lsof 工具

内容提要

1. 熟悉 lsof 的功能
2. 掌握 lsof 命令的使用

lsof 的功能和命令格式

在系统管理中常常用到 lsof 工具，是系统监测工具之一。lsof（list open files）可以用来查看正在运行中的进程打开了哪些文件、目录和套接字。

lsof [http://www.proxyserve.net/index.php?q=aHR0cDovL21hbi5jeC9sc29m] 的命令格式如下：

```
lsof [OPTIONS] [names]
```

lsof 的选项丰富，下面仅列出一些基本的，更多的选项请查阅其手册。

选项	说明
-h	显示使用帮助信息
-a	表示所列出的选项是"与"逻辑，都必须满足时才显示结果
-R	显示进程的 PPID 列
-l	不将 UID 转化为用户登录名
-n	不将 IP 转换为主机名
-P	不将服务端口号转化为服务名称
-u Username/UID	显示由属于指定用户的进程打开的文件
-g gid	显示属于指定组的进程打开的文件
-d FD	显示指定文件描述符（file descriptors）的进程
-c string	显示命令列中包含指定字符串 string 的进程打开的文件
-c /string/	与上面的功能相同，/ / 中可以使用正则表达式
+d Dirname	显示指定目录下被进程打开的文件
+D Dirname	与上面的功能相同，但是会搜索目录下的所有子目录
-i	显示所有网络进程打开的文件

下面着重谈一下 -i 选项，它可跟如下参数进行输出限制：

```
-i [46][protocol][@hostname|hostaddr][:service|port]
```

其中：

- **4** -- IPv4
- **6** -- IPv6
- **protocol** -- TCP 或 UDP
- **hostname** -- 网络主机名
- **hostaddr** -- IP 地址
- **service** -- /etc/service 中的服务名
- **port** -- 服务端口号

下面给出几个使用 -i 选项的例子

- **-i 6** -- 仅限于 IPv6
- **-i TCP:25** -- TCP 且端口号为 25
- **-i @1.2.3.4** -- IPv4 地址为 1.2.3.4
- **-i @[3ffe:1ebc::1]:1234** -- IPv6 地址为 3ffe:1ebc::1，端口号为 1234
- **-i UDP:who** - UDP 协议的 who 服务端口
- **-i TCP@lsof.itap:513** -- TCP 协议的 513 端口，主机名为 lsof.itap

- **-i tcp@foo:1-10,smtp,99** -- TCP 协议的端口 1到10、smtp 服务端口和端口 99，主机名为 foo
- **-i tcp@bar:smtp-nameserver** -- TCP 协议的端口 smtp 到 nameserver, 主机名为 bar
- **-i :time** -- TCP 或 UDP 协议的 time 服务端口

