Integratie met core van eStreamer en probleemoplossing

Inhoud

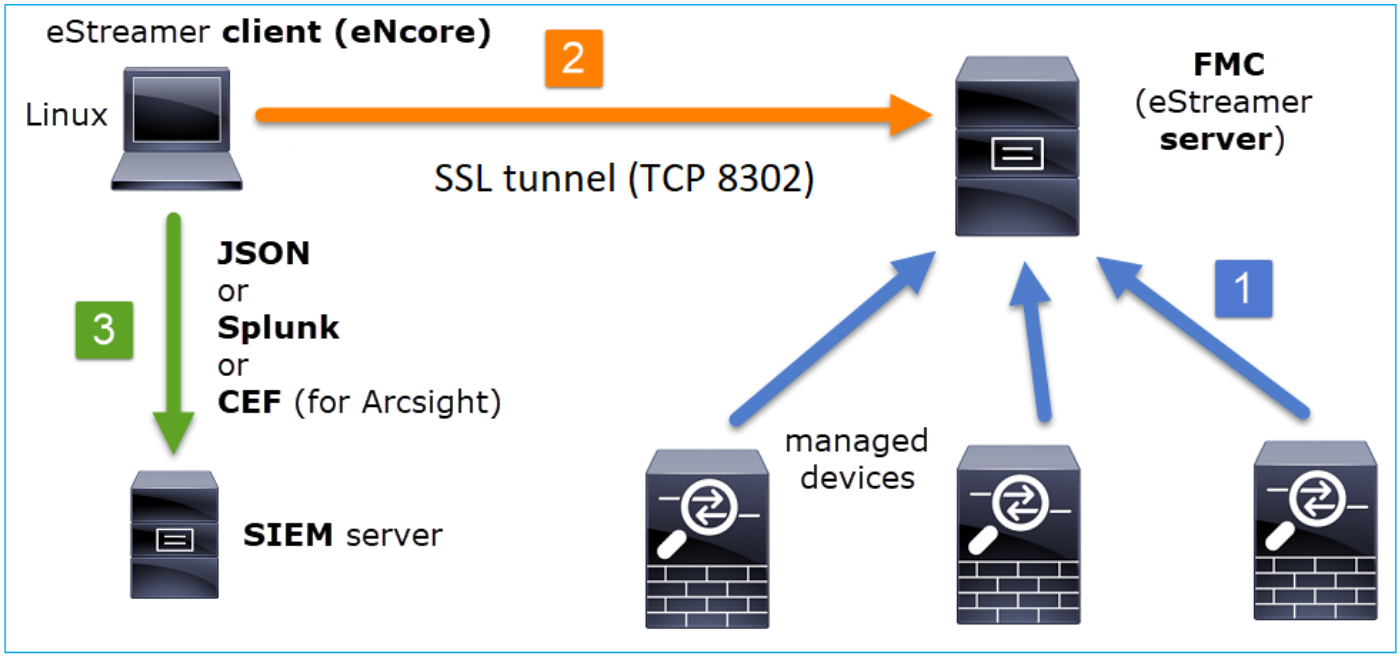
Inleiding

Dit document beschrijft de Cisco Event Streamer (ook bekend als eStreamer) Ncore CLI-client. In het bijzonder beschrijft het de bewerking en geeft het informatie over het oplossen van problemen. Daarnaast behandelt het voorkomende problemen die worden gezien door het Cisco Technical Assistance Center (TAC), en vaak gestelde vragen (FAQ).

Bijgedragen door David Torres Rivas, Mikis Zafeiroudis, Cisco TAC-engineers.

Overzicht

Necore is een all-purpose client, die alle mogelijke gebeurtenissen van de eStreamer server (FMC) vraagt, ontleedt de binaire inhoud en outputs in verschillende indelingen ter ondersteuning van andere Security Information en Event Management-tools (SIEM's).



