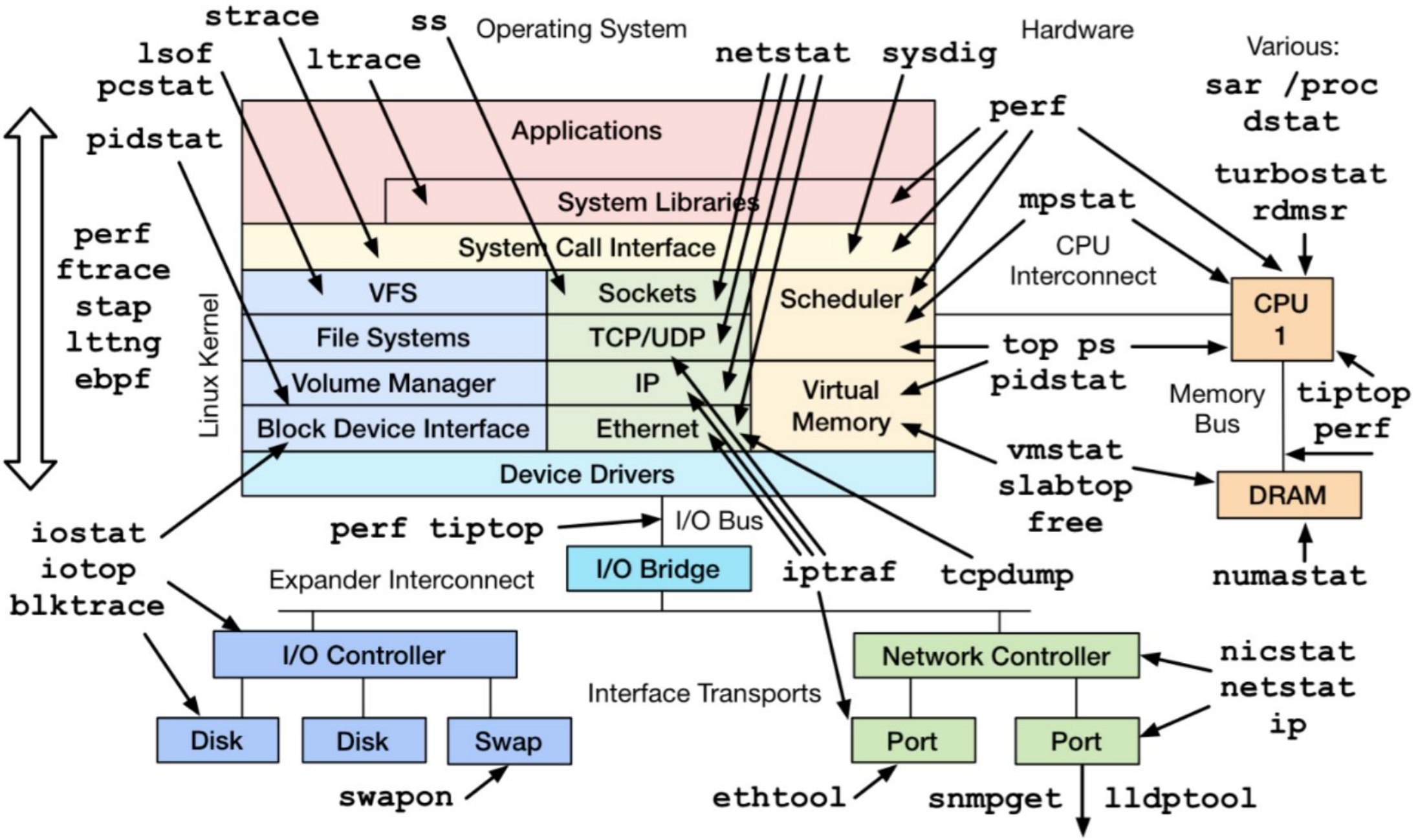
线上运维(工具篇)

何钦

2017/07/18


strace
ss
Operating System
Hardware
Various:
lsof
pcstat
ltrace
netstat
sysdig
sar /proc
dstat
perf
pidstat
Applications
System Libraries
turbostat
rdmsr
mpstat
perf
ftrace
stap
lttng
ebpf
System Call Interface
CPU
Interconnect
VFS
Sockets
Scheduler
CPU
1
Linux Kernel
File Systems
TCP/UDP
top ps
pidstat
Volume Manager
IP
Virtual
Memory
Memory
Bus
tiptop
perf
Block Device Interface
Ethernet
vmstat
slabtop
free
Device Drivers
DRAM
iostat
iotop
blktrace
perf tiptop
I/O Bus
I/O Bridge
iptraf
tcpdump
numastat
Expander Interconnect
I/O Controller
Network Controller
nicstat
netstat
ip
Interface Transports
Disk
Disk
Swap
Port
Port
swapon
ethtool
snmpget
lldptool

tcpdump

sudo tcpdump -w /tmp/a.cap -s 0 -i eth0 port 3000 and host 127.0.0.1

sudo tcpdump -r /tmp/a.cap -A port 61001 and host xx.xx.xx.xx

```
[heqin@engine-fps-coproxy00 ~]$ sudo tcpdump -w /tmp/fuck.cap port 61304 -s 0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C24584 packets captured
31111 packets received by filter
6362 packets dropped by kernel
[heqin@engine-fps-coproxy00 ~]$
```

