 BIOS安全 记着要在BIOS设置中设定一个BIOS密码，不接收软盘启动。这样可以阻止不怀好意的人用专门的启动盘启动你的Linux系统，并避免别人更改BIOS设置，如更改软盘启动设置或不弹出密码框直接启动服务器等。 LILO安全 在“ /etc/lilo.conf ”文件中添加3个参数：time-out、restricted 和 password。这些选项会在启动时间（如“ linux single ”）转到启动转载程序过程中，要求提供密码。 步骤1 编辑lilo.conf文件（/etc/lilo.conf），添加和更改这三个选项： QUOTE: boot=/dev/hda map=/boot/map install=/boot/boot.b time-out=00 #change this line to 00 prompt Default=linux restricted #add this line password=gt. #add this line and put your password image=/boot/vmlinuz-2.2.14-12 label=linux initrd=/boot/initrd-2.2.14-12.img root=/dev/hda6 read-only 步骤2 由于其中的密码未加密，“ /etc/lilo.conf ”文件只对根用户为可读。 [root@kapil /]# chmod 600 /etc/lilo.conf （不再为全局可读） 步骤3 作了上述修改后，更新配置文件“ /etc/lilo.conf ”。 [Root@kapil /]# /sbin/lilo -v （更新lilo.conf文件） 步骤4 还有一个方法使“ /etc/lilo.conf ”更安全，那就是用chattr命令将其设为不可改： [root@kapil /]# chattr i /etc/lilo.conf 它将阻止任何对“ lilo.conf ”文件的更改，无论是否故意。 关于lilo安全的更多信息，请参考LILO。 禁用所有专门帐号 在lp, sync, shutdown, halt, news, uucp, operator, games, gopher等系统中，将你不使用的所有默认用户帐号和群组帐号删除。 要删除用户

帐号： [root@kapil /]# userdel LP 要删除群组帐号： [root@kapil /]# groupdel LP 选择恰当的密码 选择密码时要遵循如下原则：密码长度：安装Linux系统时默认的最短密码长度为5个字符。这个长度还不够，应该增为8个。要改为8个字符，必须编辑 login.defs 文件（/etc/login.defs）： PASS_MIN_LEN 5 改为： PASS_MIN_LEN 8 “ login.defs ”是登录程序的配置文件。启用盲区密码支持 请启用盲区密码功能。要实现这一点，使用“ /usr/sbin/authconfig ”实用程序。如果想把系统中现有的密码和群组改为盲区密码和群组，则分别用 pwconv 和 grpconv 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