[**每天一个Linux命令（45）lsof命令**](http://www.cnblogs.com/MenAngel/p/5575479.html)

**lsof命令用于查看你进程打开的文件，端口(TCP、UDP)，找回/恢复删除的文件，打开文件的进程。**

**(1)用法:**

**用法:**  lsof  [参数]  [文件]

**(2)功能:**

**功能:**  lsof 命令可显示系统打开的文件.(因为 lsof 需要访问核心内存和各种文件，所以必须以 root 用户的身份运行它才能够充分地发挥其功能。)

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。

**(3)选项参数:**

1) +D<目录>  　　　　递归列出目录下被打开的文件

2) -u s 　　　　　　　 列出login name或UID为 s的程序

3) -c<进程名> 　　　  列出指定进程所打开的文件

4) -i<条件>  　　　　  列出符合条件的进程。（4、6、协议、:端口、 @ip ）

5) -n 　　　　　　　　 -n<目录>  列出使用NFS的文件

**(4)实例:**

1)[sunjimeng@localhost ~]$ lsof |more -20

无任何参数，显示当前系统已经打开的正在使用的所有文件

[sunjimeng@localhost ~]$ lsof |more -20

COMMAND PID TID USER FD TYPE DEVICE SIZE/OFF NODE NAME  
进程名称 标志符 线程id 所有者 文件描述符 文件类型 磁盘名称 文件大小 索引节点 文件名称

Systemd 1 root cwd unknown /proc/1/cwd (readlink: Permission denied)

systemd 1 root rtd unknown /proc/1/root (readlink: Permission denied)

systemd 1 root txt unknown /proc/1/exe (readlink: Permission denied)

systemd 1 root NOFD /proc/1/fd (opendir: Permission denied)

kthreadd 2 root cwd unknown /proc/2/cwd (readlink: Permission denied)

kthreadd 2 root rtd unknown /proc/2/root (readlink: Permission denied)

kthreadd 2 root txt unknown /proc/2/exe (readlink: Permission denied)

kthreadd 2 root NOFD /proc/2/fd (opendir: Permission denied)

ksoftirqd 3 root cwd unknown /proc/3/cwd (readlink: Permission denied)

ksoftirqd 3 root rtd unknown /proc/3/root (readlink: Permission denied)

ksoftirqd 3 root txt unknown /proc/3/exe (readlink: Permission denied)

ksoftirqd 3 root NOFD /proc/3/fd (opendir: Permission denied)

kworker/0 5 root cwd unknown /proc/5/cwd (readlink: Permission denied)

kworker/0 5 root rtd unknown /proc/5/root (readlink: Permission denied)

kworker/0 5 root txt unknown /proc/5/exe (readlink: Permission denied)

kworker/0 5 root NOFD /proc/5/fd (opendir: Permission denied)

migration 7 root cwd unknown /proc/7/cwd (readlink: Permission denied)

migration 7 root rtd unknown /proc/7/root (readlink: Permission denied) //是根目录到软连接

migration 7 root txt unknown /proc/7/exe (readlink: Permission denied)

--More--

FW的详解:

1)cwd(current work dirctory): 应用程序的当前工作目录，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

3)rtd: root directory

4)0: 表示标准输出

5)1: 表示标准输入

6)2: 表示标准错误

TYPE：文件类型，如DIR、REG等，常见的文件类型:

（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

DEVICE：指定磁盘的名称

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

2)[root@localhost root]# lsof /bin/bash

查看与指定文件相关的进程的信息，即找出使用此文件的进程

[root@localhost root]# lsof /bin/bash

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

ksmtuned 807 root txt REG 8,3 960384 34340720 /usr/bin/bash

bash 35234 sunjimeng txt REG 8,3 960384 34340720 /usr/bin/bash

bash 38651 root txt REG 8,3 960384 34340720 /usr/bin/bash

3)[root@localhost /]# lsof +D /home/sunjimeng/.local/share

递归查看某个目录的文件信息

[root@localhost /]# lsof +D /home/sunjimeng/.local/share

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

nautilus 3387 sunjimeng mem REG 8,3 32768 71239928 /home/sunjimeng/.local/share/gvfs-metadata/home-ddf07f21.log

