用Swatch做Linux日志分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E7_94_A8Swatch_E5_c103_144465.htm Swatch从字面上可以简单理解为Watcher(守护者). 其它的日志分析软件定期地扫描日志文件, 向你报告系统已经发生的问题或者状况. Swatch程序不仅能够做这些, 而且它能够像Syslogd守护程序那样主动的扫描日志文件并对特定的日志消息采取修复行动. 一. 准备 1. 下载和解压缩最新的Swatch软件包.建议从Swatch的官方网站获得可靠的Swatch软件包. 下载网址: http://sourceforge.net/projects/swatch/ 1) 创建Swatch软件包存放的目录. #mkdir -p /usr/local/src/log 2) 解压缩源代码包, 在log目录下会生成一个新的目录apache_1.3.33 #tar zpxf swatch-3.1.1.tar.gz 二. 安装 #cd swatch-3.1.1#make#make test#make install#make realclean Swatch程序安装成功后, Perl模块将会用于Swatch程序的运行. 三. 配置 Swatch程序使用正向表达式(Regular Expressions)来发现感兴趣的目标行. 一旦Swatch发现某一行匹配预设定的模式, 它会立即采取行动, 比如说屏幕打印, 发送电子邮件, 或者采取用户预先设定的行动. watchfor /[dD]enied｜/DEN.*ED/ech-o boldbell 3mailexe-c "/etc/call_pager 5551234 08" 上面的脚本是Swatch配置文件一个部分的例子. 首先Swatch在指定的日志文件中寻找包含设定单词"denied, Denied, 或者其它以DEN开始或者以ED结束的单词的行. 一旦搜索到某行包含三个搜索单词中的任何一个. Swatch程序立即向终端显示粗体行和响铃三下, 然后发送电子邮件给运行swatch程序的用户(通常是 root用户)警报所在行和执

行/etc/call_paper程序, 忽略sendmail, fax, unimportant stuff. 在这个例子当中, 搜索字符串sendmail, fax和unimportant stuff将被忽略. 甚至他们符合预定搜索字符串中的一个. 四. 使用 使用Swatch非常的简单, 如通常使用Swatch日志, 运行: swatch --config-file=/home/zhaoke/swatch.conf --examine=/var/log/messages 上面的例子中配置文件所在的系统绝对路径是/home/zhaoke/swatch.conf, 需要检查的日志文件是/var/log/messages. 使用swatch检查不段增加的日志文件: swatch --config-file=/home/zhaoke/swatch.conf --tail-file=/var/log/messages 