- pmacct HCD
- nfacctd
- HCD
- «»

IP- «» — HCD (Hydra Collector Daemon). , .

- NetFlow v5 / sFlow **pmacct**. , NetFlow, `pmacct nfacctd`, , sFlow — `sfacctd`.
- (,).

pmacct HCD

, NetFlow sFlow, `pmacct` .

1. HCD .
2. `pmacct`:

```
user@server:~$ sudo aptitude update         \\
               sudo aptitude install pmacct
```

nfacctd

`/etc/pmacct/nfacctd.conf`, :

```
daemonize: true
pidfile: /var/run/hydra/hcd/nfacctd.pid
logfile: /var/log/hydra/hcd/nfacctd.log

nfacctd_ip: 127.0.0.1
nfacctd_port: 9992

aggregate[agg-ba]: src_net,src_mask,dst_host
aggregate[agg-ab]: src_host,dst_net,dst_mask

aggregate_filter[agg-ab]: src net 1.2.3.4/17 or src net 5.6.7.8/19
aggregate_filter[agg-ba]: dst net 1.2.3.4/17 or dst net 5.6.7.8/19

plugins: memory[agg-ba], memory[agg-ab]

imt_path[agg-ba]: /var/run/hydra/hcd/ipacc-agg-ba.pipe
imt_path[agg-ab]: /var/run/hydra/hcd/ipacc-agg-ab.pipe

networks_file: /etc/pmacct/networks.lst

refresh_maps: true
plugin_buffer_size: 50240
plugin_pipe_size: 50240000
imt_buckets: 65537
imt_mem_pools_size: 1024000
```

nfacctd_ip nfacctd_port, IP- (localhost) UDP-, NetFlow. , , .

, , -ab ( ) -ba ( ), «». , «» 2.1.15, agg.

aggregate_filter , NetFlow- , (ba) (ab) . , . 1.2.3.4/17 5.6.7.8/19. libpcap (tcpdump, wireshark . .). (.):

```
aggregate_filter[agg-ab]: src net X or src net Y ... or src net Z
```

, ... or src net ... ... or dst net ....

/etc/pmacct/networks.lst , :

```
!    ( )
1.2.3.4/17
5.6.7.8/19
```

CIDR-, .

, logfile, logrotate:

/etc/logrotate.d/nfacctd

```
/var/log/hydra/hcd/nfacctd.log {
    daily
    rotate 90
    delaycompress
    dateext
    missingok
    su hcd hcd
    postrotate
        /usr/bin/killall -HUP nfacctd
    endscript
}
```

nfacctd . HCD hcd. , /etc/pmacct .

nfacctd.

HCD

1. HCD, /etc/hydra/hcd/hcd.conf :

```
# For Netflow (nfacctd)
module current_statistics = on

# For custom statistics format
module external_statistics = off

#      «».
server id = 37301

# IP-  ,      hcd  XML-RPC  .
#       hcd     .
#  ,        (. )     .
server ip = 127.0.0.1
server port = 8888

#      XML-RPC   hcd
server login = hydra
server password = 123
```

module current_statistics module external_statistics .

2. HCD :

```
user@server:~$ sudo /etc/init.d/hcd run
```

, :

```
InstallSignalHandlers root INFO Installing signal handlers...
CreateXMLRPCServer root INFO Initializing XML-RPC server at 127.0.0.1:8888...
RunXMLRPCServer root INFO Starting XML-RPC server...
```

3. , nfacctd :

```
user@server:~$ sudo ps aux|grep nfacctd
hcd      16035  0.1  0.0  19740 12072 ?        S    May10  40:31 nfacctd: Core Process [default]
hcd      16081  0.0  0.0  23072 14552 ?        S    May10  26:23 nfacctd: IMT Plugin [agg-ba]
hcd      16082  0.0  0.0  20176 11644 ?        S    May10  26:50 nfacctd: IMT Plugin [agg-ab]
```

4. , Netflow- nfacctd :

```
user@server:~$ sudo tcpdump -i eth0 udp port 9992
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:06:27.965803 IP 90.151.176.22.23801 > 90.151.179.106.9992: UDP, length 1464
20:06:27.966830 IP 90.151.176.22.23801 > 90.151.179.106.9992: UDP, length 1464
20:06:27.966837 IP 90.151.176.22.23801 > 90.151.179.106.9992: UDP, length 1464
```

