

## An lsof Tutorial and Primer

lsof is the Linux/Unix über-tool. I use it most for getting network connection related information from a system, but that's just the beginning for this amazing and little-known application. The tool is aptly called lsof because it "lists open files". And remember, in Unix just about everything (including a network socket) is a file.

\*\* lsof is also the Linux/Unix command with the most switches. It has so many it has to use both pluses and minuses.

```
usage: [-?abhlLnNoOPRstUvV] [+|-c c] [+|-d s] [+D D] [+|-f[CG]]
  [-F [f]] [-g [s]] [-i [i]] [+|-L [l]] [+|-M] [-o [o]]
  [-p s] [+|-r [t]] [-S [t]] [-T [t]] [-u s] [+|-w] [-x [fl]] [--] [names]
```

As you can see, lsof has a truly staggering number of options. You can use it to get information about devices on your system, what a given user is touching at any given point, or even what files or network connectivity a process is using. lsof replaces my need for both netstat and ps entirely. It has everything I get from those tools and much, much more.

### Show Your Network Connections

Show all connections with `-i`

```
lsof -i
COMMAND PID USER  FD   TYPE DEVICE SIZE NODE NAME
dhcpcd 6061 root  4u IPv4 4510 UDP  *:bootpc
sshd 7703 root  3u IPv6 6499 TCP  *:ssh (LISTEN)
sshd 7892 root  3u IPv6 6757 TCP  10.10.1.5:ssh->192.168.1.5:49901 (ESTABLISHED)
```

Show only TCP (works the same for UDP)

```
lsof -iTCP
COMMAND PID USER  FD   TYPE DEVICE SIZE NODE NAME
sshd 7703 root  3u IPv6 6499 TCP  *:ssh (LISTEN)
sshd 7892 root  3u IPv6 6757 TCP  10.10.1.5:ssh->192.168.1.5:49901 (ESTABLISHED)
```

`-i :port` shows all networking related to a given port

```
lsof -i :22
COMMAND PID USER  FD   TYPE DEVICE SIZE NODE NAME
sshd 7703 root  3u IPv6 6499 TCP  *:ssh (LISTEN)
sshd 7892 root  3u IPv6 6757 TCP  10.10.1.5:ssh->192.168.1.5:49901 (ESTABLISHED)
```

To show connections to a specific host, use `@host`

```
lsof -i@192.168.1.5
sshd 7892 root  3u IPv6 6757 TCP  10.10.1.5:ssh->192.168.1.5:49901 (ESTABLISHED)
```

Show connections based on the host and the port using `@host:port`

```
lsof -i@192.168.1.5:22
sshd 7892 root  3u IPv6 6757 TCP  10.10.1.5:ssh->192.168.1.5:49901 (ESTABLISHED)
```

Grepping for "LISTEN" shows what ports your system is waiting for connections on

```
lsof -i | grep LISTEN
iTunes      400 daniel  16u IPv4 0x4575228  0t0 TCP  *:daap (LISTEN)
```

# An lsof Tutorial and Primer

Grepping for "ESTABLISHED" shows current active connections

```
lsof -i | grep ESTABLISHED
firefox-b 169 daniel 49u IPv4 0t0 TCP 1.2.3.3:1863->1.2.3.4:http (ESTABLISHED)
```

## Working with Users, Processes, and Files

You can also get information on various users, processes, and files on your system using lsof:

Show what a given user has open using `-u`

```
lsof -u daniel
-- snipped --
Dock 155 daniel txt REG 14,2 2798436 823208 /usr/lib/libicucore.A.dylib
Dock 155 daniel txt REG 14,2 1580212 823126 /usr/lib/libobjc.A.dylib
Dock 155 daniel txt REG 14,2 2934184 823498 /usr/lib/libstdc++.6.0.4.dylib
Dock 155 daniel txt REG 14,2 132008 823505 /usr/lib/libgcc_s.1.dylib
Dock 155 daniel txt REG 14,2 212160 823214 /usr/lib/libauto.dylib
-- snipped --
```

