

简单，可复制
点点滴滴，尽在文中

公告

史上最好用的免费翻墙利器

小团队的免费svn空间

昵称：[ggjucheng](#)
 园龄：5年4个月
 粉丝：1188
 关注：6
[+加关注](#)

博客地图

- [c/c++笔记](#)
- 本人学习c/c++的一些笔记
- [db笔记](#)
- [mysql nosql](#)
- [hadoop笔记](#)
- 本人工作中hadoop的心得
- [internet笔记](#)
- [互联网学习笔记](#)
- [java笔记](#)
- [java平台笔记](#)
- [Linux/Unix笔记](#)
- 本人学习linux/unix的笔记
- [TCP/IP笔记](#)
- 本人学习TCP/IP的心得和笔记
- [web开发](#)
- [html css js php etc.....](#)
- [技术花絮](#)
- 非技术的技术
- [其他笔记本](#)
- 比较零碎的技术文章归类
- [学习指南](#)
- IT技术学习路线,IT经典书籍学习和下载

友情链接

- [IT短篇笑话](#)
- 百忙中，可以看看it短篇笑话，笑一笑，放松下！
- [挺不错的免费svn空间](#)
- 国内挺不错的svn免费空间，很适合小团队使用
- [相当好用的免费翻墙利器](#)
- 相当好用的免费翻墙利器,程序员居家必用

积分与排名

linux lsof命令详解


简介

lsof(list open files)是一个列出当前系统打开文件的工具。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。

输出信息含义

在终端下输入lsof即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 用户的身份运行它能够充分地发挥其功能。

直接输入lsof部分输出为：



COMMAND	PID	USER	FD	TYPE	DEVICE
SIZE/OFF	NODE NAME				
init	1	root	cwd	DIR	8,1
4096	2	/			
init	1	root	rtd	DIR	8,1
4096	2	/			
init	1	root	txt	REG	8,1
150584	654127	/sbin/init			
udev	415	root	0u	CHR	1,3
0t0	6254	/dev/null			
udev	415	root	1u	CHR	1,3
0t0	6254	/dev/null			
udev	415	root	2u	CHR	1,3
0t0	6254	/dev/null			
udev	690	root	mem	REG	8,1
51736	302589	/lib/x86_64-linux-gnu/libnss_files-2.13.so			
syslog	1246	syslog	2w	REG	8,1
10187	245418	/var/log/auth.log			
syslog	1246	syslog	3w	REG	8,1
10118	245342	/var/log/syslog			
dd	1271	root	0r	REG	0,3
0	4026532038	/proc/kmsg			
dd	1271	root	1w	FIFO	0,15
0t0	409	/run/klogd/kmsg			
dd	1271	root	2u	CHR	1,3
0t0	6254	/dev/null			

积分 - 983209
排名 - 64

最新评论

1. Re:mysql load操作

自己找到方法了。。。LOAD DATA LOCAL INFILE
'/home/dev/t_active_device.20170508.sql' INTO TABLE clientType_lic.....

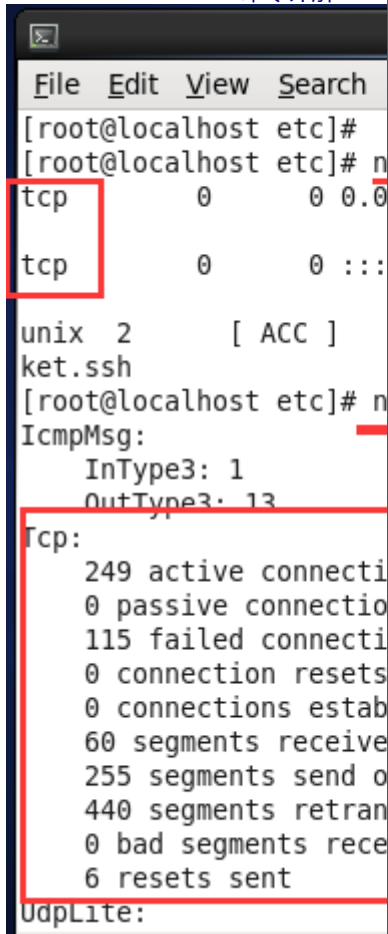
--豪放婉约派程序员

2. Re:mysql load操作

楼主你好。为什么指定列之后就不能加分隔符了？比如以下这句无法执行：LOAD DATA LOCAL INFILE
'/home/dev/t_active_device.20170508.sql' INT.....

