Comprendre eStreamer et dépanner l'intégration du noyau

Contenu

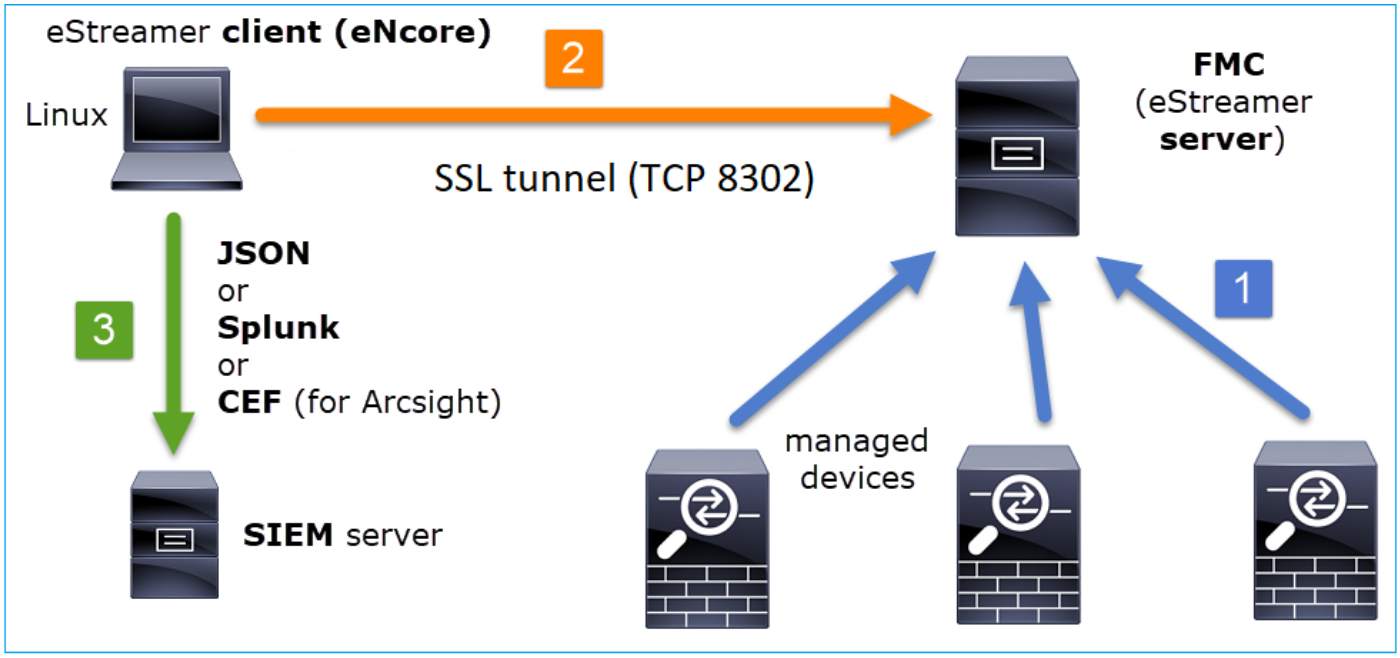
Introduction

Ce document décrit le client CLI Core Event Streamer de Cisco (également appelé eStreamer). Plus précisément, il décrit l'opération et fournit des informations de dépannage. En outre, il couvre les problèmes courants constatés par le centre d'assistance technique Cisco (TAC) ainsi que les questions fréquemment posées (FAQ).

Avec la collaboration de David Torres Rivas, Mikis Zafeiroudis, ingénieurs du TAC Cisco.

Aperçu

eCore est un client polyvalent qui demande tous les événements possibles au serveur eStreamer (FMC), analyse le contenu binaire et génère des événements dans différents formats pour prendre en charge d'autres outils SIEM (Security Information and Event Management Tools).



