lsof

显示Linux系统当前已打开的所有文件列表 `lsof -p pid`

补充说明

lsof命令 用于查看你进程打开的文件，打开文件的进程，进程打开的端口(TCP、UDP)、找回/恢复删除的文件。是十分方便的系统监视工具，因为lsof命令需要访问核心内存和各种文件，所以需要root用户执行。

在linux环境下，任何事物都以文件的形式存在，通过文件不仅仅可以访问常规数据，还可以访问网络连接和硬件。所以如传输控制协议 (TCP) 和用户数据报协议 (UDP) 套接字等，系统在后台都为该应用程序分配了一个文件描述符，无论这个文件的本质如何，该文件描述符为应用程序与基础操作系统之间的交互提供了通用接口。因为应用程序打开文件的描述符列表提供了大量关于这个应用程序本身的信息，因此通过lsof工具能够查看这个列表对系统监测以及排错将是很有帮助的。

语法

```
lsof (选项)
```

选项

```
-a：列出打开文件存在的进程；
-c<进程名>：列出指定进程所打开的文件；
-g：列出GID号进程详情；
-d<文件号>：列出占用该文件号的进程；
+d<目录>：列出目录下被打开的文件；
+D<目录>：递归列出目录下被打开的文件；
-n<目录>：列出使用NFS的文件；
-i<条件>：列出符合条件的进程（协议、:端口  @ip  
-p<进程号>：列出指定进程号所打开的文件；
-u：列出UID号进程详情；
-h：显示帮助信息；
-v：显示版本信息
```

实例

```
lsof
command     PID USER   FD      type             DEVICE     SIZE       NODE
NAME
init          1 root  cwd       DIR                8,2     4096          2 /
init          1 root  rtd       DIR                8,2     4096          2 /
init          1 root  txt       REG                8,2    43496    6121706
/sbin/init
init          1 root  mem       REG                8,2   143600    7823908
/lib64/ld-2.5.so
init          1 root  mem       REG                8,2  1722304    7823915
/lib64/libc-2.5.so
init          1 root  mem       REG                8,2    23360    7823919
/lib64/libdl-2.5.so
init          1 root  mem       REG                8,2    95464    7824116
/lib64/libselinux.so.1
```

```
init          1 root  mem       REG                8,2   247496    7823947
/lib64/libsepol.so.1
init          1 root   10u      FIFO              0,17                1233
/dev/initctl
migration     2 root  cwd       DIR                8,2     4096          2 /
migration     2 root  rtd       DIR                8,2     4096          2 /
migration     2 root  txt   unknown
/proc/2/exe
ksoftirqd     3 root  cwd       DIR                8,2     4096          2 /
ksoftirqd     3 root  rtd       DIR                8,2     4096          2 /
ksoftirqd     3 root  txt   unknown
/proc/3/exe
migration     4 root  cwd       DIR                8,2     4096          2 /
migration     4 root  rtd       DIR                8,2     4096          2 /
migration     4 root  txt   unknown
/proc/4/exe
ksoftirqd     5 root  cwd       DIR                8,2     4096          2 /
ksoftirqd     5 root  rtd       DIR                8,2     4096          2 /
ksoftirqd     5 root  txt   unknown
/proc/5/exe
events/0      6 root  cwd       DIR                8,2     4096          2 /
events/0      6 root  rtd       DIR                8,2     4096          2 /
events/0      6 root  txt   unknown
/proc/6/exe
events/1      7 root  cwd       DIR                8,2     4096          2 /
```

lsof输出各列信息的意义如下：

- COMMAND：进程的名称
- PID：进程标识符
- PPID：父进程标识符（需要指定-R参数）
- USER：进程所有者
- PGID：进程所属组
- FD：文件描述符，应用程序通过文件描述符识别该文件。

文件描述符列表：

1. cwd：表示current work dirctory：即：应用程序的当前工作目录，这是该应用程序启动的目录，除非它本身对这个目录进行更改
2. txt：该类型的文件是程序代码，如应用程序二进制文件本身或共享库，如上列表中显示的 /sbin/init 程序
3. lnn：library references (AIX);
4. er：FD information error (see NAME column);
5. jld：jail directory (FreeBSD);
6. ltx：shared library text (code and data);
7. mxx ：hex memory-mapped type number xx.
8. m86：DOS Merge mapped file;
9. mem：memory-mapped file;
10. mmap：memory-mapped device;
11. pd：parent directory;
12. rtd：root directory;
13. tr：kernel trace file (OpenBSD);

14. v86 VP/ix mapped file;
15. 0：表示标准输出
16. 1：表示标准输入
17. 2：表示标准错误

一般在标准输出、标准错误、标准输入后还跟着文件状态模式：

1. u表示该文件被打开并处于读取/写入模式。
2. r表示该文件被打开并处于只读模式。
3. w表示该文件被打开并处于写入模式。
4. 空格：表示该文件的状态模式为unknow且没有锁定。
5. -：表示该文件的状态模式为unknow且被锁定。

同时在文件状态模式后面，还跟着相关的锁：

1. N for a Solaris NFS lock of unknown type;
2. r for read lock on part of the file;
3. R for a read lock on the entire file;
4. w for a write lock on part of the file;文件的部分写锁）
5. W for a write lock on the entire file;整个文件的写锁）
6. u for a read and write lock of any length;
7. U for a lock of unknown type;
8. x for an SCO OpenServer Xenix lock on part of the file;
9. X for an SCO OpenServer Xenix lock on the entire file;
10. space if there is no lock.

文件类型：

1. DIR表示目录。
2. CHR表示字符类型。
3. BLK块设备类型。
4. UNIX UNIX 域套接字。
5. FIFO先进先出 (FIFO) 队列。
6. IPv4网际协议 (IP) 套接字。
7. DEVICE指定磁盘的名称
8. SIZE文件的大小
9. NODE索引节点（文件在磁盘上的标识）
10. NAME打开文件的确切名称
11. REG常规文件

列出指定进程号所打开的文件:

```
lsof -p $pid
```

获取端口对应的进程ID=>pid

```
lsof -i:9981 -P -t -sTCP:LISTEN
```

列出打开文件的进程:

```
lsof $filename
```