linux查看系统的日志的一些实用操作

last

-a 把从何处登入系统的主机名称或ip地址，显示在最后一行。

-d 指定记录文件。指定记录文件。将IP地址转换成主机名称。

-f <记录文件>　指定记录文件。

-n <显示列数>或-<显示列数>　设置列出名单的显示列数。

-R 不显示登入系统的主机名称或IP地址。

-x 显示系统关机，重新开机，以及执行等级的改变等信息

以下看所有的重启、关机记录

last | grep reboot

last | grep shutdown

history

列出所有的历史记录：

[zzs@Linux] # history

只列出最近10条记录：

[zzs@linux] # history 10 (注,history和10中间有空格)

使用命令记录号码执行命令,执行历史清单中的第99条命令

[zzs@linux] #!99 (!和99中间没有空格)

重复执行上一个命令

[zzs@linux] #!!

执行最后一次以rpm开头的命令(!? ?代表的是字符串,这个String可以随便输，Shell会从最后一条历史命令向前搜索，最先匹配的一条命令将会得到执行。)

[zzs@linux] #!rpm

逐屏列出所有的历史记录：

[zzs@linux]# history | more

立即清空history当前所有历史命令的记录

[zzs@linux] #history -c

cat, tail 和 watch

系统所有的日志都在 /var/log 下面自己看(具体用途可以自己查,附录列出一些常用的日志)

cat /var/log/syslog 等

cat /var/log/*.log

tail -f

如果日志在更新，如何实时查看 tail -f /var/log/messages

还可以使用 watch -d -n 1 cat /var/log/messages

-d表示高亮不同的地方，-n表示多少秒刷新一次。

该指令，不会直接返回命令行，而是实时打印日志文件中新增加的内容，

这一特性，对于查看日志是非常有效的。如果想终止输出，按 Ctrl+C 即可。

除此之外还有more， less ，dmesg|more,这里就不作一一列举了,因为命令太多了,关键看个人喜好和业务需求.个人常用的就是以上那些

linux日志文件说明

/var/log/message 系统启动后的信息和错误日志，是Red Hat Linux中最常用的日志之一

/var/log/secure 与安全相关的日志信息

/var/log/maillog 与邮件相关的日志信息

/var/log/cron 与定时任务相关的日志信息

/var/log/spooler 与UUCP和news设备相关的日志信息

/var/log/boot.log 守护进程启动和停止相关的日志消息

/var/log/wtmp 该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件