tcpdump

一次短连接的交互过程

```
[root@kvm10563 ~]# tcpdump   port 9999 -i lo -nn -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes

17:56:34.491899 IP 127.0.0.1.43243 > 127.0.0.1.9999: Flags [S], seq 1869134814, win 32768, options [mss 16396,sackOK,TS val 3726666166 ecr 3726665921,nop,wscale 7], length 0
17:56:34.491926 IP 127.0.0.1.9999 > 127.0.0.1.43243: Flags [S.], seq 3025595832, ack 1869134815, win 32768, options [mss 16396,sackOK,TS val 3726666166 ecr 3726666166,nop,wscale 7
], length 0
17:56:34.491938 IP 127.0.0.1.43243 > 127.0.0.1.9999: Flags [.], ack 1, win 256, options [nop,nop,TS val 3726666166 ecr 3726666166], length 0
17:56:38.222643 IP 127.0.0.1.43243 > 127.0.0.1.9999: Flags [P.], seq 1:21, ack 1, win 256, options [nop,nop,TS val 3726669897 ecr 3726666166], length 20
17:56:38.222677 IP 127.0.0.1.9999 > 127.0.0.1.43243: Flags [.], ack 21, win 256, options [nop,nop,TS val 3726669897 ecr 3726669897], length 0
17:56:38.222778 IP 127.0.0.1.9999 > 127.0.0.1.43243: Flags [P.], seq 1:10, ack 21, win 256, options [nop,nop,TS val 3726669897 ecr 3726669897], length 9
17:56:38.222882 IP 127.0.0.1.43243 > 127.0.0.1.9999: Flags [.], ack 10, win 256, options [nop,nop,TS val 3726669897 ecr 3726669897], length 0
17:56:39.309721 IP 127.0.0.1.43243 > 127.0.0.1.9999: Flags [F.], seq 21, ack 10, win 256, options [nop,nop,TS val 3726670984 ecr 3726669897], length 0
17:56:39.309832 IP 127.0.0.1.9999 > 127.0.0.1.43243: Flags [F.], seq 10, ack 22, win 256, options [nop,nop,TS val 3726670984 ecr 3726670984], length 0
17:56:39.309850 IP 127.0.0.1.43243 > 127.0.0.1.9999: Flags [.], ack 11, win 256, options [nop,nop,TS val 3726670984 ecr 3726670984], length 0
```

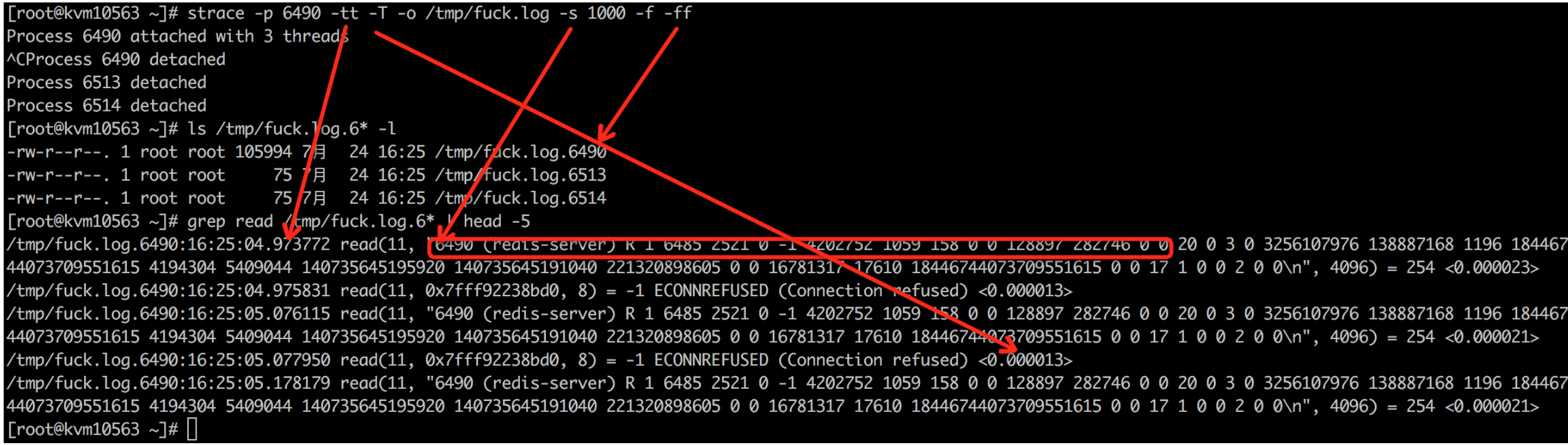
```
[root@kvm10563 ~]# tcpdump   port 9999 -i lo -nn -n -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes

17:59:21.741982 IP 127.0.0.1.58507 > 127.0.0.1.9999: Flags [S], seq 226574049, win 32768, options [mss 16396,sackOK,TS val 3726833416 ecr 3726833300,nop,wscale 7], length 0
.>..............@....'.
."..."......
17:59:21.742011 IP 127.0.0.1.9999 > 127.0.0.1.58507: Flags [S.], seq 1342967181, ack 226574050, win 32768, options [mss 16396,sackOK,TS val 3726833416 ecr 3726833416,nop,wscale 7]
, length 0
.>...../.....@......'...P.
."..."......
17:59:21.742024 IP 127.0.0.1.58507 > 127.0.0.1.9999: Flags [.], ack 1, win 256, options [nop,nop,TS val 3726833416 ecr 3726833416], length 0
.....................'.
."..."..
17:59:24.097653 IP 127.0.0.1.58507 > 127.0.0.1.9999: Flags [P.], seq 1:23, ack 1, win 256, options [nop,nop,TS val 3726835772 ecr 3726833416], length 22
......>..............'.
.#.<."..*2
$3
get
$3
abc

17:59:24.097694 IP 127.0.0.1.9999 > 127.0.0.1.58507: Flags [.], ack 23, win 256, options [nop,nop,TS val 3726835772 ecr 3726835772], length 0
.>......M..........'...P.
.#.<.#.<
17:59:24.097771 IP 127.0.0.1.9999 > 127.0.0.1.58507: Flags [P.], seq 1:6, ack 23, win 256, options [nop,nop,TS val 3726835772 ecr 3726835772], length 5
.>......-..........'...P.
.#.<.#.<$-1

17:59:24.097847 IP 127.0.0.1.58507 > 127.0.0.1.9999: Flags [.], ack 6, win 256, options [nop,nop,TS val 3726835772 ecr 3726835772], length 0
......H.............'.
.#.<.#.<
17:59:25.709642 IP 127.0.0.1.58507 > 127.0.0.1.9999: Flags [F.], seq 23, ack 6, win 256, options [nop,nop,TS val 3726837384 ecr 3726835772], length 0
.....................'.
.#...#.<
17:59:25.710041 IP 127.0.0.1.9999 > 127.0.0.1.58507: Flags [F.], seq 6, ack 24, win 256, options [nop,nop,TS val 3726837384 ecr 3726837384], length 0
.>.................'...P.
.#...#..
17:59:25.710061 IP 127.0.0.1.58507 > 127.0.0.1.9999: Flags [.], ack 7, win 256, options [nop,nop,TS val 3726837384 ecr 3726837384], length 0
.....................'.
.#...#..
```

```
18:00:48.742915 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.60162: Flags [P.], seq 1957502292:1957502365, ack 3212646603, win 227, options
[nop,nop,TS val 4060638954 ecr 4068029952], length 73
18:00:48.754394 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [.], ack 1611, win 1424, options [nop,nop,TS val 4068029963 ecr 40
60638965], length 0
18:00:48.754398 IP engine-fps-coproxy01.ys.diditaxi.com.60162 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [.], ack 977, win 6248, options [nop,nop,TS val 4068029963 ecr 406
0638965], length 0
18:00:48.754914 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 5968:6086, ack 1611, win 1424, options [nop,nop,TS val 4
068029964 ecr 4060638965], length 118
18:00:48.754938 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.61304: Flags [P.], seq 1611:1646, ack 6086, win 8555, options [nop,nop,TS val 4
060638966 ecr 4068029964], length 35
18:00:48.755385 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6086:6204, ack 1646, win 1424, options [nop,nop,TS val 4
068029964 ecr 4060638966], length 118
18:00:48.755420 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6204:6295, ack 1646, win 1424, options [nop,nop,TS val 4
068029964 ecr 4060638966], length 91
18:00:48.755425 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6295:6413, ack 1646, win 1424, options [nop,nop,TS val 4
068029964 ecr 4060638966], length 118
18:00:48.755444 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.61304: Flags [.], ack 6413, win 8555, options [nop,nop,TS val 4060638966 ecr 40
68029964], length 0
18:00:48.755468 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.61304: Flags [P.], seq 1646:1740, ack 6413, win 8555, options [nop,nop,TS val 4
060638966 ecr 4068029964], length 94
18:00:48.755541 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6413:6531, ack 1740, win 1424, options [nop,nop,TS val 4
068029964 ecr 4060638966], length 118
18:00:48.755587 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.61304: Flags [P.], seq 1740:1775, ack 6531, win 8555, options [nop,nop,TS val 4
060638966 ecr 4068029964], length 35
18:00:48.755679 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6531:6639, ack 1775, win 1424, options [nop,nop,TS val 4
068029965 ecr 4060638966], length 108
18:00:48.755732 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.61304: Flags [P.], seq 1775:1780, ack 6639, win 8555, options [nop,nop,TS val 4
060638966 ecr 4068029965], length 5
18:00:48.755736 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.60162: Flags [P.], seq 977:1085, ack 1, win 227, options [nop,nop,TS val 406063
8966 ecr 4068029963], length 108
18:00:48.755863 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6639:6757, ack 1780, win 1424, options [nop,nop,TS val 4
068029965 ecr 4060638966], length 118
18:00:48.755894 IP engine-fps-coproxy00.ys.diditaxi.com.6016 > engine-fps-coproxy01.ys.diditaxi.com.61304: Flags [P.], seq 1780:1815, ack 6757, win 8555, options [nop,nop,TS val 4
060638967 ecr 4068029965], length 35
18:00:48.755964 IP engine-fps-coproxy01.ys.diditaxi.com.61304 > engine-fps-coproxy00.ys.diditaxi.com.6016: Flags [P.], seq 6757:6848, ack 1815, win 1424, options [nop,nop,TS val 4
```

