 关于swap持续增长怀疑存在内存泄露，对于什么原因引起的泄露，初步怀疑与服务器玩家上下线登录时内存未释放有关。 问题排查的思路： (1)确定标准系统中哪些情况会造成swap的持续增长 (2)确定swap的增长与系统其它性能指标的关系，这个使用Excel分析比较麻烦，经常需要动态加载某条曲线，改良中。 (3)如何在不修改程序版本的基础上，优化这种现象(Linux系统参数调整) (4)程序的哪一部分可能形成这样的开销情况(大量使用内存进行交互)，缩小排查的范围(拟定后期的测试计划) 怀疑和系统的连接数与mysql的连接数有关，一个用户登录到底使用了几个Connections问题(mysql端)，连接数不释放也可能造成内存持续增长 可能与外网的内存分配机制，这个方面待确定 可能和外网的CentOS系统ipc参数有关，这个系统参数的配置可以在一定程序上缓解系统的压力，优化内存的使用和分配机制 超级详细Tcpdump 的用法： 第一种是关于类型的关键字，主要包括host，net，port, 例如 host 210.27.48.2，指明 210.27.48.2是一台主机，net 202.0.0.0 指明 202.0.0.0是一个网络地址，port 23 指明端口号是23。如果没有指定类型，缺省的类型是host. 第二种是确定传输方向的关键字，主要包括src , dst ,dst or src, dst and src ,这些关键字指明了传输的方向。举例说明，src 210.27.48.2 ,指明ip包中源地址是210.27.48.2 , dst net 202.0.0.0 指明目的网络地址是202.0.0.0 。如果没有指明方向关键字，则缺省是src or dst关键字。 第三种是协议的关键字，主要包

括fddi,ip,arp,rarp,tcp,udp等类型。Fddi指明是在FDDI(分布式光纤数据接口网络)上的特定 的网络协议，实际上它是"ether"的别名，fddi和ether具有类似的源地址和目的地址，所以可以将fddi协议包当作ether的包进行处理和 分析。其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任何协议，则tcpdump将会监听所有协议的信息包。 除了这三种类型的关键字之外，其他重要的关键字如下：gateway, broadcast,less,greater,还有三种逻辑运算，取非运算是 not ! , 与运算是and,amp..或运算 是or , | | ；这些关键字可以组合起来构成强大的组合条件来满足人们的需要，下面举几个例子来说明。 普通情况下，直接启动tcpdump将监视第一个网络界面上所有流过的数据包。# tcpdump tcpdump: listening on fxp011:58:47.873028 202.102.245.40.netbios-ns > 202.102.245.127.netbios-ns: udp 5011:58:47.974331 0:10:7b:8:3a:56 > 1:80:c2:0:0:0 802.1d ui/C len=43 0000 0000 0080 0000 1007 cf08 0900 0000 0e80 0000 902b 4695 0980 8701 0014 0002 000f 0000 902b 4695 0008 0011:58:48.373134 0:0:e8:5b:6d:85 > Broadcast sap e0 ui/C len=97 ffff 0060 0004 ffff ffff ffff ffff ffff 0452 ffff ffff 0000 e85b 6d85 4008 0002 0640 4d41 5354 4552 5f57 4542 0000 0000 0000 00使用-i参数指定tcpdump监听的网络界面，这在计算机具有多个网络界面时非常有用，使用-c参数指定要监听的数据包数量，使用-w参数指定将监听到的数据包写入文件中保存 A想要截获所有210.27.48.1 的主机收到的和发出的所有的数据包：#tcpdump host 210.27.48.1 B想要截获主机210.27.48.1 和主机210.27.48.2 或210.27.48.3的通信，使用命令：（在命令行中适用 括号时，一定要#tcpdump host 210.27.48.1 and \

(210.27.48.2 or 210.27.48.3 \) C如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：#tcpdump ip host 210.27.48.1 and ! 210.27.48.2D如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令：#tcpdump tcp port 23 host 210.27.48.1E 对本机的udp 123 端口进行监视 123 为ntp的服务端口# tcpdump udp port 123 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