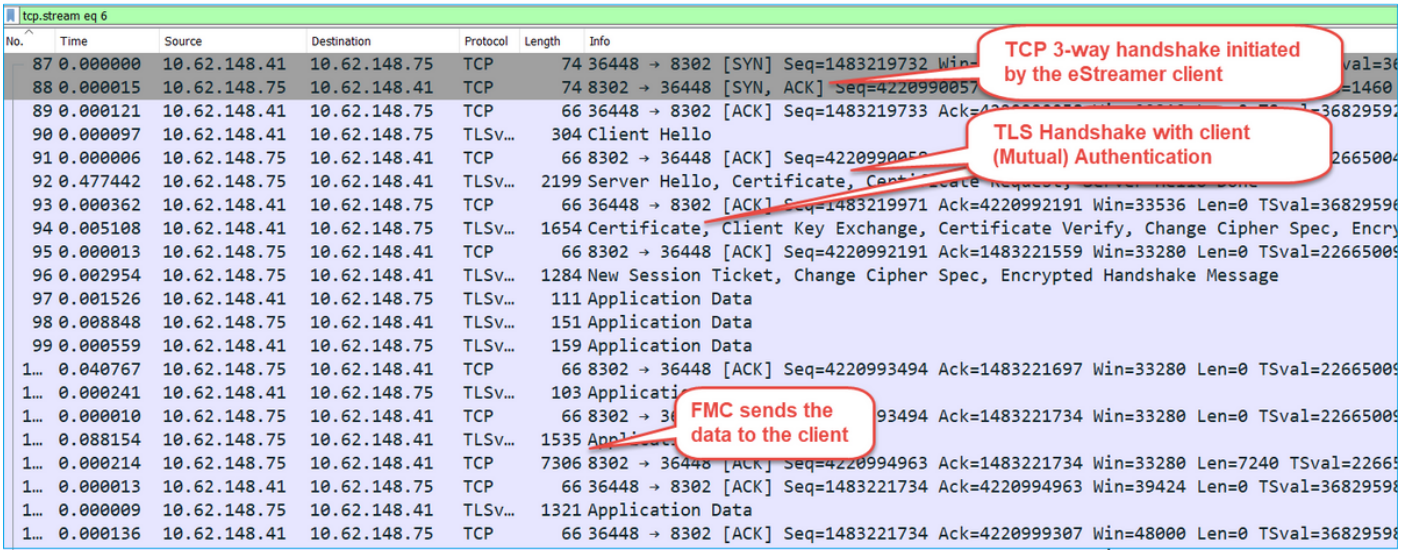
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100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

Zusammenfassung:

- Der Client initiiert den SSL-Tunnel, um Daten anzufordern (Pull).
- Sobald der Tunnel eingerichtet ist, bleibt der Tunnel aktiv und der FMC überträgt Daten (z. B. Verbindungsereignisse), sobald er von den verwalteten Geräten abgerufen wird.



In diesem Beispiel ist IP 10.62.148.41 der eStreamer-Client (Core), während IP 10.62.148.75 das FMC ist:



Konfigurieren

Weitere Informationen zum Core-CLI-Client finden Sie im eStreamer Core CLI Operations Guide

v3.5.

Einzelheiten zur eStreamer-Anwendung sowie zu den FMC-Konfigurationsschritten finden Sie im Event Streamer Integration Guide.

estreamer.conf-Dateioptimierung

Dieser Abschnitt beschreibt, was auf estreamer.conf geändert werden kann oder muss, damit die Lösung ordnungsgemäß funktioniert. Die Datei estreamer.conf befindet sich im *path*/eStreamer-Core-Verzeichnis. Hier ein Beispiel für den Dateiinhalt:

```
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
```

Der Bereich "Abonnement"

Um die Event Streamer Request zum Server (FMC) zu ändern, ändern Sie den Abschnitt eStreamer.conf Subscriptions. Wenn Sie beispielsweise erweiterte Anforderungen auf false festlegen, ändert dies die EventStream-Anforderung auf FMC:

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

Bei erweiterten Anforderungen = 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
```

Bei erweiterten Anforderungen = 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
```

Der Bereich Protokollierung

So aktivieren Sie das Debuggen auf der Core-CLI, bearbeiten Sie die Datei estreamer.conf, und ändern Sie die Protokollstufe:

```
 "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
    },
```

Der Bereich Monitor

Um die Anzahl der Ereignisse/Sekunde, die verarbeitet werden, und das aktuelle Lesezeichen anzuzeigen, bearbeiten Sie den Abschnitt für den Monitor auf estreamer.conf:

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

Weitere wichtige Tasten der obersten Ebene:

```
"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.
```

Dieser Wert kann zwischen 2 und 12 festgelegt werden. Die Leistung soll durch mehr Prozesse verbessert werden, es entstehen jedoch für jeden Prozess Gemeinkosten. Das Ergebnis ist, dass optimale Leistung mit der richtigen Kombination aus "Anzahl der Prozesse" und der Verarbeitungsfähigkeit des Host-Rechners erreicht wird. Die besten verfügbaren Richtlinien sind:

- Für 2 Kerne: "Workerprozesse": 4
- Für 4 oder mehr Kerne: "Workerprozesse": 12

Fehlerbehebung

Allgemeine eStreamer-Fehlerbehebungsverfahren finden Sie in diesem Dokument [Problembehebung zwischen FireSIGHT System und eStreamer Client (SIEM).]

Zu Testzwecken können Sie die Funktion "Core as a Vorderround" (Core als Vordergrundprozess) aktivieren und die Kommunikation mit FMC überprüfen.

```
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
0007006500060006f0002008300000000
2020-06-04 11:48:00,653 Monitor      INFO     Running. 0 handled; average rate 1.2 ev/sec;
```

Gleichzeitig können Sie auf dem FMC Protokolle wie diese sehen, wenn der Ncore-Streamer-Client die Verbindung herstellt. Beachten Sie, dass die FMC-Backend-Zeitzone immer UTC ist:

```
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
```

Zu sammelnde Artikel, bevor Sie das Cisco Technical Assistance Center (TAC) kontaktieren

Es wird dringend empfohlen, diese Punkte zu sammeln, bevor Sie sich an das Cisco TAC wenden:

- Die Version von eStreamer Core
- Die Version von Python
- Die Version des Host-Betriebssystems
- Werden Ereignisse auf dem FMC angezeigt? Screenshot von Ereignissen + FMC eStreamer-Konfiguration teilen
- Aktivieren Sie Debug auf der Core-CLI (wie im "logging section" beschrieben).
- Erstellen einer Fehlerbehebungsdatei vom FMC
- Stellen Sie diese Dateien von Netcore bereit:
  estreamer.conf
  estreamer.log

Häufige Probleme

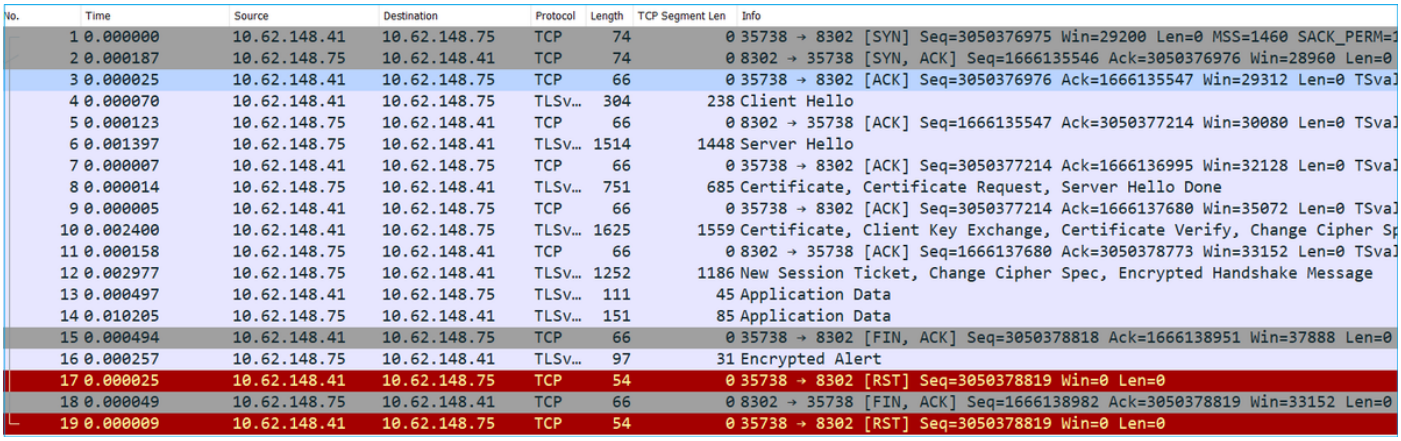
Keine Verbindung am TCP-Port 8302

Telnet vom eStreamer-Client zum FMC-Port 8302 und Überprüfen der Verbindungsherstellung

Darüber hinaus können Sie mit der Kerntestoption die Verbindung testen:

```
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
```

Dies ist ein erfolgreicher Verbindungsversuch, wie in Wireshark (10.62.148.41 ist die Core-IP, während 10.62.148.75 das FMC ist):



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

ZertifikatsCN stimmt nicht mit dem Remote-Host überein

Befindet sich der eStreamer-Client hinter NAT, muss das Zertifikat mit der Upstream-IP-Adresse generiert werden. Andernfalls treten Fehler wie diese auf:

```
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
```

Die FMC-DNS-Auflösung für den eStreamer-Client ist falsch.

