Linux操作系统的定期检查和维护介绍 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_Linux_E6_93_8D_E4_BD_c103_145093.htm 引:俗话说：“ 道高一尺，魔高一丈 ”。只要是连上网的计算机，就有可被入侵。因此系统的定期检查和维护是相当重要的，对于及时发现入侵很有帮助，有助于我们亡羊补牢。 我们要赶在入侵者还没有破坏系统和数据之前把它们清理出去。所以下面就给大家讲一下这方面的技巧。 一、优化分区结构 这对维护很有好处，我们应该把Linux的文件系统分成几个主要的分区，每个分区分别进行不同的配置和安装，一般情况下至少要建立/、 /usr/local 、/var和/home等分区。/usr可以安装成只读并且可以被认为是不可修改的。如果/usr中有任何文件发生了改变，那么系统将立即发出安全报警。当然这不包括用户自己改变/usr中的内容。/lib、/boot和/sbin的安装和设置也一样。在安装时应该尽量将它们设置为只读，并且对它们的文件、目录和属性进行的任何修改都会导致系统报警。 当然将所有主要的分区都设置为只读是不可能的,有的分区如/var等，其自身的性质就决定了不能将它们设置为只读，但应该不允许它具有执行权限。 二、保护log文件 当与log文件和log备份一起使用时不可变和只添加这两种文件属性特别有用。这通常需要在log更新脚本中添加一些控制命令。 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