

LILO 的安全配置

September 6, 2000

Sinbad Technical Publications
Website: <http://sinbad.zhoubin.com>
© Copyright 2000, All Rights Reserved

下面一些参数配置可以避免在启动时用单用户模式获得 **root shell**。

delay=x

这个数值决定了 **LILO** 等待多长时间（以 10 秒为单位）接受用户输入，然后才启动默认的选项。如果不是多系统启动，其值应设为 **0**。

prompt

有了这个选项，**LILO** 将等待用户的输入，在没有设置 **timeout** 的情况下，**LILO** 不会自行启动系统。

restricted

如果用户输入了参数（例如 **linux single**）来启动，这个选项将要求用户输入密码。

password=

这个选项和 **restricted** 一起使用，其值是用户设定的密码。由于是明文存放，所以 **/etc/lilo.conf** 要设置为仅 **root** 可读写。

下面给出一个 **/etc/lilo.conf** 的例子：

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=100
default=linux
image=/boot/vmlinuz-2.2.12-20
label=linux
root=/dev/hda1
read-only
restricted
password=kpAsSb0rv_f
```

上面的配置有以下功能：

1. 以/boot/vmlinuz-2.2.12 内核来启动系统，它存放在 IDE1 硬盘上在 MBR 之后的第一个分区上。

2. 可以正常的远程启动系统，但如果输入“linux single”，LILO 将要求输入密码。

3. 如果用参数“linux single”启动系统，timeout 选项给出 10 秒时间接受输入密码。

还需要注意以下步骤：

1. BIOS 一定要设置密码保护并且仅从 C 盘启动。

2. /etc/lilo.conf 设置为不可变，用 chattr 命令：

```
# chattr +i /etc/lilo.conf
```

这将会防止 lilo.conf 无意中或其他原因被修改。如果以后需要改动，必须先去掉不可变的标记：

```
# chattr -i /etc/lilo.conf
```

提示：只有 root 才能对文件设置不可变的标记。