Établissement de la connexion eStreamer

Le client (noyau) initie une connexion au port TCP 8302 FMC où la connexion SSL est effectuée :

```
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>
```

Le FMC accepte la connexion, effectue une connexion SSL sur le même port et vérifie le nom commun (CN) du client :

```
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
```

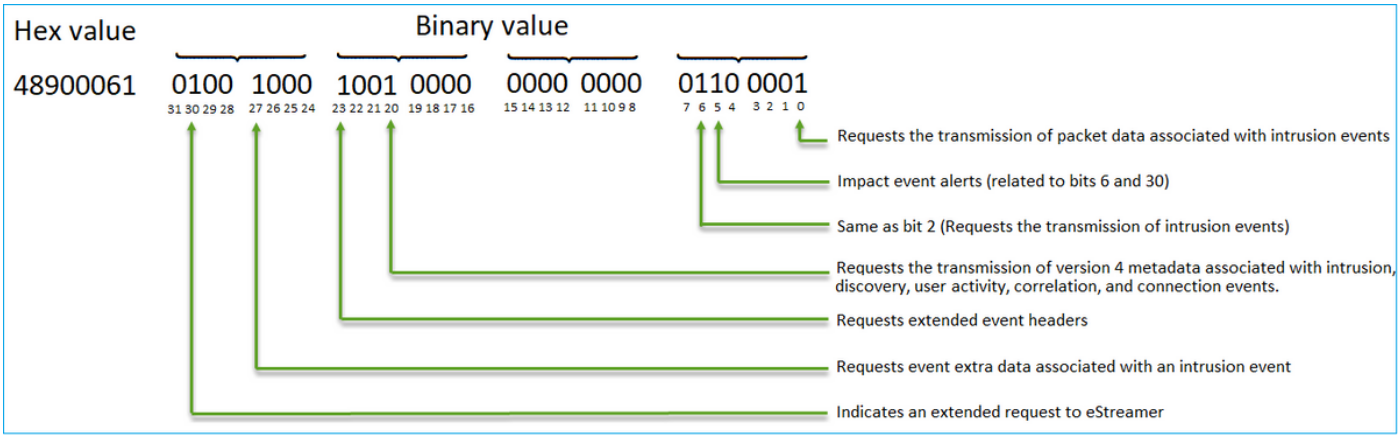
Le client eStreamer vérifie ensuite sa configuration et son fichier de signet afin de déterminer les événements à demander et l'heure de début :

```
2020-03-02 07:18:11,500 Connection   INFO     Connecting to 10.48.26.49:8302
2020-03-02 07:18:11,500 Connection   INFO     Using TLS v1.2
2020-03-02 07:18:11,500 Monitor      INFO     Starting Monitor.
2020-03-02 07:18:11,500 Monitor      INFO     Starting. 0 handled; average rate 0 ev/sec;
2020-03-02 07:18:11,501 Writer       INFO     Starting process.
2020-03-02 07:18:11,506 Transformer  INFO     Starting process.
2020-03-02 07:18:11,985 Bookmark     INFO     Bookmark file /root/eStreamer-eNcore/10.48.26.49-
8302_bookmark.dat does not exist.
2020-03-02 07:18:11,986 Settings     INFO     Timestamp: Start = 2 (Bookmark = 0)
2020-03-02 07:18:11,986 Receiver     INFO     EventStreamRequestMessage:
00010002000000080000000048900061
2020-03-02 07:18:11,986 SubscriberParser INFO     Starting process.
2020-03-02 07:18:11,996 Bookmark     INFO     Bookmark file /root/eStreamer-eNcore/10.48.26.49-
8302_bookmark.dat does not exist.
2020-03-02 07:18:11,996 Settings     INFO     Timestamp: Start = 2 (Bookmark = 0)
2020-03-02 07:18:11,997 Receiver     INFO     StreamingRequestMessage:
000108010000003800001a0b0000003848900061000000000009000c000400150009001f000b003d000e00470004005b
0007006500060060f0002008300000000
```

EventStreamRequest peut être corrélé sur 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 est la représentation hexadécimale des indicateurs de requête décrits sur les indicateurs de requête et doit être converti en binaire afin de comprendre si le client a demandé les données requises. Voici un exemple :



> **Note**: Certains bits d'indicateur peuvent modifier les informations fournies si des demandes étendues sont lancées.

En fonction des bits de requête, le FMC transmet les données au client eStreamer.

Qui initie la connexion eStreamer et le transfert de données ?