--豪放婉约派程序员

3. Re:Linux netstat命令详解



```
[root@localhost etc]# netstat -t
tcp        0      0 0.0.0.0:0          0.0.0.0:0          LISTENING
tcp        0      0 0.0.0.0:0          0.0.0.0:0          LISTENING

unix 2      [ ACC ]
ket.ssh
[root@localhost etc]# netstat -u
IcmpMsg:
  InType3: 1
  OutType3: 13

tcp:
  249 active connections
  0 passive connections
  115 failed connections
  0 connection resets
  0 connections established
  60 segments received
  255 segments sent
  440 segments retransmitted
  0 bad segments received
  6 resets sent

udpLite:
```

--Elsa-软件测试工程师

4. Re:Linux netstat命令详解

GOOD THX

--唔知叫咩名

5. Re:JAVA正则表达式: Pattern类与Matcher类详解(转)

```
Pattern
p=Pattern.compile("\\d+");
Matcher
m=p.matcher("aaa2223bb");
m.find();//匹配2223
m.start();//返.....
```

--悟空代码

阅读排行榜

1. linux awk命令详解(870166)



每行显示一个打开的文件，若不指定条件默认将显示所有进程打开的所有文件。

lsof输出各列信息的意义如下：

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。如cwd、txt等 TYPE：文件类型，如DIR、REG等

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

FD 列中的文件描述符cwd 值表示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，txt 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。

其次数值表示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。如上的最后一行文件/dev/initctl，其文件描述符为 10。u 表示该文件被打开并处于读取/写入模式，而不是只读 (r) 或只写 (w) 模式。同时还有大写 的W 表示该应用程序具有对整个文件的写锁。该文件描述符用于确保每次只能打开一个应用程序实例。初始打开每个应用程序时，都具有三个文件描述符，从 0 到 2，分别表示标准输入、输出和错误流。所以大多数应用程序所打开的文件的 FD 都是从 3 开始。

与 FD 列相比，Type 列则比较直观。文件和目录分别称为 REG 和 DIR。而CHR 和 BLK，分别表示字符和块设备；或者 UNIX、FIFO 和 IPv4，分别表示 UNIX 域套接字、先进先出 (FIFO) 队列和网际协议 (IP) 套接字。

常用参数

lsof语法格式是：

lsof [options] filename



lsof abc.txt 显示开启文件abc.txt的进程

lsof -c abc 显示abc进程现在打开的文件

lsof -c -p 1234 列出进程号为1234的进程所打开的文件

lsof -g gid 显示归属gid的进程情况

lsof +d /usr/local/ 显示目录下被进程开启的文件

lsof +D /usr/local/ 同上，但是会搜索目录下的目录，时间较长

lsof -d 4 显示使用fd为4的进程

lsof -i 用以显示符合条件的进程情况

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

46 --> IPv4 or IPv6

protocol --> TCP or UDP

hostname --> Internet host name

hostaddr --> IPv4地址

service --> /etc/service中的 service name (可以不止一个)

port --> 端口号 (可以不止一个)

2. Linux tcpdump命令详解(577586)
3. Linux netstat命令详解(413642)
4. linux grep命令详解(295262)
5. Linux GCC常用命令(266891)

评论排行榜

1. linux awk命令详解(29)
2. Linux tcpdump命令详解(24)
3. Linux netstat命令详解(21)
4. Linux入门——适合初学者(19)
5. Linux GCC常用命令(18)

推荐排行榜

1. linux awk命令详解(91)
2. Linux tcpdump命令详解(54)
3. Linux netstat命令详解(47)
4. Linux GCC常用命令(46)
5. Linux入门——适合初学者(39)



lsof使用实例

查找谁在使用文件系统

在卸载文件系统时，如果该文件系统中有任何打开的文件，操作通常将会失败。那么通过lsof可以找出那些进程在使用当前要卸载的文件系统，如下：

```
# lsof /GTES11/  
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME  
bash 4208 root cwd DIR 3,1 4096 2 /GTES11/  
vim 4230 root cwd DIR 3,1 4096 2 /GTES11/
```

在这个示例中，用户root正在其/GTES11目录中进行一些操作。一个 bash是实例正在运行，并且它当前的目录为/GTES11，另一个则显示的是vim正在编辑/GTES11下的文件。要成功地卸载/GTES11，应该在通知用户以确保情况正常之后，中止这些进程。这个示例说明了应用程序的当前工作目录非常重要，因为它仍保持着文件资源，并且可以防止文件系统被卸载。这就是为什么大部分守护进程（后台进程）将它们的目录更改为根目录、或服务特定的目录（如 sendmail 示例中的 /var/spool/mqueue）的原因，以避免该守护进程阻止卸载不相关的文件系统。

恢复删除的文件

当Linux计算机受到入侵时，常见的情况是日志文件被删除，以掩盖攻击者的踪迹。管理错误也可能导致意外删除重要的文件，比如在清理旧日志时，意外地删除了数据库的活动事务日志。有时可以通过lsof来恢复这些文件。

