Red Hat Linux 9

Red Hat Linux 定制指南

Red Hat Linux 9: Red Hat Linux 定制指南

Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
电话：+1 919 754 3700
电话：888 733 4281
传真：+1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

rhl-cg(ZH-CN)-9-Print-RHI (2003-02-20T01:08)

目录

介绍

欢迎使用《*Red Hat Linux* 定制指南》。

《*Red Hat Linux* 定制指南》包含关于如何定制Red Hat Linux 系统来满足你的需要的信息。如果你需要一本步骤分明、面向任务的指南来帮助你配置和定制系统，这本书就是你的理想选择。本书讨论了许多中等难度的课题，它们包括：

- 设置网卡（NIC）
- 执行kickstart 安装
- 配置Samba 共享
- 使用RPM 来管理软件
- 判定系统信息
- 升级内核

本书被分成下面几个主要部分：

- 与安装相关的信息
- 与网络相关的配置
- 系统配置
- 软件包管理

该指南假定你对Red Hat Linux 系统已有基本的了解。如果你需要涉及基本课题的参考资料，譬如配置桌面或播放音频光盘，请参阅《*Red Hat Linux* 入门指南》。如果你需要更高级的文档，譬如Red Hat Linux 文件系统总览，请参阅《*Red Hat Linux* 参考指南》。

Red Hat Linux 指南手册的HTML 和PDF 版本在文档光盘上可以找到，它们也可以在http://www.redhat.com/docs/ 网站中找到。

注记

虽然本书尽可能地反映了最新信息，你应该阅读“*Red Hat Linux* 发行注记”来获得在我们的文档定稿之前还没来得及包括的信息。它们可以在Red Hat Linux 的第一张光盘上找到，也可以在以下网址上找到：

```
http://www.redhat.com/docs/manuals/linux
```

1. 本书的更变

本书在从前的基础上做了些增补，包括了Red Hat Linux 9 中的新功能，以及许多被读者要求的课题。本书中的重要改变包括：

实现磁盘配额

‘ 新增了这一章来解释如何配置和管理磁盘配额。

验证配置

‘ 新增了这一章来解释如何使用验证配置工具。

用户配置

‘ 本章被扩展来包括管理用户和组群的命令行工具，并且解释了系统上添加了新用户后的情形。

Samba

‘ 本章被扩充来包括新增的**Samba** 服务器配置工具。

打印机配置

‘ 本章为新增的打印机配置工具界面、**GNOME** 打印管理器、以及面板上的拖放打印机图标重新撰写。

Kickstart

‘ kickstart 选项已被更新来包括Red Hat Linux 9 中的新选项。“**Kickstart** 配置器”这一章也被更新来包括一些新功能。

网络配置

‘ 本章已为最新的网络管理工具界面和功能而更新。

时间和日期配置

‘ 本章已被移到《*Red Hat Linux* 入门指南》。

2. 文档约定

在你阅读这本手册的时候，你会注意到某些字词使用了不同的字体、大小和粗细。这种突出显示是有矩可循的；用同一风格来代表不同字词以表明它们属于同一类型。用这种方式来代表的各种字词类型包括：

`command`

‘ Linux 命令（以及其它操作系统的命令，若使用的话）用这种方式代表。它向你表明你可以在命令行中键入词或词组然后按[Enter] 键来启用命令。有时，命令中会包括应用另一种方式显示的词（例如文件名），在这种情况下，它们被视为命令的一部分，因而整个词组都会被显示为命令。例如：

使用`cat testfile` 命令来查看当前工作目录中一个叫做`testfile` 的文件。

`filename`

‘ 文件名、目录名、路径、以及RPM 软件包名用这种方式代表。它表明在你的Red Hat Linux 系统上存在着一个叫这个名称的文件或目录。例如：

你的主目录中的`.bashrc` 文件包括你自用的bash shell 定义和别名。

`/etc/fstab` 文件包括关于不同系统设备和文件系统的信息。

如果你想使用一个万维网服务器日志文件分析程序的话，安装`webalizer` RPM。

application

‘ 这种方式向你表明该程序是一个终端用户的应用程序（与系统软件相对）。例如：

使用**Mozilla** 来浏览万维网。

[key]

‘ 键盘上的按键用这种方式代表。例如：

要使用[Tab] 键补全，键入一个字符然后按[Tab] 键。你的终端机上就会显示目录中起首为那个字符的文件列表。

[key]-[combination]

‘ 一个击键的组合用这种方式代表。例如：

[Ctrl]-[Alt]-[Backspace] 击键组合会退出你的图形会话，把你返回到图形登录屏幕或控制台。

「**GUI** 界面上的文本」

‘ 在GUI 界面屏幕或窗口中的标题、词汇、或短语会用这种方式显示。它用来标明某个GUI 屏幕或GUI 屏幕上的某个元素（譬如与复选箱或字段相关的文本）。例如：

如果你想要在你的屏幕保护程序停止前要求口令的话，选择「需要口令」复选箱。

「**GUI** 屏幕或窗口上的最上级菜单」

‘ 用这种方式表示的词汇表明它位于一个下拉菜单的最上级。如果你在GUI 屏幕上点击了这个词，应出现菜单的其它部分。例如：

在GNOME 终端的「文件」下，你会看到「新建标签」选项，它允许你在同一窗口中打开多个shell 提示。

如果你需要在GUI 菜单上点击一系列命令的话，它们会如下面的例子中所示：

点击面板上的「主菜单」=> 「编程」 => 「**Emacs**」来启动**Emacs** 文本编辑器。

「**GUI** 屏幕或窗口中的按钮」

‘ 这种方式表明它是GUI 屏幕上可点击的按钮。例如：

点击「后退」按钮来返回到你刚才查看的网页。

`computer output`

‘ 这类方式的文本表明它是计算机在命令行中显示的输出。你键入命令的反应、错误讯息、以及程序或脚本中向你要求输入的互动式提示，都是用这种格式来代表的。例如：

使用ls 命令来显示目录的内容：

```
$ ls
Desktop       about.html   logs    paulwesterberg.png
Mail        backupfiles   mail    reports
```

命令返回的输出（在上面的例子中，是目录的内容）用这种方式来显示。

`prompt`

‘ 提示是计算机在向你表明它在等待你的输入。它会用这种方式来显示。例如：

```
$
```

```
#
```

```
[stephen@maturin stephen]$
```

```
leopard login:
```

`user input`

‘ 用户键入的文本。无论是在命令行中还是在GUI 屏幕上的文本箱内的输入都会用这种方式来显示。在下面的例子中，**`text`** 用这种方式显示：

要把你的系统引导入基于文本的安装程序，你需要在`boot:` 提示下键入**`text`** 命令。

除此之外，我们还使用几种不同的方式来强调某些信息。按照信息对你的系统的重要程度，它们被标为注记、窍门、重要、小心、或警告。例如：

注记

切记，Linux 区分大小写。换一句话说，rose 不是ROSE 或rOsE。

窍门

目录/usr/share/doc 包括了关于你的系统上安装的软件包的附加信息。

重要

如果你修改了DHCP 配置文件，这些改变在你重启DHCP 守护进程之后才会生效。

小心

不要以根用户身份来执行日常任务— 使用一个常规的用户帐号，除非你需要使用根帐号来进行系统管理任务。

警告

如果你选择要不进行手工分区，服务器安装会删除所有安装了的硬盘驱动器上的现存分区。除非你确信你没有需要保留的数据，请不要选择这种安装类型。

3. 未来的扩充

《*Red Hat Linux* 定制指南》是Red Hat 为Red Hat Linux 用户提供及时有效的支持所做出的承诺中的一部分。随着新工具和新程序的发行，本指南也会被扩充来包括这些新工具和新程序。

3.1. 递交你的反馈

如果你在《*Red Hat Linux* 定制指南》中发现了错别字，或者有改进本书的建议，我们很希望能收到您的来函！请向Bugzilla（http://bugzilla.redhat.com/bugzilla/）提交一份关于rhl-cg 的报告。

在提交报告的时候，请明确指定本书的标记：

```
rhl-cg(ZH-CN)-9-Print-RHI(2003-02-20T01:08)
```

只有指定这本指南的标记，我们才能确切了解您的指南的版本。

如果你有改进本书的建议，请尽可能详细地阐明。如果你发现了错误，请包括所在章节及段落，因此我们可以轻易地查找到。

4. 注册支持

如果你有一份Red Hat Linux 9 的正式版本，请记住注册以便获得Red Hat 顾客可以享受的诸多权益。

依据你购买的Red Hat Linux 产品而定，你可以享受部分或全部以下列举的权益：

- Red Hat 支持— 从Red Hat, Inc. 的支持组中获得关于安装问题的帮助。
- Red Hat 网络— 轻松地更新你的软件包，以及接收为你的系统定制的安全通知。详情请参阅http://rhn.redhat.com。
- *Under the Brim: The Red Hat E-Newsletter* — 每个月可直接从Red Hat 获取最新的新闻和产品信息。

要注册，请访问：http://www.redhat.com/apps/activate/。你可以在Red Hat Linux 产品盒内的黑色、红色和白色的登记卡上找到你的产品ID。

关于Red Hat Linux 的技术支持的详细资料，请参阅《*Red Hat Linux* 安装指南》中的附录：获取技术支持。

感谢您选择了Red Hat Linux！祝您一切顺利！

Red Hat 文档组

I. 文件系统

文件系统（*File system*）指代贮存在计算机上的文件和目录。文件系统可以有不同的格式，叫做文件系统类型（*file system types*）。这些格式决定信息是如何被贮存为文件和目录。某些文件系统类型贮存重复数据，某些文件系统类型加快硬盘驱动器的存取速度。这个部分讨论ext3、交换区、RAID、和LVM 文件系统类型。它还讨论了`parted` 这个用户管理分区的工具。

目录

redhat.

1. ext3 文件系统

从Red Hat Linux 7.2 发行版本开始，默认的文件系统已从ext2 格式转换成登记式*ext3* 文件系统。

1.1. ext3 的特性

一言以蔽之，ext3 文件系统是ext2 文件系统的增进版本。这些增进提供了以下优越性：

可用性

- 在异常断电或系统崩溃（又称不洁系统关机，*unclean system shutdown*）发生时，每个在系统上挂载了的ext2 文件系统必须要使用`e2fsck` 程序来检查其一致性。这是一个很费时的过程，特别是在检查包含大量文件的庞大文件卷时，它会大大耽搁引导时间。在这期间，文件卷上的所有数据都不能被访问。

  由ext3 文件系统提供的登记报表方式意味着不洁系统关机后没必要再进行此类文件系统检查。使用ext3 系统时，一致性检查只在某些罕见的硬件失效（如硬盘驱动器失效）情况下才发生。不洁系统关机后，ext 文件系统的恢复时间不根据文件系统的大小或文件的数量而定，而是根据用于维护一致性的登记日志（*journal*）的大小而定。根据你的硬件速度，默认的登记日志只需花大约一秒钟来恢复。

数据完好性

- ext3 文件系统在发送了不洁系统关机时提供更强健的数据完好性。ext3 文件系统允许你选择你的数据接受的保护类型和级别。Red Hat Linux 9 默认配置ext3 文件卷来保持数据与文件系统状态的高度一致性。

速度

- 尽管ext3 把数据写入不止一次，它的总处理能力在多数情况小仍比ext2 系统要高。这是因为ext3 的登记报表方式优化了硬盘驱动器的头运动。你可以从三种登记模式中选择来优化速度，但是这么做会在保持数据完好性方面做出一些牺牲。

简易转换

- 你可以轻而易举地不经重新格式化而把ext2 转换为ext3 系统，从而获得强健的登记式文件系统的优越性。请参阅第1.3 节 来获取如何完成这一任务的说明。

如果你执行Red Hat Linux 9 的完整安装，被分配给系统的Linux 分区的默认文件系统就是ext3。如果你从某个使用ext2 分区的Red Hat Linux 版本中升级，安装程序就会允许你把这些分区转换为ext3 分区，并且不会丢失数据。细节请参阅《*Red Hat Linux* 安装指南》的附录“升级现存系统”。

以下各节会指导你进行ext3 分区的创建和微调。如果你有ext2 分区，并在运行Red Hat Linux 9，你可以跳过以下的分区和格式化章节，直接转到第1.3 节。

1.2. 创建一个ext3 文件系统

安装后，你有时会有必要创建一个新的ext3 文件下。譬如，如果你给Red Hat Linux 系统添加了一个新的磁盘驱动器，你可能想给这个磁盘驱动器分区，并使用ext3 文件系统。

创建ext3 文件系统的步骤如下所列：

1. 使用`parted` 或`fdisk` 来创建分区。
2. 使用`mkfs` 来把分区格式化为ext3 文件系统。

3. 使用e2label给分区标签。
4. 创建挂载点。
5. 把分区添加到/etc/fstab 文件中。

关于执行这些步骤的信息，请参阅第5章。

1.3. 转换到ext3 文件系统

tune2fs 程序能够不改变分区上的已存数据来给现存的ext2 文件系统添加一个登记报表。如果文件系统在改换期间已被挂载，该登记报表就会被显示为文件系统的根目录中的.journal 文件。如果文件系统没有被挂载，登记报表就会被隐藏，根本就不会出现在文件系统中。

要把ext2 文件系统转换成ext3，登录为根用户后键入：

```
/sbin/tune2fs -j /dev/hdbX
```

在以上命令中，把/dev/*hdb* 替换成设备名，把*X* 替换成分区号码。

以上命令执行完毕后，请确定把/etc/fstab 文件中的ext2 文件系统改成ext3 文件系统。

如果你在转换你的根文件系统，你将需要使用一个initrd 映像（或RAM 磁盘）来引导。要创建它，运行mkinitrd 程序。关于使用mkinitrd 命令的信息，请键入man mkinitrd。还请确定你的GRUB 或LILO 配置会载入initrd。

如果改换没有成功，系统仍旧能够引导，只不过文件系统将会被挂载为ext2 而不是ext3。

1.4. 还原到ext2 文件系统

因为ext3 相对来说比较新，某些磁盘工具可能还不支持它。例如，你可能需要使用resize2fs 来缩小某分区，该命令不支持ext3。在这种情况下，可能会有必要把文件系统暂时还原成ext2。

要还原分区，你必须首先卸载分区。方法是登录为根用户，然后键入：

```
umount /dev/hdbX
```

在以上命令中，把/dev/*hdb* 替换成设备名称，把*X* 替换成分区号码。本节以后的示例命令将会使用*hdb1* 来代表设备和分区。

下一步，把文件系统类型改回ext2，以根用户身份键入以下命令：

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

以根用户身份键入以下命令来检查分区的错误：

```
/sbin/e2fsck -y /dev/hdb1
```

然后通过键入以下命令来把分区重新挂载为ext2 文件系统：

```
mount -t ext2 /dev/hdb1 /mount/point
```

在以上命令中，把*/mount/point* 替换成分区的挂载点。

下一步，删除根目录下的.journal 文件。方法是转换到分区的挂载目录中，然后键入：

```
rm -f .journal
```

你现在就有一个ext2 分区了。

如果你永久地把分区改换成ext2，请记住更新/etc/fstab 文件。

2.

交换空间

2.1. 交换空间是什么

Linux 中的交换空间（*Swap space*）在物理内存（RAM）被充满时被使用。如果系统需要更多的内存资源，而物理内存已经充满，内存中不活跃的页就会被移到交换空间去。虽然交换空间可以为带有少量内存的机器提供帮助，但是这种方法不应该被当做是对内存的取代。交换空间位于硬盘驱动器上，它比进入物理内存要慢。

交换空间可以是一个专用的交换分区（推荐的方法），交换文件，或两者的组合。

交换空间的总大小应该相当于你的计算机内存的两倍和32 MB这两个值中较大的一个，但是它不能超过2048 MB（2 GB）。

2.2. 添加交换空间

有时，你会有必要在安装后添加更多的交换空间。例如，你把系统内存从64 MB 升级到128 MB，但是你只有128 MB 的交换内存。如果你执行的是大量使用内存的操作或运行需要大量内存的程序，把交换区增加到256 MB 可能会对你有利。

你有两种选择：添加一个交换分区或添加一个交换文件。推荐你添加一个交换分区，不过，若你没有多少空闲空间可用，创建交换分区可能会不大容易。

要添加一个交换分区（假设/dev/hdb2 是你想添加的交换分区）：

1. 硬盘驱动器不能在被使用（分区不能被挂载，交换分区不能被启用）。要达到这一目的的最简单方法是在救援模式下引导你的系统。请参阅第9章来获得将系统引导入救援模式的说明。当提示挂载文件系统时，选择「跳过」。

   如果驱动器不包含任何被使用的分区，你还可以卸载这些分区，使用swapoff 命令来关闭硬盘驱动器上的所有交换空间。

2. 使用parted 或fdisk 来创建交换分区。parted 比fdisk 使用起来更方便，因此，只有parted 在这里会被说明。要使用parted 来创建交换分区：

   - 在shell 提示下以根用户身份键入命令：parted /dev/*hdb*。这里的/dev/*hdb* 是你的带有空闲空间的硬盘驱动器的设备名称。
   - 在(parted) 提示下，键入**print** 来查看现存的分区和空闲空间的数量。起止值以MB 为单位。判定硬盘驱动器上的空闲空间数量，以及你想给新建的交换分区分配的空间数量。
   - 在(parted) 提示下，键入**mkpartfs *part-type* linux-swap *start end***，这里的*part-type* 是primary、extended、logical 中的一个，*start* 是分区的起始点，*end* 是分区的终止点。

     
     警告

     改变会立即发生，在键入时请谨慎从事。

   - 键入**quit** 来退出parted。

3. 现在，你就可以创建交换分区了，使用mkswap 命令来设置交换分区。在shell 提示下以根用户身份键入以下命令：

   ```
   mkswap /dev/hdb2
   ```

4. 要立即启用交换分区，键入以下命令：

```
swapon /dev/hdb2
```

5. 要在引导时启用，编辑/etc/fstab 文件来包括以下行：
```
/dev/hdb2       swap         swap  defaults   0 0
```
在系统下次引导时，它就会启用新建的交换分区。

6. 新添了交换分区并启用它之后，请查看cat /proc/swaps 或free 命令的输出来确保交换分区已被启用了。

要添加交换文件：

1. 判定新交换文件的大小，将大小乘以1024 来判定块的大小。例如，大小的64 MB 的交换文件的块大小为65536。
2. 在shell 提示下以根用户身份键入以下命令，其中的count 等于想要的块大小：
```
dd if=/dev/zero of=/swapfile bs=1024 count=65536
```
3. 使用以下命令来设置交换文件：
```
mkswap /swapfile
```
4. 要立即启用交换文件而不是在引导时自动启用，使用以下命令：
```
swapon /swapfile
```
5. 要在引导时启用，编辑/etc/fstab 文件来包含以下行：
```
/swapfile       swap         swap  defaults   0 0
```
系统下次引导时，它就会启用新建的交换文件。

6. 新添了交换分区并启用它之后，请查看cat /proc/swaps 或free 命令的输出来确保交换分区已被启用了。

2.3. 删除交换空间

要删除交换分区：

1. 硬盘驱动器不能在被使用（分区不能被挂载，交换分区不能被启用）。要达到这一目的的最简单方法是在救援模式下引导你的系统。请参阅第9章来获得将系统引导入救援模式的说明。当提示挂载文件系统时，选择「跳过」。

   如果驱动器不包含任何被使用的分区，你还可以卸载这些分区，使用swapoff 命令来关闭硬盘驱动器上的所有交换空间。

2. 在shell 提示下以根用户身份键入以下命令来确定交换分区已被禁用（这里的/dev/hdb2 是交换分区）：
```
swapoff /dev/hdb2
```
3. 从/etc/fstab 文件中删除这个项目。
4. 使用parted 或fdisk 来删除分区。只有parted 在这里会被说明。要使用parted 来删除分区：
   - 在shell 提示下以根用户身份键入命令：parted /dev/*hdb*。这里的/dev/*hdb* 是你的带有交换空间的硬盘驱动器的设备名称。
   - 在(parted) 提示下，键入**print** 来查看现存的分区并判定你想删除的交换分区的次要号码。
   - 在(parted) 提示下，键入**rm *MINOR***，这里的*MINOR* 是你想删除的分区的次要号码。


警告

改变会立即发生，你必须键入正确的次要号码。

- 键入**quit** 来退出parted。

要删除交换文件：

1. 在shell 提示下以根用户身份执行以下命令来禁用交换文件（这里的/swapfile 是交换文件）：
   ```
   swapoff /swapfile
   ```
2. 从/etc/fstab 中删除该项目。
3. 删除实际文件：
   ```
   rm /swapfile
   ```

2.4. 移动交换空间

要把交换空间从某处移到另一处，请首先遵循删除交换空间的说明，再遵循添加交换空间的说明。

redhat.

3. 独立磁盘冗余阵列（RAID）

3.1. RAID 是什么?

RAID 的基本目的是把多个小型廉价的磁盘驱动器合并成一组阵列来达到大型昂贵的驱动器所无法达到的性能或冗余性。这个驱动器阵列在计算机眼中就如同一个单一的逻辑贮存单元或驱动器。

RAID 是一种在多个磁盘上分散信息的方法。它使用磁盘分条（*disk striping*，RAID 级别0）、磁盘镜像（*disk mirroring*，RAID 级别1）、和带有奇偶校验的磁盘分条（*disk striping with parity*，RAID 级别5）之类的技术来达到冗余性，减低潜伏时间，并且（或者）增加磁盘读写的带宽，提高从硬盘崩溃中恢复的能力。

RAID 的基本原理是，数据必须使用一致的形式被分散到阵列中的驱动器上。要打到这个目的，数据必须被分割成大小一致的“块”（大小通常是32K 或64K，也可使用不同大小）。每一块都会根据所用的RAID 级别而写入其中的一个硬盘驱动器。当数据要被读取时，这个进程就会反过来进行，造成一个多个驱动器好象是一个大驱动器的假象。

3.2. 谁应该使用RAID

任何需要使大量数据触手可及的人（如一般的系统管理员）都可以从RAID 技术中受益。使用RAID 的主要原因包括：

- 加快速度
- 使用一个虚拟磁盘，从而增加贮存容量
- 减少磁盘失效带来的不利影响

3.3. 硬件RAID 和软件RAID

RAID 技术有两种：硬件RAID 和软件RAID。

3.3.1. 硬件RAID

基于硬件的系统独立于主机之外地来管理RAID 子系统，并且它在主机处只用一个磁盘来代表每一组RAID 阵列。

连接到SCSI 控制器的，把RAID 阵列表示为单个SCSI 驱动器的设备就是一个硬件RAID 的例子。一个外部的RAID 系统把所有RAID 处理“智能”都转移到位于内部磁盘子系统中的控制器中。整个子系统都是通过一个普通的SCSI 控制器连接到主机上，对主机而言，它就象一个单一的磁盘。

RAID 控制器还以卡的形式出现。它充当操作系统的SCSI 控制器，但却控制所有驱动器本身的实际通讯。在这些情况下，你把驱动器插入到RAID 控制器中，就如同SCSI 控制器一般，但是，在这之后，你把它们添加到RAID 控制器的配置里，操作系统决不会知道其中的区别。

3.3.2. 软件RAID

软件RAID 在内核磁盘（块设备）编码中实现各类RAID 级别。因为它不需要昂贵的磁盘控制器卡或热交换底盘[1]，软件RAID 提供了最廉价的解决方法。它还可以用在较便宜的IDE 磁盘以及SCSI 磁盘。使用今日的快速CPU，软件RAID 的性能能够超出硬件RAID。

1. 热交换底盘允许你不必给系统断电而移除硬盘驱动器。

Linux 内核的MD 驱动程序是RAID 解决方案的一个例子。它完全独立于硬件。基于软件的阵列的性能独立于服务器CPU 的性能和载量之外。

关于在Red Hat Linux 安装程序中配置软件RAID 的信息，请参阅第10章。

以下为那些对软件RAID 功能感兴趣的用户列举了一些它的最重要的特性：

- 使用线程的重建进程
- 基于内核的配置
- 不必重建而可在Linux 机器间移植阵列
- 使用空闲的系统资源在后台重建阵列
- 对可热交换的驱动器的支持
- 对CPU 的自动检测以便利用某些CPU 优化功能

3.4. RAID 级别和线形支持

RAID 支持各类配置，包括级别0、1、4、5、和线形。这些RAID 类型的定义如下：

- 级别*0* — RAID 级别0，经常被称作“分条”，它是面向性能的分条数据映射技术。这意味着被写入阵列的数据被分割成条，然后被写入阵列中的其它磁盘成员，从而允许低费用的高度I/O 性能，但是它不提供冗余性。级别0 阵列的贮存能力等于硬件RAID 所有成员磁盘的总能力或软件RAID 中所有成员分区的总能力。
- 级别*1* — RAID 级别1，或“镜像”，被使用的时期长于任何其它形式的RAID。级别1 通过在阵列中的每个成员磁盘上写入相同的数据（在磁盘上留一个“镜像”副本）来提供冗余性。由于镜像的简单性和高度的数据可用性，它目前仍然很流行。使用两个以上磁盘操作的级别1 可能会在读取时使用并行访问来获得高速数据传输，但是它更常用的是独立操作以提供高速I/O 传输率。级别1 提供了极佳的数据可靠性，并提高了读取任务繁重的程序的执行性能，但是它相对的费用也较高。[2] 级别1 阵列的贮存能力与硬件RAID 中镜像的硬盘之一或软件RAID 中镜像的分区之一的储存能力相同。
- 级别*4* — 级别4 使用集中到单个磁盘驱动器上的奇偶校验[3] 来保护数据。它更适合于事务性的I/O 而不是大型文件传输。由于专职的奇偶校验磁盘代表了固有瓶颈，级别4 极少在没有写回缓存之类的技术陪同的情况下使用。虽然级别4 在某些分区方案中是一种可选项目，它在Red Hat Linux RAID 安装中却不是一个允许的选项。[4] 硬件级别4 的贮存能力相对于所有成员磁盘去掉一个后的贮存能力。软件级别4 的贮存能力相对于所有成员分区去掉一个后的贮存能力（如果它们的大小相同的话）。
- 级别*5* — 这是最普遍的RAID 类型。通过在某些或全部阵列成员磁盘驱动器中分布奇偶校验，RAID 级别5 避免了级别4 中固有的写入瓶颈。唯一的性能瓶颈是奇偶计算进程。使用现代的CPU 和软件RAID，这种情况通常不是什么大问题。与级别4 一样，其结果是非对称性能，读取大大地超过了写入性能。级别5 经常与写回缓存一起使用来减低这种非对称性。硬件级别5 的贮存能力相当于所有成员磁盘去掉一个后的贮存能力。软件RAID 级别5 的贮存能力相当于所有成员分区去掉一个后的贮存能力（如果它们的大小相同）。

---

2. RAID 级别1 的代价很高，因为你把相同的信息写入阵列中的所有磁盘，这浪费了驱动器空间。譬如，如果你设立了RAID 级别1，因而你的根分区（/）存在于两个40G 的驱动器上，你虽然总共有80G 空间，却只能访问其中的40G，因为另外的40G 就如同前40G 的镜像一样。
3. 奇偶校验的信息是基于阵列中的其它磁盘成员的内容来计算的。当阵列中的某个磁盘上的数据失效时，这则信息就会被用来重建数据。然后，在替换失效磁盘之前，被重建的数据可以用来满足失败磁盘上的I/O 请求；在替换失效磁盘之后，它可以用来在新磁盘上重建数据。
4. RAID 级别4 与级别5 所占空间相同，但是级别5 却优于级别4。由于这个原因，级别4 不被支持。

- 线形*RAID* — 线形RAID 是一种简单的驱动器聚组以便创建一个较大的虚拟驱动器。在线形RAID 中，区块从一个成员驱动器到另一个成员驱动器被依次分配，只有在第一个驱动器被完全填充后，才转到下一个驱动器。这种聚组没有提供任何性能方面的利益，因为I/O 操作不太可能在成员驱动器间被分开。线形RAID 也没有提供任何冗余性，事实上，它降低了可靠性— 如果任何一个成员驱动器失效了，整个阵列都不能被使用。它的贮存能力是所有成员磁盘的总和。

redhat.

4. 逻辑卷管理器（LVM）

从Red Hat Linux 8.0 开始，逻辑卷管理器（LVM）可以在硬盘驱动器分配上使用。

LVM 是一种把硬盘驱动器空间分配成逻辑卷的方法，这样硬盘就不必使用分区而被简易地重划大小。

使用LVM，硬盘驱动器或硬盘驱动器集合就会分配给一个或多个物理卷（*physical volumes*）。物理卷无法跨越一个以上驱动器。

物理卷被合并成逻辑卷组（*logical volume group*），唯一的例外是/boot 分区。/boot 分区不能位于逻辑卷组，因为引导装载程序无法读取它。如果你想把/ 分区放在逻辑卷上，你需要创建一个分开的/boot 分区，它不属于卷组的一部分。

由于物理卷无法跨越一个以上驱动器，如果你想让逻辑卷组跨越一个以上驱动器，你就应该在驱动器上创建一个或多个物理卷。

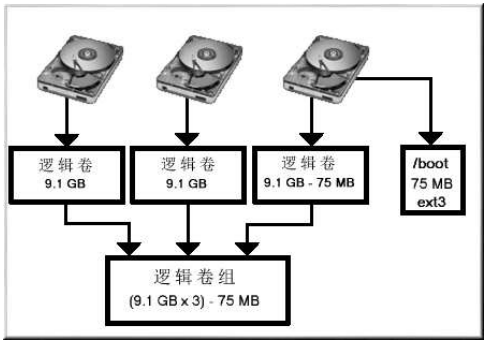


图**4-1.** 逻辑卷组

逻辑卷组被分成逻辑卷（*logical volumes*），它们被分配了挂载点（如/home 和/），以及文件系统类型（如ext3）。当“分区”达到了它们的极限，逻辑卷组中的空闲空间就可以被添加给逻辑卷来增加分区的大小。当某个新的硬盘驱动器被添加到系统上，它可以被添加到逻辑卷组中，逻辑卷是可以扩展的分区。

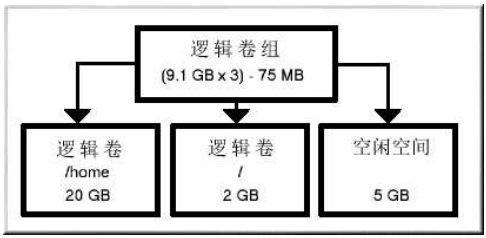


图**4-2.** 逻辑卷

另一方面，如果系统使用ext3 文件系统来分区，硬盘驱动器将被分隔成指定大小的分区。如果某分区被填满，要扩展该分区的大小并不那么容易。即便某分区被移到另一个硬盘驱动器上，原来的硬盘驱动器空间必须得被重新分配为不同的分区或不被使用。

LVM 支持必须被编译入内核。默认的Red Hat Linux 9 内核中已编译入了LVM 支持。

要了解在Red Hat Linux 安装过程中配置LVM 的详情，请参阅第11章。

redhat.

5.

管理磁盘贮存区

在你安装了Red Hat Linux 系统后，你可能想查看现存的分区表，改变分区的大小，删除分区，或从空闲空间或附加的硬盘驱动器上添加分区。parted 工具会允许你执行这些任务。本章讨论如何使用parted 命令来执行文件系统任务。此外，你还可以使用fdisk 来执行多数此类任务（除重新划分分区以外）。要获得fdisk 的更多信息，请阅读其说明书页（man）或信息页（info）。

如果你想查看或监视系统的磁盘空间用量，请参考第26.3 节。

你必须安装了parted 软件包才能使用parted 工具。要启动parted，在shell 提示下以根用户身份键入命令parted */dev/hdb*，这里的*/dev/hdb* 是你想配置的设备名称。你会看到一个(parted) 提示。键入help 来查看可用命令的列表。

如果你想创建、删除分区或重新划分分区大小，分区所在设备不能正在被使用（分区不能被挂载，并且交换空间不能被启用）。达到这个目的的最简单方法是在救援模式中引导系统。请参考第9章来获得引导到救援模式的说明。当提示挂载文件系统时，选择「跳过」。

如果驱动器不包含任何正在被使用的分区，你可以使用umount 命令来卸载分区，使用swapoff 命令来关闭硬盘驱动器上的交换空间。

表5-1包含一列最常用的parted 命令。随后的章节详细地解释了其中的一部分。

命令	描述
check *minor-num*	执行文件系统的简单检查
cp *from to*	把文件系统从一个分区复制到另一个分区；*from* 和*to* 是分区的次要号码
help	显示可用的命令列表
mklabel *label*	为分区表创建磁盘标签
mkfs *minor-num file-system-type*	创建类型为*file-system-type* 的文件系统
mkpart *part-type fs-type start-mb end-mb*	不创建新文件系统而制作分区
mkpartfs *part-type fs-type start-mb end-mb*	制作分区并创建指定的文件系统
move *minor-num start-mb end-mb*	移动分区
print	显示分区表
quit	Quit parted
resize *minor-num start-mb end-mb*	重新划分分区大小，从*start-mb* 到*end-mb*
rm *minor-num*	删除分区
select *device*	选择另一个设备来配置
set *minor-num flag state*	在分区上设置标志；*state* 要么是on，要么是off

表**5-1. parted** 命令

5.1. 查看分区表

启动了parted 后，键入以下命令来查看分区表：

```
print
```

A table similar to the following will appear:

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor  Start   End  Type   Filesystem Flags
1    0.031  101.975 primary ext3   boot
2   101.975  611.850 primary linux-swap
3   611.851  760.891 primary ext3
4   760.891 9758.232 extended      lba
5   760.922 9758.232 logical ext3
```

第一行显示了磁盘的大小；第二行显示了磁盘标签类型；剩余的输出显示了分区表。在分区表中，**Minor**（次要）标签是分区号码。例如，次要号码为1 的分区和/dev/hda1 相对。**Start**（开始）和**End**（结束）值以MB 为单位。**Type**（类型）是primary、extended、logical 中的一个。**Filesystem**（文件系统）是文件系统的类型，它可以是ext2、ext3、FAT、hfs、jfs、linux-swap、ntfs、reiserfs、hp-ufs、sun-ufs 或xfs 之一。**Flags**（标志）列列出了分区被设置的标准。可用的标志有：boot、root、swap、hidden、raid、lvm 或lba。


窍门

要不重新启动parted 来选择不同的设备，使用select 命令，再紧跟设备名，如/dev/hdb。然后，你便可以查看或配置它的分区表。

5.2. 创建分区


警告

不要试图在正在被使用的设备上创建分区。

在创建分区前，引导入救援模式（或卸载设备上的所有分区并关闭设备上的交换空间）。

启动parted，/dev/*hda* 是要在其中创建分区的设备：

```
parted /dev/hda
```

查看当前的分区表来判定设备上是否有足够的空闲空间。

```
print
```

如果空闲空间不够，你可以重新划分现存分区的大小。详情请参阅第5.4 节。

5.2.1. 制作分区

根据分区表来决定新分区的起止点和分区类型。每个设备上只能有四个主分区（无扩展分区）。如果你想有四个以上分区，你可以有三个主分区，一个扩展分区，在扩展分区内你可以有多个逻辑分区。关于磁盘分区的概述，请参阅《*Red Hat Linux* 安装指南》中的附录“*An Introduction to Disk Partitions*”。

例如，要在某个硬盘驱动器上从1024 MB 到2048 MB 间创建一个文件系统为ext2 的主分区，键入以下命令：

```
mkpart primary ext3 1024 2048
```


窍门

如果你使用mkpartfs 命令，分区创建后文件系统也会被创建。然而，parted 不支持创建ext3 文件系统。因此，如果你想创建一个ext3 文件系统，请使用mkpart，然后使用稍后会说明的mkfs 命令来创建文件系统。mkpartfs 可以在linux-swap 文件系统类型上使用。

只有你一按[Enter]键，改变就会发生，因此在执行前请检查一下命令。

创建了分区后，使用print 命令来确认所建分区在分区表中，并具备正确的分区类型、文件系统类型和大小。你还需要记住新分区的次要号码，这样你才可以给它注以标签。你应该查看

```
cat /proc/partitions
```

的输出来确定内核能够识别这个新分区。

5.2.2. 格式化分区

分区现在还没有文件系统。用下面的命令来创建文件系统：

```
/sbin/mkfs -t ext3 /dev/hdb3
```


警告

格式化分区会永久地破坏目前存在于该分区上的任何数据。

5.2.3. 给分区注明标签

下一步，给分区注明标签。例如，如果新分区是/dev/hda3，你想把它标为/work：

```
e2label /dev/hda3 /work
```

Red Hat Linux 安装程序默认使用分区的挂载点作为分区的标签来确定标签的独特性。你可以使用任何想用的标签。

5.2.4. 创建挂载点

以根用户身份创建挂载点：

```
mkdir /work
```

5.2.5. 添加到/etc/fstab

以根用户身份编辑/etc/fstab 文件来包括新分区。新添的这一行应该类似：

```
LABEL=/work     /work       ext3  defaults   1 2
```

第一列应该包含LABEL=，然后跟随你给分区注明的标签。第二列应该包含新分区的挂载点，下一列应该是文件系统类型（如ext3 或swap）。如果你想了解更多关于格式化的信息，请阅读man fstab 的说明书（man）页。

如果第四列是defaults 这个词，分区就会在引导时被挂载。要不重新引导而挂载分区，以根用户身份键入以下命令：

```
mount /work
```

5.3. 删除分区


警告

不要试图删除正在被使用的设备上的分区。

在删除分区前，引导入救援模式（或卸载设备上的所有分区，关闭设备上的交换空间）。

启动parted，这里的/dev/*hda* 是你要在其中删除分区的设备：

```
parted /dev/hda
```

查看当前的分区表来判定要删除的分区的次要号码：

```
print
```

使用rm 来删除分区。例如，要删除次要号码为3 的分区：

```
rm 3
```

只有你一按[Enter]键，改变就会发生，因此在执行前请检查一下命令。

删除了分区后，使用print 命令来确认分区在分区表中已被删除。你还应该查看

```
cat /proc/partitions
```

的输出来确定内核知道分区已被删除。

最后一步是把它从/etc/fstab 文件中删除。找到和已被删除的分区相应的行，然后从文件中删除它。

5.4. 重新划分分区大小


警告

不要试图重新划分正在被使用的设备上的分区的大小。

在重新划分分区大小前，引导入救援模式（或卸载设备上的所有分区并关闭设备上的交换空间）。启动parted，/dev/*hda* 是要在其中重新划分分区大小的设备：

```
parted /dev/hda
```

查看当前的分区表来判定要重划大小的分区的次要号码以及它的起止点：

```
print
```


警告

要重划大小的分区上已用的空间必须大于新建的大小。

要重新划分分区大小，使用resize 命令，然后跟随分区的次要号码，以MB 为单位的起始点和终止点。例如：

```
resize 3 1024 2048
```

分区被重新划分了大小后，使用print 命令来确认分区已被正确地重新划分了大小，并且具备正确的分区类型和文件系统类型。

在正常模式下重新引导了系统后，使用df 命令来确定分区已被挂载，并且它们的新大小也已被识别。

redhat.

6. 实现磁盘配额

除了监视系统上使用的磁盘空间（请参阅第26.3.1 节），你还可以通过实现磁盘配额来限制磁盘空间，因此当用户使用了过多的磁盘空间或分区将要充满时，系统管理员就会接到警告。

磁盘配额可以为个体用户配置也可以为用户组配置。这种灵活性既能够给每个用户分配一个较小的配额来处理“个人”文件（如电子邮件和报告），又允许了他们正从事的项目能够拥有较大的配额（假定项目有自己的组群）。

除此以外，配额不仅能够被设置成对所用磁盘块数量的控制，还能够被设置成对内节点数量的控制。由于内节点包含文件相关的信息，对内节点的控制能够控制可被创建的文件数量。

要实现磁盘配额，quota RPM 必须在系统上被安装。关于安装RPM 软件包的详情，请参阅第V 部分。

6.1. 配置磁盘配额

要实现磁盘配额，请使用以下步骤：

1. 修改/etc/fstab来启用每个文件系统的配额
2. 重新挂载文件系统
3. 创建配额文件，重新生成磁盘用量表
4. 分配配额

以上步骤在下面各节中被详细讨论。

6.1.1. 启用配额

以根用户身份使用你喜欢的编辑器来给需要配额的文件系统添加usrquota 和（或）grpquota 选项：

```
LABEL=/     /       ext3  defaults    1 1
LABEL=/boot   /boot     ext3  defaults    1 2
none      /dev/pts    devpts gid=5,mode=620 0 0
LABEL=/home   /home     ext3  defaults,usrquota,grpquota 1 2
none      /proc     proc  defaults    0 0
none      /dev/shm    tmpfs defaults    0 0
/dev/hda2    swap     swap  defaults    0 0
/dev/cdrom    /mnt/cdrom   udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0    /mnt/floppy   auto  noauto,owner,kudzu 0 0
```

在上面的例子中，/home 文件系统上启用了用户和组群配额。

6.1.2. 重新挂载文件系统

添加了userquota 和grpquota 选项后，重新挂载每个相应fstab 条目被修改的文件系统。如果某文件系统没有被任何进程使用，使用umount 命令后再紧跟着mount 命令来重新挂载这个文件系统。如果某文件系统正在被使用，要重新挂载该文件系统的最简捷方法是重新引导系统。

6.1.3. 创建配额文件

重新挂载了每个启用了配额的文件系统后，系统现在就能够使用磁盘配额了。不过，文件系统本身尚且不能支持配额。下一步是运行quotacheck 命令。

quotacheck 命令检查启用了配额的文件系统，并为每个文件系统建立一个当前磁盘用来的表。该表会被用来更新操作系统的磁盘用量文件。此外，文件系统的磁盘配额文件也被更新。

要在文件系统上创建配额文件（aquota.user 和aquota.group），使用quotacheck 命令的-c 选项。例如，如果用户和组群配额都为/home 分区启用了，在/home 目录下创建这些文件：

```
quotacheck -acug /home
```

-a 选项意味着在/etc/mtab 中所有挂载了的非NFS 文件系统都会被检查来决定是否启用了配额。-c 选项指定每个启用了配额的文件系统都应该创建配额文件，-u 选项指定检查用户配额，-g 选项指定检查组群配额。

如果-u 或-g 选项被指定，只有用户配额文件被创建。如果只指定了-g 选项，只有组群配额文件会被创建。

文件被创建后，运行以下命令来生成每个启用了配额的文件系统的当前磁盘用量表：

```
quotacheck -avug
```

所用选项如下：

- a — 检查所有启用了配额的在本地挂载的文件系统
- v — 在检查配额过程中显示详细的状态信息
- u — 检查用户磁盘配额信息
- g — 检查组群磁盘配额信息

quotacheck 运行完毕后，和启用配额（用户和/或组群）相应的配额文件中就会写入用于每个启用了配额的文件系统（如/home）的数据。

6.1.4. 为每用户分配配额

最后一步是使用edquota 命令分配磁盘配额。

要为用户配置配额，以根用户身份在shell 提示下执行以下命令：

```
edquota username
```

为每个你想实现配额的用户执行该步骤。例如，如果在/etc/fstab 中为/home 分区（/dev/hda3）启用了配额，执行了edquota testuser 命令后，系统默认的编辑器中就会有如下显示：

```
Disk quotas for user testuser (uid 501):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440436     0     0   37418    0    0
```

注记

edquota 使用EDITOR 环境变量所定义的文本编辑器。要改变这个编辑器，把EDITOR 环境变量设置为到你选中的编辑器的完整路径。

第一列是启用了配额的文件系统的名称。第二列显示了用户当前使用的块数。随后的两列用来设置用户在该文件系统上的软硬块限度。inodes 列显示了用户当前使用的内节点数量。最后两列用来设置用户在该文件系统上的软硬内节点限度。

硬限是用户或组群可以使用的磁盘空间的绝对最大值。达到了该限度后，磁盘空间就不能再被用户或组群使用了。

软限定义可被使用的最大磁盘空间量。和硬限不同的是，软限可以在一段时期内被超过。这段时期被称为过渡期（*grace period*）。过渡期可以用秒钟、分钟、小时、天数、周数、或月数表示。

如果以上值中的任何一个被设置为0，那个限度就不会被设置。在文本编辑器中，改变想要的限度。如：，

```
Disk quotas for user testuser (uid 501):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440436  500000  550000  37418    0   0
```

要校验用户的配额是否被设置，使用以下命令：

```
quota testuser
```

6.1.5. 为每组群分配配额

配额还可以根据组群来分配。例如，要为devel 组群设置组群配额，使用以下命令（在设置组群配额前，该组群必须存在）：

```
edquota -g devel
```

以上命令在文本编辑器中显示现存的组群配额：

```
Disk quotas for group devel (gid 505):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440400    0    0   37418    0   0
```

修改限度，保存文件，然后配置配额。

要校验组群配额是否被设置，使用以下命令：

```
quota -g devel
```

6.1.6. 为每文件系统分配配额

要根据每个启用了组群的文件系统来分配配额，使用以下命令：

```
edquota -t
```

和另一个edquota 命令相似，这个命令也会在文本编辑器中打开当前的文件系统配额：

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
 Filesystem      Block grace period   Inode grace period
 /dev/hda3          7days        7days
```

改变块过渡期或内节点过渡期，保存对文件的改变，然后退出文本编辑器。

6.2. 管理磁盘配额

如果配额被实现，它们就需要被维护— 主要维护方式是观察。查看配额是否被超出并确保配额的正确性。当然，如果用户屡次超出他们的配额或者持续地达到他们的软限，系统管理员就可以根据用户类型和磁盘空间对他们工作的影响来做出几种决策。管理员可以帮助用户来检索对磁盘空间的使用，也可以按需要增加用户的配额。

6.2.1. 报告磁盘配额

创建磁盘用量报告需要运行repquota 工具。例如，repquota /home 命令会生成以下输出：

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
          Block limits       File limits
User     used  soft  hard grace  used soft hard grace
----------------------------------------------------------------------
root   --   36   0   0      4  0  0
tfox   --  540   0   0     125  0  0
testuser -- 440400 500000 550000    37418  0  0
```

要查看所有启用了配额的文件系统的磁盘用量，使用以下命令：

```
repquota -a
```

这份报告虽然看起来很简单，有几点仍需要做一下说明。显示在每个用户后面的-- 是一种判断用户是否超出其块限度或内节点限度的快速方法。如果任何一个软限被超出，相应的- 行就会被- 代替；第一个- 代表块限度，第二个代表内节点限度。

grace 列通常是空白。如果某个软限被超出，这一列就会包含过渡期中的剩余时间。如果过渡期已超过了，其中就会显示none。

6.2.2. 保持配额的正确性

当某文件系统没有被完整地卸载（如，由于系统崩溃），这就有必要运行quotacheck。不过，即便系统没有崩溃，quotacheck 也可以被定期经常运行。定期运行以下命令来保持配额的正确性（所用选项在第6.1.1 节中被描述）：

```
quotacheck -avug
```

要定期运行它的最简单方法是使用cron。以根用户身份，你既可以使用crontab -e 命令来调度定期的quotacheck，也可以在以下目录之一内放置一个运行quotacheck 的脚本（使用最时候你需要的间隔期间）：

- /etc/cron.hourly
- /etc/cron.daily
- /etc/cron.weekly
- /etc/cron.monthly

最精确的配额统计数据可以在所分析的文件系统没有被活跃使用时获得。因此，cron 任务应该在文件系统被最少使用时调度。如果这一时间在使用配额的文件系统中并不统一，则使用多个cron 任务在不同的时间为每个文件系统运行quotacheck。

请参考第28章来获取关于配置cron 的详情。

6.2.3. 启用和禁用

你可以不必把配额设置为0来禁用它们。要关闭用户和组群配额，使用以下命令：

```
quotaoff -vaug
```

如果-u或-g选项没有被指定，只有用户配额被禁用。如果只指定了-g选项，只有组群配额会被禁用。

要重新启用配额，使用带有同样选项的quotaon命令。

例如，要为所有文件系统启用用户和组群配额：