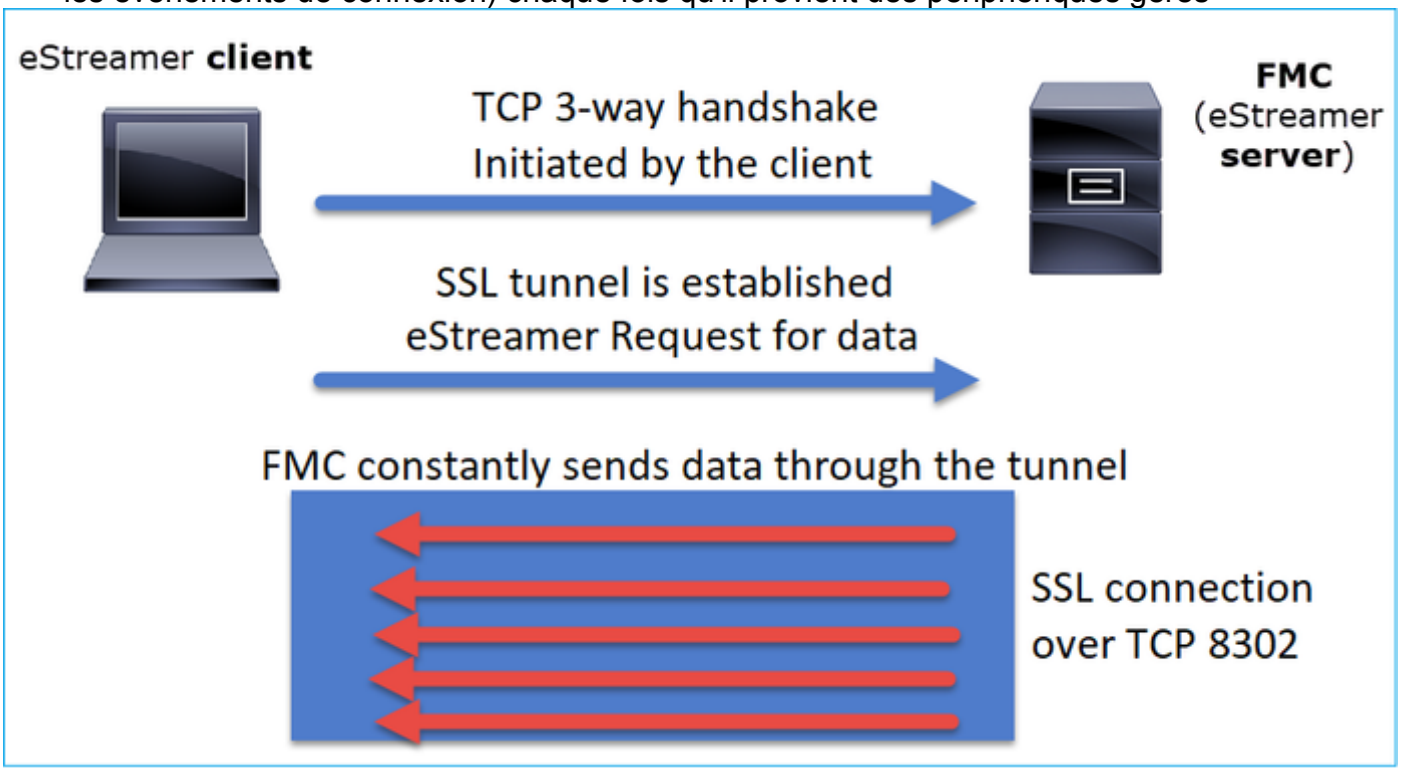
Client eStreamer. Plus précisément, le client établit une connexion TCP (échange en trois étapes), puis il y a une négociation SSL avec l'authentification (mutuelle) du client. Enfin, via le tunnel établi, le FMC envoie les données chaque fois qu'il y a des données à envoyer :

```
root@kali:~/eStreamer-eNcore# ./encore.sh foreground
```

