

Isof Examples and Tips

The Isof command lists open files, sockets, and pipes. To learn more about a Unix system, run Isof on them to see what files are held open (such as libraries or log files) and what ports daemons listen to. Knowing the normal operating state of a system will help when debugging the system:

```
# Isof | less -S
```

```
...
```

However, Isof does not show all the information required to debug a problem. See also netstat for routing table and send and receive queue size information.

Search for Open Files

A single open file can prevent a filesystem from being unmounted. Isof should be run as the superuser (root) to see all open files. The following example shows an open file under the mount point /mnt being used by vim.

```
# Isof /mnt
```

```
vim 1481 user 3u VREG 14,6 4096
```

```
306536 /mnt/.test.swp
```

For more information about a particular process, use the -p option to Isof:

```
# Isof -p 1481
```

```
COMMAND PID USER FD TYPE DEVICE
```

```
SIZE/OFF NODE NAME
```

```
...
```

To close an open file, the process holding the file open will need to be closed, either by quitting out of it, or via a command like kill. Avoid using the -9 or -KILL options to the kill command if possible.

Show Listen Addresses

Daemons may either bind to the global 0.0.0.0 IPv4 address, or to specific addresses, such as 127.0.0.1 (localhost). A daemon bound to the localhost address will only be reachable from the system itself. Use the -i and -nP options to Isof to show listening ports without lookups on hostnames and services. For example, the following shows the Apache httpd daemon running on localhost at the non-standard port of 8000. Other systems will not be able to connect to this httpd processes: good for security, bad for remote connectivity.

```
# Isof -i -nP | grep httpd
```

```
httpd 2318 apache
```

```
16u IPv4 0x019922bc 0t0 TCP 127.0.0.1:8000 (LISTEN)
```

```
httpd 2319 apache 16u
```

Isof Examples and Tips

```
IPv4 0x019922bc 0t0 TCP 127.0.0.1:8000 (LISTEN)
httpd 2322 apache 16u IPv4
```

```
0x019922bc 0t0 TCP 127.0.0.1:8000 (LISTEN)
```

In contrast, the following OpenSSH sshd process will accept connections from other systems, as it is bound to the 0.0.0.0 address, as indicated by the * preceding the port number.

```
# Isof -i -P | grep sshd
```

```
sshd 2361 root 3u
```

```
IPv4 2658 TCP *:22 (LISTEN)
```

Certain applications listen on many different ports, such as the Berkeley Internet Name Daemon (BIND) named daemon, version 9.

```
# Isof -i -nP | grep ^named
```

```
named 284 named 5u
```

```
IPv6 0x01388be0 0t0 UDP *:53
```

```
named 284 named 6u IPv6 0x01664e80 0t0 TCP *:53
```

```
(LISTEN)
```

```
named 284 named 7u IPv4 0x01388b10 0t0 UDP 127.0.0.1:53
```

```
named 284
```

```
named 8u IPv4 0x01870570 0t0 TCP 127.0.0.1:53 (LISTEN)
```

```
named 284 named 9u
```

```
IPv4 0x01388a40 0t0 UDP *:49164
```

```
named 284 named 10u IPv6 0x01388970 0t0 UDP
```

```
*:49165
```

```
named 284 named 11u IPv4 0x0186fd54 0t0 TCP *:953 (LISTEN)
```

```
named
```

```
284 named 13u IPv4 0x01387ee0 0t0 UDP 192.0.2.1:53
```

```
named 284 named 14u IPv4
```

```
0x01999ce4 0t0 TCP 192.0.2.1:53 (LISTEN)
```

A process may not work for other reasons, such as a firewall, access service control like tcp_wrappers, or some other misconfiguration. Use ping, telnet, or nmap to check from a remote system whether something else may be blocking the request, or run tcpdump to see whether connections leave the source or arrive at the target system.

Isof Examples and Tips

Mangle the Current Working Directory

Isof in conjunction with the GNU Project Debugger (GDB) can alter the current working directory of another process, for example if a shell is left open on a mount point that must be remounted. Use gdb at your own risk! A simpler solution: kill the bash process with a HUP signal.

```
$ Isof | egrep '^C|/nfs/server'  
COMMAND PID
```

```
USER FD TYPE DEVICE SIZE/OFF NODE NAME  
bash 17328 jmates cwd VDIR 14,2 102
```

```
1456154 /nfs/server
```

1. Attach gdb to the above bash process
Either launch gdb and attach, or attach directly via the gdb bash 17328 command.

```
$ gdb -q  
(gdb) attach
```

```
17328  
Attaching to process 17328.  
Reading symbols for shared
```

```
libraries . done  
Reading symbols for shared libraries .... done  
0x900137a4
```

```
in read ()
```

2. Change the working directory
After the chdir(2) call, use Isof to examine the current working directory.

```
(gdb) call (int) chdir("/")  
$1 = 0  
(gdb)
```

```
shell Isof -p 17328 | fgrep cwd  
bash 17328 jmates cwd VDIR 14,2
```

```
1224 2 /
```

3. When done, change the directory back

Isof Examples and Tips

```
(gdb) call (int) chdir("/nfs/server")
$2 =
0
(gdb) shell Isof -p 17328 | fgrep cwd
bash 17328 jmates cwd

VDIR 14,2 102 1456154 /nfs/server
(gdb) detach
Detaching from
```

```
process 17328 thread 0xd03.
(gdb) quit
```

For a list of other functions and system calls available, use the `info functions` command under `gdb`, then consult the man pages or source to see how the function should be called.

```
$ cat show-functions
info

functions
detach
$ gdb -batch -x show-functions bash 17328 >

bash.fun
```

Again, use `gdb` at your own risk!