Streamer-verbindingsinrichting

De client (Ncore) initieert een verbinding met FMC TCP poort 8302 waar SSL-handdruk wordt uitgevoerd:

```
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>
```

Het FMC accepteert de verbinding, voert SSL-handdruk uit op dezelfde poort en verifieert de client Common Name (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
```

De eStreamer-client controleert vervolgens de configuratie en het boekenbestand van de client om

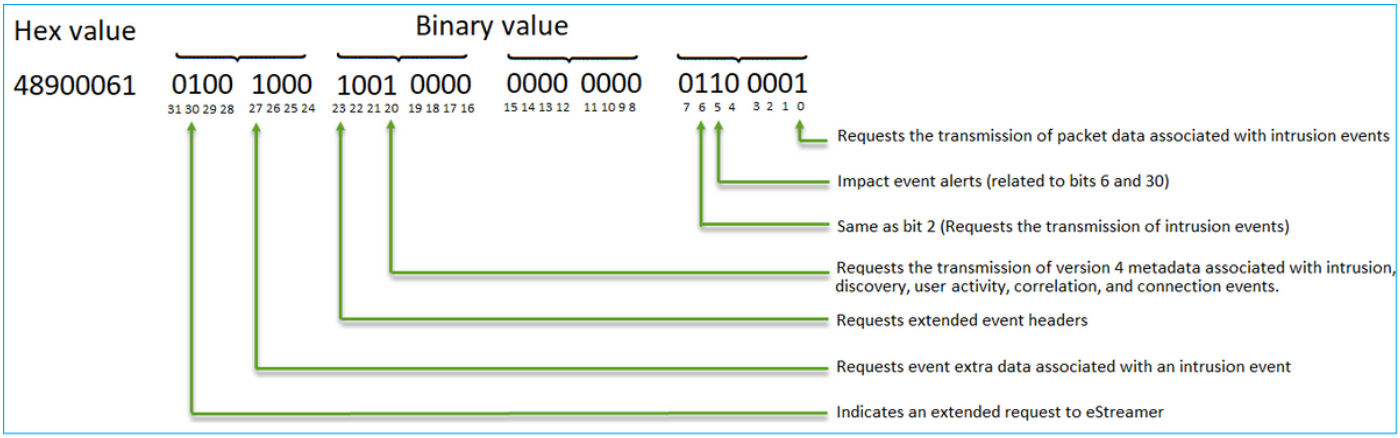
te bepalen welke gebeurtenissen u wilt aanvragen en op welk tijdstip u start:

```
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
```

EventStreamApplication kan worden gecorreleerd op FMC:

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

EventStreamApplication is de hexadecimale weergave van de verzoekvlaggen die op de Vlaggen van het verzoek worden beschreven en moet in binair getal worden geconverteerd om te begrijpen of de client de vereiste gegevens heeft opgevraagd. Dit is een voorbeeld:



> Opmerking: Sommige vlaggenbits zouden de verstrekte informatie kunnen wijzigen indien uitgebreide aanvragen worden ingediend.

Op basis van de informatie-informatie die wordt gevraagd, drukt het FMC de gegevens op de eStreamer-client.

Wie initieert de eStreamer-verbinding en gegevensoverdracht?

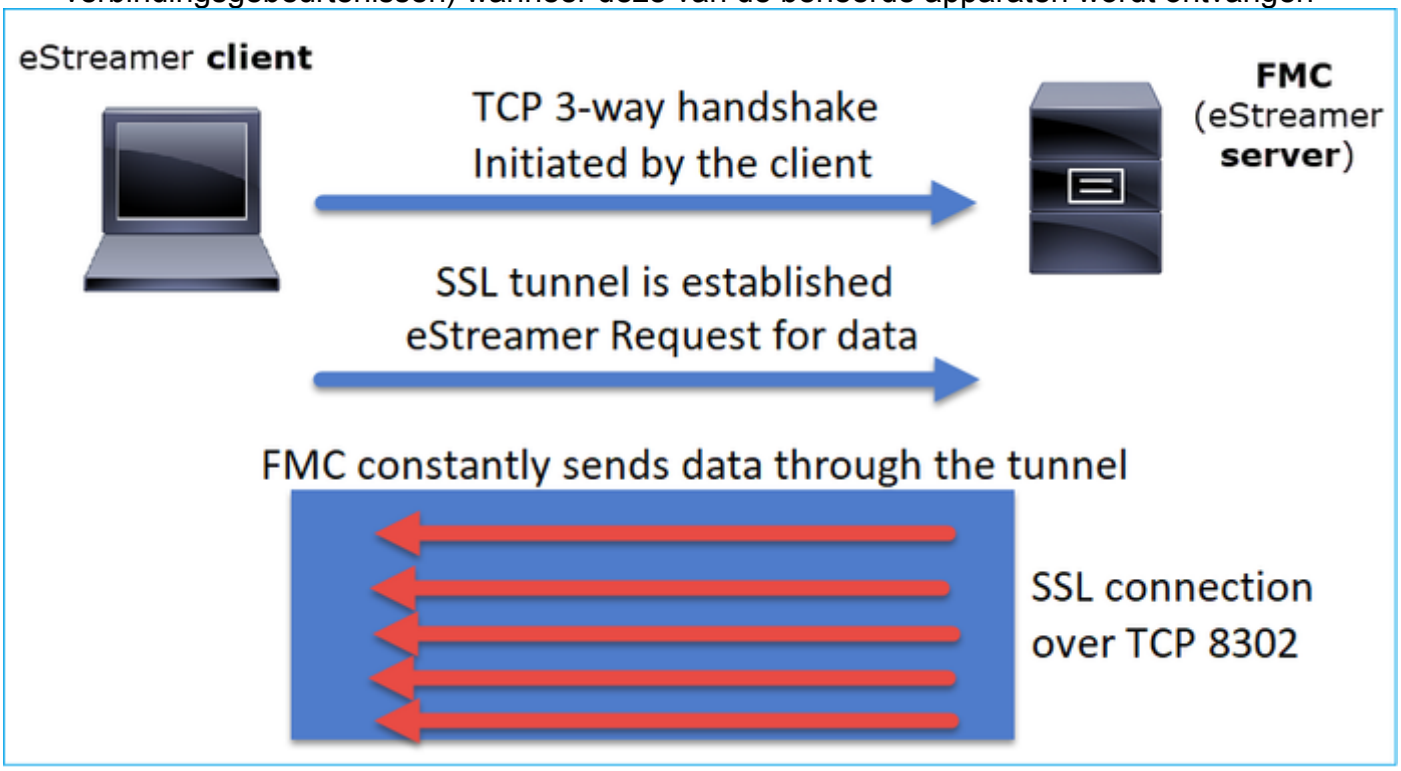
De eStreamer client. In het bijzonder, vestigt de client een TCP verbinding (3-way handshake), dan is er een SSL onderhandeling met Client (mutual) authenticatie. Ten slotte stuurt het FMC via

de gevestigde tunnel de gegevens door wanneer er gegevens worden verzonden:

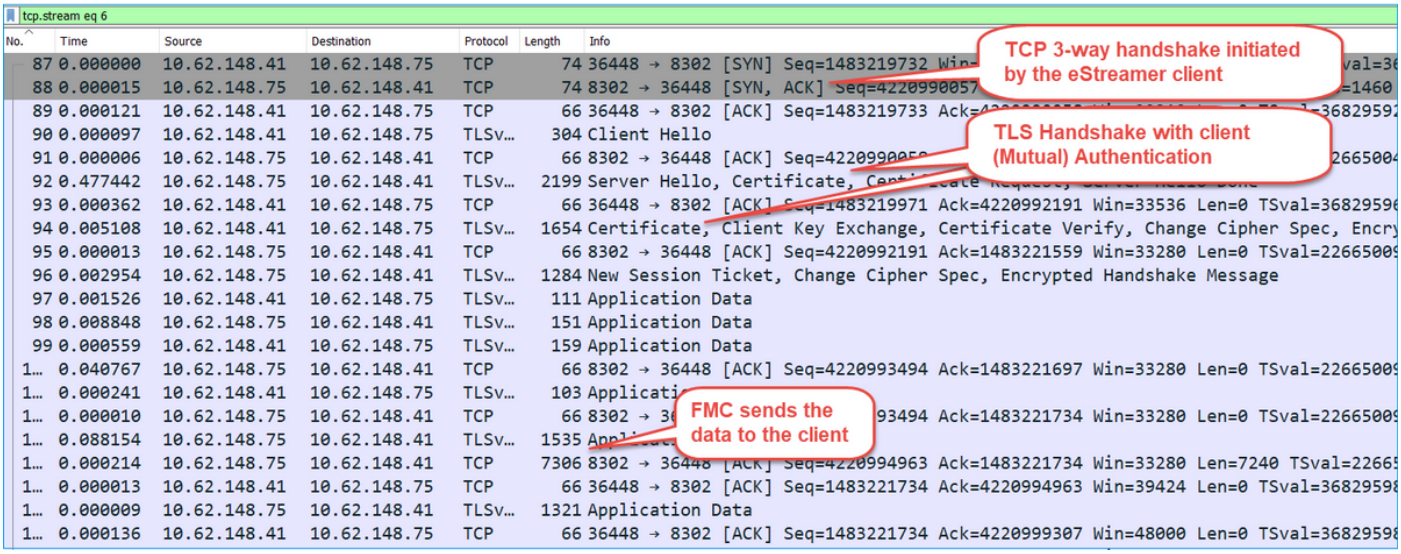
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100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

Samengevat:

- De client stelt de SSL-tunnel in om gegevens te vragen (trek)
- Zodra de tunnel tot stand is gebracht blijft de tunnel omhoog en drukt het FMC gegevens (bv. verbindingsgebeurtenissen) wanneer deze van de beheerde apparaten wordt ontvangen



In dit voorbeeld is IP 10.62.148.41 de eStreamer-client (Ncore) en IP 10.62.148.75 het FMC:



No.	Time	Source	Destination	Protocol	Length	Info
87	0.000000	10.62.148.41	10.62.148.75	TCP	74	36448 → 8302 [SYN] Seq=1483219732 Win=
88	0.000015	10.62.148.75	10.62.148.41	TCP	74	8302 → 36448 [SYN, ACK] Seq=4220990057
89	0.000121	10.62.148.41	10.62.148.75	TCP	66	36448 → 8302 [ACK] Seq=1483219733 Ack=
90	0.000097	10.62.148.41	10.62.148.75	TLSv…	304	Client Hello
91	0.000006	10.62.148.75	10.62.148.41	TCP	66	8302 → 36448 [ACK] Seq=4220990
