在Linux系统中安装系统日志服务器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__E5_9C_A8Linux_E7_B3_c103_645433.htm 对管理员来说，日志非常有用，但大量的日志又很麻烦。当一些事件运行错误时，日志可以对故障排除起到至关重要的作用，特别是在安全性相关问题上。但是如果攻击者危害到你的主机，日志将会告诉你，对于主机来说这很有用.你需要给数据中心发信息。保护日志非常重要，一个中央日志服务器会更容易管理、分析和查找它们。针对这一点，我将向你展示如何把多个主机的系统日志集中收集到一个主机上来管理，即Linux上的中央系统日志服务器。 首先，所有集中的系统日志服务器都应该建成一个安全和硬化的主机。在主机上没有一点关于保护和集中化你们日志方面。其次，你怎样能从你的主机上获得日志呢？ 让我们开始安装中央系统日志服务器。我将举例说明如果使用rSyslog，实际的标准Linux系统日志。Ubuntu和红帽常使用它，并且通过文件/etc/rsyslog.conf进行管理。文件中包含许多指定的特殊系统日志：有的是控制台方面的，有的是文件方面或其它主机的。 首先，我们需要载入合适的TCP和UDP插件以支持接收系统日志。把下面的代码添加到rsyslog.conf的头部： $modload imtcp $modload imudp $InputTCPServerRun 10514 $UDPServerRun 514 载入的这两个模块能支持监听TCP和UDP的端口，并且指定哪个端口来接受事件，在这种情况下，使用TCP的10514端口和UDP的514端口。你需要确认一下本地防火墙(在你的主机和中央系统日志服务器之间的防火墙) 下面我们需要指定一些规则来告诉rSyslog在哪放输入事件

。如果你不添加任何规则，输入事件将按照本地的规则进行处理，并且与本地主机的事件交织在一起。我们需要在上面添加节之后和本地处理系统日志之前来正确的指定这个规则，例如： if $fromhost-ip isequal 192.168.0.2 then /var/log/192.168.0.2.log 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