```
quotaon -vaug
```

要为指定文件系统（如/home）启用配额：

```
quotaon -vug /home
```

如果-u或-g选项没有指定，那么仅用户配额会被启用。如果只指定了-g选项，仅组群配额会被启用。

6.3. 其它资料

关于磁盘配额的更多信息，请参考以下资料。

6.3.1. 安装了的文档

- quotacheck、edquota、repquota、quota、quotaon quotaoff的说明书（man）页。

6.3.2. 相关书籍

- *Red Hat Linux* 系统管理启蒙手册 — 在http://www.redhat.com/docs 网页及文档光盘上可以找到。该手册包含为新Red Hat Linux 系统管理员提供的有关贮存管理（包含磁盘配额）的背景信息。

II. 与安装相关的信息

《*Red Hat Linux* 安装指南》讨论了Red Hat Linux 的安装和一些基本的安装后故障排除。然而，高级安装选项却在本书中被讨论。这个部分提供了对*kickstart*（一种自动化安装技术）的说明、系统恢复模式（在正常运行级别中无法引导时该如何引导系统）、如何在安装中配置RAID、以及如何在安装中配置LVM。阅读《*Red Hat Linux* 安装指南》的同时参照这个部分来进行以上提及的高级安装任务。

目录

7. kickstart 安装

7.1. kickstart 安装是什么?

许多系统管理员更倾向于使用自动化的安装方法来在他们的机器上安装Red Hat Linux。为满足这种需要，Red Hat 开创了kickstart 安装方法。使用kickstart ，系统管理员可以创建单个文件，该文件包括对典型Red Hat Linux 安装中所询问的问题的回答。

kickstart 文件可以被保留在单个服务器系统上，并可以被个体计算机在安装过程中读取。这种安装方法能够支持使用单个kickstart 文件来在多台机器上安装Red Hat Linux，从而成为网络和系统管理员的理想选择。

kickstart 让你自动化大部分Red Hat Linux 的安装任务。

7.2. 如何执行kickstart 安装

kickstart 安装可以使用本地光盘、本地硬盘驱动器、或通过NFS、FTP、HTTP 来执行。

要使用kickstart ，你必须：

1. 创建一个kickstart 文件。
2. 创建一个带有kickstart 文件的引导盘，或在网络上提供该文件。
3. 筹备安装树。
4. 开始kickstart 安装。

本章详细解释了这些步骤。

7.3. 创建kickstart 文件

kickstart 文件是一个简单的文本文件，包含一个项目列表，每个项目都用关键字标明。你可以通过编辑Red Hat Linux 文档光盘中`RH-DOCS`目录里的`sample.ks`文件，使用**kickstart** 配置器来创建它；或从头编写。Red Hat Linux 安装程序还根据你在安装中的选择创建了一个kickstart 文件的例子。它被写入文件`/root/anaconda-ks.cfg`中。你应该可以使用任何文本编辑器或能把文件储存为ASCII 文本的文字处理器来编辑它。

首先，在你创建kickstart 文件时留意下列问题：

- 每小节必须按顺序指定。除非特别申明，每节内的项目不必按序排列。小节的顺序为：
  - 命令节— 参阅第7.4 节来获取kickstart 选项的列表。你必须包括要求的选项。
  - `%packages` 节— 详情请参阅第7.5 节。
  - `%pre` 和`%post` 节— 这两节不必按顺序，也不是必需的。详情请参阅第7.6 节和第7.7 节。

- 不必需的项目可以被省略。
- 省略任何必需的项目会导致安装程序提示用户输入对这个项目的回答，就如同用户在典型的安装过程中被提示的一样。只有给予回答之后，安装才会继续自动进行（除非它又发现一个省略的项目）。
- 以井号（“#”）开头的句行被当作注释而被忽略。
- 对于kickstart 升级，下列项目是必需的：

- 语言
- 语言支持
- 安装方法
- 设备的技术规范（若设备是执行安装所需的）
- 键盘设置
- upgrade 关键字
- 引导装载程序配置

若对升级指定了其它项目，那些项目将被忽略（注意，这包括软件包选择）。

7.4. kickstart 选项

下列选项可以被放置在kickstart 文件中。如果你更喜欢使用图形化界面来创建kickstart 文件，你可以使用 **kickstart** 配置器应用程序。详情请参阅第8章。

注意

如果某选项后面跟随了一个等号（=），它后面就必须指定一个值。在示例命令中，括号（[]）中的选项是命令的可选参数。

`autostep`（可选）

‘ 和`interactive` 相似，只不过它自动为你转到下一屏幕。它大多用于调试。

`auth` 或`authconfig`（必需）

‘ 为系统设置验证选项。它和`authconfig` 命令相似，后者可以在安装后运行。按照默认设置，口令通常是加密的却并不是屏蔽的。

`--enablemd5`

‘ 每个用户口令都使用md5 加密。

`--enablenis`

‘ 启用NIS 支持。按照默认设置，`--enablenis` 使用它在网络上发现的任何域。几乎在所有情况下，域都应该使用`--nisdomain=` 选项来手工设置。

`--nisdomain=`

‘ 用在NIS 服务的NIS 域名。

`--nisserver=`

‘ 用来提供NIS 服务的服务器（默认通过广播）。

`--useshadow` 或`--enableshadow`

‘ 使用屏蔽口令。

--enableldap

‘ 启用/etc/nsswitch.conf 中的LDAP 支持，允许你的系统从LDAP 目录中检索关于用户的信息（UID、主目录、shell 等等）。要使用该选项，你必须安装了nss_ldap 软件包。你必须还得使用--ldapserver= 和--ldapbasedn= 来指定服务器和基准DN。

--enableldapauth

‘ 使用LDAP 验证方法。它启用了pam_ldap 模块和LDAP 目录来验证及改变口令。要使用该选项，你必须安装了nss_ldap 软件包。你必须还得使用--ldapserver= 和--ldapbasedn= 来指定服务器和基准DN。

--ldapserver=

‘ 如果你指定了--enableldap 或--enableldapauth，则使用该选项来指定要使用的LDAP 服务器的名称。该选项在/etc/ldap.conf 文件中被设置。

--ldapbasedn=

‘ 如果你指定了--enableldap 或--enableldapauth，则该选项指定了贮存用户信息的LDAP 目录树中的DN（识别名称）。它设置在/etc/ldap.conf 文件中。

--enableldaptls

‘ 使用TLS（传输层安全）查寻。该选项允许LDAP 在验证前向LDAP 服务器发送加密的用户名和口令。

--enablekrb5

‘ 使用Kerberos 5 来验证用户。Kerberos 自身并不知道关于主目录、UID、或shell 的信息。因此，如果你启用了Kerberos，你将需要使该工作站了解这些用户帐号的信息，方法是使用/usr/sbin/useradd 命令，或启用LDAP、NIS、或Hesiod。如果你要使用该选项，你必须装有pam_krb5 软件包。

--krb5realm=

‘ 你的工作站所属的Kerberos 5 领域。

--krb5kdc=

‘ 为领域请求提供服务的KDC。如果你的领域内有多个KDC，使用逗号（,）来分隔它们。

--krb5adminserver=

‘ 你的领域内还运行kadmind 的KDC。该服务器处理改变口令以及其它管理请求。如果你有不止一个KDC，该服务器必须是主KDC。

--enablehesiod

‘ 为查寻用户主目录、UID、和shell 而启用Hesiod 支持。关于如何在你的网络上设置和使用Hesiod 的详情，请参阅/usr/share/doc/glibc-2.x.x/README.hesiod 文件。它包括在glibc 软件包中。Hesiod 是DNS 的一个扩展，它使用DNS 记录来贮存关于用户、组群以及其它项目的信息。

--hesiodlhs

‘ Hesiod LHS（“左首，left-hand side”）选项，设置在/etc/hesiod.conf 中。该选项被Hesiod 库用来判定在查寻DNS 信息时用来搜索的名称，与LDAP 使用基准DN 的意义相似。

--hesiodrhs

‘ Hesiod RHS（“右首，right-hand side”）选项，设置在/etc/hesiod.conf 文件中。该选项被Hesiod 库用来判定在查寻DNS 信息时用来搜索的名称，与LDAP 使用基准DN 的意义相似。


窍门

要查寻用户“jim”的信息，Hesiod 库查寻*jim.passwd*<*LHS*><*RHS*>，它应该被解析成类似他的passwd 项目的TXT 记录（jim:*:501:501:Jungle Jim:/home/jim:/bin/bash）。组群的情况也是如此，只不过使用的是*jim.group*<*LHS*><*RHS*>。

要按号码来查寻用户和组群，指定“501.uid”为“jim.passwd”的CNAME，指定“501.gid”为“jim.group”的CNAME。注意，在库判定搜索名称时，LHS 和RHS 的前面不放“点[.]”，因此LHS 和RHS 通常用点开头。

--enablesmbauth

‘ 使用SMB 服务器（典型为Samba 或Windows 服务器）来验证用户。SMB 验证支持不知道关于主目录、UID、或shell 的信息。因此，若你启用该选项，你将需要使该工作站了解这些用户帐号的信息，方法是使用/usr/sbin/useradd 命令，或启用LDAP、NIS、或Hesiod。如果你要使用该选项，你必须装有pam_smb 软件包。

--smbservers=

‘ 用来做SMB 验证的服务器名称。要指定不止一个服务器，用逗号（,）来分隔它们。

--smbworkgroup=

‘ SMB 服务器的工作组名称。

--enablecache

‘ 启用nscd 服务。nscd 服务缓存关于用户、组群和各类其它信息。如果你选择要通过网络，使用LDAP、NIS、或hesiod 来传递关于用户和组群的信息，缓存就会特别有用。

bootloader（必需）

‘ 指定引导装载程序应该如何被安装，以及应该安装LILO 还是GRUB。安装和升级都需要这个选项。对升级而言，如果没有指定--useLilo，而且LILO 是当前的引导装载程序，引导装载程序就会被改为GRUB。要在升级时保留LILO，使用bootloader --upgrade 选项。

--append=

‘ 指定内核参数。要指定多个参数，使用空格分隔它们。例如：

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

--location=

‘ 指定写入引导记录的位置。有效值如下：**mbr**（默认值）；**partition**（在包含内核分区的第一个扇区上安装引导装载程序）；或**none**（不安装引导转载程序）。

--password=

‘ 如果使用GRUB，使用这个选项来设置GRUB 引导装载程序口令。它应该被用来限制对GRUB shell 的访问，因为在那里你可以传递任意内核选项。

`--md5pass=`

‘ 若干使用GRUB，和`--password=`相似，只不过口令应该已经被加密。

`--useLilo`

‘ 使用LILO而非GRUB引导装载程序。

`--linear`

‘ 若使用LILO，使用`linear` LILO选项；它的目的仅是后向兼容（现在默认使用linear）。

`--nolinear`

‘ 若使用LILO，使用`nolinear` LILO选项；linear是默认。

`--lba32`

‘ 若使用LILO，强制使用lba32模式而非自动检测。

`--upgrade`

‘ 升级现存的引导装载程序配置，保留其中原有的项目。该选项仅可用于升级。

`clearpart`（可选）

‘ 在创建新分区之前，从系统上删除分区。默认不会删除任何分区。

注记

如果使用了`clearpart`命令，那么`--onpart`命令就不能被用在逻辑分区上。

`--linux`

‘ 删除所有Linux分区。

`--all`

‘ 删除系统上所有分区。

`--drives=`

‘ 指定要从中删除分区的驱动器。例如，以下命令删除主要IDE控制器上的前两个驱动器上的分区：

```
clearpart --drives hda,hdb
```

`--initlabel`

‘ 把磁盘卷标初始为你的体系的默认值（例如：x86使用`msdos`，Itanium使用`gpt`）。这个选项很有用，因为在安装了新硬盘驱动器后，安装程序就不会问你是否应初始磁盘卷标。

`device`（可选）

‘ 在多数PCI 系统上，安装程序会正确地自动探测到以太网卡和SCSI 卡。然而，在较老的系统上和某些PCI 系统上，kickstart 需要一点提示才能找到正确的设备。`device` 命令告诉安装程序来安装额外的模块，它的格式是：
`device` <*type*> <*moduleName*> `--opts=`<*options*>

<*type*>

‘ 使用`scsi` 或`eth` 来替换

<*moduleName*>

‘ 使用应该被安装的内核模块的名称来替换。

`--opts=`

‘ 传递给内核模块的选项。注意，如果把选项放在引号里，你可以传递多个选项。譬如：
`--opts="aic152x=0x340 io=11"`

`deviceprobe`（可选）

‘ 强制探测PCI 总线，并为所有设备载入可用的模块。

`driverdisk`（可选）

‘ 驱动程序盘可以在kickstart 安装中使用。你需要把驱动程序盘的内容复制到系统硬盘驱动器某分区的根目录中。然后，你需要使用`driverdisk` 命令来告诉安装程序到哪里区寻找驱动程序盘。
`driverdisk` <*partition*> [`--type=`<*fstype*>]

<*partition*>

‘ 包含驱动程序盘的分区。

`--type=`

‘ 文件系统类型（如：vfat、ext2、ext3）。

`firewall`（可选）

‘ 防火墙选项可以在kickstart 中配置。该配置和安装程序中的「防火墙配置」 屏幕相对应：
`firewall` <*securitylevel*> [`--trust=`] <*incoming*> [`--port=`]

<*securitylevel*>

‘ 使用以下安全级别之一来替换：

- `--high`
- `--medium`
- `--disabled`

`--trust=`

‘ 在这里列出设备，如eth0，会允许所有来自该设备的交通能穿过防火墙。要列出不止一个设备，使用`--trust eth0 --trust eth1`。千万不要使用象`--trust eth0, eth1` 这样用逗号分隔的格式。

<incoming>

‘ 使用以下服务来替换，从而允许指定的服务穿过防火墙。

- --dhcp
- --ssh
- --telnet
- --smtp
- --http
- --ftp

--port=

‘ 你可以使用“端口：协议”的格式来指定允许穿过防火墙的端口。譬如，如果你想允许IMAP访问通过防火墙，你可以指定imap:tcp。你还可以具体指定数字端口，譬如，要允许UDP包在端口1234上通过，指定1234:udp。要指定多个端口，用逗号分隔它们。

install（可选）

‘ 告诉系统重新安装而不是升级现有系统。这是默认模式。对安装而言，你必须从cdrom、harddrive、nfs、或url（用于ftp或http安装）中指定一个安装类型。install命令和安装方法命令必须在分开的行上。

cdrom

‘ 从系统上的第一个光盘驱动器中安装。

harddrive

‘ 从本地驱动器的Red Hat安装树中安装，它必须是vfat或ext2。

- --partition=

  要从中安装的分区（如sdb2）。

- --dir=

  包含安装树的RedHat目录的目录。

例如：

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

nfs

‘ 从指定的NFS服务器安装。

- --server=

  要从中安装的服务器（主机名或IP）。

- --dir=

  包含安装树的RedHat目录的目录。

例如：

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

url

‘ 通过FTP 或HTTP 从远程服务器上的安装树中安装。

例如：

```
url --url http://<server>/<dir>
```

或：

```
url --url ftp://<username>:<password>@<server>/<dir>
```

interactive（可选）

‘ 在安装中使用kickstart 文件中提供的信息，但是允许查看和修改给定值。你会看到安装程序中的每个屏幕，其中预填了kickstart 文件中选定的值，你可以点击「下一步」来接受这些值，也可以改变这些值再点击「下一步」来继续。请参阅autostep。

keyboard（必需）

‘ 设置系统键盘类型。这里是i386、Itanium、和Alpha 机器上可用键盘的列表：

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

文件/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py 中也包含了这个列表，它是rhpl 软件包的一部分。

lang（必需）

‘ 设置安装中使用的语言。譬如，要把语言设为英语，kickstart 文件应该包括下面一行：

```
lang en_US
```

文件/usr/share/redhat-config-language/locale-list 的每一行的第一列提供了有效的语言代号的列表，它是redhat-config-languages 软件包的一部分。

langsupport（必需）

‘ 设置要在系统上安装的语言。它使用的语言代号和lang 一样。

如果你只想安装一种语言，请指定它。譬如，要安装和使用法语fr_FR：

```
langsupport fr_FR
```

--default=

‘ 如果你想安装不止一种语言支持，你必须指定默认语言。

譬如，要安装英语和法语，并使用英语为默认语言：

```
langsupport --default=en_US fr_FR
```

如果你使用--default，后面仅跟一种语言，那么，所有语言将会被安装，指定的语言为默认。

lilo（被bootloader 替换）

‘

警告

该选项已被bootloader 代替，它的目的只是提供后向兼容。请参阅bootloader。

指定引导装载程序应如何在系统上被安装。按照默认设置，LILO 安装在第一张磁盘上的MBR 上，如果DOS 分区存在，则默认安装双引导系统（如果用户在`LILO:` 提示下键入**`dos`**，DOS/Windows 系统就会被引导）。

`--append <`*`params`*`>`

‘ 指定内核参数。

`--linear`

‘ 使用`linear` LILO 选项；它的目的只是提供后向兼容（现在默认使用linear）。

`--nolinear`

‘ 使用`nolinear` LILO 选项；现在默认使用linear。

`--location=`

‘ 指定写入LILO 引导记录的位置。有效的值有：**`mbr`**（默认）或**`partition`**（在包含内核的分区上的第一个扇区上安装引导安装程序）。如果不指定位置，LILO 就不会被安装。

`--lba32`

‘ 强制使用lba32 模式而非自动检测。

`lilocheck`（可选）

‘ 如果`lilocheck` 存在，安装程序就会在第一个硬盘驱动器的MBR 上检查LILO，若找到，就会重新引导系统— 在这种情况下，不会执行任何安装。这会防止kickstart 重新安装一个已安装了的系统。

`logvol`（必需）

‘ 使用以下语法来为逻辑卷管理（LVM）创建逻辑卷：

```
logvol mountpoint --vgname=name --size=size --name=name
```

首先创建分区，然后创建逻辑卷组，再创建逻辑卷。例如：

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`mouse`（必需）

‘ 为系统的GUI 和文本模式配置鼠标。选项有：

`--device=`

‘ 鼠标所在的设备（如`--device=ttyS0`）。

`--emulthree`

‘ 若存在，同时点击鼠标的左右两键就会被X 窗口系统当做点击了鼠标的中间按钮。如果你有一个两键鼠标，应使用该选项。

在选项之后，鼠标类型可使用以下类型之一：

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,
geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,

thinking, thinkingps/2, logitech, logitechcc, logibm, logimman,
logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew,
```

msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries, mmhittab, sun, none

这个列表可以在/usr/lib/python2.2/site-packages/rhpl/mouse.py 文件中找到。该文件是rhpl 软件包的一部分。

如果给出的鼠标命令没有附带任何参数，或这个命令被省略，安装程序就会试图自动检查鼠标。该进程可用于多数现代鼠标。

network（可选）

‘ 为系统配置网络信息。如果kickstart 安装不需要联网（换一句话说，它不是通过NFS、HTTP、或FTP 安装的），系统的联网就不会被配置。如果安装确实需要联网，但网络信息在kickstart 文件中没有被提供，Red Hat Linux 安装程序会假定安装应该通过eth0 和动态IP 地址来进行（BOOTP/DHCP），并把最终的安装了的系统配置成动态地判定IP 地址。network 选项为kickstart 安装和已安装系统通过网络配置联网信息。

--bootproto=

‘ dhcp、bootp、或static 中的一个。

它默认为dhcp。bootp 和dhcp 被同等对待。

DHCP 方法使用DHCP 服务器系统来获取它的联网配置。你可以会猜到，BOOTP 方法和它很相似，要求BOOTP 服务器来提供网络配置。要指示系统使用DHCP：

```
network --bootproto=dhcp
```

要指示某机器使用BOOTP 来获取它的联网配置，在kickstart 文件中使用以下行：

```
network --bootproto=bootp
```

静态方法要求你在kickstart 文件中输入所有必需的联网信息。如它的名称所暗示，这些信息是静态的，将会在安装中和安装后使用。用于静态联网的这一行比较复杂，因为你必须把所有网络配置信息在一行内包括。你必须指定IP 地址、子网掩码、网关和名称服务器。例如（“\”表明它们在一行）：

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

如果你使用静态方法，请注意以下两个限制：

- 所有静态联网配置信息都必须在一行上指定；你不能使用反斜线来换行。
- 你只能在此指定一个名称服务器。不过，若需要，你可以使用kickstart file 的%post 节（在第7.7 节中被描述）来添加更多名称服务器。

--device=

‘ 用来选择用于安装的指定以太网设备。注意，除非kickstart 文件是本地文件（如ks=floppy），使用--device= 将不会有效，因为安装程序将会配置网络来寻找kickstart 文件。例如：

```
network --bootproto=dhcp --device=eth0
```

--ip=

‘ 要安装的机器的IP 地址。

--gateway=

‘ IP 地址形式的默认网关。

--nameserver=

‘ 主名称服务器，IP 地址格式。

--nodns

‘ 不要配置任何DNS 服务器。

--netmask=

‘ 安装的系统的子网掩码。

--hostname=

‘ 安装的系统的主机名。

part 或partition（安装所必需的，升级所忽略的）

‘ 在系统上创建分区。

如果系统上的不同分区上存在不止一个Red Hat Linux 安装，安装程序会询问用户应该升级哪个安装。


警告

除非使用了--noformat 和--onpart，所有创建的分区都会被格式化，这是安装过程的一部分。

<mntpoint>

‘ *<mntpoint>* 是分区将要挂载的位置，必须使用以下格式之一：

- */<path>*

  例如：/、/usr、/home

- swap

  该分区将被用作交换空间。

  要自动决定交换区的大小，使用--recommended选项：
  swap --recommended

  自动生成的交换区的最小值将不会小于系统的内存，不会大于系统内存的两倍。

- raid.*<id>*

  该分区将会被用作软件RAID（请参见raid）。

- pv.*<id>*

  将会用于LVM 的分区（请参见logvol）。

--size=

‘ 以MB 为单位的分区最小值。在此处指定一个整数值，如500。不要在数字后面加MB。

--grow

‘ 告诉分区使用所有可用空间（若有），或使用设置的最大值。

--maxsize=

‘ 当分区被设置为可扩充时，以MB 为单位的分区最大值。在这里指定一个整数值，不要在数字后加MB。

--noformat

‘ 告诉安装程序不要格式化分区，和--onpart 命令一起使用。

--onpart= or --usepart=

‘ 把分区放在已存在的设备上。例如：
partition /home --onpart=hda1

会把/home 放在/dev/hda1 上，而这个分区必须已经存在。

--ondisk= 或--ondrive=

‘ 强制分区在特定磁盘上创建。譬如，--ondisk sdb 会把分区放在系统的第二个SCSI 磁盘上。

--asprimary

‘ 把分区强行自动指派为主分区，否则分区过程就会失败。

--bytes-per-inode=

‘ 指定的数字代表文件系统上每个节点在创建时的字节数。它必须使用十进制格式。对于你想增加文件系统上的节点数量的应用程序，该选项就会很有用。

--type=（被fstype 替换）

‘ 该选项已不再可用。请使用fstype。

--fstype=

‘ 为分区设置文件系统类型。合法值有：**ext2**、**ext3**、**swap**、和**vfat**。

--start=

‘ 指定分区的起始柱面。它要求使用--ondisk 或ondrive 来指定驱动器。它还要求使用--end 来指定终结柱面，或使用--size 来指定分区大小。

--end=

‘ 指定分区的终结柱面。它要求使用--start 来指定分区的起始柱面。

--badblocks

‘ 指定分区应检查坏块。sectors.

注记

如果由于某种原因，分区失败了，诊断迅息会显示在第三号虚拟控制台上。

raid（可选）

‘ 组成软件RAID 设备。该命令的格式是：
raid <*mntpoint*> --level=<*level*> --device=<*mddevice*> <*partitions**>

<*mntpoint*>

‘ 挂载RAID 文件系统的位置。如果它是/，RAID 级别必须是1，除非引导分区（/boot）存在。如果引导分区存在，/boot 分区必须是级别1，根（/）分区可以是任何可用的类型。<*partitions**>（代表多个分区可以被列举）列举了要添加到RAID 阵列的RAID 标记。

--level=

‘ 要使用的RAID 级别（0、1、或5）。

--device=

‘ 要使用的RAID 设备的名称（如md0 或md1）。RAID 设备的范围从md0 直到md7，每个设备只能被使用一次。

--spares=

‘ 指定RAID 阵列应该被指派N 个备用驱动器。备用驱动器可以被用来在驱动器失败时重建阵列。

--fstype=

‘ 为RAID 阵列设置文件系统类型。合法值有：ext2、ext3、swap、和vfat。

--noformat

‘ 不要格式化RAID 阵列。

下面的例子显示了如何为/ 创建RAID 级别1 分区，为/usr 创建RAID 级别5 分区，假定你的系统上有三个SCSI 磁盘。它还创建三个交换分区，每个驱动器上一个。

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

reboot（可选）

‘ 安装完成后重新引导系统（无参数）。通常，kickstart 显示一条消息，并等待用户按任意键后才重新引导。

rootpw（必需）

‘ 把系统的根口令设置为<*password*> 参数。

```
rootpw [--iscrypted] <password>
```

--iscrypted

‘ 如果该选项存在，口令就会假定已被加密。

skipx（可选）

‘ 如果存在，安装的系统上就不会配置X。

text（可选）

‘ 在文本模式下执行kickstart 安装。kickstart 安装默认在图形模式下安装。

timezone（必需）

‘ 把系统的时区设置为<*timezone*>，它可以是timeconfig 列举的任何时区。

```
timezone [--utc] <timezone>
```

--utc

‘ 如果存在，系统就会假定硬件时钟被设置为UTC（格林威治标准）时间。

upgrade（可选）

‘ 告诉系统升级现存系统，而不是安装一个新系统。你必须从cdrom、harddrive、nfs、或url（用于ftp和http）中指定安装树的位置。详情请参见install。

xconfig（可选）

‘ 配置X窗口系统。如果该选项没有给出，而X被安装了，用户将需要在安装过程中手工配置X；如果你的最终系统上没有安装X，则不应该使用该选项。

--noprobe

‘ 不要探测显示器。

--card=

‘ 使用指定的视频卡；该卡的名称应该来自hwdata 软件包的/usr/share/hwdata/Cards 中的视频卡列表。这个列表还可以在**Kickstart** 配置器的**X** 配置器屏幕上找到。如果参数没有提供，安装程序会探测该卡的PCI 总线。由于AGP 是PCI 总线的一部分，若支持，AGP 卡就会被探测到。探测顺序由母板的PCI 扫描顺序决定。

--videoram=

‘ 指定视频卡的视频内存数量。

--monitor=

‘ 使用指定显示器；显示器的名称应该来自hwdata 的/usr/share/hwdata/MonitorsDB 中的显示器列表。这个列表还可以在**Kickstart** 配置器的**X** 配置器屏幕上找到。如果提供了**--hsync** 或**--vsync**，该选项会被忽略。如果没有提供显示器信息，安装程序会试图自动探测它。

--hsync=

‘ 指定显示器的水平频率。

--vsync=

‘ 指定显示器的垂直频率。

--defaultdesktop=

‘ 把默认桌面设置成GNOME 或KDE（假定GNOME 和/或KDE 通过%packages 被安装了）。

--startxonboot

‘ 在安装的系统上使用图形化登录。

--resolution=

‘ 指定安装的系统上X 窗口系统的默认分辨率。有效值有：640x480、800x600、1024x768、1152x864、1280x1024、1400x1050、1600x1200。请确定指定与视频卡和显示器兼容的分辨率。

--depth=

‘ 指定安装的系统上的X窗口系统的默认色彩深度。有效值有：8、16、24、和32。请确定指定与视频卡和显示器兼容的色彩深度。

volgroup（可选）

‘ 用来创建逻辑卷管理（LVM）组，其语法格式为：
volgroup *name partition*

首先创建分区，然后创建逻辑卷组，再创建逻辑卷。例如：
```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

zerombr（可选）

‘ 如果zerombr被指定，它唯一的参数是yes，所有在磁盘上发现的无效分区表就会被初始化。这会破坏带有无效分区表的磁盘上的所有数据。该命令的格式如下：
```
zerombr yes
```

其它格式均无效。

%include

‘ 使用%include */path/to/file* 命令来在kickstart 文件中包括另一个文件的内容，就好像这些内容本来就在kickstart 文件里%include 所在的位置中一样。

7.5. 软件包选择

使用%packages 命令来开始kickstart 文件中列举要安装的软件包的部分（只限于安装，因为升级中软件包选择不被支持）。

你可以使用单个软件包名称或软件包组的名称来指定它们。安装程序定义了许多包含相关软件包的软件包组。请参见第一张Red Hat Linux 光盘上的RedHat/base/comps.xml 文件来获取软件包组的列表。每组都有id、用户可见性值、名称、描述、以及其中包含的软件包列表。在软件包列表中，若该组被选定要安装，被标为必需的软件包总是被安装。被标为默认的软件包会被默认选择，而标为可选的软件包必须被具体指定才能被安装，即便该组已经选定要被安装。

在多数情况下，你只需列举想要的软件包组，而不必一一列举单个软件包。注意，Core 和Base 软件包组总是被默认选择，因此你不必在%packages 部分中指定它们。

以下是%packages 部分的示例：

```
%packages
@ X Window System
@ GNOME Desktop Environment
@ Graphical Internet
@ Sound and Video
galeon
```

如上所示，组群被一行行地指定，以@ 符号起首，然后是空格，然后是如comps.xml 文件中指定的组群的全名。不加附带的起首符号会指定单个软件包（如以上例子中的galeon 行指定的是单个软件包）。

你还可以从默认的软件包列表中指定要不安装的软件包：

```
@ Games and Entertainment
-kdegames
```

%packages 有两个可用选项。

--resolvedeps

‘ 安装列举的软件包，并自动解决软件包依赖关系。如果该选项没有被指定，而软件包依赖关系却存在，自动安装就会暂停并提示用户。例如：
%packages --resolvedeps

--ignoredeps

‘ 忽略未解决的依赖关系，并安装所列举的没有依赖关系的软件包。例如：
%packages --ignoredeps

--ignoremissing[1]

‘ 忽略缺少的软件包或软件包组，而不是暂停安装来向用户询问是中止还是继续安装。例如：
%packages --ignoremissing

7.6. 预安装脚本

你可以添加系统要在解析ks.cfg 文件之后立即运行的命令。这一节必须位于kickstart 文件的结尾处（在命令之后），而且必须以%pre 命令开头。注意，你在%pre 部分可以访问网络；然而，名称服务（*name service*）在此时还没有被配置，因此只有IP 地址才能奏效。

注记

注意，预安装脚本不在改换了的根环境（chroot）中运行。

--interpreter */usr/bin/python*

‘ 允许你指定不同的脚本语言，如Python。把*/usr/bin/python* 替换成你想使用的脚本语言。

7.6.1. 范例

以下是%pre 节的示例：

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
 mymedia=‘cat $file/media‘
 if [ $mymedia == "disk" ] ; then
   hds="$hds ‘basename $file‘"
 fi
done
```

1. 该选项是Red Hat Linux 9 中新添的。

```
set $hds
numhd=‘echo $#‘

drive1=‘echo $hds | cut -d’ ’ -f1‘
drive2=‘echo $hds | cut -d’ ’ -f2‘

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
 #2 drives
 echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
 echo "clearpart --all" >> /tmp/part-include
 echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
 echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
 echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
 echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
 #1 drive
 echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
 echo "clearpart --all" >> /tmp/part-include
 echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
 echo "part swap --recommended" >> /tmp/part-include
 echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
 echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

该脚本判定系统上的硬盘驱动器的数量，并根据系统上有一个还是两个驱动器而编写带有不同分区方案的文本文件。与其在kickstart 文件中有一组分区命令，你可以包括以下行：

```
%include /tmp/part-include
```

在脚本中选择的分区命令会被使用。

7.7. 安装后脚本

你可以添加系统在安装完成后要运行的命令。这一节必须位于kickstart 文件的结尾处，而且必须以%post 命令开头。它对于安装额外软件包或配置额外名称服务器等任务很有帮助。

注记

如果你使用静态IP 信息配置了网络，包括名称服务器，你可以在%post 部分中访问网络并解析IP 地址。如果你使用DHCP 配置网络，当安装执行到%post 部分时，/etc/resolv.conf 文件还没有完成。你可以访问网络，但是你不能解析IP 地址。因此，如果你使用DHCP，你必须在%post 这一节中指定IP 地址。

注记

安装后脚本在chroot 环境中运行；因此，象复制安装介质中的脚本或RPM 之类的任务将不能被执行。

`--nochroot`

‘ 允许你指定你想在chroot 环境之外运行的命令。

下面的例子把`/etc/resolv.conf` 文件复制到刚刚安装了的文件系统上。

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter /usr/bin/python`

‘ 允许你指定不同的脚本语言，如Python。用你想用的脚本语言来替换`/usr/bin/python`。

7.7.1. 范例

要启动和关闭服务：

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

要从NFS 共享中运行叫做`runme` 的脚本：

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

给系统添加用户：

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/' bob
```

7.8. 如何使kickstart 文件可被利用

kickstart 文件必须位于以下几个位置之一：

- 在引导盘上
- 在引导光盘上
- 在网络上

通常，kickstart 文件被复制到引导盘上，或在网络上提供。基于网络的方法使用最普遍，因为多数kickstart 安装是在联网的计算机上执行的。

让我们更深入地看一看存放kickstart 文件的位置。

7.8.1. 创建Kickstart 引导盘

要执行基于软盘的kickstart 安装，kickstart 文件必须被命名为`ks.cfg`，且必须位于引导盘的最上级目录里。关于创建引导盘的说明请参阅《*Red Hat Linux* 安装指南》中的“制作安装引导盘”这个章节。因为Red Hat Linux 引导盘使用MS-DOS 格式，因此你可以使用`mcopy` 命令来在Linux 中复制kickstart 文件：

```
mcopy ks.cfg a:
```

另外，你也可以使用Windows 来复制该文件。你还可以使用文件类型vfat 来在Red Hat Linux 挂载MS-DOS 引导盘，然后使用cp 命令来复制该文件。

7.8.2. 创建kickstart 引导光盘

要执行基于光盘的kickstart 安装，kickstart 文件必须被命名为ks.cfg，而且必须位于引导光盘的最上级目录中。因为光盘是只读的，这个文件必须被添加到被写入光盘的、用来创建映像的目录中。关于创建引导光盘的说明，请参阅《*Red Hat Linux* 安装指南》中的“制作安装引导光盘”这一章节。不过，在制作file.iso 映像文件之前，请把ks.cfg kickstart 文件复制到isolinux/ 目录中。

7.8.3. 在网络上提供Kickstart 文件

使用kickstart 的网络安装比较普遍，因为系统管理员可以快速轻松地自动化许多联网计算机的安装。一般说来，这种方法对于在局域网上具有BOOTP/DHCP 和NFS 服务器的管理员来说，使用最普遍。BOOTP/DHCP 服务器用来给客户提供联网信息，在安装中使用的文件则由NFS 服务器提供。这两项服务经常在同一部机器上运行，但是这并不是必需的。

要执行基于网络的kickstart 安装，你的网络上必须有一个BOOTP/DHCP 服务器，而且它必须包括关于你要在其上安装Red Hat Linux 的机器的配置信息。BOOTP/DHCP 服务器会给客户提供它的联网信息以及kickstart 文件的位置。

如果kickstart 文件被BOOTP/DHCP 服务器指定，客户系统就会试图使用NFS 来挂载该文件的路径，并把指定文件复制到客户上，把它用作kickstart 文件。所需的确切设置要依你使用的BOOTP/DHCP 服务器而定。

下面是从用于Red Hat Linux 随带的DHCP 服务器的dhcpd.conf 文件中所摘录的一行：

```
filename "/usr/new-machine/kickstart/";
next-server blarg.redhat.com;
```

注意，你应该把filename 后面的值替换为kickstart 文件的名称（或kickstart 文件所在的目录），把next-server 后面的值替换成NFS 服务器的名称。

如果BOOTP/DHCP 服务器返回的文件以斜线（“/”）结束，它就会被当做路径。在这种情况下，客户系统会使用NFS 来挂载该路径，然后搜索某一指定文件。客户搜索的文件名是：

```
<ip-addr>-kickstart
```

文件名的<*ip-addr*> 部分应该被点式的客户IP 地址替换。譬如，IP 地址为10.10.0.1 的计算机的文件名应为10.10.0.1-kickstart。

注意，如果你不指定服务器名称，客户系统就会试图使用回答BOOTP/DHCP 请求的服务器来作为它的NFS 服务器。如果你不指定路径或文件名，客户系统会试图从BOOTP/DHCP 服务器挂载/kickstart，然后使用和前面描述的<*ip-addr*>-kickstart 文件名相同的方法来搜索kickstart 文件。

7.9. 提供安装树

kickstart 安装需要使用安装树（*installation tree*）。安装树是二进制Red Hat Linux 光盘的复制，它具备与光盘相同的目录结构。

如果你执行的是基于光盘的安装，在开始kickstart 安装前把Red Hat Linux 光盘#1 插入计算机。

如果你执行的是硬盘驱动器安装，请确定二进制Red Hat Linux 光盘的映像位于计算机的硬盘驱动器上。

如果你执行的是基于网络（NFS、FTP、或HTTP）安装，你必须通过网络来提供安装树。详情请参阅《*Red Hat Linux* 安装指南》中的“筹备网络安装”这一章节。

7.10. 开始kickstart 安装

要开始kickstart 安装，你必须从Red Hat Linux 引导软盘、Red Hat Linux 引导光盘、或Red Hat Linux 安装光盘#1 中安装，在引导提示下输入一个特殊的引导命令。如果ks 命令行参数被传递给内核，安装程序就会寻找kickstart 文件。

引导软盘

‘ 如果kickstart 文件位于引导软盘上，如第7.8.1 节中所描述，使用驱动器中的软盘来引导，然后在boot: 下输入以下命令：
linux ks=floppy

光盘#1 和软盘

‘ 如果ks.cfg 文件位于软盘上的vfat 或ext2 文件系统上，而你要从Red Hat Linux 安装光盘#1 中引导，你也可以使用**linux ks=floppy** 命令。

另一种可行的引导命令是从Red Hat Linux 光盘#1 中引导，并把kickstart 文件放在软盘的vfat 或ext2 文件系统上。要达到这个目的，在boot: 提示下输入以下命令：
linux ks=hd:fd0:/ks.cfg

使用驱动程序盘

‘ 如果kickstart 需要使用驱动程序盘，你还需要指定**dd** 选项。例如，要从引导盘中引导，并使用驱动程序盘，在boot: 提示下输入以下命令：
linux ks=floppy dd

引导光盘

‘ 如果kickstart 文件位于引导光盘上，如第7.8.2 节中所描述，把光盘插入系统，引导系统，然后在boot: 提示下输入以下命令（ks.cfg 是kickstart 文件的名称）：
linux ks=cdrom:/ks.cfg

其它启动kickstart 安装的方法如下列举：

ks=nfs:<*server*>:/<*path*>

‘ 安装程序会在NFS 服务器<*server*> 上的<*path*> 中寻找kickstart 文件。安装程序会使用DHCP 来配置以太网卡。譬如，如果你的NFS 服务器是server.example.com，kickstart 文件位于NFS 共享/mydir/ks.cfg 上，正确的引导命令应该是：ks=nfs:server.example.com:/mydir/ks.cfg。

ks=http://<*server*>/<*path*>

‘ 安装程序会在HTTP 服务器<*server*> 上的<*path*> 中寻找kickstart 文件。安装程序会使用DHCP 来配置以太网卡。譬如，如果你的HTTP 服务器是server.example.com，kickstart 文件位于HTTP 目录/mydir/ks.cfg 中，正确的引导命令应该是：ks=http://server.example.com/mydir/ks.cfg。

ks=floppy

‘ 安装程序会在/dev/fd0 驱动器中的软盘上的vfat 或ext2 文件系统中寻找ks.cfg 文件。

ks=floppy:/<*path*>

‘ 安装程序会在/dev/fd0 驱动器中的软盘上的vfat 或ext2 文件系统中寻找名称为<*path*> 的kickstart 文件。

`ks=hd:<device>:/<file>`

‘ 安装程序会在`<device>`上挂载文件系统（必须是vfat 或ext2），然后在该文件系统中寻找kickstart 配置文件`<file>`（譬如，`ks=hd:sda3/mydir/ks.cfg`）。

注记

第二个冒号是Red Hat Linux 9 中的语法改变。

`ks=file:/<file>`

‘ 安装程序会试图从文件系统中读取`<file>`文件；不必执行挂载。这通常在kickstart 文件已经位于`initrd`映像时使用。

`ks=cdrom:/<path>`

‘ 安装程序会在光盘中寻找kickstart 文件`<path>`。

`ks`

‘ 如果`ks`被单独使用，安装程序会配置系统的以太网卡使用DHCP。系统将会使用DHCP 回应的“bootServer”作为NFS 服务器，并从中读取kickstart 文件（它默认与DHCP 服务器相同）。kickstart 文件的名称可以是下面一种：

- 如果DHCP 被指定，bootfile 以`/`开头，由DHCP 提供的bootfile 就会在NFS 服务器上被查找。
- 如果DHCP 被指定，bootfile 不以`/`开头，由DHCP 提供的bootfile 就会在NFS 服务器上的`/kickstart`目录中被查找。
- 如果DHCP 没有指定bootfile，安装程序就会试图读取文件`/kickstart/1.2.3.4-kickstart`，这里的`1.2.3.4`是要安装的机器的IP 地址。

`ksdevice=<device>`

‘ 安装程序会使用该网络设备来连接到网络。譬如，要使用通过eth1 设备连接到系统上的NFS 服务器上的kickstart 文件来启动kickstart 安装，在`boot:`提示下使用`ks=nfs:<server:>/<path> ksdevice=eth1`命令。

8. Kickstart 配置器

Kickstart 配置器允许你使用图形化用户界面来创建kickstart 文件，因此你不必记住文件的正确语法。

要使用**Kickstart** 配置器，你必须运行X 窗口系统。要启动**Kickstart** 配置器，选择面板上的「主菜单」 => 「系统工具」 => 「**Kickstart**」，或键入`/usr/sbin/redhat-config-kickstart` 命令。

在你创建kickstart 文件的时候，你可以随时选择「文件」 => 「预览」来评审你当前的选择。

8.1. 基本配置

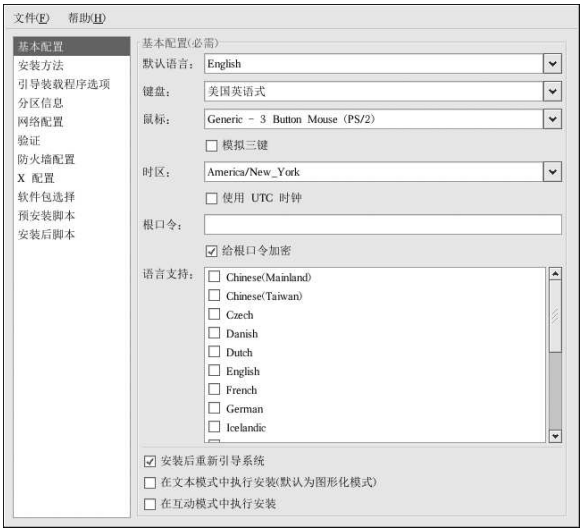


图**8-1.** 基本配置

从「语言」菜单中选择要在安装中使用，并在安装后用做默认的语言。

从「键盘」菜单中选择系统的键盘类型。

从「鼠标」菜单中选择系统的鼠标类型。如果你选择了「无鼠标」，鼠标就不会被配置。如果你选择了「探测鼠标」，安装程序就会试图自动探测鼠标。多数现代鼠标都可以被探测到。

如果你有一个两键鼠标，你可以选择「模拟三键」来模拟三键鼠标。如果该选项被选，同时点击鼠标的左右两键就会被认为是点击了鼠标的中间按钮。

从「时区」菜单中，选择系统使用的时区。要配置系统使用UTC，选择「使用**UTC** 时钟」。

在「根口令」文本字段内输入想用的根口令。如果你想在文件中保存口令时加密，选择「加密根口令」。如果加密选项被选，当文件被保存时，你键入的普通文本就会被加密并写入kickstart 文件中。不要键入已经加密的口令然后又选择要给它加密。

除了在「语言」下拉菜单中选择的语言之外，要安装其它附加语言，在「语言支持」列表中选择它们。从「语言」下拉菜单中选择的语言在安装后被用作默认语言。不过，默认语言可以在安装后使用语言配置工具（`redhat-config-language`）来改变。

选择「安装后重新引导系统」会在安装结束后自动重新引导系统。

kickstart 安装默认使用图形化模式执行。要超越默认值而使用文本模式，选择「在文本模式中执行安装」选项。

你可以使用互动模式执行kickstart 安装。这意味着安装程序会使用所有在kickstart 文件中预设的选项，但是它允许你在继续到下一个屏幕前预览选项。要继续到下一个屏幕上，在你同意设置后点击「下一步」按钮。如果你对预设的选项不满意，你可以在继续安装前改变它们。如果你更喜欢这类安装，选择「在互动模式中执行安装」按钮。

8.2. 安装方法

图**8-2.** 安装方法

「安装方法」屏幕允许你选择执行新安装或升级安装。如果你选择升级，「分区信息」和「软件包选择」选项就会被禁用。它们不被kickstart 升级所支持。

在这个屏幕上，你还需选择kickstart 安装的类型。可选的类型如下：

- 「光盘驱动器」 — 选择这个选项来从Red Hat Linux 光盘中安装Red Hat Linux。
- 「**NFS**」 — 如果你打算从NFS 共享目录中安装Red Hat Linux，选择该选项。两个要求你输入NFS 服务器和目录的文本字段箱会出现。输入NFS 服务器的完整域名或IP 地址；以及包含安装树的`RedHat` 目录。譬如，如果你的NFS 服务器包含`/mirrors/redhat/i386/RedHat`，在要求NFS 目录的字段内输入`/mirrors/redhat/i386`。
- 「**FTP**」 — 如果你打算从FTP 服务器安装Red Hat Linux，选择该选项。两个要求你输入FTP 服务器和目录的文本字段箱会出现。输入FTP 服务器的完整域名或IP 地址；以及包含`RedHat` 目录的FTP 目录名。譬如，如果你的FTP 服务器包含`/mirrors/redhat/i386/RedHat`，在要

求FTP 目录的字段内输入/mirrors/redhat/i386。如果FTP 服务器要求用户名和口令，也请指定它们。

- 「**HTTP**」 — 如果你打算从HTTP 服务器安装Red Hat Linux，选择该选项。两个要求你输入HTTP 服务器和目录的文本字段箱会出现。输入HTTP 服务器的完整域名或IP 地址；以及包含RedHat 目录的HTTP 目录名。譬如，如果你的HTTP 服务器包含/mirrors/redhat/i386/RedHat，在要求HTTP 目录的字段内输入/mirrors/redhat/i386。
- 「硬盘驱动器」 — 如果你打算从硬盘驱动器安装Red Hat Linux，选择该选项。两个要求你输入硬盘驱动器分区和目录的文本字段箱会出现。硬盘驱动器安装需要使用ISO（或光盘）映像。请在安装前确定先校验ISO 映像的完整性。要校验它们，使用md5sum 程序和《*Red Hat Linux* 安装指南》中讨论的linux mediacheck 引导选项。在「硬盘驱动器分区」文本箱内输入包含ISO 映像的硬盘分区（如/dev/hda1），然后在「硬盘驱动器目录」文本箱内输入包含ISO 映像的目录。

8.3. 引导装载程序选项

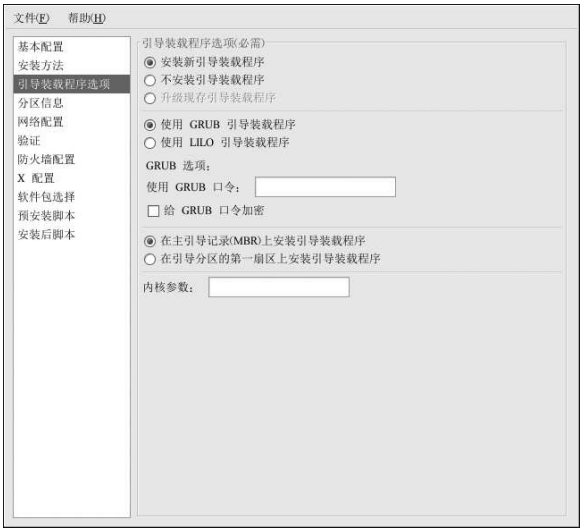


图**8-3.** 引导装载程序选项

你可以选择安装GRUB 或LILO 作为引导装载程序。如果你不想安装引导装载程序，选择「不安装引导装载程序」。如果你选择要不安装引导装载程序，请确定你创建了引导盘或有其它引导Red Hat Linux 系统的方法（如第三方引导装载程序）。

如果你选择要安装引导装载程序，你必须还得选择要安装哪一个（GRUB 或LILO）以及安装在哪里（主引导记录或/boot 分区的第一个扇区）。如果你打算把它用作引导装载程序，把它安装到MBR 上，如果你用的是不同的引导装载程序，把LILO 或GRUB 装在/boot 分区的第一个扇区上，并配置其它引导装载程序来引导Red Hat Linux。

要在系统引导时向内核传递特殊参数，把它们输入到「内核参数」文本字段内。譬如，如果你有一个IDE 光盘刻录器，你可以告诉内核在使用**cdrecord** 前必须得载入SCSI 模拟驱动程序，方法是把**hdd=ide-scsi** 输入为内核参数（这里的**hdd** 是光盘设备）。

如果你选择的引导装载程序是GRUB，你可以配置一个GRUB 口令来保护它。在「使用**GRUB** 口令」文本字段内输入这个口令。如果你想在文件中把口令加密保存，选择「加密**GRUB** 口令」。当文件被存盘后，你键入的普通文本口令就会被加密写入kickstart 文件。不要键入已加密的口令然后又选择给它加密。

如果你选择的引导装载程序是LILO，选择你是否要使用线形模式，以及是否要强制使用lba32 模式。

如果在「安装方法」页上选择了「升级现有安装」，选择「升级现有引导装载程序」来升级现存的引导装载程序配置并保留其中原有的项目。

8.4. 分区信息

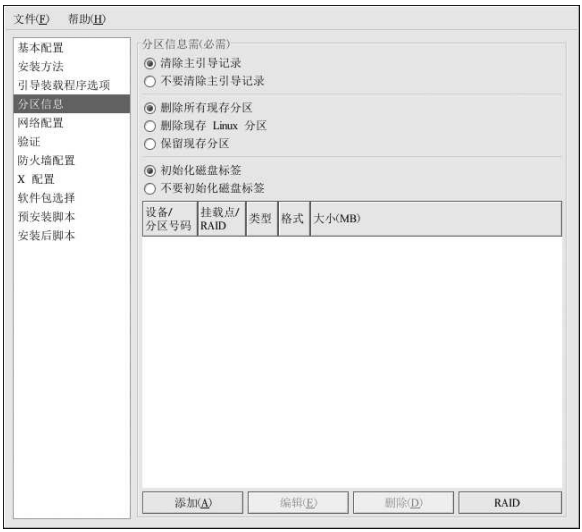


图**8-4.** 分区信息

选择是否要清除主引导记录（MBR）。你还可以选择删除所有分区、删除所有现存的Linux 分区、或保留现存分区。

你可以把磁盘卷标初始为系统体系的默认值（例如，x86 使用`msdos`，Itanium 使用`gpt`）。如果你在一个崭新的硬盘驱动器上安装，选择「初始化磁盘标签」。

8.4.1. 创建分区

要创建分区，点击「添加」按钮。如图8-5所示的「分区选项」窗口就会出现。为新分区选择挂载点、文件系统类型和分区大小。你还可以从下列选项中选择：

- 在「附加的大小选项」部分中，选择分区要使用固定大小、指定大小、还是使用驱动器上的全部剩余空间。如果你把文件系统类型选为交换区（swap），你可以选择让安装程序使用建议值而不是指定的大小来创建交换分区。
- 强制分区被创建为主分区。

- 在指定硬盘驱动器上创建分区。譬如，要在第一个IDE 硬盘（/dev/hda）上制作分区，把**hda** 指定为驱动器。不要在驱动器名称中包括/dev。
- 使用现存分区。譬如，要在第一个IDE 硬盘上的第一个分区（/dev/hda1）上制作分区，把**hda1** 指定为分区。不要在分区名中包括/dev。
- 把分区格式化为选定的文件系统类型。

图**8-5.** 创建分区

要编辑某现存分区，从列表中选择它，然后点击「编辑」按钮。一个和你添加分区相同的「分区选项」窗口会出现，如图8-5所示，只不过它上面的值已被预填。修改分区选项，然后点击「确定」。

要删除某现存分区，从列表中选择它，然后点击「删除」按钮。

8.4.1.1. 创建软件**RAID** 分区

阅读第3章来学习有关RAID 和RAID 级别的知识。你可以配置RAID 0、1、和5。

要创建软件RAID 分区，使用以下步骤：

1. 点击「**RAID**」按钮。
2. 选择「创建软件**RAID** 分区」。
3. 按前面描述的方法来配置分区，只不过选择「软件**RAID**」作为文件系统类型。此外，你必须指定要制作分区的硬盘驱动器或指定要使用的现存分区。

图**8-6.** 创建软件**RAID** 分区

重复这些步骤来为你的RAID 设置创建所需的分区。不是你所有的分区都一定要是RAID 分区。

创建了构成RAID 设备所需的所有分区后，遵循以下步骤：

1. 点击「**RAID**」按钮。
2. 选择「创建**RAID** 设备」。
3. 选择挂载点、文件系统类型、RAID 设备名称、RAID 级别、RAID 成员、软件RAID 设备的备件数量、以及是否要格式化RAID 设备。

图**8-7.** 创建软件**RAID** 设备

4. 点击「确定」来把设备添加到列表中。

8.5. 网络配置

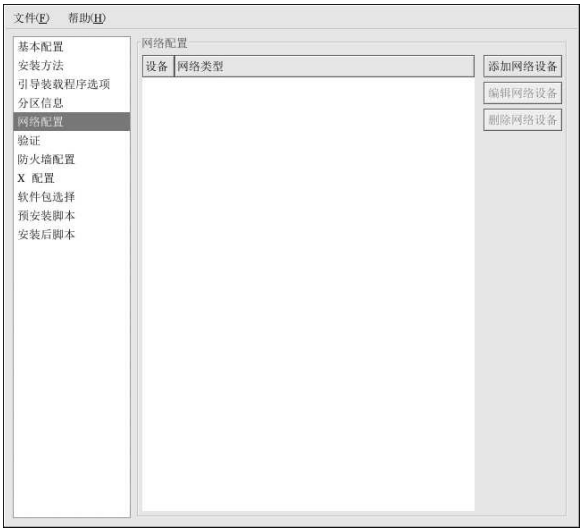


图**8-8.** 网络配置

如果要通过kickstart 安装的系统没有以太网卡，则不要在「网络配置」页上配置它。

只有在你选择了网络类型的安装方法（NFS、FTP 或HTTP）时才需要联网。联网可以随时在安装后使用网络管理工具（`redhat-config-network`）来配置。详情请参阅第12章。

对于系统上的每个以太网卡，点击「添加网络设备」，然后选择网络设备和设备的网络类型。第一个以太网卡选择**eth0** 作为网络设备，第二个以太网卡选择**eth1**，依此类推。

