系统管理

一、进程管理

1、进程管理简介

2、进程管理的查看

3、杀死进程

4、修改进程优先级

二、工作管理

1、工作管理简介

2、工作管理方法

3、后台命令脱离登录终端执行

三、系统资源查看

四、系统定时任务

**进程管理**

1. ***进程管理简介***

进程是正在执行的一个程序或命令，每一个进程都是一运行的实体都要自己的地址空间，并占用一定的系统资源。简言之，进程就是正在执行的程序或命令，程序运行过程中会占用一定的资源。

一个简单的命令，例如ls，和一个服务例如httpd，都属于进程，不同的是服务的进程会常驻内存当中，等待被访问。所有的程序，只要运行，都会产生一系列的进程，每当有一个客户端连接我的服务时，就会多产生一个进程。Apache默认并发连接数是400，我们可以改到2048，因此httpd服务最多可以产生两千多个进程并发。

**进程管理的作用：<按优先级排列>**

a> 判断服务器的健康状态

b> 查看系统中所有进程

c> 杀死进程

当发现某一进程CPU占用率很高，导致服务器接近死机，我们不可以直接杀死程序，所有程序都有正确的结束方式，直接杀死进程是在正确关闭服务功能不起作用的时候，被迫采用的手段。

如果是系统的合理进程占用了大量的资源，我们不可以直接杀死进程，这样容易使服务器直接down掉，我们需要考题提升服务器性能，CPU性能不足，可以考虑增加服务器个数，建立集群。如果是某个非法进程在耗费服务器资源，我们也不可以直接杀死进程，因为直接杀死进程，并不会彻底阻止该进程重新启动，因此，需要彻底清除该程序之后，才允许杀死进程。

终止进程是进程管理当中最不重要的方法。

1. ***进程管理的查看***

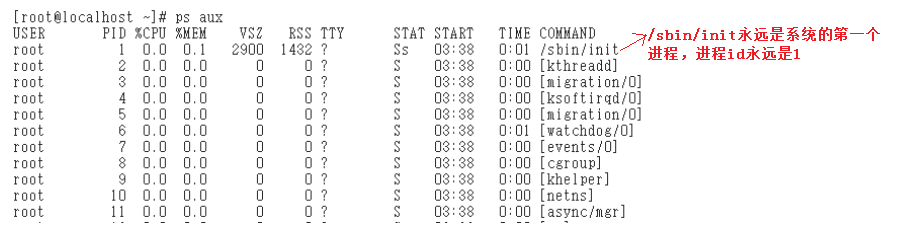
a> ps 和 pstree命令。

ps aux #查看系统中所有进程，使用BSD操作系统格式

ps -le #查看系统中所有进程，使用Linux标准命令格式

选项：

-a ：显示一个终端的多有进程，除了会话引线



/sbin/init是所有进程的父进程，PID在1000以内的均为系统默认的系统进程

ps命令的输出解释：

USER：该进程是由哪个用户产生的

PID：该进程的ID号

%CPU：该进程占用CPU资源的百分比，占用越高，进程越耗费资源

%MEM：该进程占用物理内存的百分比，占用越高，进程越耗费资源

VSZ：该进程占用虚拟内存的大小，单位KB

RSS：该进程占用实际物理内存的大小，单位KB

TTY：该进程是哪个终端中运行的。Tty1-tty7代表本地控制台终端，tty1-tty6时本地的字符界面终端，tty7是图形终端，pts/0-255代表虚拟终端。？表示进程不是由用户通过终端启动的，而是由内核直接启动的服务。

