The sys admin's daily grind: lsof

The Long and the Short of It

The shorter a command, the longer the list of support parameters. This rule applies to lsof, one of Charly's favorite commands. *By Charly Kühnast*

If you type `lsof` without parameters, the output is a long list of open files. This outpouring is sorted by PID; thus, it starts with `init`. On a laptop I was using as a lab machine, the list includes no fewer than 6,778 entries, which is not my understanding of intelligible. However, almost all of the command-line parameters that `lsof` is happy to accept will reduce the volume.

For example, if I want to know which process is accessing a certain file, I just pass its name in to `lsof` as a parameter. The

```
lsof /var/log/syslog
```

command returns the following results (which I have curtailed slightly):

```
COMMAND   PID   USER
rsyslogd 683   syslog
```

In other words, rsyslog is running on my system. Additionally, I would like to know the other files rsyslog is juggling:

```
lsof -c rsyslog
```

Alternatively, I could output all the files that belong to the `syslog` user account, for which I need the `-u syslog` option. Because everything on Linux is a file, including network sockets,

```
lsof -iTCP
```

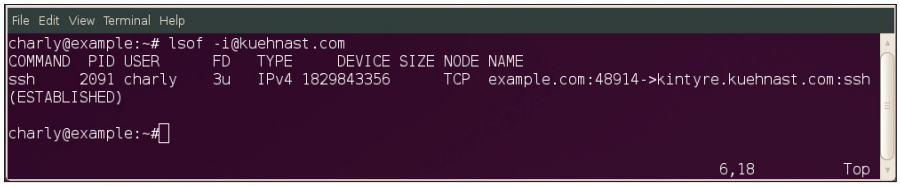

Figure 1: Analyzing outgoing connections with `lsof -i@example.com`.

lists all the current network connections. If I just want to see the services listening for connections, I can use:

```
lsof -iTCP | grep LISTEN
```

On the other hand, if I am only interested in traffic on a certain port, for example SSH, the

```
lsof -i :22
```

parameter will list all the connections associated with port 22.

Know What's Going Out

To filter for outward bound connections to a specific server, add to the `-i` parameter an `@` followed by the name or IP address of the target system (e.g., Figure 1). I can reduce the number of hits further by adding the target port number:

```
lsof -i@example.com:22
```

I'm sure the `lsof` inventors, led by Victor A. Abell, had users like me in mind when they created the `-a` option, which lets you concatenate filter functions. The command

```
lsof -a -u charly -i@example.com:22
```

lists all outgoing SSH connections to the *example.com* server opened by user `charly`.

At second glance, especially if you type `man lsof`, you might find `lsof` is an indispensable tool for any system administrator. ■■■

CHARLY KÜHNAST

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.