See what files and network connections a command is using with `-c`

```
lsof -c syslog-ng
COMMAND  PID USER  FD  TYPE  DEVICE  SIZE  NODE NAME
syslog-ng 7547 root  cwd  DIR   3,3    4096   2 /
syslog-ng 7547 root  rtd  DIR   3,3    4096   2 /
syslog-ng 7547 root  txt  REG   3,3 113524 1064970 /usr/sbin/syslog-ng
syslog-ng 7547 root  mem  REG   0,0   0 [heap]
syslog-ng 7547 root  mem  REG   3,3 105435 850412 /lib/libpthread-2.4.so
syslog-ng 7547 root  mem  REG   3,3 1197180 850396 /lib/libc-2.4.so
syslog-ng 7547 root  mem  REG   3,3 59868 850413 /lib/libresolv-2.4.so
syslog-ng 7547 root  mem  REG   3,3 72784 850404 /lib/libnsl-2.4.so
syslog-ng 7547 root  mem  REG   3,3 32040 850414 /lib/librt-2.4.so
syslog-ng 7547 root  mem  REG   3,3 126163 850385 /lib/ld-2.4.so
-- snipped --
```

Pointing to a file shows what's interacting with that file

```
lsof /var/log/messages
COMMAND  PID USER  FD  TYPE  DEVICE  SIZE  NODE NAME
syslog-ng 7547 root   4w  REG   3,3 217309 834024 /var/log/messages
```

The `-p` switch lets you see what a given process ID has open, which is good for learning more about unknown processes

```
lsof -p 10075
-- snipped --
sshd 10068 root  mem  REG   3,3 34808 850407 /lib/libnss_files-2.4.so
sshd 10068 root  mem  REG   3,3 34924 850409 /lib/libnss_nis-2.4.so
sshd 10068 root  mem  REG   3,3 26596 850405 /lib/libnss_compat-2.4.so
sshd 10068 root  mem  REG   3,3 200152 509940 /usr/lib/libssl.so.0.9.7
sshd 10068 root  mem  REG   3,3 46216 510014 /usr/lib/liblber-2.3
sshd 10068 root  mem  REG   3,3 59868 850413 /lib/libresolv-2.4.so
sshd 10068 root  mem  REG   3,3 1197180 850396 /lib/libc-2.4.so
sshd 10068 root  mem  REG   3,3 22168 850398 /lib/libcrypt-2.4.so
sshd 10068 root  mem  REG   3,3 72784 850404 /lib/libnsl-2.4.so
sshd 10068 root  mem  REG   3,3 70632 850417 /lib/libz.so.1.2.3
sshd 10068 root  mem  REG   3,3 9992 850416 /lib/libutil-2.4.so
```

# An lsof Tutorial and Primer

-- snipped --

The -t option returns just a PID

```
lsof -t -c Mail
350
ps aux | grep Mail
daniel 350 0.0 1.5 405980 31452 ?? S   Mon07PM 2:50.28 /Applications/Mail.app
```

## Advanced Usage

Using -a allows you to combine search terms, so the query below says, "show me everything running as daniel connected to 1.1.1.1"

```
lsof -a -u daniel -i @1.1.1.1
bkdr  1893 daniel 3u IPv6 3456 TCP 10.10.1.10:1234->1.1.1.1:31337 (ESTABLISHED)
```

Using the -t and -c options together you can HUP processes

```
kill -HUP `lsof -t -c sshd`
```

You can also use the -t with -u to kill everything a user has open

```
kill -9 `lsof -t -u daniel`
```

lsof +L1 shows you all open files that have a link count less than 1, often indicative of a cracker trying to hide something

```
lsof +L1
(hopefully nothing)
```

## Conclusion

This primer just scratches the surface of lsof's functionality. For a full reference, run `man lsof` or check out the online version. I hope this has been useful to you, and as always, comments and corrections are welcomed.

## References

The lsof man page:

<http://www.netadmintools.com/html/lsof.man.html>