strace

sudo strace -p pid -o /tmp/fuck.log -f -ff -t -TT -s 1000

sudo strace -s 100 -o /tmp/fuck.log ./a.out ...(如果a.out是后台进程， 需要手动kill a.out)



lsof

sudo lsof -p pid -P -n

sudo lsof -i:8080

```
[root@kvm10563 ~]# lsof -i:8080
COMMAND  PID   USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
nginx   8564   root    6u  IPv4 1476691809      0t0  TCP *:webcache (LISTEN)
nginx   8565 nobody    6u  IPv4 1476691809      0t0  TCP *:webcache (LISTEN)
[root@kvm10563 ~]#
```

```
[root@kvm10563 ~]# lsof -p 6490  -P -n
COMMAND    PID USER   FD   TYPE     DEVICE SIZE/OFF    NODE NAME
redis-ser 6490 root  cwd    DIR      252,3     4096 3028169 /root/work/didiredis3.2.8
redis-ser 6490 root  rtd    DIR      252,3     4096       2 /
redis-ser 6490 root  txt    REG      252,3  4755519 3028600 /root/work/didiredis3.2.8/src/redis-server
redis-ser 6490 root  mem    REG      252,3   157072 2097380 /lib64/ld-2.12.so
redis-ser 6490 root  mem    REG      252,3  1928936 2097591 /lib64/libc-2.12.so
redis-ser 6490 root  mem    REG      252,3   599480 2097629 /lib64/libm-2.12.so
redis-ser 6490 root  mem    REG      252,3   145936 2097610 /lib64/libpthread-2.12.so
redis-ser 6490 root  mem    REG      252,3    22536 2129303 /lib64/libdl-2.12.so
redis-ser 6490 root  mem    REG      252,3 99164480 4064503 /usr/lib/locale/locale-archive
redis-ser 6490 root    0r   CHR        1,3      0t0    3788 /dev/null
redis-ser 6490 root    1w   REG      252,3     3627 3028624 /root/work/didiredis3.2.8/7001/fucklog
redis-ser 6490 root    2w   REG      252,3     3627 3028624 /root/work/didiredis3.2.8/7001/fucklog
redis-ser 6490 root    3u   REG        0,9        0    3786 [eventpoll]
redis-ser 6490 root    4u  IPv6 1483392465      0t0     TCP *:7001 (LISTEN)
redis-ser 6490 root    5u  IPv4 1483392467      0t0     TCP *:7001 (LISTEN)
redis-ser 6490 root    6w   REG      252,3       80 3028609 /root/work/didiredis3.2.8/appendonly.aof (deleted)
redis-ser 6490 root    7wW  REG      252,3     1186 3028628 /root/work/didiredis3.2.8/7001/nodes.conf
redis-ser 6490 root    8u  IPv6 1483392503      0t0     TCP *:17001 (LISTEN)
redis-ser 6490 root    9u  IPv4 1483392507      0t0     TCP *:17001 (LISTEN)
redis-ser 6490 root   10u  IPv4 1537377038      0t0     TCP 127.0.0.1:7001->127.0.0.1:41843 (ESTABLISHED)
redis-ser 6490 root   12u  IPv4 1483392811      0t0     TCP 127.0.0.1:17001->127.0.0.1:52913 (ESTABLISHED)
redis-ser 6490 root   13u  IPv4 1483392814      0t0     TCP 127.0.0.1:52446->127.0.0.1:17003 (ESTABLISHED)
redis-ser 6490 root   14u  IPv4 1483392816      0t0     TCP 127.0.0.1:51245->127.0.0.1:17002 (ESTABLISHED)
redis-ser 6490 root   15u  IPv4 1483392828      0t0     TCP 127.0.0.1:17001->127.0.0.1:52917 (ESTABLISHED)
redis-ser 6490 root   16u  IPv4 1483392848      0t0     TCP 127.0.0.1:54060->127.0.0.1:17004 (ESTABLISHED)
```

lsof

```
FD is followed by one of these characters, describing the mode under which the file is open:

     r for read access;
     w for write access;
     u for read and write access;
     space if mode unknown and no lock
          character follows;
     '-' if mode unknown and lock
          character follows.

The mode character is followed by one of these lock characters, describing the type of lock applied to the file:

     N for a Solaris NFS lock of unknown type;
     r for read lock on part of the file;
     R for a read lock on the entire file;
     w for a write lock on part of the file;
     W for a write lock on the entire file;
     u for a read and write lock of any length;
     U for a lock of unknown type;
     x for an SCO OpenServer Xenix lock on part      of the file;
     X for an SCO OpenServer Xenix lock on the      entire file;
     space if there is no lock.
```

