Поиск процесса который активно использует сеть и диск

Смотрим загрузку сети

```
$ nload
```

Смотрим кто жрет диск

```
$ sudo iotop
```

```
Total DISK READ :    679.22 K/s | Total DISK WRITE :      0.00 B/s
Actual DISK READ:    679.22 K/s | Actual DISK WRITE:      0.00 B/s
  TID  PRIO   USER   DISK READ   DISK WRITE  SWAPIN     IO>  COMMAND
21952  be/4 nobody  679.22 K/s     0.00 B/s  0.00 %  0.00 % smbd --foreground --no-process-group
1536   be/0 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [kdmflush]
1      be/4 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % systemd --switched-root --system --deserialize 22
2      be/4 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [kthreadd]
3      be/4 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [ksoftirqd/0]
5      be/0 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [kworker/0:0H]
7      rt/4 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [migration/0]
8      be/4 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [rcu_bh]
9      be/4 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [rcu_sched]
10     be/0 root      0.00 B/s     0.00 B/s  0.00 %  0.00 % [lru-add-drain]
```

У нас происходит интенсивное чтение

```
$ sudo iostat -kx 1
avg-cpu:   %user   %nice   %system   %iowait   %steal   %idle
           1,01    0,00      0,50      0,00     0,00   98,49

Device:    rrqm/s   wrqm/s    r/s   w/s   rkB/s  wkB/s avgrq-
sz  avgqu-sz  await  r_await w_await  svctm  %util
sda           0,00     0,00   0,00  0,00    0,00   0,00
0,00      0,00   0,00     0,00    0,00   0,00  0,00
sdb           0,00     0,00   4,00  0,00  512,00   0,00
256,00      0,00   1,00     1,00    0,00   1,00  0,40
dm-0          0,00     0,00   0,00  0,00    0,00   0,00
0,00      0,00   0,00     0,00    0,00   0,00  0,00
dm-1          0,00     0,00   0,00  0,00    0,00   0,00
0,00      0,00   0,00     0,00    0,00   0,00  0,00
dm-2          0,00     0,00   4,00  0,00  512,00   0,00
256,00      0,00   1,00     1,00    0,00   1,00  0,40
```

atop тоже показывает нагрузку

```
$ atop
PRC | sys     0.24s | user 0.20s | #proc  205 | #trun      1 |
#tslpi  281 | #tslpu     0 | #zombie 2    | clones 0     |
| no procacct  |
CPU | sys       2% | user    2% | irq     0% | idle    196% |
wait     0% | guest     0% | ipc notavail | cycl unknown |
curf 1.20GHz | curscal 60%  |
cpu | sys       1% | user    1% | irq     0% | idle     98% |
cpu001 w 0% | guest     0% | ipc notavail | cycl unknown |
curf 1.20GHz | curscal 60%  |
cpu | sys       1% | user    1% | irq     0% | idle     98% |
cpu000 w 0% | guest     0% | ipc notavail | cycl unknown |
curf 1.20GHz | curscal 60%  |
CPL | avg1     0.03 | avg5  0.12 | avg15 0.18 |             |
| csw     6822 | intr 9628    |            |             |
numcpu 2     |
MEM | tot      2.7G | free 80.4M | cache 1.2G | buff    0.0M |
slab  82.9M | shmem 126.8M | shrss 0.0M   | vmbal 0.0M   |
hptot 0.0M   | hpuse 0.0M   |
SWP | tot      2.0G | free  1.9G |           |             |
|             |              |             | vmcom 3.1G   |
```

```
vmlim 3.4G   |
LVM | centos-home   | busy    0% | read    58 | write      0 |
KiB/r   130 | KiB/w      0 | MBr/s 0.7    | MBw/s 0.0    | avq
1.00     | avio 0.52 ms |
DSK | sdb           | busy    0% | read    58 | write      0 |
KiB/r   130 | KiB/w      0 | MBr/s 0.7    | MBw/s 0.0    | avq
1.00     | avio 0.50 ms |
NET | transport     | tcpi  3039 | tcpo  5389 | udpi       6 |
udpo       6 | tcpao      0 | tcppo 0      | tcprs 0      |
tcpie 0      | udpie 0      |
NET | network       | ipi   3048 | ipo    474 | ipfrw      3 |
deliv  3045 |               |              |              |
icmpi 0      | icmpo 0      |
NET | enp3s1     0% | pcki  3061 | pcko  5490 | sp 1000 Mbps |
si 252 Kbps | so 6606 Kbps | erri 0       | erro 0       |
drpi 0       | drpo 0       |
NET | enp2s0     0% | pcki    90 | pcko    87 | sp 1000 Mbps |
si   5 Kbps | so   63 Kbps | erri 0       | erro 0       |
drpi 0       | drpo 0       |
NET | lo       ---- | pcki     4 | pcko     4 | sp    0 Mbps |
si   0 Kbps | so    0 Kbps | erri 0       | erro 0       |
drpi 0       | drpo 0       |

  PID    SYSCPU  USRCPU   VGROW  RGROW  RUID   EUID    ST  EXC
THR  S CPUNR  CPU  CMD   1/1
22073     0.07s   0.06s      0K     0K  root   root    --    -
1  S     1   1%  nload
20416     0.05s   0.04s      0K     0K  nobody nobody  --    -
2  S     0   1%  smbd
22195     0.06s   0.03s      0K     0K  svm    svm     --    -
1  R     0   1%  atop
```