nautilus 3387 sunjimeng mem REG 8,3 764 71239927 /home/sunjimeng/.local/share/gvfs-metadata/home

nautilus 3387 sunjimeng 15r REG 8,3 764 71239927 /home/sunjimeng/.local/share/gvfs-metadata/home

nautilus 3387 sunjimeng 16r REG 8,3 32768 71239928 /home/sunjimeng/.local/share/gvfs-metadata/home-ddf07f21.log

evolution 3426 sunjimeng 11u REG 8,3 14336 104003229 /home/sunjimeng/.local/share/evolution/addressbook/system/contacts.db

tracker-s 3447 sunjimeng 15w REG 8,3 210635 71234252 /home/sunjimeng/.local/share/tracker/data/tracker-store.journal

4)[root@localhost dir1]# lsof |grep '/home/sunjimeng/Document/dir1'

不用+D参数得到与某个文件有关的进程信息的方法

[root@localhost dir1]# lsof +D /home/sunjimeng/Document/dir1

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

bash 38651 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

lsof 41562 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

lsof 41563 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

[root@localhost dir1]# lsof |grep '/home/sunjimeng/Document/dir1'

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

bash 38651 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

lsof 41628 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

grep 41629 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

lsof 41630 root cwd DIR 8,3 30 36004773 /home/sunjimeng/Document/dir1

5)[root@localhost /]# lsof -u sunjimeng |more -20

列出某个用户打开的所有文件相关的进程信息

[root@localhost /]# lsof -u sunjimeng |more -20

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

gnome-key 2967 sunjimeng cwd DIR 8,3 6 71227180 /var/gdm

gnome-key 2967 sunjimeng rtd DIR 8,3 4096 128 /

gnome-key 2967 sunjimeng txt REG 8,3 1038688 35649707 /usr/bin/gnome-keyring-daemon

gnome-key 2967 sunjimeng mem REG 8,3 50496 68402049 /usr/lib64/gio/modules/libdconfsettings.so

gnome-key 2967 sunjimeng mem REG 8,3 106065056 34340715 /usr/lib/locale/locale-archive

gnome-key 2967 sunjimeng mem REG 8,3 153184 67393930 /usr/lib64/liblzma.so.5.0.99

gnome-key 2967 sunjimeng mem REG 8,3 398272 67393933 /usr/lib64/libpcre.so.1.2.0

gnome-key 2967 sunjimeng mem REG 8,3 44088 67328582 /usr/lib64/librt-2.17.so

gnome-key 2967 sunjimeng mem REG 8,3 110808 67328580 /usr/lib64/libresolv-2.17.so

gnome-key 2967 sunjimeng mem REG 8,3 147120 67393944 /usr/lib64/libselinux.so.1

gnome-key 2967 sunjimeng mem REG 8,3 90632 67393947 /usr/lib64/libz.so.1.2.7

gnome-key 2967 sunjimeng mem REG 8,3 32296 67394691 /usr/lib64/libffi.so.6.0.1

gnome-key 2967 sunjimeng mem REG 8,3 15616 67394699 /usr/lib64/libgmodule-2.0.so.0.4000.0

gnome-key 2967 sunjimeng mem REG 8,3 2107760 67328552 /usr/lib64/libc-2.17.so

gnome-key 2967 sunjimeng mem REG 8,3 141616 67328578 /usr/lib64/libpthread-2.17.so

gnome-key 2967 sunjimeng mem REG 8,3 19736 67394316 /usr/lib64/libcap-ng.so.0.0.0

gnome-key 2967 sunjimeng mem REG 8,3 19384 67394141 /usr/lib64/libgpg-error.so.0.10.0

gnome-key 2967 sunjimeng mem REG 8,3 19512 67328558 /usr/lib64/libdl-2.17.so

gnome-key 2967 sunjimeng mem REG 8,3 534488 67394280 /usr/lib64/libgcrypt.so.11.8.2