关于/proc/

/proc/interrupts

/proc/swaps

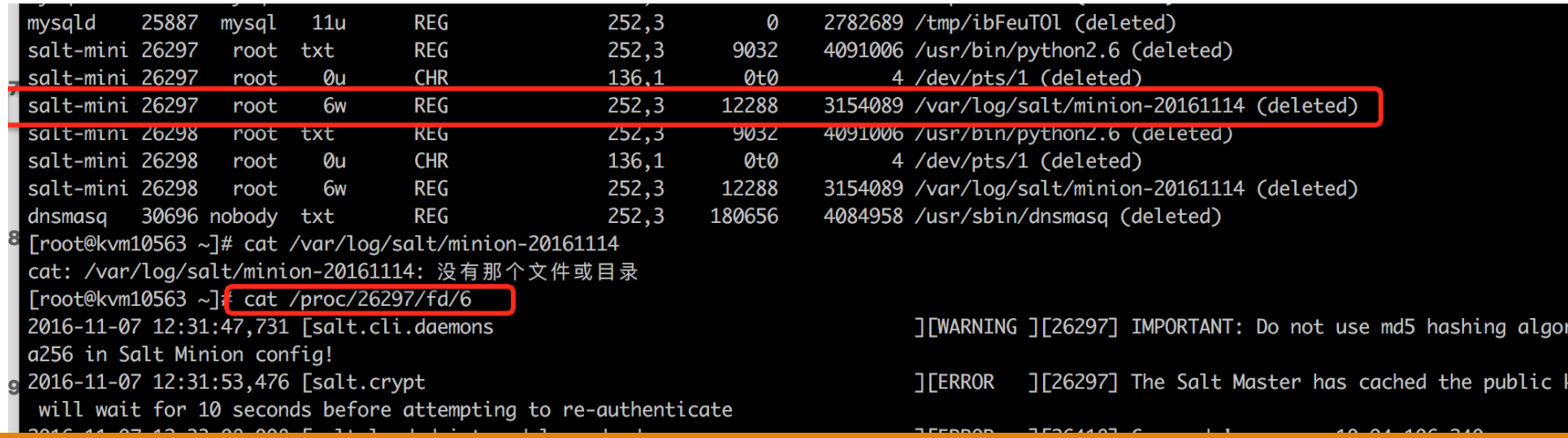
/proc/{pid}/limites

/proc/{pid}/smaps（内存泄漏？）

/proc/{pid}/cwd

/proc/{pid}/fd/{fd}

关于deleted？



pidof

```
[heqin@engine-fps-coproxy00 ~]$ pidof redis-server
35935 35741 35554 35291 35105 34901 34714 34494 34243 34040 33812 33514 33265 33062 32856 32662 32476 32210 32014 31820 31634 31371 31185 30973 30786 30566 30380 30112 29926 29726
 29539 29284
[heqin@engine-fps-coproxy00 ~]$
```

```
readlink("/proc/19576/exe", "/sbin/mingetty (deleted)", 4096) = 24
readlink("/proc/19657/exe", 0x7b7d80, 4096) = -1 ENOENT (No such file or directory)
readlink("/proc/19810/exe", "/root/goroot_online/src/github.com/foundation/didiredis2.8.13/src/redis-server (deleted)", 4096) = 88
readlink("/proc/20189/exe", "/usr/sbin/sshd", 4096) = 14
readlink("/proc/20192/exe", "/bin/bash", 4096) = 9
readlink("/proc/20995/exe", "/usr/bin/vim", 4096) = 12
readlink("/proc/21294/exe", "/usr/sbin/ntpd", 4096) = 14
readlink("/proc/22404/exe", "/root/work/fusion/fusion.r2/output/bin/r2", 4096) = 41
readlink("/proc/22668/exe", "/root/work/fusion/fusion.r2/output/bin/r2", 4096) = 41
readlink("/proc/23309/exe", "/usr/bin/vim", 4096) = 12
readlink("/proc/23317/exe", "/bin/sleep", 4096) = 10
readlink("/proc/23321/exe", "/usr/bin/strace", 4096) = 15
readlink("/proc/23324/exe", "/sbin/killall5", 4096) = 14
readlink("/proc/23717/exe", "/usr/bin/python", 4096) = 15
readlink("/proc/25779/exe", "/bin/bash", 4096) = 9
readlink("/proc/25887/exe", "/usr/libexec/mysqld", 4096) = 19
readlink("/proc/26297/exe", "/usr/bin/python2.6 (deleted)", 4096) = 28
readlink("/proc/26298/exe", "/usr/bin/python2.6 (deleted)", 4096) = 28
readlink("/proc/26962/exe", "/root/goroot_online/src/github.com/foundation/didiredis2.8.13/src/redis-server", 4096) = 78
readlink("/proc/29855/exe", "/sbin/udevd", 4096) = 11
readlink("/proc/30653/exe", "/usr/sbin/libvirtd", 4096) = 18
readlink("/proc/30696/exe", "/usr/sbin/dnsmasq (deleted)", 4096) = 27
readlink("/proc/32108/exe", "/usr/sbin/httpd", 4096) = 15
26962 19810 16473 14085 6498 6497 6496 6495 6494 6493 6492 6491 6490 3274
+++ exited with 0 +++
[root@kvm10563 ~]# strace -e readlink -s 1000 pidof redis-server
```