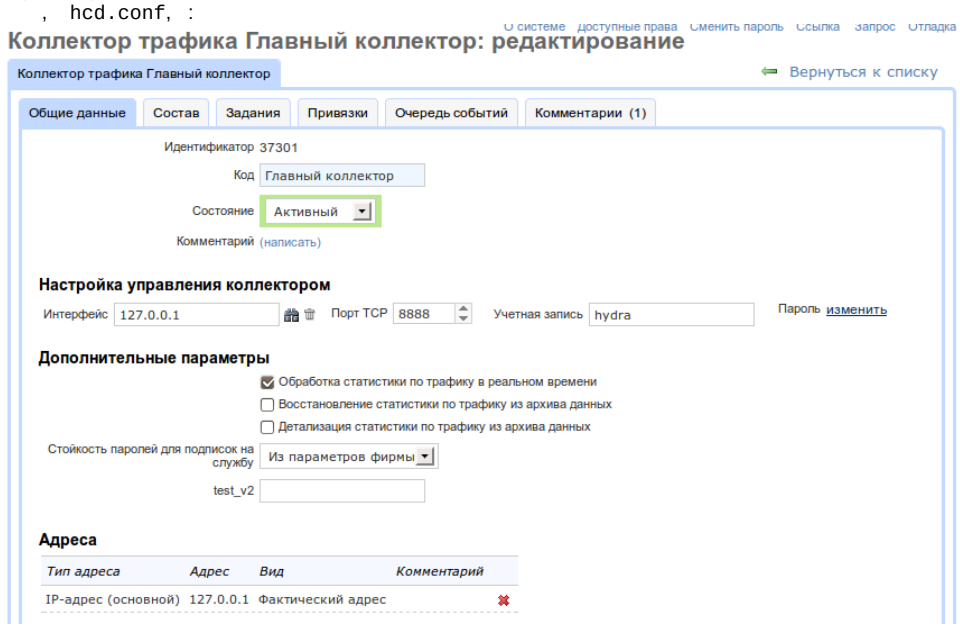
```
user@server:~$ /usr/bin/pmacct -s -p /var/run/hydra/hcd/ipacc-agg-ab.pipe | head
SRC_IP              DST_IP          DST_MASK  PACKETS  BYTES
90.151.179.157      0.0.0.0         0         186      18297
90.151.176.222      90.151.176.0    21        44       7788
10.5.9.12           10.0.0.0        8         2        463
90.151.176.107      0.0.0.0         0         513      239569
...
```

pmacct. , : SRC_IP DST_IP DST_MASK PACKETS BYTES

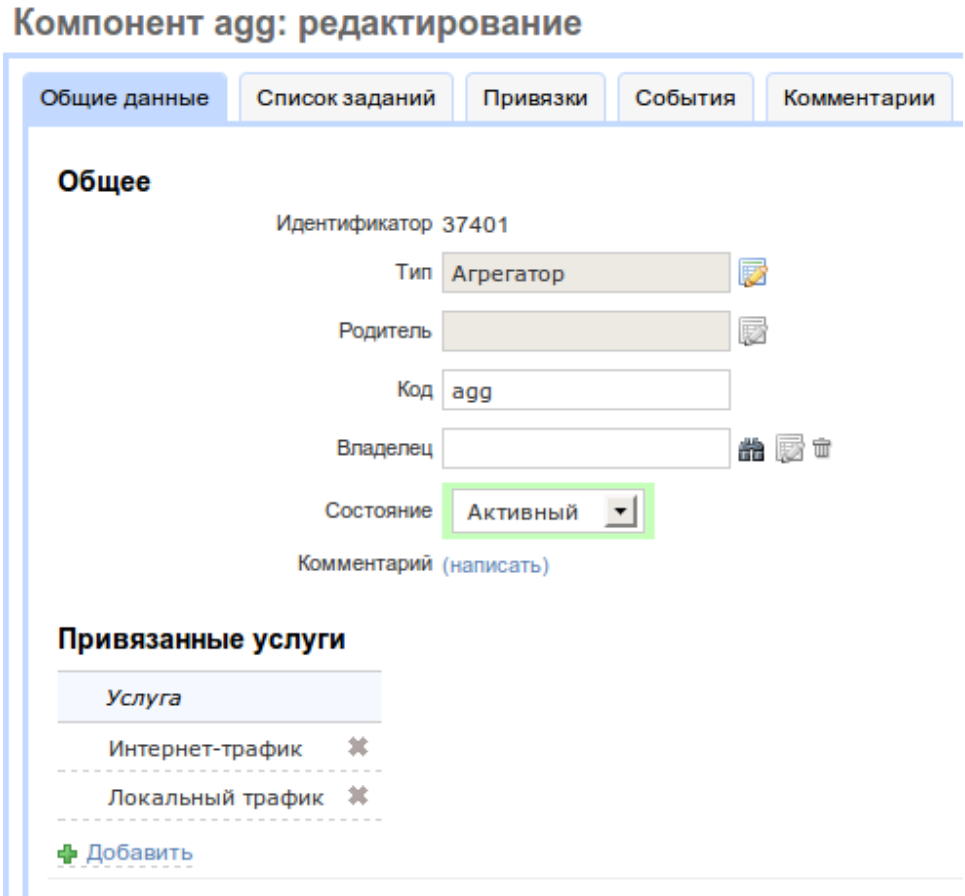
- , iptables.