92	0.477442	10.62.148.75	10.62.148.41	TLSv…	2199	Server Hello, Certificate,
93	0.000362	10.62.148.41	10.62.148.75	TCP	66	36448 → 8302 [ACK] Seq=1483219971 Ack=4220992191 Win=33536 Len=0 TSval=3682959
94	0.005108	10.62.148.41	10.62.148.75	TLSv…	1654	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encry
95	0.000013	10.62.148.75	10.62.148.41	TCP	66	8302 → 36448 [ACK] Seq=4220992191 Ack=1483221559 Win=33280 Len=0 TSval=2266500
96	0.002954	10.62.148.75	10.62.148.41	TLSv…	1284	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
97	0.001526	10.62.148.41	10.62.148.75	TLSv…	111	Application Data
98	0.008848	10.62.148.75	10.62.148.41	TLSv…	151	Application Data
99	0.000559	10.62.148.41	10.62.148.75	TLSv…	159	Application Data
1…	0.040767	10.62.148.75	10.62.148.41	TCP	66	8302 → 36448 [ACK] Seq=4220993494 Ack=1483221697 Win=33280 Len=0 TSval=2266500
1…	0.000241	10.62.148.41	10.62.148.75	TLSv…	103	Applicati
1…	0.000010	10.62.148.75	10.62.148.41	TCP	66	8302 → 3 93494 Ack=1483221734 Win=33280 Len=0 TSval=2266500
1…	0.088154	10.62.148.75	10.62.148.41	TLSv…	1535	Appli
1…	0.000214	10.62.148.75	10.62.148.41	TCP	7306	8302 → 36448 [ACK] Seq=4220994963 Ack=1483221734 Win=33280 Len=7240 TSval=2266
1…	0.000013	10.62.148.41	10.62.148.75	TCP	66	36448 → 8302 [ACK] Seq=1483221734 Ack=4220994963 Win=39424 Len=0 TSval=3682959
1…	0.000009	10.62.148.75	10.62.148.41	TLSv…	1321	Application Data
1…	0.000136	10.62.148.41	10.62.148.75	TCP	66	36448 → 8302 [ACK] Seq=1483221734 Ack=4220999307 Win=48000 Len=0 TSval=3682959

Configureren

Raadpleeg voor meer informatie over de Ncore CLI client eStreamer Ncore CLI Operations Guide v3.5.

De details van de eStreamer-toepassing en de configuratiesstappen van het FMC worden besproken in de Event Streamer Integration Guide.

estreamer.conf bestandsindelingen

In dit deel wordt beschreven wat er op estreamer.conf kan of moet worden aangepast om de oplossing goed te laten werken. Het bestand estreamer.conf bevindt zich in de path/eStreamer-Ncore folder. Hier volgt een voorbeeld van de inhoud van het bestand:

```
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
```

De abonnementssectie

Als u het verzoek om Event Streamer naar de server (FMC) wilt wijzigen, wijzigt u het gedeelte eStreamer.conf-abonnementen. Bijvoorbeeld wanneer u uitgebreide verzoeken om vals in te stellen verandert het EventStream verzoek op 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
        },
```

Met uitgebreide verzoeken = vals:

```
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
```

Met verlengde verzoeken = waar:

```
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
```

Het loggedeelte

U kunt debugs op Ncore CLI als volgt het bestand estreamer.conf bewerken en het logniveau wijzigen:

```
 "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
    },
```

Het gedeelte van de monitor

Om het aantal gebeurtenissen/tweede verwerkte en huidige favoriet te zien, bewerk het monitor gedeelte op 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)
  },
```

Andere relevante toetsen van het hoogste niveau:

```
"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.
```

Deze waarde kan worden ingesteld van 2 tot 12. Meer processen zijn bedoeld om de prestaties te verbeteren, maar bij elk proces zijn er overheadkosten. Het resultaat is dat optimale prestaties worden bereikt met de juiste combinatie van "aantal processen" met de verwerkingscapaciteit van de host machine. De beste beschikbare richtsnoeren zijn:

- Voor twee kernen: "Werknemersprocessen": 4
- Voor 4 of meer kernen: "Werknemersprocessen": 12

Problemen oplossen

Voor generieke procedures voor probleemoplossing in eStreamer kunt u naar dit document [problemen bij probleemoplossing tussen FireSIGHT System en eStreamer Client (SIEM) verwijzen]

Voor testdoeleinden kunt u Ncore als voorgrondproces inschakelen en de communicatie met FMC controleren

```
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;
```

Tegelijkertijd kun je op FMC logbestanden zoals deze zien wanneer de Ncore rationer client de verbinding maakt. Merk op dat de FMC backend-tijdzone altijd UTC is:

```
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
```

Te verzamelen items voordat u contact opneemt met Cisco Technical Assistance Center (TAC)

Het is sterk aanbevolen om deze items te verzamelen voordat u contact opneemt met Cisco TAC:

- De versie van eStreamer Ncore
- De versie van Python
- De versie van host OS
- Zie je de gebeurtenissen op de FMC? Deel een screenshot van de gebeurtenissen + FMC eStreamer-configuratie
- Schakel debug in op core CLI (zoals beschreven in het bloggedeelte)
- Een bestand voor probleemoplossing vanuit FMC genereren
- Geef deze bestanden op:
  estreamer.conf
  estreamer.log

Gemeenschappelijke kwesties

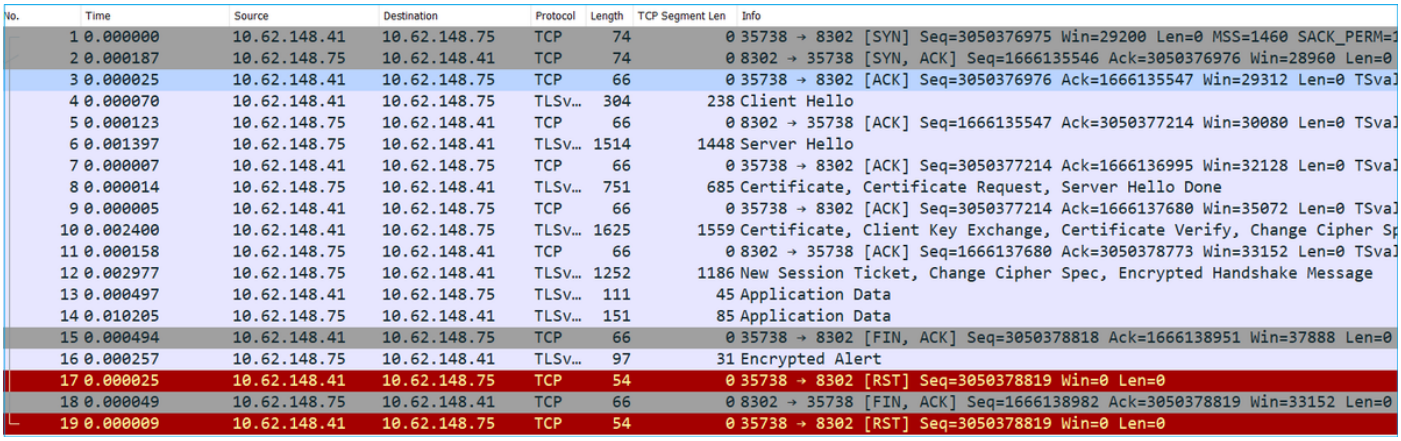
Geen connectiviteit op TCP-poort 8302

Telnet van de eStreamer-client naar FMC-poort 8302 en verifieert de connectiviteit.

Daarnaast kunt u de Ncore test optie gebruiken om de connectiviteit te 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
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
```

