美国虚拟主机linux系统下的安全设置Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E7_BE_8E_E5_9B_BD_E8_99_9A_E6_c103_645321.htm 美国虚拟主机大都使用Linux操作系统，因此当用户在使用美国虚拟主机的时候，Linux系统的安全问题就成为了使用者最为关心的问题，毕竟谁都希望自己操作的是一个稳定又安全的系统。 什么是Linux呢？Liunx的官方定义：“ Linux是一种UNIX操作系统的克隆，它（的内核）由Linux Torvalds以及网络上组织松散的黑客队伍一起从零开始编写而成。LINUX的目标是保持和POSIX的兼容。 ”众所周知，Linux是一种开放源代码的操作系统，由于它的自由开放性和技术先进性，顺应了广大软件开发商及用户日益高涨的对信息系统知情权的要求，从而迅速赢得了普遍的支持和认同，并得以迅速传播。 美国虚拟主机Linux系统下的安全设置需要从三个方面去考虑： 首先，Linux系统本身的安全优势： 1、Open的思想，开放源代码，自主改进或定制 2、Free的精神，自由使用 3、完善的网络功能,内置TCP/IP协议 4、真正意义上的多任务、多用户操作系统 5、完全运行于保护模式，充分利用了CUP性能 6、先进的内存管理机制，更加有效地利用物理内存 7、稳定性，安全性，高效性 8、与UNIX系统在源代码级兼容，符合IEEE POSIX标准 9、支持数十种文件系统格式 10、设备独立性，良好的可移植性 11、无昂贵的版权费，低成本 正是因为Linux的安全特性，使得它在市场中保持了一定的占有率，且市场占有率有扩大的趋势。 其次，当你使用Linux操作系统处理安全问题时，下面的一些规则和技巧也许会派上用场。 1.在以root

身份登录时，避免做一些常规工作。这会减少你感染病毒的风险，并且可以防止你犯一些错误。 2.如果可能的话，在一台远程机器上工作时，尽量使用加密连接。使用SSH来代替telnet、ftp、rsh、rlogin应当成为标准的操作规范。因为SSH的安全性众所周知。 3.尽量保持与网络有关的最重要的程序包的最新，最好订阅一些相应的邮件列表以获得bind、postfix、ssh等程序的最新版本的公告。同样的原则也适用于与本地安全相关的软件。 4.禁用你并不绝对需要的任何用于服务器正常工作的任何网络服务。这会使你的系统更加安全。可以用netstat程序发现套接字状态为LISTEN的开放端口。 5.来自SUSE的RPM程序包都进行了数字签名。你可以在控制台上输入下面的内容来验证任何SUSE RPM程序包的完整性：rpm chechsig package.rpm。所需要的公共gpg-key要在安装时要复制到root的主目录。 6.经常检查用户和系统文件的备份。请记住：如果你没有测试备份是否正常工作，它就形同虚设，毫无价值。 7.检查你的日志文件。在可能的情况下，编写小型的脚本程序来搜索可疑的项目。 8.设置安全措施要保证其冗余性。多看到一些安全消息总比没有消息要好得多。固得全能美国空间,免备案,多子目录绑定。 最后，在选择美国虚拟主机的时候，一个好的运营商能为用户省却许多麻烦，这包括主机投放机房的位置和质量，运营商的服务质量等等，都是用户必须考虑的因素。 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