Falls FMC falsche DNS-Einträge für den eStreamer-Client hat, erreichen die Ereignisse den Client nicht. Um festzustellen, ob es sich um ein Problem handelt, nehmen Sie eine Erfassung auf dem FMC vor. In diesem Beispiel empfängt das FMC ein TCP-SYN-Paket vom Streamer-Client-Host ksec-sfvm-win7-3.cisco.com:

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

Sie können das **-n**-Flag verwenden, um die aufgelöste IP anzuzeigen:

```
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
```

Alternativ können Sie das Befehlswerkzeug **nslookup** über die FMC-CLI verwenden:

```
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
```

eStreamer-Kommunikationsproblem aufgrund eines SSL-Zertifikatsfehlers

Stellen Sie sicher, dass der eStreamer-Client das richtige FMC SSL-Zertifikat verwendet. Wenn das Zertifikat in den Dateien FMC /var/log/message nicht korrekt ist, werden folgende Ereignisse angezeigt:

```
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
```

Sie können den eStreamer-Client auf dem FMC löschen und neu konfigurieren. Dadurch wird das SSL-Zertifikat neu generiert. Importieren Sie das neue Zertifikat in den eStreamer-Client.

Falsche auf eStreamer konfigurierte IP-Adresse für ASA SFR-Modulintegration

Auf dem eStreamer-Client müssen Sie die IP-Adresse des SFR-Moduls verwenden. Auf der ASA-Ausführung den Befehl **show sfr module details**, um die Modul-IP anzuzeigen.

ArcSight Common Event Format (CEF)

Der Arcsight Common Event Format Standard definiert die Schlüsselwert-Paare, die von der Core CLI gesendet werden müssen. Wenn Unstimmigkeiten bei den Daten von Arcisght vorliegen, d. h.: fehlende Felder, ungeordnet oder einige Daten auf dem Arcsight-Client nicht korrekt analysiert werden, ist es hilfreich, die Konfiguration so zu ändern, dass sie in eine Protokolldatei geschrieben wird. So können Sie feststellen, wo das Problem liegt.

```
    "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-Ereignisse werden in einer Zeile geschrieben, in der jedes Feld durch das Rohr "|" getrennt ist:

```
<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-Client zeigt nicht alle Protokolle an

Dies ist häufig auf eine Überbelegung des eStreamer-Clients zurückzuführen (zu viele Ereignisse wurden vom FMC gesendet). Führen Sie diesen Befehl auf der Client-Seite von eStreamer aus, und überprüfen Sie, ob der Zähler Recv-Q hoch ist. Dies ist die Anzahl der Bytes, die nicht vom Benutzerprogramm kopiert wurden, das mit diesem Socket verbunden ist. In diesem Beispiel sind auf der Clientseite 143143 Byte ausstehend:

```
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
```

Überprüfen Sie die Ereignisse pro Sekunde, die der eStreamer-Client empfangen hat. Hier erhalten Sie einen Hinweis auf die Ereignisrate pro Sekunde:

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

Versuchen Sie, die vom eStreamer-Client angeforderte Datenmenge oder die vom FMC gesendeten Ereignistypen zu reduzieren. Alternativ können Sie versuchen, die Anzahl der Ressourcen zu erhöhen, die auf der eStreamer-Clientseite zugewiesen sind.

Häufig gestellte Fragen (FAQ)

Wo erhalte ich das Ncore-CLI-Paket?

- Besuchen Sie die Seite zum Herunterladen der FMC-Software, **Firepower System Tools and APIs - Ncore for CEF.**
- Alternativ können Sie die neueste Core-Datei unter https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets herunterladen.

Wenn eine vollständige FMC-Sicherung ausgeführt wird, generiert der eStreamer keine

Ereignisse. Ist das normal?

Ja, es ist erwartetes Verhalten. Im FMC-Konfigurationsleitfaden Wann sollten Sie eine Sicherung durchführen?

Während das System Sicherungsdaten sammelt, kann es zu einer vorübergehenden Pause bei der Datenkorrelation (nur FMC) kommen, und Sie können möglicherweise daran gehindert werden, Konfigurationen für die Sicherung zu ändern.