Dit is een succesvolle poging om verbinding te maken, zoals te zien is in Wireshark (10.62.148.41 is het core IP en 10.62.148.75 is het 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

Certificaat CON komt niet overeen met de afstandsbediening

Als de eStreamer-client achter NAT ligt, moet het certificaat met het upstream IP-adres gegenereerd worden of worden er fouten zoals deze gezien:

```
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
```

FMC DNS-resolutie voor eStreamer-client is niet correct

Indien FMC onjuiste DNS-items voor de eStreamer-client hebben, bereiken de gebeurtenissen niet de client. Om te identificeren of dit het probleem is, neem dan een opname op het FMC. In dit voorbeeld ontvangt het FMC een TCP SYN-pakket van de gestroomlijnde 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
```

U kunt de **-n** vlag gebruiken om de opgeloste IP te zien:

```
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
```

U kunt ook het commando gereedschap van de FMC CLI gebruiken:

```
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
```

Probleem bij e-streamer-communicatie door SSL-certificaatfout

Zorg ervoor dat de eStreamer-client het juiste FMC SSL-certificaat gebruikt. Als het certificaat niet correct is op FMC/var/log/bericht bestanden ziet u deze gebeurtenissen:

```
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
```

U kunt de eStreamer-client op FMC verwijderen en opnieuw configureren. Hierdoor wordt het SSL-certificaat opnieuw gegenereerd. Importeer het nieuwe certificaat in de eStreamer-client.

Onjuist IP-adres ingesteld op eStreamer voor ASA SFR-module - integratie

Op eStreamer client moet u de SFR module IP gebruiken. Op ASA run de opdracht **toont** de **sfr module details** om de module IP te zien.

ArcSight Common Event Format (CEF)

De Arcsight Common Event Format-standaard definieert de belangrijke waardepparen die van Ncore CLI moeten worden verstuurd. Als er inconsistentie is in de gegevens over Arcisght, dat wil zeggen: ontbrekende velden, buiten orde, of sommige gegevens worden niet correct geparseerd op Arcsight client, het is handig om de configuratie aan te passen om naar een logbestand te schrijven door in te stellen. Dit helpt te bepalen waar het probleem ligt.

```
    "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-gebeurtenissen worden geschreven in een regel met elk veld gescheiden door leiding "|":

```
<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
```

Streamer-client geeft niet alle kaarten weer

Dit is vaak het gevolg van overabonnement op eStreamer-klanten (te veel gebeurtenissen die door het FMC worden verstuurd). Start deze opdracht op de client-kant eStreamer en controleer of de teller Recv-Q hoog is. Dit is de telling van bytes die niet zijn gekopieerd door het gebruikersprogramma dat op deze socket is aangesloten. In dit voorbeeld zijn er 143143 Bytes in behandeling aan de kant van de cliënt:

```
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
```

Controleer de gebeurtenissen per seconde die door de eStreamer-client zijn ontvangen. Dit geeft een indicatie van de gebeurtenissen per seconde:

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

Probeer de hoeveelheid gegevens die door de eStreamer-client is gevraagd of de door het FMC verzonden gebeurtenissen te verminderen. U kunt ook proberen de hoeveelheid middelen die aan de kant van de eStreamer-client is toegewezen, te verhogen.

Vaak gestelde vragen (FAQ)

Waar kan het pakket Ncore-cli vandaan komen?

- Controleer de downloaden-pagina van de FMC-software, **Firepower System Tools en API's - Core voor CEF**
- U kunt ook het laatste kernbestand kopen op https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets

Wanneer er een volledige back-up van de FMC wordt uitgevoerd, genereert eStreamer geen gebeurtenissen. Is dit normaal?

Ja, het wordt verwacht. Van de FMC Config Guide bij back-up:

Tijdens het verzamelen van back-upgegevens is er mogelijk een tijdelijke pauze in gegevenscorrelatie (alleen FMC) en het is mogelijk dat u geen configuraties met betrekking tot de back-up kunt wijzigen.

Zijn er speciale licenties vereist voor FMC-integratie met eStreamer-client (bijvoorbeeld Qradar)?

