Table of Contents

fastdpi_stat.log

Находится в папке: `/var/log/dpi/fastdpi_stat.log`
В данном логе хранится статистика по трафику, который обрабатывает СКАТ DPI

```
[STAT    ][2022/04/07-13:36:24:608426] Memory usage : 'Virtual'/'Resident'
177805156352/3238039552
[STAT    ][2022/04/07-13:36:24:608441] CPU statistics :
        cpu_total : 18.8%us  1.7%sy  0.0%ni 79.5%id  0.0%wa
                cpu0 :  4.6%us  2.7%sy  0.0%ni 92.8%id  0.0%wa
                cpu1 : 20.1%us  0.4%sy  0.0%ni 79.5%id  0.0%wa
                cpu2 : 19.5%us  0.4%sy  0.0%ni 80.1%id  0.0%wa
                cpu3 : 23.4%us  2.1%sy  0.0%ni 74.5%id  0.0%wa
```

На данном участке stat лога:
`[2022/04/07-13:36:24:608426]` — дата и время съема информации

`'Virtual'/'Resident'` — тип памяти.
`Virtual` — виртуальный размер процесса. Показывает общее количество памяти, которое способна адресовать программа в данный момент времени
`Resident` — показывает, сколько физической памяти использует процесс.
После этого параметра идут конкретные значения

`CPU statistics` — статистика по загрузке процессора
`cpu_total` — общая загрузка процессора
`cpu0`, `cpu1`, `cpu2`, `cpu3` — загрузка по конкретному ядру
`us` — сколько всего на данный момент используется
`sy` — сколько на данный момент использует система
`id` — сколько на данный момент свободно
`wa` — показывает процент операций, готовых быть выполненных процессором, но находящихся в состоянии ожидания от диска

Информация по интерфейсам:

```
[STAT    ][2022/04/08-16:25:25:309501] Interface statistics :
        Cluster #0 Absolute Stats Rcvd: [5000 pkts][527701 bytes][1+2=3 pkts
dropped]
        Cluster #0 : IF 01-00.0 (01:00.0):
                Absolute Stats Rcvd: [4873 pkts][507823 bytes][0 pkts
dropped]
                                Send: [127 pkts][19878 bytes]
                                Esnd: [0 err_pkts][0.00 %]
                                Drop: [0 pkts][0 bytes]
                                Pthr: [0 pkts][0 bytes]
                                Emit: [0 pkts][0 bytes]
                                Eemt: [0 err_pkts][0.00 %]
                Actual   Stats Rcvd: [0 bytes][0.00 Mbit/sec]
                                     [0 pkts ][0.00 pkt/sec]
                                Send: [0 bytes][0.00 Mbit/sec]
```

```
                                    [0 pkts ][0.00 pkt/sec]
                                Esnd: [0 err_pkts][0.00 %]
                                Drop: [0 bytes][0.00 %]
                                    [0 pkts ][0.00 %]
                                Pthr: [0 bytes][0.00 %]
                                    [0 pkts ][0.00 %]
                                Emit: [0 bytes][0.00 Mbit/sec]
                                    [0 pkts ][0.00 pkt/sec]
                                Eemt: [0 err_pkts][0.00 %]
        Cluster #0 : IF 01-00.1 (01:00.1):
                Absolute Stats Rcvd: [127 pkts][19878 bytes][0 pkts dropped]
                                Send: [4873 pkts][507823 bytes]
                                Esnd: [0 err_pkts][0.00 %]
                                Drop: [0 pkts][0 bytes]
                                Pthr: [0 pkts][0 bytes]
                                Emit: [0 pkts][0 bytes]
                                Eemt: [0 err_pkts][0.00 %]
                Actual   Stats Rcvd: [0 bytes][0.00 Mbit/sec]
                                    [0 pkts ][0.00 pkt/sec]
                                Send: [0 bytes][0.00 Mbit/sec]
                                    [0 pkts ][0.00 pkt/sec]
                                Esnd: [0 err_pkts][0.00 %]
                                Drop: [0 bytes][0.00 %]
                                    [0 pkts ][0.00 %]
                                Pthr: [0 bytes][0.00 %]
                                    [0 pkts ][0.00 %]
                                Emit: [0 bytes][0.00 Mbit/sec]
                                    [0 pkts ][0.00 pkt/sec]
                                Eemt: [0 err_pkts][0.00 %]
          Cluster #0 : Aggregated Actual stats: [Captured 0.00
pkt/sec][Processed 0.00     pkt/sec][Send 0.00 pkt/sec]
```

`Absolute Stats Rcvd` — суммарная статистика принятых пакетов/байт, заблокированных пакетов на всех интерфейсах, с момента последнего перезапуска процесса fastDPI
[1+2=3 pkts dropped]
1 — потери на порту (даже не прочитали, буфер переполнен)
2 — не смог обработать СКАТ

Далее идет информация по каждому конкретному интерфейсу

`Cluster #0 : IF 01-00.0 (01:00.0)`:
`Absolute Stats` — полная статистика принятых пакетов/байт, заблокированных пакетов на интерфейсе `01-00.0`

