

简单高效：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_ti2020/145/2021_2022__E7_AE_80_E5_8D_95_E9_AB_98_E6_c103_145144.htm 日志文件是我们发现系统问题的重要参考信息. 大部分的系统服务出现问题时都会给syslogd(系统日志守护进程)发送消息. 然后用户发觉并根据错误提示信息采取行动. 然而对于1000行以上的日志文件, 我们必须使用日志检查工具节省时间和避免漏掉重要信息. 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. 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