tr

tr \ ,

tr -d ,

```
[heqin@engine-fps-coproxy00 ~]$ pidof redis-server | tr \  ,
35935,35741,35554,35291,35105,34901,34714,34494,34243,34040,33812,33514,33265,33062,32856,32662,32476,32210,32014,31820,31634,31371,31185,30973,30786,30566,30380,30112,29926,29726
,29539,29284
[heqin@engine-fps-coproxy00 ~]$ pidof redis-server | tr \  , | tr -d ,
359353574135554352913510534901347143449434243340403381233514332653306232856326623247632210320143182031634313713118530973307863056630380301122992629726295392 84
[heqin@engine-fps-coproxy00 ~]$
```

awk

substr

length

~/xx/

NF/NR/FNR

getline

-F

-v k=v

BEGIN/ END

```
[root@kvm10563 ~]# cat key.txt
1,张三
2,李四
[root@kvm10563 ~]# cat test.txt
1,100
2,200
[root@kvm10563 ~]# awk -F,  '{if(NR==FNR) key[$1]=$2; else print key[$1],$2}' key.txt test.txt
张三 100
李四 200
[root@kvm10563 ~]#
```

sed

sed -n '1,4'p file

sed -n '/abc/,/def/'p file

sed -i 's/abc/def/'g file

```
[heqin@gs-gsspam-coproxy07 ~]$ sudo tcpdump -r /tmp/a.cap   -nn -n -A | head -30
reading from file /tmp/a.cap, link-type EN10MB (Ethernet)
16:59:43.439541 IP 100.70.140.59.3000 > 100.69.195.53.59697: Flags [P.], seq 3174425767:3174425775, ack 3840296549, win 1453, options [nop,nop,TS val 1058388832 ecr 1626765525], len
gth 8
E..<y...@..
dF.;dE.5...1.5....Fe.....+.....
?..``.x.:30384

16:59:43.439542 IP 100.69.171.30.53863 > 100.70.140.59.3000: Flags [.], ack 556888364, win 6152, options [nop,nop,TS val 3215124977 ecr 1058388832], length 0
E`.4....=.N.dE..dF.;.g..v...!1q,....J......
....?..`
16:59:43.439546 IP 100.70.140.59.3000 > 100.69.64.61.31185: Flags [P.], seq 4281274209:4281274216, ack 306257437, win 1453, options [nop,nop,TS val 1058388832 ecr 3217526738], lengt
h 7
E..;F...@...dF.;dE@=..y../.a.A.......1.....
?..`....:4200

16:59:43.439551 IP 100.70.140.59.3000 > 100.69.195.53.59697: Flags [P.], seq 8:12, ack 1, win 1453, options [nop,nop,TS val 1058388832 ecr 1626765525], length 4
dF.;dE.5...1.5....Fe.....'.....
?..``.x.:1

16:59:43.439555 IP 100.69.65.32.52155 > 100.70.140.59.3000: Flags [P.], seq 867077901:867078057, ack 2209792693, win 6152, options [nop,nop,TS val 3217310860 ecr 1058388831], length
 156
........5...... dF.;....3..
..D.?.._*3
$6
APPEND
$31
loclist_0_390
16:59:43.439559 IP 100.70.140.59.3000 > 100.69.64.61.31185: Flags [P.], seq 7:11, ack 1, win 1453, options [nop,nop,TS val 1058388832 ecr 3217526738], length 4
E..8F...@...dF.;dE@=..y../.h.A.............
?..`....:1

16:59:43.439570 IP 100.69.190.37.51104 > 100.70.140.59.3000: Flags [P.], seq 1225667993:1225668149, ack 3144416710, win 501, options [nop,nop,TS val 2041903234 ecr 1058388831], leng
th 156
E`..Pm..=..odE.%dF.;....I.5..k.......<.....
y...?.._*3
[heqin@gs-gsspam-coproxy07 ~]$ sudo tcpdump -r /tmp/a.cap   -nn -n -A  | awk '{if ($0~/\ >\ .*\[P/) {if($5~/\.3000:/) {s[$3":"]=$1;lastkey=$3":";} else {print $1 " " s[$5], op[$5];}
;} if(substr($0,0,1) == "$"&&lastkey!=""){getline;op[lastkey]=$0;lastkey="";} }'  | tail -10
reading from file /tmp/a.cap, link-type EN10MB (Ethernet)
16:59:44.269044 16:59:44.268894 APPEND
16:59:44.269054 16:59:44.268933 APPEND
16:59:44.269056 16:59:44.268891 APPEND
16:59:44.269057 16:59:44.268879 APPEND
```

cut

cut -d, -f1-5

cut -d\ -f1,3

有时候不想数（适合简单的格式）： cat xx.log | head -1 | tr \ \\n | cat -vn

cat xx.log | cut -d\ -f11

echo（好看点）

-n 不加换行

-e 转义支持

```
heqin@op-sven-opsec00.gz01:~$ ifind -s gztest | while read i; do echo -ne $(date)"\t"; dssh -n $i "hostname;"; done

We get [4] results with query gztest
Mon Jul 31 17:25:41 CST 2017    fd-gztest-coproxy01.gz01
Mon Jul 31 17:25:41 CST 2017    fd-gztest-rds00.gz01
Mon Jul 31 17:25:42 CST 2017    fd-gztest-coproxy00.gz01
Mon Jul 31 17:25:42 CST 2017    fd-gztest-rds01.gz01
heqin@op-sven-opsec00.gz01:~$
```

sort + uniq

sort -n -t, -kxx,xx

uniq -c

```
[root@kvm10563 ~]# cat fuck | sort -t, -k2 -k1
4,aaa,3
1,aaa,5
2,bbb,1
[root@kvm10563 ~]# cat fuck | sort -t, -k2,2 -k1
1,aaa,5
4,aaa,3
2,bbb,1
[root@kvm10563 ~]# cat fuck | sort -t, -k2,2 -k1,1
1,aaa,5
4,aaa,3
2,bbb,1
```