Nee

Waar komen eStreamer-evenementen vandaan?

Het VCC. Met name krijgt het FMC de gebeurtenissen van de beheerde apparaten (FTD) en stuurt deze naar de eStreamer-client(s) zoals Ncore, ArcSight, Splunk, QRadar, LogRhythm, enz.

Is er een compatibiliteitsmatrix tussen Splunk en Ncore?

Controleer de Splunk-documenten op informatie over de compatibiliteit. Bijvoorbeeld, om te zien welke versies van het Splunk compatibel zijn met Audio versie 3.6.8 controle https://splunkbase.splunk.com/app/3662/

Kan eStreamer Ncore gegevens van meerdere VCC's consumeren?

Op het moment van schrijven, nee. Controleer verbeteringsverzoek CSCvq14351

Wat zijn de aanbevolen opties om eStreamer te configureren voor installatie van FMC High Availability (HA)?

Aanbevolen wordt alleen de actieve FMC-eenheid voor eStreamer te configureren. Als u beide FMC-eenheden voor eStreamer instelt, ontvangt SIEM dubbele gebeurtenissen omdat de standby-FMC op eStreamer-verzoek reageert. Verwante aanvraag voor versterking: CSCvi95944

Is het voor een FMC-upgrade nodig om handmatig nieuwe eStreamer-certificaten te genereren?

Nee

Worden de Security Intelligence-gebeurtenissen naar eStreamer-client verstuurd? Is het mogelijk om Security Intelligence-gebeurtenissen als een aparte categorie te selecteren en ze naar een eStreamer-client te sturen?

De gebeurtenissen van de veiligheidsinlichtingendienst (SI) zijn opgenomen in de categorie verbindingsgebeurtenissen en niet in een afzonderlijke categorie. Daarom is er geen afzonderlijke SI-gebeurtenis die naar de stroomverdeler wordt gestuurd. Verwante aanvraag voor versterking: CSCva39052

Is het mogelijk om op FMC de sensoren/beheerde apparaten te specificeren waarbij hun eStreamer-gebeurtenissen naar de eStreamer-client worden verstuurd?

Met slechts één FMC-domein op dit moment is dit niet mogelijk. Verwante verbeteringsaanvraag CSCvt31270. U kunt ook op FMC in twee verschillende domeinen configureren. In het eerste domein, voegt u alle beheerde apparaten toe die u wilt eStreamer voor en configureren de eStreamer client. Voor het tweede domein, voegt u de rest van de apparaten toe en vormt geen eStreamer.

Wat is de versie van eStreamer op Firepower? Ik heb deze informatie nodig voor de SIEM-configuratie (bijvoorbeeld LogRhythm)

U kunt de versie van Firepower (FMC) van het FMC UI-venster als volgt controleren **naar Help** (rechterbovenhoek) **> Info > Software-versie**

Wanneer FMC is ingesteld met domeinen hoe de domeininformatie in de FMC eStreamer-gegevens moet worden weergegeven?

