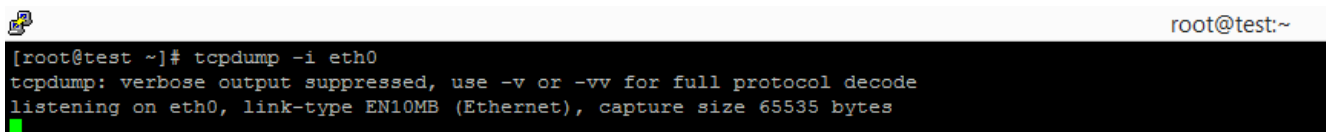


# Command umum monitoring server berbasis linux

*Halo, kali ini akan dibahas tentang command umum yang biasa digunakan untuk memantau kondisi server, seperti mengecek kapasitas hdd, ram, dan jaringan, dan sebagainya.*

Pertama adalah command `tcpdump -i xxx` , contoh : `tcpdump -i eth0` (interface internet card kalian, dalam contoh ini interfacenya adalah `eth0`) . `Tcpdump` sendiri adalah command yang umum digunakan untuk mengetahui paket jaringan kalian / dalam hal ini untuk mengetahui lalu lintas paket TCP/IP yang dikirim atau diterima oleh interface jaringan kalian.

*Contoh nya adalah sebagai berikut :*

A terminal window screenshot showing the execution of the 'tcpdump -i eth0' command. The terminal title is 'root@test:~'. The command prompt is '[root@test ~]# tcpdump -i eth0'. The output shows 'tcpdump: verbose output suppressed, use -v or -vv for full protocol decode' and 'listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes'. A green cursor is visible at the end of the output line.

```
root@test:~  
[root@test ~]# tcpdump -i eth0  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

Kedua adalah command `netstat -a | more` , atau network statistics. Gampangnya, command ini berguna untuk memonitor statistik dari paket jaringan yang masuk dan keluar. Command ini mirip dengan command windows yang juga menggunakan `netstat` untuk memonitor jaringannya. Dan command ini juga berguna bagi sysadmin jika ada gangguan koneksi jaringan sehingga para sysadmin bisa melihat network mana yang bermasalah / error.

*Contohnya adalah sebagai berikut :*



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 *:pop3                  *:*                     LISTEN
tcp    0      0 localhost:783           *:*                     LISTEN
tcp    0      0 *:nbx-ser               *:*                     LISTEN
tcp    0      0 *:imap                  *:*                     LISTEN
tcp    0      0 *:http                  *:*                     LISTEN
tcp    0      0 *:nbx-dir               *:*                     LISTEN
tcp    0      0 *:urd                   *:*                     LISTEN
tcp    0      0 *:ftp                   *:*                     LISTEN
tcp    0      0 test.cpanel.ea4.com:domain *:*                     LISTEN
tcp    0      0 localhost:domain       *:*                     LISTEN
tcp    0      0 *:ssh                   *:*                     LISTEN
tcp    0      0 *:smtp                  *:*                     LISTEN
tcp    0      0 localhost:rndc         *:*                     LISTEN
tcp    0      0 *:https                 *:*                     LISTEN
tcp    0      0 *:tsrmagt               *:*                     LISTEN
tcp    0      0 *:tpcsrcvr              *:*                     LISTEN
tcp    0      0 *:idware-router        *:*                     LISTEN
tcp    0      0 *:autodesk-nlm         *:*                     LISTEN
tcp    0      0 *:imaps                 *:*                     LISTEN
tcp    0      0 *:infowave              *:*                     LISTEN
tcp    0      0 localhost:decbsrv     *:*                     LISTEN
tcp    0      0 *:radsec                *:*                     LISTEN
tcp    0      0 *:pop3s                 *:*                     LISTEN
tcp    0      0 *:gnunet                 *:*                     LISTEN
tcp    0      0 *:eli                   *:*                     LISTEN
tcp    0      0 *:submission            *:*                     LISTEN
tcp    0      0 test.cpanel.ea4.com:ssh where-am-i:62463       ESTABLISHED
tcp    0      0 localhost:gnunet       localhost:45820        TIME_WAIT
tcp    0      0 localhost:55574        localhost:rndc         TIME_WAIT
tcp    0      0 localhost:tsrmagt      localhost:36048        TIME_WAIT
tcp    0      0 localhost:41957        localhost:smtp         TIME_WAIT
tcp    0      0 localhost:decbsrv     localhost:48034        TIME_WAIT
tcp    0      0 *:pop3                  *:*                     LISTEN
tcp    0      0 localhost:783          *:*                     LISTEN
tcp    0      0 *:imap                  *:*                     LISTEN
tcp    0      0 *:http                  *:*                     LISTEN
tcp    0      0 *:urd                   *:*                     LISTEN
tcp    0      0 *:ftp                   *:*                     LISTEN
tcp    0      0 *:ssh                   *:*                     LISTEN
tcp    0      0 *:smtp                  *:*                     LISTEN
tcp    0      0 *:https                 *:*                     LISTEN
tcp    0      0 *:imaps                 *:*                     LISTEN
tcp    0      0 *:pop3s                 *:*                     LISTEN
tcp    0      0 *:mysql                 *:*                     LISTEN
tcp    0      0 *:submission            *:*                     LISTEN
tcp    0      0 localhost:44758        localhost:783          TIME_WAIT
udp    0      0 test.cpanel.ea4.com:domain *:*                     LISTEN
udp    0      0 localhost:domain       *:*                     LISTEN
udp    0      0 *:bootpc                *:*                     LISTEN
--More--
```