top

-u user

-p pid,pid,pid

-H

zx <> 就是好看

-b -d 1 > /tmp/fuck

iotop

sudo iotop -t -d 1 -b -o

```
12:11:23  8873 be/4 xiaoju      0.00 B/s    7.48 K/s  0.00 %  0.09 % consul agent -config-file client.json
^C[heqin@fd-codis-dash00 ~]$ sudo iotop  -t -d 1 -b -o
Total DISK READ: 0.00 B/s | Total DISK WRITE: 0.00 B/s
    TIME  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN      IO    COMMAND
Total DISK READ: 0.00 B/s | Total DISK WRITE: 18.72 K/s
    TIME  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN      IO    COMMAND
13:28:21 24812 be/4 root        0.00 B/s   11.23 K/s  0.00 %  0.01 % ./didi-odin-super-agent -c product.cfg
13:28:21  5966 be/4 root        0.00 B/s    7.49 K/s  0.00 %  0.00 % sap1002
Total DISK READ: 0.00 B/s | Total DISK WRITE: 409.72 K/s
    TIME  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN      IO    COMMAND
13:28:23  2081 be/3 root        0.00 B/s  372.47 K/s  0.00 %  0.02 % [jbd2/sda2-8]
13:28:23  8826 be/4 xiaoju      0.00 B/s    3.72 K/s  0.00 %  0.00 % consul agent -config-file client.json
13:28:23 19833 be/4 root        0.00 B/s    3.72 K/s  0.00 %  0.00 % odin-agent start -f /etc/odin-agent.conf
13:28:23  4301 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % ./didi-odin-deploy-agent -c product.cfg
13:28:23  4941 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % ./didi-odin-deploy-agent -c product.cfg
13:28:23  4766 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % ./didi-odin-deploy-agent -c product.cfg
13:28:23  4917 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % ./didi-odin-deploy-agent -c product.cfg
Total DISK READ: 0.00 B/s | Total DISK WRITE: 0.00 B/s
    TIME  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN      IO    COMMAND
```

mpstat

```
[heqin@fd-codis-dash00 ~]$ mpstat -P ALL 1
Linux 2.6.32-573.18.1.el6.toav2.x86_64 (fd-codis-dash00.gz01)   08/04/2017      _x86_64_        (48 CPU)

01:29:59 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
01:30:00 PM  all    0.08    0.00    0.04    0.00    0.00    0.00    0.00    0.00   99.87
01:30:00 PM    0    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    1    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    2    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    3    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    4    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    5    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    6    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    7    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM    8    0.99    0.00    0.99    0.00    0.00    0.00    0.00    0.00   98.02
01:30:00 PM    9    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   10    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   11    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   16    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
01:30:00 PM   17    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```

grep

egrep -o '[0-9]*.[0-9]*.[0-9]*.[0-9]*'

-A 1

-B 2

-C 3

-i

-I(ai)

-l (le)

paste

paste a b

perf

sudo perf top

sudo perf top -p pid -g

sudo perf record ls -g

sudo perf report -i perf.data