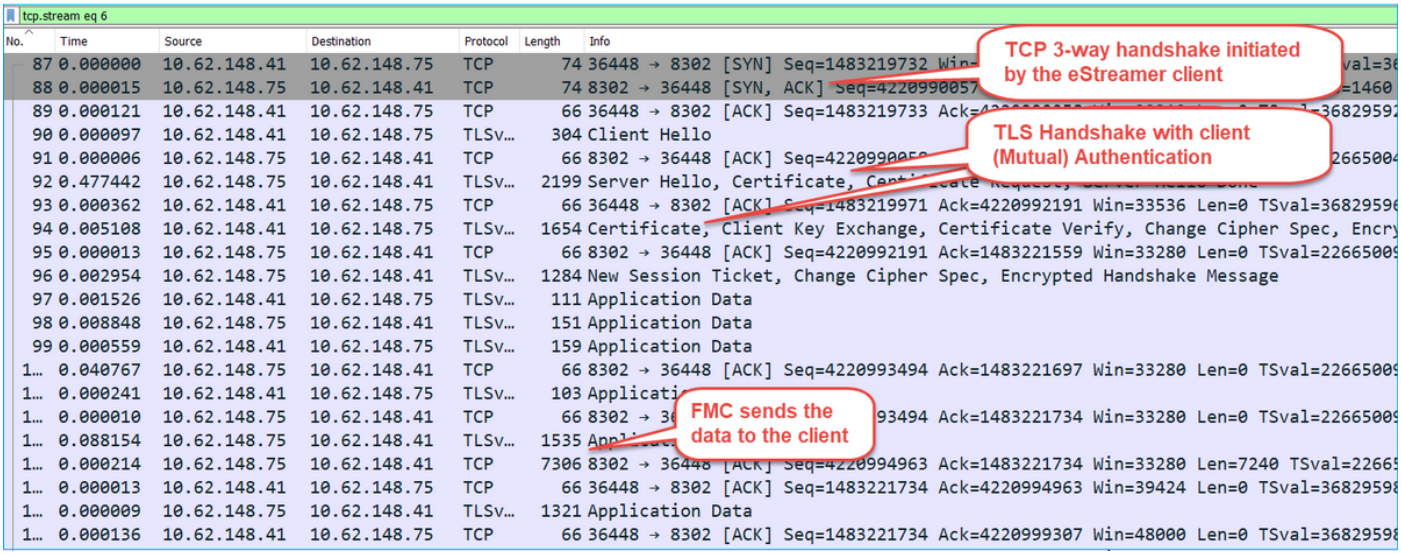
```
2020-06-03 20:50:53,365 Monitor      INFO     Running. 100 handled; average rate 0.42 ev/sec;
2020-06-03 20:52:53,488 Monitor      INFO     Running. 100 handled; average rate 0.28 ev/sec;
2020-06-03 20:54:53,601 Monitor      INFO     Running. 100 handled; average rate 0.21 ev/sec;
2020-06-03 20:56:53,725 Monitor      INFO     Running. 100 handled; average rate 0.17 ev/sec;
```

En résumé :

- Le client lance le tunnel SSL pour demander des données (extraction)
- Une fois le tunnel établi, le tunnel reste actif et le FMC transmet les données (par exemple, les événements de connexion) chaque fois qu'il provient des périphériques gérés



Dans cet exemple, l'adresse IP 10.62.148.41 est le client eStreamer (eCore) tandis que l'adresse IP 10.62.148.75 est le FMC :



Configuration

Pour plus d'informations sur le client CLI ncore, reportez-vous au [Guide d'exploitation CLI ncore eStreamer v3.5.]

Les détails de l'application eStreamer ainsi que les étapes de configuration FMC sont traités dans le Guide d'intégration de Event Streamer.

paramétrage de fichier estreamer.conf

Cette section décrit ce qui peut ou doit être modifié sur estreamer.conf pour que la solution fonctionne correctement. Le fichier estreamer.conf se trouve dans le répertoire *path*/eStreamer-NetCore. Voici un exemple du contenu du fichier :

```
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 section Abonnement

Pour modifier la requête Event Streamer en direction du serveur (FMC), modifiez la section Abonnements eStreamer.conf. Par exemple, lorsque vous affectez la valeur false aux demandes étendues, il modifie EventStream Request sur 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
        },
```

Avec demandes étendues = 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
```

Avec demandes étendues = 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 section logging

Pour activer les débogages sur l'interface de ligne de commande de ncore, modifiez le fichier estreamer.conf et modifiez le niveau du journal :

