Comprender eStreamer y solucionar problemas de integración de núcleo

Contenido

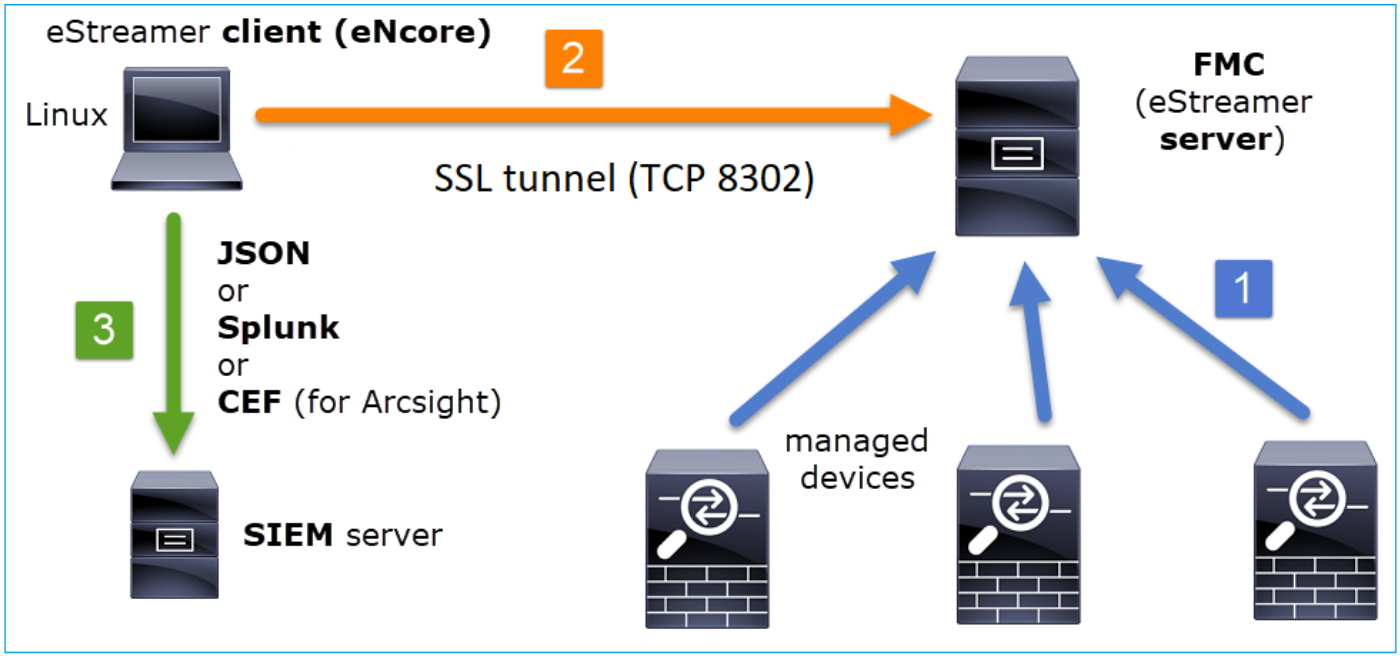
Introducción

Este documento describe el cliente CLI de núcleo de Cisco Event Streamer (también conocido como eStreamer). Específicamente, describe la operación y proporciona información de troubleshooting. Además, cubre los problemas más comunes que se ven en el centro de asistencia técnica Cisco Technical Assistance Center (TAC) junto con las preguntas frecuentes (FAQ).

Colaborado por David Torres Rivas, Mikis Zafeiroudis, Ingenieros del TAC de Cisco.

Overview

eNcore es un cliente de uso general, que solicita todos los eventos posibles del servidor eStreamer (FMC), analiza el contenido binario y genera eventos en diversos formatos para admitir otras herramientas de información de seguridad y gestión de eventos (SIEM).