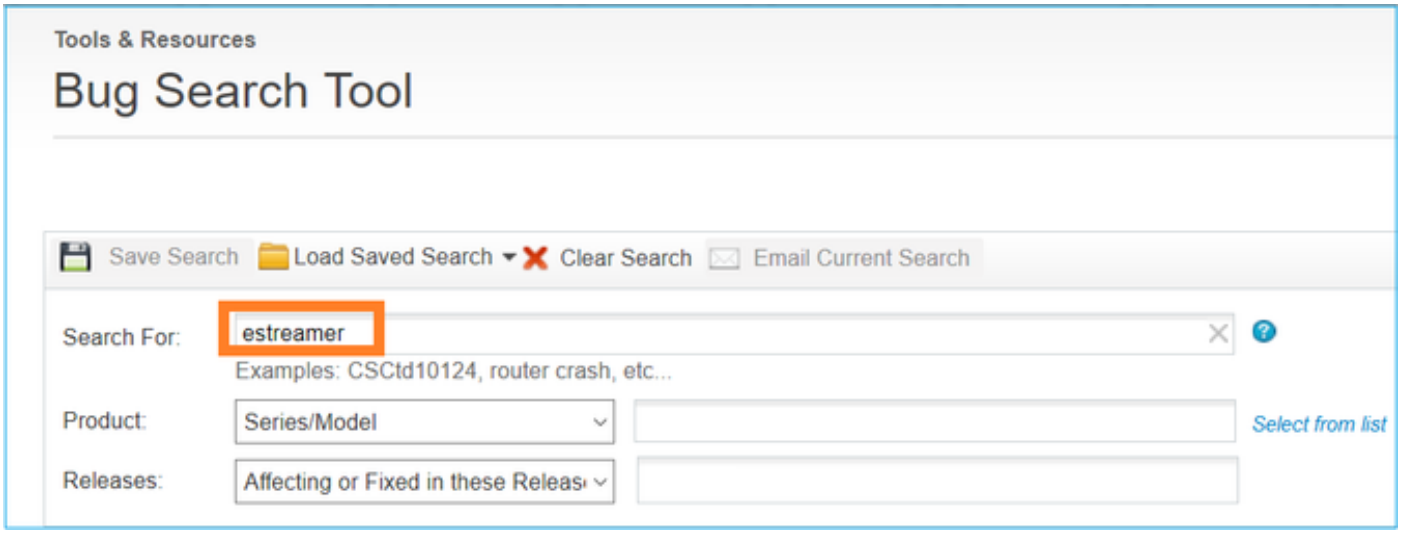
In de eStreamer Integration Guide controleert u het **NetMap-ID** naast het Record Type in het header-gedeelte van veel verschillende typen records. Het NetMap ID-nummer kan worden geconverteerd naar Domain of Devices-naam met behulp van respectievelijk **Netmap Domain**

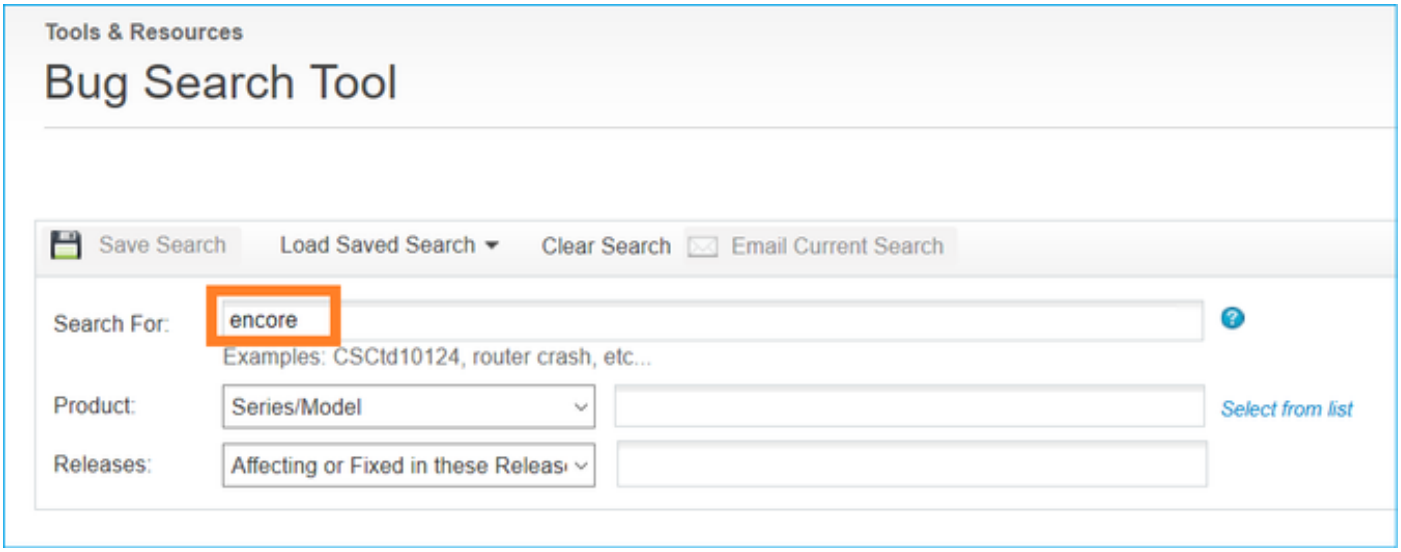
Metagegevens (Record Type 350) en **Managed Devices Record** (Record Type 123).

De clienttoepassing moet de binaire gegevens en metagegevens interpreteren volgens de informatie in de eStreamer Integration Guide.

Bekende problemen

Open de [zoekfunctie voor bugs] en zoek naar stroomlijning en andere problemen, bijvoorbeeld.





Gerelateerde informatie

- Streamer Server-streaming