```
 "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 section Surveillance

Pour afficher le nombre d'événements/seconde traités et le signet en cours, modifiez la section de surveillance sur 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)
  },
```

Autres clés de niveau supérieur pertinentes :

```
"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.
```

Cette valeur peut être définie entre 2 et 12. Plus de processus sont destinés à améliorer les performances, mais chaque processus comporte un coût supplémentaire. Il en résulte que les performances optimales sont obtenues grâce à la bonne combinaison du « nombre de processus » et de la capacité de traitement de la machine hôte. Les meilleures directives disponibles sont les suivantes :

- Pour 2 coeurs : « workerProcesses » : 4
- Pour 4 coeurs ou plus : « workerProcesses » : 12

Dépannage

Pour les procédures de dépannage eStreamer génériques, reportez-vous à ce document [Dépannage des problèmes entre FireSIGHT System et eStreamer Client (SIEM)]

Àdes fins de test, vous pouvez activer NetCore en tant que processus de premier plan et vérifier la communication avec 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
0007006500060006f0002008300000000
2020-06-04 11:48:00,653 Monitor      INFO     Running. 0 handled; average rate 1.2 ev/sec;
```

En même temps, sur FMC, vous pouvez voir des journaux comme ceux-ci lorsque le client de flux d'accès NetCore établit la connexion. Notez que le fuseau horaire principal FMC est toujours 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
```

Éléments à collecter avant de contacter le centre d'assistance technique Cisco (TAC)

Il est vivement recommandé de collecter ces éléments avant de contacter le TAC Cisco :

- Version d'eStreamer NetCore
- La version de Python
- Version du système d'exploitation hôte
- Voyez-vous des événements sur FMC ? Partager une capture d'écran d'événements + configuration de FMC eStreamer
- Activer le débogage sur l'interface de ligne de commande (comme décrit dans la section 'logging')
- Générer un fichier de dépannage à partir de FMC
- Fournissez ces fichiers à partir de NetCore :
  estreamer.conf
  estreamer.log

Problèmes courants

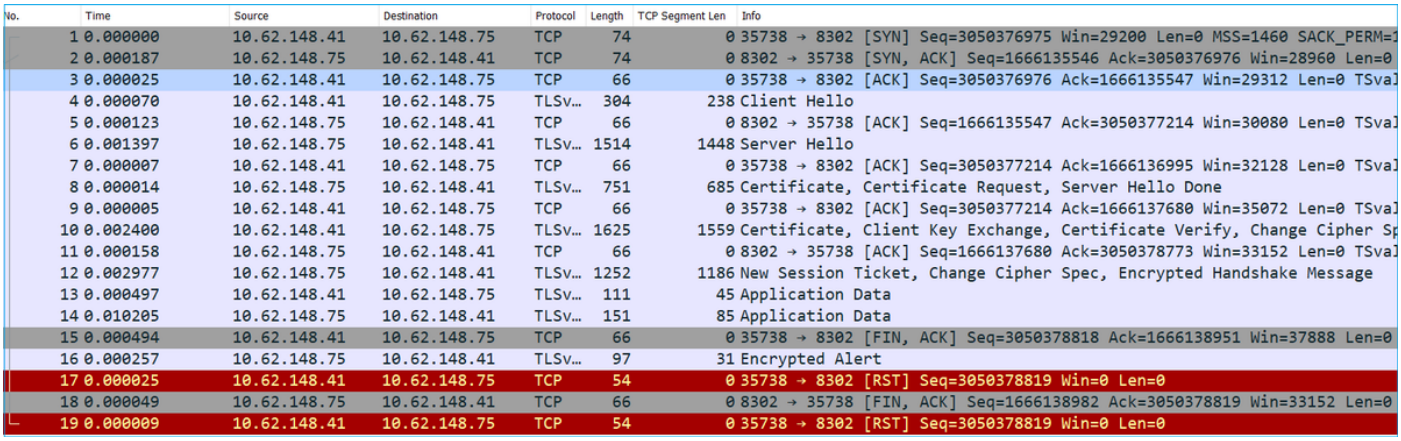
Aucune connectivité sur le port TCP 8302

Établissez une connexion Telnet entre le client eStreamer et le port FMC 8302 et vérifiez que la connectivité est établie.

En outre, vous pouvez utiliser l'option de test Core pour tester la connectivité :