8.6. 验证

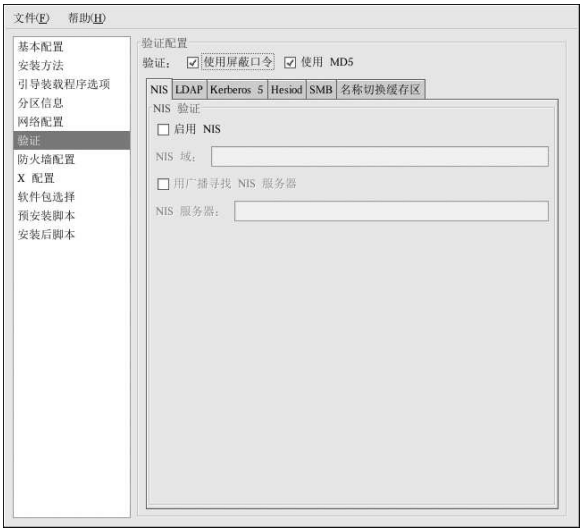


图**8-9.** 验证

在「验证」部分，选择用户口令是否使用屏蔽和MD5 加密。推荐你使用这些选项，它们被默认选择。

「验证配置」选项允许你配置下列验证方法：

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- 名称切换缓存

这些方法不被默认启用。要启用一种或多种方法，点击恰当的标签，然后点击「启用」旁边的复选箱，接着输入用于该验证方法的适当信息。

8.7. 防火墙配置

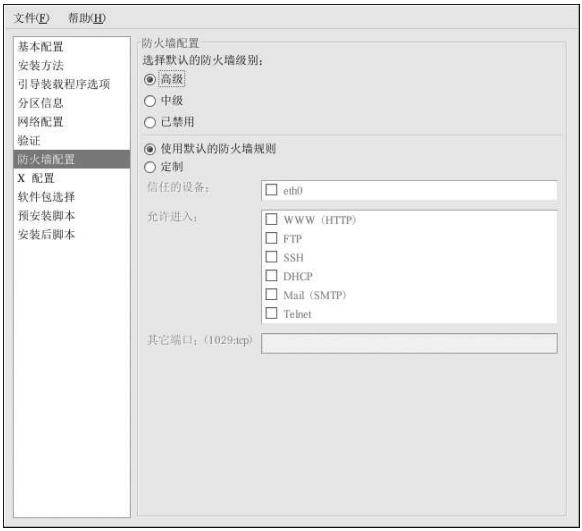


图**8-10.** 防火墙配置

「防火墙配置」窗口与Red Hat Linux 安装程序和安全级别配置工具中的屏幕一模一样。在「高级」、「中级」和「已禁用」这些级别中选择。关于这些安全级别的详细信息，请参阅第13.1 节。

8.8. X 配置

如果你要安装X 窗口系统，你可以在kickstart 安装过程中配置它。方法是，在如图8-11所示的「**X** 配置」窗口上选择「配置**X** 窗口系统」按钮。如果该选项没有被选，X 配置选项就会被禁用，`skipx` 选项就会被写入kickstart 文件。

8.8.1. 常规

配置X 的第一步是选择默认的色彩深度和分辨率。从相应的下拉菜单中选择它们。请确定指定与你的视频卡和显示器兼容的色彩深度及分辨率。

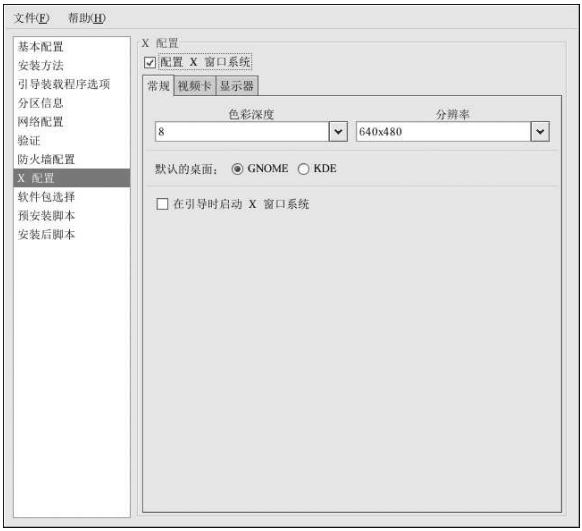


图**8-11. X** 配置- 常规

如果你把GNOME 和KDE 桌面都安装了，你需要选择一个默认的桌面。如果你只安装了一个桌面，请确定选择它。当系统被安装后，用户可以选择他们想默认使用的桌面。关于GNOME 和KDE 的详细信息，请参阅《*Red Hat Linux* 安装指南》和《*Red Hat Linux* 入门指南》。

下一步，选择你在系统引导时是否要启动X 窗口系统。该选项会在带有图形化登录屏幕的运行级别5 中启动系统。在系统被安装后，你可以修改/etc/inittab 配置文件来改变这一选项。

8.8.2. 视频卡

「探测视频卡」被默认选择。如果你想让安装程序在安装中探测视频卡，则接受默认设置。多数现代视频卡都能被探测到。如果你选择了该选项，并且安装程序无法成功地探测视频卡，安装程序就会在视频卡配置屏幕上中止。要继续安装进程，从视频卡列表中选择一个，然后点击「下一步」。

另外，你也可以从「视频卡」 标签上的列表中选择，如图8-12所示。在「视频卡内存」下拉菜单中选择视频内存数量。这些值会被安装程序用来配置X 窗口系统。

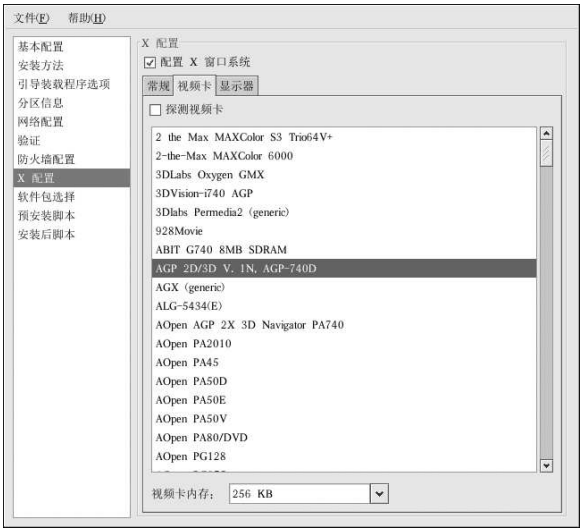


图**8-12. X** 配置- 视频卡

8.8.3. 显示器

配置了视频卡之后，点击「显示器」标签，如图8-13所示。

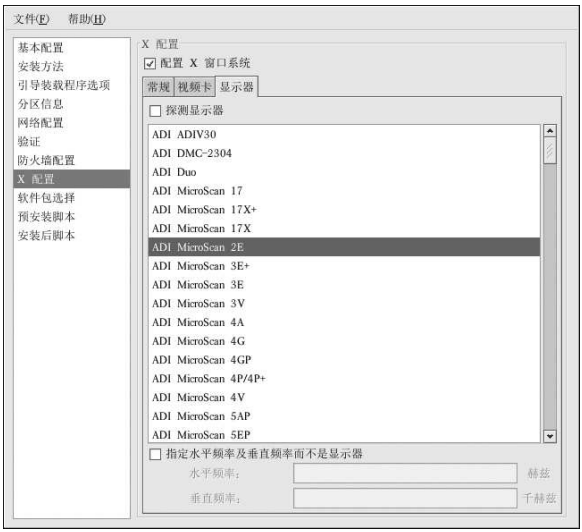


图**8-13. X** 配置- 显示器

「探测显示器」被默认选择。如果你想让安装程序在安装中探测显示器，则接受默认值。多数现代显示器都能被探测到。如果你选择了该选项，并且安装程序无法成功地探测显示器，安装程序就会在显示器配置屏幕上中止。要继续安装进程，从显示器列表中选择一个，然后点击「下一步」。

另外，你也可以从列表中选择显示器。你还可以选择「指定水平频率及垂直频率而不是显示器」选项来指定显示器的水平和垂直频率。这在你的显示器没有在列表中列出的情况下有用。注意，当这个选项被启用，显示器列表就会被禁用。

8.9. 软件包选择

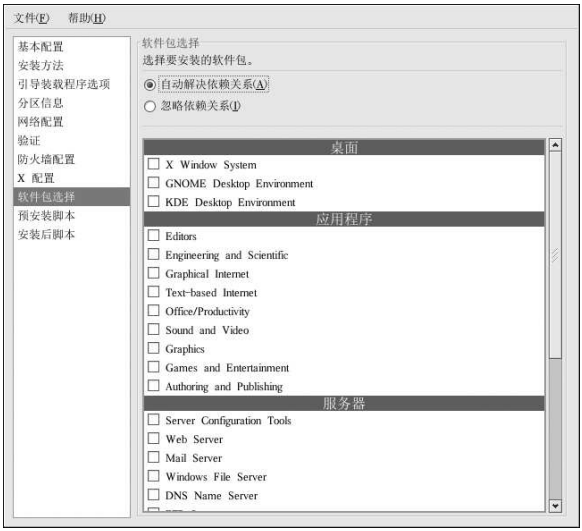


图**8-14.** 软件包选择

「软件包选择」窗口允许你选择要安装的软件包组。

还有一些选项能够帮助你自动解决或忽略软件包依赖关系。

目前，**Kickstart** 配置器不允许你选择单个软件包。要安装单个软件包，在你保存了kickstart 文件后，修改其中的%packages 部分。详情请参阅第7.5 节。

8.10. 预安装脚本

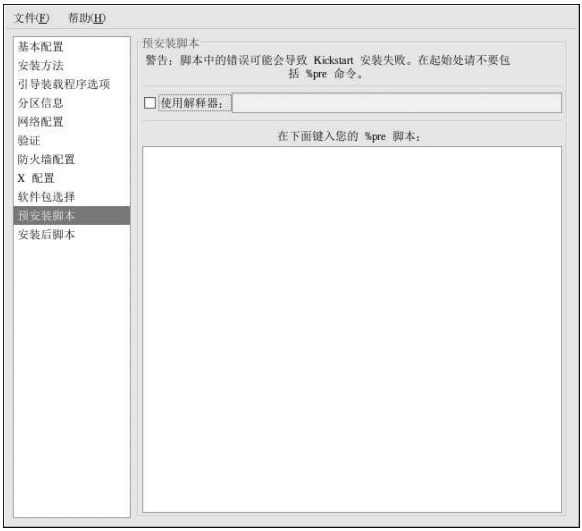


图**8-15.** 预安装脚本

你可以添加系统在解析kickstart 文件后，安装开始前要运行的命令。如果你在kickstart 文件中配置了网络，联网在这部分被处理前会被启用。如果你想包括一个预安装脚本，在文本区域内输入它。

要指定用来执行脚本的语言，选择「使用解释器」选项，并在它旁边的文本箱内输入它。例如，你可以为Python 脚本指定**`/usr/bin/python2.2`**。该选项和在你的kickstart 文件中使用`%pre --interpreter` *`/usr/bin/python2.2`* 相对应。


小心

不要包括`%pre` 命令。它会自动为你添加。

8.11. 安装后脚本

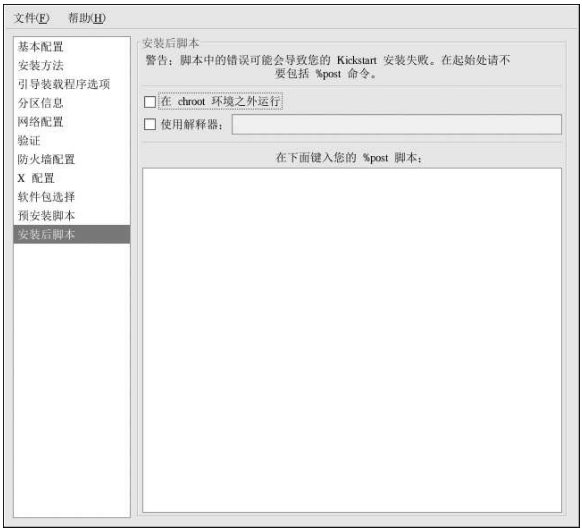


图**8-16.** 安装后脚本

你还可以添加系统在安装结束后要执行的命令。如果你在kickstart 文件中正确地配置了网络，联网就会被启用，该脚本中就可以包含访问网络资源的命令。如果你想包括一个安装后脚本，在文本区域内输入它。


小心

不要包括`%post` 命令。它会自动为你添加。

譬如，要改变新安装的系统上的每日消息（message of the day），在`%post` 部分添加以下命令：

```
echo "Hackers will be punished!" > /etc/motd
```


窍门

你可以在第7.7.1 节中找到更多范例。

8.11.1. Chroot 环境

如果你想让安装后脚本在chroot 环境之外运行，点击「安装后」窗口顶端该选项旁边的复选箱。这和使用`%post` 部分中的`--nochroot` 选项效果相同。

如果你想在安装后部分，在chroot 环境之外对新安装的文件系统做一些改变，你必须在/mnt/sysimage 后面加上目录名。

譬如，如果你选择了「在**chroot** 环境之外运行」，前面的例子就需要被改为：

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

8.11.2. 使用解释器

要指定用来执行脚本的语言，选择「使用解释器」选项，并在它旁边的文本箱内输入它。例如，你可以为Python 脚本指定**/usr/bin/python2.2**。该选项和在你的kickstart 文件中使用`%pre --interpreter` */usr/bin/python2.2* 相对应。

8.12. 保存文件

完成了kickstart 选项的选择后，要评审kickstart 文件的内容，选择「文件」 => 「预览」。

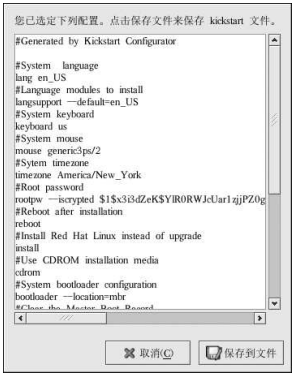


图**8-17.** 预览

要保存kickstart 文件，点击预览窗口中的「保存到文件」按钮。要不预览而保存文件，选择「文件」 => 「保存文件」或按[Ctrl]-[S]。一个对话框会出现。选择要保存文件的位置。

保存文件之后，请参阅第7.10 节来获取如何启动kickstart 安装的信息。

9. 基本系统恢复

虽说车到山前必有路，问题出现时总会有相应的解决办法，但是这些解决办法却要求你理解并熟悉系统。本章描述了如何引导入救援模式和单用户模式，你可以在这些模式中使用你的知识和能力来修复系统。

9.1. 常见问题

你可能会鉴于以下几个原因而需要引导入一种恢复模式：

- 你无法正常引导入Red Hat Linux（运行级别3 或5）。
- 你遇到了硬件或软件问题，并且你想把几个重要的文件从系统硬盘中取出。
- 你忘记了根口令。

9.1.1. 无法引导入Red Hat Linux

这个问题通常是由于在安装了Red Hat Linux 之后安装另一个操作系统造成的。某些操作系统假定你的计算机上没有安装任何其它操作系统，因而覆盖最初包含GRUB 或LILO 引导装载程序的主引导记录（MBR）。如果引导装载程序被这种方式覆盖了，除非你进入救援模式并重新配置引导装载程序，你将无法引导Red Hat Linux。

另一个常见问题出现在使用分区工具来重划分区大小或在安装后从空闲空间中创建新分区从而改变了分区的顺序之后。如果你的/ 分区的分区号码改变了，引导装载程序将无法找到它来挂载这个分区。要解决这个问题，引导入救援模式，若使用GRUB，修改/boot/grub/grub.conf 文件，若使用LILO 则修改/etc/lilo.conf 文件。你必须在修改LILO 配置文件时还运行/sbin/lilo 命令。

9.1.2. 硬件或软件问题

这一类包括的情况比较广泛。其中两种可能的情况是硬盘驱动器失效或在引导装载程序的配置文件中指定了无效的设备或内核。如果以上任何一种情况发生了，你将无法引导入Red Hat Linux。然而，如果你引导入系统恢复模式之一，你也许能够解决这个问题，或至少抢救出你的最重要的文件。

9.1.3. 根口令

如果你忘记了根口令该怎么办？要把它重设为另一个口令，引导入救援模式或单用户模式，并使用passwd 命令来重设根口令。

9.2. 引导入救援模式

救援模式提供了完全从磁盘、光盘或其它引导方式而不是从系统硬盘驱动器中引导一个小型Red Hat Linux 环境的能力。

如它的名称所暗示，救援模式是用来把你从某种情况中解救出来的模式。在正常操作中，你的Red Hat Linux 系统使用位于系统硬盘上的文件来处理一切事务— 运行程序；贮存文件；诸如此类。

然而，在有些情况下，你可能无法使Red Hat Linux 运行得完整到可以访问系统硬盘上文件的程度。使用救援模式，即便你无法从硬盘上运行Red Hat Linux，你也可以存取贮存在该系统硬盘上的文件。

要引导入救援模式，你必须能够使用以下方法之一来引导系统：

- 通过从根据`bootdisk.img`映像制作的安装引导盘来引导系统。[1]
- 通过从安装引导光盘[2]中引导。
- 通过从Red Hat Linux 光盘#1 中引导。

使用以上方法引导后，在安装引导提示下输入以下命令：

`linux rescue`

你会被提示回答几个基本的问题，包括要使用的语言。它还提示你选择有效救援映像的位置。从「本地光盘」、「硬盘驱动器」、「**NFS** 映像」、「**FTP**」、或「**HTTP**」中选择。所选位置中必须包含一个有效的安装树，这个安装树必须和你用来引导的光盘#1 中的Red Hat Linux 版本相同。如果你使用一个引导光盘或磁盘来启动救援模式，这个安装树必须和创建介质所用的安装树相同。关于如何在硬盘驱动器、NFS 服务器、FTP 服务器、或HTTP 服务器上设置安装树的信息，请参阅《*Red Hat Linux* 安装指南》。

如果你选择的救援映像不需要网络连接，你会被征询是否要建立网络连接。如果你想把文件备份到另一台计算机上或从共享网络位置上安装一些PRM 软件包时，网络连接会很有用。

你还会看到以下消息：

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage. You can then make any changes required to your
system. If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

如果你选择「继续」，它会试图把你的文件系统挂载到`/mnt/sysimage`目录下。如果它挂载分区失败，它会通知你。如果你选择「只读」，它会试图在`/mnt/sysimage`目录下挂载你的文件系统，但是挂载模式为只读。如果你选择「跳过」，你的文件系统将不会被挂载。如果你任务你的文件系统已损坏，选择「跳过」。

一旦你的系统进入了救援模式，在VC（虚拟控制台）1 和VC 2（使用[Ctrl]-[Alt]-[F1] 组合键来进入VC 1，[Ctrl]-[Alt]-[F2] 来进入VC 2）上会出现提示：

```
-/bin/sh-2.05b#
```

如果你选择了「继续」来自动挂载你的分区，并且它们被成功地挂载了，那么你就会进入单用户模式。

即便你的文件系统被挂载，救援模式中的默认根分区只不过是一个临时的根分区，而不是正常用户模式（运行级别3 或5）中的文件系统根分区。如果你选择要挂载文件系统，并且它被成功地挂载了，你可以通过执行以下命令来把救援模式的根分区改变为你的文件系统的根分区：

```
chroot /mnt/sysimage
```

---

1. 要创建安装引导盘，插入一张空白磁盘，使用Red Hat Linux 光盘1 上的`images/bootdisk.img`文件，并执行命令：`dd if=bootdisk.img of=/dev/fd0`。
2. 要创建安装引导光盘，请参阅《*Red Hat Linux* 安装指南》中的说明。

如果你需要运行rpm之类的命令，改变根分区就会很有用，因为这类命令要求你的根分区被挂载为/。要退出chroot环境，键入exit，你就会返回到提示。

如果你选择「跳过」，你仍可以试图在救援模式中手工挂载分区，方法是：创建一个目录，如，*/foo*，然后键入以下命令：

```
mount -t ext3 /dev/hda5 /foo
```

在以上命令中，*/foo* 是你创建的目录，*/dev/hda5* 是你想挂载的分区。如果分区的类型是ext2，则把ext3替换为ext2。

如果你不知道分区的名称，使用以下命令来列举它们：

```
fdisk -l
```

从提示下，你可以运行许多有用的命令，例如：

- list-harddrives，列举系统中的硬盘驱动器
- ssh、scp和ping，查看网络是否被启动
- dump和restore，用于带有磁带驱动器的用户
- parted和fdisk，用来管理分区
- rpm，用于安装或升级软件
- joe，用来编辑配置文件（如果你试图启动其它常用的编辑器，如emacs、pico或vi，joe编辑器仍会被启动。）

9.3. 引导入单用户模式

单用户模式的优越性之一是你不必使用引导软盘或引导光盘；不过，它仍旧给你提供了把文件系统挂载为只读模式或干脆不挂载这两种选择。

在单用户模式中，你的计算机引导入运行级别1。你的本地文件系统被挂载，但是你的网络不会被激活。你有一个可用的系统维护shell。和救援模式不同，单用户模式会自动试图挂载你的文件系统；如果你的文件系统无法被成功挂载，不要使用单用户模式。如果你的系统上的运行级别1的配置被损坏，你就不能使用单用户模式。

如果你的系统引导了，但是在引导后却不允许你登录，你可以试着使用单用户模式。

如果你使用的是GRUB，使用以下步骤来引导入单用户模式：

1. 如果你配置了GRUB口令，键入p并输入口令。
2. 选择带有你想引导的内核版本的**Red Hat Linux**，然后键入e来编辑。你会看到用于所选卷标的配置文件中的一个项目列表。
3. 选择起首为kernel的行，然后键入e来编辑那一行。
4. 转到行尾，然后键入**single**（按[空格]键，然后键入**single**）。按[Enter]来退出编辑模式。
5. 回到了GRUB屏幕后，键入b来引导入单用户模式。

如果你使用的是LILO，在LILO引导提示（如果你使用的是图形化LILO，你必须按[Ctrl]-[x]来退出图形化屏幕后再进入boot:提示）后键入：

```
linux single
```

9.4. 引导入紧急模式

在紧急模式中，你会被引导入尽可能少的系统环境中。根文件系统将会被挂载为只读模式，而且几乎什么都不会被设置。紧急模式优于单用户模式之处在于：在紧急模式中，init 文件没有被载入。如果init 被损坏或停止运行，你仍可以挂载文件来恢复在重新安装中会丢失的数据。

要引导入紧急模式，使用在第9.3 节中描述的引导单用户的方法。其中有一个例外，把关键字**single** 替换成关键字**emergency**。

redhat.

10.

软件RAID 配置

首先请阅读第3章来了解一下RAID、硬件和软件RAID 间的区别、以及RAID 0、1、和5 之间的区别。

软件RAID 能够在Red Hat Linux 的图形化安装期间或kickstart 安装期间配置。本章讨论如何使用**Disk Druid** 界面来在安装期间配置软件RAID。

在你创建RAID 设备之前，你必须首先创建RAID 分区，然后遵循以下步骤：

1. 在「磁盘分区设置」屏幕上，选择「用**Disk Druid** 手工分区」。
2. 在**Disk Druid** 中，选择「新建」来创建一个新分区。
3. 你不能输入一个挂载点（在你创建了RAID 设备后你才可以做）。
4. 从「文件系统类型」下拉菜单中选择「软件**RAID**」，如图10-1所示。

图**10-1.** 创建一个新**RAID** 分区

5. 对于「允许的驱动器」，选择要在其上创建RAID 的驱动器。如果你有多个驱动器，所有驱动器都会在这里被选择，你必须取消选择你不想在上面创建RAID 的驱动器。
6. 输入你想要的分区大小。
7. 选择「固定大小」来使物理卷具备指定大小，选择「指定空间大小**(MB)**」，输入以MB 为单位的大小来给物理卷大小一个范围，或选择「使用全部可用空间」来使它的大小扩充到填满整个硬盘的可用空间。如果你有不止一个可扩展的分区，它们会分享磁盘上的可用空闲空间。
8. 如果你想让这个分区成为主分区，选择「强制为主分区」。
9. 如果你想让安装程序在格式化硬盘驱动器之前检查磁盘坏块，选择「检查磁盘坏块」。
10. 点击「确定」来返回到主屏幕。

重复这些步骤来创建你的RAID 设置所需的分区。注意，不是所有的分区都必须是RAID 分区。譬如，你可以仅把/home 分区配置为软件RAID 设备。

一旦你创建了所有所需的「软件**RAID**」分区，遵循以下步骤：

1. 在**Disk Druid** 的主分区屏幕上（参见图10-3）选择「**RAID**」按钮。
2. 接着，图10-2就会出现，你可以在这里制作RAID 设备。

图**10-2.** 制作**RAID** 设备

3. 输入挂载点。
4. 为分区选择文件系统类型。
5. 为RAID 设备选择设备名称，如：**md0**。
6. 选择你的RAID 级别。可供选择的有：**RAID 0**、 **RAID 1**、和**RAID 5**。

注记

如果你想把/boot 制成RAID 分区，你必须选择RAID 级别1，而且它必须使用前两个驱动器之一（首先IDE，其次SCSI）。如果你不想把/boot 制成RAID 分区，但是你要把/ 制成RAID 分区，它必须是RAID 级别1，而且它必须是前两个驱动器之一（首先IDE，其次SCSI）。

7. 你刚刚创建的RAID 分区会出现在「**RAID** 成员」列表中。从这个列表中选择要创建RAID 设备的分区。
8. 如果配置的是RAID 1 和RAID 5，请指定备用分区的数量。如果某个软件RAID 分区失效了，这个备用的分区会自动被用作替换分区。对每一个你想指定的备用分区，你必须制作一个额外的软件RAID 分区（RAID 设备中的分区以外的）。在前一步骤中，为RAID 设备以及备件选择分区。
9. 点击了「确定」后，RAID 设备会出现在「驱动器摘要」列表中，如图10-3所示。这时，你可以继续安装进程。要获取进一步说明，请参阅《*Red Hat Linux* 安装指南》。

图**10-3. RAID** 阵列已创建

11.

LVM 配置

LVM 可以在Red Hat Linux 的图形化安装过程中或kickstart 安装过程中被配置。你还可以使用 lvm 软件包中的工具来创建你的LVM 配置。但是本章会集中说明如何在Red Hat Linux 安装过程中使用**Disk Druid** 来完成这项任务。

首先请阅读第4章来了解LVM。以下是对配置LVM 所需步骤的概述：

- 从硬盘驱动器中创建物理卷（*physical volumes*）。
- 从物理卷中创建卷组（*volume groups*）。
- 从卷组中创建逻辑卷（*logical volumes*），并分派逻辑卷挂载点。

注记

你只能在GUI 安装模式中编辑LVM 卷组。在文本安装模式中，你可以给已存逻辑卷分派挂载点。

要在Red Hat Linux 安装过程中创建带有逻辑卷的逻辑卷组，步骤如下：

1. 在「磁盘分区设置」屏幕上，选择「用**Disk Druid** 手工分区」.
2. 选择「新建」.
3. 你将不能够输入挂载点（创建了卷组后你便可以输入）。
4. 从「文件系统类型」下拉菜单中选择「物理卷**(LVM)**」，如图11-1所示。

图**11-1.** 创建物理卷

5. 物理卷必须局限于一个驱动器上。对于「允许的驱动器」项目，选择你要在其上创建物理卷的驱动器。如果你有多个驱动器，所有驱动器都会在这里被选择，你必须取消选择其它的驱动器，只保留一个你想在上面创建物理卷的驱动器。
6. 输入你所需的物理卷的大小。
7. 选择「固定大小」来使物理卷具备指定大小，选择「指定空间大小**(MB)**」，输入以MB 为单位的大小来给物理卷大小一个范围，或选择「使用全部可用空间」来使它的大小扩充到填满

整个硬盘的可用空间。如果你有不止一个可扩展的物理卷，它们会分享磁盘上的可用空闲空间。

8. 如果你想让这个分区成为主分区，选择「强制为主分区」。
9. 如果你想让安装程序在格式化硬盘驱动器之前检查磁盘坏块，选择「检查磁盘坏块」。
10. 点击「确定」来返回到主屏幕。

重复这些步骤来创建你的LVM 设置所需的物理卷。例如，如果你想让卷组跨越不止一个驱动器，则在每个驱动器上都创建一个物理卷。

警告

/boot 分区不能够位于卷组中，因为引导装载程序无法从中读取它。如果你想让根分区位于逻辑卷组中，你需要创建分开的、不属于卷组的/boot 分区。

创建了所有的物理卷后，请遵循以下步骤：

1. 点击「**LVM**」按钮来把物理卷汇集到卷组中。基本上说，卷组是物理卷的集合。你可以有多个逻辑卷组，但是一个物理卷只能位于一个卷组中。

注记

在逻辑卷组中保留了一些磁盘空间作为管理费用。物理卷的总和可能和卷组的大小不相等；不过，所显示的逻辑卷的大小是正确的。

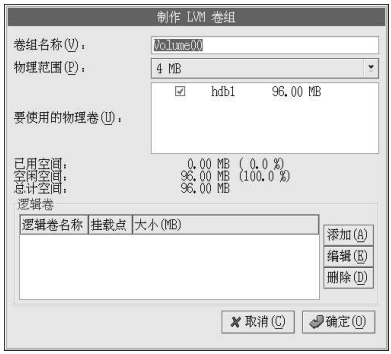


图**11-2.** 创建**LVM** 设备

2. 如果需要，你可以改变「卷组名称」。
3. 卷组内的所有逻辑卷必须按物理范围（*physical extent*）单位被分配。按照默认设置，物理范围被设置为4 MB；因此，逻辑卷的大小必须能够被4 MB 整除。如果你输入的大小不是4 MB 的整倍数，安装程序将会自动选择最接近4 MB 整倍数的数值。建议你不要改变这个设置。
4. 选择要用在卷组中的物理卷。
5. 创建带有/home 之类挂载点的逻辑卷。切记，/boot 不能够是逻辑卷。要添加逻辑卷，点击「逻辑卷」部分中的「添加」按钮。一个如图11-3所示的窗口就会出现。

图**11-3.** 创建逻辑卷

为每个你想创建的逻辑卷重复以上步骤。

窍门

你可能想在逻辑卷组中保留一些空闲空间，因此以后你可以扩展逻辑卷。

图**11-4.** 逻辑卷被创建

III. 与网络相关的配置

解释了如何配置网络之后，这一章讨论与联网相关的课题，例如：如何允许远程登录；如何在网络上共享文件和目录；如何设置万维网服务器。

目录

12.
网络配置

计算机需要网络连接才能和其它计算机通讯。这是通过由操作系统识别接口卡（如：以太网卡、ISDN 调制解调器、权标环），并配置该接口来连接到网络上来实现的。

网络管理工具可以用来配置以下类型的网络接口：

- 以太网
- ISDN
- 调制解调器
- xDSL
- 权标环
- CIPE
- 无线设备

要使用网络管理工具，你必须具备根特权。要启动这个程序，点击面板上的「主菜单」 => 「系统设置」 => 「网络」，或在shell 提示（如**XTerm** 或**GNOME** 终端）下键入`redhat-config-network` 命令。如果你键入了这个命令，若X 在运行，则图形化版本会被显示，否则，基于文本的版本会被显示。要强制运行基于文本的版本，使用`redhat-config-network-tui` 命令。

图**12-1.** 网络管理工具

如果你更喜欢直接修改配置文件，请参阅《*Red Hat Linux* 参考指南》来获取关于这些配置文件的位置和内容的信息。


窍门

访问Red Hat 硬件兼容性列表（http://hardware.redhat.com/hcl/）来判定Red Hat Linux 是否支持你的硬件设备。

12.1. 总览

要使用网络管理工具来配置网络连接，执行以下步骤：

1. 把物理硬件设备添加到硬件列表中。
2. 添加和该物理硬件设备相关的网络设备。
3. 配置主机名和DNS 设置。
4. 配置你无法通过DNS 查寻的主机。

本章将会针对每类网络连接来讨论以上的每一个步骤。

12.2. 建立以太网连接

要建立以太网连接，你需要一张网卡（NIC），一条网络电缆（通常是CAT5 电缆），以及要连接的网络。不同的网络配置使用不同的速度，请确定你的NIC 与你想连接的网络兼容。

要添加以太网连接，执行以下步骤：

1. 点击「设备」标签。
2. 点击工具栏上的「新建」按钮。
3. 从「设备类型」列表中选择「以太网连接」，然后点击「前进」。
4. 如果你已经把网卡添加到了硬件列表中，则从「以太网卡」列表中选择它。否则，选择「其它以太网卡」来添加硬件设备。

注记

安装程序通常会检测支持的以太网设备，并提示你配置它们。如果你在安装中已配置了以太网设备，它们会出现在「硬件」标签下的硬件列表内。

5. 如果你选择了「其它以太网卡」，「选择以太网适配器」窗口就会出现。选择该以太网卡的制造商和型号。选择该设备的名称。如果它是系统的第一个以太网卡，把**eth0** 选作设备名；如果它是第二个以太网卡，把**eth1** 选作设备名；依此类推。网络管理工具还允许你为NIC 配置资源。点击「前进」来继续。
6. 在「配置网络设置」页上（如图12-2所示），你可以选择DHCP 或静态IP 地址。如果该设备在每次网络启动时都被指定不同的IP 地址，就不要为其指定主机名。点击「前进」来继续。
7. 点击「创建以太网设备」上的「应用」按钮。

图12-2. 以太网设置

配置了以太网设备后，它就会出现在图12-3所示的设备列表中。

图12-3. 以太网设备

请确定选择「文件」 => 「保存」来保存改变。

添加了以太网设备后，你可以从设备列表中选择它，然后点击「编辑」来编辑它的配置。譬如，当某设备被添加，它被默认配置成引导时启动。要改变这个设置，选择编辑该设备，修改「当计算机启动时激活设备」的值，然后保存改变。

当设备被添加后，它不会被立即激活，你会看到「不活跃」状态。要激活某设备，从设备列表中选择它，然后点击「激活」按钮。如果系统配置了要在计算机启动是激活设备（默认），你不必重新执行这一步骤。

如果某个以太网所关联的设备不止一个，以后的设备就是设备别名（*device aliases*）。设备别名允许你给一个物理设备设置多个虚拟设备，因此一个物理设备可以有多个IP 地址。例如，你可以配置eth1 设备和eth1:1 设备。详情请参阅第12.13 节。

12.3. 建立ISDN 连接

ISDN 连接是使用ISDN 调制解调器卡通过由电话公司安装的特殊电话线建立的互联网连接。ISDN 连接在欧洲很流行。

要添加ISDN 连接，遵循以下步骤：

1. 点击「设备」标签。
2. 点击工具栏上的「新建」按钮。
3. 从「设备类型」列表中选择「**ISDN** 连接」，然后点击「前进」。
4. 从下拉菜单中选择ISDN 适配器。然后为该适配器配置资源和D 频道协议。点击「前进」来继续。

图**12-4. ISDN** 设置

5. 如果你的ISP 在预配置的列表中，选择它。否则，输入关于你的ISP 帐号的信息。如果你不了解这些信息，请联系你的ISP。点击「前进」。
6. 在「**IP** 设置」窗口上，选择要使用的「封装模式」，以及是通过DHCP 来获取IP 地址还是静态地设置它。结束后点击「前进」。
7. 在「建立拨号连接」页上，点击「应用」。

配置了ISDN 设备后，它会在设备列表中以**ISDN** 设备出现，如图12-5所示。

请确定选择「文件」 => 「保存」来保存改变。

添加了ISDN 设备后，你可以从设备列表中选择它，然后点击「编辑」来编辑它的配置。譬如，当某设备被添加，它被默认配置成引导时启动。你可以编辑它的配置来修改这项设置。压缩、PPP 选项、登录名、口令等等都可以被改变。

当设备被添加后，它不会被立即激活，你会看到「不活跃」状态。要激活某设备，从设备列表中选择它，然后点击「激活」按钮。如果系统配置了要在计算机启动是激活设备（默认），你不必重新执行这一步骤。

图**12-5. ISDN** 设备

12.4. 建立调制解调器连接

调制解调器可以用来配置通过活跃电话线进行的互联网连接。你需要一个互联网服务提供者（ISP）帐号（又称拨号帐号）。

要添加调制解调器连接，遵循以下步骤：

1. 点击「设备」标签。
2. 点击工具栏上的「新建」按钮。
3. 从「设备类型」列表中选择「调制解调器连接」，然后点击「前进」。
4. 如果在硬件列表中你已有一个配置了的调制解调器（在「硬件」标签上），网络管理工具假定你要用它来建立调制解调器连接。如果没有已配置了的调制解调器，它会试图检测系统中的调制解调器。探测可能会花一段时间。如果找到了一个调制解调器，一则消息会显示，警告你所显示的设置不是探测中找到的值。
5. 探测后，如图12-6所示的窗口就会显示。

图**12-6.** 调制解调器设置

6. 配置调制解调器、波特率、流控制、以及调制解调器音量。如果你不知道这些值，但是调制解调器被成功地探测到，则接受默认值。如果你没有按键式电话连线方式，取消选择相应的复选箱。点击「前进」。

7. 如果你的ISP 在预配置的列表中，选择它。否则，输入关于你的ISP 帐号的信息。如果你不了解这些信息，请联系你的ISP。点击「前进」。
8. 在「**IP** 设置」窗口上，选择要使用的「封装模式」，以及是通过DHCP 来获取IP 地址还是静态地设置它。结束后点击「前进」。
9. 在「建立拨号连接」页上，点击「应用」。

配置了调制解调器设备后，它会在设备列表中以「调制解调器」设备出现，如图12-7所示。

图**12-7.** 调制解调器设备

请确定选择「文件」=>「保存」来保存改变。

添加了调制解调器设备后，你可以从设备列表中选择它，然后点击「编辑」来编辑它的配置。譬如，当某设备被添加，它被默认配置成引导时启动。你可以编辑它的配置来修改这项设置。压缩、PPP 选项、登录名、口令等等都可以被改变。

当设备被添加后，它不会被立即激活，你会看到「不活跃」状态。要激活某设备，从设备列表中选择它，然后点击「激活」按钮。如果系统配置了要在计算机启动是激活设备（默认），你不必重新执行这一步骤。

12.5. 建立xDSL 连接

DSL 代表数码用户线路（Digital Subscriber Lines）。它的类型有ADSL、IDSL、和SDSL。网络管理工具使用xDSL 这个术语来指代所有类型的DSL 连接。

某些DSL 提供者要求你使用以太网卡来配置系统通过DHCP 获取IP 地址。某些DSL 提供者要求你使用以太网卡来配置PPPoE（以太网上的点对点协议）。请向你的DSL 提供者咨询应该使用的方法。

如果你被要求使用DHCP，请参阅第12.2 节来配置你的以太网卡。

如果你被要求使用PPPoE，遵循以下步骤：

1. 点击「设备」标签。
2. 点击工具栏上的「新建」按钮。
3. 从「设备类型」列表中选择「**xDSL** 连接」，然后点击「前进」。
4. 如果你的以太网卡在硬件列表中，从这一页的下拉菜单中选择「以太网设备」，如图12-8所示。否则，「选择以太网适配器」窗口会出现。

注记

安装程序通常会检测支持的以太网设备，并提示你配置它们。如果你在安装中已配置了以太网设备，它们会出现在「硬件」标签下的硬件列表内。

图**12-8. xDSL** 设置

5. 如果「选择以太网适配器」窗口出现，选择该以太网卡的制造商和型号。选择该设备的名称。如果它是系统的第一个以太网卡，把**eth0** 选作设备名；如果它是第二个以太网卡，把**eth1** 选作设备名；依此类推。网络管理工具还允许你为NIC 配置资源。点击「前进」来继续。
6. 输入「提供商名称」、「登录名」、和「口令」。如果你有一个T-Online 账号，与其在默认窗口中输入「登录名」和「口令」，你可以点击「**T-Online** 账号设置」按钮，并输入所需信息。点击「前进」来继续。
7. 在「建立**DSL** 连接」页上，点击「应用」。

配置了DSL 连接后，它会出现在如图12-7所示的列表中。

图**12-9. xDSL** 设备

请确定选择「文件」 => 「保存」来保存改变。

添加了以太网设备后，你可以从设备列表中选择它，然后点击「编辑」来编辑它的配置。譬如，当某设备被添加，它被默认配置成引导时启动。要改变这个设置，编辑它的配置。

当设备被添加后，它不会被立即激活，你会看到「不活跃」状态。要激活某设备，从设备列表中选择它，然后点击「激活」按钮。如果系统配置了要在计算机启动是激活设备（默认），你不必重新执行这一步骤。

12.6. 建立权标环连接

在权标环网络中，所有的计算机都以圆环方式连接。权标（*token*），或特殊网络包，在权标环里流动，从而允许计算机彼此发送信息。

窍门

关于在Linux 下使用权标环的详细信息，请参阅*Linux Token Ring Project*，该网站位于：http://www.linuxtr.net/。

要添加权标环连接，遵循以下步骤：

1. 点击「设备」标签。
2. 点击工具栏上的「新建」按钮。
3. 从「设备类型」列表中选择「权标环连接」，然后点击「前进」。
4. 如果你已经在硬件列表中添加了一个权标环卡，从「以太网卡」列表中选择它。否则，选择「其它权标环卡」来添加硬件设备。
5. 如果你选择了「其它权标环卡」，如图12-10 所示的「选择权标环适配器」窗口会出现。选择适配器的制造商和型号。选择设备名称。如果它是系统的第一张权标环卡，选择**tr0**；如果它是第二张权标环卡，选择**tr1**，依此类推。网络管理工具还允许用户为适配器配置资源。点击「前进」来继续。

图**12-10.** 权标环设置

6. 在「配置网络设置」页上，选择DHCP 或静态IP 地址。你可以为设备指定一个主机名。如果该设备在每次启动网络时都接收到一个动态IP 地址，则不要指定主机名。点击「前进」来继续。
7. 在「创建权标环设备」页上，点击「应用」。

配置了权标环设备后，它会出现在如图12-11所示的设备列表中。

图**12-11.** 权标环设备

请确定选择「文件」 => 「保存」来保存改变。

添加了设备后，你可以从设备列表中选择它，然后点击「编辑」来编辑它的配置。譬如，你可以配置是否要在引导时启动它。

当设备被添加后，它不会被立即激活，你会看到「不活跃」状态。要激活某设备，从设备列表中选择它，然后点击「激活」按钮。如果系统配置了要在计算机启动是激活设备（默认），你不必重新执行这一步骤。

12.7. 建立CIPE 连接

CIPE 代表加密IP 封装（Crypto IP Encapsulation）。它用来配置IP 隧道设备。譬如，CIPE 可以用来从外界进入虚拟专用网络（VPN）。如果你需要设置CIPE 设备，请向你的系统管理员询问正确的设置值。

图**12-12. CIPE** 设置


窍门

关于CIPE 和设置CIPE 的更多信息，请参阅《*Red Hat Linux* 安全指南》。

12.8. 建立无线连接

无线以太网设备现在越来越流行。该配置和以太网配置相似，只不过它允许你配置SSID 等设置，以及你的无线设备的钥匙。

要添加无线以太网连接，遵循以下步骤：

1. 点击「设备」标签。
2. 点击工具栏上的「新建」按钮。
3. 从「设备类型」列表中选择「无线连接」，然后点击「前进」。
4. 如果你已经把无线网卡添加到了硬件列表，从「以太网卡」列表中选择它。否则，选择「其它无线卡」来添加硬件设备。


注记

安装程序通常会检测支持的无线以太网设备，并提示你配置它们。如果你在安装中已配置了以太网设备，它们会出现在「硬件」标签下的硬件列表内。

5. 如果你选择了「其它无线卡」，「选择以太网适配器」窗口会出现。选择该以太网卡的制造商和型号。如果它是系统的第一个以太网卡，把**eth0** 选作设备名；如果它是第二个以太网卡，把**eth1** 选作设备名；依此类推。网络管理工具还允许你为无线网卡配置资源。点击「前进」来继续。
6. 在如图12-13所示的「配置无线连接」页上，为无线设备配置设置。

图**12-13.** 无线设置

7. 在「配置网络设置」页上，选择DHCP 或静态IP 地址。你可以为设备指定一个主机名。如果该设备在每次启动网络时都接收到一个动态IP 地址，则不要指定主机名。点击「前进」来继续。
8. 在「创建无线连接」页上，点击「应用」。

配置了无线设备后，它就会出现在如图12-14所示的设备列表上。

图**12-14.** 无线设备

请确定选择「文件」 => 「保存」来保存改变。

添加了无线设备后，你可以从设备列表中选择它，然后点击「编辑」来编辑它的配置。譬如，你可以配置是否要在引导时启动它。

当设备被添加后，它不会被立即激活，你会看到「不活跃」状态。要激活某设备，从设备列表中选择它，然后点击「激活」按钮。如果系统配置了要在计算机启动是激活设备（默认），你不必重新执行这一步骤。

12.9. 管理DNS 设置

DNS 标签允许你配置系统的主机名、域、名称服务器和搜索域。名称服务器用来查寻网络上的其它主机。

如果DNS 服务器要从DHCP 或PPPoE 中检索到（或从ISP 中检索），不要添加主要、次要或第三DNS 服务器。

如果主机名被动态地从DHCP 或PPPoE 中检索（或从ISP 中检索），请不要改变它。

图**12-15. DNS** 配置


注记

名称服务器部分不是用来把系统配置成名称服务器的，而是用来配置系统解析IP 地址和主机名所用的名称服务器。

12.10. 管理主机

「主机」标签允许你从/etc/hosts 文件中添加、编辑、或删除主机。该文件包含IP 地址和它们相对应的主机名。

当你的系统试图把主机名解析为IP 地址或判定IP 地址的主机名时，它在使用名称服务器前首先参照/etc/hosts 文件（若你使用的是默认的Red Hat Linux 配置）。如果IP 地址被列在/etc/hosts 文件中，名称服务器就不会被使用。如果你的网络包括没有列在DNS 内的IP 地址，推荐你把它们添加到/etc/hosts 文件中。

要在/etc/hosts 文件中添加项目，点击「主机」标签下的「新建」按钮，提供要求的信息，然后点击「确定」。选择「文件」 => 「保存」或按[Ctrl]-[S] 来把改变保存到/etc/hosts 文件中。你不必重新启动网络或网络服务，因为该文件在每个地址被解析时都会被参照。


警告

不要删除localhost 项目。即便系统没有网络连接或持续运行的网络连接，某些程序仍需要通过localhost 环回界面来连接系统。

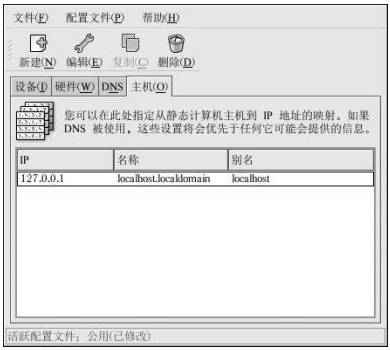


图**12-16.** 主机配置


穷门

要改变查寻顺序，编辑/etc/host.conf 文件。order hosts, bind 这一行指定/etc/hosts 优先于名称服务器。把这一行改为order bind, hosts 会配置你的系统首先使用名称服务器来解析主机名和IP 地址。如果IP 地址无法通过名称服务器被解析，你的系统会在/etc/hosts 文件中查寻IP 地址。

12.11. 激活设备

网络设备可以被配置为在引导时活跃或不活跃。例如，调制解调器连接的网络设备通常不在引导时被启动；而以太网连接通常在引导时被启动。如果你的网络设备被配置成不在引导时启动，你可以使用**Red Hat** 控制网络程序来在引导后激活它。要启动它，点击面板上的「主菜单」 => 「系统工具」 => 「网络设备控制」，或键入命令redhat-control-network.

图**12-17.** 激活设备

要激活某设备，从列表中选择它，点击「激活」按钮。要停止该设备，从列表中选择它，点击「解除」。

如果配置了不止一个网络配置文件，它们在界面中被列出，并可以被激活。详情请参阅第12.12节。

12.12. 使用配置文件

每个物理硬件设备可以创建多个逻辑网络设备。例如，如果你的系统上有一个以太网卡（eth0），你可以使用不同的绰号和不同的配置选项来配置逻辑网络设备。这些设备都和eth0 相关联。

逻辑网络设备与设备别名不同。和同一物理设备相关联的逻辑网络设备必须存在于不同的配置文件中，并且不能被同时激活。设备别名也与同一物理硬件设备相关联，但是和同一物理硬件相关联的设备别名能够同时被激活。关于创建设备别名的详情，请参阅第12.13 节。

配置文件（*Profiles*）可以被用来为不同的网络创建多个配置集合。配置集合中除了主机和DNS 设置外还可以包含逻辑设备。配置了配置文件后，你可以使用网络管理工具来在它们之间切换使用。

按照默认设置，其中一个配置文件为「公用」。要创建新配置文件，选择「配置文件」=>「新建」，然后为配置文件输入一个独特的名称。

你现在正在修改如主窗口底部的状态栏所示的新配置文件。

点击已经在列表中的某个现存设备，然后点击「复制」按钮来把某个现存设备复制到逻辑网络设备。如果你使用「新建」按钮，创建的会是网络别名，这是不正确的。要改变逻辑设备的属性，从列表中选择它，然后点击「编辑」。例如，绰号可以被改成一个更具描述性的名称，如**eth0_office**，因此它可以被更容易地被识别。

在设备列表中，有一列被标为「配置文件」的复选箱。对每个配置文件，你都可以选择或取消选择设备。只选择被包括在当前选中配置文件中的设备。例如，如果你在一个叫做**Office** 的配置文件中创建了一个叫做**eth0_office** 的逻辑设备，并想在该配置文件被选时激活这个逻辑设备，取消选择eth0 设备，选择eth0_office 设备。

例如，图12-18显示了一个带有逻辑设备**eth0_office** 的叫做**Office** 的配置文件。它配置使用DHCP来激活第一个以太网卡。

图**12-18. Office** 配置文件

注意，如图12-19所示的**Home** 配置文件激活**eth0_home** 逻辑设备，该设备与eth0 相关联。

图**12-19. Home** 配置文件

你还可以配置`eth0`来只激活**Office** 配置文件，而在**Home** 配置文件中只激活ppp（调制解调器）设备。另一个例子是让「公用」配置文件激活`eth0`，而使用**Away** 配置文件在旅行时用来激活ppp 设备。

引导时不能激活配置文件。只有在「公用」配置文件（默认的配置文件）中被设置在引导时激活的设备才能在引导时被激活。系统引导后，点击面板上的「主菜单」(on the Panel) => 「系统工具」 => 「网络设备控制」（或键入`redhat-control-network`命令）来选择一个配置文件并激活它。激活配置文件部分只有在除了默认的「公用」配置文件外，你还有其它配置文件的情况下才会出现在网络设备控制界面中。

或者，使用以下命令来启用配置文件（把<*`profilename`*>替换为配置文件的名称）：

```
redhat-config-network-cmd --profile <profilename> --activate
```

12.13. 设备别名

设备别名（*Device aliases*）是和同一物理硬件相关联的虚拟设备，但是它们可以同时被激活，并拥有不同的IP 地址。它们通常使用设备名、冒号和数字来代表（例如：eth0:1）。它们在你想给系统多个IP 地址却只有一个网卡时很有用处。

配置了以太网设备，如`eth0`之后，要使用静态IP 地址（DHCP 不能使用别名），转到「设备」标签，并点击「新建」。选择配置了别名的以太网卡，设置别名的静态IP 地址，然后点击「应用」来创建它。因为以太网卡的设备已经存在，刚刚创建的只不过是一个别名，如`eth0:1`。


警告

如果你要给以太网设备配置别名，那么这个设备和别名都不能配置使用DHCP。你必须手工配置IP 地址。

图12-20显示了`eth0`设备的一个别名。注意`eth0:1`设备— `eth0`的第一个别名。`eth0`的第二个别名的设备名会是`eth0:2`，依此类推。要修改设备别名的设置，如是否要在引导时激活，或别名号码，从列表中选择它，然后点击「编辑」按钮。

图**12-20.** 网络设备别名示例

选择某个别名，点击「激活」按钮来激活这个别名。如果你配置了多个配置文件，选择要包括它的配置文件。

要校验别名是否被激活，使用`/sbin/ifconfig`命令。其输入应该显示该设备和设备别名拥有不同的IP 地址：

```
eth0   Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
     inet addr:192.168.100.5 Bcast:192.168.100.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
     TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
     collisions:475 txqueuelen:100
     RX bytes:55075551 (52.5 Mb) TX bytes:178108895 (169.8 Mb)
     Interrupt:10 Base address:0x9000

eth0:1  Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
     inet addr:192.168.100.42 Bcast:192.168.100.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     Interrupt:10 Base address:0x9000

lo    Link encap:Local Loopback
     inet addr:127.0.0.1 Mask:255.0.0.0
     UP LOOPBACK RUNNING MTU:16436 Metric:1
     RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
     TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:1627579 (1.5 Mb) TX bytes:1627579 (1.5 Mb)
```

13.