Sind spezielle Lizenzen für die FMC-Integration mit dem eStreamer-Client (z. B. Qradar) erforderlich?

Nein

Woher stammen die eStreamer-Veranstaltungen?

Das FMC Der FMC empfängt die Ereignisse von den verwalteten Geräten (FTD) und leitet sie an die eStreamer-Clients wie Ncore, ArcSight, Splunk, QRadar, LogRhythm usw. weiter.

Gibt es eine Kompatibilitätsmatrix zwischen Splunk und Ncore?

Kompatibilitätsinformationen finden Sie in den Splunk-Dokumenten. Um z. B. herauszufinden, welche Splunk-Versionen mit der Core Version 3.6.8 kompatibel sind, lesen Sie https://splunkbase.splunk.com/app/3662/

Kann eStreamer Core Daten von mehreren FMCs verbrauchen?

Zum Zeitpunkt dieser Veröffentlichung No. Check Enhancement Request CSCvq14351

Welche Optionen werden für die Konfiguration von eStreamer für die Einrichtung von FMC High Availability (HA) empfohlen?

Es wird empfohlen, nur die aktive FMC-Einheit für eStreamer zu konfigurieren. Wenn Sie beide FMC-Einheiten für eStreamer konfigurieren, empfängt das SIEM doppelte Ereignisse, da das Standby-FMC auf eStreamer-Anfragen reagiert. Verwandte Verbesserungsanfrage: CSCvi95944

Ist bei einem FMC-Upgrade die manuelle Generierung neuer eStreamer-Zertifikate erforderlich?

Nein

Werden Security Intelligence-Ereignisse an den eStreamer-Client gesendet? Ist es möglich, Security Intelligence-Ereignisse als separate Kategorie auszuwählen und an einen eStreamer-Client zu senden?

Die Security Intelligence (SI)-Ereignisse sind in der Kategorie von Connection-Ereignissen enthalten und nicht als separate Kategorie. Aus diesem Grund gibt es kein separates SI-Ereignis, das an den Streamer gesendet wird. Verwandte Verbesserungsanfrage: CSCva39052

Ist es möglich, auf dem FMC die Sensoren/verwalteten Geräte anzugeben, deren eStreamer-Ereignisse an den eStreamer-Client gesendet werden?

Da derzeit nur eine FMC-Domäne vorhanden ist, ist dies nicht möglich. Zugehörige Verbesserungsanfrage CSCvt31270. Alternativ können Sie auf FMC zwei verschiedene Domänen konfigurieren. In der ersten Domäne fügen Sie alle verwalteten Geräte hinzu, die Sie eStreamer für den eStreamer-Client aktivieren und konfigurieren möchten. Für die zweite Domäne fügen Sie die restlichen Geräte hinzu und konfigurieren eStreamer nicht.

Wie lautet die Version von eStreamer auf der FirePOWER? Ich benötige diese Informationen für die SIEM-Konfiguration (z. B. LogRhythm).

Um die FirePOWER (FMC)-Version von der FMC-Benutzeroberfläche aus zu überprüfen, navigieren Sie zu **Hilfe** (oben rechts) **> Info > Software version.**

Wie werden die Domäneninformationen in den FMC eStreamer-Daten angezeigt, wenn FMC mit Domänen konfiguriert ist?

