Linux系统下使用Syslog进行远程登录 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022_Linux_E7_B3_BB_E7_BB_c103_145088.htm 管理登录文件是网络管理的重要一部分。每个Linux都具有Syslog的标准功能，它既能登录本地文件，又能登录远程系统。如果你要在一台被攻陷的机器上查看登录文件，特别是在你不太确定攻击者是否已清除登录文件，销毁登录踪迹的情况下，它的作用就尤其关键了。安装syslog进行远程登录是及其容易的。你只需在你准备收到登录记录的系统上，使用－r选项，配置syslog，这样就可以让你接收到远程登录的记录。 比如，在Mandrake Linux系统上，编辑/etc/sysconfig/syslog文件，根据如下所列改变SYSLOGD_OPTIONS的参数。 SYSLOGD_OPTIONS="-r -m 0" 下一步，重新启动syslog服务。你也应该确保该机器上的防火墙允许从其它发送登录记录的机器访问UDP端口514。在你要发送登录记录的系统上，修改/etc/syslog.conf文件，增加类似如下的内容到末尾； *.info @loghost.mydomain.com 这就表示syslog发送所有 *.info等级的登录记录到loghost.mydomain.com的主页。你能够改变你想要进行远程登录的设施，但是*.info通常是充分的。在这台机器上，也同样重新启动syslog，确保防火墙允许从本地主机的UDP端口514上，发送到远程机器。 一个主机上的登录记录应该此刻就出现在远程主机上，同时包括该主机自己的登录信息。比如，你的登录文件是这样的： Jan 8 13:23:22 loghost fam[3627]: connect: Connection refused Jan 8 13:23:24 remote.mydomain.com su(pam_unix)[3166]: session closed for user root 正如你

从/var/log/messages片断看到的一样，syslog登录信息是与loghost(当地机器)和远程mydomain.com（远程主机）同样的文件。这时，安装登录监督到登录主机上，用来提醒你想要监督的任何特定的内容（比如失败的登录）。