基本防火墙配置

如同建筑物中的防火墙会试图防止火势蔓延，计算机中的防火墙会试图防止计算机病毒蔓延到你的系统中。它还能防止未经授权的用户进入你的系统。防火墙存在于你的计算机和网络之间，它可以判定你的计算机上哪些服务可以被网络上的远程用户访问。一个正确配置的防火墙能够极大地增强你的系统安全性。我们提议你为所以连接到互联网上的Red Hat Linux 系统配置一个防火墙。

13.1. 安全级别配置工具

Red Hat Linux 安装中的「防火墙配置」屏幕给你提供了几个可供选择的选项：高级、中级、无防火墙；你还可以选择要允许的指定设备、进入服务、和端口等。

安装后，你可以使用安全级别配置工具来改变系统的安全级别。如果你更喜欢使用基于向导的程序，请参阅第13.2 节。

要启动这个程序，选择面板上的「主菜单」 => 「系统设置」 => 「安全级别」，或在shell（如XTerm 或GNOME 终端）下键入`redhat-config-securitylevel`命令。

图**13-1.** 安全级别配置工具

从下拉菜单中选择想要的安全级别。

「高级」

‘ 如果你选择「高级」，你的系统将不会接受没有被你刻意定义的连接（默认设置以外的连接）按照默认设置，只有以下连接会被允许：

- DNS 回应
- DHCP — 因此，任何使用DHCP 的网络界面都可以被正确的配置。

如果你选择「高级」，你的防火墙将不会允许以下连接：

- 活跃状态FTP（在多数客户机中默认使用的被动状态FTP，应该能够正常运行。）
- IRC DCC 文件传输
- RealAudio™
- 远程X 窗口系统客户

如果你要把系统连接到互联网上，但是不打算把它当作服务器来运行，这是最安全的选择。如果你需要额外的服务，你可以选择「定制」来允许指定的服务穿过防火墙。

注记

如果你选择了中级或高级防火墙，网络验证方法（NIS 和LDAP）将无法奏效。

「中级」

‘ 如果你选择「中级」，你的防火墙将不会允许远程机器访问你的系统上的某些资源。按照默认设置，对以下资源的访问是默认不允许的：

- 低于1023 的端口— 这些是标准要保留的端口，主要被一些系统服务所使用，如：**FTP**、**SSH**、**telnet**，**HTTP** 和**NIS**。
- NFS 服务器端口(2049) — NFS 对远程服务器和本地客户都已禁用。
- 为远程X 客户机设立的本地X 窗口系统显示。
- X 字体服务器端口（按照默认设置，**xfs** 不监听网络；它在字体服务器中被禁用。）

如果您想准许到**RealAudio™** 之类资源的访问，但仍要堵塞到普通系统服务的访问，选择「中级」。您可以选择「定制」来允许具体指定的服务穿过防火墙。

注记

如果你选择了中级或高级防火墙，网络验证方法（NIS 和LDAP）将无法奏效。

「无防火墙」

‘ 无防火墙给予完全访问权并不做任何安全检查。系统检查是对某些服务的禁用。建议你只有在一个可信任的网络（非互联网）中运行时，或者你想稍后再进行详细的防火墙配置时才选此项。

选择「定制」来添加信任的设备或允许附加的进入服务。

「信任的设备」

‘ 选择任何一个「信任的设备」会允许所有来自该设备的到你的系统的交通。它不在防火墙规则的限制之内。譬如，如果你在运行一个本地网络，但是通过PPP 拨号连接到了互联网上，你可以选择「**eth0**」，所有来自你的本地网络的交通就会被允许。把「**eth0**」选为“信任的设备”意味著所有通过以太网的交通都会被允许，但是通过ppp0 接口的交通仍受防火墙的限制。如果你想现在某个接口上的交通，就不要选择它。

建议你不要把连接到公共网络，如互联网，上的设备选为「信任的设备」。

「允许进入」

‘ 启用这些选项将允许具体指定的服务穿过防火墙。注意，在工作站类型安装中，大多数这类服务在系统内不存在。

「**DHCP**」

‘ 如果你允许进入的DHCP 查询和回应，你会允许任何使用DHCP 来判定其IP 地址的网络接口。DHCP 通常是启用的。如果DHCP 没有被启用，你的计算机就不再能够获取IP 地址。

「**SSH**」

‘ *S*ecure （安全）*SH*ell (SSH) 是用来在远程机器上登录及执行命令的协议套件。如果你计划使用SSH 工具通过防火墙来进入你的机器，启用该选项。你必须安装`openssh-server` 软件包才能使用SSH 工具来远程地进入你的机器。

「**Telnet**」

‘ Telnet 是一种远程登录机器的协议。Telnet 的通信是不加密的，没有提供任何防止网络刺探之类的安全措施。建议你不要允许进入的Telnet 访问。如果你想允许进入的Telnet 访问，你必须安装`telnet-server` 软件包。

「**WWW (HTTP)**」

‘ HTTP 协议被Apache（以及其它万维网服务器）用来提供网页。如果你打算使你的万维网服务器公开可用，请启用该选项。你不必启用该选项来本地查看网页或开发网页。如果你想提供网页，你必须安装`apache` 软件包。

启用「**WWW (HTTP)**」不会为HTTPS 打开一个端口。要启用HTTPS，在「其它端口」字段中指定它。

「邮件**(SMTP)**」

‘ 如果你想允许进入的邮件穿过你的防火墙，因此你的远程主机能够直接连接到你的机器来散发邮件，则启用该选项。如果你只想从使用POP3 或IMAP 的ISP 服务器来收取邮件，或则使用**fetchmail** 之类的工具，则不必启用这个选项。注意，不正确配置的SMTP 服务器会允许远程机器使用你的服务器来发送垃圾邮件。

「**FTP**」

‘ FTP 协议被用来在网络上的机器间传输文件。如果你打算使你的FTP 服务器公开可用，启用该选项。你需要安装`vsftpd` 软件包才能是该选项能够发生作用。

点击「确定」来激活防火墙。点击了「确定」后，选定的选项就会被转换成`iptables` 命令并写入`/etc/sysconfig/iptables` 文件。`iptables` 服务也被启动，因此，保存了选定选项后，防火墙就会被立即激活。


警告

如果你在`/etc/sysconfig/iptables` 文件中配置了一个防火墙或防火墙规则，在你选择了「无防火墙」并点击了「确定」来保存改变之后，这个文件就会被删除。

选定的选项还被写入`/etc/sysconfig/redhat-config-securitylevel` 文件，因此这些设置在程序下次启动时被恢复。请不要手工编辑该文件。

要激活`iptables` 服务，并在引导时自动启动，请参阅第13.3 节来获取详情。

13.2. GNOME Lokkit

GNOME Lokkit 允许你通过建立基本的ipchains 联网规则来为普通用户配置防火墙设置。你不必编写这些规则，该程序会向你提出一系列关于你如何使用系统的问题，然后把它们写入/etc/sysconfig/ipchains 文件。

你不应该使用**GNOME Lokkit** 来生成复杂的防火墙规则。该程序的目的是帮助普通用户在使用调制解调器、电缆、或DSL 连接到互联网上时进行自我保护。要配置特指的防火墙规则，请参阅《*Red Hat Linux* 参考指南》 书中的“使用*iptables* 来建立防火墙”这一章。

要禁用指定的服务或拒绝指定的主机和用户，请参阅第14章。

要启动图形化的f **GNOME Lokkit**，选择「主菜单」 => 「系统工具」 => 「更多系统工具」 => **Lokkit**，或在shell 提示下以根用户身份键入gnome-lokkit 命令。如果你没有安装X 窗口系统，或者你优选基于文本的程序，在shell 提示下键入lokkit 命令来启动这个程序的文本模式。

13.2.1. 基本

图**13-2.** 基本

在启动程序之后，为你的系统选择相应的安全级别：

- 「**High Security**」 — 这一选项会禁用几乎所有激活网络所需的DNS 回应和DHCP 之外的网络连接。IRC、ICQ、其它即时消息传递服务、以及RealAudio™ 在没有代理的情况下都无法运行。
- 「**Low Security**」 — 该选项将不会允许到系统的远程连接，包括NFS 连接和远程X 窗口系统会话。在端口1023 之下运行的服务将不会接受连接，包括FTP、SSH、Telnet、以及HTTP。
- 「**Disable Firewall**」 — 该选项不会创建任何安全规则。建议你只有在信任的网络（非互联网）中运行时，或在大型防火墙之后运行时，或自行编写定制的防火墙规则时才选择该选项。如果你选定了这个选项并点击了「下一步」，请跳到第13.3 节这一节。你的系统的安全级别将不会被改变。

13.2.2. 本地主机

如果系统上有以太网设备，「**Local Hosts**」页会允许你配置防火墙规则是否要应用到发送给每个设备的连接请求。如果该设备把系统连接到防火墙后的局域网，并不直接连接到互联网，选择「**Yes**」。如果该以太网卡把系统连接到电缆或DSL 调制解调器，我们提议你选择「**No**」。

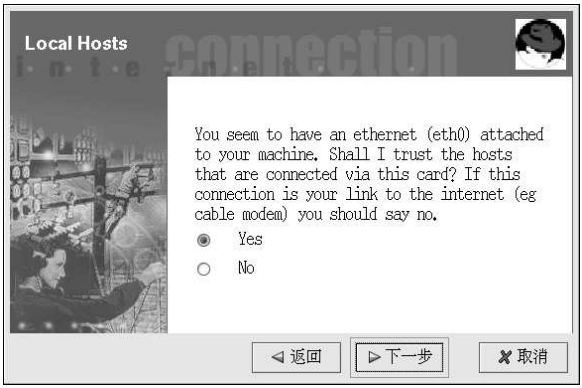


图**13-3. Local Hosts**（本地主机）

13.2.3. DHCP

如果你使用DHCP 来激活系统上的任何以太网接口，你必须对DHCP 问题回答「**Yes**」。如果你回答了“No”，你将无法使用以太网接口来建立连接。许多电缆和DSL 互联网提供者要求你使用DHCP 来建立互联网连接。

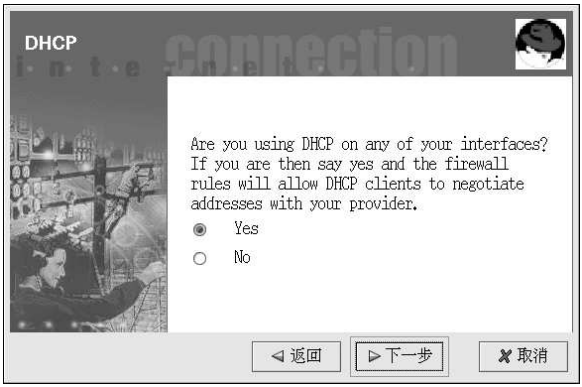


图**13-4. DHCP**

13.2.4. 配置服务

GNOME Lokkit 还允许你启动或停止普通服务。如果你在配置服务时回答了「是」，你就会得到有关下列服务的提示：

- 「**Web Server**」 — 如果你打算让用户连接到在你的系统上运行的万维网服务器（如Apache），请选择该选项；如果你只打算查看你自己的系统或网络上其它服务器上的网页，则不必选择该选项。

- 「**Incoming Mail**」 — 如果你的系统需要接受进入的邮件，选择该选项。如果你只打算使用IMAP、POP3、或fetchmail 来检索电子邮件，则不必选择该选项。
- 「**Secure Shell**」 — 安全Shell，或SSH，是一个用来在远程机器上通过加密连接来登录和执行命令的工具套件。如果你需要通过ssh 来远程地访问你的机器，选择该选项。
- 「**Telnet**」 — Telnet 允许你远程登录到你的机器上，不过，它并不安全。它在网络中发送的是纯文本（包括口令）。推荐你使用SSH 在你的机器上远程登录。如果你需要使用telnet 来访问你的系统，选择该选项。

要禁用你不需要的其它服务，使用服务配置工具（参阅第14.3 节）或**ntsysv** （参阅第14.4 节），或`chkconfig`（参阅第14.5 节）。

13.2.5. 激活防火墙

点击「结束」会把防火墙规则写入`/etc/sysconfig/iptables` 文件，并通过启动`iptables` 服务来启动防火墙。


警告

如果你配置了防火墙，或在`/etc/sysconfig/iptables` 文件中配置了防火墙规则，你若选择了「**Disable Firewall**」并点击「结束」来保存所做改变，这些防火墙规则就会被删除。

我们强烈建议你从机器而不是远程X 会话中运行**GNOME Lokkit**。如果你禁用了到你的机器的远程访问，你将无法再进入系统来禁用防火墙规则。

如果你不想写入防火墙规则，点击「取消」。

13.2.5.1. 邮件转发

邮件转发（mail relay）是允许其它系统通过它来发寄电子邮件的系统。如果你的系统是一个邮件转发站，某些人便可能用它来通过你的机器散发垃圾邮件。

如果你选定要启用邮件服务，在「**Activate Firewall**」页上点击「结束」后，你会被提示是否检查邮件转发。如果你回答了「**Yes**」来检查邮件转发，**GNOME Lokkit** 就会试图连接*Mail Abuse Prevention System* 网站（http://www.mail-abuse.org/），并运行邮件转发测试程序。测试结果会在结束后显示。如果你的系统向邮件转发开放，强烈推荐你配置Sendmail 来避免它的发生。

13.3. 激活`iptables` 服务

防火墙规则只有在`iptables` 服务运行的时候才能被激活。要手工启动服务，使用以下命令：

```
/sbin/service iptables restart
```

要确保它在系统引导时启动，使用以下命令：

```
/sbin/chkconfig --level 345 iptables on
```

`ipchains` 服务不能和`iptables` 服务同时运行。要确定`ipchains` 服务被禁用，执行以下命令：

```
/sbin/chkconfig --level 345 ipchains off
```

你还可以使用服务配置工具来激活`iptables` 和`ipchains` 服务，详情请参阅第14.3 节。

14.

控制对服务的访问

维护Red Hat Linux 系统的安全性极端重要。管理系统安全的方法之一是谨慎管理对系统服务的使用。你的系统可能需要提供对某些服务的公开利用（譬如`httpd`，如果你在运行万维网服务器的话）。然而，如果你不需要提供某项服务，则应该把它关闭— 这会降低你对可能会出现的偷机取巧情况的曝光率。

管理对系统服务访问的方法有好几种。你必须根据服务、系统配置、以及你对Linux 的掌握程度来决定应使用哪一种方法。

拒绝对某一服务的使用的最简便方法是将其关闭。不论是由`xinetd`（我们会在本章节后面详细讨论）管理的服务，还是在`/etc/rc.d` 层次中的服务，都可以使用以下三种不同的应用程序来配置其启动或停止：

- 服务配置工具 — 一个图形化应用程序，它显示了每项服务的描述，以及每项服务是否在引导时启动（运行级别3、4、5），并允许你启动、停止、或重新启动每项服务。
- **ntsysv** — 基于文本的程序。它允许你为每个运行级别配置引导时要启动的服务。对于不属于`xinetd` 的服务而言，改变不会立即生效。你不能使用这个程序来启动、停止、或重新启动不属于`xinetd` 的服务服务。
- `chkconfig` — 一个允许你在不同运行级别启动和关闭服务的命令行工具。对于不属于`xinetd` 的服务而言，改变不会立即生效。你不能使用这个工具程序来启动、停止、或重新启动不属于`xinetd` 的服务服务。

你可能会发现以上工具比使用下面这些方法更简单— 手工编辑位于`/etc/rc.d` 目录下的大量符号链接，或者编辑`/etc/xinetd.d` 中的`xinetd` 配置文件。

管理对系统服务的使用的另一种方法是通过使用`iptables` 来配置IP 防火墙。如果你是Linux 新手，请注意，`iptables` 可能不是你的最佳解决办法。设置`iptables` 是一项复杂的作业，最好由经验丰富的Linux 系统管理员来执行。

从另一角度而言，`iptables` 的优越性是它的灵活性。譬如，如果你需要一个定制的解决方案来为某些主机提供到某些服务的使用权，`iptables` 能够为你提供。关于`iptables` 的详情，请参阅《*Red Hat Linux* 参考指南》和《*Red Hat Linux* 安全指南》。

此外，如果你寻找的是能够为你的家用机器设置常规访问规则的工具程序，并且（或者）你还是Linux 新手，你应该尝试使用安全级别配置工具（`redhat-config-securitylevel`）。该工具允许你为系统选择安全级别，它和Red Hat Linux 安装程序中的「防火墙配置」屏幕相似。你还可以使用**GNOME Lokkit**。**GNOME Lokkit** 是一种GUI 工具，它会向你询问一些你要如何使用你的机器的问题。根据你的回答，它会为你配置一个简单的防火墙。关于这些工具的详情，请参阅第13章。如果需要更明确的防火墙规则，请参阅《*Red Hat Linux* 参考指南》中的`iptables` 这一章。

14.1. 运行级别

在你配置到服务的访问之前，你必须理解Linux 运行级别。运行级别是一种状态，或模式（*mode*），它由列在`/etc/rc.d/rc<x>.d` 目录中的服务来定义，其中`<x>` 是运行级别的数字。

Red Hat Linux 使用下列运行级别：

- 0 — 停运
- 1 — 单用户模式
- 2 — 没有使用（可由用户定义）

- 3 — 完全的多用户模式
- 4 — 没有使用（可由用户定义）
- 5 — 完全的多用户模式（带有基于X 的登录屏幕）
- 6 — 重新引导

如果你使用的是文本登录屏幕，你是在运行级别3 中操作。如果你使用的是图形化登录屏幕，你是在运行级别5 中操作。

默认的运行级别可以通过修改/etc/inittab 文件来改变，该文件在接近开头的地方有一行与下面相似：

```
id:5:initdefault:
```

把这一行中的数字改成你想要的运行级别。所做改变在系统重新引导之后才会生效。

要立即改变运行级别，使用命令telinit，其后跟随运行级别数字。你必须是根用户才能使用这项命令。

14.2. TCP 会绕程序

许多UNIX 系统管理员对使用TCP 会绕程序来管理对某些网络服务的使用比较熟悉。由xinetd（以及任何带有内建libwrap 支持的程序）管理的服务能够使用TCP 会绕程序来管理使用权。xinetd 能够使用/etc/hosts.allow 和/etc/hosts.deny 文件来配置到系统服务的使用。如文件的名称所暗示，hosts.allow 包含一个允许客户使用被xinetd 所控制的网络服务的规则列表，hosts.deny 文件包含拒绝使用权的规则。hosts.allow 文件优先于hosts.deny 文件。对使用权限的授予或拒绝可以根据个别IP 地址（或主机名）或一类客户而定。详情请参阅《*Red Hat Linux* 参考指南》和hosts_access 的说明书（man）页第五章（man 5 hosts_access）。

14.2.1. xinetd

要控制到互联网服务的访问，使用xinetd。它是inetd 的安全替换品。xinetd 守护进程保存系统资源，提供访问控制和日志记录，并可以用来启动特殊目的的服务器。xinetd 能够用来提供到某些主机的访问；拒绝到某些服务的访问；限制进入连接的频率和（或）连接造成的载量等等。

xinetd 无时不在运行并监听它所管理的所有端口上的服务。当某个要连接它管理的某项服务的请求到达时，xinetd 就会为该服务启动合适的服务器。

xinetd 的配置文件是/etc/xinetd.conf，但是它只包括几个默认值以及包含/etc/xinetd.d 目录中的配置文件。如果目录的指令。要启用或禁用某项xinetd 服务，编辑位于/etc/xinetd.d 目录中的配置文件。如果disable 属性被设为**yes**，该项服务已禁用。如果disable 属性被设为**no**，则该项服务已被启用。你可以使用服务配置工具、**ntsysv** 或chkconfig 来编辑任何一个xinetd 配置文件或改变它的启用状态。要获得由xinetd 控制的网络服务列表，使用ls /etc/xinetd.d 命令来列举/etc/xinetd.d 目录的内容。

14.3. 服务配置工具

服务配置工具是图形化应用程序。它由Red Hat 开发，用来配置/etc/rc.d/init.d 中在引导时（对运行级别3、4、5 而言）要启动哪些SysV 服务，哪些xinetd 服务。它允许你启动、停止、和重新启动SysV 服务以及重新启动xinetd。

要从桌面启动服务配置工具，点击面板上的「主菜单」 => 「系统设置」 => 「服务器设置」 => 「服务」，或在shell 提示下（如**XTerm** 或**GNOME** 终端），键入命令redhat-config-services。

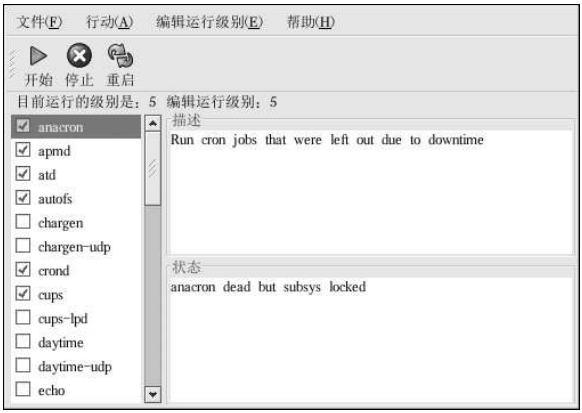


图**14-1.** 服务配置工具

服务配置工具显示当前运行级别以及你目前正编辑的运行级别。要编辑不同的运行级别，从下拉菜单中选择「编辑运行级别」，然后选择运行级别3、4、或5。关于对运行级别的描述，请参阅第14.1 节。

服务配置工具不但列出了/etc/rc.d/init.d 中的服务，还列出了由xinetd 控制的服务。点击左侧列表中的服务名来显示该服务的简短描述以及它的服务状态。如果这个服务不是xinetd 服务，状态窗口会显示该服务目前是否在运行。如果该服务被xinetd 所控制，状态窗口会显示「**xinetd** 服务」这个短语。

要立即启动、停止、或重新启动某项服务，从列表中选择该项服务，然后点击工具栏上的相应按钮（或从「行动」下拉菜单中选择行动）。如果该服务是一个xinetd 服务，行动按钮会被禁用，因为它们不能被单个地启动或停止。

如果你通过选择或取消选择服务名旁的复选箱来启用或禁用了xinetd 服务，你必须从下拉菜单中选择「文件」 => 「保存改变」来重新启动xinetd，并立即启用或禁用你所改变的xinetd 服务。xinetd 还被配置成自动记忆设置。你可以同时启用或禁用多个xinetd 服务，在结束后再保存改变。

譬如，假设你选择在运行级别3 中启用rsync，并保存了改变。rsync 服务会立刻被启用。下一次xinetd 被启动时，rsync 仍会被启用。


警告

当你保存了xinetd 服务中所做的改变，重新启动了xinetd 后，改变就会立即生效。当你保存了对其它服务的改变，运行级别会被重新配置，但是改变不会立即生效。

要在引导时为当前选中的运行级别启用不属于xinetd 的服务，选择列表中该服务名旁的复选箱。配置了运行级别后，通过选择下拉菜单上的「文件」 => 「保存改变」来应用改变。运行级别配置会被改变，但是不会被重新启动；这样，改变就不会立即生效。

譬如，假定你在配置运行级别3。如果你把anacron 服务的状态从“被选”改成“不选”，然后选择「保存改变」，运行级别3 的配置会被改变，因此anacron 在引导时就不会被启动。但是，运行级别3 没有被重新初始化，因此anacron 仍在运行。这时，从下列选择中任选一个：

1. 停止anacron 服务— 要关闭该服务，从列表中选择它，然后点击「停止」按钮。一条声明服务已被成功停止的消息就会被显示出来。

2. 重新初始化运行级别— 重新初始化运行级别的方法是：打开shell 提示，然后键入命令`telinit 3`（这里的3 是运行级别数字）。如果你改变了多个服务的「引导时启动」值，并想立即激活改变，推荐你使用这种方法。
3. 什么都不做— 你不必停止anacron 服务。你可以等到系统重新引导时才停止该服务。在系统下一次引导时，运行级别就会被初始化为不运行anacron 服务。

14.4. ntsysv

ntsysv 工具为激活或停运服务提供了简单的界面。你可以使用**ntsysv** 来启动或关闭由xinetd 管理的服务。你还可以使用**ntsysv** 来配置运行级别。按照默认设置，只有当前运行级别会被配置。要配置不同的运行级别，使用`--level` 选项来指定一个或多个运行级别。譬如，命令`ntsysv --level 345` 配置运行级别3、4、和5。

ntsysv 的界面和文本模式的安装程序的工作方式相仿。使用上下箭头来上下查看列表。使用空格键来选择或取消选择服务，或用来“按”「确定」和「取消」按钮。要在服务列表和「确定」、「取消」按钮中切换，使用[Tab]键。***** 标明某服务被设为启动。[F1] 键会弹出每项服务的简短描述。


警告

由xinetd 管理的服务会立即受到**ntsysv** 的影响。其它服务则不会立即生效。你必须使用`service` *`daemon`* `stop` 命令来停止某项服务。在前面的例子中，把*daemon* 换成你想停止的服务名称，譬如，httpd。把stop 换成start 或restart 来启动或重新启动某服务。

14.5. chkconfig

`chkconfig` 命令也可以用来激活和停运服务。如果你使用`chkconfig --list` 命令，你会看到一个系统服务列表，以及它们在运行级别0 到6 中已被启动（on）或停止（off）。在列表末端，你会看到由xinetd 管理的服务部分。

如果你使用`chkconfig --list` 来查询由xinetd 管理的服务，你会看到xinetd 服务是被启用（on）还是被关闭（off）了。譬如，命令`chkconfig --list finger` 返回了下列输出：

```
finger    on
```

如上所示，`finger` 作为xinetd 服务被启用。如果xinetd 在运行，`finger` 就会被启用。

如果你使用`chkconfig --list` 来查询`/etc/rc.d` 中的服务，你会看到服务在每个运行级别中的设置。譬如，命令`chkconfig --list anacron` 返回了下列输出：

```
anacron    0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

`chkconfig` 还能用来设置某一服务在某一指定的运行级别内被启动还是被停运。譬如，要在运行级别3、4、5 中停运`nscd` 服务，使用下面的命令：

```
chkconfig --level 345 nscd off
```


警告

由xinetd 管理的服务会立即被chkconfig 影响。譬如，如果xinetd 在运行，`finger` 被禁用，那么执行了`chkconfig finger on` 命令后，`finger` 就不必手工地重新启动xinetd 来立即被启用。对其它服务的改变在使用chkconfig 之后不会立即生效。你必须使用`service` *`daemon`* `stop` 命令来停止个别服务。在

前面的例子中，把*daemon* 换成你想停止的服务名称，如httpd。把stop 换成start 或restart 来启动或重新启动该服务。

14.6. 其它资料

详细信息请参考下列资料。

14.6.1. 安装了的文档

- ntsysv、chkconfig、xinetd 和xinetd.conf 的说明书（man）页。
- man 5 hosts_access — 主机访问控制文件格式的说明书（man）页（在第5 章）。

14.6.2. 有用的网站

- http://www.xinetd.org — xinetd 网页。它包含更详细的功能列表和配置文件范例。

14.6.3. 相关书籍

- 《*Red Hat Linux* 参考指南》, Red Hat, Inc. — 这本指南手册包含了关于TCP 会绕程序和xinetd 如何允许或拒绝访问的详细信息，如何使用它们来配置网络访问的详细信息，以及创建iptables 防火墙规则的说明。

15. OpenSSH

OpenSSH 是SSH （*S*ecure *SH*ell）协议的免费开源实现。它用安全、加密的网络连接工具代替了telnet、ftp、rlogin、rsh 和rcp 工具。OpenSSH 支持SSH 协议的版本1.3、1.5、和2。自从OpenSSH 的版本2.9 以来，默认的协议是版本2，该协议默认使用RSA 钥匙。

15.1. 为什么使用SSH?

使用OpenSSH 工具将会增进你的系统安全性。所有使用OpenSSH 工具的通讯，包括口令，都会被加密。telnet 和ftp 使用纯文本口令，并被明文发送。这些信息可能会被截取，口令可能会被检索，然后未经授权的人员可能会使用截取的口令登录进你的系统而对你的系统造成危害。你应该尽可能地使用OpenSSH 的工具集合来避免这些安全问题。

另一个使用OpenSSH 的原因是，它自动把DISPLAY 变量转发给客户机器。换一句话说，如果你在本地机器上运行X 窗口系统，并且使用ssh 命令登录到了远程机器上，当你在远程机器上执行一个需要X 的程序时，它会显示在你的本地机器上。如果你偏爱图形化系统管理工具，却不能够总是亲身访问该服务器，这就会为你的工作大开方便之门。

15.2. 配置OpenSSH 服务器

要运行OpenSSH 服务器，你必须首先确定你安装了正确的RPM 软件包。openssh-server 软件包是必不可少的，并且它依赖于openssh 软件包的安装与否。

OpenSSH 守护进程使用/etc/ssh/sshd_config 配置文件。Red Hat Linux 9 安装的默认配置文件在多数情况下应该足以胜任。如果你想使用没有被默认的sshd_config 文件提供的方式来配置守护进程，请阅读sshd 的说明书（man）页来获取能够在配置文件中定义的关键字列表。

要启动OpenSSH 服务，使用/sbin/service sshd start 命令。要停止OpenSSH 服务器，使用/sbin/service sshd stop 命令。如果你想让守护进程在引导时自动启动，请参阅第14章来获取关于如何管理服务的信息。

如果你重新安装了Red Hat Linux 系统，任何在它被重装前使用OpenSSH 工具连接到这个系统上的客户在它被重装后将会看到下列消息：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

重装后的系统会为自己创建一组新的身份标识钥匙；因此客户会看到RSA 主机钥匙改变的警告。如果你想保存系统原有的主机钥匙，备份/etc/ssh/ssh_host*key* 文件，然后在系统重装后恢复它。该过程会保留系统的身份。当客户机在该系统重装后试图连接它，它们就不会看到以上的警告信息。

15.3. 配置OpenSSH 客户

要从客户机连接到OpenSSH 服务器上，你必须在客户机器上装有openssh-clients 和openssh 软件包。

15.3.1. 使用ssh 命令

ssh 命令是rlogin、rsh 和telnet 命令的安全替换。它允许你在远程机器上登录并在其上执行命令。

使用ssh 来登录到远程机器和使用telnet 相似。要登录到一个叫做penguin.example.net 的远程机器，在shell 提示下键入下面的命令：

```
ssh penguin.example.net
```

第一次使用ssh 在远程机器上登录时，你会看到和下面相仿的消息：

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

键入**yes** 来继续。这会把该服务器添加到你的已知主机的列表中，如下面的消息所示：

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

下一步，你会看到向你询问远程主机口令的提示。在输入口令后，你就会在远程主机的shell 提示下了。如果你没有指定用户名，你在本地客户机器上登录用的用户名就会被传递给远程机器。如果你想指定不同的用户名，使用下面的命令：

```
ssh username@penguin.example.net
```

你还可以使用`ssh -l username penguin.example.net`。

ssh 命令可以用来在远程机器上不经shell 提示登录而执行命令。它的语法格式是：`ssh hostname command`。譬如，如果你想在远程主机penguin.example.net 上执行`ls /usr/share/doc` 命令，在shell 提示下键入下面的命令：

```
ssh penguin.example.net ls /usr/share/doc
```

在你输入了正确的口令之后，/usr/share/doc 这个远程目录中的内容就会被显示，然后你就会被返回到你的本地shell 提示下。

15.3.2. 使用scp 命令

scp 命令可以用来通过安全、加密的连接在机器间传输文件。它与rcp 相似。

把本地文件传输给远程系统的一般语法是：

```
scp localfile username@tohostname:/newfilename
```

localfile 指定源文件，*username@tohostname:/newfilename* 指定目标文件。

要把本地文件shadowman 传送到你在penguin.example.net 上的账号内，在shell 提示下键入（把*username* 替换成你的用户名）：

```
scp shadowman username@penguin.example.net:/home/username
```

这会把本地文件shadowman 传输给penguin.example.net 上的/home/*username*/shadowman 文件。

把远程文件传输给本地系统的一般语法是：

```
scp username@tohostname:/remotefile /newlocalfile
```

remotefile 指定源文件，*newlocalfile* 指定目标文件。

源文件可以由多个文件组成。譬如，要把目录/downloads 的内容传输到远程机器penguin.example.net 上现存的uploads 目录，在shell 提示下键入下列命令：

```
scp /downloads/* username@penguin.example.net:/uploads/
```

15.3.3. 使用sftp 命令

sftp 工具可以用来打开一次安全互动的FTP 会话。它与ftp 相似，只不过，它使用安全、加密的连接。它的一般语法是：*sftp username@hostname.com*。一旦通过验证，你可以使用一组和使用FTP 相似的命令。请参阅sftp 的说明书页（man）来获取这些命令的列表。要阅读说明书页，在shell 提示下执行man sftp 命令。sftp 工具只在OpenSSH 版本2.5.0p1 以上才有。

15.3.4. 生成钥匙对

如果你不想每次使用ssh、scp 或sftp 时都要输入口令来连接远程机器，你可以生成一对授权钥匙。

钥匙必须为每个用户生成。要为某用户生成钥匙，用想连接到远程机器的用户身份来遵循下面的步骤。如果你用根用户的身份完成了下列步骤，就只有根用户才能使用这对钥匙。

从OpenSSH 版本3.0 开始，~/.ssh/authorized_keys2、~/.ssh/known_hosts2 和/etc/ssh_known_hosts2 就会过时。SSH 协议1 和2 共享~/.ssh/authorized_keys、~/.ssh/known_hosts 和/etc/ssh/ssh_known_hosts 文件。

Red Hat Linux 9 默认使用SSH 协议2 和RSA 钥匙。


窍门

如果你重装了Red Hat Linux，但是想保留现有的钥匙对，备份你的主目录中的.ssh 目录。重装后，把该目录复制回主目录。该进程可为系统上的所有用户进行，包括根用户。

15.3.4.1. 为版本2 生成RSA 钥匙对

使用下列步骤来为SSH 协议的版本2 生成RSA 钥匙对。从OpenSSH 2.9 开始，它已成为默认设置。

1. 要生成RSA 钥匙对与协议的版本2 合作，在shell 提示下键入下列命令：
   ```
   ssh-keygen -t rsa
   ```
   接受~/.ssh/id_rsa 的默认位置。输入一个与你的帐号口令不同的口令句，再输入一次来确认。

   公钥被写入~/.ssh/id_rsa.pub。密钥被写入~/.ssh/id_rsa。决不能把密钥出示给任何人。
2. 使用chmod 755 ~/.ssh 命令改变你的.ssh 目录的许可权限。
3. 把~/.ssh/id_rsa.pub 的内容复制到你想连接的机器上的~/.ssh/authorized_keys 文件中。如果~/.ssh/authorized_keys 不存在，你可以把~/.ssh/id_rsa.pub 文件复制到那个机器上的~/.ssh/authorized_keys 文件中。
4. 如果你运行的是GNOME，跳到第15.3.4.4 节。如果你没在运行X 窗口系统，跳到第15.3.4.5 节。

15.3.4.2. 为版本2 生成DSA 钥匙对

使用下面的步骤来为SSH 协议的版本2 生成DSA 钥匙对。

1. 要生成用于协议的版本2 的DSA 钥匙对，在shell 提示下键入下面的命令：
   ```
   ssh-keygen -t dsa
   ```
   接受~/.ssh/id_dsa 的默认位置。输入一个与你的帐号口令不同的口令句，再输入一次来确认。

   
   窍门

   口令句是用来验证用户的一串词汇和字符。口令句和一般口令的不同之处在于：在口令句中你可以使用空格或制表符。口令句通常比一般口令长，因为它们通常使用短语而不仅仅用一个词。

   公钥被写入~/.ssh/id_dsa.pub。密钥被写入~/.ssh/id_dsa。决不能把密钥出示给任何人，这一点很重要。
2. 使用chmod 755 ~/.ssh 命令改变你的.ssh 目录的许可权限。
3. 把~/.ssh/id_dsa.pub 的内容复制到你想连接的机器中的~/.ssh/authorized_keys 文件中。如果文件~/.ssh/authorized_keys 不存在，你可以把~/.ssh/id_dsa.pub 文件复制到那个机器上的~/.ssh/authorized_keys文件中。
4. 如果你运行的是GNOME，跳到第15.3.4.4 节。如果你没在运行X 窗口系统，跳到第15.3.4.5 节。

15.3.4.3. 为版本1.3 和1.5 生成DSA 钥匙对

使用下面的步骤来生成用于SSH 协议版本1 的RSA 钥匙对。如果你只在使用DSA 的系统间连接，则不需要RSA 版本1.3 或RSA 版本1.5 钥匙对。

1. 要生成RSA （版本1.3 和1.5 协议）钥匙对，在shell 提示下键入下列命令：
   ```
   ssh-keygen -t rsa1
   ```
   接受默认的位置（~/.ssh/identity）。输入和你的帐号口令不同的口令句。再输入一次来确认。

   公钥被写入~/.ssh/identity.pub。密钥被写入~/.ssh/identity。不要把你的密钥出示给任何人。
2. 使用chmod 755 ~/.ssh 和chmod 644 ~/.ssh/identity.pub 命令改变你的.ssh 目录和密钥的许可权限。
3. 把~/.ssh/identity.pub 的内容复制到你想连接的机器中的~/.ssh/authorized_keys 文件中。如果文件~/.ssh/authorized_keys 不存在，你可以把~/.ssh/identity.pub 文件复制到远程机器上的~/.ssh/authorized_keys 文件中。
4. 如果你运行的是GNOME，跳到第15.3.4.4 节。如果你没在运行GNOME，跳到第15.3.4.5 节。

15.3.4.4. 在GNOME 中配置ssh-agent

ssh-agent 工具可以用来保存你的口令句，因此你不必在每次引发ssh 或scp 连接时都输入口令。如果你在使用GNOME，openssh-askpass-gnome 工具可以用来在你登录到GNOME 时提示你输入口令句，并把它一直保留到你从GNOME 中注销之时。你不必为本次GNOME 会话中任何ssh 或scp 连接输入口令或口令句。如果你不打算使用GNOME，请参阅第15.3.4.5 节。

要在GNOME 会话中保存口令句，遵循下列步骤：

1. 你需要安装openssh-askpass-gnome 软件包；你可以使用rpm -q openssh-askpass-gnome 命令来判定该软件包是否已被安装。如果它没有被安装，从你的Red Hat Linux 光盘集合、Red Hat FTP 镜像站点、或使用Red Hat 网络来安装它。
2. 点击「主菜单」（在面板上）=> 「首选项」 => 「更多首选项」 => 「会话」。然后点击「启动程序」标签。点击「增加」，在「启动命令」文本字段内输入**/usr/bin/ssh-add**。把它的优先级设为比任何现存命令都高的数字以确保它最后才执行。ssh-add 的优先级数字最好是70 或更高。优先级数字越高，优先级越低。如果你列出了其它程序，该程序的优先级应该最低。点击「关闭」来退出该程序。
3. 注销后再登录进GNOME；换一句话说，重新启动X 服务器。在GNOME 启动后，一个提示你输入口令句的对话框就会出现。输入要求的口令句。如果你把DSA 和RSA 两者都配置了，你会被提示两者都输入。从现在起，你就不会被ssh、scp 或sftp 提示输入口令了。

15.3.4.5. 配置ssh-agent

ssh-agent 可以用来储存你的口令句，因此你在每次使用ssh 或scp 连接时就不必总是输入它。如果你不在运行X 窗口系统，则在shell 提示中遵循这些步骤。如果你在运行GNOME，但是不想配置它来在你登录时提示你输入口令（参阅第15.3.4.4 节），这个过程可以在类似xterm 的终端窗口中进行。如果你在运行X 却不是GNOME，这个过程可以在终端中进行。可是，你的口令只能在该终端窗口中被记住，它不是全局设置。

1. 在shell 提示下，键入下面的命令：
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
2. 然后，键入下面的命令：
   ```
   ssh-add
   ```
   接着，输入你的口令。如果你配置了不止一个钥匙对，你会被提示输入每个口令。
3. 当你注销后，口令句就会被忘记。你必须在每次登录到虚拟控制台或打开终端窗口时都执行这两条命令。

15.4. 其它资料

OpenSSH 和OpenSSL 工程处于不断地开发中，因此关于它们的最新信息通常位于它们的官方网站中。OpenSSH 和OpenSSL 工具的说明书（man）页也是个获取详细信息的好地方。

15.4.1. 安装了的文档

- ssh、scp、sftp、sshd 和ssh-keygen 的说明书（man）页— 关于它们的说明书页包括如何使用这些命令的信息，以及所有能与它们一起使用的参数。

15.4.2. 有用的网站

- http://www.openssh.com — OpenSSH FAQ 网页、错误报告、邮件列表、工程宗旨、以及关于安全功能的更技术性的解释。
- http://www.openssl.org — OpenSSL FAQ 网页、邮件列表、以及对于工程宗旨的描述。
- http://www.freessh.org — 用于其它平台的SSH 客户软件。

16. 网络文件系统（NFS）

网络文件系统（NFS）是一种在网络上的机器间共享文件的方法，文件就如同位于客户的本地硬盘驱动器上一样。Red Hat Linux 既可以是NFS 服务器也可以是NFS 客户，这意味着它可以把文件系统导出给其它系统，也可以挂载从其它机器上导入的文件系统。

16.1. 为什么使用NFS?

NFS 对于在同一网络上的多个用户间共享目录很有用途。譬如，一组致力于同一工程项目的用户可以通过使用NFS 文件系统（通常被称作NFS 共享）中的一个挂载为/myproject 的共享目录来存取该工程项目的文件。要存取共享的文件，用户进入各自机器上的/myproject 目录。这种方法既不用输入口令又不用记忆特殊命令，就仿佛该目录位于用户的本地机器上一样。

16.2. 挂载NFS 文件系统

使用mount 命令来挂载另一个机器上的NFS 文件系统：

```
mount shadowman.example.com:/misc/export /misc/local
```


警告

本地机器上的挂载点目录（以上例子中的/mnt/local）必须存在。

在这项命令中，shadowman.example.com 是NFS 文件服务器的主机名；/misc/export 是shadowman 要导出的文件系统；/misc/local 是该文件系统在本地机器上的挂载位置。mount 命令运行之后（而且如果客户具有来自shadowman.example.com NFS 服务器的正确权限的话），客户用户可以执行ls /misc/local 命令来显示shadowman.example.com 上的/misc/export 目录中的文件列表。

16.2.1. 使用/etc/fstab 来挂载NFS 文件系统

要挂载其它机器上的NFS 共享的另一种方法是在/etc/fstab 文件中添加一行。这一行中必须声明NFS 服务器的主机名，要导出的目录，以及要挂载NFS 共享的本地机器目录。你必须是根用户才能修改/etc/fstab 文件。

/etc/fstab 中每行的一般语法如下所示：

```
server:/usr/local/pub  /pub  nfs  rsize=8192,wsize=8192,timeo=14,intr
```

挂载点/pub 在客户机器上必须存在。在客户系统的/etc/fstab 文件中把这一行添加完毕后，在shell 提示下键入命令mount /pub，以及将会从服务器中挂载的挂载点/pub。

16.2.2. 使用autofs 来挂载NFS 文件系统

挂载NFS 共享的第三种方法是使用autofs。autofs 使用automount 守护进程来管理你的挂载点，它只在文件系统被访问时才动态地挂载它们。

autofs 咨询主映射配置文件/etc/auto.master 来决定要定义哪些挂载点。然后，它使用适用于各个挂载点的参数来启动automount 进程。主映射配置中的每一行都定义一个挂载点，一个分开的映射文件定义在该挂载点下要挂载的文件系统。譬如，/etc/auto.misc 文件可能会定义/misc 目录中的挂载点；这种关系在/etc/auto.master 文件中会被定义。

auto.master 文件中的每个项目都有三个字段。第一个字段是挂载点。第二个字段是映射文件的位置，第三个字段可选。第三个字段可以包括超时数值之类的信息。

譬如，要在你的机器上的/misc/myproject 挂载点上挂载远程机器penguin.example.net 上的/project52 目录，在auto.master 文件中添加以下行：

```
/misc  /etc/auto.misc --timeout 60
```

在/etc/auto.misc 文件中添加以下行：

```
myproject -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

/etc/auto.misc 中的第一个字段是/misc 子目录的名称。该目录被automount 动态地创建。它不应该在客户机器上实际存在。第二个字段包括挂载选项，如：rw 代表读写访问权。第三个字段是要导出的NFS 的位置，包括主机名和目录。

注记

目录/misc 在本地文件系统中必须存在。在本地文件系统的/misc 目录中不应该有子目录。

autofs 是一种服务。要启动这项服务，在shell 提示下，键入以下命令：

```
/sbin/service autofs restart
```

要查看活跃的挂载点，在shell 提示下键入以下命令：

```
/sbin/service autofs status
```

如果你在autofs 运行时修改了/etc/auto.master 配置文件，你必须在shell 提示下键入以下命令来通知automount 守护进程重新载入配置文件：

```
/sbin/service autofs reload
```

若想了解如何配置autofs 以便在引导时启动，请参阅第14章 中关于管理服务的信息。

16.3. 导出NFS 文件系统

从NFS 服务器中共享文件又称导出目录。**NFS** 服务器配置工具可以用来把系统配置成NFS 服务器。

要使用**NFS** 服务器配置工具，你必须运行X 窗口系统，具备根特权，并且安装了redhat-config-nfs RPM 软件包。要启动这个程序，点击面板上的「主菜单」 => 「系统设置」 => 「服务器设置」 => 「**NFS** 服务器」，或键入redhat-config-nfs 命令。

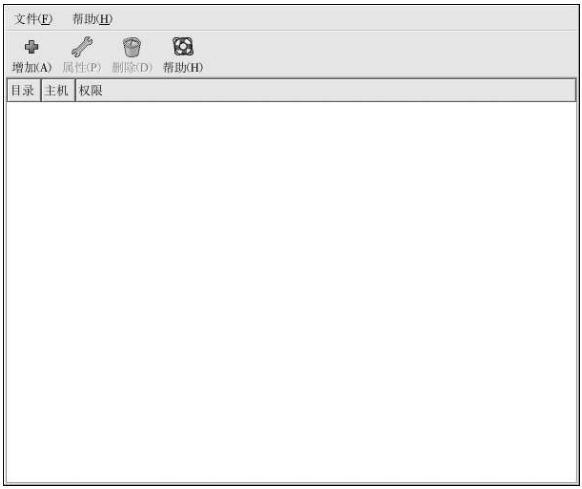


图**16-1. NFS** 服务器配置工具

要添加NFS 共享，点击「添加」按钮。如图16-2所示的对话框会出现。

「基本」活页标签要求以下信息：

- 「目录」 — 指定要共享的目录，如`/tmp`。
- 「主机」 — 指定要共享目录的主机。请参阅第16.3.2 节来获取对格式的解释。
- 「基本权限」 — 指定目录应该有只读权限还是读写权限。

图**16-2.** 添加共享

「常规选项」活页标签允许你配置以下选项：

- 「允许来自高于**1024** 的端口的连接」 — 在号码小于1024 的端口上启动的服务必须以根用户身份启动。选择这个选项来允许根用户以外的用户来启动NFS 服务。该选项和`insecure` 相对应。
- 「允许不安全的文件锁定」 — 不需要锁定请求。该选项和`insecure_locks` 相对应。

- 「禁用子树检查」 — 如果某文件系统的子目录被导出，但是整个文件系统没有被导出，服务器会检查所请求的文件是否在导出的子目录中。这种检查叫做子树检查（*subtree checking*）。选择这个选项来禁用子树检查。如果整个文件系统被导出，选择禁用子树检查可以提高传输率。该选项和no_subtree_check 相对应。
- 「按要求同步写操作」 — 默认被启用，该选项不允许服务器在请求被写入磁盘前回复这些请求。该选项和sync 相对应。如果它没有被选择，async 选项会被使用。
  - 「立即强制同步写操作」 — 不推迟写入磁盘的操作。该选项和no_wdelay 相对应。

「用户访问」活页标签允许你配置以下选项：

- 「把远程根用户当作本地根用户」 — 按照默认设置，根用户的用户ID 和组群ID 都是0。根权限压缩（Root squashing）把用户ID 0 和组群ID 0 映射为匿名的用户和组群ID，因此客户上的根用户就不会在NFS 服务器上具备根特权。如果这个选项被选，根用户就不会被映射为匿名用户，客户上的根用户就会对导出的目录拥有根特权。选择这个选项会大大降低系统的安全性。除非绝对必要，请不要选择它。该选项和no_root_squash 相对应。
- 「把所有客户用户当作匿名用户」 — 如果该选项被选，所有用户和组群ID 都会被映射为匿名用户。该选项和all_squash 相对应。
  - 「为匿名用户指定本地用户**ID**」 — 如果「把所有客户用户当作匿名用户」被选，这个选项会让你为匿名用户指定一个用户ID。该选项和corresponds to anonuid 相对应。
  - 「为匿名用户指定本地组群**ID**」 — 如果「把所有客户用户当作匿名用户」被选，这个选项会让你为匿名用户指定一个组群ID。该选项和corresponds to anongid 相对应。

要编辑NFS 共享，从列表中选择它，然后点击「属性」按钮。要删除某个现存NFS 共享，从列表中选择它，然后点击「删除」按钮。

点击了「确定」来从列表中添加、编辑、或删除某个NFS 共享后，改变就会立即生效— 服务器守护进程被重新启动，原有的配置文件被保存为/etc/exports.bak。新的配置文件被写入/etc/exports。

NFS 服务器配置工具直接读写/etc/exports 配置文件。因此，这个文件在使用该工具后可以被手工修改；手工修改了该文件后也可以使用这个工具（假定手工修改时使用了正确的语法）。

16.3.1. 命令行配置

如果你更喜欢使用文本编辑器来编辑配置文件或者你没有安装X 窗口系统，你可以直接修改配置文件。

/etc/exports 文件控制NFS 服务器要导出哪些目录。它的格式如下：

```
directory hostname(options)
```

唯一需要指定的选项是sync 和async 之一（建议使用sync is recommended）。如果指定了sync，服务器在请求所做的改变被写入磁盘之前就不会回复这些请求。

例如：

```
/misc/export  speedy.example.com(sync)
```

会允许来自speedy.example.com 的用户使用默认的只读权限来挂载/misc/export，但是：

```
/misc/export  speedy.example.com(rw,sync)
```

将会允许来自speedy.example.com 的用户使用读写权限来挂载/misc/export。

请参阅第16.3.2 节来获取关于主机名格式的解释。

请参阅《*Red Hat Linux* 参考指南》来获取可以被指定的选项的列表。


小心

请谨慎处理/etc/exports 文件中的空格。如果主机名和括号内的选项之间没有空格，这些选项就只应用于这个主机名。如果在主机名和选项之间有空格，这些选项就是全局应用的。例如，请仔细查看以下行：

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

第一行给来自speedy.example.com 的用户以读写权限并拒绝所有其他用户。第二行给来自speedy.example.com 的用户以只读权限（默认设置），并给予所有其他用户以读写权限。

在你每次改变/etc/exports 的时候，你必须把改变通知给NFS 守护进程，或使用以下命令来重新载入配置文件：

```
/sbin/service nfs reload
```

16.3.2. 主机名格式

主机可以使用以下格式：

- 单个机器— 一个全限定域名（能够被服务器解析的），主机名（能够被服务器解析的），或IP 地址。
- 使用通配符指定的一系列机器— 使用“*”或“?”字符来指定字符串匹配。通配符不能被用在IP 地址中；如果逆向DNS 查寻失败了，通配符可能碰巧会奏效。当你在全限定域名中指定通配符时，点（.）不包括在通配符的匹配项目内。例如：*.example.com 包括one.example.com，但不包括one.two.example.com.
- IP 网络— 使用*a.b.c.d/z*，这里的*a.b.c.d* 是网络，*z* 是子网掩码中的位数（如192.168.0.0/24）。另一种可以接受的格式是*a.b.c.d/netmask*，这里的*a.b.c.d* 是网络，*netmask* 是子网掩码（如192.168.100.8/255.255.255.0）。
- Netgroups — 格式为*@group-name*，这里的*group-name* 是NIS netgroup 的名称。

16.3.3. 启动和停止服务器

在导出NFS 文件系统的服务器上，nfs 服务必须在运行。

使用以下命令来查看NFS 守护进程的状态：

```
/sbin/service nfs status
```

使用以下命令来启动NFS 守护进程：

```
/sbin/service nfs start
```

使用以下命令来停止NFS 守护进程：

```
/sbin/service nfs stop
```

要在引导时启动nfs 服务，使用以下命令：

```
/sbin/chkconfig --level 345 nfs on
```

你还可以使用chkconfig、**ntsysv** 或服务配置工具来配置要在引导时启动哪些服务。详情请参阅第14章。

16.4. 其它资料

本章讨论了使用NFS 的基本知识。要获得更详尽的信息，请参阅下列资料。

16.4.1. 安装了的文档

- nfsd、mountd、exports、auto.master、和autofs（在说明书的第5 和第8 节）的说明书（man）页— 这些说明书页向你说明了NFS 和autofs 配置文件的正确语法。

16.4.2. 有用的网站

- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — 来自Linux 文档计划的*Linux NFS-HOWTO*。

16.4.3. 相关书籍

- *Managing NFS and NIS Services*，作者：Hal Stern；O’Reilly & Associates, Inc.

