网络工程师Linux系统日志的分析 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/252/2021_2022__E7_BD_91_E7_BB_9C_E5_B7_A5_E7_c103_252882.htm 日志文件对网络安全的重要作用是不可低估的，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，或者在受到攻击和黑客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，所有的日志文件都在/var/log下。默认情况下，Linux的日志文件已经足够强大，但没有记录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。 Linux日志系统简介：日志对于系统的安全来说非常重要，它记录了系统每天发生的各种各样的事情，用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。日志主要的功能是审计和监测。它还可以实时地监测系统状态，监测和追踪侵入者。Linux系统一般有3个主要的日志子系统：连接时间日志、进程统计日志和错误日志。 RedHat Linux常见的日志文件和常用命令：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。 配置Linux日志文件：日志也应该是用户注意的地方。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的日志文件已经足够强大，但没有记录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。 管理Linux日志文件工具：logrotate简介：如果服务器有大量的用户的话，这些日志文件的大小会很快地增加，在服务器硬盘不是非常充足的情况下，必须采取措施防止日志文件将硬盘撑爆。现代的Linux版本都有一个小程序，名为logrotate，用来帮助用户管理日志文件，它以自己的守护进程工作。logrotate周期性地旋转日志文件，可以周期性地把每个日志文件重命名成一个备份名字，然后让它的守护进程开始使用一个日志文件的新的拷贝。这就是为什么在/var/log/下看到许多诸如maillog、maillog.1、maillog.2、boot.log.1、boot.log.2之类的文件名。它由一个配置文件驱动，该文件是/etc/logroatate.conf Linux下常用日志分析工具logcheck简介：对于拥有大量账户、系统繁忙的Linux系统而言，其日志文件是极其庞大的，很多没有用的信息会将值得注意的信息淹没，给用户分析日志带来了很大的不便。现在有一些专门用于分析日志的工具，如Logcheck和Friends。Logcheck用来分析庞大的日志文件，过滤出有潜在安全风险或其他不正常情况的日志项目，然后以电子邮件的形式通知指定的用户。它是