当进程打开了某个文件时，只要该进程保持打开该文件，即使将其删除，它依然存在于磁盘中。这意味着，进程并不知道文件已经被删除，它仍然可以向打开该文件时提供给它的文件描述符进行读取和写入。除了该进程之外，这个文件是不可见的，因为已经删除了其相应的目录索引节点。

在/proc 目录下，其中包含了反映内核和进程树的各种文件。/proc目录挂载的是在内存中所映射的一块区域，所以这些文件和目录并不存在于磁盘中，因此当我们对这些文件进行读取和写入时，实际上是在从内存中获取相关信息。大多数与 lsof 相关的信息都存储于以进程的 PID 命名的目录中，即 /proc/1234 中包含的是 PID 为 1234 的进程的信息。每个进程目录中存在着各种文件，它们可以使得应用程序简单地了解进程的内存空间、文件描述符列表、指向磁盘上的文件的符号链接和其他系统信息。lsof 程序使用该信息和其他关于内核内部状态的信息来产生其输出。所以lsof 可以显示进程的文件描述符和相关的文件名等信息。也就是我们通过访问进程的文件描述符可以找到该文件的相关信息。

当系统中的某个文件被意外地删除了，只要这个时候系统中还有进程正在访问该文件，那么我们就可以通过lsof从/proc目录下恢复该文件的内容。假如由于误操作将/var/log/messages文件删除掉了，那么这时要将/var/log/messages文件恢复的方法如下：

首先使用lsof来查看当前是否有进程打开/var/log/messages文件，如下：

```
# lsof |grep /var/log/messages  
syslogd 1283 root 2w REG 3,3 5381017 1773647 /var/log/messages  
(deleted)
```

从上面的信息可以看到 PID 1283 (syslogd) 打开文件的文件描述符为 2。同时还可以看到/var/log/messages已经标记被删除了。因此我们可以在

/proc/1283/fd/2 (fd下的每个以数字命名的文件表示进程对应的文件描述符) 中查看相应的信息, 如下:

```
# head -n 10 /proc/1283/fd/2
```

```
Aug 4 13:50:15 holmes86 syslogd 1.4.1: restart.
```

```
Aug 4 13:50:15 holmes86 kernel: klogd 1.4.1, log source =  
/proc/kmsg started.
```

```
Aug 4 13:50:15 holmes86 kernel: Linux version 2.6.22.1-8
```

```
(root@everestbuilder.linux-ren.org) (gcc version 4.2.0) #1 SMP Wed
```

```
Jul 18 11:18:32 EDT 2007 Aug 4 13:50:15 holmes86 kernel: BIOS-
```

```
provided physical RAM map: Aug 4 13:50:15 holmes86 kernel: BIOS-  
e820: 0000000000000000 - 00000000000009f000 (usable) Aug 4
```

```
13:50:15 holmes86 kernel: BIOS-e820: 00000000000009f000 -
```

```
000000000000a0000 (reserved) Aug 4 13:50:15 holmes86 kernel:
```

```
BIOS-e820: 00000000000100000 - 0000000001f7d3800 (usable) Aug 4
```

```
13:50:15 holmes86 kernel: BIOS-e820: 0000000001f7d3800 -
```

```
00000000020000000 (reserved) Aug 4 13:50:15 holmes86 kernel:
```

```
BIOS-e820: 000000000e0000000 - 00000000f0007000 (reserved) Aug 4
```

```
13:50:15 holmes86 kernel: BIOS-e820: 00000000f0008000 -
```

```
00000000f000c000 (reserved)
```

从上面的信息可以看出, 查看 /proc/8663/fd/15 就可以得到所要恢复的数据。

如果可以通过文件描述符查看相应的数据, 那么就可以使用 I/O 重定向将其复制到文件中, 如:

```
cat /proc/1283/fd/2 > /var/log/messages
```

对于许多应用程序, 尤其是日志文件和数据库, 这种恢复删除文件的方法非常有用。

实用命令



```
lsof `which httpd` //那个进程在使用apache的可执行文件  
lsof /etc/passwd //那个进程在占用/etc/passwd  
lsof /dev/hda6 //那个进程在占用hda6  
lsof /dev/cdrom //那个进程在占用光驱  
lsof -c sendmail //查看sendmail进程的文件使用情况  
lsof -c courier -u ^zahn //显示出那些文件被以courier打头的进程打开, 但是并不属于用户zahn  
lsof -p 30297 //显示那些文件被pid为30297的进程打开  
lsof -D /tmp 显示所有在/tmp文件夹中打开的instance和文件的进程。但是symbol文件并不在列  
  
lsof -u1000 //查看uid是100的用户的进程的文件使用情况  
lsof -utony //查看用户tony的进程的文件使用情况  
lsof -u^tony //查看不是用户tony的进程的文件使用情况 (^是取反的意思)  
lsof -i //显示所有打开的端口  
lsof -i:80 //显示所有打开80端口的进程  
lsof -i -U //显示所有打开的端口和UNIX domain文件  
lsof -i UDP@[url]www.akadia.com:123 //显示那些进程打开了到www.akadia.com的UDP的123(ntp)端口的链接  
lsof -i tcp@ohaha.ks.edu.tw:ftp -r //不断查看目前ftp连接的情况(-r, lsof会永远不断的执行, 直到收到中断信号, +r, lsof会一直执行, 直到没有档案被显示, 缺省是15s刷新)  
lsof -i tcp@ohaha.ks.edu.tw:ftp -n //lsof -n 不将IP转换为hostname, 缺省是不加上-n参数
```