```
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
```

Il s'agit d'une tentative de connexion réussie, comme le montre Wireshark (10.62.148.41 est l'adresse IP principale tandis que 10.62.148.75 est le 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

Le certificat CN ne correspond pas à l'hôte distant

Si le client eStreamer est derrière NAT, le certificat doit être généré avec l'adresse IP en amont ou des erreurs comme celles-ci sont visibles :

```
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
```

Résolution DNS FMC du client eStreamer incorrecte

Si FMC a des entrées DNS incorrectes pour le client eStreamer, les événements n'atteignent pas le client. Pour déterminer si c'est le problème, prenez une capture sur FMC. Dans cet exemple, le FMC reçoit un paquet SYN TCP de l'hôte client de flux 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
```

Vous pouvez utiliser l'indicateur **-n** pour voir l'adresse IP résolue :

```
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
```

Vous pouvez également utiliser l'outil de commande **nslookup** de l'interface de ligne de commande 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
```

Problème de communication eStreamer en raison d'une erreur de certificat SSL

Assurez-vous que le client eStreamer utilise le certificat SSL FMC correct. Si le certificat est incorrect dans les fichiers FMC /var/log/message, les événements suivants s'affichent :

```
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
```

Vous pouvez supprimer le client eStreamer sur FMC et le reconfigurer. Ceci régénère le certificat SSL. Importez le nouveau certificat dans le client eStreamer.

Mauvaise adresse IP configurée sur eStreamer pour l'intégration du module ASA SFR

Sur le client eStreamer, vous devez utiliser l'adresse IP du module SFR. Sur ASA exécutez la commande **show sfr module details** pour voir l'IP du module.

Format d'événement commun ArcSight (CEF)

La norme Arcsight Common Event Format Standard définit les paires clé-valeur qui doivent être envoyées à partir de l'interface CLI principale. En cas d'incohérence sur les données reçues sur Arcisght, c'est-à-dire : champs manquants, désactivés ou certaines données ne sont pas analysées correctement sur le client Arcsight, il est utile de modifier la configuration pour écrire dans un fichier journal en définissant un paramètre. Cela permet de déterminer où se trouve le problème.

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

Les événements CEF RAW sont écrits dans une ligne avec chaque champ séparé par un canal “| ” :

```
<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
```

Le client eStreamer n'affiche pas tous les journaux

Cela est souvent dû à la sursouscription du client eStreamer (trop d'événements envoyés par le FMC). Exécutez cette commande côté client eStreamer et vérifiez si le compteur Recv-Q est élevé. Il s'agit du nombre d'octets non copiés par le programme utilisateur connecté à ce socket. Dans cet exemple, il y a 143143 octets en attente côté client :