STAT：进程状态---- >R<运行>、S<睡眠>、T<停止状态>、s<包含子进程>、+<位于后台>

START：该进程的启动时间

TIME：该进程占用CPU的运算时间，不是系统时间

COMMAND：进程名

pstree #查看进程树

选项： -p：显示进程的PID

-u：显示进程的所属用户

top #检查系统的健康状况

选项： -d：指定投票命令每隔几秒更新一次，默认3 秒，Windows每1秒刷新

-b：使用批处理模式输出，一般和”-n”合用

-n：次数，指定投票命令执行的次数，一般和”-b”选项合用

在top命令的交互模式当中可以执行的命令：

？或h：显示交互模式的帮助

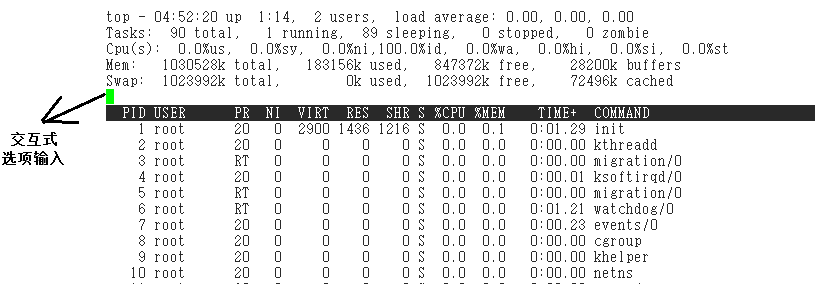
P :以CPU使用率排序，与Windows相同，默认此项

M：以内存的使用率排序

N：以PID排序

q：退出top

top -b -n 1 > top.log #将所有进程信息放到日志文件中。



我们可以通过最上方五行信息来判断服务器的健康状况。

**第一行：任务队列信息**

|  |  |
| --- | --- |
| 内容 | 说明 |
| 04:52:20 | 系统当前时间 |
| up 1:14 | 系统运行时间 |
| 2 users | 当前登录了两个用户 |
| Load average：0.00,0.00，0.00 | 系统在之前的1分钟，5分钟，15分钟的平均负载。一般认为负载小于核数时，负载较小。大于核数，表示系统已经超出负载。 |

运维服务器的目的是不让服务器出问题，让用户可以正常的访问服务器。服务器间隔重启的时间越长，服务器出现问题的可能越大，因为缓存和临时文件无法下自动清除，即使Linux要比Windows稳定，但这也是不可避免的。服务器追求的无故障率，而不是系统持续运行时间。

服务器长时间不用重启，并不代表服务器没有问题，相反，服务器需要定时重启。高压力服务器，例如网络游戏都有定是维护时间，一般一周一次，让服务器重启，使状态归零。低压力服务器一般也需要一月重启一次，保证系统稳定。

关于平均负载，一般情况下，不能大于核数。如果平均负载大于核数，但各项指标均再可以接受的范围内，例如内存占用达到70%，CPU占用率达到60%~70%，可以不进行处理。因此，平均负载只是一个经验值。

**第二行：进程信息**

|  |  |
| --- | --- |
| 内容 | 说明 |
| Tasks: 90total | 系统中的进程总数 |
| 1 running | 正在运行的进程数 |
| 89 sleeping | 睡眠的进程 |
| 0 stopped | 正在停止的进程 |
| 0 zombie | 僵尸<僵死>进程。如果不是0，需要手工检查僵尸进程 |

如果关闭了父进程，子进程应该也相应关闭。换句话说，有时候我们运行某些程序，需要用到底层进程的支持，例如显卡等，当我们把显卡卸载掉之后，理论上我们正在运行的程序也会关闭。但某些特殊情况，我们关闭掉依赖进程之后，子进程没有正常关闭，也不能正常运行，而是卡在了系统当中，一般不会出现僵尸进程。如果某个进程长期存在，没有自动关闭，如果该进程并不是特别重要，可以选择杀死进程。

**第三行：CPU信息**

|  |  |
| --- | --- |
| 内容 | 说明 |
| Cpu(s): 0.0%us | 用户模式占用的CPU百分比 |
| 0.0%sy | 系统模式占用的CPU百分比 |
| 0.0%ni | 改变过优先级的用户进程占用的CPU百分比 |
| 100.0%id | 空闲CPU的CPU百分比 |
| 0.0%wa | 等待输入/输出法进程的占用的CPU百分比 |
| 0.0%hi | 硬中断请求服务占用的CPU百分比 |
| 0.0%hi | 软中断请求服务占用的CPU百分比 |
| 0.0%st | st(Steal time)虚拟时间百分比，就是当有 |

**第四列：物理内存信息**

|  |  |
| --- | --- |
| 内容 | 说明 |
| Mem：1030528k total | 物理内存的总量，单位kb |
| 184040k used | 已经使用的物理内存数量 |
| 846488k free | 空闲的物理内存数量，我们使用的是虚拟机，总共只分配了1G内存 |
| 28912k buffers | 作为***缓冲*** 的内存数量 |