--More--

6)[root@localhost /]# lsof -c sleep　　　　　　　　列出与程序有关的文件

[root@localhost /]# lsof -c sleep

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

sleep 42253 root cwd DIR 8,3 4096 128 /

sleep 42253 root rtd DIR 8,3 4096 128 /

sleep 42253 root txt REG 8,3 33088 34268435 /usr/bin/sleep

sleep 42253 root mem REG 8,3 106065056 34340715 /usr/lib/locale/locale-archive

sleep 42253 root mem REG 8,3 2107760 67328552 /usr/lib64/libc-2.17.so

sleep 42253 root mem REG 8,3 164336 67328545 /usr/lib64/ld-2.17.so

sleep 42253 root 0r CHR 1,3 0t0 1045 /dev/null

sleep 42253 root 1u unix 0xffff880080995a00 0t0 18112 socket

sleep 42253 root 2u unix 0xffff880080995a00 0t0 18112 socket

[root@localhost /]# lsof |grep sleep //等价

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

sleep 42993 root cwd DIR 8,3 4096 128 /

sleep 42993 root rtd DIR 8,3 4096 128 /

sleep 42993 root txt REG 8,3 33088 34268435 /usr/bin/sleep

sleep 42993 root mem REG 8,3 106065056 34340715 /usr/lib/locale/locale-archive

sleep 42993 root mem REG 8,3 2107760 67328552 /usr/lib64/libc-2.17.so

sleep 42993 root mem REG 8,3 164336 67328545 /usr/lib64/ld-2.17.so

sleep 42993 root 0r CHR 1,3 0t0 1045 /dev/null

sleep 42993 root 1u unix 0xffff880080995a00 0t0 18112 socket

sleep 42993 root 2u unix 0xffff880080995a00 0t0 18112 socket

7)[root@localhost /]# lsof -i　　　　　　列出所有的网络连接

[root@localhost /]# lsof -i

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

chronyd 787 chrony 1u IPv4 16222 0t0 UDP \*:ntp

chronyd 787 chrony 2u IPv6 16223 0t0 UDP \*:ntp

chronyd 787 chrony 3u IPv4 16224 0t0 UDP localhost:323

chronyd 787 chrony 5u IPv6 16225 0t0 UDP localhost:323

avahi-dae 790 avahi 12u IPv4 17290 0t0 UDP \*:mdns

avahi-dae 790 avahi 13u IPv4 17291 0t0 UDP \*:44093

sshd 1282 root 3u IPv4 20803 0t0 TCP \*:ssh (LISTEN)

sshd 1282 root 4u IPv6 20805 0t0 TCP \*:ssh (LISTEN)

master 2527 root 13u IPv4 22473 0t0 TCP localhost:smtp (LISTEN)

master 2527 root 14u IPv6 22474 0t0 TCP localhost:smtp (LISTEN)

cupsd 3269 root 11u IPv6 27563 0t0 TCP localhost:ipp (LISTEN)

cupsd 3269 root 12u IPv4 27564 0t0 TCP localhost:ipp (LISTEN)

列出使用指定协议的网络连接：

[root@localhost /]# lsof -i TCP

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

sshd 1282 root 3u IPv4 20803 0t0 TCP \*:ssh (LISTEN)

sshd 1282 root 4u IPv6 20805 0t0 TCP \*:ssh (LISTEN)

master 2527 root 13u IPv4 22473 0t0 TCP localhost:smtp (LISTEN)

master 2527 root 14u IPv6 22474 0t0 TCP localhost:smtp (LISTEN)

cupsd 3269 root 11u IPv6 27563 0t0 TCP localhost:ipp (LISTEN)

cupsd 3269 root 12u IPv4 27564 0t0 TCP localhost:ipp (LISTEN)

8)[root@localhost /]# lsof -n /home/sunjimeng

列出指定目录下使用NFS文件系统的所有文件

[root@localhost /]# lsof -n /home/sunjimeng

lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs

Output information may be incomplete.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

gnome-ses 2990 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

gnome-set 3168 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

gnome-she 3265 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

gsd-print 3282 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

nautilus 3387 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

vmtoolsd 3435 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

tracker-m 3442 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

tracker-s 3447 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

abrt-appl 3450 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

top 15226 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

gnome-ter 35226 sunjimeng cwd DIR 8,3 4096 137 /home/sunjimeng

**(5)其他:**

lsof可以打开的文件的类型:

1.普通文件

2.目录

3.网络文件系统的文件

4.字符或设备文件

5.(函数)共享库

6.管道，命名管道

7.符号链接

8.网络文件（例如：NFS file、网络socket，unix域名socket）

9.还有其它类型的文件，等等。