- `Rcvd: [4873 pkts][507823 bytes][0 pkts dropped]` — принятые пакеты/байты
- `Send: [127 pkts][19878 bytes]` — переданные пакеты/байты
- `Esnd: [0 err_pkts][0.00 %]` — ошибки, возникшие при отправке пакетов
- `Drop: [0 pkts][0 bytes]` — дропнуто пакетов/байт, в результате работы фильтрации/полисинга и т.п. ("хорошие" дропы)
- `Pthr: [0 pkts][0 bytes]` — количество пакетов/байт, проходящих без анализа и обработки

- `Emit: [0 pkts][0 bytes]` — пакеты, которые сформировал CKAT
- `Eemt: [0 err_pkts][0.00 %]` — ошибки, возникшие при отправке пакетов, сформированных CKAT

`Actual Stats` — фактическая статистика принятых пакетов/байт, заблокированных пакетов на интерфейсе `01-00.0`
`Aggregated Actual stats` — совокупная статистика на кластер: сколько захвачено, обработано, отправлено пакетов/сек

```
[STAT    ][2022/04/08-16:25:25:309514] [HAL] DPDK device statistics:
        dev 01-00.0 (01:00.0)
             RX pkt/bytes abs (delta):            4873/390871          (0/0)
             TX pkt/bytes abs (delta):             127/16830           (0/0)
                Error pkts, abs/delta: rx_queue_full=0/0, bad_pkt=0/0,
tx_fail=0/0, rx_nombuf=0/0
        dev 01-00.1 (01:00.1)
             RX pkt/bytes abs (delta):             127/16830           (0/0)
             TX pkt/bytes abs (delta):            4873/390871          (0/0)
                Error pkts, abs/delta: rx_queue_full=0/0, bad_pkt=0/0,
tx_fail=0/0, rx_nombuf=0/0


[STAT    ][2022/04/08-16:25:25:309514] [HAL] DPDK device statistics:
        dev 01-00.0 (01:00.0)
             RX pkt/bytes abs (delta):            4873/390871          (0/0)
             TX pkt/bytes abs (delta):             127/16830           (0/0)
                Error pkts, abs/delta: rx_queue_full=0/0, bad_pkt=0/0,
tx_fail=0/0, rx_nombuf=0/0
        dev 01-00.1 (01:00.1)
             RX pkt/bytes abs (delta):             127/16830           (0/0)
             TX pkt/bytes abs (delta):            4873/390871          (0/0)
                Error pkts, abs/delta: rx_queue_full=0/0, bad_pkt=0/0,
tx_fail=0/0, rx_nombuf=0/0
[STAT    ][2022/04/08-16:25:25:309644]  [HAL][DPDK] Dispatcher statistics
abs/delta:
                         drop (worker queue full)           |  empty NIC RX
|       RX packets
        Cluster #0:               0/0           0.0%/  0.0% | 100.0%/100.0%
|            5000/0
```

Выше приведена статистика по интерфейсам:
`RX pkt/bytes abs (delta): 4873/390871 (0/0)` — принято пакетов/байт
`4873/390871` — с момента старта
`(0/0)` — за последние 15 сек (с момента последнего вывода в stat лог)

`TX pkt/bytes abs (delta):` — отправлено пакетов/байт

```
Error pkts, abs/delta: rx_queue_full=0/0, bad_pkt=0/0, tx_fail=0/0,
rx_nombuf=0/0
```

`rx_queue_full=0/0` — переполнение очереди диспетчера

bad_pkt=0/0 — плохие пакеты
tx_fail=0/0 — ошибки при отправке
rx_nombuf=0/0 — не хватило буфера на прием

drop (worker queue full) — нелегитимные дропы (переполнение обработчика)

empty NIC RX — процент холостых опросов rx-очередей карт — абсолютный процент (с начала работы CKAT) и относительный (дельта с последнего вывода в stat-лог). 100% — значит, входных пакетов нет, диспетчер работает вхолостую

```
[STAT    ][2022/04/08-16:25:25:309647] [HAL][DPDK/SQRX] Mempool state:
        cluster #0: avail_count=24448, in-use_count=8319
```

Использование пула памяти dpdk_mempool_size:
avail_count — доступно для использования
in-use_count — используется на текущий момент

На участке ниже представлена статистика по размерам пакетов, также добавлены диапазоны Jumbo Frames

```
[STAT    ][2022/04/08-16:25:25:309650] Packet size (abs/delta, in %):
                          <=64       <=128       <=256       <=512
<=1024      <=2048      <=4096      <=8192     >8192
        subs->inet:   0.5/0.0    98.7/0.0     0.6/0.0     0.2/0.0
0.0/0.0     0.0/0.0     0.0/0.0     0.0/0.0     0.0/0.0
        inet->subs:  17.3/0.0    51.2/0.0    25.2/0.0     6.3/0.0
0.0/0.0     0.0/0.0     0.0/0.0     0.0/0.0     0.0/0.0
```

