Содержание

fastdpi_stat.log

It is located in the folder: `/var/log/dpi/fastdpi_stat.log\\`. This log contains statistics on the traffic processed by SSG 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
```

This site has a stat log:
`[2022/04/07-13:36:24:608426]` — date and time of data capture

`'Virtual'/'Resident'` — memory type.
`Virtual` — virtual process size. Shows the total amount of memory that the program is able to address at a given time
`Resident` — shows how much physical memory the process uses.
This parameter is followed by specific values

`CPU statistics` — CPU utilization statistics
`cpu_total` — total CPU utilization
`cpu0`, `cpu1`, `cpu2`, `cpu3` — kernel-specific loading
`us` — how much is currently in use
`sy` — how much the system is currently using
`id` — how much is currently available
`wa` — shows the percentage of operations ready to be executed by the processor but pending from the disk

Interface information:

```
[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` — total statistics of received packets/bytes, blocked packets on all interfaces, since the last restart of the fastDPI process
[1+2=3 pkts dropped]
1 — losses on the port (not even read, buffer overflowed)
2 — SSG couldn't process

This is followed by information on each specific interface

`Cluster #0 : IF 01-00.0 (01:00.0)`:
`Absolute Stats` — full statistics of received packets/bytes, blocked packets on interface `01-00.0`

- `Rcvd: [4873 pkts][507823 bytes][0 pkts dropped]` — received packets/bytes
- `Send: [127 pkts][19878 bytes]` — packets/bytes transmitted
- `Esnd: [0 err_pkts][0.00 %]` — errors that occurred when sending packets
- `Drop: [0 pkts][0 bytes]` — dropped packets/bytes, as a result of filtering/policing, etc. (“good” drops)
- `Pthr: [0 pkts][0 bytes]` — number of packets/bytes passing without analysis and processing
- `Emit: [0 pkts][0 bytes]` — the packets that the SSG generated

- Eemt: [0 err_pkts][0.00 %] — errors occurred when sending SSG-generated packets

Actual Stats — actual statistics of received packets/bytes, blocked packets on interface 01-00.0
Aggregated Actual stats — aggregate statistics per cluster: how many packets captured, processed, sent/sec.

```
[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
```

Above are the statistics for the interfaces:
RX pkt/bytes abs (delta): 4873/390871 (0/0) — packets/byte received
4873/390871 — from the start
(0/0) — for the last 15 sec (since the last stat log output)

TX pkt/bytes abs (delta): — packets sent/byte

```
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 — dispatcher queue overflow
bad_pkt=0/0 — bad packages
tx_fail=0/0 — sending errors
rx_nombuf=0/0 — there wasn't enough buffer for reception

`drop (worker queue full)` — illegitimate drops (handler overflow)

`empty NIC RX` — percentage of idle polling of rx queues of cards - absolute percentage (since the beginning of SSG operation) and relative (delta since the last output to stat-log). 100% - means that there are no input packets, the dispatcher is idle

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

Memory Pool Utilization `dpdk_mempool_size`:
`avail_count` — available for use
`in-use_count` — currently in use

The plot below shows statistics on packet sizes, and Jumbo Frames ranges have also been added

```
[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
```

The following are statistics on protocols
IP statistics:
This shows the number of streams (flow) and information about them

```
[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` — shows allocated memory occupancy for IPv4 flow
616 — busy, 4896000 — total. This parameter is set in the total file. This parameter is set in the `/etc/dpi/fastdpi.conf` file (`mem_tracking_flow`)

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

new — number of new flows
`close` — flow rate
`rei` — ready for reuse

```
[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` — processing errors. This is a critical counter. It should be zero (everything is fine here)
`IPv4_ste_invlen` — errors of read lengths from the input frame (when the actual length diverges from the length specified in the header). I.e. the reason is in the package

`0/0/0` — ip/tcp/udp

Blocking statistics:
These parameters are scheduled for each specific thread (`thread_slave`), as well as the total value (`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` — URL checked / blocked (similar for ssl, cna, sni, quic)
`chnprc=0` — change parser http ←→ https
`ccheck/ip_check/lock=11607/1326/0` — IP/port check statistics

`11607` — should have run an IP check
`1326` — how many times the test was actually performed
`0` — blocked packets

Below are the statistics on firewall and syn packages:

```
[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` — total SYN packets
`syn_ack` — total SYN-ACK packets
`actual:` — the same, only for the last 15 seconds (since the last output to stat log) + number of SYN/SYN-ACK per second