RedHatLinux常见日志文件和常用命令 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022_RedHatLinu_c103_144082.htm 成功地管理任何系统的关键之一，是要知道系统中正在发生什么事。Linux 中提供了异常日志，并且日志的细节是可配置的。Linux 日志都以明文形式存储，所以用户不需要特殊的工具就可以搜索和阅读它们。还可以编写脚本，来扫描这些日志，并基于它们的内容去自动执行某些功能。 Linux 日志存储在 /var/log 目录中。这里有几个由系统维护的日志文件，但其他服务和程序也可能会把它们的日志放在这里。大多数日志只有root账户才可以读，不过修改文件的访问权限就可以让其他人可读。 RedHat Linux常用的日志文件 RedHat Linux常见的日志文件详述如下 /var/log/boot.log 该文件记录了系统在引导过程中发生的事件，就是Linux系统开机自检过程显示的信息。 /var/log/cron 该日志文件记录crontab守护进程crond所派生的子进程的动作，前面加上用户、登录时间和PID，以及派生出的进程的动作。CMD的一个动作是cron派生出一个调度进程的常见情况。REPLACE（替换）动作记录用户对它的cron文件的更新，该文件列出了要周期性执行的任务调度。 RELOAD动作在REPLACE动作后不久发生，这意味着cron注意到一个用户的cron文件被更新而cron需要把它重新装入内存。该文件可能会查到一些反常的情况。 /var/log/maillog 该日志文件记录了每一个发送到系统或从系统发出的电子邮件的活动。它可以用来查看用户使用哪个系统发送工具或把数据发送到哪个系统。下面是该日志文件的片段： QUOTE: Sep 4 17:23:52 UNIX sendmail[1950]:

g849Npp01950: from=root, size=25, class=0, nrcpts=1, msgid=200209040923.g849Npp01950@redhat.pfcc.com.cn>, relay=root@localhost Sep 4 17:23:55 UNIX sendmail[1950]: g849Npp01950: to=lzy@fcceec.net, ctladdr=root (0/0), delay=00:00:04, xdelay=00:00:03, mailer=esmtp, pri=30025, relay=fcceec.net. [10.152.8.2], dsn=2.0.0, stat=Sent (Message queued) /var/log/messages 该日志文件是许多进程日志文件的汇总，从该文件可以看出任何入侵企图或成功的入侵。如以下几行： QUOTE: Sep 3 08:30:17 UNIX login[1275]: FAILED LOGIN 2 FROM (null) FOR suying, Authentication failure Sep 4 17:40:28 UNIX -- suying[2017]: LOGIN ON pts/1 BY suying FROM fcceec.www.ec8.pfcc.com.cn Sep 4 17:40:39 UNIX su(pam_unix)[2048]: session opened for user root by suying(uid=999) 该文件的格式是每一行包含日期、主机名、程序名，后面是包含PID或内核标识的方括号、一个冒号和一个空格，最后是消息。该文件有一个不足，就是被记录的入侵企图和成功的入侵事件，被淹没在大量的正常进程的记录中。但该文件可以由/etc/syslog文件进行定制。由/etc/syslog.conf配置文件决定系统如何写入/var/messages。有关如何配置/etc/syslog.conf文件决定系统日志记录的行为，将在后面详细叙述。 /var/log/syslog 默认RedHat Linux不生成该日志文件，但可以配置/etc/syslog.conf让系统生成该日志文件。它和/etc/log/messages日志文件不同，它只记录警告信息，常常是系统出问题的信息，所以更应该关注该文件。要让系统生成该日志文件，在/etc/syslog.conf文件中加上：*.warning /var/log/syslog 该日志文件能记录当用户登录时login记录下的

错误口令、Sendmail的问题、su命令执行失败等信息。下面是一条记录： QUOTE: Sep 6 16:47:52 UNIX login(pam_unix)[2384]: check pass. user unknown /var/log/secure 该日志文件记录与安全相关的信息。该日志文件的部分内容如下： QUOTE: Sep 4 16:05:09 UNIX xinetd[711]: START: ftp pid=1815 from=127.0.0.1 Sep 4 16:05:09 UNIX xinetd[1815]: USERID: ftp OTHER :root Sep 4 16:07:24 UNIX xinetd[711]: EXIT: ftp pid=1815 duration=135(sec) Sep 4 16:10:05 UNIX xinetd[711]: START: ftp pid=1846 from=127.0.0.1 Sep 4 16:10:05 UNIX xinetd[1846]: USERID: ftp OTHER :root Sep 4 16:16:26 UNIX xinetd[711]: EXIT: ftp pid=1846 duration=381(sec) Sep 4 17:40:20 UNIX xinetd[711]: START: telnet pid=2016 from=10.152.8.2 /var/log/lastlog 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com