«»

1. «».
2. (-> ->) . *Collector*.
3. , hcd.conf, :



4. . *agg*. , :



5. , , .
6. . , . « ».

1. «» (-> ->) /P- , 0. .
2. , HCD «» , , NTP 1 .
3. , :

- , (— «»), .
- .
- .
  - .
    - IP-/ (Netflow/sFlow).
- .
- " " " " . (/etc/pmacct/networks.lst).
- .
  - ( ) (— «») .
    - .
    - (, -., . ..).
      - .
- .
  - (->).
    - .
    - .

1. (-> ,). .
2. . , , .

:

- *TNS:no listener (TNS:).* HCD . .

1. «» (->).
2. :
   -
   - ()
   -
   - IP/ A
   - A
   - IP/ B
   - B
   -
   -
3. .
4. , :
   - *IP-* (. #).
   - / , .
   - .
   - .

hcd NetFlow/sFlow, , , Cisco SCE (RDR). **«»** , NetFlow, , 20-30 /. nfacctd NetFlow. flow-tools, NetFlow flow-report, HCD .

HCD

HCD , pmacct., hcd.conf :

```
module current_statistics = off
module external_statistics = on # (  )

# ...

aggregator autostart = off
aggregator autoattach = off
```

HCD CSV, — («;»). :

```
EXT_GOOD_ID;EXT_OBJECT_ID;D_BEGIN;D_END;ADDR_1/MASK_1;ADDR_2/MASK_2;BYTES
```

EXT_GOOD_ID	«»
EXT_OBJECT_ID	«»
D_BEGIN	(Unix timestamp, UTC)
D_END	(Unix timestamp, UTC)
ADDR_1/MASK_1	IP- () CIDR-. IP- 32
ADDR_2/MASK_2	IP- () CIDR-
BYTES	

:

```
39501;;1291242554;1291242554;10.5.10.6/32;0.0.0.0/0;900
```

, HCD— (, .), — (.).

EXT_OBJECT_ID EXT_GOOD_ID, ADDR_1/MASK_1 ADDR_2/MASK_2 . ID , , ( ), — IP-.

. *ADDR_2/MASK_2* "" . .

HCD hcdctl, . :

```
user@server:~$ hcdctl.py [OPTIONS] putfile <statistics name>
```

:

- -f < >
- -u http://user:password@host:port(HCD)

<statistics name> . (agg) -ab( ) -ba( ).

EXT_OBJECT_ID EXT_GOOD_ID, , , <statistics name> agg-ab. IP-(ADDR_1/MASK_1 ADDR_2/MASK_2), HCD — (agg-ab), — (agg-ba).

:

```
user@server:~$ hcdctl.py -f /tmp/stat-out.txt -u http://hydra:q123@127.0.0.1:8888 putfile agg-ab
user@server:~$ hcdctl.py -f /tmp/stat-in.txt -u http://hydra:q123@127.0.0.1:8888 putfile agg-ba
```

:

/var/log/hydra/hcd/nfacctd.log

```
WARN ( agg-print/print ): Unable to write data: try with a larger 'print_cache_entries' value.
```

/etc/pmacct/nfacctd.conf :

/etc/pmacct/nfacctd.conf

```
print_cache_entries[agg-ab]: 32771
```

agg-ab - , :

```
user@server:~$ sudo /etc/init.d/ncd stop
user@server:~$ sudo /etc/init.d/nfacct stop
user@server:~$ sudo /etc/init.d/hcd start
user@server:~$ sudo ps aux | grep nfacctd
```

.

HCD, , , netflow .

```
docker run -it --rm networkstatic/nflow-generator -t {  } -p 9992
```