**第五列：交换分区的占比**

|  |  |
| --- | --- |
| 内容 | 说明 |
| Swap: 1023992k total | 交换分区（虚拟内存）的总大小 |
| 0k used, | 已经使用的交互分区的大小 |
| 1023992k free | 空闲交换分区的大小 |
| 72524k cached | 作为***缓存*** 的交互分区的大小 |

缓冲buffer：加速了数据的写入，减少了对硬盘的写操作

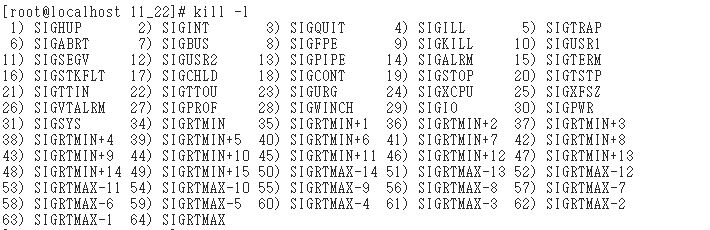
缓存cache：加速了数据的读取

做数据库搜索，网页的调用，负载均衡时才需要考虑缓冲和缓存。

Swap可以手动添加。

1. ***杀死进程***

kill -l #查看可用的进程信号



kill命令只可以杀死单一进程。killall命令和pkill可以杀死一系列进程

Linux支持64个进程信号。

kill -进程信号 进程PID

常用进程信号：

信号1：SIGHUP，重新加载配置文件，启动服务，但不会将原来在线的用户踢掉，即平滑重启。

信号9：SIGKILL强制终止进程

信号15：SIGTERM正常结束进程，默认选项。

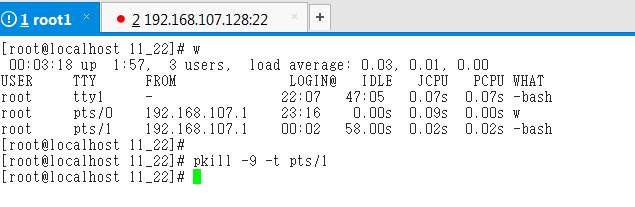
killall 选项 -进程信号 进程名

选项：-i：交互式杀死进程，即询问是否要杀死某个进程

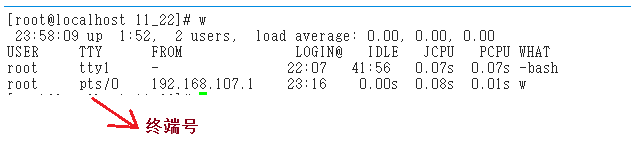
-I：忽略进程名的大小写

pkill 选项 -进程信号 进程名

选项：-t 终端号：按照终端号踢出用户



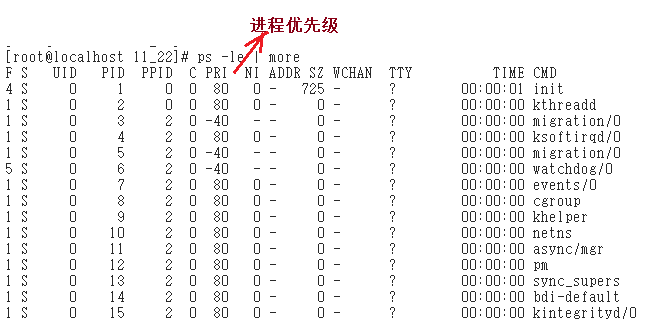
辅助命令w：查看当前登录用户



只有超级用户可以踢出其他用户，通过-t踢出用户，更加准确，如果同时登录了两个root，先下手为强！

***4、修改进程优先级 <了解 >***

Linux是一个多用户，多任务的操作系统，Linux系统中通知运行着非常多的进程。但CPU在一个时钟周期内只能运算一个命令，进程优先级决定了每个进程处理的先后顺序。对于多核CPU，每个CPU在一个时钟周期内处理一个进程。优先级的管理在内核裁剪或内核编程中十分重要。



