配置Linux日志文件 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/462/2021_2022__E9_85_8D_E7_BD_AELinu_c103_462192.htm 不要低估日志文件对网络安全的重要作用，因为日志文件能够详细记录系统每天发生的各种各样的事件，用户可以通过日志文件检查错误产生的原因，或者在受到攻击、被入侵时追踪攻击者的踪迹。日志的两个比较重要的作用是审核和监测。配置好的Linux的日志非常强大。对于Linux系统而言，所有的日志文件在/var/log下。默认情况下，Linux的日志文件没有记录FTP的活动。用户可以通过修改/etc/ftpacess让系统记录FTP的一切活动。
/etc/syslog.conf的格式 Linux系统的日志文件是可以配置的，在前面的章节中已经介绍了如何定制Apache、wu-ftpd、Sendmail的日志文件。Linux系统的日志文件是由/etc/syslog.conf决定的，用户有必要花时间仔细配置一下/etc/syslog.conf.下面是/etc/syslog.conf的范例： # Log all kernel messages to the kernlog.# Logging much else clutters up the screen.kern.*/var/log/kernlog# Log anything (except mail) of level info or higher.# Dont log private authentication messages!*.info.mail.none.news.none.authpriv.none.cron.none/var/log/messages*.warning/var/log/syslog# The authpriv file has restricted access.authpriv.* /var/log/secure# Log all the mail messages in one place.mail.*/var/log/maillog# Log cron stuffcron.*/var/log/cron# Everybody gets emergency messages, plus log them on another# machine.*.emerg# Save mail and news errors of level err and higher in a# special

file.uucp,news.crit/var/log/spooler# Save boot messages also to boot.loglocal7.*/var/log/boot.log# INNnews.=crit /var/log/news/news.critnews.=err /var/log/news/news.errnews.notice /var/log/news/news.notice. 可以看出，该配置文件的每一行的第一个字段列出要被记录的信息种类，第二个字段则列出被记录的位置。第一个字段使用下面的格式：facility.level[；facility.level…] 此处的faciity是产生信息的系统应用程序或工具，level则是这个信息的重要程度。level的重要程度由低到高依次是：debug（调试消息）、info（一般消息）、notice（值得注意的消息）、warning（警告）、err（一般性错误）、crit（严重错误）、alert（或emerg，紧急情况）。 facility包含有：auth（认证系统，如login或su，即询问用户名和口令）、cron（系统执行定时任务时发出的信息）、daemon（某些系统的守护程序的syslog，如由in.ftpd产生的log）、kern（内核的信息）、lpr（打印机的信息）、mail（处理邮件的守护进程发出的信息）、mark（定时发送消息的时标程序）、news（新闻组的守护进程的信息）、user（本地用户的应用程序的信息）、uucp（uucp子系统的信息）和“ * ”（表示所有可能的facility）。 将日志文件记录到远程主机 如果有另一个Linux或UNIX系统，那么可以配置日志文件，让其把消息发到另外一个系统并记录下来。这也是为什么上面的所有日志文件都记录了主机名的原因。要实现这个功能，在该配置文件中，指定一个记录动作，后面接一个由“ @ ”开头的远程系统的主机名，如下例：*.warn；authpriv.notice；auth.notice @bright.hacker.com.cn 同时，还要将接受消息的目的系统设置为允许这种操作。此例

主机bright.hacker.com.cn的syslogd守护进程要用-r参数启动。如果不使用-r参数，则目标主机的syslogd将丢弃这个消息以避免DoS攻击使硬盘塞满虚假消息。并且确保目标主机的/etc/service文件必须设置syslog服务所使用的UDP端口514（这也是RedHat Linux默认的设置）。如果syslogd守护进程用了-r和-h参数，那么，参数-h将允许转发消息。也就是说，如果系统B的syslogd用了-h参数，这样，当系统A把消息转发到系统B后，系统B就把来自系统A和它自己的消息转发到系统C. 将警告信息发送到控制台 syslogd可以将任何从内核发出的重要程度为emerg或alert的信息发送到控制台。控制台是指虚拟控制台或启动时加-C参数的xterm.要实现这一功能，在/etc/syslog.conf文件中加上下面一行：kern.emerg /dev/console 这样，当系统内核发生错误而发出消息时，用户能够马上知道并且进行处理。如果用了“*”，就是一旦内核发生错误，就将消息发送给所有在线用户，但只有这个用户正在登录的时候才能看到。修改了/etc/syslog.conf文件后，必须重新启动syslogd守护进程以使配置更改生效，请执行下面的命令：#/etc/rc.d/init.d/syslog restart 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