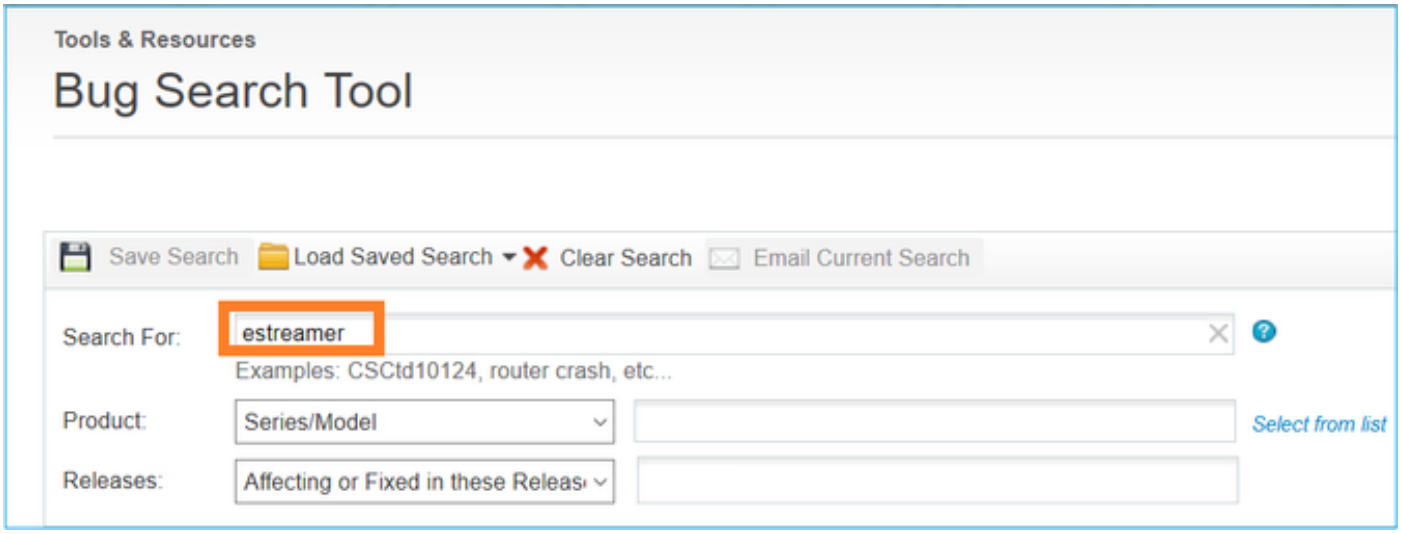
Im eStreamer Integration Guide überprüfen Sie die **Netmap ID**-Nummer neben dem Record Type

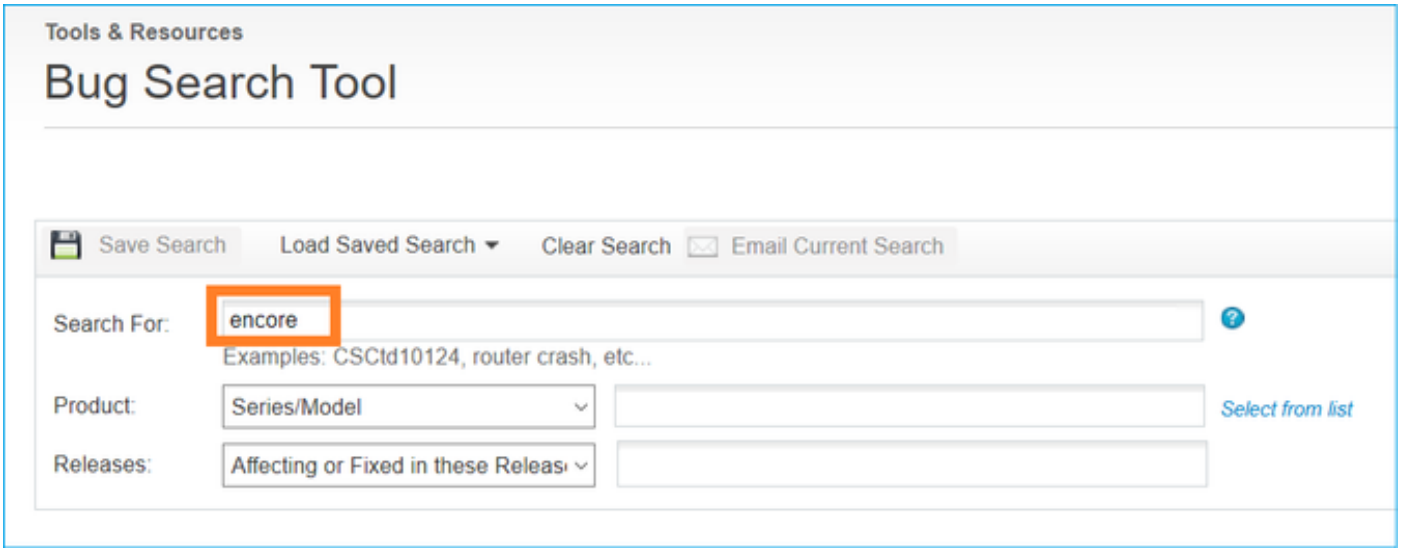
im Header-Abschnitt vieler verschiedener Datensatztypen. Die Netmap-ID-Nummer kann mithilfe von **Netmap Domain Metadata** (Record Type 350) und **Managed Device Record Metadata** (Record Type 123) in Domänen- oder Gerätenamen konvertiert werden.

Die Clientanwendung muss die binären Daten und Metadaten entsprechend den Informationen im eStreamer Integration Guide interpretieren.

Bekannte Probleme

Öffnen Sie das Bug Search Tool und suchen Sie nach Streamer- und Encore-Problemen, z.B.





Zugehörige Informationen

- eStreamer-Server-Streaming