* PRI 代表Priority，NI代表Nice。这两个都表示优先级。数字越小代表该进程优先级越高。用户只能修改NI，不能修改PRI，但最终的优先级PRI是两者的和
* 用户只能修改NI的值，不能直接修改PRI。
* NI值范围为-20~19，普通用户调整NI值的范围为0~19，而且只能调整自己的进程，且只能调高NI值，不能降低。
* Root用户可以设定进程NI值为负值，而且可以调整任何用户的进程。
* Pri(最终值) = Pri(原始值) + NI

nice命令

nice 选项 命令 #nice命令可以给新执行的Ingles知己而富于NI值，但是不能修改已经存在进程的NI值，即使用NI命令之前，需要将服务停止，重新启动。

选项：-n NI值：给命令赋予NI值

eg：nice -n -5 service httpd start

renice优先级 PID #修改已经存在进程的NI值的命令，即每次只能修改一个进程的优先级

eg：renice -10 1845

**工作管理**

1. ***工作管理简介***

工作管理指的是在单个登录的终端中，同时管理多个工作的行为。在Linux工作管理中，其实就是将当前的工作放到后台执行。查询当前系统中的后台程序使用的命令是jobs。

在Linux中，当某些服务启动之后，如果不放入后台，他会一直占用当前的shell，例如MYSQL。如果想要执行其他操作的话，需要将mysql服务终止掉。如果不想将该服务终止，就需要将该服务放入后台。

**注意事项：**

a> 当前的登录终端，只能管理当前终端的工作，而不能管理其他登录终端的工作。

也就是说，放入后天的服务是需要绑定终端的。Mysql服务发现了这个问题，当调用mysql服务的启动脚本时，它会将MySQL设置为可以脱离当前终端操作的服务，当MySQL服务在当前终端上放入后台时，关闭当前终端，mysql服务不会终止，但其他服务如果关闭的当前终端，服务也会跟着结束。

b> 放入后台的命令必须可以持续运行一段时间，这样我们才能捕捉和操作这个工作

例如：将ls、cd等命令房后后台是没有意义的，回车之后就会结束

c> 放入后台执行的命令不能和当前用户有交互或需要前台输入，否则放入后台只能暂停，而不能执行

例如：将vim命令放入后台，只能暂停，不肯能继续执行。因为vim命令是需要和用户进行交互的。

1. ***工作管理方法***

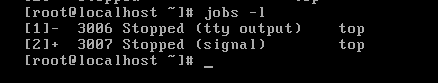
**1>把命令放入后台<以top命令为例>**

在执行的命令后加 & # 把命令放入后台，并在后台执行

top # 按下ctrl+z快捷键，放在后台暂停

**2>查看后台工作**

jobs [-l] # -l 显示工作的PID



注： “+”表示最近一个放入后台的工作，也是工作恢复时默认恢复的工作，“-”表示倒数第二个放入后台的工作

**3>将后台暂停的工作恢复到前台执行**

fg %工作号 # %可以省略，但是注意工作号和PID的区别

**4>把后台暂停的工作恢复到后台执行**

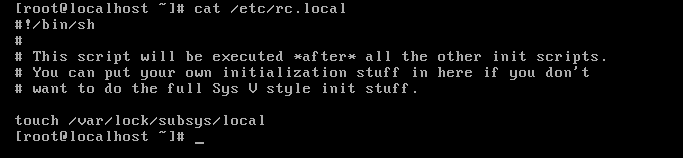
bg %工作号 # 后台恢复执行的命令，是不能和前台有交互的，否则不能恢复到后台执行

1. ***后台命令脱离登录终端执行***

把命令放入后台，只能在当前登录终端执行。一旦退出或关闭终端，后台程序就会停止。

**后台命令脱离登录终端执行的方法：**

1>把需要后台执行想命令加入到/etc/rc.local 文件



开机默认创建文件 /var/lock/subsys/local，目的是为了查看系统开机时间。

如果想要后台运行的一个程序持续运行，可以把这个进程完全写到该文件中，那么该进程就可以持续运行。因为它是系统直接调用的，没有绑定到终端。

2>使用系统定时任务，让系统在指定的时间执行某个后台命令

使用系统定时任务，可能会导致不生效！！！

3>使用nohup命令

命令格式：

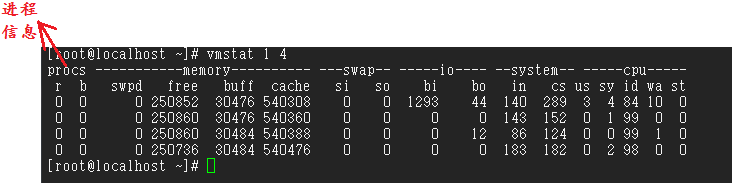
nohup [命令] &

|  |
| --- |
| 在 /root 目录下创建文件 for.sh，内容如下：    nohup运行该文件  切换终端，然后可以通过 ps aux | grep for.sh 查看 |

