lsof

lsof meaning ‘LiSt Open Files’ is used to find out which files are open by which process. As we all know Linux/Unix considers everything as a files (pipes, sockets, directories, devices etc). One of the reason to use lsof command is when a disk cannot be unmounted as it says the files are being used. With the help of this command we can easily identify the files which are in use.

#### 1. List all Open Files with lsof Command

In the below example, it will show long listing of open files some of them are extracted for better understanding which displays the columns like Command, PID, USER, FD, TYPE etc.

# lsof  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
init 1 root cwd DIR 253,0 4096 2 /  
init 1 root rtd DIR 253,0 4096 2 /  
init 1 root txt REG 253,0 145180 147164 /sbin/init  
init 1 root mem REG 253,0 1889704 190149 /lib/libc-2.12.so  
init 1 root 0u CHR 1,3 0t0 3764 /dev/null  
init 1 root 1u CHR 1,3 0t0 3764 /dev/null  
init 1 root 2u CHR 1,3 0t0 3764 /dev/null  
init 1 root 3r FIFO 0,8 0t0 8449 pipe  
init 1 root 4w FIFO 0,8 0t0 8449 pipe  
init 1 root 5r DIR 0,10 0 1 inotify  
init 1 root 6r DIR 0,10 0 1 inotify  
init 1 root 7u unix 0xc1513880 0t0 8450 socket

Sections and it’s values are self-explanatory. However, we’ll review FD & TYPE columns more precisely.

FD – stands for File descriptor and may seen some of the values as:

1. cwd current working directory
2. rtd root directory
3. txt program text (code and data)
4. mem memory-mapped file

Also in FD column numbers like 1u is actual file descriptor and followed by u,r,w of it’s mode as:

1. r for read access.
2. w for write access.
3. u for read and write access.

TYPE – of files and it’s identification.

1. DIR – Directory
2. REG – Regular file
3. CHR – Character special file.
4. FIFO – First In First Out

#### 2. List User Specific Opened Files

The below command will display the list of all opened files of user tecmint.

# lsof -u tecmint  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
sshd 1838 tecmint cwd DIR 253,0 4096 2 /  
sshd 1838 tecmint rtd DIR 253,0 4096 2 /  
sshd 1838 tecmint txt REG 253,0 532336 188129 /usr/sbin/sshd  
sshd 1838 tecmint mem REG 253,0 19784 190237 /lib/libdl-2.12.so  
sshd 1838 tecmint mem REG 253,0 122436 190247 /lib/libselinux.so.1  
sshd 1838 tecmint mem REG 253,0 255968 190256 /lib/libgssapi\_krb5.so.2.2  
sshd 1838 tecmint mem REG 253,0 874580 190255 /lib/libkrb5.so.3.3

#### 3. Find Processes running on Specific Port

To find out all the running process of specific port, just use the following command with option -i. The below example will list all running process of port 22.

# lsof -i TCP:22  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
sshd 1471 root 3u IPv4 12683 0t0 TCP \*:ssh (LISTEN)  
sshd 1471 root 4u IPv6 12685 0t0 TCP \*:ssh (LISTEN)

#### 4. List Only IPv4 & IPv6 Open Files

In below example shows only IPv4 and IPv6 network files open with separate commands.

# lsof -i 4  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
rpcbind 1203 rpc 6u IPv4 11326 0t0 UDP \*:sunrpc  
rpcbind 1203 rpc 7u IPv4 11330 0t0 UDP \*:954  
rpcbind 1203 rpc 8u IPv4 11331 0t0 TCP \*:sunrpc (LISTEN)  
avahi-dae 1241 avahi 13u IPv4 11579 0t0 UDP \*:mdns  
avahi-dae 1241 avahi 14u IPv4 11580 0t0 UDP \*:58600  
  
# lsof -i 6  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
rpcbind 1203 rpc 9u IPv6 11333 0t0 UDP \*:sunrpc  
rpcbind 1203 rpc 10u IPv6 11335 0t0 UDP \*:954  
rpcbind 1203 rpc 11u IPv6 11336 0t0 TCP \*:sunrpc (LISTEN)  
rpc.statd 1277 rpcuser 10u IPv6 11858 0t0 UDP \*:55800  
rpc.statd 1277 rpcuser 11u IPv6 11862 0t0 TCP \*:56428 (LISTEN)  
cupsd 1346 root 6u IPv6 12112 0t0 TCP localhost:ipp (LISTEN)

#### 5. List Open Files of TCP Port ranges 1-1024

To list all the running process of open files of TCP Port ranges from 1-1024.

