Linux用户登录记录日志和相关查看命令汇总 - 珠穆戏朗玛 - 博客园

1 utmp、wtmp、btmp文件

Linux用户登录信息放在三个文件中:

1 /var/run/utmp：记录当前正在登录系统的用户信息，默认由who和w记录当前登录用户的信息，uptime记录系统启动时间;

2 /var/log/wtmp：记录当前正在登录和历史登录系统的用户信息，默认由last命令查看;

3 /var/log/btmp：记录失败的登录尝试信息，默认由lastb命令查看。

这三个文件都是二进制数据文件，并且三个文件结构完全相同，是由/usr/include/bits/utmp.h文件定义了这三个文件的结构体。

默认情况下文件的日志信息会通过logrotate日志管理工具定期清理。logrotate的配置文件是/etc/logrotate.conf，此处是logrotate的缺省设置，通常不需要对它进行修改。日志文件的轮循压缩等设置存放在独立的配置文件中，它（们）放在/etc/logrotate.d/目录下，它会覆盖缺省设置。

如果不想记录相关信息，则可以直接将相关文件删除即可。如果系统不存在该文件，则需要在此路径touch一个文件就可以继续记录相关信息了。

此外:

如果想禁用who命令，则只需要将utmp的可读权限去掉就行，这样非root用户就不能用此命令了；如果是btmp文件，手工创建的话注意权限必须为600，否则不能正确写入信息。

2 相关命令介绍

好了，下面开始介绍查看这三个日志文件的命令了。分别是lastlog、last、lastb、ac、who、w、users、utmpdump。

其中last、lastb、who、utmpdump可以通过指定参数而查看三个中的任意一个文件。

2.1 lastlog:

列出所有用户最近登录的信息，或者指定用户的最近登录信息。lastlog引用的是/var/log/lastlog文件中的信息，包括login-name、port、last login time

lzx-clone1:/var/log # lastlogUsername Port Latestroot pts/1 Wed Oct 1914:37:46 +08002016bin **Never logged in**daemon **Never logged in**gdm **Never logged in**admin **Never logged in**lzx pts/3 Wed Oct 1915:15:24 +08002016

2.2 last

列出当前和曾经登入系统的用户信息，它默认读取的是/var/log/wtmp文件的信息。输出的内容包括：用户名、终端位置、登录源信息、开始时间、结束时间、持续时间。注意最后一行输出的是wtmp文件起始记录的时间。当然也可以通过last -f参数指定读取文件，可以是/var/log/btmp、/var/run/utmp

[root@CLMUGR-APP-D-01 log]# lastroot pts/010.200.108.92 Tue Oct 1815:04 still logged in root pts/110.200.108.92 Wed Oct 1217:02 still logged in root pts/010.200.108.92 Wed Oct 1209:20 - 16:58 (07:38) root pts/010.200.108.92 Sat Oct 810:40 - 14:45 (04:05) root pts/010.200.108.92 Wed Aug 3110:52 - 08:44 (21:52) root pts/010.200.108.92 Fri Jul 813:08 - 09:41 (25+20:32)reboot system boot 2.6.32-431.el6.x Tue Jan 1319:40 - 19:44 (00:04) wtmp begins Tue Jan 1319:40:222015

2.3 lastb

列出失败尝试的登录信息，和last命令功能完全相同，只不过它默认读取的是/var/log/btmp文件的信息。当然也可以通过last -f参数指定读取文件，可以是/var/log/btmp、/var/run/utmp

[root@CLMUGR-APP-D-01 log]# lastbroot ssh:notty 10.200.108.92 Wed Oct 1917:11 - 17:11 (00:00) root ssh:notty 10.200.108.92 Wed Oct 1917:11 - 17:11 (00:00) root ssh:notty 10.200.108.92 Wed Oct 1917:10 - 17:10 (00:00) root ssh:notty 10.200.108.92 Wed Oct 1917:10 - 17:10 (00:00) btmp begins Wed Oct 1917:10:122016

lzx-clone1:/var/log # lastb -F -f /var/log/wtmproot pts/010.200.108.92 Tue Mar 811:04:362016 - Tue Mar 811:04:362016 (00:00) wtmp begins Tue Mar 811:04:362016

2.4 ac

输出所有用户总的连接时间，默认单位是小时。由于ac是基于wtmp统计的，所以修改或者删除wtmp文件都会使ac的结果受影响。(Suse默认没有该命令)

[root@cloudexpress ~]# ac

total 7404.62

2.5 who

查看当前登入系统的用户信息。其中who -m等效于who am i。

语法who [OPTION]... [FILE | ARG1 ARG2]。

who命令强大的一点是，它既可以读取utmp文件也可以读取wtmp文件，默认没有指定FILE参数时，who查询的是utmp的内容。当然可以指定FILE参数，比如who -aH /var/log/wtmp,则此时查看的是wtmp文件。

查看当前运行级别

[root@CLMUGR-APP-D-01 log]# who -rH

名称 线路 时间 空闲 进程号 备注

运行级别 5 2016-07-08 13:01

查看登录用户和用户数≈users

lzx-clone1:/var/run # who -q

root root root root

users=4

2.6 w

查看当前登入系统的用户信息及用户当前的进程（而who命令只能看用户不能看进程）。该命令能查看的信息包括字系统当前时间，系统运行时间，登陆系统用户总数及系统1、5、10分钟内的平均负载信息。后面的信息是用户，终端，登录源，login time，idle time，JCPU，PCPU，当前执行的进程等。

w的信息来自两个文件：用户登录信息来自/var/run/utmp，进程信息来自/proc/.

lzx-clone1:/var/log # w15:26:40 up 12 days, 56 min, 4 users, load average: 0.14, 0.16, 0.20USER TTY LOGIN@ IDLE JCPU PCPU WHATroot :0 10Oct16 ?xdm? 43:330.69s /usr/bin/gnome-sessionroot pts/0 Wed14 40.00s 0.19s 0.00s wroot pts/1 Wed14 23:01m 0.06s 0.06s -bashroot pts/2 10Oct16 9days 0.01s 0.01s /bin/bash -l

2.7 users

显示当前正在登入统的用户名。语法是users [OPTION]... [FILE]。如果未指定FILE参数则默认读取的是/var/run/utmp，当然也可以指定通用相关文件/var/log/wtmp，此时输出的就不是当前用户了。

[root@CLMUGR-APP-D-01 log]# users

root root

2.8 utmpdump

utmpdump用于转储二进制日志文件到文本格式的文件以便查看，同时也可以修改二进制文件！！包括/var/run/utmp、/var/log/wtmp、/var/log/btmp。语法为：utmpdump [options] [filename]。修改文件实际就可以抹除系统记录，所以一定要设置好权限，防止非法入侵。

例子：修改utmp或wtmp。由于这些都是二进制日志文件，你不能像编辑文件一样来编辑它们。取而代之是，你可以将其内容输出成为文本格式，并修改文本输出内容，然后将修改后的内容导入回二进制日志中。如下：

utmpdump /var/log/utmp > tmp_output.txt #导出文件信息 #<使用文本编辑器修改 tmp_output.txt>utmpdump -r tmp_output.txt > /var/log/utmp #导入到源文件中

参考：

使用utmpdump 监控 CentOS 用户登录历史

Linux man utmpdump