17. Samba

Samba 使用SMB 协议通过网络连接来共享文件和打印机. 支持该协议的操作系统包括Microsoft Windows（通过它的**Network Neighborhood**）、OS/2、和Linux。

17.1. 为什么使用Samba?

如果你的网络中既有Windows 机器又有Linux 机器，Samba 就会发挥作用。Samba 会允许文件和打印机被你的网络中的所有系统共享。如果你只打算在Red Hat Linux 机器间共享文件，请参阅第16章。如果你只打算在Red Hat Linux 机器间共享打印机，请参阅第27章。

17.2. 配置Samba 服务器

默认的配置文件（`/etc/samba/smb.conf`）允许用户作为Samba 共享来查看他们的Red Hat Linux 主目录。它还把为Red Hat Linux 配置的打印机作为Samba 共享打印机来共享。换一句话说，你可以在你的Red Hat Linux 系统上连接打印机，然后从网络上的Windows 机器来打印。

17.2.1. 图形化配置

要使用图形化界面来配置Samba，使用**Samba** 服务器配置工具。要使用命令行来配置，请跳到第17.2.2 节。

Samba 服务器配置工具是用来管理Samba 共享、用户、以及基本服务器设置的图形化界面。它修改`/etc/samba/` 目录中的配置文件。没有使用该程序进行的改变都会被保留。

要使用该程序，你必须在运行X 窗口系统，具备根特权，并且安装了`redhat-config-samba` RPM 软件包。要从桌面启动**Samba** 服务器配置工具，点击面板上的「主菜单」 => 「系统设置」 => 「服务器设置」 => 「**Samba** 服务器」，或在shell 提示（如XTerm 或GNOME 终端）下键入`redhat-config-samba` 命令。

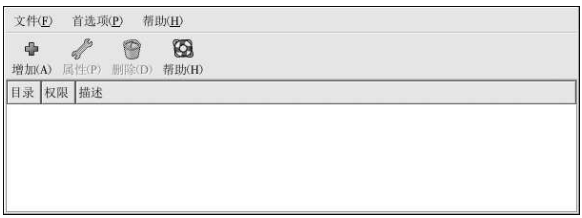


图**17-1. Samba** 服务器配置工具

注记

Samba 服务器配置工具不显示允许用户在Samba 服务器上查看他们自己的主目录的共享打印机或默认文件段。

17.2.1.1. 配置服务器设置

配置Samba 服务器的第一步是配置服务器的基本设置和几个安全选项。启动了应用程序后，选择「首选项」 => 「服务器设置」。「基本」活页标签如图17-2所示。

图**17-2.** 配置基本服务器设置

在「基本」标签上，指定计算机应在的工作组以及对计算机的简短描述。它们与`smb.conf` 中的`workgroup` 和`server string` 选项相对应。

图**17-3.** 配置安全服务器设置

「安全」标签包含以下选项：

- 「验证模式」 — 它和`security` 选项相对应。选择以下验证模式中的一种。
  - 「域」 — Samba 服务器依赖于Windows NT 主要或备份域控制器来校验用户。服务器把用户名和口令传递给控制器，然后等待它们被返回。在「验证服务器」字段中指定主要或备份域控制器的NetBIOS 名称。

    「加密口令」选项如果被选，它必须被设置为「是」。
  - 「服务器」 — Samba 服务器试图通过把用户名和口令组合传递给另一个Samba 服务器来校验它们。如果它无法校验，服务器会试图使用用户验证模式来校验它们。在「验证服务器」字段中指定另一个Samba 服务器的NetBIOS 名称。
  - 「共享」 — Samba 用户不必为每个Samba 服务器都输入用户名和口令组合。它们在试图连接Samba 服务器上的指定共享时才会被提示输入用户名和口令。
  - 「用户」 — （默认）Samba 用户必须为每个Samba 服务器提供一个有效的用户名和口令。如果你想让「**Windows** 用户名」选项生效，选择这个选项。详情请参阅第17.2.1.2 节。

- 「加密口令」— （默认值为「是」）如果用户从Windows 98、带有服务包的Windows NT 4.0、或其它最近版本的Microsoft Windows 中连接，该选项必须被启用。口令在服务器和客户间使用加密格式而非可被截取的纯文本格式传输。它和`encrypted passwords` 选项相对应。关于加密Samba 口令的详情，请参阅第17.2.3 节。
- 「来宾账号」— 当用户或来宾用户要登录入Samba 服务器时，他们必须被映射到服务器上的有效用户。选择系统上的现存用户名之一作为来宾Samba 账号。当用户使用来宾账号登录入Samba 服务器，他们拥有和这个用户相同的特权。该选项和`guest account` 选项相对应。

点击了「确定」后，所做改变会被写入配置文件，守护进程会被重新启动；因此改变会立即生效。

17.2.1.2. 管理Samba 用户

Samba 服务器配置工具要求在添加Samba 用户之前，在充当Samba 服务器的Red Hat Linux 系统上必须存在一个活跃的现存用户账号。Samba 用户和这个现存的Red Hat Linux 用户账号相关联。

图**17-4.** 管理**Samba** 用户

要添加Samba 用户，选择「首选项」 => 「**Samba** 用户」，然后点击「添加用户」按钮。在「创建新**Samba** 用户」窗口中的本地系统上的现存用户列表中选择「**Unix** 用户名」。

如果用户在Windows 机器上有一个不同的用户名，并将从Windows 机器上登录入Samba 服务器，请在「**Windows** 用户名」字段中指定Windows 用户名。「服务器设置」首选项的「安全」活页上的「验证模式」必须被设置为「用户」才能是这个选项生效。

你还需要为Samba 用户配置一个「**Samba** 口令」，并再键入一次来确认这个口令。即便你选择了为Samba 使用加密口令，仍建议你为所有用户设置的Samba 口令不同于他们的Red Hat Linux 系统口令。

要编辑某个现存用户，从列表中选择它，然后点击「编辑用户」。要删除某个现存的Samba 用户，选择这个用户，然后点击「删除用户」按钮。删除Samba 用户不会删除相关的Red Hat Linux 用户账号。

点击了「确定」按钮后，用户就会被立即修改。

17.2.1.3. 添加共享

图17-5. 添加共享

要添加共享，点击「添加」按钮。「基本」活页标签配置以下选项：

- 「目录」 — 通过Samba 共享的目录。这个目录必须存在。
- 「描述」 — 对共享的简短描述。
- 「基本权限」 — 用户应该只能够读取共享目录中的文件还是应该能够读写共享目录中的文件。

在「访问」活页标签上，选择是否要只允许指定的用户来访问共享还是允许所有Samba 用户来访问共享。如果你选择了要允许指定用户访问，从可用的Samba 用户列表中选择这些用户。

点击了「确定」按钮后，共享就会立即被添加。

17.2.2. 命令行配置

Samba 使用`/etc/samba/smb.conf` 作为它的配置文件。如果你改变了这个配置文件，这个改变直到你使用`service smb restart` 命令重启Samba 守护进程后才会生效。

要指定Windows 工作组和对它的简短描述，编辑`smb.conf` 文件中的以下几行：

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

把*WORKGROUPNAME* 换成你的机器所属的Windows 工作组名。*BRIEF COMMENT ABOUT SERVER* 是可选的，它被用作关于Samba 系统的Windows 注释。

要在你的Linux 系统上创建Samba 共享目录，在`smb.conf` 文件中添加以下几行（根据你和你的系统需要修改了该文件之后）：

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

上面的例子允许用户tfox 和carole 从Samba 客户中读写Samba 服务器上的目录`/home/share`。

17.2.3. 加密口令

在Red Hat Linux 9 中，加密口令被默认启用，因为它更安全。如果加密口令没有被使用，纯文本口令就会被使用，它能够被别人使用网络分组嗅探器来截取。建议你使用加密口令。

Microsoft SMB 协议最初使用纯文本口令。然而，带有服务包3 或更高的Windows NT 4.0、Windows 98、Windows 2000、Windows ME、以及Windows XP 要求加密的Samba 口令。要在Red Hat Linux 系统和运行以上Windows 操作系统的系统间使用Samba，你可以编辑Windows 注册器来使用纯文本口令过配置你的Linux 系统的Samba 来使用加密口令。如果你选择要修改你的注册器，你必须为你的全部Windows 机器这么做— 这很冒险，有可能导致进一步的冲突。为了更高的安全性，推荐你使用加密口令。

要在你的Red Hat Linux 系统上配置Samba 使用加密口令，遵循以下步骤：

1. 为Samba 创建一个单独的口令文件。要根据你的现存/etc/passwd 文件来创建，在shell 提示下键入以下命令：
   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   如果系统使用NIS，键入以下命令：
   ```
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   mksmbpasswd.sh 脚本和samba 软件包一起被安装在你的/usr/bin 目录上。
2. 改变Samba 口令文件的权限许可，因此只有根用户才有读写权限：
   ```
   chmod 600 /etc/samba/smbpasswd
   ```
3. 这个脚本不会把用户口令复制到新文件，Samba 用户账号在没有设置口令之前不会被激活。为了更高的安全性，建议你把用户的Samba 口令设置为不同于用户的Red Hat Linux 口令的口令。要设置每个Samba 用户的口令，使用以下命令（把*username* 替换为每个用户的用户名）：
   ```
   smbpasswd username
   ```
4. 加密口令必须在Samba 配置文件中被启用。在smb.conf 文件中，请确定以下行没有被注释掉：
   ```
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
   ```
5. 在shell 提示下键入service smb restart 来确定smb 服务被启动。
6. 如果你想让smb 服务被自动启动，使用**ntsysv**、chkconfig、或服务配置工具来在运行时间启用它。详情请参阅第14章。


窍门

阅读/usr/share/doc/samba-<*version*>/docs/htmldocs/ENCRYPTION.html 来进一步了解有关加密口令的信息。（把<*version*> 替换为你安装了的Samba 版本号码）。

当使用了passwd 命令后，pam_smbpass PAM 模块能够被用来同步用户的Samba 口令和他们的系统口令。如果用户启用了passwd 命令，他用来登录到Red Hat Linux 系统的口令以及他要连接Samba 共享所必须提供的口令就会被改变。

要启动这个功能，把以下行添加到/etc/pam.d/system-auth 的启动pam_cracklib.so 之下：

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

17.2.4. 启动和停止服务器

在通过Samba 共享目录的服务器上必须运行smb 服务。

使用以下命令来查看Samba 守护进程的状态：

```
/sbin/service smb status
```

使用以下命令来启动守护进程：

```
/sbin/service smb start
```

使用以下命令来停止守护进程：

```
/sbin/service smb stop
```

要在引导时启动smb 服务，使用以下命令：

```
/sbin/chkconfig --level 345 smb on
```

你还可以使用chkconfig、**ntsysv** 或服务配置工具来配置要在引导时启动的服务。详情请参阅第14章。

17.3. 连接Samba 共享

要从Microsoft Windows 机器上连接Linux Samba 共享，使用**Network Neighborhood** 或图形化文件管理器。

要从Linux 系统中连接Samba 共享，从shell 提示下，键入以下命令：

```
smbclient //hostname/sharename -U username
```

把*hostname* 替换为你想连接的Samba 服务器的主机名或IP 地址，把*sharename* 替换为你想浏览的共享目录的名称，把*username* 替换成系统的Samba 用户名。输入正确的口令或按[Enter] 键（若不要求该用户的口令）。

如果你看到了smb:\> 提示，你就已成功地登录了。登录后，键入**help** 来获得一个命令列表。如果你想浏览你的主目录的内容，把*sharename* 替换成你的用户名。如果每有使用-U 选项，当前用户的用户名就会被传递给Samba。

要退出smbclient，在smb:\> 提示下键入**exit**。

你还可以使用**Nautilus** 来查看你的网络上的可用Samba 共享。选择面板上的「主菜单」 => 「网络服务器」来查看你的网络上的Samba 工作组的列表。你还可以在Nautilus 的「位置：」栏里键入**smb:** 来查看工作组。

如图17-6所示，在网络上每个可用SMB 工作组旁边都会出现一个图标。

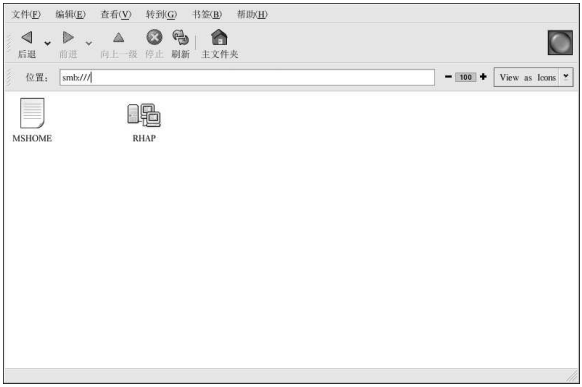


图**17-6. Nautilus** 中的**SMB** 工作组

双击工作组图标之一来查看哪个工作组内的计算机的列表。

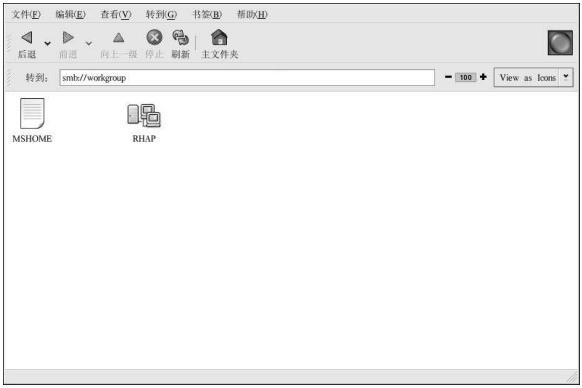


图**17-7. Nautilus** 中的**SMB** 机器

如你在图17-7中所见，工作组内每个机器都有一个图标。双击某个图标来查看该机器上的Samba 共享。如果需要用户名和口令组合，你会被提示输入它们。

你也可以在「位置：」栏内使用以下语法（把*user*、*password*、*servername*、和*sharename* 替换成相应值）来指定用户名和口令的组合：

```
smb://user:password@servername/sharename/
```

17.4. 其它资料

对于这里没有涉及到的配置选项，请参阅以下资料。

17.4.1. 安装了的文档

- `smb.conf` 的说明书页（man）— 解释该如何配置Samba 配置文件
- `smbd` 的说明书页（man）—描述Samba 守护进程的工作原理
- `/usr/share/doc/samba-<version-number>/docs/` — 包括在`samba` 软件包中的HTML 和文本帮助文件

17.4.2. 有用的网站

- http://www.samba.org — Samba 网页，包含许多关于邮件列表和GUI 界面列表信息等的有用文档。

redhat.

18. 动态主机配置协议（DHCP）

动态主机配置协议（DHCP）是用来自动给客户机器分配TCP/IP 信息的网络协议。每个DHCP 客户都连接到中央位置的DHCP 服务器，该服务器会返回包括IP 地址、网关和DNS 服务器信息的客户网络配置。

18.1. 为什么使用DHCP

DHCP 在快速发送客户网络配置方面很有用场。当配置客户系统时，管理员可以选择DHCP，并不必输入IP 地址、子网掩码、网关、或DNS 服务器。客户从DHCP 服务器中检索这些信息。DHCP 在管理员想改变大量系统的IP 地址时也大有用途。与其重新配置所有系统，管理员只需编辑服务器上的一个DHCP 配置文件即可获得新IP 地址集合。如果某机构的DNS 服务器改变了，这种改变只需在DHCP 服务器上而不必在DHCP 客户上进行。一旦客户的网络被重新启动（或客户重新引导系统），改变就会生效。

除此之外，如果便携电脑或任何类型的可移计算机被配置使用DHCP，只要每个办公室都有一个允许它联网的DHCP 服务器，它就可以不必重新配置而在办公室间自由移动。

18.2. 配置DHCP 服务器

你可以使用配置文件`/etc/dhcpd.conf` 来配置DHCP 服务器。

DHCP 还使用`/var/lib/dhcp/dhcpd.leases` 文件来贮存客户租期数据库。详情请参阅第18.2.2 节。

18.2.1. 配置文件

配置DHCP 服务器的第一步是创建贮存客户网络信息的配置文件。全局选项可以为所有客户声明，可选选项可以为每个客户系统声明。

该配置文件可以使用任何附加的制表符或空行来进行简单格式化。关键字是区分大小写的，起首为井号（#）的行是注释。

目前实现了两种DNS 更新方案— 特殊DNS 更新模式和过渡性DHCP-DNS 互动草图更新模式。如果这两种模式被接受为IETF 标准进程的一部分，就会出现第三个模式— 标准DNS 更新方法。DHCP 服务器必须配置使用这两种当前方案中的一种。版本3.0b2pl11 以及更早的版本使用特殊模式；不过，这种模式已经过时。如果你想保留相同的行为方式，在配置文件的开头添加以下一行：

```
ddns-update-style ad-hoc;
```

要使用推荐的模式，在配置文件的开头添加以下一行：

```
ddns-update-style interim;
```

请阅读`dhcpd.conf` 的说明书（man）页来获得有关不同模式的细节。

配置文件中有两类陈述：

- 参数— 表明如何执行任务，是否要执行任务，或将哪些网络配置选项发送给客户。
- 声明— 描述网络的布局；描述客户；提供客户的地址；或把一组参数应用到一组声明中。

某些参数必须以option 关键字开头，它们也被称为选项。选项配置DHCP 的可选选项；而参数配置的是必选的或控制DHCP 服务器行为的值。

在使用大括号（{ }）的部分之前声明的参数（包括选项）通常被当做全局参数。全局参数应用位于其下的所有部分。


重要

如果你改变了配置文件，这些改变在你使用service dhcpd restart 命令来重新启动DHCP 守护进程之后才会生效。

在例18-1中，routers、subnet-mask、domain-name、domain-name-servers 和time-offset选项被用于所有在它们下面声明的host 声明中。

如例18-1所示，你可以声明subnet。你必须为你的网络中的每一个子网包括一个subnet 声明，否则，DHCP 服务器可能无法启动。

在这个例子中，子网中的每个DHCP 客户都带有全局选项，并且声明了range。客户被分配给range 之内的IP 地址。

```
subnet 192.168.1.0 netmask 255.255.255.0 {
   option routers        192.168.1.254;
   option subnet-mask      255.255.255.0;

   option domain-name      "example.com";
   option domain-name-servers   192.168.1.1;

   option time-offset      -18000;  # Eastern Standard Time

 range 192.168.1.10 192.168.1.100;
}
```

例**18-1.** 子网声明

所有共享同一物理网络的子网应该在shared-network 声明之内声明，如例18-2所示。在shared-network 之内，但在被包围起来的subnet 声明之外的参数被当做全局参数。shared-network 的名称应该是对网络有描述性的标题，例如，使用test-lab 来描述所有处于实验室（test lab）环境中的子网。

```
shared-network name {
  option domain-name      "test.redhat.com";
  option domain-name-servers   ns1.redhat.com, ns2.redhat.com;
  option routers        192.168.1.254;
  more parameters for EXAMPLE shared-network
  subnet 192.168.1.0 netmask 255.255.255.0 {
    parameters for subnet
    range 192.168.1.1 192.168.1.31;
  }
  subnet 192.168.1.32 netmask 255.255.255.0 {
    parameters for subnet
    range 192.168.1.33 192.168.1.63;
  }
}
```

例**18-2.** 共享网络声明

如例18-3中所演示，group 声明可以用来把全局参数应用到一组声明中。你可以组合共享的网络、子网、主机或其它组群。

```
group {
  option routers        192.168.1.254;
  option subnet-mask      255.255.255.0;

  option domain-name      "example.com";
  option domain-name-servers    192.168.1.1;

  option time-offset      -18000;   # Eastern Standard Time

  host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
  }

  host raleigh {
    option host-name "raleigh.example.com";
    hardware ethernet 00:A1:DD:74:C3:F2;
    fixed-address 192.168.1.6;
  }
}
```

例**18-3.** 组群声明

要配置将动态IP 地址租给子网内系统的DHCP 服务器，用你的数值来修改例18-4。它为客户声明一个默认租期、最长租期、以及网络配置值。范例中把range 192.168.1.10 和192.168.1.100 之间的IP 地址分配给客户。

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.100;
}
```

例**18-4.** 范围参数

要根据网卡的MAC 地址给客户分配IP 地址，使用host 声明内的hardware ethernet 参数。如例18-5中所演示，host apex 声明表明：网卡的MAC 地址为00:A0:78:8E:9E:AA 的系统所分配的IP 地址将一直是192.168.1.4。

注意，你还可以使用可选的参数host-name 来为客户分配主机名。

```
host apex {
 option host-name "apex.example.com";
 hardware ethernet 00:A0:78:8E:9E:AA;
 fixed-address 192.168.1.4;
}
```

例18-5. 使用DHCP 的静态IP 地址


窍门

你可以使用Red Hat Linux 9 的配置文件范例作为样板，然后在其上添加你自己定制的配置选项。使用下面的命令把它复制到正确的位置里：

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

（这里的<version-number> 是你使用的DHCP 版本）。

要获取选项陈述及其作用的完整列表，请参阅dhcp-options 的说明书（man）页。

18.2.2. 租期数据库

在DHCP 服务器上，/var/lib/dhcp/dhcpd.leases 文件中存放着DHCP 的客户租期数据库。该文件不应该被手工修改。每个新近分配的IP 地址的DHCP 租期信息都会自动储存在租期数据库中。该信息包括租期的长度；IP 地址被分配的对象；租期的开始和终止日期；以及用来检索租期的网卡的MAC 地址。

租期数据库中所用的时间是格林威治标准时间（GMT），不是本地时间。

租期数据库不时被重建，因此它不算太大。首先，所有已知的租期会被储存到一个临时的租期数据库中，dhcpd.leases 文件被重命名为dhcpd.leases~，然后，临时租期数据库被写入dhcpd.leases 文件。

在租期数据库被重命名为备份文件，新文件被写入之前，DHCP 守护进程有可能被杀死，系统也有可能会崩溃。如果发生了这种情况，启动服务所需的dhcpd.leases 文件就不会存在。这时，请不要创建新租期文件。因为这样做会丢失所有原有的旧租期文件，从而导致更多问题。正确的办法是把dhcpd.leases~ 备份文件重命名为dhcpd.leases，然后再启动守护进程。

18.2.3. 启动和停止服务器


重要

在你首次启动DHCP 服务器之时，除非系统上存在dhcpd.leases 文件，服务器将无法被启动。如果这个文件不存在的话，使用touch /var/lib/dhcp/dhcpd.leases 命令来创建一个。

要启动DHCP 服务，使用/sbin/service dhcpd start 命令。要停止DHCP 服务器，使用/sbin/service dhcpd stop 命令。如果你想让守护进程在引导时自动启动，请参阅第14章中关于如何管理服务的信息。

如果你的系统连接了不止一个网络界面，但是你只想让DHCP 服务器启动其中之一，你可以配置DHCP 服务器只在那个设备上启动。在/etc/sysconfig/dhcpd 中，把界面的名称添加到DHCPDARGS 的列表中：

```
# Command line options here
DHCPDARGS=eth0
```

如果你有一个带有两个网卡的防火墙机器，这种方法就会大派用场。一个网卡可以被配置成DHCP客户来从互联网上检索IP地址；另一个网卡可以被用作防火墙之后的内部网络的DHCP服务器。仅指定连接到内部网络的网卡使系统更加安全，因为用户无法通过互联网来连接它的守护进程。

其它可在`/etc/sysconfig/dhcpd`中指定的命令行选项包括：

- `-p <portnum>` — 指定dhcpd应该监听的udp端口号码。默认值为67。DHCP服务器在比指定的udp端口大一位的端口号码上把回应传输给DHCP客户。譬如，如果你接受了默认的端口67，服务器在端口67上监听请求，然后在端口68上回应客户。如果你在此处指定了一个端口号码来使用DHCP转发代理，你所指定的DHCP转发代理的监听端口也必须是同一端口。详情请参阅第18.2.4节。
- `-f` — 把守护进程作为前台进程运行。这在调试时最常用。
- `-d` — 把DCHP服务器守护进程记录到标准错误描述器中。这在调试时最常用。如果它没有指定，日志将被写入`/var/log/messages`。
- `-cf filename` — 指定配置文件的位置。默认位置是`/etc/dhcpd.conf`。
- `-lf filename` — 指定租期数据库文件的位置。如果租期数据库文件已存在，在DHCP服务器每次启动时使用同一个文件至关重要。强烈建议你只在无关紧要的机器上为调试目的才使用该选项。默认的位置是`/var/lib/dhcp/dhcpd.leases`.
- `-q` — 在启动该守护进程时，不要显示整篇版权信息。

18.2.4. DHCP 转发代理

DHCP的转发代理（`dhcrelay`）允许你把无DHCP服务器的子网内的DHCP和BOOTP请求转发给其它子网内的一个或多个DHCP服务器。

当某个DHCP客户请求信息时，DHCP转发代理把该请求转发给DHCP转发代理启动时所指定的一列DHCP服务器。当某个DHCP服务器返回一个回应时，该回应被广播或单播给发送最初请求的网络。

除非使用`INTERFACES`指令在`/etc/sysconfig/dhcrelay`文件中指定了接口，DHCP转发代理监听所有接口上的DHCP请求。

要启动DHCP转发代理，使用`service dhcrelay start`命令。

18.3. 配置DHCP客户

配置DHCP客户的第一步是确定内核能够识别网卡。多数网卡会在安装过程中被识别，系统会为该卡配置恰当的内核模块。如果你在安装后安装了一张网卡，**Kudzu** [1] 应该会识别它，并提示你为它配置相应的内核模块。请确定查看Red Hat Linux的硬件兼容列表，它位于http://hardware.redhat.com/hcl/。如果网卡不是由安装程序或**Kudzu**配置的，而且你知道要为它载入哪个内核模块，那么请参阅第31章中关于载入内核模块的细节。

要手工配置DHCP客户，你需要修改`/etc/sysconfig/network`文件来启用联网；并修改`/etc/sysconfig/network-scripts`目录中每个网络设备的配置文件。在该目录中，每个设备都有一个叫做`ifcfg-eth0`的配置文件，这里的`eth0`是网络设备的名称。

`/etc/sysconfig/network`文件应该包含以下行：

```
NETWORKING=yes
```

1. **Kudzu**是在系统引导时运行的硬件探测工具，它用来判定系统上增加或移除了哪些硬件。

你的这个文件中可能有更多信息，但是如果你想在引导时启动联网，NETWORKING 变量必须被设为yes。

/etc/sysconfig/network-scripts/ifcfg-eth0 文件应该包含以下几行：

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

每个你想配置使用DHCP 的设备都需要一个配置文件。

如果你首选图形化界面来配置DHCP 客户，请参阅第12章 来获取关于使用网络管理工具来配置网络接口使用DHCP 的详情。

18.4. 其它资料

要获取这里没有涉及的配置选项的信息，请参考下列资料。

18.4.1. 安装了的文档

- dhcpd 的说明书（man）页— 描述DHCP 守护进程的运行原理
- dhcpd.conf 的说明书（man）页— 解释如何配置DHCP 配置文件；包括一些例子
- dhcpd.leases 的说明书（man）页— 解释如何配置DHCP 租期文件；包括一些例子
- dhcp-options 的说明书（man）页— 解释在dhcpd.conf 中声明DHCP 选项的语法；包括一些例子
- dhcrelay 的说明书（man）页— 解释DHCP 转发代理和它的配置选项

19. Apache HTTP 服务器配置

在Red Hat Linux 8.0 中，Apache HTTP 服务器被更新到版本2.0，它使用不同的配置选项。从Red Hat Linux 7.3 开始，RPM 软件包也被重新命名为`httpd`。如果你想手工地迁移现存的配置文件，请参阅`/usr/share/doc/httpd-<ver>/migration.html` 或《*Red Hat Linux* 参考指南》中的迁移向导。

如果你在以前的Red Hat Linux 版本中使用**HTTP** 配置工具配置了Apache HTTP 服务器，然后执行升级，你可以使用这个应用程序来把配置文件迁移到版本2.0 的新格式。启动**HTTP** 配置工具，改变配置，然后保存。所保存的配置文件就会与版本2.0 兼容。

HTTP 配置工具允许你为Apache HTTP 服务器配置`/etc/httpd/conf/httpd.conf` 配置文件。它不使用旧的`srm.conf` 或`access.conf` 配置文件；把它们留为空白。你可以通过图形化界面来配置指令，例如虚拟主机、记录属性和最大数量连接等。

只有包括在Red Hat Linux 中的模块可以使用**HTTP** 配置工具来配置。如果你安装了额外的模块，它们不能使用这个工具来安装。

你需要安装`httpd` 和`redhat-config-httpd` RPM 软件包才能使用**HTTP** 配置工具。它还需要X 窗口系统和根权限。要启动这个程序，点击「主菜单」 => 「系统设置」 => 「服务器设置」 => 「**HTTP** 服务器」，或在shell（例如，XTerm 或GNOME 终端）提示中键入`redhat-config-httpd` 命令。


小心

如果你想使用这个工具，请不要手工编辑`/etc/httpd/conf/httpd.conf` 配置文件。**HTTP** 配置工具在你保存改变并退出程序后自动生成这个文件。如果你想添加**HTTP** 配置工具中没有的额外模块或配置选项，你也不能使用这个工具。

使用**HTTP** 配置工具来配置Apache HTTP 服务器的一般步骤如下所述：

1. 在「主」标签下配置基本设置。
2. 点击「虚拟主机」标签来配置默认设置。
3. 在「虚拟主机」标签下，配置默认的虚拟主机。
4. 如果你想为不止一个URL 或虚拟主机提供服务，则添加额外的虚拟主机。
5. 在「服务器」标签下配置服务器设置。
6. 在「性能微调」标签下配置连接设置。
7. 把所有必要的文件复制到`DocumentRoot` 和`cgi-bin` 目录中。
8. 退出程序并保存你的设置。

19.1. 基本设置

使用「主」标签来配置基本服务器设置。

图**19-1.** 基本设置

在「服务器名称」文本字段中输入你有权使用的完整域名。该选项和`httpd.conf` 中的`ServerName` 指令相对应。`ServerName` 指令设置万维网服务器的主机名。它用来创建URL 的重导向。如果你没有定义服务器名称，万维网服务器会试图从系统中的IP 地址来解析它。服务器名称不一定非要是它的IP 地址。譬如，你可能想把你的服务器名称设为www.example.com，而你的服务器的实际DNS 名称却是foo.example.com.

在「网主电子邮件地址」文本字段中输入万维网服务器维护者的电子邮件地址。该选项和`httpd.conf` 中的`ServerAdmin` 指令相对应。如果你配置服务器的错误页要包含电子邮件地址，该地址将会被用户用来向服务器的管理员提交问题。默认的值是：root@localhost。

使用「可用地址」文本字段来定义服务器接受进入连接请求的端口。该选项和`httpd.conf` 中的`Listen` 指令相对应。Red Hat 默认配置Apache HTTP 服务器在端口80 上监听非安全万维网通讯。

点击「添加」按钮来定义接受请求的其它端口。一个如图19-2所示的窗口会出现。你可以选择「监听所有地址」选项来在定义的端口上监听所有IP 地址，也可以在「地址」字段中指定服务器会接受请求的地址。每个端口只能指定一个IP 地址。如果你想在同一端口号码上指定多个IP 地址，请为每个IP 地址分别创建条目。如果有可能，使用IP 地址而不是域名，这样会避免DNS 查寻失败。详情请参阅http://httpd.apache.org/docs-2.0/dns-caveats.html 中的*Issues Regarding DNS and Apache*。

在「地址」字段中输入星号（*）的效果和选择监听所有地址一样。点击「可用地址」框架中的「编辑」按钮和点击添加按钮所显示的窗口相同，只不过前者窗口中的字段值已被预设。要删除某一条目，选择它然后点击删除按钮。


窍门

如果你设置了服务器来监听1024 以下的端口，你必须是根用户才能启动它。对于1024 和以上的端口，`httpd` 可以被普通用户启动。

图19-2. 可用地址

19.2. 默认设置

定义了「服务器名称」、「网主电子邮件地址」、以及「可用地址」之后，点击「虚拟主机」标签，然后点击上面的「编辑默认设置」按钮。如图19-3所示的窗口会出现。在该窗口中为你的万维网服务器配置默认设置。如果你添加了一个虚拟主机，你为该虚拟主机配置的设置会被优先采用。对于虚拟主机内没有定义的指令，就会使用默认值。

19.2.1. 站点配置

「目录页搜索列表」和「错误页」中的默认值对于多数服务器都适用。如果你不能肯定这些设置，请不要修改它们。

图19-3. 站点配置

「目录页搜索列表」中列出的项目定义DirectoryIndex指令。DirectoryIndex是用户通过在目录名后指定正斜线（/）来请求目录索引时，由服务器提供的默认网页。

譬如，当某用户请求网页http://*www.example.com*/*this_directory*/ 时，他会得到DirectoryIndex网页（若存在），或由服务器生成的目录列表。服务器会试图寻

找DirectoryIndex 指令中列出的文件，并提供它找到的第一个文件。 如果它没找到任何文件，并且Options Indexes 为该目录设置，服务器就会生成并返回一个HTML 格式的列表，列出该目录中的子目录和文件。

使用「错误代号」这一节来配置Apache HTTP 服务器在出现错误和问题时把客户重导向给本地或外部URL。该选项和ErrorDocument 指令相对应。如果当客户试图连接Apache HTTP 服务器时出现了问题或错误，默认行动是显示「错误代号」列中的简单错误迅息。要取代默认配置，选择该错误代号，然后点击「编辑」按钮。选择「默认」来显示默认的简短错误迅息。选择「**URL**」来把客户重导向到一个外部URL，并在「位置」字段中輸入包括http:// 在内的URL。选择「文件」来把客户重导向到一个内部URL，并在万维网服务器的文档根下輸入文件的路径。位置必须以斜线（/）开头，并相对于文档根的位置。

譬如，要把404 “没有找到”错误代号重导向到你在404.html 文件中创建的网页，把404.html 复制到*DocumentRoot*/errors/404.html。在这个例子里，*DocumentRoot* 是你定义的文档根目录（默认为/var/www/html）。然后，选择「文件」作为「**404** - 没有找到」错误代号的行为，然后輸入/errors/404.html 作为「位置」。

从「默认错误页页脚」菜单中，你可以选择下列选项之一：

- 「显示页脚和电子邮件地址」 — 在所有错误页中显示默认页脚以及在ServerAdmin 指令中指定的网站维护者的电子邮件地址。关于配置ServerAdmin 指令的详细信息，请参阅第19.3.1.1 节。
- 「显示页脚」 — 在错误页的底部只显示默认的页脚。
- 「无页脚」 — 在错误页的底部不显示页脚。

19.2.2. 记录日志

服务器默认把传輸日志写入/var/log/httpd/access_log 文件，把错误日志写入/var/log/httpd/error_log 文件。

传輸日志包含一个所有对万维网服务器连接企图的列表。它记录试图连接的客户的IP 地址，试图连接的日期和时间，以及试图检索的万维网服务器上的文件。輸入要贮存该信息的路径和文件名。如果路径和文件名不以斜线（/）开头，该路径就是相对于配置的服务器根目录而言。该选项与TransferLog 指令相对应。

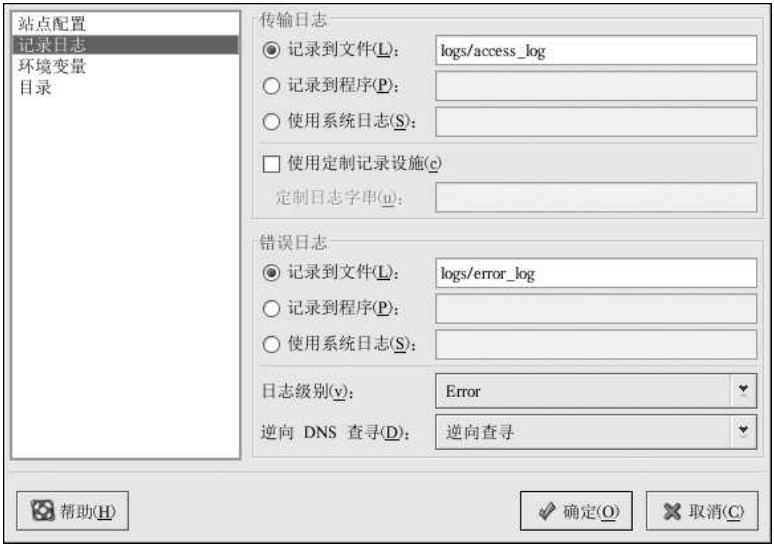


图**19-4.** 记录日志

你可以配置定制的日志格式。方法是，选择「使用定制记录设施」，然后在「定制日志字串」字段中输入定制的日志字符串。它配置`LogFormat`指令。请参阅 http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats 来获取该指令的格式信息。

错误日志包含所发生的服务器错误的列表。输入你要贮存该信息的路径和文件名。如果路径和文件名不以斜线（/）开头，该路径就是相对于配置的服务器根目录而言。该选项与`ErrorLog`指令相对应。

使用「日志级别」菜单来设置错误日志中错误讯息的详细程度。它可以被设置成（从最简略到最详细）emerg、alert、crit、error、warn、notice、info 或debug。该选项和`LogLevel`指令相对应。

「逆向**DNS** 查寻」菜单中选定的值定义`HostnameLookups`指令。选择「无逆向查寻」会关闭它。选择「逆向查寻」会启用它。选择「双重逆向查寻」把值设为双重。

如果你选择了「逆向查寻」，你的服务器会自动为每个从你的万维网服务器请求文档的连接解析IP地址。解析IP 地址意味着你的服务器会连接DNS 来寻找和某IP 地址相对应的主机名。

如果你选择了「双重逆向查寻」，你的服务器会执行双重逆向查寻DNS。换一句话说，执行了一次逆向查寻后，服务器会在结果上再执行一次正向查寻。在正向查寻中，至少应有一个IP 地址匹配第一次逆向查寻中的地址。

通常说来，你应该把该选项设为「无逆向查寻」，因为DNS 请求会给你的服务器增加载量，你的服务器的速度可能会减慢。如果你的服务非常繁忙，试图执行逆向查寻或双重逆向查寻的影响就会非常明显。

逆向查寻和双重逆向查寻从互联网整体上来说也是个问题。所有查寻主机名的个别连接加在一起的效应不容忽视。因此，为你自己的万维网服务器考虑，也为整个互联网的利益考虑，你应该把该选项设为「无逆向查寻」。

19.2.3. 环境变量

为了CGI 脚本或服务器端嵌入（SSI）页，有时有必要修改环境变量。Apache HTTP 服务器可以使用`mod_env`模块来配置被传递给CGI 脚本和SSI 页的环境变量。使用「环境变量」页来为该模块配置指令。

图**19-5.** 环境变量

使用「为**CGI** 脚本设置」部分来设置要传递给CGI 脚本和SSI 页的环境变量。譬如，要把环境变量MAXNUM 设为50，点击「为**CGI** 脚本设置」内的「添加」按钮，如图19-5所示。然后在「环境变量」文本字段内键入**MAXNUM**，在「设置的值」文本字段内键入**50**。点击「确定」。「为**CGI** 脚本设置」部分配置SetEnv 指令。

使用「传递给**CGI** 脚本」部分来在服务器首次启动CGI 脚本时传递环境变量值。要查看该环境变量，在shell 提示下键入env。点击「传递给**CGI** 脚本」内的「添加」按钮，在弹出的对话框中输入环境变量的名称。点击「确定」来把它添加到列表中。传递给**CGI** 脚本部分配置PassEnv 指令。

如果你想删除某个环境变量，因此它的值就不会传递给CGI 脚本和SSI 页，使用「为**CGI** 脚本取消设置」部分。点击其中的「添加」按钮，然后输入要取消设置的环境变量名称。它和UnsetEnv 指令相对应。

要编辑这些环境变量值，从列表中选择它，然后点击相应的「编辑」按钮。要从列表中删除任一项目，点击相应的「编辑」按钮。

要进一步了解Apache HTTP 服务器中的环境变量，请参考下面的网页：

```
http://httpd.apache.org/docs-2.0/env.html
```

19.2.4. 目录

使用「目录」页来为指定目录配置选项。它与<Directory> 指令相对应。

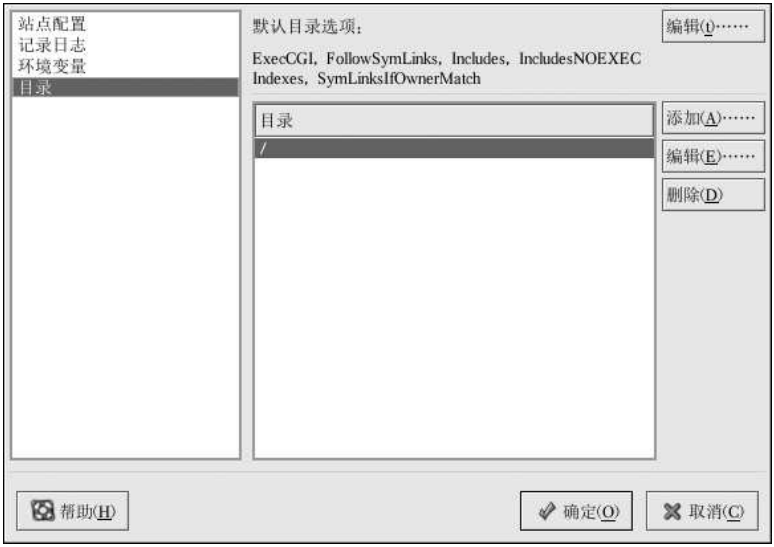


图19-6. 目录

点击右上角的「编辑」按钮来为所有没有在下面的「目录」列表中指定的目录配置「默认目录选项」。你选择的选项被列举在 <Directory> 指令内的 Options 指令中。你可以配置下列选项：

- **ExecCGI** — 允许执行CGI 脚本。如果该选项没有被选，CGI 脚本就不会被执行。
- **FollowSymLinks** — 允许追随符号链接。
- **Includes** — 允许服务器端嵌入。
- **IncludesNOEXEC** — 允许服务器端嵌入，但是在CGI 脚本中禁用#exec 和#include 命令。
- **Indexes** — 如果请求的目录中不存在DirectoryIndex（如index.html），则显示目录内容的格式化了的列表。
- **Multiview** — 支持content-negotiated multiviews；该选项被默认禁用。
- **SymLinksIfOwnerMatch** — 只有在目标文件或目录和链接的所有者相同时，才追随该符号链接。

要为指定目录指定选项，点击「目录」列表箱旁边的「添加」按钮。如图19-7 所示的窗口会出现。在窗口底部的「目录」文本字段内输入你要配置的目录。从右首的列表中选择选项，并用左首的选项配置Order 指令。Order 指令控制allow 和deny 指令被评价的顺序。在「允许主机来自」和「拒绝主机来自」文本字段内，你可以指定下列值之一：

- 允许所有主机— 键入**all** 来允许到所有主机的访问。
- 部分域名— 允许所有名称匹配指定字符串或以指定字符串结束的主机的访问。
- 完整IP 地址— 允许到特定IP 地址的访问。
- 子网— 如**192.168.1.0/255.255.255.0**
- 网络CIDR 具体规范— 如**10.3.0.0/16**

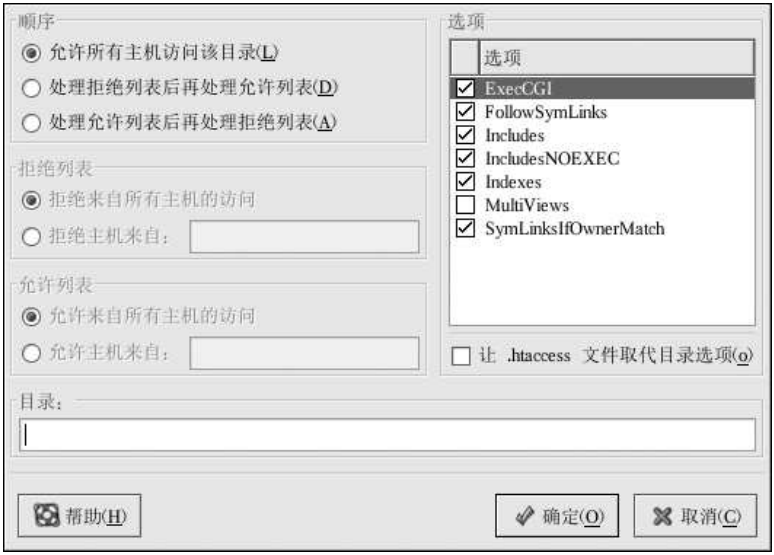


图**19-7.** 目录设置

如果你选择了「让**.htaccess** 文件取代目录选项」，`.htaccess` 文件中的配置指令就会被优先选用。

19.3. 虚拟主机设置

你可以使用**HTTP** 配置工具来配置虚拟主机。虚拟主机允许你为不同的IP 地址、主机名或同一机器上的不同端口运行不同的服务器。譬如，你可以在同一个万维网服务器上使用虚拟主机来运行http://www.example.com 和http://www.anotherexample.com 这两个网站。对于默认的虚拟主机和基于IP 的虚拟主机，该选项和<VirtualHost> 指令相对应；对于基于名称的虚拟主机，该选项和<NameVirtualHost> 指令相对应。

为某个虚拟主机设置的指令只应用于该虚拟主机。如果某指令使用「编辑默认设置」按钮为整个服务器全局设置，而虚拟主机设置中却没有被定义，那么默认设置就会被使用。譬如，你可以在「主」标签中定义「网主电子邮件地址」，而不必在每个虚拟主机中个别定义电子邮件地址。

HTTP 配置工具包括如图19-8所示的默认虚拟主机。

图**19-8.** 虚拟主机

http://httpd.apache.org/docs-2.0/vhosts/ 和在你的机器上安装的Apache HTTP 服务器文档提供了更多关于虚拟主机的信息。

19.3.1. 添加和编辑虚拟主机

要添加虚拟主机，点击「虚拟主机」标签，然后点击「添加」按钮。你还可以从列表中选择一个虚拟主机，然后点击「编辑」按钮来编辑它。

19.3.1.1. 常规选项

「常规选项」设置只应用于你正在配置的虚拟主机。在「虚拟主机名称」文本字段内设置虚拟主机的名称。该名称被**HTTP** 配置工具用来区别不同的虚拟主机。

把「文档根目录」的值设为包含该虚拟主机根文档（如index.html）的目录。该选项和 <VirtualHost> 指令内的DocumentRoot 指令相对应。在Red Hat Linux 7 之前，所提供的Apache HTTP 服务器使用/home/httpd/html 作为DocumentRoot。可是在Red Hat Linux 9 中，默认的DocumentRoot 是/var/www/html。

「网主电子邮件地址」和VirtualHost 内的ServerAdmin 指令相对应。如果你选择了要在错误页里显示页脚和电子邮件地址的话，该地址被用在错误页内的页脚上。

在「主机信息」部分，选择「默认虚拟主机」、「基于**IP** 的虚拟主机」、或「基于名称的虚拟主机」。

「默认虚拟主机」

- 你应该只配置一个默认虚拟主机（切记，默认只有一个设置）。当请求的IP 地址没有在另一个虚拟主机中确切列出时，默认的虚拟主机就会被使用。如果默认虚拟主机没有被定义，主服务器设置就会被使用。

「基于**IP** 的虚拟主机」

- 如果你选择了「基于**IP** 的虚拟主机」，一个根据服务器的IP 地址来配置<VirtualHost> 指令的屏幕就会出现。在「**IP** 地址」字段内指定IP 地址。要指定多于一个IP 地址，用空格把它们分开。要指定端口，使用*IP Address:Port* 格式。使用“:*”来为该IP 地址配置所有端口。在「服务器主机名」字段中指定虚拟主机的主机名。

「基于名称的虚拟主机」

‘ 如果你选择了「基于名称的虚拟主机」，一个根据服务器的主机名称来配置NameVirtualHost指令的窗口就会出现。在「**IP** 地址」字段内指定IP地址。要指定多于一个IP地址，用空格把它们分开。要指定端口，使用*IP Address:Port*格式。使用“:*”来为该IP地址配置所有端口。在「服务器主机名」字段中指定虚拟主机的主机名。在「别名」部分，点击「添加」来添加主机名的别名。添加别名会在NameVirtualHost指令内添加ServerAlias指令。

19.3.1.2. SSL

注记

你不可以在SSL中使用基于名称的虚拟主机，因为SSL握手（浏览器接受安全万维网服务器的证书时）发生在识别正确的基于名称的虚拟主机的HTTP请求之前。如果你想使用基于名称的虚拟主机，它们只能在你的非安全万维网服务器中使用。

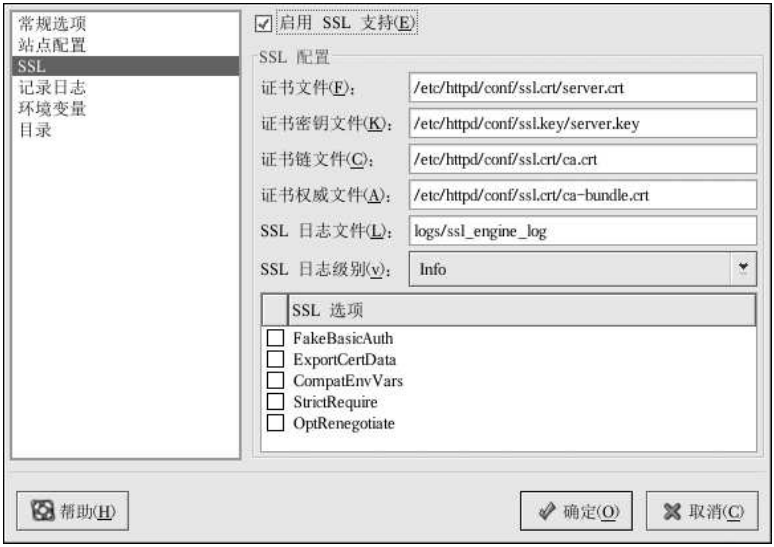


图**19-9. SSL** 支持

如果Apache HTTP服务器没有配置SSL支持，Apache HTTP服务器和它的客户之间的通信就不会被加密。这对于不包括私人或保密信息的网站来说是可行的。譬如，发行开源软件和文档的开源网站就不必使用安全通讯。然而，索求信用卡信息的电子商务网站就应该使用Apache SSL支持来加密通讯。启用Apache SSL支持会启用mod_ssl安全模块。要通过**HTTP** 配置工具来启用它，你必须在「主」标签=>「可用地址」中允许通过端口443的访问。详情请参阅第19.1节。然后，在「虚拟主机」标签中选择虚拟主机名，点击「编辑」按钮，从左首的菜单中选择「**SSL**」，并且选择「启用**SSL** 支持」选项，如图19-9所示。「**SSL** 配置」部分被预配置了虚构的数码证书。数码证书为你的安全万维网服务器提供验证，并向客户万维网浏览器表明安全服务器的身份。你必须

另行购买自己的数码证书。不要在你的网站使用Red Hat Linux 中提供的虚构证书。关于购买CA认可的数码证书的详情，请参阅第20章。

19.3.1.3. 其它虚拟主机选项

虚拟主机的「站点配置」、「环境变量」、以及「目录」选项和你点击了「编辑默认设置」按钮以后所见的指令相同。只不过，这里的配置仅用于你正在配置的个别虚拟主机。关于这些选项的细节，请参阅第19.2 节。

19.4. 服务器设置

「服务器」标签允许你配置基本的服务器设置。默认设置在多数情况下都是适用的。

图19-10. 服务器配置

「锁文件」的值和LockFile 指令相对应。在服务器使用USE_FCNTL_SERIALIZED_ACCEPT或USE_FLOCK_SERIALIZED_ACCEPT 编译时，该指令把路径设为锁文件所用的路径。它必须贮存在本地磁盘上。除非logs 目录位于NFS 共享上。如果事实如此，你应该把默认值改为本地磁盘上某处只能被根用户读取的目录。

「**PID** 文件」的值和PidFile 指令相对应。该指令设置服务器记录进程ID（PID）的文件。该文件应该只能够被根用户读取。多数情况下，你应该使用默认值。

「核心转储目录」的值和CoreDumpDirectory 指令相对应。Apache HTTP 服务器在转储核心前会试图转换到该目录中。默认值是ServerRoot。然而，如果运行服务器的用户所使用的身份没有到该目录的写权限，核心转储就无法被写入。如果你想把核心转储写入磁盘以用于调试目的，请把这个值改为能够被服务器的运行身份写入的目录。

「用户」的值和User 指令相对应。它设置服务器回答请求所用的userid。用户的设置决定服务器的访问权限。该用户所无法访问的文件，你的网站来宾也不能够访问。默认的User 是apache。

该用户应该仅拥有一定特权，因此它能够存取外部用户可以看见的文件。该用户还是所有被服务器生出的CGI 进程的所有者。它不应该被允许执行任何目的不是回答HTTP 请求的编码。

警告

除非你知道自己在做什么，不要把User 指令设为根用户。把User 设为根用户会为你的万维网服务器制造极大的安全漏洞。

在正常操作中，httpd 父进程首先以根用户身份来运行，但是，它会立即被交给apache 用户。服务器必须以根用户启动的原因是，它需要关联到1024 以下的端口。1024 以下的端口是为系统使用而保留的，因此只有根用户才有使用权。一旦服务器把自己连接到它的端口，它就会在接受任何连接请求前把进程交给apache 用户。

Group 的值与Group 指令相对应。Group 指令和User 指令很相似。它设置服务器回答请求所用的组群。默认组群也是apache。

19.5. 调整性能

点击「调整性能」标签来配置你想使用的服务器子进程的最大数量，以及客户连接方面的Apache HTTP 服务器选项。这些选项的默认设置在多数情况下是恰当的。改变这些设置会影响你的万维网服务器的整体性能。

图**19-11.** 调整性能

把「最多连接数量」设为服务器能够同时处理的客户请求的最多数量。服务器为每个连接创建一个httpd 子进程。进程数量达到最大限度后，直到某子进程结束，万维网服务器才能够接受新客户连接。如果不重新编译Apache，你为该选项设置的值将不能超高256。该选项与MaxClients 指令相对应。

「连接超时」定义你的服务器在通信时等候传输和回应的秒数。特别是，「连接超时」定义你的服务器在接收GET 请求时要等多久，在接收POST 或PUT 请求的TCP 包时要等多久，以及在回应TCP 包的ACK 之间要等多久。「连接超时」被默认设为300 秒，这在多数情况下都是适用的。该选项与TimeOut 指令相对应。

把「每次连接最多请求数量」设为每个持续连接所允许的最多请求次数。默认值为100，这应该在多数情况下都适用。该选项与MaxRequestsPerChild 指令相对应。

如果你选择了「允许每次连接可有无限制请求」选项，MaxKeepAliveRequests 指令的值就会是0，这会允许无限制的请求次数。

如果你取消选择了「允许持久性连接」选项，KeepAlive 指令就会被设为false。如果你选择了它，KeepAlive 指令就会被设为true，并且KeepAliveTimeout 指令的值会被设为「下次连接的

超时时间」中选定的值。该指令设置的超时秒数是你的服务器在回答了一项请求之后，关闭连接之前，等待下一个请求时会等候的秒数。一旦接收到请求，服务器就会改用「连接超时」中的值。

把「持续连接」设为一个较大的数值可能会导致服务器速度减慢，这要依据试图连接该服务器的用户数量而定。该选项的数值越大，等候前一个用户再次连接的服务器进程就越多。

19.6. 保存设置

如果你不想保存所做的Apache HTTP 服务器配置，点击**HTTP** 配置工具窗口右下角的「取消」按钮。你会被提示确认。如果你点击了「是」来确认该选择，你的设置就不会被保存。

如果你想保存你所做的Apache HTTP 服务器配置，点击**HTTP** 配置工具窗口右下角的「确定」按钮。一个对话框就会出现。如果你点击了「是」，你的设置就会被保存在`/etc/httpd/conf/httpd.conf` 中。切记，你的原有配置会被覆盖。

如果这是你第一次使用**HTTP** 配置工具，你会看到一个警告你配置文件已经被手工修改的对话框。如果**HTTP** 配置工具检测到`httpd.conf` 配置文件已被手工修改，它会把手工修改的文件保存为`/etc/httpd/conf/httpd.conf.bak`。


重要

保存设置之后，你必须使用`service httpd restart` 命令来重新启动`httpd` 守护进程。你必须是根用户才能执行该命令。

19.7. 其它资料

要进一步了解Apache HTTP 服务器，请参考下列资料。

19.7.1. 安装了的文档

- Apache HTTP 服务器文档— 如果你安装了`httpd-manual` 软件包，并且在运行Apache HTTP 服务器守护进程（`httpd`），你可以查看Apache HTTP 服务器的文档。打开一个万维网浏览器，然后在运行Apache HTTP 服务器的服务器上跳到URL：http://localhost。接下来，点击「文档」链接。
- `/usr/share/docs/httpd-`*`<version>`* — *Apache Migration HOWTO* 文档包含了从版本1.3 到版本2.0 的一系列改变以及如何手工迁移配置文件的信息。

19.7.2. 有用的网站

- http://www.apache.org — *The Apache Software Foundation*。
- http://httpd.apache.org/docs-2.0/ — Apache 软件基金会关于Apache HTTP 服务器版本2.0 的文档，包括*Apache HTTP 服务器Version 2.0 User's Guide*。
- http://localhost/manual/index.html — 在你的本地系统上启动了Apache HTTP 服务器服务器后，你可以使用该URL 来查看Apache HTTP 服务器版本2.0 的文档。
- http://www.redhat.com/support/resources/web_ftp/apache.html — Red Hat 的技术支持维护一个有用的Apache HTTP 服务器链接的列表。
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html —由Red Hat 编译的Red Hat Linux Apache Centralized Knowledgebase 。

19.7.3. 相关书籍

- *Apache: The Definitive Guide*，作者：Ben Laurie 和Peter Laurie；O'Reilly & Associates, Inc. 出版
- *Red Hat Linux* 参考指南; Red Hat, Inc. — 这本参考指南包括了从Apache HTTP 服务器版本1.3 手工迁移到Apache HTTP 服务器版本2.0 的说明，有关Apache HTTP 服务器指令的更详细信息，以及在Apache HTTP 服务器中添加模块的说明。

redhat.