Establecimiento de conexión eStreamer

El cliente (núcleo) inicia una conexión al puerto TCP 8302 de FMC donde se realiza el intercambio de señales SSL:

```
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>
```

El FMC acepta la conexión, realiza el intercambio de señales SSL en el mismo puerto y verifica el nombre común del cliente (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
```

A continuación, el cliente eStreamer verifica su configuración y el archivo de marcadores para

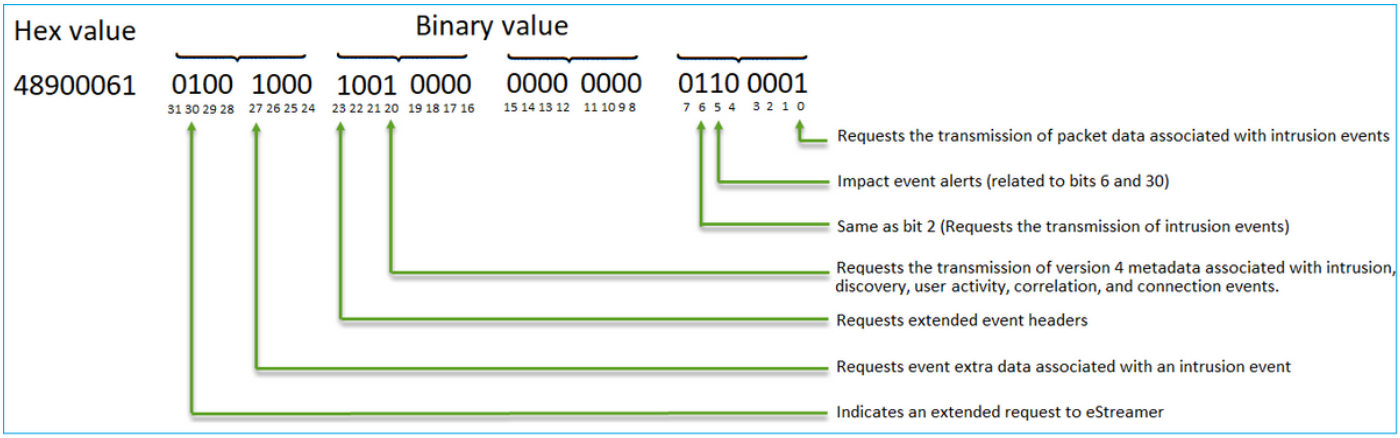
determinar qué eventos solicitar y la hora de inicio:

```
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
```

EventStreamRequest se puede correlacionar en 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
```

EventStreamRequest es la representación hexadecimal de los indicadores de solicitud descritos en Request Flags y se debe convertir en binario para comprender si el cliente solicitó los datos requeridos. Aquí tiene un ejemplo:



> **Nota:** Algunos bits de indicador pueden cambiar la información proporcionada si se inician las solicitudes extendidas.

En función de los bits de solicitud, el FMC envía los datos al cliente eStreamer.

¿Quién inicia la conexión eStreamer y la transferencia de datos?