# lsof -i TCP:1-1024  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
rpcbind 1203 rpc 11u IPv6 11336 0t0 TCP \*:sunrpc (LISTEN)  
cupsd 1346 root 7u IPv4 12113 0t0 TCP localhost:ipp (LISTEN)  
sshd 1471 root 4u IPv6 12685 0t0 TCP \*:ssh (LISTEN)  
master 1551 root 13u IPv6 12898 0t0 TCP localhost:smtp (LISTEN)  
sshd 1834 root 3r IPv4 15101 0t0 TCP 192.168.0.2:ssh->192.168.0.1:conclave-cpp (ESTABLISHED)  
sshd 1838 tecmint 3u IPv4 15101 0t0 TCP 192.168.0.2:ssh->192.168.0.1:conclave-cpp (ESTABLISHED)  
sshd 1871 root 3r IPv4 15842 0t0 TCP 192.168.0.2:ssh->192.168.0.1:groove (ESTABLISHED)  
httpd 1918 root 5u IPv6 15991 0t0 TCP \*:http (LISTEN)  
httpd 1918 root 7u IPv6 15995 0t0 TCP \*:https (LISTEN)

#### 6. Exclude User with ‘^’ Character

Here, we have excluded root user. You can exclude a particular user using ‘^’ with command as shown above.

# lsof -i -u^root  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
rpcbind 1203 rpc 6u IPv4 11326 0t0 UDP \*:sunrpc  
rpcbind 1203 rpc 7u IPv4 11330 0t0 UDP \*:954  
rpcbind 1203 rpc 8u IPv4 11331 0t0 TCP \*:sunrpc (LISTEN)  
rpcbind 1203 rpc 9u IPv6 11333 0t0 UDP \*:sunrpc  
rpcbind 1203 rpc 10u IPv6 11335 0t0 UDP \*:954  
rpcbind 1203 rpc 11u IPv6 11336 0t0 TCP \*:sunrpc (LISTEN)  
avahi-dae 1241 avahi 13u IPv4 11579 0t0 UDP \*:mdns  
avahi-dae 1241 avahi 14u IPv4 11580 0t0 UDP \*:58600  
rpc.statd 1277 rpcuser 5r IPv4 11836 0t0 UDP \*:soap-beep  
rpc.statd 1277 rpcuser 8u IPv4 11850 0t0 UDP \*:55146  
rpc.statd 1277 rpcuser 9u IPv4 11854 0t0 TCP \*:32981 (LISTEN)  
rpc.statd 1277 rpcuser 10u IPv6 11858 0t0 UDP \*:55800  
rpc.statd 1277 rpcuser 11u IPv6 11862 0t0 TCP \*:56428 (LISTEN)

#### 7. Find Out who’s Looking What Files and Commands?

Below example shows user tecmint is using command like ping and /etc directory .

# lsof -i -u tecmint  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
bash 1839 tecmint cwd DIR 253,0 12288 15 /etc  
ping 2525 tecmint cwd DIR 253,0 12288 15 /etc

#### 8. List all Network Connections

The following command with option ‘-i’ shows the list of all network connections ‘LISTENING & ESTABLISHED’.

# lsof -i  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
rpcbind 1203 rpc 6u IPv4 11326 0t0 UDP \*:sunrpc  
rpcbind 1203 rpc 7u IPv4 11330 0t0 UDP \*:954  
rpcbind 1203 rpc 11u IPv6 11336 0t0 TCP \*:sunrpc (LISTEN)  
avahi-dae 1241 avahi 13u IPv4 11579 0t0 UDP \*:mdns  
avahi-dae 1241 avahi 14u IPv4 11580 0t0 UDP \*:58600  
rpc.statd 1277 rpcuser 11u IPv6 11862 0t0 TCP \*:56428 (LISTEN)  
cupsd 1346 root 6u IPv6 12112 0t0 TCP localhost:ipp (LISTEN)  
cupsd 1346 root 7u IPv4 12113 0t0 TCP localhost:ipp (LISTEN)  
sshd 1471 root 3u IPv4 12683 0t0 TCP \*:ssh (LISTEN)  
master 1551 root 12u IPv4 12896 0t0 TCP localhost:smtp (LISTEN)  
master 1551 root 13u IPv6 12898 0t0 TCP localhost:smtp (LISTEN)  
sshd 1834 root 3r IPv4 15101 0t0 TCP 192.168.0.2:ssh->192.168.0.1:conclave-cpp (ESTABLISHED)  
httpd 1918 root 5u IPv6 15991 0t0 TCP \*:http (LISTEN)  
httpd 1918 root 7u IPv6 15995 0t0 TCP \*:https (LISTEN)  
clock-app 2362 narad 21u IPv4 22591 0t0 TCP 192.168.0.2:45284->www.gov.com:http (CLOSE\_WAIT)  
chrome 2377 narad 61u IPv4 25862 0t0 TCP 192.168.0.2:33358->maa03s04-in-f3.1e100.net:http (ESTABLISHED)  
chrome 2377 narad 80u IPv4 25866 0t0 TCP 192.168.0.2:36405->bom03s01-in-f15.1e100.net:http (ESTABLISHED)

#### 9. Search by PID

The below example only shows whose PID is 1 [One].

# lsof -p 1  
  
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
init 1 root cwd DIR 253,0 4096 2 /  
init 1 root rtd DIR 253,0 4096 2 /  
init 1 root txt REG 253,0 145180 147164 /sbin/init  
init 1 root mem REG 253,0 1889704 190149 /lib/libc-2.12.so  
init 1 root mem REG 253,0 142472 189970 /lib/ld-2.12.so

#### 10. Kill all Activity of Particular User

Sometimes you may have to kill all the processes for a specific user. Below command will kills all the processes of tecmint user.

# kill -9 `lsof -t -u tecmint`