```
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
```

Vérifiez les événements reçus par seconde par le client eStreamer. Ceci vous donne une indication des événements par seconde taux :

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

Essayez de réduire la quantité de données demandée par le client eStreamer ou les types d'événements envoyés par le FMC. Vous pouvez également essayer d'augmenter la quantité de ressources allouées côté client eStreamer.

Foire aux questions (FAQ)

Où trouver le paquet NetCie-cli ?

- Consultez la page de téléchargement du logiciel FMC, **Outils et API Firepower System - Noyau pour CEF**
- Vous pouvez également obtenir le dernier fichier de noyau à partir de https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight/tree/master/assets

Lorsqu'une sauvegarde complète FMC est en cours, eStreamer ne génère pas d'événements. Est-ce normal ?

Oui, c'est un comportement attendu. À partir du guide de configuration FMC Quand effectuer une sauvegarde :

Pendant que le système collecte des données de sauvegarde, il peut y avoir une pause temporaire dans la corrélation des données (FMC uniquement) et vous pouvez être empêché de modifier les configurations liées à la sauvegarde.

Existe-t-il des licences spéciales requises pour l'intégration de FMC au client eStreamer (par exemple Qradar) ?

Non

D'où proviennent les événements eStreamer ?

Le FMC. Plus précisément, le FMC récupère les événements des périphériques gérés (FTD) et les transmet aux clients eStreamer tels que NetCore, ArcSight, Splunk, QRadar, LogRhythm, etc.

Existe-t-il une matrice de compatibilité entre Splunk et NetCore ?

Vérifiez les documents Splunk pour obtenir des informations de compatibilité. Par exemple, pour voir quelles versions de Splunk sont compatibles avec NetCore version 3.6.8, consultez https://splunkbase.splunk.com/app/3662/

eStreamer NetCore peut-il consommer des données de plusieurs FMC ?

Au moment de la rédaction du présent document, non. Vérifiez la demande d'amélioration CSCvq14351

Quelles sont les options recommandées pour configurer eStreamer pour la haute disponibilité de FMC ?

Il est recommandé de configurer uniquement l'unité FMC active pour eStreamer. Si vous configurez les deux unités FMC pour eStreamer, le SIEM reçoit des événements en double car le FMC de secours répond à la demande eStreamer. Demande d'amélioration associée : CSCvi95944

