审计并跟踪Linux系统的异常活动详解 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/221/2021_2022__E5_AE_A1_E8_AE_A1_E5_B9_B6_E8_c103_221651.htm 一些异常用户试图移去系统上的所有活动记录(比如~/.bash_history),不过我们可以使用专门的工具来监视所有用户执行的命令。推荐你使用进程记帐来记录用户的活动,你可以通过进程记帐查看每一个用户执行的命令,包括CPU时间和内存占用。 Psacct程序提供了几个进程活动监视工具: ac, lastcomm, accton和sa。 ◆ac命令显示用户连接时间的统计。 ◆lastcomm命令显示系统执行的命令。 ◆accton命令用于打开或关闭进程记帐功能。 ◆sa命令统计系统进程记帐的情况。 1). 安装psacct或acct软件包 如果你使用RHEL, 使用up2date命令: # up2date psacct 如果你使用CentOS/Fedora Core Linux, 使用yum命令: $ sudo apt-get install acct 或 # apt-get install acct 2). 启动psacct/acct服务 在Ubuntu/Debian Linux系统上, pacct可以自动启动。(安装包会在系统上创建一个/var/account/pacct文件)。但是在Red Hat/Fedora Core/Cent OS, 你需要手动启动psacct服务。敲入下面两个命令创建/var/account/pacct文件和启动pacct服务: # chkconfig psacct on # /etc/init.d/psacct start 如果你使用Suse Linux, 服务的名称为acct, 敲入下面的命令: # chkconfig acct on # /etc/init.d/acct start 现在我们可以了解如何利用这些工具来监视用户的命令和时间。 3). 显示用户连线时间的统计信息 命令可以根据登陆数/退出数在屏幕上打印出用户的连线时间(单位为小时)。总计时间也可以打印出来。如果你执行没有任何参数的ac命令, 屏幕将会显示总计的连线时间: $ ac 100Test