分类: [Linux/Unix](#)

标签: [Linux/Unix_性能](#)

好文要顶

关注我

收藏该文

ggjucheng

关注 - 6

粉丝 - 1188

11

0

+加关注

« 上一篇 : [Linux free命令详解\(转\)](#)
» 下一篇 : [Linux netstat命令详解](#)

posted on 2012-01-08 20:45 [ggjucheng](#) 阅读(116135) 评论(6) [编辑](#) [收藏](#)

评论

- #1楼 2014-09-16 16:46 唔知叫咩名

唔错。

支持(0) 反对(0)
- #2楼 2016-10-13 20:57 不愿透露姓氏的高先生

很好,学习了

支持(0) 反对(0)
- #3楼 2017-01-18 00:35 沙漠金子

Aug 4 13:50:15 holmes86 syslogd 1.4.1: restart.

Aug 4 13:50:15 holmes86 kernel: klogd 1.4.1, log source = /proc/kmsg started.

Aug 4 13:50:15 holmes86 kernel: Linux version 2.6.22.1-8 (root@everestbuilder.linux-ren.org) (gcc version 4.2.0) #1 SMP Wed Jul 18 11:18:32 EDT 2007

Aug 4 13:50:15 holmes86 kernel: BIOS-provided physical RAM map:

Aug 4 13:50:15 holmes86 kernel: BIOS-e820: 0000000000000000 - 00000000000009f000 (usable)

Aug 4 13:50:15 holmes86 kernel: BIOS-e820: 00000000000009f000 - 000000000000a0000 (reserved)

Aug 4 13:50:15 holmes86 kernel: BIOS-e820: 00000000000100000 - 0000000001f7d3800 (usable)

Aug 4 13:50:15 holmes86 kernel: BIOS-e820: 0000000001f7d3800 - 00000000020000000 (reserved)

Aug 4 13:50:15 holmes86 kernel:

BIOS-e820: 00000000e0000000 - 00000000f0007000 (reserved) Aug 4 13:50:15 holmes86 kernel: BIOS-e820: 00000000f0008000 - 00000000f000c000 (reserved)

从上面的信息可以看出，查看 /proc/8663/fd/15 就可以得到所要恢复的数据

博主：您好，请问上面的内容 为什么查看 /proc/8663/fd/15 就可以得到所要恢复的数据 ？？

支持(0) 反对(0)

#4楼 2017-02-06 10:59 freedom_dog

@ 沙漠金子

写错了，应该是/proc/8663/fd/2

支持(0) 反对(0)

#5楼 2017-03-14 15:50 一头奔跑的猪

这个回复删除文件的方法真的很牛叉

支持(0) 反对(0)

#6楼 2017-03-17 16:04 SupremeHover

剽窃别人文章的小偷

支持(0) 反对(0)

[刷新评论](#) [刷新页面](#) [返回顶部](#)

注册用户登录后才能发表评论，请 [登录](#) 或 [注册](#)，[访问网站首页](#)。

【推荐】50万行VC++源码：大型组态工控、电力仿真CAD与GIS源码库

【推荐】中铁、中石油等大型企业的复杂报表解决方案

【活动】阿里云海外云服务全面降价助力企业全球布局

【实用】40+篇云服务器操作及运维基础知识！

**最新IT新闻:**

- Windows 10可三步重回经典XP系统外观 免安装主题
- Mozilla发起Paperstorm活动要求版权改革来挽救互联网
- 微软发布恶意软件防护引擎更新：修复“糟糕透顶”的安全漏洞
- 阿里钉钉发布M1智能考勤机：手机极速打卡神器/299元
- 映客“卖身”宣亚的待解之谜：是否牵涉借壳？

» 更多新闻...

**最新知识库文章:**

- 唱吧DevOps的落地，微服务CI/CD的范本技术解读
- 程序员，如何从平庸走向理想？
- 我为什么鼓励工程师写blog
- 怎么轻松学习JavaScript
- 如何打好前端游击战

» 更多知识库文章...

Powered by:

博客园

Copyright © ggjucheng