lsof 命令

作者： leolovenet@gmail.com
blog： http://www.leolovenet.com
weibo： http://weibo.com/leolovenet

版本： 0.1

例子：

1. 谁打开了 80 端口 (-i 选项)

    lsof -i :80

2. 谁打开了tcp连接 (-n 选项)

    lsof -ni tcp   不翻译ip的名字

3. httpd进程打开了那些文件 (大写-P选项与小写-p选项)

    lsof -nPp $(pgrep -d, httpd) 大写 -P 不翻译端口的名字，小写 -p 列出某个进程打开的文件

    lsof -nPp $(pidof -s httpd)

    lsof -nPi:80 -p $(pidof httpd -s)

4. 查看TCP状态是CLOSE_WAIT的连接(CentOS5好像不支持) (-s 选项)

    lsof -nPi -sTCP:CLOSE_WAIT

5. 谁打开了某个文件

    lsof /var/log/syslog

6. 谁打开了某个目录 (+D 为递归搜索子目录，+d 只搜索该目录) (-D/d 选项)

    lsof +D /var/log/

7. 列出“这个名字开头”的进程打开的文件（可以多次使用，指定多个名字，也可以单独指定一个名字） (-c 选项)

    lsof -c ssh   列出以ssh开头的进程名打开的文件

    lsof -c ssh -c init 列出以ssh或者init开头的进程名打开的文件

    lsof -c /^.*dog.*$/   列出以进程名中又dog字符的进程，打开的文件。 //之间为正则测试，具体看man

8. 某个用户打开了那些文件，或者 不是那个用户打开的文件列表 (-u 选项)

    lsof -u leo, 或者   lsof -u ^leo

9. 列出 Httpd 开头的进程名，打开的进程 PID (-t 选项)

    lsof -c httpd -t

10. 选项之间默认是 or 关系的，也可以指定 and 关系 (-a 选项)

    lsof -u root -c httpd   将会列出用户名位root，或者，进程名为httpd打开的文件。

lsof -u root -c httpd -a 将会列出用户名位root，并且，进程名为httpd打开的文件。

11. 自动重复执行模式 **(-r/+r 选项)**

lsof -u root -c sshd -a -r5 每隔5秒列出用户root，并且进程名为httpd打开的文件。

lsof -u root -c sshd -a +r5 每隔5秒列出用户root，并且进程名为httpd打开的文件，如果没有打开的文件的话，就不用在循环执行了。

12. 列出所有的 Network File System (NFS) **(-N 选项)**

lsof -N -u leo -a 列出所有用户 leo 打开的网络文件

选项说明:

-n 不翻译地址名字

-P (大) 不翻译端口名字

-p (小) 指定要查看的进程pid，可以同时指定多个，以逗号分隔。

e.g.: -p 120,121,123

-i 指定要查看的端口号。 **e.g.: -i:80**

还可以的格式: **[46][protocol][@hostname|hostaddr][:service|port]**

where:

- **46** specifies the IP version, IPv4 or IPv6 that applies to the following address. '6' may be be specified only if the UNIX dialect supports IPv6. If neither '4' nor '6' is specified, the following address applies to all IP versions.
- **protocol** is a protocol name - TCP, UDP
- **hostname** is an Internet host name. Unless a specific IP version is specified, open network files associated with host names of all versions will be selected.
- **hostaddr** is a numeric Internet IPv4 address in dot form; or an IPv6 numeric address in colon form, enclosed in brackets, if the UNIX dialect supports IPv6. When an IP version is selected, only its numeric addresses may be specified.
- **service** is an /etc/services name - e.g., smtp or a list of them.
- **port** is a port number, or a list of them.

example:

- **-i6** --> IPv6 only
- **TCP:25** --> TCP and port 25
- **@1.2.3.4** --> Internet IPv4 host address 1.2.3.4
- **@[3ffe:1ebc::1]:1234** --> Internet IPv6 host address 3ffe:1ebc::1, port 1234
- **UDP:who** --> UDP who service port
- **TCP@lsof.itap:513** --> TCP, port 513 and host name lsof.itap
- **tcp@foo:1-10,smtp,99** --> TCP, ports 1 through 10, service name smtp, port 99, host name foo
- **tcp@bar:1-smtp** --> TCP, ports 1 through smtp, host bar
- **:time** --> either TCP, UDP or UDPLITE time service port

-s 按照网络状态筛选 (CentOS6才支持,5不支持)

example:

-iTCP -sTCP:LISTEN to list only network files with TCP state **LISTEN**

Some common TCP state names are: CLOSED, IDLE, BOUND, LISTEN, ESTABLISHED, SYN_SENT, SYN_RCDV, ESTABLISHED, CLOSE_WAIT, FIN_WAIT1, CLOSING, LAST_ACK, FIN_WAIT_2, and TIME_WAIT.

-iUDP -sUDP:Idle to list network files with all UDP states except **Idle**

Two common UDP state names are: Unbound and Idle.

-r 重复选项，可以指定重复运行时间。类似watch命令。例如： -r10

输出格式说明:

一般的格式为：

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

大部分都很容易理解，着重说明 FD 和 TYPE

FD – Represents the file descriptor. Some of the values of FDs are,

- **cwd** – Current Working Directory
- **txt** – Text file
- **mem** – Memory mapped file

- **mmap** – Memory mapped device
- **NUMBER** – Represent the actual file descriptor. The character after the number i.e '1u', represents the mode in which the file is opened. r for read, w for write, u for read and write.

TYPE – Specifies the type of the file. Some of the values of TYPEs are,

- **REG** – Regular File
- **DIR** – Directory
- **FIFO** – First In First Out
- **CHR** – Character special file

For a complete list of FD & TYPE, refer man lsof.