```
Samples: 639K of event 'cycles', Event count (approx.): 75087909404
+   25.74%     0.26%  [kernel]                  [k] cpuidle_idle_call
+   21.04%     0.02%  [kernel]                  [k] system_call_fastpath
+   18.02%     0.09%  [kernel]                  [k] irq_exit
+   18.02%     0.06%  [kernel]                  [k] ret_from_intr
+   17.94%     0.09%  [kernel]                  [k] do_IRQ
+   16.37%     0.14%  [kernel]                  [k] do_softirq
+   16.30%     0.06%  [kernel]                  [k] call_softirq
+   16.18%     0.21%  [kernel]                  [k] __do_softirq
+   14.26%     0.91%  [kernel]                  [k] net_rx_action
-   12.31%     1.11%  [kernel]                  [k] ixgbe_poll
   - ixgbe_poll
      - 99.86% net_rx_action
           __do_softirq
           call_softirq
+   10.30%     0.04%  perf                      [.] hist_entry_iter__add
+    9.88%     0.71%  [kernel]                  [k] ixgbe_clean_rx_irq
+    9.45%     0.00%  perf                      [.] 0x0000000000032050
+    9.18%     0.00%  perf                      [.] cmd_top
+    8.56%     0.04%  [kernel]                  [k] napi_gro_receive
+    8.18%     0.05%  [kernel]                  [k] napi_skb_finish
+    8.18%     0.26%  libc-2.12.so              [.] epoll_wait
+    8.14%     0.04%  [kernel]                  [k] netif_receive_skb
+    7.99%     0.18%  [kernel]                  [k] __netif_receive_skb
+    7.35%     0.13%  [kernel]                  [k] ip_rcv
+    7.24%     0.05%  [kernel]                  [k] sys_epoll_wait
+    7.21%     0.06%  [kernel]                  [k] ip_rcv_finish
+    7.01%     0.27%  [kernel]                  [k] ep_poll
+    6.73%     0.02%  [kernel]                  [k] ip_local_deliver
+    6.71%     0.08%  [kernel]                  [k] ip_local_deliver_finish
+    6.63%     0.03%  libpthread-2.12.so        [.] 0x000000000000e77d
+    6.61%     0.25%  [kernel]                  [k] tcp_v4_rcv
+    6.54%     0.02%  [kernel]                  [k] sys_write
+    6.45%     0.11%  [kernel]                  [k] vfs_write
+    6.27%     0.04%  [kernel]                  [k] do_sync_write
```

go tool

go tool pprof http://127.0.0.1:13000/debug/pprof/heap

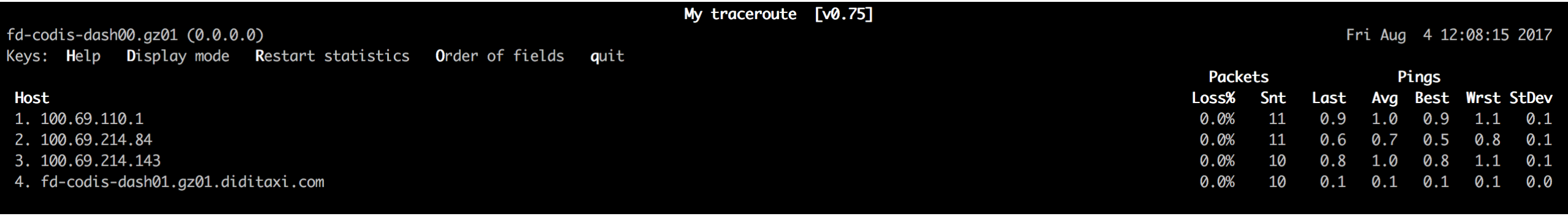
```
Server response: 404 Not Found
[heqin@fd-codis-dash00 ~]$ go tool pprof http://gs-apicachegz-coproxy02.gz01:13000/debug/pprof/heap
Fetching profile from http://gs-apicachegz-coproxy02.gz01:13000/debug/pprof/heap
Saved profile in /home/odin/heqin/pprof/pprof.gs-apicachegz-coproxy02.gz01:13000.inuse_objects.inuse_space.001.pb.gz
Entering interactive mode (type "help" for commands)
(pprof) top
480.82MB of 493.51MB total (97.43%)
Dropped 366 nodes (cum <= 2.47MB)
Showing top 10 nodes out of 42 (cum >= 158.74MB)
      flat  flat%   sum%        cum   cum%
  351.56MB 71.24% 71.24%   351.56MB 71.24%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/redis.NewConnSize
   28.62MB  5.80% 77.04%   155.18MB 31.44%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/router.(*BackendConn).newBackendReader
   27.19MB  5.51% 82.55%    27.19MB  5.51%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/backup.NewWorker
   20.75MB  4.21% 86.75%    20.75MB  4.21%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/backup.(*Worker).loopWriter
   15.66MB  3.17% 89.93%    15.66MB  3.17%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/router.NewBackendConn
      10MB  2.03% 91.95%       10MB  2.03%  go.intra.xiaojukeji.com/foundation/didicodis2.0/vendor/github.com/wandoulabs/go-zookeeper/zk.(*Conn).recvLoop
      10MB  2.03% 93.98%       10MB  2.03%  go.intra.xiaojukeji.com/foundation/didicodis2.0/vendor/github.com/wandoulabs/go-zookeeper/zk.(*Conn).sendLoop
    7.89MB  1.60% 95.58%     7.89MB  1.60%  go.intra.xiaojukeji.com/foundation/didicodis2.0/vendor/go.intra.xiaojukeji.com/golang/dlog.NewSyslogBackend
    5.58MB  1.13% 96.71%     7.58MB  1.54%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/redis.init.1
    3.55MB  0.72% 97.43%   158.74MB 32.16%  go.intra.xiaojukeji.com/foundation/didicodis2.0/pkg/proxy/router.(*BackendConn).loopWriter
(pprof) quit
[heqin@fd-codis-dash00 ~]$
```

curl

curl http://gs-apicachegz-coproxy02.gz01:13000/debug/vars -s | python -m json.tool

mtr

sudo mtr 10.1.1.1



netstat

netstat -nat -p(sudo)

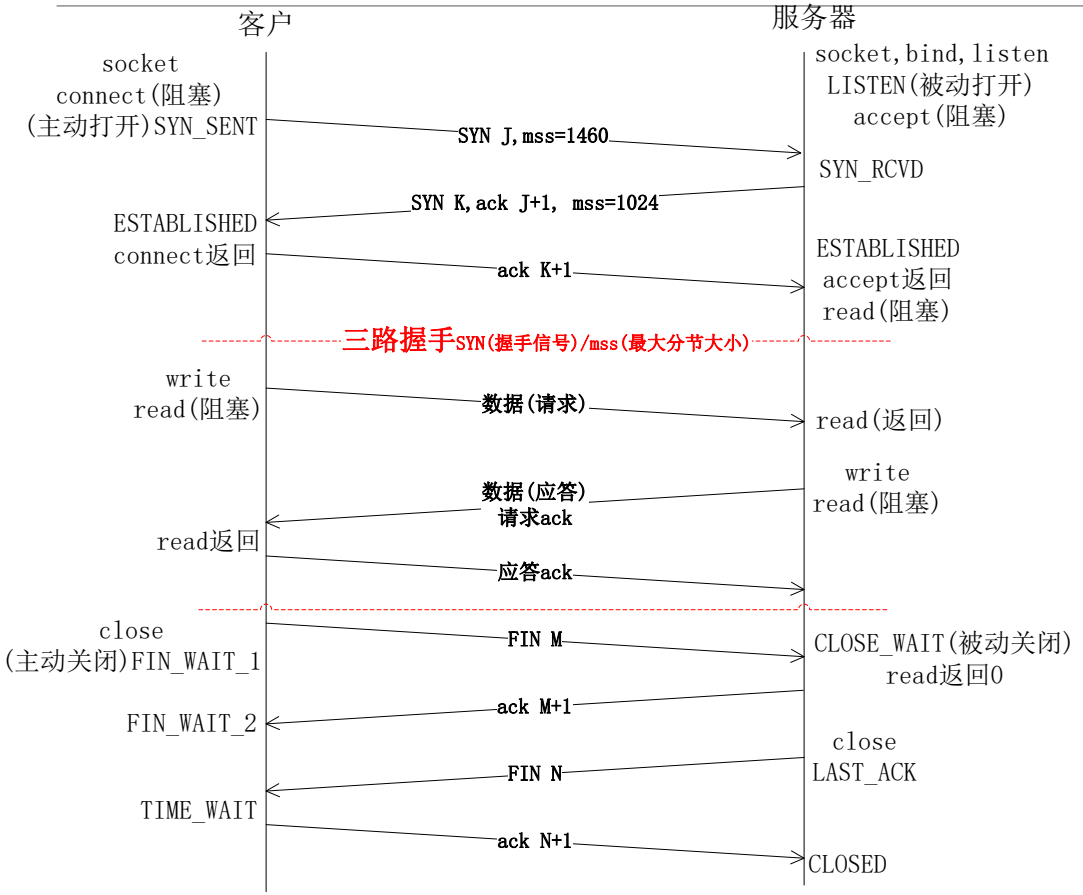
netstat -s

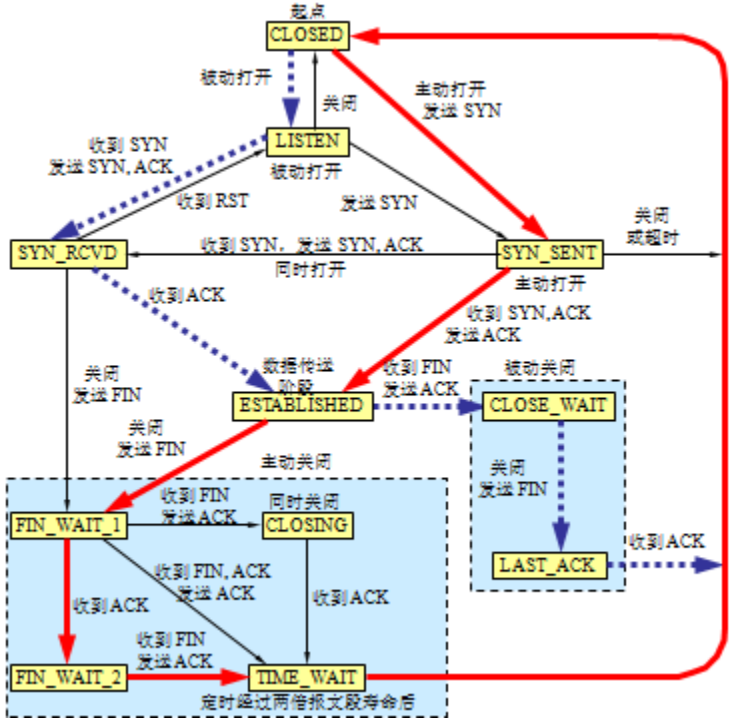
SS

ss -s

netstat -nat | awk '{s[$NF]++}END{for(i in s) print i, s[i];}'

tcp状态

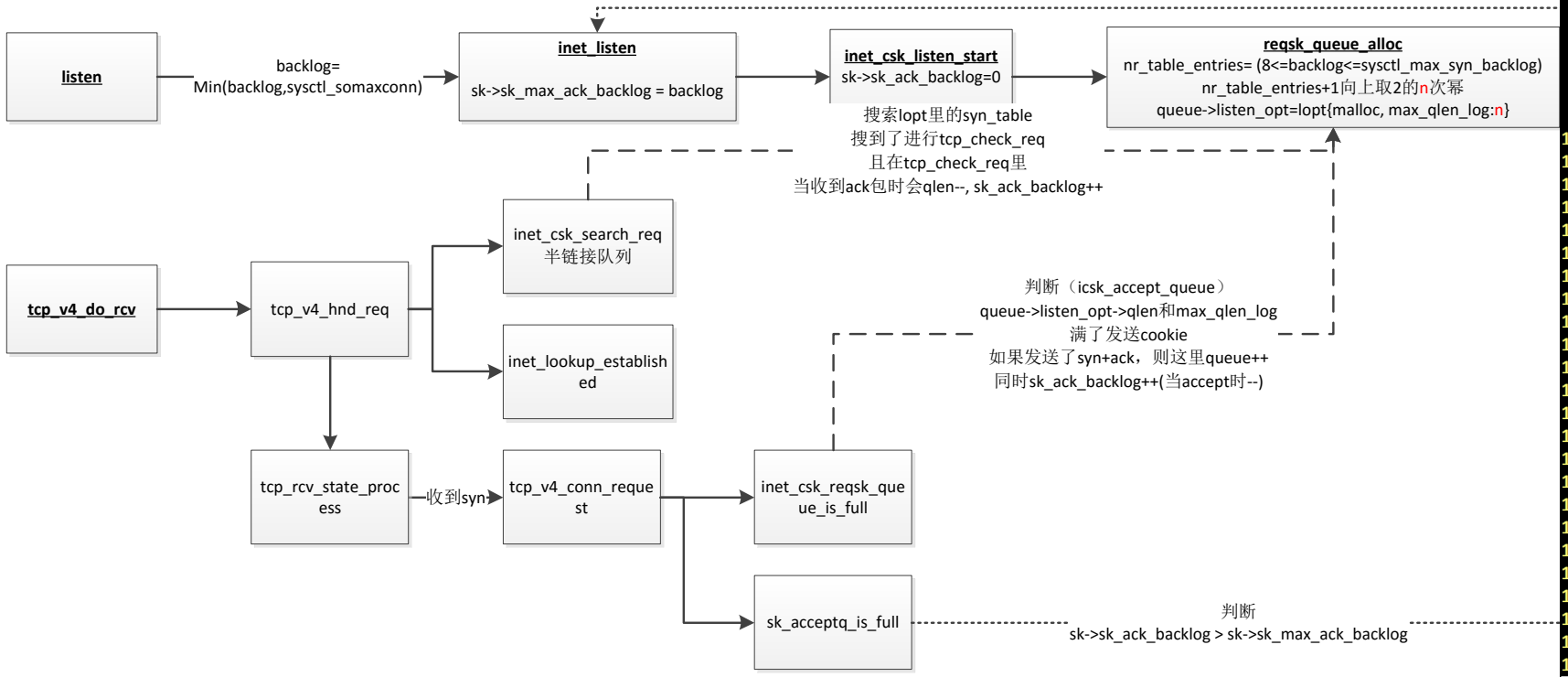




TCP的有限状态机

关于backlog

(remotes/origin/rhel-2.6.32-573.8.1.el6)




