文件查找：

grep, egrep, fgrep: 文本过滤

/var/log, .log结束文件名

ls /var/log/\*.log 文件名通配

ls /var/log | grep “.”\.log **和下面完全是两回事**

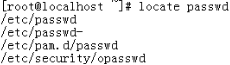
grep ".\*\.log" /var/log **这个是过滤这个文本文件中的行**

查找文件:

1) locate KEYWORD, 模糊查找, 非实时查找, 速度快

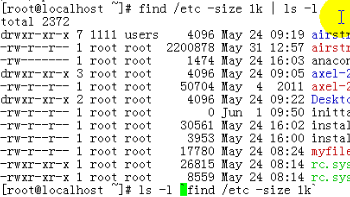
database，而非在系统上查找 有点像whatis

# updatedb 手动更新数据库



2) find： 精确，实时查找，而且可指定查找路径，速度慢；

不可以管道传给ls； 命令引用才可以



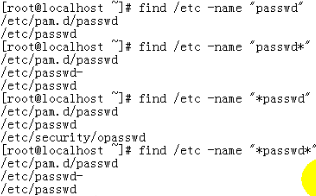
find [查找路径 ...] [查找条件] [处理动作]

查找路径：省略为当前，可以多个

**查找条件**：

-name "FILENAME" 文件名查找，也会在目录下做递归，严格区分大小写，支持通配

-iname "FILENAME" 不区分大小写



文件名还支持正则表达式

-regex 正则表达式

-iregux 忽略大小写

-user USERNAME

-group GROUPNAME

-uid UID 某用户被删除之后会显示为uid而不是用户名

-gid GID

-nouser 无主文件

-nogroup

多条件查找，条件间逻辑关系：

并：-a

或：-o

非：!, -not

find /etc –name “\*passwd\*” –o –user redhat 名称包含passwd或者属主为redhat的

-type find -type d

f 普通文件

d 目录

l 软链接

b 块设备

c 字符设备

p 管道文件

s socket文件

-size [+/-]# +大于 –小于

{k|M|G}

-size 2M 查找2M

0.8M 不符合

1M 不符合

1.1M 符合2M

-size 1k

单位是天

-atime [+/-]# 访问时间

-mtime [+/-]# 修改时间

-ctime [+/-]# 改变时间

-atime +3

单位是minute

-amin [+/-]#

-mmin [+/-]#

-cmin [+/-]#

-perm 根据权限查找

mode: 精确匹配

/mode：任何一位匹配都行

-mode：所有都得匹配

-perm 222 一个文件权限为222

-perm /222 有一个222即可

-perm -222 三人都必须至少有222但至于能不能读就不管了 666也可以

find /etc -perm 640

-perm -640

-perm /640

**处理动作：**

-print 默认 显示

-ls

-ok COMMAND {} \; 提醒用户确认 有些命令还是执行不了的

**-exec COMMAND {} \; 不提醒 {}占位符意思是找到的文件 固定格式**

找到所有没有属主属组的文件改为root所有：

find / -nouser -a -nogroup -exec chown root:root {} \;

找到所有的重命名：

find ./ -perm -002 -exec mv **{} {}.old \;**

find | xargs COMMAND 有些不能执行的可以送给xargs执行

1、查找/var目录下属主为root并且属组为mail的所有文件；

2、查找/usr目录下不属于root,bin,或student的文件；

3、查找/etc目录下最近一周内内容修改过且不属于root及student用户的文件；

4、查找当前系统上没有属主或属组且最近1天内曾被访问过的文件，并将其属主属组均修改为root；

5、查找/etc目录下大于1M的文件，并将其文件名写入/tmp/etc.largefiles文件中；

6、查找/etc目录下所有用户都没有写权限的文件，显示出其详细信息；