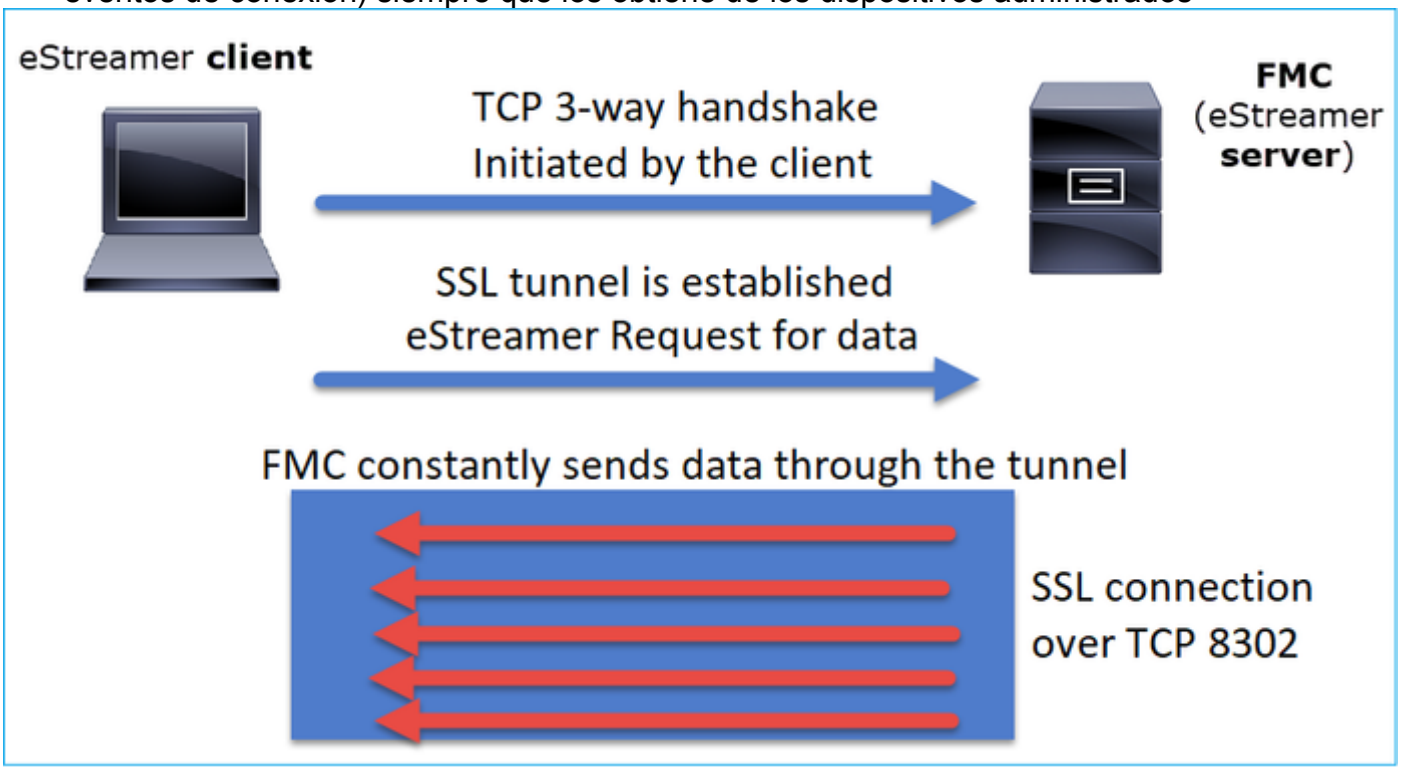
El cliente eStreamer. Específicamente, el cliente establece una conexión TCP (entrada en contacto de 3 vías) y luego hay una negociación SSL con autenticación de cliente (mutua). Por último, a través del túnel establecido, el FMC envía los datos cada vez que hay datos que deben

enviarse:

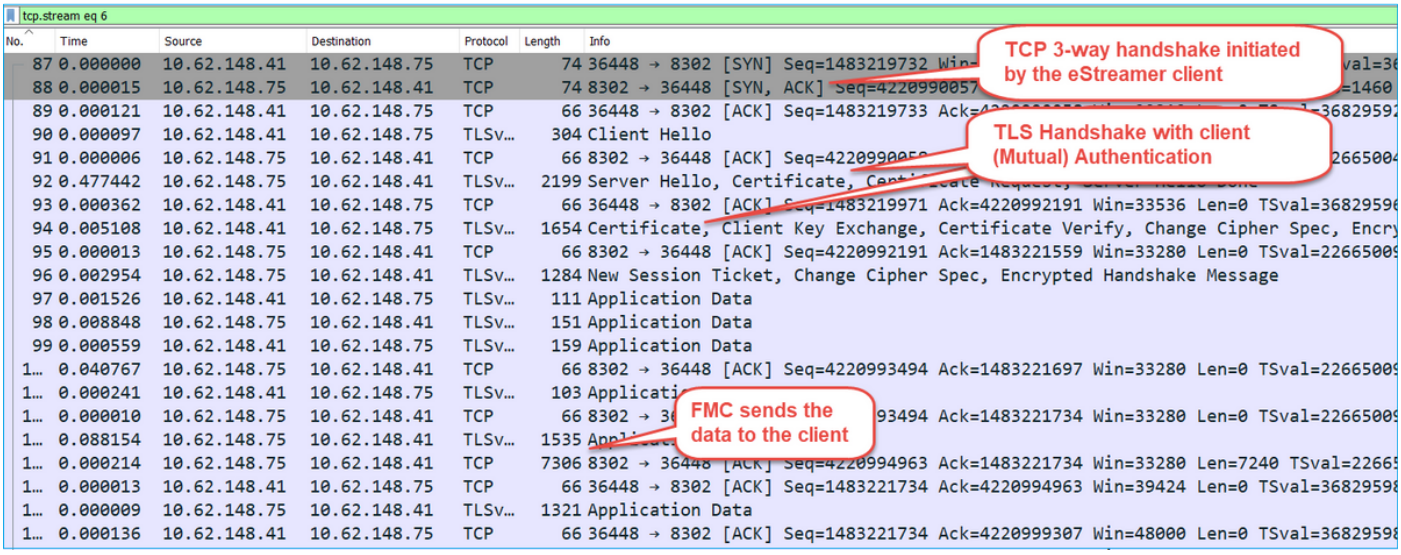
```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100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

En resumen:

- El cliente inicia el túnel SSL para solicitar datos (pull)
- Una vez establecido el túnel, el túnel permanece ACTIVO y el FMC envía datos (por ejemplo, eventos de conexión) siempre que los obtiene de los dispositivos administrados



En este ejemplo, la IP 10.62.148.41 es el cliente eStreamer (Núcleo) mientras que la IP 10.62.148.75 es el 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=4220990058
92	0.477442	10.62.148.75	10.62.148.41	TLSv…	2199	Server Hello, Certificate, Certificate Request, Server Hello Done
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	Application
1…	0.000010	10.62.148.75	10.62.148.41	TCP	66	8302 → 36 93494 Ack=1483221734 Win=33280 Len=0 TSval=2266500
1…	0.088154	10.62.148.75	10.62.148.41	TLSv…	1535	Appl
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

Configurar

Para obtener más información sobre el cliente CLI de NetCore, refiérase a eStreamer Ncore CLI Operations Guide v3.5.

Los detalles de la aplicación eStreamer junto con los pasos de configuración de FMC se tratan en la Guía de integración de Event Streamer.

Ajuste del archivo estreamer.conf

Esta sección describe lo que se puede o se debe modificar en estreamer.conf para que la solución funcione correctamente. El archivo estreamer.conf se encuentra dentro del *directorio path*/eStreamer-Net. A continuación se muestra un ejemplo del contenido del archivo:

```
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
```

La sección de suscripción

Para modificar la solicitud del generador de eventos hacia el servidor (FMC), modifique la sección de suscripciones de eStreamer.conf. Por ejemplo, cuando establece solicitudes extendidas en false, cambia EventStream Request en 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
        },
```

Con solicitudes extendidas = falso:

```
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
```

Con solicitudes extendidas = 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
```

La sección de registro

Para habilitar las depuraciones en la CLI de núcleo, edite el archivo estreamer.conf y cambie el nivel de registro:

```
 "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
    },
```

La sección Monitor

Para ver el número de eventos/segundo procesados y el marcador actual, edite la sección de supervisión en 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)
  },
```

Otras claves de nivel superior relevantes:

```
"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.
```

Este valor se puede establecer entre 2 y 12. El objetivo de más procesos es mejorar el rendimiento, pero cada proceso conlleva un coste general. El resultado es que el rendimiento óptimo se logra con la combinación correcta de "número de procesos" con la capacidad de procesamiento de la máquina host. Las mejores directrices disponibles son:

- Para 2 núcleos: "Procesos de trabajo": 4
- Para 4 o más núcleos: "Procesos de trabajo": 12

Troubleshoot

Para ver los procedimientos genéricos de solución de problemas de eStreamer, consulte este documento Solución de problemas entre FireSIGHT System y eStreamer Client (SIEM)

Para realizar pruebas, puede habilitar Núcleo como proceso en primer plano y verificar la comunicación con FMC

```
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;
```