20.

Apache HTTP 安全服务器配置

20.1. 介绍

本章提供了关于启用了mod_ssl安全模块来使用OpenSSL 库和工具包的Apache HTTP 服务器服务器的基本信息。Red Hat Linux 提供的这三个部件的组合在本章中将会被称为安全万维网服务器或安全服务器。

mod_ssl 模块是Apache HTTP 服务器的安全模块。mod_ssl 模块使用由OpenSSL 计划提供的工具来给Apache HTTP 服务器添加一项重要功能— 加密通信的能力。与之相反，使用常规HTTP，浏览器和万维网服务器间的通讯就会使用纯文本，它们在浏览器和服务器之间的路线上可能会被其它人截取并偷阅。

本章并不是这些程序的完全或唯一的文档。若你想获取关于某主题的更深入的文档，本章在合适的地方会为你指引途径。

本章将会向你显示如何安装这些程序。你还需要掌握生成密钥、证书请求、如何生成自我签名的证书、以及如何安装证书来用于你的安全服务器的必要步骤。

mod_ssl 配置文件位于/etc/httpd/conf.d/ssl.conf。要载入这个文件而使mod_ssl 能够工作，你必须在/etc/httpd/conf/httpd.conf 中包括Include conf.d/*.conf 这条声明。在Red Hat Linux 9中，该声明被默认包括在默认的Apache HTTP 服务器配置文件中。

20.2. 与安全相关的软件包概述

要启用安全服务器，你至少需要安装以下软件包：

httpd

- httpd 软件包包含httpd 守护进程和相关的工具、配置文件、图标、Apache HTTP 服务器模块、说明书（man）页和其它被Apache HTTP 服务器使用的文件。

mod_ssl

- mod_ssl 软件包包括mod_ssl 模块，它通过安全套接字层（SSL）和传输层安全（TLS）协议为Apache HTTP 服务器提供了强大的加密能力。

openssl

- openssl 软件包包含OpenSSL 工具包。OpenSSL 工具包实现SSL 和TLS 协议，还包括一个常规目的的加密库。

除此之外，其它包括在Red Hat Linux 中的软件包也可以提供一定程度的安全功能（但不是安全服务器运行所必需的）：

httpd-devel

- httpd-devel 软件包包含Apache HTTP 服务器的包含文件、头文件和APXS 工具程序。如果你打算载入额外的模块（不是该产品所提供的），你需要以上所有文件和程序。请参阅《*Red Hat Linux* 参考指南》 来获取关于使用Apache HTTP 服务器的DSO 功能来把模块载入安全服务器的详细信息。

  如果你不打算在Apache HTTP 服务器中载入额外模块，你不安装该软件包。

`httpd-manual`

- `httpd-manual` 软件包包含HTML 格式的Apache 计划的*Apache User's Guide* 说明指南。该指南还可在http://httpd.apache.org/docs-2.0/ 中找到。

OpenSSH 软件包

- The OpenSSH 软件包提供了一组用来在远程机器上登录和执行命令的OpenSSH 网络连接工具集合。OpenSSH 工具加密所有交通（包括口令），因此你可以避免被窃听，防范截取连接和其它对你的机器和远程机器间通信的攻击。

  `openssh` 软件包包括OpenSSH 客户程序和服务器都需要的核心文件。`openssh` 软件包还包括`scp`，它是`rcp`（用来在机器间复制文件）和`ftp`（用来在机器间传输文件）的安全替换。

  `openssh-askpass` 软件包支持对话框窗口的显示。该窗口在使用OpenSSH 代理时提示你输入口令。

  `openssh-askpass-gnome` 软件包可以在OpenSSH 程序提示你输入口令时和GNOME 桌面环境一起使用来显示图形化对话窗口。如果你运行的是GNOME，并使用OpenSSH 工具，你应该安装该软件包。

  `openssh-server` 软件包包括`sshd` 安全shell 守护进程和相关文件。安全shell 守护进程是OpenSSH 套件的服务器一方，如果你想允许SSH 客户连接到你的主机，你必须在主机上安装该软件包。

  `openssh-clients` 软件包包含进行加密SSH 服务器连接所需的客户程序，其中包括：`ssh`（`rsh` 的安全替换）；`sftp`（`ftp` 的安全替换，用来在机器间传输文件）；`slogin`（用于远程登录的`rlogin` 和通过Telnet 协议与另一主机通信的`telnet` 的安全替换）。

  关于OpenSSH 的详细信息，请参阅第15章、《*Red Hat Linux* 参考指南》、以及OpenSSH 的网站：http://www.openssh.com。

`openssl-devel`

- `openssl-devel` 软件包包含编译带有各类加密算式和协议支持的应用程序所需的静态库和包含文件。你只有在开发包括SSL 支持的应用程序时，才需要安装该软件包— 仅使用SSL 不必安装该软件包。

`stunnel`

- `stunnel` 软件包提供了Stunnel SSL 会绕程序。Stunnel 支持TCP 连接的SSL 加密，因此它可以为无SSL 的守护进程和协议（如POP、IMAP 和LDAP）提供加密，却不需对守护进程的编码做任何修改。

表20-1 显示了安全服务器软件包的摘要，并向你表明每个软件包对安全万维网服务安装是否必不可少。

软件包名称	是否可选可不选?
`httpd`	否
`mod_ssl`	否
`openssl`	否
`httpd-devel`	是
`httpd-manual`	是
`openssh`	是
`openssh-askpass`	是

软件包名称	是否可选可不选?
openssh-askpass-gnome	是
openssh-clients	是
openssh-server	是
openssl-devel	是
stunnel	是

表**20-1.** 安全软件包

20.3. 证书和安全概述

你的安全服务器使用安全套接字层（SSL）和（多数情况下）来自证书权威（CA）的数码证书的组合来提供安全性。SSL 处理浏览器和你的安全服务器间的加密通讯和互相验证。CA 认可的数码证书为你的安全服务器提供验证（CA 以它的名誉担保对你的机构组织身份的认证）。当你的浏览器使用SSL 加密通讯时，你会看到导航栏上的划一资源定位（URL）的开头有一个“https://”前缀。

加密依赖于钥匙的使用（你可以把它们当做数据格式的秘密编码和解码钥匙）。传统的或对称的加密术中，事务的两端都使用同一把钥匙，它们可以用这把钥匙来破译彼此的传输。在公共或非对称加密术中，有两把钥匙并存：公钥和密钥。某人或某机构把他们的密钥保密，只公布他们的公钥；使用密钥编码的数据只能用公钥才能解码。

要设置你的安全服务器，你将会使用公共加密术来创建公钥和密钥对。在多数情况下，你会向某CA 发送证书请求（包括你的公钥）、你的公司身份的证据、以及付款。CA 将会校验你的证书请求和身份，然后把你的安全万维网证书寄回给你。

安全服务器使用证书来向万维网浏览器标明身份。你可以生成你自己的证书（叫做“自签”证书），或者你可以从证书权威中获取证书。来自有声望的CA 的证书会担保与某一特定公司或机构相连的网站的身份。

另外，你也可以创建你自己的自签证书。然而请注意，自签证书不应该被用在多数生产环境中。自签证书不会被用户的浏览器自动接受— 浏览器将会征询用户是否要接受该证书并创建安全连接。请参阅第20.5 节来获取关于自签和CA 签名的证书区别的详细信息。

在你有了自签的证书或来自CA 的证书后，你需要把它安装在你的安全服务器上。

20.4. 使用已存钥匙和证书

如果你已有现存的钥匙和证书（例如，如果你要安装安全服务器来替换另一家公司的安全服务器产品），你可能将能够在安全服务器中使用你现存的钥匙和证书。在下面这两种情况下，你将无法使用现存的钥匙和证书：

- 如果你改变了你的*IP* 地址和域名 — 证书是向特定IP 地址和域名对颁发的。如果你改变了域名或IP 地址，你需要申请一份新证书。
- 如果你有一份来自*VeriSign* 的证书，但想改变服务器软件 — VeriSign 是使用较广泛的CA。如果你已有一份由于其它原因而获得的VeriSign 证书，你可能会考虑在你的新安全服务器中使用现有的VeriSign 证书，然而，你将不会被允许使用它。这是因为VeriSign 依据特定服务器软件和IP 地址/域名组合来颁发证书。

  如果你改变了以上任一参数（譬如，从前你使用了另一个安全服务器产品，现在你想使用这个安全服务器），你为从前的配置所获取的VeriSign 证书将无法在新配置中使用。你必须获取一份新证书。

如果你有可以使用的已存钥匙和证书，你将不必生成新钥匙或获取新证书。然而，你可能需要转移并更名包含钥匙和证书的文件。

把你的现存钥匙文件转移到：

```
/etc/httpd/conf/ssl.key/server.key
```

将你的现存证书文件转移到：

```
/etc/httpd/conf/ssl.crt/server.crt
```

在你转移了钥匙和证书之后，跳到第20.9 节。

如果你要升级Red Hat 安全万维网服务器，你的旧钥匙（`httpsd.key`）和证书（`httpsd.crt`）将会位于`/etc/httpd/conf/` 下。你将需要转移并重命名你的钥匙和证书，因此安全服务器才能使用它们。使用以下两个命令来转移并重命名钥匙和证书文件：

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

然后，使用下面的命令来启动安全服务器：

```
/sbin/service httpd start
```

要启动安全服务器，你会被提示輸入口令句。当你键入口令句后按[Enter] 键，服务器就会启动。

20.5. 证书类型

如果你从Red Hat Linux 提供的RPM 中安装了安全服务器，一个随机钥匙和测试证书就会被生成并放置在适当的目录中。然而，在你使用安全服务器之前，你需要生成你自己的钥匙并获取正确识别你的服务器的证书。

你需要钥匙和证书才能操作安全万维网服务— 这意味着你可以生成一个自签的证书或从某CA 处购买一份由CA 签名的证书。这两者间有什么区别呢？

由CA 签名的证书为你的服务器提供两项重要能力：

- 浏览器（通常）会自动识别证书，并且不必提示用户就能够允许开通安全连接。
- 当某CA 颁发了签名的证书，他们是在向浏览器担保提供网页的机构的身份。

如果你的安全服务器被广大公众所访问，你的安全服务器需要有CA 签名的证书，因此访问你的网站的用户可以信任该网站的确是声明拥有它的建构所拥有。在签发证书前，CA 校验申请证书的机构确实如他们所言。

多数支持SSL 的万维网浏览器有一个它们会自动接受证书的CA 列表。如果浏览器遇到一份来自列表之外的授权CA 的证书，浏览器会询问用户是否要接受连接。

你可以为你的安全服务器生成一份自签的证书，但是请留意，自签证书将不会提供和CA 签发的证书相同的功能。自签证书将不会被用户的浏览器自动识别，而且它将不会担保提供网站的机构的身份。由CA 签发的证书为安全服务器提供这两项重要的能力。如果你的安全服务器将会用在生产环境中，你可能会需要CA 签发的证书。

从CA 获取证书的手续非常简单。下面是对其步骤的简单描述：

1. 创建加密的公钥和密钥对。
2. 根据公钥创建证书请求。证书请求包括关于你的服务器和主持它的公司的信息。
3. 向某CA 发送证书请求，以及证明你的身份的文档。我们不能向你建议该选择哪个CA。你的决定可以建立在过去的经验上，或者你的朋友或同事的经验上，或者单从经济上考虑。

当你选定了一个CA 后，你需要遵循他们提供的说明来获取证书。

4. 当CA 对你的身份的真实性满意后，他们就会给你寄发一份数码证书。
5. 在你的安全服务器上安装该证书，然后开始处理安全事务。

不论你是从CA 处获取证书，还是使用自签的证书，第一个步骤都是生成钥匙。请参阅第20.6 节来获取生成钥匙的指示。

20.6. 生成钥匙

你必须是根用户才能生成钥匙。

首先，cd 到/etc/httpd/conf 目录中，使用下面的命令删除在安装中生成的假钥匙和证书：

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

其次，你需要生成你自己的随机钥匙。改换到/usr/share/ssl/certs 目录中，键入以下命令：

```
make genkey
```

你的系统会显示和以下输出相似的消息：

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

现在，你需要键入口令句。要获得最佳安全性，你的口令应至少包括八个字符，包括数字和标点，且不是词典中的现成词汇。另外请记住，你的口令是区分大小写的。

注记

你在每次启动安全服务器的时候都需要输入这个口令，因此请将它牢记在心。

重新键入口令来校验它是否正确。一旦你正确地键入了，一个包括你的钥匙，叫做>/etc/httpd/conf/ssl.key/server.key 的文件就会被创建。

注意，如果你不想在每次启动安全服务器的时候都输入口令，你将需要下面这两条命令，而不是make genkey 来创建钥匙。

使用下面的命令来创建你的钥匙：

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

然后使用这条命令来确定钥匙的权限被正确设置：

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

在你使用以上命令创建钥匙后，你将不需要使用口令句来启动安全服务器。


小心

在你的安全服务器中禁用口令功能是一种安全风险。我们不提倡你禁用安全服务器的口令功能。

不使用口令所造成的问题和主机的安全维护休戚相关。譬如，若有人危害了主机上的常规UNIX 安全系统，他就可以获取你的密钥（server.key 文件的内容）。该钥匙可以用来提供似乎是来自你的安全服务器的网页。

如果UNIX 安全系统在主机上被认真维护（及时安装操作系统的补丁和更新；不操作不必要的或冒险的服务等等），安全服务器的口令可能就不是很必要。然而，由于你的安全服务器应该没必要被频繁重新启动，输入口令所能带来的额外保险在多数情况下是值得一行的。

server.key 文件应该被系统的根用户拥有，不应该被其它用户访问。给该文件备份，将备份副本存放在安全之处。你需要备份的原因是，如果你在使用钥匙创建了证书请求后丢失了server.key 文件，你的证书就不会再生效，而CA 对此也爱莫能助。你只能再申请（并购买）一份新证书。

如果你打算从CA 处购买证书，请继续阅读第20.7 节。如果你打算生成自签的证书，请继续阅读第20.8 节。

20.7. 生成发送给CA 的证书请求

一旦你创建了钥匙，下一步就是生成证书请求，你需要把该请求发送给选中的CA。请确定你位于/usr/share/ssl/certs 目录，并键入下面的命令：

```
make certreq
```

你的系统会显示下列输出，然后还会请你输入口令句（除非你禁用了口令选项）：

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

键入你在生成钥匙时选择的口令。你的系统将会显示一些指示，然后向你询问一系列问题。你的输入会被包括在证书请求中。所显示的输出和示例回答，看起来和下面相似：

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

默认回答紧随在每项要求后面的括号内（[]）。例如，第一项要求的信息是证书要被用于的国家，如下所示：

```
Country Name (2 letter code) [GB]:
```

默认的输入出现在括号内，是**GB**。要接受默认值，只需按[Enter]，或填入你的国家的两个字母的代号。

你必须得键入剩下的值。这些输入都是不言而喻的，但是你需要遵从以下准则：

- 不要用地域或州省的缩写。用全称（如，St. Louis 应该被写成Saint Louis）。
- 如果你要把该CSR 寄发给CA，请确保在所有的字段内都提供了正确的信息，特别是`Organization Name`和`Common Name`这两项。CA 检查CSR 中提供的信息以判定你的机构是否对你所提供的`Common Name`负责。CA 将会拒绝包括他们认为无效的信息的CSR。
- 对于`Common Name`，请确定你键入了你的安全服务器的真实名称（有效的DNS 名称），而不是服务器的别名。
- `Email Address`应该是网主或系统管理员的电子邮件地址。
- 请避免@、#、&、！之类的特殊字符。某些CA 将会拒绝包含特殊字符的请求。因此，如果你的公司名称包含&，把它拼写为“and”而不使用“&”。
- 不要使用这两项附加属性：`A challenge password`和`An optional company name`。要不输入这些字段而继续，只需按[Enter]键来接受空白的默认值即可。

信息输入完毕后，一个叫做`/etc/httpd/conf/ssl.csr/server.csr`的文件就会被创建。该文件是你的证书请求，可以随时寄发给你的CA。

在你选定了CA 后，按照他们在网站提供的说明行事。这些说明会告诉你如何发送证书请求，你还需要哪些文档以及付款信息。

在你满足了CA 的要求后，他们就会给你寄发证书（通常通过电子邮件）。将它们寄发的证书保存为（或剪贴为）`/etc/httpd/conf/ssl.crt/server.crt`。请确定给该文件保留一份备份。

20.8. 创建自签的证书

你可以创建自签的证书。请注意，自签的证书将不会提供由CA 签发的证书所提供的安全担保。关于证书的详细信息，请参阅第20.5 节。

如果你想制作自签的证书，你首先需要按照第20.6 节中提供的指示来创建随机钥匙。一旦创建了钥匙，请确定你位于`/usr/share/ssl/certs`目录中，再键入下面的命令：

```
make testcert
```

你将会看到以下输出，你会被提示输入口令句（除非你生成了无口令的钥匙）：

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

输入口令句后（如果你创建了无口令的钥匙则没有提示），你会被要求输入更多信息。计算机的输出以及一组示例输入与以下的显示相仿（你需要为你的主机和机构提供正确的信息）：

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

提供了正确信息后，自签的证书就会在/etc/httpd/conf/ssl.crt/server.crt 中被创建。生成证书后，你需要使用以下命令来重新启动安全服务器：

```
/sbin/service httpd restart
```

20.9. 测试证书

要测试默认安装的测试证书、CA 签发的证书、以及自签的证书，把你的万维网服务器转到以下主页（把*server.example.com* 替换成你的域名）：

```
https://server.example.com
```

注记

注意http 后面的s。https: 前缀被用在安全HTTP 事务中。

如果你使用的是由知名CA 签发的证书，你的浏览器可能会自动接受该证书（不必提示你输入）并创建安全连接。你的浏览器不会自动识别测试或自签的证书，因为这些证书不是由CA 签发的。如果你没有使用来自CA 的证书，请遵循浏览器的指示来接受证书。

你的浏览器接受了证书后，你的安全服务器就会显示默认的主页。

20.10. 访问服务器

要访问你的安全服务器，使用和以下相似的URL：

```
https://server.example.com
```

你的非安全服务器可以使用和以下相似的URL 来访问：

```
http://server.example.com
```

安全万维网通讯的标准端口是端口443。非安全万维网通讯的标准端口是端口80。安全服务器默认配置对这两个端口都监听。因此，你不必在URL 中指定端口号码（端口号码会被假定）。

然而，如果你配置了你的服务器监听非标准的端口（除80 和443 之外的），你必须在每个URL 中指定旨在非标准端口上连接服务器的端口号码。

例如，你可能给你的服务器做了相应配置，因此你在端口12331 上运行一个非安全的虚拟主机。任何旨在连接该虚拟主机的URL 都必须在URL 中指定端口号码。下面的URL 例子会试图连接在端口12331 监听的非安全万维网服务器：

```
http://server.example.com:12331
```

20.11. 其它资料

有关Apache HTTP 服务器的额外参考资料请参阅第19.7 节。

20.11.1. 安装了的文档

- `mod_ssl documentation` — 在安装了`httpd-manual` 软件包并运行Apache HTTP 服务器的服务器上打开万维网浏览器，然后转到URL http://localhost/manual/mod/mod_ssl.html。

20.11.2. 有用的网站

- http://www.redhat.com/mailing-lists/ — 你可以在这个URL 上订阅redhat-secure-server 邮件列表。

  你还可以通过给`<redhat-secure-server-request@redhat.com>` 这个地址发送电子邮件，并在主题栏中包括*subscribe* 这个词来订阅redhat-secure-server 邮件列表。
- http://www.modssl.org — `mod_ssl` 网站是关于`mod_ssl` 的权威性信息。该网站具有丰富的文档资料，其中包括*User Manual*，位于http://www.modssl.org/docs。

20.11.3. 相关书籍

- *Apache: The Definitive Guide*，第二版，作者：Ben Laurie 和Peter Laurie；O’Reilly & Associates, Inc.

21. BIND 配置

本章假定你已经掌握了关于BIND和DNS的基本知识，因而在这里我们不会试图解释BIND和DNS的概念。本章向你解释如何使用**Bind**配置工具（`redhat-config-bind`）来配置基本的BIND服务器区块。**Bind**配置工具在每次你应用改变时创建`/etc/named.conf`配置文件和`/var/named`目录中的区块配置文件。

重要

不要编辑`/etc/named.conf`配置文件。**Bind**配置工具在你应用改变之后生成该文件。如果你想配置使用**Bind**配置工具无法配置的设置，请把它们添加到`/etc/named.custom`中。

Bind配置工具需要X窗口系统和根访问权。要启动**Bind**配置工具，点击面板上的「主菜单」 => 「系统设置」 => 「服务器设置」 => 「域名服务」，或在shell提示（如XTerm或GNOME终端）下键入`redhat-config-bind`命令。

图**21-1. Bind**配置工具

Bind配置工具把默认的区块目录配置成`/var/named`。所有指定的区块文件都是相对于该目录所言。**Bind**配置工具还包括对输入值的基本语法检查。譬如，如果一个合法的项目应该是IP地址，那么你便只被允许在文本区域中键入数字和点（.）字符。

Bind配置工具允许你添加一个正向主区，一个逆向主区，和一个从区。添加了这些区块后，你就可以从主窗口中编辑或删除它们，如图21-1所示。

添加、编辑、删除某区之后，你必须点击「保存」按钮或选择「文件」 => 「保存」来写入`/etc/named.conf`配置文件和`/var/named`目录中的每个区块文件。应用这些改变还会令named服务重新载入配置文件。选择「文件」 => 「退出」会在退出文件前保存所做改变。

21.1. 添加正向主区

要添加正向主区（又称首要主区），点击「新建」按钮，选择「正向主区块」，然后在「域名」文本区内输入主区的域名。

一个类似图21-2的新窗口会出现，其中包括以下选项：

- 「名称」 — 你在前一个窗口中输入的域名。
- 「文件名」 — DNS 数据库文件的文件名，相对于/var/named 而言。它被预设为后补了.zone 的域名。
- 「联系」 — 主区的主要电子邮件联系地址。
- 「主名称服务器**(SOA)**」 — 授权状态（SOA）记录。它指定最适合该域信息的名称服务器。
- 「序列号码」 — DNS 数据库文件的序列号码。在每次文件发生改变时，这个号码都应该向前递增，因此该区块的次名称服务器就能够检索到最新的数据。**Bind** 配置工具在每次配置发生改变的时候都会递增该号码。它还可以被手工递增，方法是点击「序列号码」值旁边的「设置」按钮。
- 「时间设置」 — 贮存在DNS 数据库文件中的「刷新」、「重试」、「过期」、和「至少」TTL（活跃时间）值。所有值都以秒为单位。
- 「记录」 — 添加、编辑、和删除关于「主机」、「别名」、和「名称服务器」之类的资源记录。

图**21-2.** 添加正向主区

「主名称服务器**(SOA)**」必须被指定，你必须点击「记录」部分的「添加」按钮来至少指定一个名称服务器记录。

配置了正向主区后，点击「确定」来返回到如图21-1所示的主窗口。从下拉菜单中，点击「保存」来写入/etc/named.conf 配置文件，以及/var/named 目录中所有单独的区块文件，并使守护进程重新载入配置文件。

该配置在/etc/named.conf 文件中创建了和以下相似的项目：

```
zone "forward.example.com" {
 type master;
 file "forward.example.com.zone";
};
```

它还创建了带有以下信息的/var/named/forward.example.com.zone 文件：

```
$TTL 86400
@   IN   SOA  ns.example.com. root.localhost (
          2 ; serial
          28800 ; refresh
          7200 ; retry
          604800 ; expire
          86400 ; ttl
          )


   IN   NS   192.168.1.1.
```

21.2. 添加逆向主区

要添加逆向主区，点击「新建」按钮并选择「逆向主区块」。输入你想配置的IP 地址范围的前三个八位组。譬如，如果你想配置的IP 地址范围是192.168.10.0/255.255.255.0，在「**IP** 地址（前**3** 个八位组）」文本区域内输入192.168.10。

一个如图21-3所示的新窗口就会出现，其中包括下列选项：

1. 「**IP** 地址」 — 你刚刚在前一个窗口内输入的前三个八位组。
2. 「逆向**IP** 地址」 — 不可编辑。根据输入的IP 地址预填的。
3. 「联系」 —主区的主要电子邮件联系地址。
4. 「文件名」 — /var/named 目录中DNS 数据库文件的名称。
5. 「主名称服务器**(SOA)**」 — 授权状态（SOA）记录。它指定最适合该域信息的名称服务器。
6. 「序列号码」 — DNS 数据库文件的序列号码。在每次文件发生改变时，这个号码都应该向前递增，因此该区块的次名称服务器就能够检索到最新的数据。**Bind** 配置工具在每次配置发生改变的时候都会递增该号码。它还可以被手工递增，方法是点击「序列号码」值旁边的「设置」按钮。
7. 「时间设置」 — 贮存在DNS 数据库文件中的「刷新」、「重试」、「过期」、和「至少」TTL（活跃时间）值。所有值都以秒为单位。
8. 「名称服务器」 — 为逆向主区添加、编辑、或删除名称服务器。至少需要一个名称服务器。
9. 「逆向地址表」 — 在逆向主区和它们的主机名内的IP 地址列表。譬如，对于逆向主区192.168.10，你可以在「逆向地址表」中添加192.168.10.1，以及主机名one.example.com.。主机名一定要以点（.）结束来表明它是主机的全名。

图**21-3.** 添加逆向主区

「主名称服务器**(SOA)**」必须被指定，你必须点击「记录」部分的「添加」按钮来至少指定一个名称服务器记录。

配置了逆向主区后，点击「确定」来返回到如图21-1所示的主窗口。从下拉菜单中，点击「保存」来写入`/etc/named.conf`配置文件，以及`/var/named`目录中所有单独的区块文件，并使守护进程重新载入配置文件。

该配置在`/etc/named.conf`文件中创建了和以下相似的项目：

```
zone "10.168.192.in-addr.arpa" {
    type master;
    file "10.168.192.in-addr.arpa.zone";
};
```

它还创建了带有以下信息的`/var/named/10.168.192.in-addr.arpa.zone`文件：

```
$TTL 86400
@   IN   SOA  ns.example.com. root.localhost (
           2 ; serial
           28800 ; refresh
           7200 ; retry
           604800 ; expire
           86400 ; ttk
           )


@   IN   NS   ns2.example.com.
```

```
1   IN   PTR  one.example.com.
2   IN   PTR  two.example.com.
```

21.3. 添加从区块

要添加从区块（又称次要主区），点击「新建」按钮并选择「从区块」。在「域名」文本区域内输入从区块的域名。

一个如图21-4所示的新窗口就会出现，其中包括下列选项：

- 「名称」 — 你在前一个窗口中输入的域名。
- 「主区块列表」 — 从区块从中检索数据的名称服务器。该值必须是有效的IP 地址。你只能在文本区域内输入数字和点（.）。
- 「文件名」 — /var/named 目录中DNS 数据库文件的名称。

图21-4. 添加从区块

配置了从区块后，点击「确定」来返回到如图21-1所示的主窗口。从下拉菜单中，点击「保存」来写入/etc/named.conf 配置文件，以及/var/named 目录中所有单独的区块文件，并使守护进程重新载入配置文件。

该配置在/etc/named.conf 文件中创建了和以下相似的项目：

```
zone "slave.example.com" {
    type slave;
    file "slave.example.com.zone";
    masters {
        1.2.3.4;
        };
};
```

配置文件/var/named/slave.example.com.zone 在named 服务从主区块服务器中下载区块数据时被创建。

22. 验证配置

当用户登录入Red Hat Linux 系统，其用户名和口令的组合必须被校验或验证（*authenticated*）以判定他是否为有效的活跃用户。有时，用于校验用户的信息位于本地系统；有时，系统把验证推延给远程系统上的用户数据库。

验证配置工具提供了配置NIS、LDAP、和Hesiod 来检索用户信息，以及把LDAP、Kerberos、和SMB 配置成验证协议的图形化界面。


注记

如果你在安装中或使用安全级别配置工具配置了中级或高级安全级别，或在**GNOME Lokkit** 程序中选择了高级或低级安全，包括NIS 和LDAP 在内的网络验证方法就不被允许穿过防火墙。

本章并不详细解释每一种不同的验证类型，而解释了如何使用验证配置工具来配置这些验证类型。

要从桌面上启动图形化版本的验证配置工具，选择面板上的「主菜单」 => 「系统设置」 => 「验证」，或在shell 提示下（如**XTerm** 或**GNOME** 终端）键入`authconfig-gtk` 命令。要启动基于文本的版本，在shell 提示下键入`authconfig` 命令。


重要

退出了验证程序后，改变会立即生效。

22.1. 用户信息

「用户信息」标签上有几个选项。要启用选项，点击它旁边的空白复选箱。要禁用选项，点击它旁边的复选箱来清空它。点击「确定」来退出程序并应用改变。

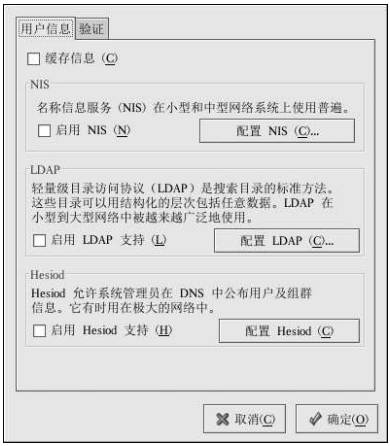


图**22-1.** 用户信息

以下的列表解释了每个选项所配置的项目：

- 「缓存用户信息」 — 选择该选项来启用名称服务缓存守护进程（nscd），并配置它在引导时启动。

  你必须安装了nscd 软件包才能使这个选项奏效。

- 「启用**NIS** 支持」 — 选择该选项来把系统配置成连接NIS 服务器来验证用户和口令的NIS 客户。点击「配置**NIS**」按钮来指定NIS 域和NIS 服务器。如果NIS 服务器没有被指定，守护进程会试图通过广播来寻找它。

  你必须安装了ypbind 软件包才能使这个选项奏效。如果启用了NIS 支持，portmap 和ypbind 服务会被启动，它们也会在引导时被启用。

- 「启用**LDAP** 支持」 — 选择这个选项来配置系统来通过LDAP 检索用户信息。点击「配置**LDAP**」按钮来指定「**LDAP** 搜索基准**DN**」和「**LDAP** 服务器」。如果「使用**TLS** 来加密连接」被选择，传输层安全就会被用来加密发送给LDAP 服务器的口令。

  你必须安装openldap-clients 软件包才能使这个选项奏效。

  关于LDAP 的更多信息，请参阅《*Red Hat Linux* 参考指南》。

- 「启用**Hesiod** 支持」 — 选择这个选项来配置系统来从远程Hesiod 数据库中检索信息，包括用户信息。

  你必须要安装hesiod 软件包。

22.2. 验证

「验证」标签允许你配置网络验证方法。要启用选项，点击它旁边的空白复选箱。要禁用选项，点击它旁边的复选箱来清空它。

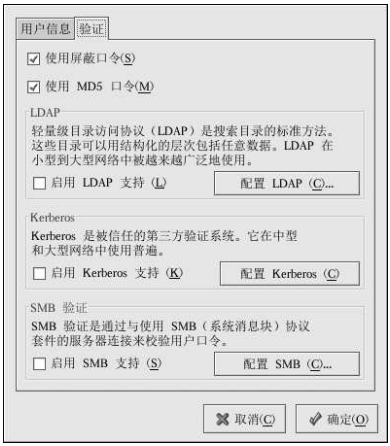


图**22-2.** 验证

以下解释了每个选项所配置的项目：

- 「使用屏蔽口令」 — 选择这个选项来在`/etc/shadow`文件中而不是`/etc/passwd`文件把口令贮存为屏蔽口令格式。屏蔽口令在安装中被默认启用，它也是我们极力推荐你用来增加系统安全性的措施。

  你必须安装了`shadow-utils`软件包才能使这个选项奏效。关于屏蔽口令的更多信息，请参阅《*Red Hat Linux* 参考指南》中的“用户和组群”这一章。

- 「使用**MD5** 口令」 — 选择这个选项来启用MD5 口令。它会允许长达256 个字符的口令而不同是通常的少于八个字符的口令。该选择在安装中被默认选择，它也是我们极力推荐你用来增加系统安全性的措施。

- 「启用**LDAP** 支持」 — 选择这个选项来让标准的启用PAM 的应用程序使用LDAP 来验证。点击「配置**LDAP**」按钮来指定以下信息：

  - 「使用**TLS** 来加密连接」 — 使用传输层安全来加密要发送给LDAP 服务器的口令。
  - 「**LDAP** 搜索基准**DN**」 — 通过它的识别名称（DN）来检索用户信息。
  - 「**LDAP** 服务器」 — 指定LDAP 服务器的IP 地址。

  你必须安装了`openldap-clients`软件包才能使这个选项奏效。关于LDAP 的详情请参阅《*Red Hat Linux* 参考指南》。

- 「启用**Kerberos** 支持」 — 选择这个选项来启用Kerberos 验证。点击「配置**Kerberos**」按钮来配置：

  - 「领域」 — 配置Kerberos 服务器的领域。领域是使用Kerberos 的网络，由一个或多个KDC，以及大量客户组成。
  - 「**KDC**」 — 定义密钥分发中心（KDC）。它是分发Kerberos 门票的机器。
  - 「管理服务器」 — 指定运行`kadmind`的管理服务器。

  你必须安装`krb5-libs`和`krb5-workstation`软件包才能使这个选项奏效。关于Kerberos 的详情请参阅《*Red Hat Linux* 参考指南》。

- 「启用**SMB** 支持」 — 该选项配置PAM 使用SMB 服务器来验证用户。点击「配置**SMB**」按钮来指定：

  - 「工作组」 — 指定要使用的SMB 工作组。

- 「域控制器」 — 指定要使用的SMB 域控制器。

22.3. 命令行版本

验证配置工具还能够作为没有界面的命令行工具来运行。命令行版本可以被用在配置脚本或kickstart 脚本中。验证选项在表22-1中被简略描述。

选项	描述
`--enableshadow`	启用屏蔽口令
`--disableshadow`	禁用屏蔽口令
`--enablemd5`	启用MD5 口令
`--disablemd5`	禁用MD5 口令
`--enablenis`	启用NIS
`--disablenis`	禁用NIS
`--nisdomain=<domain>`	指定NIS 域
`--nisserver=<server>`	指定NIS 服务器
`--enableldap`	为用户信息启用LDAP
`--disableldap`	为用户信息禁用LDAP
`--enableldaptls`	LDAP 启用TLS
`--disableldaptls`	LDAP 禁用TLS
`--enableldapauth`	验证启用LDAP
`--disableldapauth`	验证禁用LDAP
`--ldapserver=<server>`	指定LDAP 服务器
`--ldapbasedn=<dn>`	指定LDAP 基准DN
`--enablekrb5`	启用Kerberos
`--disablekrb5`	禁用Kerberos
`--krb5kdc=<kdc>`	指定Kerberos KDC
`--krb5adminserver=<server>`	指定Kerberos 管理服务器
`--krb5realm=<realm>`	指定Kerberos 领域
`--enablesmbauth`	启用SMB
`--disablesmbauth`	禁用SMB
`--smbworkgroup=<workgroup>`	指定SMB 工作组
`--smbservers=<server>`	指定SMB 服务器
`--enablehesiod`	启用Hesiod
`--disablehesiod`	禁用Hesiod
`--hesiodlhs=<lhs>`	指定Hesiod LHS

选项	描述
--hesiodrhs=<*rhs*>	指定Hesiod RHS
--enablecache	启用nscd
--disablecache	禁用nscd
--nostart	不要开始或停止portmap、ypbind 和nscd 服务，即便它们已经被配置
--kickstart	不要显示用户界面
--probe	探测和显示网络默认值

表**22-1.** 命令行选项

窍门

这些选项还可以在authconfig 的说明书（man）页或在shell 提示下键入authconfig --help 来找到。

23.

邮件传输代理（MTA）配置

邮件传输代理（*Mail Transport Agent*，*MTA*）是从Red Hat Linux 系统中发送邮件的必备程序。邮件用户代理（*Mail User Agent*，*MUA*），如**Evolution**、**Mozilla Mail**、**Mutt**，被用来阅读和编写电子邮件。当用户从MUA 中发送一份邮件，该邮件被送到MTA，然后MTA 把这份邮件发送给一系列MTA，直到它到达它的最终发送目标为止。

即便用户不打算从系统中发送电子邮件，有些自动化的任务或系统程序可能会使用`/bin/mail`命令来把包含日志消息的邮件发送给本地系统的根用户。

Red Hat Linux 9 提供了两个MTA：Sendmail 和Postfix。如果两者均安装了，`sendmail` 就是默认的MTA。邮件传输代理切换器 允许用户选择`sendmail` 或`postfix` 作为系统的默认MTA。

要使用基于文本的邮件传输代理切换器程序，你的系统上必须安装`redhat-switch-mail` RPM 软件包。如果你想使用图形化版本，则`redhat-switch-mail-gnome` 软件包也需要被安装。关于安装RPM 软件包的详情，请参阅第V 部分。

要启动邮件传输代理切换器，选择面板上的「主菜单」=>「系统工具」=>「更多系统工具」=>「邮件传输代理切换器」，或在shell 提示（如XTerm 或GNOME 终端）中键入`redhat-switch-mail`命令。

该程序会自动检测X 窗口系统是否在运行。如果它在运行，该程序就会在图形化模式中启动，如图23-1所示。如果没有检测到X，它就会在文本模式中启动。要强制邮件传输代理切换器 在文本模式下运行，使用`redhat-switch-mail-nox` 命令。

图**23-1.** 邮件传输代理切换器

如果你选择「确定」来改变MTA，被选中的邮件守护进程就会在引导时被启动，未被选中的邮件守护进程会被禁用，这样，它就不会在引导时被启用；被选中的邮件守护进程被启动，其它邮件守护进程被停止，这样，改变就会立即发生。

关于电子邮件协议和MTA 的详细资料，请参阅《*Red Hat Linux* 参考指南》。关于MUA 的详情，请参阅《*Red Hat Linux* 入门指南》。

IV. 系统配置

讨论了控制台访问以及如何从Red Hat Linux 系统上收集软件和硬件信息后，这一部分解释了常见的系统配置任务。

目录

24. 控制台访问

当普通用户（非根用户）在本地登录到计算机上，他们被授予两类特殊权限：

1. 他们可以运行某些通常无法运行的程序
2. 他们可以访问某些通常无法访问的文件（通常是用来访问磁盘、光盘等的特殊设备文件）

由于单个计算机有多个控制台，多位用户可以在同一时间内在计算机上本地登录，其中之一必定在访问这些文件的角逐中“获胜”。第一个在控制台登录的用户完全拥有那些文件。一旦第一个用户注销，下一个登录的用户就会拥有这些文件。

与之相反，每个在控制台登录的用户都被允许运行通常只限于根用户的程序来完成任务。如果X 在运行，这些行动可以被包括在图形化用户界面的菜单内。在该发行版本中，可从控制台访问的程序包括halt、poweroff、和reboot。

24.1. 禁用通过Ctrl-Alt-Del 关机

按照默认设置，/etc/inittab 文件指定你的系统可在控制台使用[Ctrl]-[Alt]-[Del] 键组合来关闭并重启系统。如果你想完全禁用这项能力，你需要把/etc/inittab 文件中下面一行变成注释，方法是在句前加一个井号（#）：

```
ca::ctrlaltdel:/sbin/shutdown-t3-rnow
```

另外，你可能只是想授予个别非根用户从控制台使用[Ctrl]-[Alt]-[Del] 来重启系统的权利。你可以通过下面的步骤来把该特权仅限定给某些用户使用：

1. 在上面显示的/etc/inittab 的那一行中添加-a 选项，如下所示：
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   -a 标志通知shutdown 命令去寻找/etc/shutdown.allow 文件，我们在下一步骤中将会创建该文件。
2. 在/etc 目录中创建一个叫做shutdown.allow 的文件。shutdown.allow 文件应该列出允许使用[Ctrl]-[Alt]-[Del] 来关闭系统的用户名。/etc/shutdown.allow 文件使用列表格式，每行列出一名用户，如下所示：
   ```
   stephen
   jack
   sophie
   ```

根据以上shutdown.allow 文件的例子，stephen、jack、和sophie 被允许使用[Ctrl]-[Alt]-[Del] 来从控制台关闭系统。当这个键组合被使用时，/etc/inittab 中的shutdown -a 就会查看/etc/shutdown.allow 中列出的用户（或根用户）是否在虚拟控制台上登录了。如果登录者是其中之一，系统关闭就会继续；否则，系统控制台上就会显示出错误消息。

关于shutdown.allow 的详细信息，请参阅shutdown 的说明书（man）页。

24.2. 禁用控制台程序访问

为了禁用用户对控制台程序的访问，你应该以根用户身份运行下面的命令：

```
rm -f /etc/security/console.apps/*
```

在控制台没有被保护的环境下（BIOS 和引导装载程序的口令没有被设置；[Ctrl]-[Alt]-[Delete] 键组合没有被禁用；电源和重设开关没有被禁用等等），你可能不想允许任何用户在控制台上运行这些默认可以从控制台上使用的命令：poweroff、halt、和reboot。

要取消这些能力，以根用户身份运行下面的命令：

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

24.3. 禁用所有控制台访问

PAM pam_console.so 模块管理控制台文件的权限和验证。（关于配置PAM 的详情，请参阅《*Red Hat Linux* 参考指南》。）如果你想禁用所有的控制台访问，包括程序和文件的访问，把所有/etc/pam.d 目录中引用pam_console.so 的句子都改为注释。以根用户使用下面的脚本就可以达到这一目的：

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

24.4. 定义控制台

pam_console.so 模块使用/etc/security/console.perms 文件来判定系统控制台上用户的权限。该文件的语法非常灵活；你可以编辑该文件以便不再应用这些指示。然而，默认文件中有一行看起来如下：

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

当用户登录后，他们会被连接到某种有名称的终端，要么是名称类似:0 或mymachine.example.com:1.0 的X 服务器，要么是类似/dev/ttyS0 或/dev/pts/2 的设备。默认设置中，本地虚拟控制台和本地X 服务器被定义为本地，但是如果你想把和你相邻的位于端口/dev/ttyS1 上的串线终端也当作本地，你可以把上面一行改为：

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

24.5. 使文件可从控制台访问

/etc/security/console.perms 文件中的某段包含以下几行：

```
<floppy>=/dev/fd[0-1]*\
/dev/floppy/*/mnt/floppy*
<sound>=/dev/dsp*/dev/audio*/dev/midi*\
/dev/mixer*/dev/sequencer\
/dev/sound/*/dev/beep
<cdrom>=/dev/cdrom*/dev/cdroms/*/dev/cdwriter*/mnt/cdrom*
```

如果有必要，你可以在这段里加入你自己编写的句子。请确定你添加的句中所指代的是正确的设备。譬如，你可以添加以下这一行：

```
<scanner>=/dev/scanner/dev/usb/scanner*
```

（当然，请确定/dev/scanner 的确是你的扫描仪设备，而不是你的硬盘驱动器。）

这是第一步。第二步是定义如何处置那些文件。在/etc/security/console.perms 文件的最后一段寻找与以下类似的句子：

```
<console>0660<floppy>0660root.floppy
<console>0600<sound>0640root
<console>0600<cdrom>0600root.disk
```

然后，添加和以下类似的一行：

```
<console> 0600 <scanner> 0600 root
```

当你在控制台登录后，你就会被给予/dev/scanner 设备的所有权，其权限是0600（仅可被你读写）。当你注销后，该设备就会被根用户所有，权限依旧是0600（现在将只能被根用户读写）。

24.6. 为其它应用程序启用控制台访问

如果你想使其它应用程序能被控制台用户访问，你要采取的步骤就会多一些。

首先，只有驻留在/sbin 或/usr/sbin 中的应用程序才能在控制台上访问，因此你想运行的程序也必须被保存在那两个目录中。满足了上面的条件后，执行下面的步骤：

1. 创建一个从你的应用程序（如以下例子中的*foo*）到/usr/bin/consolehelper 的链接：
   ```
   cd /usr/bin
   ln -s consolehelper foo
   ```
2. 创建文件/etc/security/console.apps/*foo*：
   ```
   touch /etc/security/console.apps/foo
   ```
3. 在/etc/pam.d/ 目录中为*foo* 服务创建一个PAM 配置文件。做到它的简单方法是使用halt 服务的PAM 配置文件的副本，如果你想改变行为的话，修改该文件：
   ```
   cp /etc/pam.d/halt /etc/pam.d/foo
   ```

现在，当你运行/usr/bin/*foo* 时，它就会调用consolehelper，该命令会借助/usr/sbin/userhelper 来验证用户。要验证用户，consolehelper 会询问用户的口令（若/etc/pam.d/*foo* 是/etc/pam.d/halt 文件的副本的话，否则，它会仅执行在/etc/pam.d/*foo* 中的命令），然后使用根权限来运行/usr/sbin/*foo*。

在PAM 配置文件中，应用程序可以被配置使用*pam_timestamp* 模块来记住（缓存）一次成功的尝试。当应用程序被启动并提供了正确的验证后（根口令），一个时间戳文件就会被创建。按照默认设置，成功验证会被缓存五分钟。在这段时期内，在同一会话中运行的其它配置使用pam_timestamp 的应用程序会自动为该用户验证— 用户不必再输入根口令。

该模块被包括在pam 软件包中。要启用这项功能，etc/pam.d/ 中的PAM 配置文件必须包括以下几行：

```
authsufficient/lib/security/pam_timestamp.so
sessionoptional/lib/security/pam_timestamp.so
```

第一个以auth 开头的行应该在任何auth sufficient 行之后，以session 开头的行应该在所有session optional 行之后。

如果配置使用pam_timestamp 的从面板上的「主菜单」按钮启动的应用程序被成功地验证，  图标就会显示在面板的通知区域（若你运行的是GNOME 桌面环境）。验证过期后（默认为五分钟），该图标就会消失。

用户可以通过点击图标并选择忘记验证选项来忘记缓存验证。

24.7. floppy 组群

如果由于某种原因，控制台访问对你不适用，你需要给非根用户提供到系统软盘驱动器的访问，这可以通过使用floppy 组群来达到。使用你选定的工具把用户添加到floppy 组群就可以了。这里向你提供了一个如何使用gpasswd 来把用户fred 添加到floppy 组群的例子：

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

现在，用户fred 就可以通过控制台访问系统的软盘驱动器了。

25. 用户和组群配置

用户管理器 允许你查看、修改、添加和删除本地用户和组群。

要使用用户管理器，你必须运行X 窗口系统，具备根特权，并且安装了`redhat-config-users` RPM 软件包。要从桌面启动用户管理器，点击面板上的「主菜单」 => 「系统设置」 => 「用户和组群」，或在shell 提示（如XTerm 或GNOME 终端）下键入`redhat-config-users` 命令。

图**25-1. Red Hat** 用户管理器

要查看包括系统内全部本地用户的列表，点击「用户」标签。要查看包括系统内全部本地组群的列表，点击「组群」标签。

如果你需要寻找指定的用户或组群，在「搜索过滤器」字段内键入名称的前几个字符。按[Enter]键或点击「应用过滤器」按钮。被过滤的列表就会被显示。

要给用户和组群排序，点击列名。用户或组群就会按照该列的信息被排序。

Red Hat Linux 把500 以下的用户ID 保留给系统用户。用户管理器默认不显示系统用户。要查看包括系统用户在内的所有用户，从下拉菜单中取消选择「首选项」 => 「过滤系统用户和组群」。

关于用户和组群的额外信息，请参阅《*Red Hat Linux* 参考指南》以及《*Red Hat Linux* 系统管理启蒙手册》.