**系统资源查看**

**※1、vmstat命令监控系统资源**

vmstat [刷新延时 刷新次数]



* Procs：进程信息字段

-r：等待运行的进程数，数量越大，系统越繁忙

-b：不可被唤醒的进程数，数量越大，系统越繁忙

* Memory：内存信息字段

-swap：虚拟内存的使用情况，单位KB

-free：空闲的内存容量，单位KB

-buff：缓冲的内存容量，单位KB

-cache：缓存的内存容量，单位KB

|  |
| --- |
| **缓存和缓冲的区别：**  缓存（cache）是用来加速数据从硬盘中”读取”的，而缓冲（buffer）是用来加速数据”写入”硬盘的。 |

* Swap：交换分区的信息字段

-si：从磁盘中交换到内存中数据的数量，单位KB

-so：从内存中交换到磁盘中数据的数量，单位KB，

两个数越大，证明数据需要经常在磁盘和内存之间交换，系统性能越差

* Io：磁盘读写信息字段

-bi：从块设备读入数据的总量，单位是块

-bo：写到块设备的数据的总量，单位是块。

两个数越大，代表系统的I/O越繁忙

* System：系统信息字段：

-in：每秒被中断的进程次数

-cs：每秒钟进行的事件切换次数。

两个数越大，代表系统与接口设备的通信飞航繁忙

* CPU：CPU信息字段

-us：非内核进程消耗CPU运算时间的百分比

-sy：内核进程消耗CPU运算时间的百分比

-id：空间CPU的百分比

-wa：等待I/O所消耗的CPU百分比

-st：被虚拟机所盗用的CPU占比

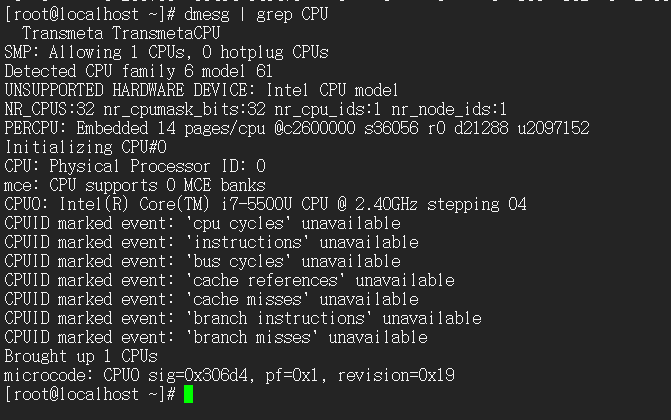
**※2、dmesg开机时内核检测信息**

dmesg

dmesg | grep CPU

显示系统的内核自检信息，对Linux来将，计算机需要自检两遍，一是硬件的BIOS自检，二是内核自检

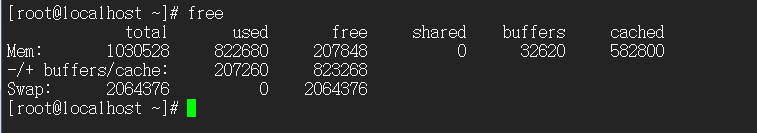
dmesg命令是用来判断当前服务器的硬件状态。



**※3、free命令查看内存使用状态**

free [-b | -k | -m | -g]