Al mismo tiempo, en FMC puede ver registros como estos cuando el cliente NetCore Streaming establece la conexión. Tenga en cuenta que la zona horaria del motor FMC es siempre UTC:

```
root@FMC2000-2:~# tail -f /var/log/messages
Jun  4 09:48:00 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Accepted
IPv4 connection from 10.62.148.41:36528/tcp
Jun  4 09:48:00 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Added
10.62.148.41(8512) to host table
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):SFUtil [INFO] Found IPv4 address 10.62.148.41 for ksec-sfvm-win7-3.cisco.com
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Resolved CN ksec-sfvm-win7-3.cisco.com to 10.62.148.41
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Matched Certificate CN:ksec-sfvm-win7-3.cisco.com to
10.62.148.41 (IPv4)
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Got EVENT_STREAM_REQUEST length 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service INFO total data size 48
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service id:5001 - length size 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service id:5000 - length size 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Publishing service id:6667 - length size 8
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] Got UEC_STREAM_REQUEST length 56
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] requested service [6667] timestamp [1591210934]
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 12, version 9
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 21, version 4
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 31, version 9
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 61, version 11
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 71, version 14
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 91, version 4
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 101, version 7
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 111, version 6
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] Got Event type 131, version 2
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):sfestreamer [INFO] EventStream Request (0x48900061): Since 1591210934 w/ NS Events
w/ NS 6.0 Events w/ Packets w/ Extra IDS Event data w/ Metadata v4 w/ RUA 5.2 Events w/ Impact
Alerts w/ 5.3 Impact Alerts w/ Impact Flags w/ RNA 5.3 Events w/ RNA 6.0
Flow w/ Policy 5.4 Events w/ FireAMP 6.0 Events w/ Filelog 6.0 Events w/ Send archive timestamp
w/ Send Detail Request
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):ConnectionHandler [INFO] creating iterator for service [6667] prefix [unified2.]
timestamp [1591210934]
Jun  4 09:48:00 FMC2000-2 SF-IMS[8512]: [8512] EventStreamer child(ksec-sfvm-win7-
3.cisco.com):Unified2Iterator [INFO] Opened /var/sf/archive/netmap_2/unified2.1591210800
Jun  4 09:48:02 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Child
with pid 8510 exited with status 5120
Jun  4 09:48:02 FMC2000-2 SF-IMS[4135]: [4135] Event Streamer:ConnectionHandler [INFO] Removed
host entry for pid: 8510
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
URLFiltering: 310f4c00-a415-11ea-bf5b-a2d6028849fe
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
```

```
URLFiltering: d637b6f0-a414-11ea-ad97-cc17b6ea4c03
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
URLFiltering: 873709b8-78b6-11ea-ae87-b82f93835447
Jun  4 09:48:04 FMC2000-2 SF-IMS[22296]: [25092] CloudAgent:url_license [INFO] Peer with active
URLFiltering: c7c0217c-78b6-11ea-a719-b7f0a277eb86
```

Elementos que se deben recopilar antes de ponerse en contacto con el Cisco Technical Assistance Center (TAC)

Se recomienda recopilar estos elementos antes de ponerse en contacto con el TAC de Cisco:

- La versión de eStreamer Net
- La versión de Python
- La versión del SO host
- ¿Ve eventos en FMC? Compartir una captura de pantalla de eventos + configuración de FMC eStreamer
- Habilite debug en la CLI de núcleo (como se describe en la 'sección registro')
- Generar un archivo de resolución de problemas de FMC
- Proporcione estos archivos desde Núcleo:
  estreamer.conf
  estreamer.log

Problemas comunes

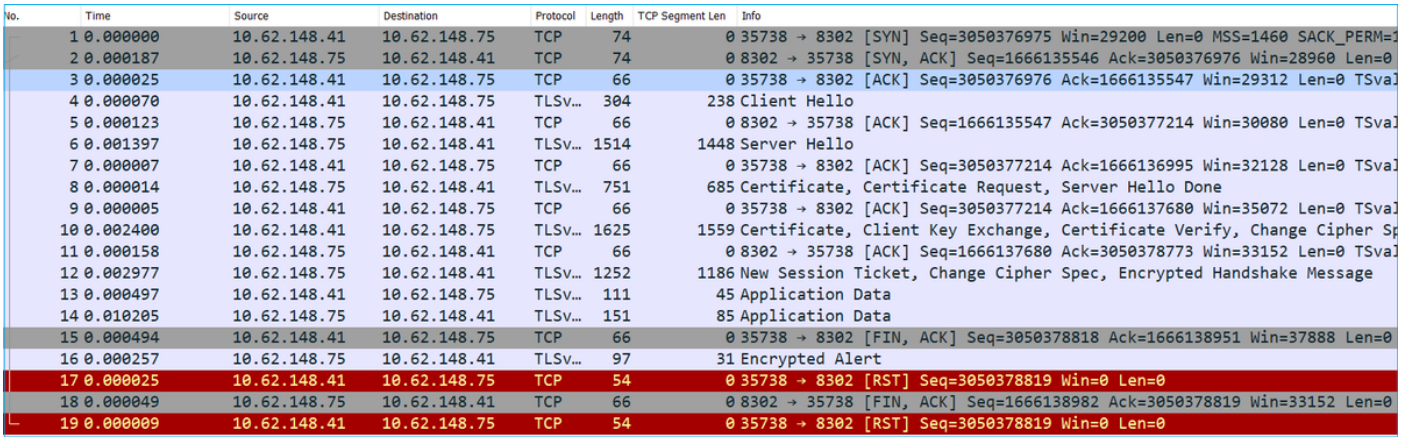
No hay conectividad en el puerto TCP 8302

Telnet del cliente eStreamer al puerto FMC 8302 y verifique que se haya establecido la conectividad.