top выводит smbd

```
top - 11:11:29 up 5 days, 1:47, 2 users, load average: 0,01,
0,09, 0,17
Tasks: 205 total,  1 running,  202 sleeping,  0 stopped,  2
zombie
%Cpu(s): 1,0 us,  1,2 sy,  0,0 ni,  97,6 id,  0,0 wa,  0,0 hi,
0,2 si,  0,0 st
KiB Mem :   2878452 total,     83172 free,   1462420 used,
1332860 buff/cache
```

```
KiB Swap:   2097148 total,   1952252 free,    144896 used.
1091920 avail Mem

  PID   USER   PR  NI   VIRT  RES   SHR S %CPU %MEM    TIME+
COMMAND
20416   nobody 20  0  438216 5612  4180 S  1,7  0,2  0:27.34
smbd
22073   root   20  0  22460  2768  1624 S  1,3  0,1  0:04.30
nload
22248   svm    20  0  162140 2396  1576 R  0,7  0,1  0:00.21
top
```

Смотрим какой файл открыт

```
$ sudo lsof -p 20416 | grep /home/
COMMAND     PID  TID  USER     FD   TYPE    DEVICE    SIZE/OFF
NODE  NAME
smbd      20416       nobody  cwd    DIR     253,2          26
1073741924  /home/video
smbd      20416       nobody    9r   REG     253,2  5688328780
3222776542
/home/video/transmission/downloads/Cartoons/История игрушек 3
(2010).mkv
```

Или

```
# ls -l /proc/20416/fd
итого 0
lr-x------ 1 root root 64 Май 6 10:52 4 -> /dev/urandom
lrwx------  1  root  root  64  Май  6  10:52  5  ->
/var/lib/samba/private/secrets.tdb
lrwx------  1  root  root  64  Май  6  10:52  6  ->
/var/lib/samba/lock/msg.lock/20416
lrwx------ 1 root root 64 Май 6 10:52 7 -> socket:[3416144]
lrwx------  1  root  root  64  Май  6  10:52  8  ->
/var/lib/samba/lock/names.tdb
lr-x------  1  root  root  64  Май  6  10:52  9  ->
/home/video/transmission/downloads/Cartoons/История игрушек 3
(2010).mkv
```

Тоже самое

```
# ls /proc/20416/fd/* | xargs -L 1 readlink
```

```
/dev/urandom
/var/lib/samba/private/secrets.tdb
/var/lib/samba/lock/msg.lock/20416
socket:[3416144]
/var/lib/samba/lock/names.tdb
/home/video/transmission/downloads/Cartoons/История игрушек 3 (2010).mkv
```

Если вас интересует материал /proc, вы можете заметить, что файлы /proc/<pid>/fd/x являются символической ссылкой на файл, с которым он связан. Вы можете прочитать значение символической ссылки с помощью команды readlink. Например, это показывает, что терминал stdin привязан к:

```
$ readlink /proc/self/fd/0
/dev/pts/43
```

или, чтобы получить все файлы для некоторого процесса,

```
ls /proc/<pid>/fd/* | xargs -L 1 readlink
```