lsof 命令举例

下面给出几个使用举例：

```
# 查看谁在使用指定的文件系统
# lsof /media/cdrom/
COMMAND  PID   USER   FD   TYPE DEVICE SIZE   NODE NAME
bash    8011   root  cwd    DIR  253,0 4096 390146 /media/cdrom/
bash    8536 osmond  cwd    DIR  253,0 4096 390146 /media/cdrom/
```

```
# 显示打开指定文件的所有进程
# lsof /var/log/messages
COMMAND  PID USER   FD   TYPE DEVICE SIZE   NODE NAME
syslogd 2048 root    2w   REG  253,0  108 847031 /var/log/messages
```

```
# 显示由指定用户 osmond 打开的所有文件
# lsof -u osmond
COMMAND  PID   USER   FD   TYPE     DEVICE     SIZE   NODE NAME
sshd    7103 osmond  cwd    DIR      253,0     4096      2 /
sshd    7103 osmond  rtd    DIR      253,0     4096      2 /
bash    7104 osmond  rtd    DIR      253,0     4096      2 /
bash    7104 osmond  cwd    DIR      253,1     4096  63489 /home/osmond
sshd    7103 osmond  txt    REG      253,0   387308 824664 /usr/sbin/sshd
sshd    7103 osmond  mem    REG      253,0   125728 554968 /lib/ld-2.5.so
sshd    7103 osmond  mem    REG      253,0    11460 826459 /usr/lib/libplds4.so
sshd    7103 osmond  DEL    REG        0,8          32290 /dev/zero
sshd    7103 osmond    0u   CHR        1,3           1402 /dev/null
sshd    7103 osmond    3u  IPv6      32264            TCP 192.168.0.101:ssh->192.168.0.77:lontalk-urgnt (ESTABLISHED)
sshd    7103 osmond    4u  unix 0xdc29c200          32295 socket
sshd    7103 osmond    6r  FIFO       0,6          32305 pipe
sshd    7103 osmond    8u   CHR        5,2            693 /dev/ptmx
bash    7104 osmond  txt    REG      253,0   722684  97572 /bin/bash
bash    7104 osmond    0u   CHR      136,0              2 /dev/pts/0
.....
```

```
# 显示指定目录下被进程打开的文件
# lsof +d /var
COMMAND  PID USER   FD   TYPE DEVICE SIZE   NODE NAME
crond   2455 root  cwd    DIR  253,0 4096 845353 /var/spool
```

```
# 显示指定文件描述符的进程（多个FD用逗号间隔）
# lsof -d txt,1
COMMAND    PID      USER   FD      TYPE     DEVICE   SIZE   NODE NAME
init         1      root  txt       REG      253,0  38620 422671 /sbin/init
migration    2      root  txt   unknown                       /proc/2/exe
udevd      441      root  txt       REG      253,0  71928 422820 /sbin/udevd
udevd      441      root    1u      CHR        1,3           1402 /dev/null
acpid     2360      root    1w      REG      253,0   1722 846999 /var/log/acpid
xinetd    2403      root    1r      CHR        1,3           1402 /dev/null
.....
```

```
# 查看属于 root 用户进程所打开的文件描述符为 txt 的文件
# lsof -a -u root -d txt
COMMAND    PID USER  FD      TYPE DEVICE   SIZE   NODE NAME
init         1 root txt       REG  253,0  38620 422671 /sbin/init
migration    2 root txt   unknown                      /proc/2/exe
.....
lsof      8527 root txt       REG  253,0 121396 823819 /usr/sbin/lsof
lsof      8528 root txt       REG  253,0 121396 823819 /usr/sbin/lsof
```

```
# 查看端口号 22 的进程的当前运行情况
# lsof -i :22
COMMAND  PID   USER   FD   TYPE DEVICE SIZE NODE NAME
sshd    2386   root    3u  IPv6   6717       TCP *:ssh (LISTEN)
sshd    7101   root    3u  IPv6  32264       TCP 192.168.0.101:ssh->192.168.0.77:lontalk-urgnt (ESTABLISHED)
sshd    7103 osmond    3u  IPv6  32264       TCP 192.168.0.101:ssh->192.168.0.77:lontalk-urgnt (ESTABLISHED)
sshd    8533   root    3u  IPv6  35679       TCP 192.168.0.101:ssh->192.168.0.77:3998 (ESTABLISHED)
sshd    8535 osmond    3u  IPv6  35679       TCP 192.168.0.101:ssh->192.168.0.77:3998 (ESTABLISHED)
```

```
# 查看包含指定 IP 的进程的当前运行情况
# lsof -i @192.168.0.77
COMMAND  PID   USER   FD   TYPE DEVICE SIZE NODE NAME
sshd    7101   root    3u  IPv6  32264       TCP 192.168.0.101:ssh->192.168.0.77:lontalk-urgnt (ESTABLISHED)
```

```
sshd    7103 osmond    3u  IPv6  32264       TCP 192.168.0.101:ssh->192.168.0.77:lontalk-urgnt (ESTABLISHED)
sshd    8533   root    3u  IPv6  35679       TCP 192.168.0.101:ssh->192.168.0.77:3998 (ESTABLISHED)
sshd    8535 osmond    3u  IPv6  35679       TCP 192.168.0.101:ssh->192.168.0.77:3998 (ESTABLISHED)
```

lsof 的输出项说明

常见的输出项说明：

COMMAND	进程的名称
PID	进程标识符
USER	进程所有者
FD	文件描述符，应用程序通过文件描述符识别该文件
TYPE	文件类型
DEVICE	磁盘的名称
SIZE	文件的大小
NODE	索引节点（文件在磁盘上的标识）
NAME	打开文件的确切名称

常见的文件描述符（file descriptors）：

cwd	程序的当前工作目录
rtd	根目录
txt	程序文本（包括代码和数据）
mem	内存映像文件
n	n为数值，应用程序的文件描述符，这是打开该文件时返回的一个整数。（0 到 2，分别表示标准输入、标准输出和标准错误输出） n 后的 r 表示打开的文件只读；w 表示打开的文件只写；u 表示打开的文件可读写。

常见的文件类型（TYPE）：

REG	普通文件
LINK	符号链接文件
DIR	目录
CHR	字符设备
BLK	块设备
FIFO	先进先出队列
unix	UNIX 域套接字
sock	不可知域套接字
inet	Internet域套接字
IPv4	IPv4 套接字
IPv6	IPv6 网络文件

参考

- http://www.ibm.com/developerworks/cn/linux/l-linux-slab-allocator/ [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy5pYm0uY29tL2RldmVsb3BlcndvcmtzL2NuL2xpbnV4L2wtbGludXgtc2xhYi1hbGxvY2F0b3Iv]
- 显示源文件
- 登录