Además, puede utilizar la opción de prueba de Ncore para probar la conectividad:

```
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
```

Este es un intento de conexión exitoso como se ve en Wireshark (10.62.148.41 es la IP principal mientras que 10.62.148.75 es el 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

El certificado CN no coincide con el host remoto

Si el cliente eStreamer está detrás de NAT, el certificado se debe generar con la dirección IP ascendente o se ven errores como estos:

```
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
```

La resolución DNS de FMC para el cliente eStreamer es incorrecta

En caso de que FMC tenga entradas de DNS erróneas para el cliente eStreamer, los eventos no llegan al cliente. Para identificar si este es el problema, tome una captura en FMC. En este ejemplo, el FMC recibe un paquete TCP SYN del host del cliente de streaming 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
```

Puede utilizar el indicador **-n** para ver la IP resuelta:

```
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
```

Como alternativa, puede utilizar la herramienta de comandos **nslookup** desde la CLI de FMC:

```
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
```

Problema de comunicación eStreamer debido a error de certificado SSL

Asegúrese de que el cliente eStreamer utiliza el certificado SSL FMC correcto. Si el certificado es incorrecto en los archivos FMC /var/log/message, verá estos eventos:

```
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
```

Puede eliminar el cliente eStreamer en FMC y reconfigurarlo. Esto regenera el certificado SSL. Importe el nuevo certificado en el cliente eStreamer.

Dirección IP incorrecta configurada en eStreamer para la integración del módulo ASA SFR

En el cliente eStreamer, debe utilizar la IP del módulo SFR. En ASA ejecute el comando **show sfr module details** para ver la IP del módulo.

Formato de evento común de ArcSight (CEF)

El estándar de formato de evento común de Arcsight define los pares clave-valor que se deben enviar desde la CLI de NetCore. Si hay inconsistencia en los datos recibidos sobre Arcisght, por ejemplo: falta campos, fuera de orden, o algunos datos no se analizan correctamente en el cliente de Arcsight, es útil modificar la configuración para escribir en un archivo de registro mediante la configuración. Esto ayuda a determinar dónde se encuentra el problema.

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

Los eventos de CEF RAW se escriben en una línea con cada campo separado por la tubería "|":

```
<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
```

El cliente eStreamer no muestra todos los registros

Esto se debe a menudo a la sobresuscripción del cliente eStreamer (demasiados eventos enviados por el FMC). Ejecute este comando en el cliente eStreamer y verifique si el contador Recv-Q es alto. Este es el recuento de bytes que el programa de usuario no ha copiado y que está conectado a este socket. En este ejemplo hay 143143 bytes pendientes en el lado cliente:

```
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
```

Verifique los eventos por segundo recibidos por el cliente eStreamer. Esto le proporciona una indicación de la velocidad de eventos por segundo:

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

Intente reducir la cantidad de datos solicitados por el cliente eStreamer o los tipos de eventos enviados por el FMC. Alternativamente, puede intentar aumentar la cantidad de recursos asignados en el lado del cliente eStreamer.

Preguntas frecuentes (FAQ)

¿Dónde obtener el paquete de Ncore-cli?

- Verifique la página de descarga del software FMC, **Firepower System Tools y API - NetCore para CEF**
- Alternativamente, puede obtener el archivo eNcore más reciente de https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets

Cuando hay una copia de seguridad completa de FMC en curso, eStreamer no genera eventos. ¿Es normal?

Sí, es un comportamiento esperado. Desde la Guía de configuración de FMC Cuándo realizar una Copia de Seguridad:

Mientras el sistema recopila datos de copia de seguridad, puede haber una pausa temporal en la correlación de datos (sólo FMC) y es posible que se le impida cambiar las configuraciones relacionadas con la copia de seguridad.

¿Se necesitan licencias especiales para la integración de FMC con el cliente eStreamer (por ejemplo, Qradar)?

No

¿De dónde se obtienen los eventos de eStreamer?

El FMC. Específicamente, el FMC obtiene los eventos de los dispositivos administrados (FTD) y los reenvía a los clientes eStreamer como NetCore, ArcSight, Splunk, QRadar, LogRhythm, etc.

¿Hay alguna matriz de compatibilidad entre Splunk y eNcore?

Verifique los documentos Splunk para obtener información de compatibilidad. Por ejemplo, para ver qué versiones de Splunk son compatibles con la versión 3.6.8 de NetCore, consulte https://splunkbase.splunk.com/app/3662/

¿Puede eStreamer NetFlow consumir datos de varios FMC?

En el momento de escribir este artículo, no. Solicitud de mejora de verificación CSCvq14351

¿Cuáles son las opciones recomendadas para configurar eStreamer para la configuración de alta

disponibilidad (HA) de FMC?

La recomendación es configurar solamente la unidad FMC activa para eStreamer. Si configura ambas unidades FMC para eStreamer, el SIEM recibe eventos duplicados porque el FMC en espera responde a la solicitud eStreamer. Solicitud de mejora relacionada: CSCvi95944

