

tcpdumpw和r的使用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\\_ti2020/644/2021\\_2022\\_tcpdumpw\\_E5\\_92\\_c103\\_644802.htm](https://www.100test.com/kao_ti2020/644/2021_2022_tcpdumpw_E5_92_c103_644802.htm) tcpdump的说明文档是这样的：-w 将原始的信息包写入。形式如 tcpdump -w /tmp/result.txt 我今天试了一下，发现其写成的文件如果用cat,vim来查看的话，都显示为乱码。来源：www.examda.com 经过man tcpdump 才知道，生成的文件必须用 tcpdump -r 来查看，如 tcpdump -r /tmp/result.txt. 其他: File 而不是分析和打印它们。它们可以在以后用 -r 标志打印出来。如果 File 为“-”，则使用标准输出。我用tcpdump抓路由器的netflow数据流，用 -w参数时候发现并不是象我想象的那样，tcpdump -w的输出并不等价于路由器直接发给我的netflow数据。编辑特别推荐: Linux系统通过手机GPRS上网设置简介 提高Apache服务器性能的四个建议 Linux认证能帮助你找到一份好工作吗 linux面试题参考答案 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](http://www.100test.com)