选项：以字节 | Kb | MB | GB 为单位显示，默认为Kb



- buffers/cache：相当于第一行used - buffers - cached

+ buffers/cache：相当于第一行free + buffers + cached

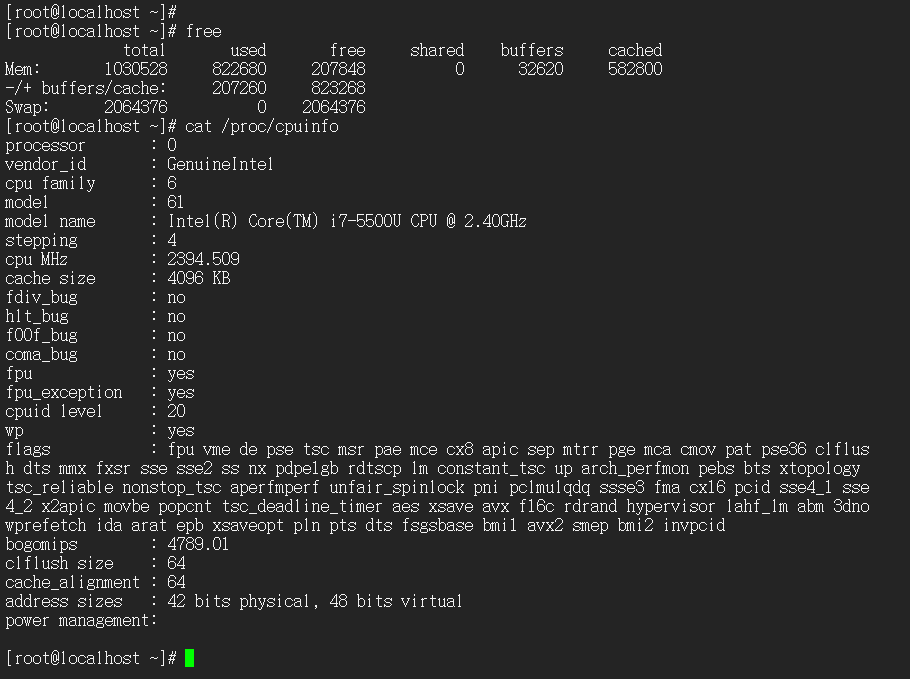
虽然看起来buffer和cached 占用了一部分内存，但实际上是作为缓冲和缓存存在，没有被系统的程序直接占用，是为了提高系统读写效率存在的

最后一行表示Swap的使用状况，swap是提高计算机性能尤其是高耗费内存性能的重要手段，因此不可以随意减少Swap分区的容量。当真实机内存小于4G，swap应该是内存的两倍，如果真实机的内存大于4G，swap最少要和内存一样。

**4、查看CPU信息**

cat /proc/cpuinfo

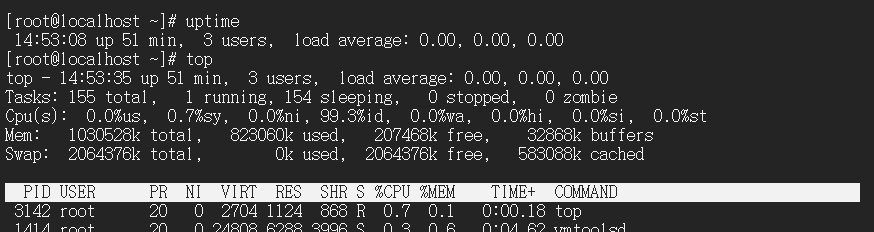
proc是用来保存内存信息的目录



**5、uptime命令**

uptime

显示系统的启动时间和平均负载，也就是top命令的第一行。W命令也可以看到这个数据。



uptime命令可以查看到系统当前时间，开机到现在的时间，登录用户数目，平均负载。和top命令第一行信息一致，但top命令本身就会造成一定的负载，如果只是简单想查看系统启动时间和平均负载，可以用uptime命令。

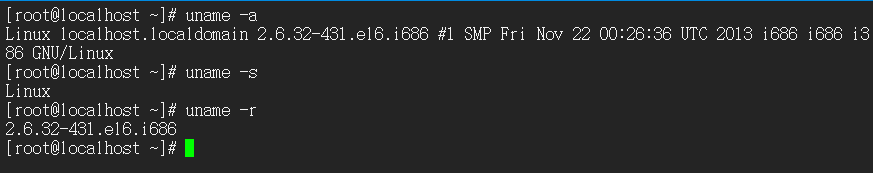
**6、查看系统与内核相关信息**

uname [选项]