Ketiga adalah command **df** , : command ini berfungsi untuk melihat kapasitas hdd pada server, mengenai command ini, banyak variasinya, namun yang umum digunakan adalah command **df -h**

**Contohnya adalah sebagai berikut :**

```
root@test ~]# df
Filesystem      1K-blocks    Used Available Use% Mounted on
dev/vda5        46674904 7464312  36832968  17% /
tmpfs           506928      6648   500280    2% /dev/shm
dev/vda1        991512      30512  909800    4% /boot
dev/vda2        9948012     22520  9413492   1% /tmp
root@test ~]#
```

```
[root@test ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda5       45G   7.2G   36G   17% /
tmpfs           496M   6.5M  489M   2% /dev/shm
/dev/vda1       969M   30M  889M   4% /boot
/dev/vda2       9.5G   22M  9.0G   1% /tmp
[root@test ~]#
```

Keempat adalah command **free** : command ini berfungsi untuk melihat kapasitas ram pada server, dan untuk command free sendiri sama seperti command **df** , command ini juga banyak variasinya, namun untuk memudahkan melihat sisa ram pada server, bisa menggunakan command **free -h**

**Contohnya adalah sebagai berikut :**

```
[root@test ~]# free
total          used          free          shared        buffers         cached
Mem:          1013860      897408      116452           6920          75164         457452
-/+ buffers/cache:      364792          649068
Swap:          4095996           79920      4016076
[root@test ~]#
```

```
[root@test ~]# free -h
total          used          free          shared        buffers         cached
Mem:           990M       876M        113M           6.8M           73M          446M
-/+ buffers/cache:      356M          633M
Swap:          3.9G           78M          3.8G
[root@test ~]#
```

Kelima adalah command **lsof** : command ini berfungsi untuk melihat file yang terbuka didalam sistem / server. Seperti proses apa dan di folder apa. Command ini juga sangat berfungsi untuk mengetahui jika ada user / folder yang mencurigakan, yang kemungkinan adalah malware, serta untuk melihat user dengan proses apa yang paling memberatkan server.