Далее идет статистика по протоколам
Статистика по IP:
Тут указано количество потоков (flow) и информация по ним

```
[STAT    ][2022/04/08-16:25:25:309664] IPv4_Statistics 'flow nodes' :
        IPv4_thread_slave=#0 : 0/0/505/0/0 ( 180/0/325 ) ( 0-0/0-0/0-0/0-0 )
                0/0/66666/66666 ( 0/0 0/0 0/0/0 )
        IPv4_thread_slave=#1 : 0/0/1796/0/0 ( 436/0/1360 ) ( 0-0/0-0/0-0/0-0
)
                0/0/66666/66666 ( 0/0 0/0 0/0/0 )
    IPv4_total : allocate=616/4896000 ( 0/0/2301/0/0/0 ) ( 616/0/1685 ) (
0-0/0-0/0-0/0-0 )
                0/0/133332/133332 ( 0/0 0/0 0/0/0 )
        IPv4_actual: new=0 [0 flw/sec] close=0 [0 flw/sec] rei=0 [0 flw/sec]
```

IPv4_total : allocate=616/4896000 — показывает заполненность аллоцированной памяти для IPv4 flow
616 — занято, 4896000 — всего. Этот параметр задается в файле /etc/dpi/fastdpi.conf (mem_tracking_flow)

```
IPv4_actual: new=0 [0 flw/sec] close=0 [0 flw/sec] rei=0 [0 flw/sec]
```

new — количество новых flow

close — количество обработанных flow
rei — готово к переиспользованию

```
[STAT    ][2022/04/12-11:15:31:688997] IPv4_Statistics_error  :
        IPv4_ste_flow   : 0/0/0
        IPv4_ste_invlen : 0/0/0
```

IPv4_ste_flow — ошибки обработки flow. Это критичный счетчик. Должен быть нулевым (тут все хорошо)
IPv4_ste_invlen — ошибки прочитанных длин из входного фрейма (когда фактическая длина расходится с указанной в заголовке). Т.е. причина в пакете

0/0/0 — ip/tcp/udp

Статистика по блокировкам:
Эти параметры расписаны для каждого конкретного потока (thread_slave), а так же суммарное значение (Total)

```
[STAT    ][2022/04/12-11:15:31:688999] Detailed statistics on HTTP :
        thread_slave=0 :
                url/lock=28/0 ( 12,0,0 )( 1,1,0 )
                ssl/lock=191/0 ( 0,54,0 )( 1,17,16 )
                        cna/lock=4/0 ( 0,37 )
                        sni/lock=187/0 ( 0,17 )
                quic/lock=0/0 ( 1,0,0 )( 0,0,0 )
                chnprc=0
                ccheck/ip_check/lock=2203/579/0 0/0/0
        thread_slave=1 :
                url/lock=187/0 ( 1287,0,0 )( 1,1,0 )
                ssl/lock=268/2 ( 0,313,0 )( 2,36,34 )
                        cna/lock=1/0 ( 0,171 )
                        sni/lock=267/2 ( 0,142 )
                quic/lock=9/0 ( 0,0,0 )( 0,0,0 )
                chnprc=0
                ccheck/ip_check/lock=9404/747/0 0/0/0
        Total :
                url/lock=215/0 ( 1299,0,0 )( 2,2,0,98879 )
                ssl/lock=459/2 ( 0,367,0 )( 3,53,50,392183 )
                        cna/lock=5/0 ( 0,208 )
                        sni/lock=454/2 ( 0,159 )
                quic/lock=9/0 ( 1,0,0 )( 0,0,0,0 )
                chnprc=0
                ccheck/ip_check/lock=11607/1326/0 0/0/0
```

url/lock — проверено URL / заблокировано (аналогично для ssl, cna, sni, quic)
chnprc=0 — изменение парсера http ←→ https
ccheck/ip_check/lock=11607/1326/0 — статистика проверки по IP/порт

11607 — должны были выполнит проверку по IP
1326 — сколько раз реально выполнялась проверка
0 — заблокировано пакетов

Ниже указана статистика по фаерволу и syn пакетам:

```
[STAT    ][2022/04/12-11:15:31:689052] FRWL statistics : 0/0/0
[STAT    ][2022/04/12-11:15:31:689054] Statistics SYN :
        total : syn=1, syn_ack=1 (0/0/0/0 0/0)
        actual: syn=0 [0 syn/sec] syn_ack=0 [0 syn_ack/sec] [prcnt=0%]
(0/0/0/0 0/0)
[STAT    ][2022/04/12-11:15:31:689052] FRWL statistics : <wrap
hi>0/0/0</wrap>
[STAT    ][2022/04/12-11:15:31:689054] Statistics SYN :
        total : syn=1, syn_ack=1 (0/0/0/0 0/0)
        actual: syn=0 [0 syn/sec] syn_ack=0 [0 syn_ack/sec] [prcnt=0%]
(0/0/0/0 0/0)
```

`total : syn=1` — всего SYN пакетов
`syn_ack` — всего SYN-ACK пакетов
`actual:` — то же самое, только за последние 15 секунд (с момента последнего вывода в stat лог) + количество SYN/SYN-ACK в секунду