选项： -a：查看系统所有相关信息

-r：查看内核版本

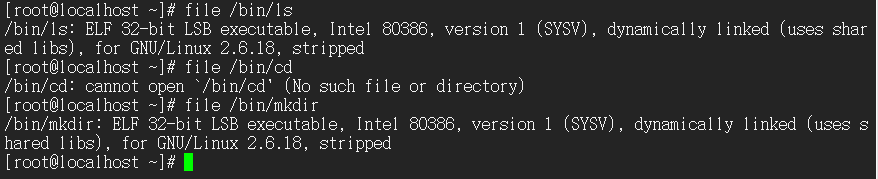
-s：查看内核名称



**7、查看当前Linux系统的操作位数**

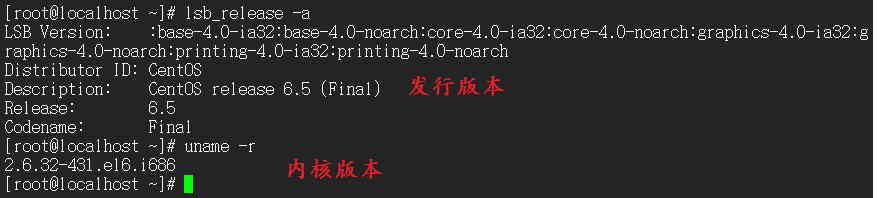
file /bin/ls

File之后可以追加任何一个系统外部命令，可以查看到当前操作系统的位数。需要注意的是，这里的位数为CPU的位数不一定相同，64的的电脑上也可以安装32位的操作系统



**8、查询当前Linux的发行版本**

lsb\_release -a



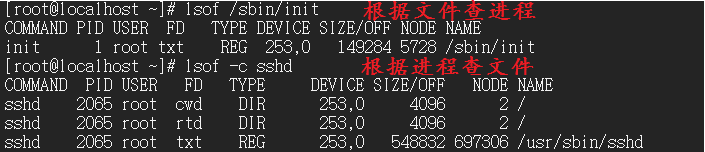
**9、列出进程打开或使用的文件信息**

lsof [选项] # 列出进程调用或打开的文件的信息

选项： -c 字符串：只列出字符串开头的进程打开的文件

-u 用户名：只列出某个用户的进程打开的文件

-p pid：列出某个PID进程打开的文件



根据文件名查进程，文件只能是系统文件，不能是用户自己创建的文件，只有系统文件才有系统进程

**系统定时任务**

Windows中的系统定时任务：开始-- >所有程序-- >附件-- > 系统工具-- >定时计划程序

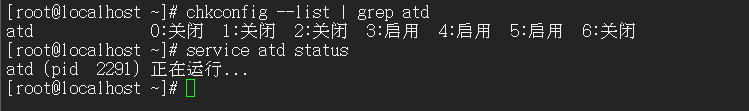
**at一次性定时任务**

1. 确定at安装

chkconfig --list | grep atd # at服务是否安装

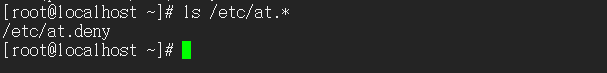
service atd restart # at服务的启动

在服务名后加 d ,表明这是一个守护进程



1. at的访问控制

* 如果系统中有 /etc/at.allow（白名单）文件，那么只有写入/etc/at.allow 文件中的用户可以使用at 命令（/etc/at.deny文件会被忽略）
* 如果系统中没有 /etc/at.allow （黑名单）文件，只有 /etc/at.deny 文件，那么写入 /etc/at.deny 文件中的用户不能使用at命令，但对root 用户不起作用
* 如果系统中这两个文件都不存在，那么只有root用户可以使用at命令。默认情况下只有黑名单



1. at命令的使用

at [选项] 时间

选项：

-m：当at工作完成后，无论是否命令有输出，都用email 通知执行at命令的用户

-c 工作号：显示该at工作的实际内容

时间：

- HH:MM 例如：02：30

- HH:MM YYYY-MM-DD 例如：02：30 2013-07-25

- HH:MM [am|pm] [month] [date] 例如：02：30 July 25

- HH:MM [am|pm] + [minutes|hours|days|weeks] 例如：now + 5minutes

其他at管理命令

atq # 查询当前服务器上的at工作

atrm [工作号] # 删除指定的at任务

at定时任务执行完毕之后，atq就不会再查询到at任务