25.1. 添加新用户

要添加新用户，点击「添加用户」按钮。一个如图25-2 所示的窗口就会出现。在适当的字段内键入新用户的用户名和全称。在「口令」和「确认口令」字段内键入口令。口令必须至少有六个字符。


窍门

用户的口令越长，其他人就越不容易猜到这个口令，从而不经许可地登录到用户的账号中。我们还建议你不要根据现成词组来选择口令，口令最好是字母、数字和特殊字符的组合。

选择一个登录shell。如果你不能确定应该选择哪一个shell，就请接受默认的/bin/bash。默认的主目录是/home/用户名。你可以改变为用户创建的主目录，或者通过取消选择「创建主目录」来不为用户创建主目录。

如果你选择要创建主目录，默认的配置文件就会从/etc/skel目录中复制到新的主目录中。

Red Hat Linux 使用用户私人组群（*user private group*，*UPG*）方案。UPG 方案并不添加或改变UNIX 处理组群的标准方法；它只不过提供了一个新约定。按照默认设置，每当你创建一个新用户的时候，一个与用户名相同的独特组群就会被创建。如果你不想创建这个组群，取消选择「为该用户创建私人组群」。

要为用户指定用户ID，选择「手工指定用户**ID**」。如果这个选项没有被选，从号码500 开始后的下一个可用用户ID 就会被分派给新用户。Red Hat Linux 把低于500 的用户ID 保留给系统用户。

点击「确定」来创建该用户。

图**25-2.** 创建新用户

要配置更高级的用户属性（譬如口令过期），或在添加用户后修改用户属性，请参阅第25.2 节。

要把用户加入到更多的用户组群中，点击「用户」标签，选择该用户，然后点击「属性」。在「用户属性」窗口中，选择「组群」标签。选择你想让该用户加入的组群，以及用户的主要组群，然后点击「确定」。

25.2. 修改用户属性

要查看某个现存用户的属性，点击「用户」标签，从用户列表中选择该用户，然后在按钮菜单中点击「属性」（或者从下拉菜单中选择「行动」=>「属性」）。一个类似图25-3的窗口就会出现。

图**25-3.** 用户属性

「用户属性」窗口被分隔成多个带标签的活页：

- 「用户数据」 — 显示在你添加用户时配置的基本用户信息。使用这个标签来改变用户的全称、口令、主目录或登录shell。
- 「账号信息」 — 如果你想让账号到达某一固定日期时过期，选择「启用账号过期」。在提供的字段内输入日期。选择「用户账号已被锁」来锁住用户账号，从而使用户无法在系统登录。
- 「口令信息」 — 这个标签显示了用户口令最后一次被改变的日期。要强制用户在一定天数之后改变口令，选择「启用口令过期」。你还可以设置允许用户改变口令之前要经过的天数，用户被警告去改变口令之前要经过的天数，以及账号变为不活跃之前要经过的天数。
- 组群 — 选择你想让用户加入的组群以及用户的主要组群。

25.3. 添加新组群

要添加新用户组群，点击「添加组群」按钮。一个类似图25-4的窗口就会出现。键入新组群的名称来创建。要为新组群指定组群ID，选择「手工指定组群**ID**」，然后选择GID。Red Hat Linux 把低于500 的组群ID 保留给系统组群。

点击「确定」来创建组群。新组群就会出现在组群列表中。

图**25-4.** 创建新组群

要在组群中添加用户，请参阅第25.4 节。

25.4. 修改组群属性

要查看某一现存组群的属性，从组群列表中选择该组群，然后在按钮菜单中点击「属性」（或选择下拉菜单「文件」=> 属性）。一个类似图25-5的窗口就会出现。

图25-5. 组群属性

「组群用户」标签显示了哪些用户是组群的成员。选择其他用户来把他们加入到组群中，或取消选择用户来把他们从组群中移除。点击「确定」或「应用」来修改该组群中的用户。

25.5. 命令行配置

如果你更喜欢使用命令行工具，或者没有安装X 窗口系统，请参考本章以下各节来配置用户和组群。

25.5.1. 添加用户

要在系统上添加用户：

1. 使用useradd 命令来创建一个锁定的用户账号：
   useradd <*username*>
2. 使用passwd 命令，通过指派口令和口令老化规则来给某账号开锁：
   passwd <*username*>

useradd 的命令行选项在表25-1中被列出。

选项	描述
-c *comment*	用户的注释。
-d *home-dir*	用来取代默认的/home/*username* 主目录。
-e *date*	禁用账号的日期，格式为：YYYY-MM-DD
-f *days*	口令过期后，账号禁用前的天数（若指定了**0**，账号在口令过期后会被立刻禁用。若指定了**-1**，口令过期后，账号将不会被禁用）。
-g *group-name*	用户默认组群的组群名或组群号码（该组群在指定前必须存在）。
-G *group-list*	用户是其中成员的额外组群名或组群号码（默认以外的）列表，用逗号分隔（组群在指定前必须存在）。
-m	若主目录不存在则创建它。
-M	不要创建主目录。

选项	描述
-n	不要为用户创建用户私人组群。
-r	创建一个UID 小于500 的不带主目录的系统账号。
-p *password*	使用crypt 加密的口令。
-s	用户的登录shell，默认为/bin/bash。
-u *uid*	用户的UID，它必须是独特的，且大于499。

表25-1. useradd 命令行选项

25.5.2. 添加组群

要给系统添加组群，使用groupadd 命令：

```
groupadd <group-name>
```

groupadd 的命令行选择在表25-2中被列出。

选项	描述
-g *gid*	组群的GID，它必须是独特的，且大于499。
-r	创建小于500 的系统组群。
-f	若组群已存在，退出并显示错误（组群不会被改变）。如果指定了-g 和-f 选项，而组群已存在，-g 选项就会被忽略。

表25-2. groupadd 命令行选项

25.5.3. 口令老化

为安全起见，要求用户定期改变他们的口令是明智之举。这可以在用户管理器的「口令信息」标签上添加或编辑用户时做到。

要从shell 提示下为用户配置口令过期，使用chage 命令，随后使用表25-3中的选项，以及用户的用户名。


重要

要使用chage 命令，屏蔽口令一定要被启用。

选项	描述
-m *days*	指定用户必须改变口令所间隔的最少天数。如果值为0，口令就不会过期。
-M *days*	指定口令有效的最多天数。当该选项指定的天数加上-d 选项指定的天数小于当前的日期，用户在使用该账号前就必须改变口令。
-d *days*	指定自从1970 年1 月1 日起，口令被改变的天数。

选项	描述
-I *days*	指定口令过期后，账号被锁前不活跃的天数。如果值为0，账号在口令过期后就不会被锁。
-E *date*	指定账号被锁的日期，日期格式为YYYY-MM-DD。若不用日期，也可以使用自1970 年1月1日后经过的天数。
-W *days*	指定口令过期前要警告用户的天数。

表**25-3. change** 命令行选项


窍门

如果chage 命令后紧跟着用户名（无其它选项），它会显示当前口令的老化数值并运行这些数值被改变。

如果系统管理员想让用户在首次登录时设置口令，用户的口令可以被设置为立即过期，从而强制用户在首次登录后立即改变它。

要强制用户在首次登录到控制台时配置口令，请遵循以下步骤。注意，若用户使用SSH 协议来登录，这个过程就行不通。

1. 锁住用户的口令 — 如果用户不存在，使用useradd 命令来创建这个用户账号，但是不要给它任何口令，所以它仍旧被锁。

   如果口令已经被启用，使用下面的命令来锁住它：
   ```
   usermod -L username
   ```
2. 强制即刻口令过期 — 键入下面的命令：
   ```
   chage -d 0 username
   ```
   该命令把口令最后一次改变的日期设置为epoch（1970年1月1）。不管口令过期策略是否存在，这个值会强制口令立即过期
3. 给账号开锁 — 达到这一目的有两种常用方法。管理员可以指派一个初始口令或空口令。

   
   警告

   不要使用passwd 来设置口令，因为它会禁用刚刚配置的口令即刻过期。

   要指派初始口令，遵循以下步骤：

   - 使用python 命令来启动命令行python 解释器。它的显示如下：
     ```
     Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
     [GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
     Type "help", "copyright", "credits" or "license" for more information.
     >>>
     ```
   - 在提示下，键入以下命令（把*passwword* 替换成要加密的口令，把*salt* 替换成恰巧两个大写或小写字母、数字、点字符或斜线字符，譬如+ ab 或+ 12）：
     ```
     import crypt; print crypt.crypt("password","salt")
     ```
     其输出的加密口令类似于12CsGd8FRcMSM。
   - 键入[Ctrl]-[D] 来退出Python 解释器。
   - 把加密口令的输出剪贴到以下命令中（不带头尾的空格）：
     ```
     usermod -p "encrypted-password" username
     ```

   与其指派初始口令，你还可以使用以下命令来指派空口令：
   ```
   usermod-p""username
   ```


小心

使用空口令对用户和管理员来说都很方便，但它却带有一个轻微的危险性——第三方可以会首先登录并进入系统。要减小这种威胁，推荐管理员在给账号开锁的时候校验用户已经做好了登录准备。

无论是哪一种情况，首次登录后，用户都会被提示输入新口令。

25.6. 对进程的解释

下列步骤演示了在启用屏蔽口令的系统上使用useradd juan命令后的情形：

1. 在/etc/passwd文件中新添了有关juan的一行。这一行的特点如下：
   - 它以用户名juan开头。
   - 口令字段有一个“x”，表示系统使用屏蔽口令。
   - 500或500以上的UID被创建。（在Red Hat Linux中，500以下的UID和GID被保留为系统使用。）
   - 500或500以上的GID被创建。
   - 可选的GECOS信息被留为空白。
   - juan的主目录被设为/home/juan/。
   - 默认的shell被设为/bin/bash。

2. 在/etc/shadow文件中新添了有关juan的一行。这一行的特点如下：
   - 它以用户名juan开头。
   - 出现在/etc/shadow文件中口令字段内的两个叹号（!!）会锁住账号。

     
     注记

     如果某个加密的口令使用了-p标志被传递，这个口令会被放置在/etc/shadow文件中用于该用户的那一行中。

   - 口令被设置为永不过期。

3. 在/etc/group文件中新添了一行有关juan组群的信息。和用户名相同的组群叫做用户私人组群（*user private group*）。关于用户私人组群的详情，请参阅第25.1节。

   在/etc/group文件中新添的这一行具有如下特点：
   - 它以组群名juan开头。
   - 口令字段有一个“x”，表示系统使用屏蔽口令。
   - GID与列举/etc/passwd文件中用户juan行中的相同。

4. 在/etc/gshadow文件中新添了有关juan组群的一行。这一行的特点如下：
   - 它以组群名juan开头。
   - 出现在/etc/gshadow文件中口令字段内的一个叹号（!）会锁住该组群。
   - 所有其它字段都为空白。

5. 用于用户juan 的目录被创建在/home/ 目录之下。该目录为用户juan 和组群juan 所有。它的读写和执行权限仅为用户juan 所有。所有其它权限都被拒绝。
6. /etc/skel/ 目录（包含默认用户设置）内的文件被复制到新建的/home/juan/ 目录中。

这时候，系统上就存在了一个叫做juan 的被锁的账号。要激活它，管理员必须使用passwd 命令该账号指派一个口令，或者还可以设置口令老化规则。

redhat.

26.

收集系统信息

在你学习如何配置系统之前，你应该学习如何收集基本的系统信息。譬如，你应该知道如何找出关于空闲内存的数量、可用硬盘驱动器空间的数量，硬盘分区方案，以及正在运行进程的信息。本章将讨论如何使用几个简单命令和程序来从你的Red Hat Linux 系统中检索这类信息。

26.1. 系统进程

ps ax命令显示一个当前系统进程的列表，该列表中包括其他用户拥有的进程。要显示进程以及它们的所有者，使用ps aux命令。该列表是一个静态列表；换一句话说，它是在你启用这项命令时正在运行的进程的快照。如果你需要一个时刻更新的运行进程列表，使用下面描述的top命令。

ps 的输出会很长。要防止它快速从屏幕中滑过，你可以把它管道输出给less 命令：

```
ps aux | less
```

你可以使用ps 命令和grep 命令的组合来查看某进程是否在运行。譬如，要判定**emacs** 是否在运行，使用下面这个命令：

```
ps ax | grep emacs
```

top 命令显示了当前正运行的进程以及关于它们的重要信息，包括它们的内存和CPU 用量。该列表既是真实时间的也是互动的。以下提供了一个top 的输出示例：

```
 00:53:01 up 6 days, 14:05,  3 users,  load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states: 18.0% user  0.1% system  16.0% nice  0.0% iowait 80.1% idle
Mem:  1030244k av, 985656k used,  44588k free,    0k shrd, 138692k buff
         424252k actv,  23220k in_d,  252356k in_c
Swap: 2040212k av, 330132k used, 1710080k free        521796k cached

  PID USER   PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
15775 joe     5   0 11028  10M 3192 S    1.5  4.2  0:46 emacs
14429 root   15   0 63620  62M 3284 R    0.5 24.7 63:33 X
17372 joe    11   0  1056 1056  840 R    0.5  0.4  0:00 top
17356 joe     2   0  4104 4104 3244 S    0.3  1.5  0:00 gnome-terminal
    1 root    0   0   544  544  476 S    0.0  0.2  0:06 init
    2 root    0   0     0    0    0 SW   0.0  0.0  0:00 kflushd
    3 root    1   0     0    0    0 SW   0.0  0.0  0:24 kupdate
    4 root    0   0     0    0    0 SW   0.0  0.0  0:00 kpiod
    5 root    0   0     0    0    0 SW   0.0  0.0  0:29 kswapd
  347 root    0   0   556  556  460 S    0.0  0.2  0:00 syslogd
  357 root    0   0   712  712  360 S    0.0  0.2  0:00 klogd
  372 bin     0   0   692  692  584 S    0.0  0.2  0:00 portmap
  388 root    0   0     0    0    0 SW   0.0  0.0  0:00 lockd
  389 root    0   0     0    0    0 SW   0.0  0.0  0:00 rpciod
  414 root    0   0   436  432  372 S    0.0  0.1  0:00 apmd
  476 root    0   0   592  592  496 S    0.0  0.2  0:00 automount
```

要退出top，按[q] 键。

可以和top 一起使用的互动命令包括：

命令	描述

命令	描述
[Space]	立即刷新显示
[h]	显示帮助屏幕
[k]	杀死某进程。你会被提示输入进程ID 以及要发送给它的信号。
[n]	改变显示的进程数量。你会被提示输入数量。
[u]	按用户排序。
[M]	按内存用量排序。
[P]	按CPU 用量排序。

表**26-1.** 互动的**top** 命令

窍门

类似于**Mozilla** 和**Nautilus** 的应用程序具备线程感知（*thread-aware*） — 多个线程会被创建来处理多个用户或多个请求，而且每个线程都有自己的PID。按照默认设置，ps 和top 只显示主（初始）线程。要查看所有线程，使用ps -m 命令或在top 中键入[Shift]-[H]组合键。

如果和top 相比，你更喜欢使用图形化界面，你可以使用**GNOME** 系统监视器。要从桌面上启动它，选择面板上的「主菜单」 => 「系统工具」 => 「系统监视器」或在X 窗口系统的shell 提示下键入gnome-system-monitor。然后选择「进程列表」标签。

GNOME 系统监视器允许你在正运行的进程列表中搜索进程，还可以查看所有进程、你拥有的进程、或活跃的进程。

要了解更多关于某进程的情况，选择该进程，然后点击「更多信息」按钮。关于该进程的细节就会显示在窗口的底部。

要停止某进程，选择该进程，然后点击「结束进程」。这有助于结束对用户输入已不再做出反应的进程。

要按指定列的信息来排序，点击该列的名称。信息被排序的那一列会用深灰色显示。

按照默认设置，**GNOME** 系统监控器不显示线程。要改变这个首选项，选择「编辑」 => 「首选项」，点击「进程列表」标签，然后选择「显示线程」。首选项还允许你配置更新间隔；每个进程默认显示的信息；以及系统监视器图表的颜色。

图**26-1. GNOME** 系统监视器

26.2. 内存用量

`free`命令显示系统的物理内存和交换区的总量，以及已使用的、空闲的、共享的、在内核缓冲内的、和被缓存的内存数量。

```
      total   used   free  shared  buffers  cached
Mem:   256812  240668   16144  105176   50520   81848
-/+ buffers/cache:  108300  148512
Swap:   265032   780  264252
```

`free -m`命令显示的信息和前面相同，但是它以MB 为单位，便于阅读。

```
      total   used   free  shared  buffers  cached
Mem:     250    235     15    102     49     79
-/+ buffers/cache:    105    145
Swap:    258     0    258
```

如果和`free`相比，你更喜欢使用图形化界面，你可以使用**GNOME** 系统监视器。要从桌面上启动它，选择面板上的「主菜单」 => 「系统工具」 => 「系统监视器」或在X 窗口系统的shell 提示下键入`gnome-system-monitor`。然后选择「进程列表」标签。

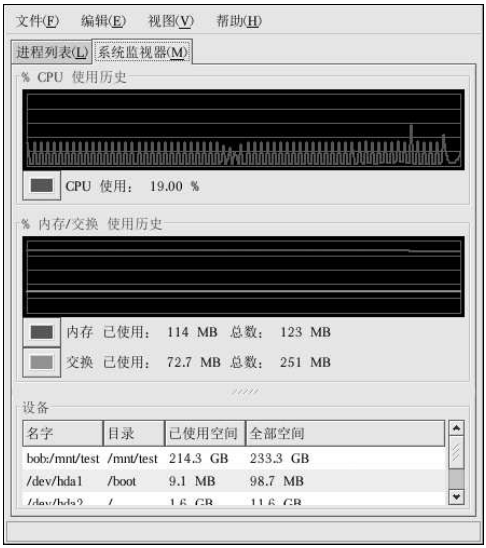


图**26-2. GNOME** 系统监视器

26.3. 文件系统

df 命令报告系统的磁盘空间用量。如果你在shell 提示下键入了df 命令，它的输出与下面相似：

```
Filesystem     1k-blocks   Used Available Use% Mounted on
/dev/hda2      10325716  2902060  6899140 30% /
/dev/hda1         15554     8656     6095 59% /boot
/dev/hda3      20722644  2664256 17005732 14% /home
none             256796        0   256796  0% /dev/shm
```

按照默认设置，该工具把分区大小显示为1KB 的块，已用的和可用的磁盘空间以KB 为单位显示。要查看以MB 和GB 为单位的信息，使用df -h 命令。-h 选项代表人可读格式。它的输出类似于：

```
Filesystem     Size Used Avail Use% Mounted on
/dev/hda2      9.8G 2.8G 6.5G 30% /
/dev/hda1       15M 8.5M 5.9M 59% /boot
/dev/hda3       20G 2.6G  16G 14% /home
none           251M   0 250M  0% /dev/shm
```

在分区列表中，有一项是/dev/shm。该项目代表系统的虚拟内存文件系统。

du 命令显示被目录中的文件使用的估计空间数量。如果你在shell 提示下键入了du 命令，每个子目录的用量都会在列表中显示，当前目录和子目录的总和也会在列表的最后一行中被显示。如果你不想查看每个子目录的用量，使用du -hs 命令来使用人可读的格式只列出目录用量总和。使用du --help 命令来查看更多选项。

要查看图形化的系统分区和磁盘空间用量，使用「系统监视器」标签，如图26-2的底部所示。


窍门

关于实现磁盘配额的信息，请参阅第6章。

26.3.1. 监控文件系统

Red Hat Linux 提供了一个叫做diskcheck 的工具程序，它监视系统上的空闲磁盘空间数量。根据配置文件的规定，当一个或多个磁盘驱动器上的用量达到指定程度时，它会向系统管理员发送电子邮件。要使用该工具，你必须安装了diskcheck RPM 软件包。

该工具作为每小时cron [1]任务运行。

以下变量可以在/etc/diskcheck.conf 文件中被定义：

- defaultCutoff — 当磁盘驱动器的用量达到这个百分比，它就会被报告。譬如，如果defaultCutoff = 90 被指定，磁盘驱动器的用量达到90%，电子邮件就会被寄出。
- cutoff[*/dev/partition*] — 超越分区的defaultCutoff。例如，如果cutoff['/dev/hda3'] = 50 被指定，当/dev/hda3 分区的用量达到50%，diskcheck 就会警告系统管理员。
- cutoff[*/mountpoint*] — 超越挂载点的defaultCutoff。譬如，如果cutoff['/home'] = 50 被指定，当/home 挂载点的用量达到50%，diskcheck 就会警告系统管理员。
- exclude — 指定diskcheck 要忽略的一个或多个分区。譬如，如果exclude = "/dev/sda2 /dev/sda4" 被指定，在/dev/sda2 或/dev/sda4 的用量达到指定的切断百分比的情况下，diskcheck 将不会警告系统管理员。
- ignore — 指定要忽略的一个或多个文件系统，格式为-x *filesystem-type*。譬如，如果ignore = "-x nfs -x iso9660" 被指定了，在nfs 或iso9660 文件系统的用量达到限制时，系统管理员将不会被警告。
- mailTo — 当分区或挂载点达到限制时，要向系统管理员发出警告的电子邮件地址。譬如，如果mailTo = "webmaster@example.com" 被指定了，警告就会被邮寄给webmaster@example.com。
- mailFrom — 指定电子邮件寄发者的身份。这有助于系统管理员过滤来自diskcheck 的邮件。譬如，如果mailFrom = "Disk Usage Monitor" 被指定了，发送给系统管理员的电子邮件的寄发者就是“磁盘用量监控器”。
- mailProg — 指定发送电子邮件警告要使用的邮寄程序。譬如，如果mailProg = "/usr/sbin/sendmail" 被指定了，Sendmail 就会被用作邮寄程序。

如果你改变了配置文件，你不必重新启动服务，因为每次cron 任务运行的时候都会重读该配置文件。你必须运行crond 服务才能执行cron 任务。要判定该守护进程是否在运行，使用/sbin/service crond status 命令。推荐你在引导时启动该服务。关于在引导时自动启动cron 服务的详细信息，请参阅第14章。

26.4. 硬件

如果你在配置硬件时遇到问题，或者只是想了解一下你的系统中有哪些硬件，你可以使用硬件浏览器程序来显示能被探测到的硬件。要在桌面环境下启动该程序，点击「主菜单」 => 「系统工具」 => 「硬件浏览器」，或在shell 提示下键入hwbrowser。如图26-3所示，它显示了你的光盘设备、软盘、硬盘驱动器和它们的分区、网络设备、指示设备、系统设备、以及视频卡。点击左侧菜单上的类别名称，有关信息就会被显示。

1. 关于cron 的详情请参阅第28章。

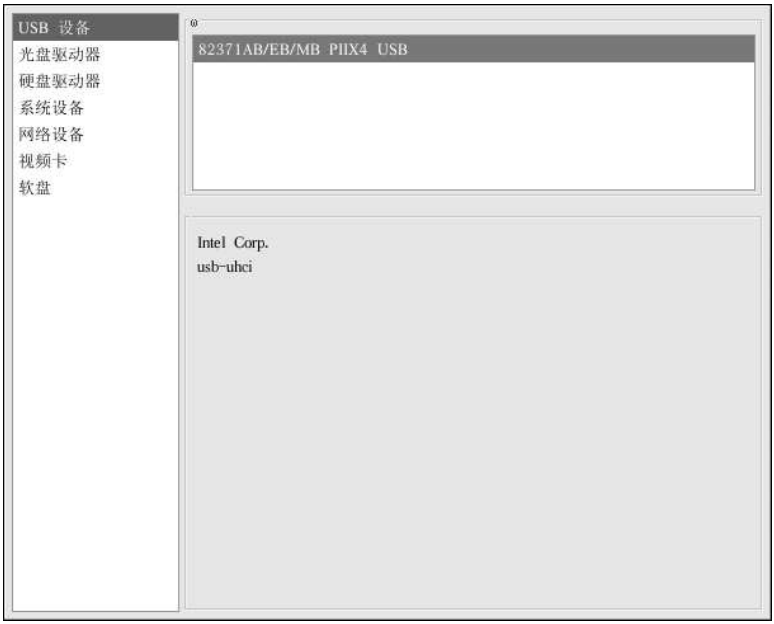


图26-3. 硬件浏览器

你还可以使用lspci命令来列举所有的PCI设备。使用lspci -v命令来获得详细的信息，或使用lspci -vv命令来获得更详细的输出。

譬如，lspci命令可以被用来判定系统视频卡的制造厂商、型号、以及内存大小：

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) (prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

如果你不知道系统网卡的制造商或型号，lspci可以帮助你来判定这些信息。

26.5. 其它资料

要学习更多关于收集系统信息的知识，请参考下列资料。

26.5.1. 安装了的文档

- ps --help — 显示了一个能够与ps一起使用的选项列表。
- top的说明书页 — 键入man top来学习关于top和它的选项的知识。
- free的说明书页 — 键入man free来学习关于free和它的选项的知识。

- `df` 的说明书页 — 键入`man df` 来学习关于`df` 和它的选项的知识。
- `du` 的说明书页 — 键入`man du` 来学习关于`du` 和它的选项的知识。
- `lspci` 的说明书页 — 键入`man lspci` 来学习更多关于`lspci` 命令和它的许多选项的信息。
- `/proc` — `/proc` 目录的内容也可以用来收集更详细的系统信息。关于`/proc` 目录的额外信息，请参阅《*Red Hat Linux* 参考指南》。

26.5.2. 相关书籍

- *Red Hat Linux* 系统管理启蒙手册; Red Hat, Inc. — 包括一个关于监视资源的章节。

27.

打印机配置

打印机配置工具允许用户在Red Hat Linux 上配置打印机，该工具为维护打印机配置文件、打印假脱机目录、和打印过滤器提供协助。

从版本9 开始，Red Hat Linux 默认使用CUPS 打印系统。从前的默认打印系统LPRng 仍被提供了。如果系统是从以前的使用LPRng 的Red Hat Linux 中升级而来的，升级过程不会使用CUPS 来替代LPRng；系统仍会继续使用LPRng。

如果系统是从以前的使用CUPS 的Red Hat Linux 版本升级而来的，升级过程会保留配置的队列，系统仍会继续使用CUPS。

打印机配置工具既能够配置CUPS，也能够配置LPRng 打印系统。根据你的系统配置而定，它会配置活跃的打印系统。

要使用打印机配置工具，你必须具备根特权。要启动这个应用程序，选择面板上的「主菜单」 => 「系统设置」 => 「打印」，或键入`redhat-config-printer` 命令。该命令会根据它所执行的环境是图形化X 窗口系统还是基于文本的控制台来自动判定它应该以图形化还是文本形式来运行程序。

你还可以通过在shell 提示下键入`redhat-config-printer-tui` 来强制打印机配置工具作为基于文本的程序运行。


重要

不要编辑`/etc/printcap` 文件或`/etc/cups/` 目录中的文件。打印机守护进程（`lpd` 或`cups`）在每次启动或重新启动时，新的配置文件都会被动态创建。当你在打印机配置工具中应用所做改变时，配置文件也会被动态创建。

如果你在使用LPRng，并想不使用打印机配置工具而添加一个打印机，请编辑`/etc/printcap.local` 文件。`/etc/printcap.local` 文件中的项目没有显示在打印机配置工具中，但是会被打印机守护进程读取。如果你从以前的Red Hat Linux 中更新，你现存的配置文件就会被转换到被这个程序使用的新格式。每当新配置文件被生成时，旧配置文件都会被保存为`/etc/printcap.old`。

如果你在使用CUPS，打印机配置工具不会显示任何没有使用打印机配置工具配置的队列或共享；不过，它也不会把它们从配置文件中删除。

图**27-1.** 打印机配置工具

你可以配置以下类型的打印队列：

- 「本地连接」 — 直接通过并行或USB 端口连接到计算机上的打印机。
- 「联网的**CUPS (IPP)**」 — 连接到能够通过TCP/IP 网络、使用互联网打印协议进入的打印机，又称IPP（例如，连接到网络上另一个运行CUPS 的Red Hat Linux 系统的打印机）。
- 「联网的**UNIX (LPD)**」 — 连接到能够通过TCP/IP 网络进入的其它UNIX 系统上的打印机（例如，连接到网络上另一个运行LPD 的Red Hat Linux 系统的打印机）。
- 「联网的**Windows (SMB)**」 — 连接到通过SMB 网络来共享打印机的其它系统上的打印机（例如，连接到Microsoft Windows™ 机器上的打印机）。
- 「联网的**Novell (NCP)**」 — 连接到使用Novell's NetWare 网络技术的其它系统上的打印机。
- 「联网的**JetDirect**」 — 通过HP JetDirect 直接连接到网络而不是计算机上的打印机。


重要

如果你添加一个新队列或修改一个现存队列，你必须应用这些改变才能使它们生效。

点击「应用」按钮来保存你所做的改变并重新启动打印机守护进程。这些改变在守护进程被重新启动前不会被写入配置文件。此外，也也可以选择「行动」 => 「行动」。

27.1. 添加本地打印机

要添加本地打印机，如通过并行端口或USB 端口连接到你的计算机上的打印机，点击打印机配置工具主窗口上的「新建」按钮。一个如图27-2所示的窗口就会出现。点击「前进」来继续。

图**27-2.** 添加打印机

在如图27-3所示的窗口中，在「名称」文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入关于打印机的简短描述，其中可以包含空格。

图27-3. 选择队列名称

点击了「前进」后，如图27-4所示的窗口就会出现。从「选择队列类型」中选择「本地连接」，然后选择设备。这个设备通常是/dev/lp0（并行打印机）或/dev/usb/lp0（USB 打印机）。如果列表中没有设备，点击「重扫描设备」来重新扫描计算机或点击「定制设备」来手工指定它。点击「前进」来继续。

图27-4. 添加本地打印机

下一步是选择打印机类型。请转到第27.7 节来继续。

27.2. 添加一个IPP 打印机

IPP 打印机是连接到运行CUPS 的同一网络上的不同Linux 系统上的打印机。按照默认配置，打印机配置工具浏览网络来寻找共享的CUPS 打印机。（该选项可以通过选择「行动」 => 「共享」来改变。）所有联网的IPP 打印机都以浏览队列的形式出现在主窗口中。

如果你在打印服务器上配置了防火墙，它必须能够在进入的UDP 端口631 上发送和接收连接。如果你在客户（发送打印请求的计算机）上配置了防火墙，它必须被允许在端口631 上发送和接收连接。

如果你禁用了自动浏览功能，你仍可以通过打印机配置工具主窗口上的「新建」按钮来添加一个联网的CUPS 打印机。它会显示一个如图27-2所示的窗口。点击「前进」来继续。

在如图27-3所示的窗口中，在「名称」文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入关于打印机的简短描述，其中可以包含空格。

点击了「前进」后，图27-5就会出现。从「选择队列类型」菜单中选择「联网的**CUPS (IPP)**」。

图**27-5.** 添加一个**IPP** 打印机

用于以下选项的文本字段会出现**:**

- 「服务器」 — 打印机所连接的远程机器的主机名或IP 地址。
- 「路径」 — 到远程机器上的打印队列的路径。

点击「前进」来继续。

下一步是选择打印机类型。请转到第27.7 节来继续。

重要

联网的IPP 打印服务器必须允许来自本地系统的连接。详情请参阅第27.13 节。

27.3. 添加远程**UNIX (LPD)** 打印机

要添加远程UNIX 打印机，如连接在同一网络上的不同Linux 系统上的打印机，点击打印机配置工具主窗口上的「新建」按钮。如图27-2所示的窗口就会出现。点击「前进」来继续。

在如图27-3所示的窗口中，在「名称」文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入关于打印机的简短描述，其中可以包含空格。

从「选择队列类型」菜单上选择「联网的**UNIX (LPD)**」，然后点击「前进」。

图27-6. 添加远程**LPD** 打印机

用于以下选项的文本字段会出现：

- 「服务器」 — 打印机所连接的远程机器的主机名或IP 地址。
- 「队列」 — 远程打印机队列。默认打印机队列通常是lp。

点击「前进」来继续。

下一步是选择打印机类型。请转到第27.7 节来继续。

重要

远程打印服务器必须从本地系统接受打印作业。详情请参阅第27.13.1 节。

27.4. 添加**Samba (SMB)** 打印机

要添加使用SMB 协议访问的打印机（如连接到Microsoft Windows 系统上的打印机），点击打印机配置工具主窗口中的「新建」按钮。如图27-2所示的窗口就会出现。点击「前进」来继续。

在如图27-3所示的窗口中，在「名称」文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入关于打印机的简短描述，其中可以包含空格。

从「选择队列类型」菜单中选择「联网的**Windows (SMB)**」，然后点击「前进」。如果打印机连接的是Microsoft Windows 系统，选择这个队列类型。

图27-7. 添加SMB 打印机

如图27-7所示，SMB 共享被自动检测到并列出。点击每个共享名称旁的箭头来扩展列表。从扩展列表中选择一个打印机。

如果你在找的打印机没有在列表中出现，点击右侧的「指定」按钮。用于以下选项的文本字段会出现：

- 「工作组」 — 共享打印机的Samba 工作组的名称。
- 「服务器」 —共享打印机的服务器的名称。
- 「共享」 — 你想用来打印的共享打印机的名称。这个名称必须和远程Windows 机器上定义的Samba 打印机的名称相同。
- 「用户名」 — 你要访问打印机所必须登录使用的用户名称。用户在Windows 系统上必须存在，并且必须有访问打印机的权限。默认的用户名典型为**guest**（Windows 服务器）或**nobody**（Samba 服务器）。
- 「口令」 — 在「用户名」字段中指定的用户的口令（若需要）。

点击「前进」来继续。然后，打印机配置工具会试图连接共享打印机。如果这个共享打印机需要用户名和口令，一个对话框会出现来提示你输入有效的共享打印机的用户名和口令。如果指定了正确的共享名称，你还可以在这里改变它。如果需要使用工作组名称来连接共享，它可以在这个对话框里指定。这个对话框和点击「指定」按钮后所显示的窗口相同。

下一步是选择打印机类型。请转到第27.7 节来继续。

警告

如果你需要使用用户名和口令，它们被明文贮存在只能被根用户和lpd 读取的文件中。这样，如果别人具备根特权，他们就有可能获悉用户名和口令。要避免这种情况的发生，访问打印机的用户名和口令应该不同于本地Red Hat Linux 系统上的用户账号。如果它们不同，那么唯一可能出现的安全漏洞会是未经授权的对打印机的使用。如果服务器上还有文件共享，建议你也使用不同于打印机队列的口令。

27.5. 添加Novell NetWare (NCP) 打印机

要添加Novell NetWare (NCP) 打印机，点击打印机配置工具主窗口上的「新建」按钮。如图27-1所示的窗口会出现。点击「前进」来继续。

在如图27-3所示的窗口中，在「名称」文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入关于打印机的简短描述，其中可以包含空格。

从「选择队列类型」菜单中选择「联网的**Novell (NCP)**」。

图**27-8.** 添加**NCP** 打印机

用于以下选项的文本字段会出现：

- 「服务器」 — 打印机所连接的NCP 系统的主机名或IP 地址。
- 「队列」 — NCP 系统上的打印机的远程队列。
- 「用户」 — 你要使用打印机所必须登录的用户名。
- 「口令」 — 为以上「用户」字段指定的口令。

下一步是选择打印机类型。请转到第27.7 节来继续。

警告

如果你需要使用用户名和口令，它们被明文贮存在只能被根用户和lpd 读取的文件中。这样，如果别人具备根特权，他们就有可能获悉用户名和口令。要避免这种情况的发生，访问打印机的用户名和口令应该不同于本地Red Hat Linux 系统上的用户账号。如果它们不同，那么唯一可能出现的安全漏洞会是未经授权的对打印机的使用。如果服务器上还有文件共享，建议你也使用不同于打印机队列的口令。

27.6. 添加**JetDirect** 打印机

要添加JetDirect 打印机，点击打印机配置工具主窗口上的「新建」 按钮。如图27-1所示的窗口就会出现。点击「前进」来继续。

在如图27-3所示的窗口中，在「名称」文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入关于打印机的简短描述，其中可以包含空格。

从「选择队列类型」菜单中选择「联网的**JetDirect**」，然后点击「前进」。

图**27-9.** 添加**JetDirect** 打印机

用于以下选项的文本字段会出现**:**

- 打印机 —JetDirect 打印机的主机名或IP 地址。
- 端口 — JetDirect 打印机监听打印作业的端口。默认端口为9100。

下一步是选择打印机类型。请转到第27.7 节来继续。

27.7. 选择打印机型号和结束

选择了打印机的队列类型后，下一步就是选择打印机型号。

你会看到一个和图27-10相似的窗口。如果它没有被自动检测到，从列表中选择它。打印机按照生产厂家分类。从拉下菜单中选择打印机的生产厂家的名称。每当选择了一个不同的生产厂家后，打印机型号列表都会被更新。从列表中选择打印机型号。

图**27-10.** 选择打印机型号

推荐的打印驱动程序是根据选定的打印机型号而选择的。打印驱动程序把你想打印的数据处理成打印机能够理解的格式。由于本地打印机是直接连接到你的计算机上的，你需要一个打印驱动程序来处理发送给打印机的数据。

如果你在配置远程打印机（IPP、LPD、SMB 或NCP），远程打印服务器通常有它自己的打印驱动程序。如果你在你的本地计算机上选择额外的打印驱动程序，数据就会被多次过滤并被转换成打印机所无法理解的格式。

要确定数据不会被多次过滤，首先请在生产厂家上选择「通用」，在打印机型号上选择「原始打印队列」或**Postscript**打印机。应用了改变后，打印一张测试页来试验新配置。如果测试失败，远程打印服务器可能没有配置打印驱动程序。试着根据远程打印机的生产厂家和型号来选择打印驱动程序，应用改变后，再打印一张测试页。


窍门

你可以在添加了打印机后选择一个不同的打印驱动程序。方法是，启动打印机配置工具，从列表中选择打印机，点击「编辑」，点击「驱动程序」标签，选择一个不同的打印驱动程序，然后应用这些改变。

27.7.1. 确认打印机配置

最后一步是确认你的打印机配置。如果设置正确，则点击「应用」来添加打印队列，否则，点击「后退」来修改打印机配置。

在主窗口中点击「应用」按钮来保存你的改变并重新启动打印机守护进程。应用了改变后，打印一张测试页来确定配置的正确性。详情请参阅第27.8 节。

如果你需要打印基本的ASCII 集合以外的字符（包括用于日文之类的语言中的字符），你必须回顾一下你的驱动程序选项，并选择「预绘制**Postscript**」。详情请参阅第27.9 节。如果你在添加了打印队列后编辑它，你还可以配置纸张大小之类的选项。

27.8. 打印测试页

配置了打印机后，你应该打印一张测试页来确定打印机能够正常运行。要打印测试页，从打印机列表中选择你想试验的打印机，然后从「测试」拉下菜单中选择合适的测试页。

如果你改变了打印驱动程序或修改了驱动程序选项，你应该打印一张测试页来测试不同的配置。

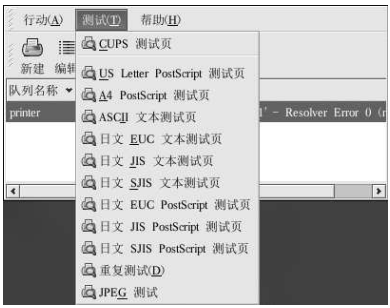


图**27-11.** 测试页选项

27.9. 修改现存打印机

要删除某个现存打印机，选择这个打印机，然后点击工具栏上的「删除」按钮。打印机就会从打印机列表中删除。点击「应用」按钮来保存改变并重新启动打印机守护进程。

要设置默认打印机，从打印机列表中选择打印机，然后选择工具栏上的「默认」按钮。默认打印机图标会在列表中默认打印机的「默认」列出现。

添加了打印机后，你还可以编辑它们的设置。从打印机列表中选择要编辑的打印机，然后点击「编辑」按钮。如图27-12所示的带活页标签的窗口就会出现。该窗口包含选中打印机的当前值。进行了必要改变后，点击「确定」按钮。点击打印机配置工具主窗口中的「应用」来保存改变并重新启动打印机守护进程。

图27-12. 编辑打印机

27.9.1. 「队列名称」

要重命名打印机或改变它的简短描述，改变「队列名称」标签中的值。点击「确定」来返回到主窗口。打印机的名称应该会在打印机列表中被改变。点击「应用」来保存改变并重新启动打印机守护进程。

27.9.2. 「队列类型」

「队列类型」标签显示了在添加打印机和它的设置时选中的队列类型。你可以改变打印机类型或仅改变它的设置。修改后，点击「确定」来返回到主窗口。点击「确定」来保存改变并重新启动打印守护进程。

根据你选择的队列类型，不同的选项会被显示。关于这些选项的描述，请参考相应的添加打印机章节。

27.9.3. 「打印机驱动程序」

「打印机驱动程序」标签显示了当前使用的打印驱动程序。如果它被改变了，点击「确定」来回到主窗口。点击「应用」来保存改变并重新启动打印守护进程。

27.9.4. 「驱动程序选项」

「驱动程序选项」标签显示了高级打印机选项。每个打印驱动器的选项会略有不同。公用选项有：

- 如果打印作业的最后一页没有从打印机中弹出（例如，换页指示灯开始闪烁），你应该选择「发送换页信号**(FF)**」。如果它不起作用，试着选择「发送传输结束信号**(EOT)**」按钮。某些打印机需要「发送换页信号**(FF)**」和「发送换页信号**(FF)**」两者来弹出最后一页。这个选项只对于LPRng 打印系统有用。
- 如果发送换页信号不起作用，你应该选择「发送传输结束信号**(EOT)**」。请参考以上的「发送换页信号**(FF)**」部分。这个选项只在LPRng 打印系统中可用。
- 如果打印驱动程序无法识别某些发送给它的数据，你应该选择「假定未知数据为文本」。只有在遇到问题时才选择这个选项。如果该选项被选，打印驱动程序会假定所有发送给它的无法识别的数据为文本。如果该选项和「将文本转换成**Postscript**」选项一起被选，打印驱动程序会假定未知数据为文本，然后把它转换成PostScript。该选项只在LPRng 打印系统中有用。
- 如果基本ASCII 集合之外的字符被发送给打印机却没有被正确打印（如日文字符），你应该选择「预绘制**Postscript**」。该选项预绘制非标准的PostScript 字体，因此它们能够被正确打印。

  如果打印机不支持你试图打印的字体，你可以试着选择这个选项。例如，选择这个选项来把日文字体打印到非日文打印机上。

  执行以上行动需要多花些时间。除非你在打印正确字体时遇到问题，请不要使用这个选项。

  还有，如果打印机无法处理PostScript 级别3 时，你也可以选择这个选项。该选项会把它转换成PostScript 级别1。
- 「**GhostScript** 预过滤」 — 允许你在打印机无法处理某个PostScript 级别时选择「无预过滤」、「转换到**PS** 级别**1**」、或「转换到**PS** 级别**2**」。该选项只在CUPS 打印系统中使用了PostScript 驱动程序时才可用。
- 「将文本转换成**Postscript**」被默认选择。如果打印机能够打印纯文本，试着在打印纯文本文档时取消选择该选项来缩短打印时间。如果使用的是CUPS 打印系统，它就不是一个可选的项目，因为文本总是会被转换成PostScript。
- 「纸张大小」允许你选择纸张的大小。该选项包括US Letter、US Legal、A3 和A4。
- 「有效的过滤区」默认为**C**。如果要打印日文字符，选择「**ja_JP**」。否则，接收默认的**C** 语区。
- 「介质源」默认为「打印机默认」。这个选项可以被改为使用另一个托盘中的纸张。

要修改驱动程序选项，点击「确定」来返回到主窗口。点击「应用」来保存改变并重新启动打印守护进程。

27.10. 保存配置文件

当你使用打印机配置工具保存打印机配置时，应用程序就会创建它自己的配置文件。这个配置文件被用来创建`/etc/cups`目录中的文件（或`lpd` 读取的`/etc/printcap` 文件）。你可以使用命令行选项来保存或恢复打印机配置工具文件。如果`/etc/cups`目录或`/etc/printcap` 文件被保存并恢复到同一位置，打印机配置就不会被恢复。这是由于打印机守护进程在每次重新启动时都会从打印机配置工具的特殊配置文件中创建一个新的`/etc/printcap` 文件。当创建系统配置文件的备份时，使用以下方法来保存打印机配置文件。如果系统使用的是LPRng 打印系统，并在`/etc/printcap.local` 文件中添加了定制设置，它应该被保存为备份系统的一部分。

要保存你的打印机配置，以根用户身份键入：

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

你的配置就会被保存到`settings.xml` 文件中。

如果这个文件被保存，它可以被用户恢复打印机设置。这在打印机配置被删除的情况下；或在重新安装了Red Hat Linux 的情况下；或在多个系统上需要同一打印机配置的情况下特别有用。在重新安装前，这个文件应该被保存在不同的系统上。要恢复配置，以根用户身份键入以下命令：

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

如果你已有了一个配置文件（你已经在系统上配置了一个或多个打印机），并想试图导入另一个配置文件，现存的配置文件就会被覆盖。如果你想保留现存配置，并在保存的文件中添加配置，你可以使用以下命令来合并文件（以根用户身份）：

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

然后，你的打印机列表就会包含你在系统上配置的打印机以及你从保存的配置文件中导入的打印机。如果导入的配置文件中有一个和系统上现存打印队列同名的队列，导入文件中的队列就会超越现存打印机。

导入了配置文件（不管有没有merge 命令），你都必须重新启动守护进程。如果你使用的是CUPS，执行以下命令：

```
/sbin/service cups restart
```

如果你使用的是LPRng，执行以下命令：

```
/sbin/service lpd restart
```

27.11. 命令行配置

如果你没有安装X，并且不想使用基于文本的程序，你可以通过命令行来添加打印机。这种方法在你从脚本中或kickstart 安装的%post 部分里添加打印机的时候很有用。

27.11.1. 添加本地打印机

要添加打印机，运行：

```
redhat-config-printer-tui --Xadd-local options
```

其选项有：

--device=*node*

‘ （必需）要使用的设备节点。例如：/dev/lp0。

--make=*make*

‘ （必需）IEEE 1284 MANUFACTURER 字符串或foomatic 数据库中的打印机生产厂商的名称（若无manufacturer 字符串）。

--model=*model*

‘ （必需）IEEE 1284 MODEL 字符串或foomatic 数据库中列出的打印机型号（若无model 字符串）。

--name=*name*

‘ （可选）新队列的名称。如果没有给定，将会使用基于设备节点（如“lp0”）的名称。

--as-default

‘ （可选）把它设为默认队列。

如果你使用的是CUPS 打印系统（默认），在添加了打印机后，使用以下命令来启动或重新启动打印机守护进程：

```
service cups restart
```

如果你使用的是LPRng 打印系统，在添加了打印机后，使用以下命令来启动或重新启动打印机守护进程：

```
service lpd restart
```

27.11.2. 删除本地打印机

你还可以通过命令行来删除打印机队列。

要以根用户身份来删除某个打印机队列，运行：

```
redhat-config-printer-tui --Xremove-local options
```

其选项有：

--device=*node*

‘ （必需）所用的设备节点，如/dev/lp0。

--make=*make*

‘ （必需）IEEE 1284 MANUFACTURER 字符串或foomatic 数据库中的打印机生产厂商的名称（若无manufacturer 字符串）。

--model=*model*

‘ （必需）IEEE 1284 MODEL 字符串或foomatic 数据库中列出的打印机型号（若无model 字符串）。

如果你使用的是CUPS 打印系统（默认），从打印机配置工具配置中删除了打印机后，使用以下命令来重新启动打印机守护进程而使改变生效：

```
service cups restart
```

如果你使用的是LPRng 打印系统，从打印机配置工具配置中删除了打印机后，使用以下命令来重新启动打印机守护进程而使改变生效：configuration, restart the printer daemon for the changes to take effect:

```
service lpd restart
```

如果你使用的是CUPS，删除了所有打印机后，你不打算再运行打印机守护进程了，执行以下命令：

```
service cups stop
```

如果你使用的是LPRng，删除了所有打印机后，你不打算再运行打印机守护进程了，执行以下命令：

```
service lpd stop
```

27.12. 管理打印作业

当你给打印机守护进程发送打印作业时（例如从**Emacs** 中打印文本文件或从**The GIMP** 中打印图像），这个打印作业被添加到打印假脱机队列中。打印假脱机队列是一个被发送给打印机的打印作业以及关于每个打印请求的信息的列表。这些信息包括打印请求的状态、发送请求的用户名、发送请求的系统主机名、作业号码等等。