Une mise à niveau FMC nécessite-t-elle de générer manuellement de nouveaux certificats eStreamer ?

Non

Les événements Security Intelligence sont-ils envoyés au client eStreamer ? Est-il possible de sélectionner des événements Security Intelligence comme une catégorie distincte et de les envoyer à un client eStreamer ?

Les événements Security Intelligence (SI) sont inclus dans la catégorie des événements Connection et non dans une catégorie distincte. Pour cette raison, il n'y a aucun événement SI distinct qui est envoyé au diffuseur. Demande d'amélioration associée : CSCva39052

Est-il possible de spécifier sur FMC les capteurs/périphériques gérés dont les événements eStreamer sont envoyés au client eStreamer ?

Avec un seul domaine FMC actuellement, cela n'est pas possible. Demande d'amélioration connexe CSCvt31270. Vous pouvez également configurer deux domaines différents sur FMC. Dans le premier domaine, vous ajoutez tous les périphériques gérés pour lesquels vous souhaitez activer eStreamer et configurer le client eStreamer. Pour le deuxième domaine, vous ajoutez le reste des périphériques et ne configurez pas eStreamer.

Quelle est la version d'eStreamer sur Firepower ? J'ai besoin de ces informations pour la configuration SIEM (par exemple, LogRhythm)

Pour vérifier la version de Firepower (FMC) à partir de l'interface utilisateur de FMC, accédez à **Aide** (coin supérieur droit) **> À propos de > Version logicielle**

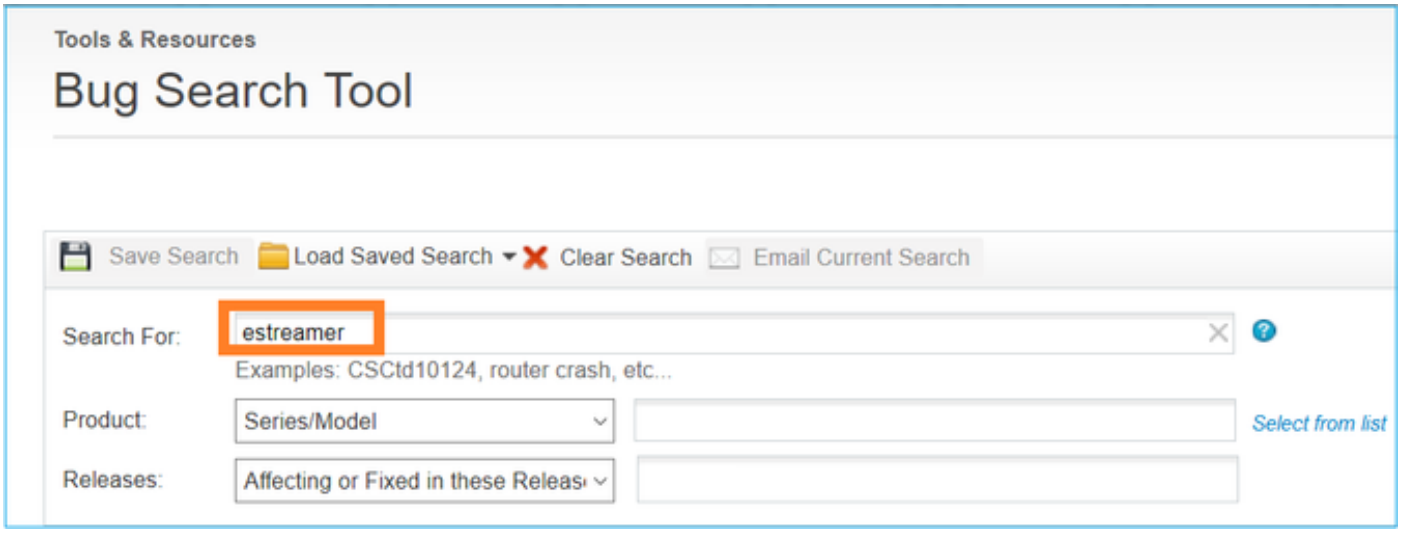
Quand FMC est configuré avec des domaines comment afficher les informations de domaine dans les données eStreamer de FMC ?

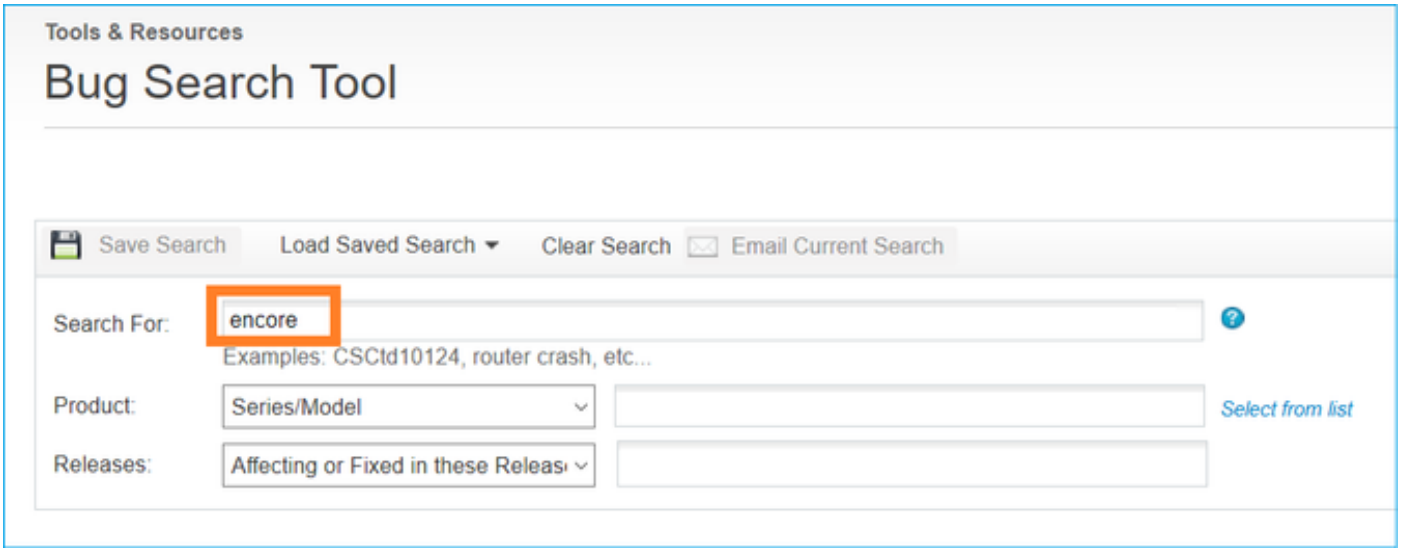
Dans le Guide d'intégration d'eStreamer, vérifiez le numéro d'**ID Netmap** en regard du Type d'enregistrement dans la section en-tête de nombreux types d'enregistrement différents. Le numéro d'ID Netmap peut être converti en nom de domaine ou de périphérique à l'aide des **métadonnées de domaine Netmap** (type d'enregistrement 350) et des **métadonnées d'enregistrement de périphérique géré** (type d'enregistrement 123), respectivement.

L'application cliente doit interpréter les données et métadonnées binaires en fonction des informations fournies dans le Guide d'intégration d'eStreamer.

Problèmes identifiés

Ouvrez l'outil de recherche de bogues et recherchez des problèmes de streaming et de rappel, par ex.





Informations connexes

- Diffusion en continu du serveur eStreamer