¿Se requiere una actualización de FMC para generar manualmente nuevos certificados eStreamer?

No

¿Se envían los eventos de Security Intelligence al cliente eStreamer? ¿Es posible seleccionar eventos de Security Intelligence como categoría independiente y enviarlos a un cliente eStreamer?

Los eventos de Security Intelligence (SI) se incluyen en la categoría de eventos Connection y no como categoría independiente. Debido a esto, no hay ningún evento SI separado que se envíe al optimizador. Solicitud de mejora relacionada: CSCva39052

¿Es posible especificar en FMC los sensores/dispositivos administrados que envían sus eventos eStreamer al cliente eStreamer?

Con sólo un dominio FMC actualmente, esto no es posible. Solicitud de mejora relacionada CSCvt31270. Alternativamente, puede configurar en FMC dos dominios diferentes. En el primer dominio, se agregan todos los dispositivos administrados para los que se desea habilitar eStreamer y configurar el cliente eStreamer. Para el segundo dominio, usted agrega el resto de los dispositivos y no configura eStreamer.

¿Cuál es la versión de eStreamer en Firepower? Necesito esta información para la configuración SIEM (por ejemplo, LogRhythm)

Para comprobar la versión de Firepower (FMC) desde la interfaz de usuario de FMC, vaya a **Ayuda** (esquina superior derecha) **> Acerca de > Versión de software**

Cuando se configura FMC con dominios, ¿cómo ver la información de dominio en los datos de FMC eStreamer?

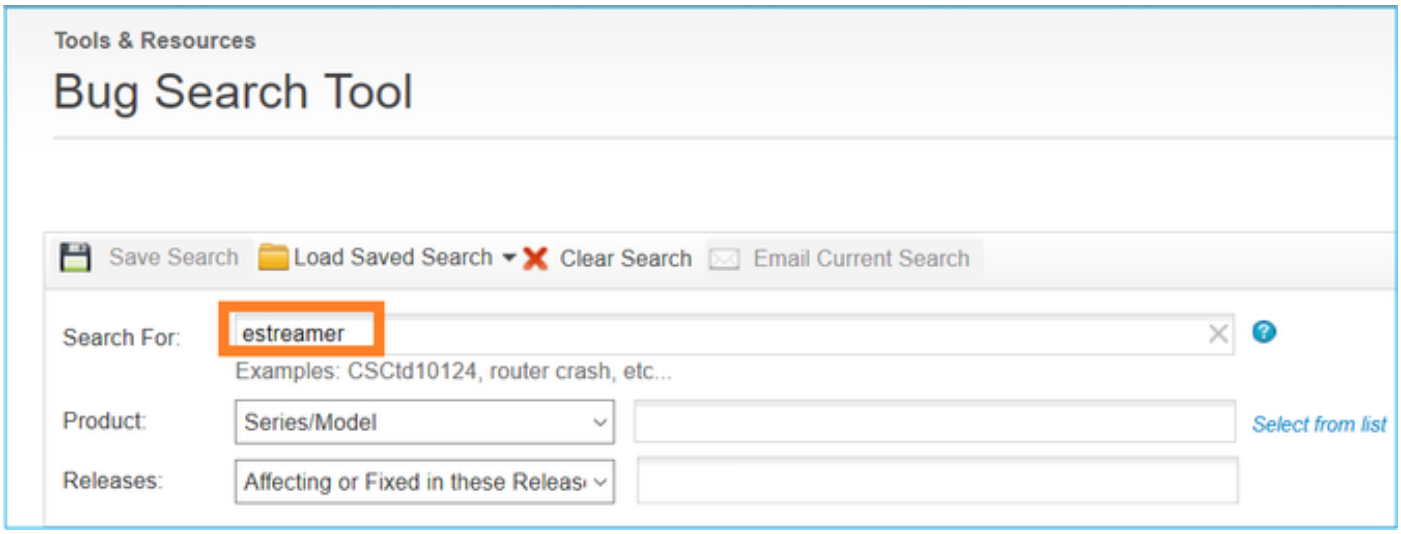
En la Guía de Integración de eStreamer verifique el **número de ID de Netmap** junto al Tipo de

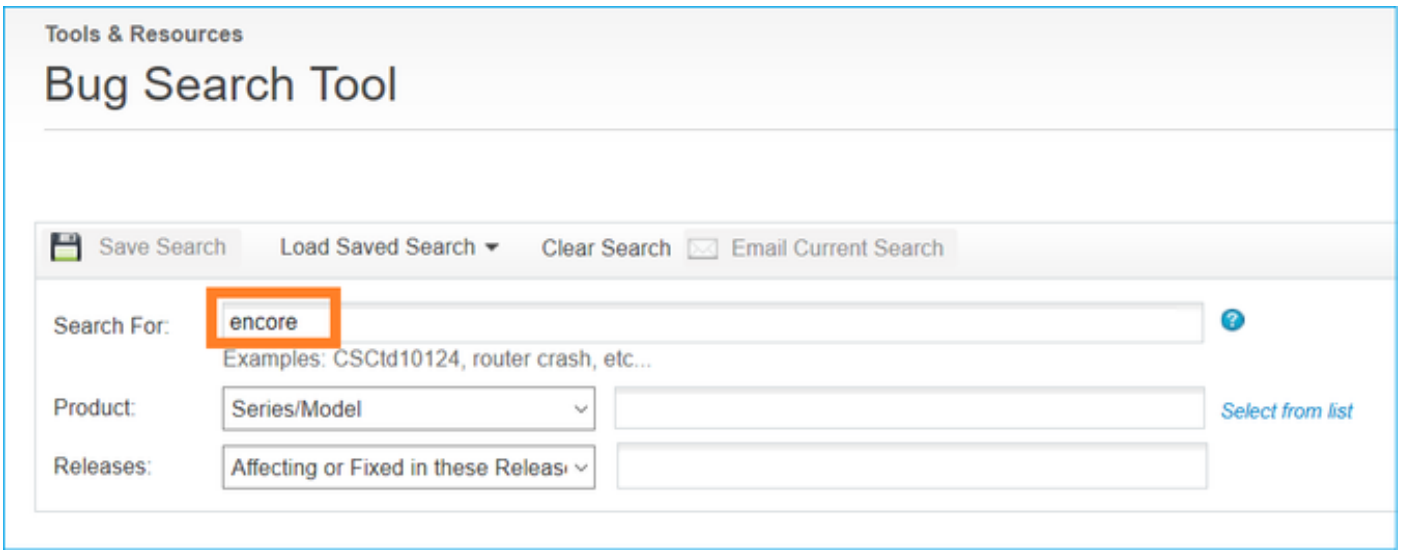
Registro en la sección de encabezado de muchos tipos de registros diferentes. El número de ID de Netmap se puede convertir en Dominio o Nombre de dispositivo mediante **Metadatos de Dominio de Netmap** (Tipo de Registro 350) y **Metadatos de Registro de Dispositivos Administrados** (Tipo de Registro 123), respectivamente.

La aplicación cliente debe interpretar los datos binarios y los metadatos según la información proporcionada en la Guía de integración de eStreamer.

Problemas conocidos

Abra la Herramienta de búsqueda de errores y busque problemas de agilización y repetición, p. ej.





Información Relacionada

- Transmisión de servidores eStreamer