**Contohnya adalah sebagai berikut :**

```

root@test~
cpanel 2163 root 12u unix 0xffff8003d6d540 0t0 12720 /usr/local/cpanel/var/cpdoveauth_domainownerd.sock
cpanel 2163 root 14r FIFO 0,8 0t0 2271233 pipe
cpanel 2163 root 15w FIFO 0,8 0t0 2271233 pipe
cpanel 2163 root 16u 0000 0,9 0 4055 [eventpoll]
cpanel 2163 root 17w REG 252,5 287843 1187787 /usr/local/cpanel/logs/error_log
cpanel 2163 root 18w REG 252,5 0 1189894 /usr/local/cpanel/logs/incoming_http_requests.log
cpanel 2163 root 19w REG 252,5 266 1189895 /usr/local/cpanel/logs/login_log
cpanel 2163 root 20w REG 252,5 1960809 1189896 /usr/local/cpanel/logs/access_log
cpanel 2163 root 21w REG 252,5 5462 1189897 /usr/local/cpanel/logs/cpwrapd_log
cpanel 2163 root 22w REG 252,5 3537 1189898 /usr/local/cpanel/logs/session_log
cpanel 2163 root 23w REG 252,5 0 1189899 /usr/local/cpanel/logs/api_tokens_log
queueproc 2171 root cwd DIR 252,5 4096 2 /
queueproc 2171 root rtd DIR 252,5 4096 2 /
queueproc 2171 root txt REG 252,5 9093 1579532 /usr/local/cpanel/3rdparty/perl/524/bin/perl
queueproc 2171 root mem REG 252,5 49965 1578615 /usr/local/cpanel/3rdparty/perl/524/lib64/perl5/cpanel_lib/x86_64-linux-64int/auto/List/Util/Util.so
queueproc 2171 root mem REG 252,5 21678 1578488 /usr/local/cpanel/3rdparty/perl/524/lib64/perl5/5.24.1/x86_64-linux-64int/auto/Fontl/Fontl.so
queueproc 2171 root mem REG 252,5 45001 1704180 /usr/local/cpanel/3rdparty/perl/524/lib64/perl5/cpanel_lib/x86_64-linux-64int/auto/JSON/XS/XS.so
queueproc 2171 root mem REG 252,5 10312 1179654 /lib64/libfreebl3.so
queueproc 2171 root mem REG 252,5 1924768 1179664 /lib64/libc-2.12.so
queueproc 2171 root mem REG 252,5 15056 1179696 /lib64/libutil-2.12.so
queueproc 2171 root mem REG 252,5 40872 1179668 /lib64/libcrypt-2.12.so
queueproc 2171 root mem REG 252,5 596864 1179672 /lib64/libm-2.12.so
queueproc 2171 root mem REG 252,5 20024 1179670 /lib64/libdl-2.12.so
queueproc 2171 root mem REG 252,5 113904 1179674 /lib64/libnsl-2.12.so
queueproc 2171 root mem REG 252,5 143280 1179688 /lib64/libpthread-2.12.so
queueproc 2171 root mem REG 252,5 176922 1578322 /usr/local/cpanel/3rdparty/perl/524/lib64/perl5/5.24.1/x86_64-linux-64int/CORE/libperl.so
queueproc 2171 root mem REG 252,5 26104 65832 /usr/lib64/libgdbm.so.2.0.0
queueproc 2171 root mem REG 252,5 159312 1179657 /lib64/ld-2.12.so
queueproc 2171 root 0r CHR 1,3 0t0 4059 /dev/null
queueproc 2171 root 1w REG 252,5 34112 1188087 /usr/local/cpanel/logs/queueprocd.log
queueproc 2171 root 2w REG 252,5 34112 1188087 /usr/local/cpanel/logs/queueprocd.log
queueproc 2171 root 4w REG 252,5 34112 1188087 /usr/local/cpanel/logs/queueprocd.log
pof 2200 cpanelconnecttrack cwd DIR 252,5 4096 526959 /var/cpanel/userhomes/cpanelconnecttrack
pof 2200 cpanelconnecttrack rtd DIR 252,5 4096 526959 /var/cpanel/userhomes/cpanelconnecttrack
pof 2200 cpanelconnecttrack txt REG 252,5 358953 2364856 /usr/local/cpanel/3rdparty/sbin/pof
pof 2200 cpanelconnecttrack mem REG 252,5 66432 1179680 /lib64/libnss_files-2.12.so
pof 2200 cpanelconnecttrack mem REG 0,6 12936 socket:[12936] (stat: No such file or directory)
pof 2200 cpanelconnecttrack mem REG 252,5 1924768 1179664 /lib64/libc-2.12.so
pof 2200 cpanelconnecttrack mem REG 252,5 258504 669696 /usr/lib64/libcap.so.1.4.0
pof 2200 cpanelconnecttrack mem REG 252,5 159312 1179657 /lib64/ld-2.12.so
pof 2200 cpanelconnecttrack 0r CHR 1,3 0t0 4059 /dev/null
pof 2200 cpanelconnecttrack 1w REG 252,5 600 526941 /var/run/restartsrv/startup/pof
pof 2200 cpanelconnecttrack 2w REG 252,5 600 526941 /var/run/restartsrv/startup/pof
pof 2200 cpanelconnecttrack 3u pack 12936 0t0 ALL type=SOCK DGRAM
pof 2200 cpanelconnecttrack 4u unix 0xffff8003d6d6780 0t0 12937 /var/cpanel/userhomes/cpanelconnecttrack/pof.socket
cpdavid 2220 root cwd DIR 252,5 4096 2 /
cpdavid 2220 root rtd DIR 252,5 4096 2 /
cpdavid 2220 root txt REG 252,5 417360 670109 /usr/local/cpanel/libexec/cpdavid-dormant
cpdavid 2220 root mem REG 252,5 10312 1179654 /lib64/libfreebl3.so
cpdavid 2220 root mem REG 252,5 1924768 1179664 /lib64/libc-2.12.so
cpdavid 2220 root mem REG 252,5 15056 1179696 /lib64/libutil-2.12.so
cpdavid 2220 root mem REG 252,5 40872 1179668 /lib64/libcrypt-2.12.so

```

Ya demikian beberapa command umum yang digunakan untuk memonitor server kalian yang berbasis linux, jika ada kekurangan dalam informasi yang diberikan, silahkan googling atau cari refrensi di forum ☐