```
85 /** struct listen_sock - listen state
86  *
87  * @max_qlen_log - log_2 of maximal queued SYNs/REQUESTs
88  */
89 struct listen_sock {
90     u8          max_qlen_log;
91     /* 3 bytes hole, try to use */
92     int         qlen;
93     int         qlen_young;
94     int         clock_hand;
95     u32         hash_rnd;
96     u32         nr_table_entries;
97     struct request_sock *syn_table[0];
98 };
99
100 /** struct request_sock_queue - queue of request_socks
101  *
102  * @rskq_accept_head - FIFO head of established children
103  * @rskq_accept_tail - FIFO tail of established children
104  * @rskq_defer_accept - User waits for some data after accept()
105  * @syn_wait_lock - serializer
106  *
107  * %syn_wait_lock is necessary only to avoid proc interface having to gra
108  * lock sock while browsing the listening hash (otherwise it's deadlock p
109  *
110  * This lock is acquired in read mode only from listening_get_next() seq_
111  * op and it's acquired in write mode _only_ from code that is actively
112  * changing rskq_accept_head. All readers that are holding the master soc
113  * don't need to grab this lock in read mode too as rskq_accept_head. wri
114  * are always protected from the main sock lock.
115  */
116 struct request_sock_queue {
117     struct request_sock *rskq_accept_head;
118     struct request_sock *rskq_accept_tail;
119     rwlock_t        syn_wait_lock;
120     u8          rskq_defer_accept;
121     /* 3 bytes hole, try to pack */
122     struct listen_sock  *listen_opt;
123 };
include/net/request_sock.h                                    123,2
```

tsar / sar

sar -r 1

sar -n DEV 1

sar -f /var/log/sa/sarxx

tsar --tcp -i1 -l

tsar --io -i1 -l

tsar --io --ndays 7

(指标异常→源码)

pstack

pstack pid

shell 循环

for((;;)); do...; done

for((i=0;i<100;++i)); do echo $i; done

for i in *log* ; do echo rm -f $i; done

cat xx.log| while read i; do echo $i | wc -c ; done

ifind -s coproxy | while read i; do dssh -n $i "hostname"; done

```
0
[root@kvm10563 tmp]# k=0; echo  -e '1\n2' | while read i; do k=$i; echo $k; done ; echo $k
1
2
0
[root@kvm10563 tmp]#
```

last

一台新机器，给你sudo权限，你能找到什么信息？