linux日志管理命令详解Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022_linux_E6_97_A5_E5_BF_c103_645335.htm 日志对于安全来说，非常重要，他记录了系统每天发生的各种各样的事情，你可以通过他来检查错误发生的原因，或者受到攻击时攻击者留下的痕迹。日志主要的功能有：审计和监测。他还可以实时的监测系统状态，监测和追踪侵入者等等。 在Linux系统中，有三个主要的日志子系统： 连接时间日志--由多个程序执行，把纪录写入到/var/log/wtmp和/var/run/utmp，login等程序更新wtmp和utmp文件，使系统管理员能够跟踪谁在何时登录到系统。进程统计--由系统内核执行。当一个进程终止时，为每个进程往进程统计文件（pacct或acct）中写一个纪录。进程统计的目的是为系统中的基本服务提供命令使用统计。 错误日志--由syslogd执行。各种系统守护进程、用户程序和内核通过syslog向文件/var/log/messages报告值得注意的事件。另外有许多UNIX程序创建日志。像HTTP和FTP这样提供网络服务的服务器也保持详细的日志。 常用的日志文件如下： access-log 纪录HTTP/web的传输 acct/pacct 纪录用户命令 aculog 纪录MODEM的活动 btmp 纪录失败的纪录 lastlog 纪录最近几次成功登录的事件和最后一次不成功的登录 messages 从syslog中记录信息（有的链接到syslog文件） sudolog 纪录使用sudo发出的命令 sulog 纪录使用su命令的使用 syslog 从syslog中记录信息（通常链接到messages文件） utmp 纪录当前登录的每个用户 wtmp 一个用户每次登录进入和退出时间的永久纪录 xferlog 纪录FTP会话 utmp、wtmp和lastlog日志文件是多

数重用UNIX日志子系统的关键--保持用户登录进入和退出的纪录。 有关当前登录用户的信息记录在文件 utmp中； 登录进入和退出纪录在文件wtmp中； 最后一次登录文件可以用lastlog命令察看。 数据交换、关机和重起也记录在wtmp文件中。 所有的纪录都包含时间戳。这些文件（lastlog通常不大）在具有大量用户的系统中增长十分迅速。例如wtmp文件可以无限增长，除非定期截取。许多系统以一天或者一周为单位把wtmp配置成循环使用。它通常由cron运行的脚本来修改。这些脚本重新命名并循环使用wtmp文件。通常，wtmp在第一天结束后命名为wtmp.1；第二天后wtmp.1变为wtmp.2等等，直到wtmp.7。 每次有一个用户登录时，login程序在文件lastlog中察看用户的UID。如果找到了，则把用户上次登录、退出时间和主机名写到标准输出中，然后 login程序在lastlog中纪录新的登录时间。在新的lastlog纪录写入后，utmp文件打开并插入用户的utmp纪录。该纪录一直用到用户登录退出时删除。utmp文件被各种命令文件使用，包括who、w、users和finger。 下一步，login程序打开文件wtmp附加用户的utmp纪录。当用户登录退出时，具有更新时间戳的同一utmp纪录附加到文件中。wtmp文件被程序last和ac使用。 具体命令wtmp和utmp文件都是二进制文件，他们不能被诸如tail命令剪贴或合并（使用cat命令）。用户需要使用who、w、users、last和ac来使用这两个文件包含的信息。 