如果你运行的是图形化桌面环境，点击面板上的「打印机管理器」图标来启动**GNOME** 打印管理器，如图27-13所示。

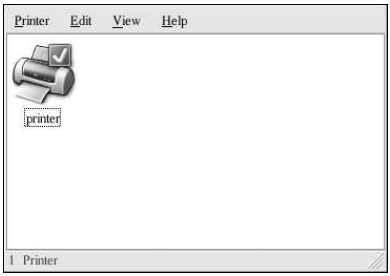


图**27-13. GNOME** 打印管理器

它还可以从面板上启动。点击「主菜单」 => 「系统工具」 => 「打印管理器」。

要改变打印机设置，右击打印机图标，然后选择「属性」。打印机配置工具就会被启动。

双击一个已配置的打印机来查看打印假脱机，如图27-14所示。

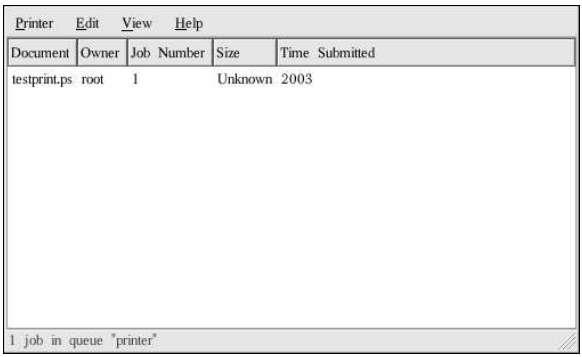


图**27-14.** 打印作业列表

要取消在**GNOME** 打印管理器中列出的某一作业，从列表中选择它，然后选择「编辑」 => 「取消文档」。

如果打印假脱机中有活跃的打印作业，打印机通知图标可能会出现在桌面面板上的「面板通知区域」，如图27-15所示。因为它每隔五秒探测一次打印作业，较短的打印作业可能不会显示图标。

图**27-15.** 打印机通知图标

点击打印机通知图标会启动**GNOME** 打印管理器来显示当前打印作业的列表。

面板上还有一个「打印管理器」图标。要从**Nautilus** 打印某文件，浏览该文件的位置，把它拖放到面板上的「打印管理器」图标。如图27-16所示的窗口就会出现。点击「确定」来开始打印这个文件。

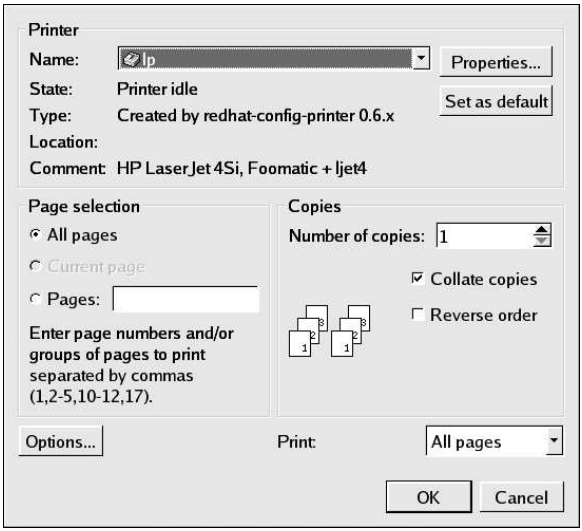


图**27-16.** 打印校验窗口

要从shell 提示查看打印假脱机中的打印作业列表，键入`lpq` 命令。最后几行和以下输出相似：

```
Rank  Owner/ID      Class Job Files    Size Time
active user@localhost+902  A  902 sample.txt 2050 01:20:46
```

例**27-1. `lpq` 的输出示例**

如果你想取消某个打印作业，使用`lpq` 命令找出这个作业的号码，然后使用`lprm` 作业号码。例如，`lprm 902` 会取消例27-1所示的打印作业。你必须具备正确的权限才能够取消某个打印作业。除非你在打印机所连接的计算机上登录为根用户，你不能取消被其他用户开始的打印作业。

你还可以直接从shell 提示下打印文件。例如，`lpr sample.txt` 命令会打印`sample.txt` 这个文本文件。打印过滤器决定文件的类型并将其转换成打印机能够理解的格式。

27.13. 共享打印机

打印机配置工具的共享配置选项能力只有在使用CUPS 打印系统时才有效。要配置LPRng 的共享，请参阅第27.13.1 节。

允许网络上不同计算机上的用户打印到你的系统上叫做共享（*sharing*）的打印机。按默认设置，使用打印机配置工具配置的打印机不是共享打印机。

要共享一个配置了的打印机，启动打印机配置工具，从列表中选择一个打印机。然后选择「行动」=>「共享」。

注记

如果没有选择打印机，「行动」 => 「共享」只显示系统范围内的共享选项，它们一般显示在「行动」活页标签中。

在「队列」活页标签上，选择使队列可被其他用户利用的选项。

图**27-17.** 队列选项

选择了要共享队列后，按照默认设置，所有主机都会被允许打印到共享打印机。允许网络上的所有系统都能够打印到队列中可能会很危险，特别是在系统直接连接到互联网的情况下。推荐你改变这个选项，方法是：选择「所有主机」，点击「编辑」按钮来显示如图27-18所示的窗口。

如果你在打印服务器上配置了防火墙，它必须能够在进入的UDP 端口631 上发送和接收连接。如果你在客户（发送打印请求的计算机）上配置了防火墙。它必须被允许在端口631 上发送和接收连接。

图**27-18.** 允许的主机

「常规」标签为所有打印机配置设置，包括那些打印机配置工具中看不到的打印机。其中有两个选项：

图**27-19.** 系统范围的共享选项

- 「自动寻找远程共享队列」 — 被默认选择。这个选项启用IPP 浏览，这意味着当网络上其它机器广播它们拥有的队列时，这些队列会被自动添加到系统的打印机列表中；由IPP 浏览所发现的打印机不需要额外的配置。该选项不自动共享本地系统上配置的打印机。
- 「启用**LPD** 协议」 — 该选项允许打印机使用`cups-lpd` 服务从配置使用LPD 协议的客户中接收打印作业。`cups-lpd` 服务是一种`xinetd` 服务。

警告

如果启用了该选项，从LPD 客户接收到的所有主机中的所有打印作业都会被接受。

27.13.1. 使用**LPRng** 共享打印机

如果你运行的是LPRng 打印系统，你可以手工地配置共享。要允许网络上的系统打印到Red Hat Linux 系统上配置的打印机，使用以下步骤：

1. 创建/etc/accepthost 文件。在这个文件中，添加你想允许打印访问的系统的IP 地址或主机名。每行一个IP 或主机名。
2. 在/etc/lpd.perms 中取消以下行的注释符号：
```
ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost
```
3. 重新启动守护进程来使改变生效：
```
service lpd restart
```

27.14. 切换打印系统

要切换打印系统，运行打印机系统切换器程序。选择面板上的「主菜单」 => 「系统设置」 => 「更多系统设置」 => 打印机系统切换器，或在shell 提示（如XTerm 或GNOME 终端）下键入redhat-switch-printer 命令。

这个程序自动检测X 窗口系统是否在运行。如果它在运行，程序就会在图形化模式中启动，如图27-20所示。如果X 没有被检测到，程序就会在文本模式中启动。要强制在文本模式中启动程序，使用redhat-switch-printer-nox 命令。

图27-20. 打印机系统切换器

选择**LPRng** 或**CUPS** 打印系统。在Red Hat Linux 9 中，CUPS 是默认的打印系统。如果你只安装了一个打印系统，它就是所显示的唯一选项。

如果你选择「确定」来改变打印系统，选定的打印守护进程就能够在引导时被启动，未选定的打印守护进程会被禁用，因此它不会在引导时被启动。选定的打印守护进程即刻被启用，未选定的打印守护进程即刻被停用，因此改变会立即生效。

27.15. 其它资料

要了解更多关于在Red Hat Linux 上打印的信息，请参考下列资料。

27.15.1. 安装了的文档

- `man printcap` — `/etc/printcap` 打印机配置文件的说明书页。
- `map lpr` — 允许你从命令行打印文件的 `lpr` 命令的说明书页。
- `man lpd` — LPRng 打印机守护进程的说明书页。
- `man lprm` — 用来从LPRng 假脱机队列中删除打印作业的命令行工具的说明书页。
- `man mpage` — 用来在一张纸上打印多页的命令行工具的说明书页。
- `man cupsd` — CUPS 打印机守护进程的说明书页。
- `man cupsd.conf` — CUPS 打印机守护进程配置文件的说明书页。
- `man classes.conf` — CUPS 类别配置文件的说明书页。

27.15.2. 有用的网站

- http://www.linuxprinting.org — *GNU/Linux Printing* 包含了大量关于在Linux 上打印的信息。
- http://www.cups.org/ — 关于CUPS 的文档、FAQ、和新闻组。

28. 自动化的任务

在Linux 中，任务可以被配置在指定的时间段、指定的日期、或系统平均载量低于指定的数量时自动运行。Red Hat Linux 预配置了对重要系统任务的运行，以便使系统能够时时被更新。譬如，被locate 命令使用的slocate 数据库每日都被更新。系统管理员可使用自动化的任务来执行定期备份、监控系统、运行定制脚本等等。

Red Hat Linux 随带四个自动化任务的工具：cron、anacron、at、和batch。

28.1. cron

cron 是一个可以用来根据时间、日期、月份、星期的组合来调度对重复任务的执行的守护进程。

cron 假定系统持续运行。如果当某任务被调度时系统不在运行，该任务就不会被执行。要根据时间段而非确切时间来配置任务，请参阅第28.2 节。要调度一次性的任务，请参阅第28.3 节。

要使用cron 服务，你必须安装了vixie-cron RPM 软件包，而且必须在运行crond 服务。要判定该软件包是否已安装，使用rpm -q vixie-cron 命令。要判定该服务是否在运行，使用/sbin/service crond status 命令。

28.1.1. 配置cron 任务

cron 的主配置文件是/etc/crontab，它包括下面几行：

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

前四行是用来配置cron 任务运行环境的变量。SHELL 变量的值告诉系统要使用哪个shell 环境（在这个例子里是bash shell）；PATH 变量定义用来执行命令的路径。cron 任务的输出被邮寄给MAILTO 变量定义的用户名。如果MAILTO 变量被定义为空白字符串（MAILTO=""），电子邮件就不会被寄出。HOME 变量可以用来设置在执行命令或脚本时使用的主目录。

/etc/crontab 文件中的每一行都代表一项任务，它的格式是：

```
minute hour day month dayofweek command
```

- minute — 分钟，从0 到59 之间的任何整数
- hour — 小时，从0 到23 之间的任何整数
- day — 日期，从1 到31 之间的任何整数（如果指定了月份，必须是该月份的有效日期）
- month — 月份，从1 到12 之间的任何整数（或使用月份的英文简写如jan、feb 等等）
- dayofweek — 星期，从0 到7 之间的任何整数，这里的0 或7 代表星期日（或使用星期的英文简写如sun、mon 等等）

- command — 要执行的命令（命令可以是ls /proc >> /tmp/proc之类的命令，也可以是执行你自行编写的脚本的命令。）

在以上任何值中，星号（*）可以用来代表所有有效的值。譬如，月份值中的星号意味着在满足其它制约条件后每月都执行该命令。

整数间的短线（-）指定一个整数范围。譬如，**1-4**意味着整数1、2、3、4。

用逗号（,）隔开的一系列值指定一个列表。譬如，**3, 4, 6, 8**标明这四个指定的整数。

正斜线（/）可以用来指定间隔频率。在范围后加上**/<*integer*>**意味着在范围内可以跳过integer。譬如，**0-59/2**可以用来在分钟字段定义每两分钟。间隔频率值还可以和星号一起使用。例如，***/3**的值可以用在月份字段中表示每三个月运行一次任务。

开头为井号（#）的行是注释，不会被处理。

如你在/etc/crontab文件中所见，它使用run-parts脚本来执行/etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly和/etc/cron.monthly目录中的脚本，这些脚本被相应地每小时、每日、每周、或每月执行。这些目录中的文件应该是shell脚本。

如果某cron任务需要根据调度来执行，而不是每小时、每日、每周、或每月地执行，它可以被添加到/etc/cron.d目录中。该目录中的所有文件使用和/etc/crontab中一样的语法。范例请参见例28-1。

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

例**28-1. crontab**的例子

根用户以外的用户可以使用crontab工具来配置cron任务。所有用户定义的crontab都被保存在/var/spool/cron目录中，并使用创建它们的用户身份来执行。要以某用户身份创建一个crontab项目，登录为该用户，然后键入crontab -e命令，使用由VISUAL或EDITOR环境变量指定的编辑器来编辑该用户的crontab。该文件使用的格式和/etc/crontab相同。当对crontab所做的改变被保存后，该crontab文件就会根据该用户名被保存，并写入文件/var/spool/cron/*username*中。

cron守护进程每分钟都检查/etc/crontab文件、etc/cron.d/目录、以及/var/spool/cron目录中的改变。如果发现了改变，它们就会被载入内存。这样，当某个crontab文件改变后就不必重新启动守护进程了。

28.1.2. 控制对cron的使用

/etc/cron.allow和/etc/cron.deny文件被用来限制对cron的使用。这两个使用控制文件的格式都是每行一个用户。两个文件都不允许空格。如果使用控制文件被修改了，cron守护进程（crond）不必被重启。使用控制文件在每次用户添加或删除一项cron任务时都会被读取。

无论使用控制文件中的规定如何，根用户都总是可以使用cron。

如果cron.allow文件存在，只有其中列出的用户才被允许使用cron，并且cron.deny文件会被忽略。

如果cron.allow文件不存在，所有在cron.deny中列出的用户都被禁止使用cron。

28.1.3. 启动和停止服务

要启动cron 服务，使用/sbin/service crond start 命令。要停止该服务，使用/sbin/service crond stop命令。推荐你在引导时启动该服务。关于如何在引导时自动启动cron 服务的详情，请参阅第14章。

28.2. anacron

anacron 是和cron 相似的任务调度器，只不过它并不要求系统持续运行。它可以用来运行通常由cron 运行的每日、每周、和每月的作业。

要使用anacron 服务，你必须安装了anacron RPM 软件包，而且anacron 服务必须在运行。要判定该软件包是否被安装，使用rpm -q anacron 命令。要判定该服务是否在运行，使用/sbin/service anacron status命令。

28.2.1. 配置anacron 任务

anacron 任务被列在配置文件/etc/anacrontab 中。文件中的每一行都代表一项任务，格式是：

```
period delay job-identifier command
```

- period — 命令执行的频率（天数）
- delay — 延迟时间（分钟）
- job-identifier — 任务的描述，用在anacron 的消息中，并作为作业时间戳文件的名称，只能包括非空白的字符（除斜线外）。
- command — 要执行的命令

对于每项任务，anacron 先判定该任务是否已在配置文件的period 字段中指定的期间内被执行了。如果它在给定期间内还没有被执行，anacron 会等待delay 字段中指定的分钟数，然后执行command 字段中指定的命令。

任务完成后，anacron 在/var/spool/anacron 目录内的时间戳文件中记录日期。只有日期被记录（无时间），而且job-identifier 的值被用作时间戳文件的名称。

和cron 配置文件一样，SHELL 和PATH 之类的环境变量可以在/etc/anacrontab 文件的前部定义。

默认的配置文件看起来和以下相似：

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1   5   cron.daily      run-parts /etc/cron.daily
7   10  cron.weekly     run-parts /etc/cron.weekly
30  15  cron.monthly    run-parts /etc/cron.monthly
```

图28-1. 默认的anacrontab

如你在图28-1 中所见，配置Red Hat Linux anacron 的目的是确保每日、每周、和每月的cron 任务都被运行。

28.2.2. 启动和停止服务

要启动anacron 服务，使用/sbin/service anacron start 命令。要停止该服务，使用/sbin/service anacron stop 命令。推荐你在引导时启动该服务。关于在引导时自动启动anacron 的详情，请参阅第14章。

28.3. at 和batch

cron 和anacron 被用来调度重复的任务，at 命令被用来在指定时间内调度一次性的任务。batch 命令被用来在系统平均载量降到0.8 以下时执行一次性的任务。

要使用at 或batch 命令，你必须安装了at RPM 软件包，并且atd 服务必须在运行。要判定该软件包是否被安装了，使用rpm -q at 命令。要判定该服务是否在运行，使用/sbin/service atd status 命令。

28.3.1. 配置at 作业

要在某一指定时间内调度一项一次性作业，键入at *time* 命令。这里的*time* 是执行命令的时间。*time* 参数可以是下面格式中任何一种：

- HH:MM 格式— 譬如，04:00 代表4:00AM。如果时间已过，它就会在第二天的这一时间执行。
- midnight — 代表12:00AM。
- noon — 代表12:00PM。
- teatime — 代表4:00PM。
- 英文月名日期年份格式— 譬如，January 15 2002 代表2002 年1 月15 日。年份可有可无。
- MMDDYY、MM/DD/YY、或MM.DD.YY 格式— 譬如，011502 代表2002 年1 月15 日。
- now + 时间— 时间以minutes、hours、days、或weeks 为单位。譬如，now + 5 days 代表命令应该在5 天之后的此时此刻执行。

时间必须要被先指定，接着是可有可无的日期。关于时间格式的详情，请阅读/usr/share/doc/at-<*version*> /timespec 文本文件。

键入了at 命令和它的时间参数后，at> 提示就会出现。键入要执行的命令，按[Enter] 键，然后键入Ctrl-D。你可以指定多条命令，方法是键入每一条命令后按[Enter] 键。键入所有命令后，按[Enter] 键转入一个空行，然后再键入Ctrl-D。或者，你也可以在提示后输入shell 脚本，在脚本的每一行后按[Enter] 键，然后在空行处键入Ctrl-D 来退出。如果输入的是脚本，所用的shell 就会是用户的SHELL 环境变量中设置的值，用户的登录shell，或是/bin/sh（使用最先发现的）。

如果这组命令或脚本试图在标准输出中显示信息，该输出会用电子邮件方式被邮寄给用户。

使用命令atq 来查看等待运行的作业。详情请参阅第28.3.3 节。

at 命令的用法能够被制约。详情请参阅第28.3.5 节。

28.3.2. 配置batch 作业

要在系统平均载量降到0.8 以下时执行某项一次性的任务，使用batch 命令。

键入batch 命令后，at> 提示就会出现。键入要执行的命令，按[Enter] 键，然后键入Ctrl-D。你可以指定多条命令，方法是键入每一条命令后按[Enter] 键。键入所有命令后，按[Enter] 键转入一个空行，然后再键入Ctrl-D。或者，你也可以在提示后输入shell 脚本，在脚本的每一行后按[Enter] 键，然后在空行处键入Ctrl-D 来退出。如果输入的是脚本，所用的shell 就会是用户的SHELL 环境变量中设置的值，用户的登录shell，或是/bin/sh（使用最先发现的）。系统平均载量一降到0.8 以下，这组命令或脚本就会被执行。

如果这组命令或脚本试图在标准输出中显示信息，该输出会用电子邮件方式被邮寄给用户。

使用命令atq 来查看等待运行的作业。详情请参阅第28.3.3 节。

batch 命令的用法能够被制约。详情请参阅第28.3.5 节。

28.3.3. 查看等待运行的作业

要查看等待运行的at 和batch 作业，使用atq 命令。它显示一列等待运行的作业，每项作业只占据一行。每一行的格式都是：作业号码、日期、小时、作业类别、以及用户名。用户只能查看他们自己的作业。如果根用户执行atq 命令，所有用户的全部作业都会被显示。

28.3.4. 其它的命令行选项

at 和batch 的其它命令行选项包括：

选项	描述
-f	从文件中读取命令或shell 脚本，而非在提示后指定它们。
-m	在作业完成后，给用户发送电子邮件。
-v	显示作业将被执行的时间。

表28-1. at 和batch 的命令行选项

28.3.5. 控制对at 和batch 的使用

/etc/at.allow 和/etc/at.deny 文件可以用来限制对at 和batch 命令的使用。这两个使用控制文件的格式都是每行一个用户。两个文件都不允许使用空白字符。如果使用控制文件被修改了，at 守护进程（atd）不必被重启。每次用户试图执行at 或batch 命令时，使用控制文件都会被读取。

不论使用控制文件如何规定，根用户都总是可以执行at 和batch 命令。

如果at.allow 文件存在，只有其中列出的用户才能使用at 或batch 命令，at.deny 文件会被忽略。

如果at.allow 文件不存在，所有在at.deny 文件中列出的用户都被禁止使用at 和batch 命令。

28.3.6. 启动和停止服务

要启动at 服务，使用/sbin/service atd start 命令。要停止该服务，使用/sbin/service atd stop 命令。建议你在引导时启动该服务。关于在引导时自动启动at 服务的详情，请参阅第14章。

28.4. 其它资料

要了解更多关于配置自动化任务的知识，请参阅下列资料。

28.4.1. 安装了的文档

- cron 的说明书（man）页— 对cron 的总述。
- crontab 的说明书（man）页，第1 和第5 章— 第1 章的说明书页包含对crontab 文件的总述。第5 章包含文件的格式，以及一些范例。
- /usr/share/doc/at-<*version*>/timespec 包含了关于可为cron 作业指定的时间格式的更详细信息。
- anacron 的说明书（man）页— 对anacron 和它的命令行选项的描述。
- anacrontab 的说明书（man）页— 对anacron 配置文件的概述。
- /usr/share/doc/anacron-<*version*>/README — 描述了anacron 及其用途。
- at 的说明书（man）页— 对at 和batch 命令以及它们的命令行选项的描述。

29. 日志文件

日志文件（*Log files*）是包含关于系统消息的文件，包括内核、服务、在系统上运行的应用程序等。不同的日志文件记载不同的信息。例如，有的是默认的系统日志文件，有的仅用于安全消息，有的记载cron 任务的日志。

当你在试图诊断和解决系统问题时，如试图载入内核驱动程序或寻找对系统未经授权的使用企图时，日志文件会很有用。本章讨论要到哪里去寻找日志文件，如何查看日志文件，以及在日志文件中查看什么。

某些日志文件被叫做syslogd 的守护进程控制。被syslogd 维护的日志消息列表可以在/etc/syslog.conf 配置文件中找到。

29.1. 定位日志文件

多数日志文件位于/var/log 目录中。某些程序如httpd 和samba 在/var/log 中有单独的存放它们自己的日志文件的目录。

注意，日志文件目录中会有多个后面带有数字的文件。这些文件是在日志文件被循环时创建的。日志文件被循环使用，因此文件不会变得太大。logrotate 软件包中包含一个能够自动根据/etc/logrotate.conf 配置文件和/etc/logrotate.d 目录中的配置文件来循环日志文件的cron 任务。按照默认配置，日志每周都被循环，并被保留四周之久。

29.2. 查看日志文件

多数日志文件使用纯文本格式。你可以使用任何文本编辑器如**Vi** 或**Emacs** 来查看它们。某些日志文件可以被系统上所有用户查看；不过，你需要拥有根特权来阅读多数日志文件。

要在互动的、真实时间的应用程序中查看系统日志文件，使用日志查看器。要启动这个应用程序，点击面板上的「主菜单」 => 「系统工具」 => 「系统日志」，或在shell 提示下键入redhat-logviewer 命令。

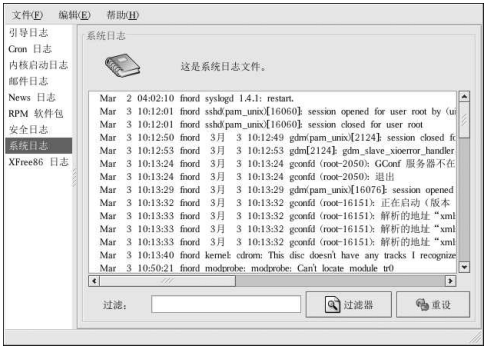


图**29-1.** 日志查看器

这个应用程序只能显示存在的日志文件；因此，其列表可能会与图29-1所示的略有不同。要查看它能够查看的完整日志列表，请参见配置文件/etc/sysconfig/redhat-logviewer。

按照默认设置，当前的可查看的日志文件每隔30 秒被刷新一次。要改变刷新率，从下拉菜单中选择「编辑」 => 「首选项」。如图29-2所示的窗口会出现。在「日志文件」标签中，点击刷新率旁边的上下箭头来改变它。点击「关闭」来返回到主窗口。刷新率会被立即改变。要手工刷新当前可以查看的文件，选择「文件」 => 「即刻刷新」或按[Ctrl]-[R]。

要过滤日志文件的内容来查找关键字，在「过滤：」文本字段中输入关键字，然后点击「过滤器」。点击「重设」来重设内容。

你可以在「日志文件」标签中改变程序所要查找日志文件的位置。从列表中选择日志文件，然后点击「改变位置」按钮。键入日志文件的新位置，或点击「浏览」按钮来从文件选择对话框中定位文件位置。点击「确定」来返回到首选项窗口，然后点击「关闭」来返回到主窗口。

图**29-2.** 日志文件的位置

29.3. 检查日志文件

日志查看器可以被配置在包含警告关键字的行旁边来显示警告图标。要添加警告词，从下拉菜单中选择「编辑」 => 「首选项」，然后点击「警告」标签。点击「添加」按钮来添加警告词。要删除一个警告词，从列表中选择它，然后点击「删除」。

图**29-3.** 警告

30. 升级内核

为了确保内核的完整性和对它所支持的硬件的兼容性，Red Hat Linux 内核由Red Hat 内核小组定制建构。在内核被Red Hat 发行之前，它一定要通过一系列严格的质量保证测试。

Red Hat Linux 内核使用RPM 格式打包，因而它们易于升级和校验。例如，由Red Hat, Inc. 发行的`kernel` RPM 软件包被安装后，`initrd` 映像会被创建；这样，在你安装了不同的内核后，你就没必要使用`mkinitrd` 命令。如果你安装了GRUB 或LILO 的话，它还会修改引导装载程序的配置文件来包括这个新内核。

本章仅讨论在x86 系统上升级内核的必要步骤。


警告

建构你自行定制的内核是不被Red Hat Linux 安装支持组支持的。关于从源码中建构定制内核的详情，请参阅附录A。

30.1. 2.4 版本的内核

Red Hat Linux 随带定制的2.4 内核，它包括以下功能：

- 内核源码的目录是`/usr/src/linux-2.4/`，而不是`/usr/src/linux/`。
- 对ext3 文件系统的支持。
- 对多重处理器（SMP）的支持。
- 对USB 的支持。
- 对IEEE 1394 设备（又称FireWire™）的初步支持。

30.2. 准备升级

在你升级内核之前，你应该先采取几项预防措施。第一步是确定你有一张适用于你的系统的可运行的引导盘以防万一出现问题。如果引导装载程序没有被正确配置来引导新内核，除非你有引导盘，否则就无法引导系统。

要创建引导盘，在shell 提示下登录为根用户，然后键入以下命令：

```
/sbin/mkbootdisk `uname -r`
```


窍门

请参考`mkbootdisk` 的说明书页（man）来阅读更多选项。

在继续前，使用引导盘来重新引导你的机器以校验该软盘的可运行性。

但愿你不必使用引导盘，但是你应该把它存放在一个安全的地方以防万一。

要判定你已安装了哪些内核软件包，在shell 提示下执行下面的命令：

```
rpm -qa | grep kernel
```

依据你执行的安装类型而定（你的版本号码和软件包可能不同），该命令的输出会包括某些或全部在下面列出的软件包：

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

从输出中，你可以判定你需要下载哪些软件包来执行内核升级。对于单处理器系统而言，只有`kernel`软件包是必需的。

如果你的计算机不只有一个处理器，你需要包括支持多处理器的`kernel-smp`软件包。强烈建议你仍安装`kernel`软件包，以防万一多处理器内核不能在你的系统中正确运行。

如果你的计算机的内存超过了4GB，你必须安装`kernel-bigmem`软件包才能使系统使用多于4GB的内存。强烈建议你仍旧安装`kernel`软件包以用于调试。`kernel-bigmem`软件包仅为i686体系建构。

如果你需要PCMCIA支持（例如在便携电脑上），`kernel-pcmcia-cs`软件包就必不可少。

除非你想重新编译内核，或把系统用于内核开发，你不需要`kernel-source`软件包。

`kernel-doc`软件包包括内核开发文档，它不是必需的。如果你的系统被用于内核开发，则推荐你安装它。

`kernel-util`软件包包括能够用来控制内核或系统硬件的工具程序，它也不是必需的。

Red Hat建构的内核为不同的x86版本做了优化。选项有：用于AMD Athlon™ 和AMD Duron™ 系统的`athlon`；用于Intel® Pentium® II、Intel® Pentium® III、和Intel® Pentium® 4 系统的`i686`；用于Intel® Pentium® 和AMD K6™ 系统的`i586`。如果你不知道你的x86 系统的版本，使用为`i386`版本建构的内核；它是为所有基于x86 的系统建构的。

RPM 软件包的x86 版本被包括在文件名中。例如：`kernel-2.4.20-2.47.1.athlon.rpm` 是为AMD Athlon™ 和AMD Duron™ 系统优化的，`kernel-2.4.20-2.47.1.i686.rpm` 是为Intel® Pentium® II、Intel® Pentium® III、和Intel® Pentium® 4 系统优化的。在你判定了软件包之后，你需要升级内核，为`kernel`、`kernel-smp`、和`kernel-bigmem`软件包选择正确的体系。其它软件包使用`i386`版本。

30.3. 下载升级了的内核

要判定是否有可用于你的系统的升级内核，方法有好几种。

- 进入http://www.redhat.com/apps/support/errata/ 网站，选择你使用的Red Hat Linux 版本，然后查看它的勘误。内核勘误通常在安全顾问（**Security Advisories**）部分下。从勘误列表中点击内核勘误来查看它的详细勘误报告。在勘误报告中，有一个需要的RPM 列表，以及从Red Hat FTP 站点下载它们的链接。你还可以从Red Hat FTP 的镜像站点中下载它们。镜像站点的列表在http://www.redhat.com/download/mirror.html 中。
- 使用Red Hat 网络来下载内核RPM 软件包并安装它们。Red Hat 网络能够下载最新的内核、升级系统上的内核、如果必要，创建初始RAM 映像，并配置引导装载程序来载入新内核。要获取更多信息，请参阅 http://www.redhat.com/docs/manuals/RHNetwork/ 上的*Red Hat* 网络*User Reference Guide*。

如果你从Red Hat Linux 的勘误网页上下载了RPM 软件包，或只使用了Red Hat 网络来下载软件包，继续阅读第30.4 节。如果你使用了Red Hat 网络来下载并安装更新了的内核，遵循第30.5 节和第30.6 节中的说明。只不过，不要把内核改成默认引导项，因为Red Hat 网络会自动把默认内核改成最新版本。

30.4. 执行升级

检索到所有必要的软件包后，你就可以开始升级现存内核了。在shell 提示下登录为根用户，转换到包含内核RPM 软件包的目录中，遵循以下步骤：


重要

强烈建议你保留旧内核，以防万一新内核出现问题。

使用rpm 命令的-i 选项来保留就内核。如果你使用了-U 选项来升级kernel软件包，它会覆盖当前安装了的内核。该命令为（内核版本和x86 版本会有所不同）：

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

如果系统是多处理器系统，还需安装kernel-smp 软件包（内核版本和x86 版本会有所不同）：

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

如果系统是基于i686 的，并包含超过4GB 的内存，还需安装为i686 体系建构的kernel-bigmem 软件包（内核版本和x86 版本会有所不同）：

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

如果你打算升级kernel-source、kernel-docs、或kernel-utils 软件包，你可能不需要保留老版本。使用下面的命令来升级这些软件包（版本会有所不同）：

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

如果系统需要PCMCIA 支持（例如便携电脑），你还需要安装kernel-pcmcia-cs 并保留老版本。如果你使用了-i 选项，它可能会返回冲突，因为老内核需要该软件包来引导带有PCMCIA 支持的系统。要绕过这个问题，使用--force 选项，如下所示（版本会有所不同）：

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

下一步是校验初始RAM 磁盘映像是否被创建。详情请参阅第30.5 节。

30.5. 校验初始RAM 磁盘映像

如果系统使用ext3 文件系统或SCSI 控制器，你就需要初始RAM 磁盘。初始RAM 磁盘的目的是允许模块化的内核在它能够进入模块通常驻留的设备之前具备进入内核需要从该设备引导的模块的能力。

初始RAM 磁盘通过使用mkinitrd 命令来创建。然而，如果内核及其相关文件是从Red Hat, Inc. 发行的RPM 软件包中安装或升级的话，这个步骤会被自动执行；因此，它不必被手工进行。要校验它是否被创建了，使用ls -l /boot 命令来确定initrd-2.4.20-2.47.1.img文件被创建了（版本应该匹配刚刚安装了的内核的版本）。

下一步是校验引导装载程序已被配置来引导新内核。详情请参阅第30.6 节。

30.6. 校验引导装载程序

如果你安装了GRUB 或LILO 引导装载程序，kernel RPM 软件包配置它们来引导刚刚安装的内核，但是它并不配置引导装载程序默认引导新内核。

确认一下引导装载程序已被配置成引导新内核总是值得提倡的。这是至关重要的一步。如果引导装载程序被配置得不正确，你将无法引导你的系统。若这种情况发生了，使用你从前创建的引导盘来引导你的系统，然后再试图配置你的引导装载程序。

30.6.1. GRUB

如果你选择了GRUB 作为引导装载程序，请确认/boot/grub/grub.conf 文件中包含的title 部分中的版本与你刚刚安装的kernel 软件包的版本相同（如果你安装了kernel-smp 和/或kernel-bigmem，你也会看到这个部分）：

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#     all kernel and initrd paths are relative to /boot/, eg.
#     root (hd0,0)
#     kernel /vmlinuz-version ro root=/dev/hda2
#     initrd /initrd-version.img
#boot=/dev/hda
default=3
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
    initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
    initrd /initrd-2.4.20-2.30.img
```

如果你创建了单独的/boot 分区，到内核与initrd 映像的路径是相对于/boot 分区而言的。

注意，默认引导项目没有被设置为新内核。要配置GRUB 来默认引导新内核，把default 变量的值改成包含新内核的title 部分的号码。这个号码从0 开始。例如，如果新内核是第二个title 部分，把default 设置为**1**。

你可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

30.6.2. LILO

如果你选择了LILO 作为引导装载程序，请确认/etc/lilo.conf 文件中包含的image 部分中的版本与你刚刚安装的kernel 软件包的版本相同（如果你安装了kernel-smp 和/或kernel-bigmem，你也会看到这个部分）：

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
    label=2.4.20-2.47.1
```

```
    initrd=/boot/initrd-2.4.20-2.47.1.img
    read-only
    append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
    label=2.4.20-2.30
    initrd=/boot/initrd-2.4.20-2.30.img
    read-only
    append="root=LABEL=/"
```

注意，默认引导项目没有被设置为新内核。要配置LILO 来默认引导新内核，把default 变量的值改成包含新内核的image 部分中的label 的值。以根用户身份运行/sbin/lilo 命令来启用改变。运行后，其输出会与如下相似：

```
Added 2.4.20-2.47.1 *
Added linux
```

2.4.20-2.47.1 后面的* 意味著那部分中的内核是LILO 会默认引导的内核。

你可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

31. 内核模块

Linux 内核具有模块化设计。在引导时，只有少量的驻留内核被载入内存。这之后，无论何时用户要求使用驻留内核中没有的功能，某内核模块（*kernel module*），有时又称驱动程序（*driver*）。就会被动态地载入内存。

在安装过程中，系统上的硬件会被探测。基于探测结果和用户提供的信息，安装程序会决定哪些模块需要在引导时被载入。安装程序会设置动态载入机制来透明地运行。

如果安装后添加了新硬件，而这个硬件需要一个内核模块，系统必须被配置来为新硬件载入正确的内核模块。当系统使用新硬件引导后，**Kudzu** 程序会运行，如果新硬件被支持，它就会被检测到，该程序还会为它配置模块。你也可以通过编辑模块配置文件`/etc/modules.conf` 来手工指定这个模块。

注记

用来显示X 窗口系统界面的视频卡模块是`XFree86` 软件包的一部分，而不是内核的一部分；因此，本章并不应用于该模块。

例如，如果某系统包括了一个SMC EtherPower 10 PCI 网卡，模块配置文件包含以下行：

```
alias eth0 tulip
```

如果系统上添加了第二个网卡，它和第一个网卡一模一样，在`/etc/modules.conf` 中添加这一行：

```
alias eth1 tulip
```

要获得内核模块的字母顺序列表以及这些模块所支持的硬件，请参阅《*Red Hat Linux* 参考指南》。

31.1. 内核模块工具

如果安装了`modutils` 软件包，你还可以使用一组管理内核模块的命令。使用这些命令来判定模块是否被成功地载入了，或为一件新硬件试验不同的模块。

`/sbin/lsmod` 命令显示了当前载入了的模块列表。例如：

```
Module        Size Used by  Not tainted
iptable_filter    2412  0 (autoclean) (unused)
ip_tables      15864  1 [iptable_filter]
nfs         84632  1 (autoclean)
lockd        59536  1 (autoclean) [nfs]
sunrpc       87452  1 (autoclean) [nfs lockd]
soundcore       7044  0 (autoclean)
ide-cd       35836  0 (autoclean)
cdrom        34144  0 (autoclean) [ide-cd]
parport_pc      19204  1 (autoclean)
lp          9188  0 (autoclean)
parport      39072  1 (autoclean) [parport_pc lp]
autofs       13692  0 (autoclean) (unused)
e100         62148  1
```

```
microcode       5184  0 (autoclean)
keybdev         2976  0 (unused)
mousedev        5656  1
hid            22308  0 (unused)
input           6208  0 [keybdev mousedev hid]
usb-uhci       27468  0 (unused)
usbcore        82752  1 [hid usb-uhci]
ext3           91464  2
jbd            56336  2 [ext3]
```

对每行而言，第一列是模块名称；第二列是模块大小；第三列是用量计数。

用量计数后面的信息对每个模块而言都有所不同。如果(unused)被列在某模块的那行中，该模块当前就没在使用。如果(autoclean)被列在某模块的那行中，该模块可以被rmmod -a命令自动清洗。当这个命令被执行后，所有自从上次被自动清洗后未被使用的被标记了“autoclean”的模块都会被卸载。Red Hat Linux 不默认执行自动清洗行动。

如果模块名称被列举在行尾的括号内，括号内的模块就依赖于列举在这一行的第一列中的模块。例如，在以下行中：

```
usbcore        82752  1 [hid usb-uhci]
```

hid 和usb-uhci 内核模块依赖于usbcore 模块。

/sbin/lsmod 输出和查看/proc/modules 的输出相同。

要载入内核模块，使用/sbin/modprobe 命令，然后跟着内核模块的名称。按照默认设置，modprobe 试图从/lib/modules/<*kernel-version*>/kernel/drivers/ 子目录中载入模块。每类模块都有一个子目录，如用于网络接口驱动程序的net/ 子目录。某些内核模块有模块依赖关系，这意味着你必须首先载入其它模块才能载入这些模块。/sbin/modprobe 命令检查这些依赖关系，并在载入指定模块前载入满足这些依赖关系的模块。

例如：

```
/sbin/modprobe hid
```

这个命令载入任何满足依赖关系的模块，然后再载入hid 模块。

要在/sbin/modprobe 执行命令的时候把它们都显示在屏幕上，使用-v 选项。例如：

```
/sbin/modprobe -v hid
```

所显示的输出和下面相似：

```
/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

你还可以使用/sbin/insmod 命令来载入内核模块；不过它不解决依赖关系。因此，推荐你使用/sbin/modprobe 命令。

要卸载内核模块，使用/sbin/rmmod 命令和模块名称。rmmod 工具只卸载不在使用的、和不是被正使用的模块所依赖的模块。

例如：

```
/sbin/rmmod hid
```

这个命令卸载hid 内核模块。

另一个有用的模块工具是modinfo。使用/sbin/modinfo 命令来显示关于内核模块的信息。一般语法是：

`/sbin/modinfo [options] <module>`

包括-d 在内的选项显示了关于模块的简短描述，-p 选项列举了模块所支持的参数。要获取选项的完整列表，请参阅modinfo 的说明书页（man modinfo）。

31.2. 其它资料

关于内核模块和它们的工具的更多信息，请参考以下资料。

31.2.1. 安装了的文档

- lsmod 的说明书页（man）— 对它的输出的描述和解释。
- insmod 的说明书页（man）— 对命令行选项的描述和列举。
- modprobe 的说明书页（man）— 对命令行选项的描述和列举。
- rmmod 的说明书页（man）— 对命令行选项的描述和列举。
- modinfo 的说明书页（man）— 对命令行选项的描述和列举。
- /usr/src/linux-2.4/Documentation/modules.txt — 如何编译和使用内核模块。

31.2.2. 有用的网站

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — 来自Linux 文档计划的*Linux Loadable Kernel Module HOWTO*。

V. 软件包管理

Red Hat Linux 系统上的所有软件都被分成可被安装、升级、或删除的RPM 软件包。这个部分描述了如何使用图形化和命令行工具来管理Red Hat Linux 系统上的RPM 软件包。

目录

redhat.

32.

使用RPM 来管理软件包

RPM 软件包管理器（RPM）是开放打包系统，任何人都可以使用。它在Red Hat Linux，以及其它Linux 和UNIX 系统上运行。Red Hat, Inc. 鼓励其它销售商在他们自己的产品上使用RPM 技术。RPM 按照GPL 条款被发行。

对于终端用户来说，RPM 简化了系统更新。安装、删除安装、升级RPM 软件包可以使用简短的命令就可完成。RPM 维护一个已安装软件包和它们的文件的数据库，因此，你可以在系统上使用功能强大的查询和校验。如果你更喜欢图形化界面，你可以使用软件包管理工具来执行许多RPM 命令。详情请参阅第33章。

在升级中，RPM 处理配置文件时非常谨慎，因此你决不会丢失你定制的配置— 这是你用普通的`.tar.gz` 文件所无法达到的。

对于开发者来说，RPM允许你把软件编码和程序打包，然后提供给终端用户。这个进程非常简单，它能从你创建的单个文件或补丁中驱动。这种对你的“纯净”源码、补丁和建构指令的清晰描述减轻了发行软件新版本所带来的维护负担。

注记

因为RPM 要对你的系统做适当改变，你必须是根用户才能安装、删除、或升级某个RPM 软件包。

32.1. RPM 的设计目标

为了理解如何使用RPM，我们应该先来了解RPM 的设计目标：

可升级性

- 使用RPM，你可以不必全盘重装就可以在系统上升级个别组件。当你得到一个基于RPM 的操作系统的新发行版本（如Red Hat Linux），你不必重新安装你的系统（基于其它打包系统的操作系统需要重装）。RPM 允许智能化、自动化地就地升级你的系统。软件包中的配置文件在升级中被保留，因此你不会丢失定制的设置。你不需要特殊的升级文件来升级某软件包，因为在系统上安装和升级软件包使用同样的RPM 文件。

强大的查询功能

- RPM 被设计来提供强大的查询功能。你可以在整个数据库中搜索软件包或某些特定文件。你还可以轻易地了解到哪个文件属于哪个软件包，软件包来自哪里。RPM 软件包的文件包括在被压缩的归档中，其中有定制的二进制档头，该档头内包含关于软件包及其内容的信息，允许你快速简捷地查询个体软件包。

系统校验

- 另一项强大的功能是软件包校验。如果你担心你可能删除了某软件包上的一个重要文件，只需校验该软件包即可。任何异常情况都会向你通知。到时，你可以在必要时重装该软件包。你修改过的配置文件在重装中会被保留。

纯净源码

- 一个重要的设计目标是允许使用与软件的原创者所发行源码一致的“纯净”软件源码。使用RPM，你会有纯净源码、使用过的补丁、以及完整的建构指令。这是一个重要的优越性。首先，如果程序的新版本被推出，你不必从头开始编译。你可以看一看补丁来判定你可能需

要做什么。使用这种技术，所有内编译的默认值，以及为正确建构软件而进行的任何改变都一目了然。

保持源码纯净的目的似乎只对开发者来说是重要的，但是它也会给终端用户带来高质量的软件。我们想在此感谢BOGUS 的发行人员，感谢他们最先开创了纯净源码这一概念。

32.2. 使用RPM

RPM 有五种基本操作模式（不包括软件包建构）：安装、删除安装、升级、查询和校验。本章节包括对每一模式的总览。想了解完整的选项和细节，请使用`rpm --help`命令，或阅读第32.5 节中关于RPM 的信息。

32.2.1. 寻找RPM 软件包

在使用RPM 之前，你必须知道要到哪里去寻找它们。在互联网上搜索会返回许多RPM 仓库，但是如果你要找的是由Red Hat 建构的RPM 软件包，你可以在下面几个地方找到它们：

- Red Hat Linux 光盘
- Red Hat 勘误网页：http://www.redhat.com/apps/support/errata/
- Red Hat FTP 镜像网站：http://www.redhat.com/download/mirror.html
- Red Hat 网络— 关于Red Hat 网络的详情，请参阅第34章。

32.2.2. 安装

典型的RPM 软件包名称类似于`foo-1.0-1.i386.rpm`。该文件名包括软件包名称（`foo`）、版本（`1.0`）、发行版本（`1`）、以及体系（`i386`）。安装软件包简单之极，登录为根用户，然后在shell 提示下键入下面的命令：

```
rpm -Uvh foo-1.0-1.i386.rpm
```

如果安装成功，你会看到如下所示的输出：

```
Preparing...        ########################################### [100%]
   1:foo            ########################################### [100%]
```

如上面所示，RPM 显示软件包的名称，然后在软件包被安装时在屏幕上打印井号来显示安装进度。

从RPM 版本4.1 开始，在安装或升级软件包时会检查软件包的签名。如果签名校验失败，你就会看到如下所示的错误消息：

```
error: V3 DSA signature: BAD, key ID 0352860f
```

如果它是新的、只针对文件头的签名，你会看到如下所示的错误消息：

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

如果你没有安装合适的钥匙来校验签名，消息中就会包含`NOKEY`，如：

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

关于校验软件包签名的详细信息，请参阅第32.3 节。

注记

如果你要安装内核软件包，你应该使用rpm -ivh。详情请参阅第30章。

虽然安装软件包旨在简单易行，但是你有时也会看到错误。

32.2.2.1. 软件包已安装

如果某软件包的同一版本已经安装，你就会看到：

```
Preparing...        ########################################### [100%]
package foo-1.0-1 is already installed
```

如果你在软件包已安装的情况下仍打算安装同一版本的软件包，你可以使用--replacepkgs 选项，它告诉RPM 来忽略这个错误：

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

如果从RPM 安装的文件被删除了，或者你想安装RPM 中的最初配置文件，该选项就会很有用。

32.2.2.2. 文件冲突

如果你试图安装的软件包中包含已被另一个软件包或同一软件包的早期版本安装了的文件，你会看到：

```
Preparing...        ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

要使RPM 忽略这个错误，使用--replacefiles 选项：

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

32.2.2.3. 未解决的依赖关系

RPM 软件包可能“依赖”于其它软件包，这意味着它们需要安装其它软件包才能正确运行。如果你试图安装具有未解决依赖关系的软件包，你会看到：

```
Preparing...        ########################################### [100%]
error: Failed dependencies:
    bar.so.2 is needed by foo-1.0-1
  Suggested resolutions:
    bar-2.0.20-3.i386.rpm
```

如果你安装的是Red Hat，它通常会向你建议解决依赖关系所需的软件包。在Red Hat Linux 光盘或Red Hat FTP 站点（或镜像）上找到这个软件包，使用以下命令来添加：

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

如果这两个软件包都安装成功，你会看到：

```
Preparing...        ########################################### [100%]
   1:foo        ########################################### [ 50%]
   2:bar        ########################################### [100%]
```

如果它不向你建议解决依赖关系所需的软件包，你可以试用--redhatprovides 选项来判定哪个软件包包含所需的文件。你需要安装rpmdb-redhat 软件包才能使用这个选项。

```
rpm -q --redhatprovides bar.so.2
```

如果包含bar.so.2 的软件包在来自rpmdb-redhat 软件包的安装了的数据库中，该软件包的名称就会被显示：

```
bar-2.0.20-3.i386.rpm
```

如果你想强制安装（不是好办法，因为软件包可能不能够正确运行），使用--nodeps 选项。

32.2.3. 删除安装

删除软件包和安装软件包一样简单。在shell 提示下键入下面的命令：

```
rpm -e foo
```

注记

注意，我们使用软件包名称 foo，而不是原始的软件包文件 foo-1.0-1.i386.rpm。要删除某软件包，你需要把foo 换成原始软件包的实际名称。

你在删除安装某软件包时也会遇到依赖关系错误，当另一个已安装的软件包依赖于你试图删除的软件包时，依赖关系错误就会发生。例如：

```
Preparing...        ########################################### [100%]
error: removing these packages would break dependencies:
    foo is needed by bar-2.0.20-3.i386.rpm
```

要使RPM 忽略这个错误，并强制删除该软件包（不是个好办法，因为依赖于它的软件包可能无法正常运行），使用--nodeps 选项。

32.2.4. 升级

升级软件包和安装类似。在shell 提示下键入以下命令：

```
rpm -Uvh foo-2.0-1.i386.rpm
```

你在上面的例子里看不到的是，RPM 自动删除foo 软件包的任何老版本。事实上，你可能想一直使用-U 来安装软件包，因为即便没有安装软件包的任何先前版本，它也可以用来安装该软件包。

因为RPM 对软件包和配置文件执行智能升级，你可能会看到和下面相似的消息：

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

这条消息意味着你对配置文件所作的改变可能不会和软件包中的新配置文件“前向兼容”，因此，RPM 保存了你的原始文件，并安装了一个新文件。你应该调查一下这两个配置文件的区别，然后尽快地解决这些区别来确保系统继续正确运行。

升级实际上是删除和安装的组合，因此，在RPM 升级中，你除了遇到删除和安装中会遇到的错误外，还会看到另一个错误。如果RPM 认为你试图升级到软件包的老版本，你会看到：

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

要使RPM 强制“升级”，使用--oldpackage 选项：

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

32.2.5. 刷新

刷新软件包和升级软件包相似。在shell 提示下键入以下命令：

```
rpm -Fvh foo-1.2-1.i386.rpm
```

RPM 的刷新选项比较在命令行上指定的软件包的版本和你的系统上已安装的版本。当RPM 的刷新选项处理的版本比你已安装的版本更新，它就会被升级到更新的版本。然而，如果某软件包先前没有安装，RPM 的刷新选项将不会安装该软件包。这和RPM 的升级选项不同，因为不管该软件包的老版本是否已被安装，升级选项都会安装该软件包。

RPM 的刷新选项可以用于单个软件包或一组软件包。如果你刚刚下载了大量不同的软件包，你只想升级那些已安装在你的系统上的软件包，刷新即可达到目的。如果使用刷新，你不必在使用RPM 前从下载的软件包组中删除不必要的软件包。

在这种情况下，你单使用下面的命令就可以了：

```
rpm -Fvh *.rpm
```

RPM 将只会自动升级那些已经在系统上安装的软件包。

32.2.6. 查询

使用rpm -q 命令来查询安装的软件包的数据库。rpm -q foo 命令会显示安装的软件包foo 的名称、版本、和发行号码：

```
foo-2.0-1
```

注记

注意，我们使用的是软件包名称 foo。要查询软件包，你需要把foo 换成实际软件包名称。

与其指定软件包名称，你可以和-q 一起使用下列选项来指定你要查询的软件包。它们叫做软件包指定选项。

- -a 查询所有已安装的软件包。
- -f <*file*> 会查询拥有<*file*> 的软件包。当指定文件时，你必须指定文件的完整路径（如/usr/bin/ls）。
- -p <*packagefile*> 查询软件包<*packagefile*>。

指定被查询的软件包要显示哪些信息的方法多种多样。以下选项用来选择你要搜索的信息类型。它们叫做信息选择选项。

- -i 显示软件包信息，包括名称、描述、发行版本、大小、制造日期、生产商，以及其它杂项。

- -l 显示软件包所含的文件列表。
- -s 显示软件包中所有文件的状态。
- -d 显示被标记为文档（man 页、info 页、README 等等）的文件列表。
- -c 显示被标记为配置文件的文件列表。你在安装后改变这些文件来使软件包适用于你的系统（譬如，sendmail.cf、passwd、inittab 等等）。

对于用来显示文件列表的选项，你可以在命令后添加-v 来用你熟悉的ls -l 格式来显示文件列表。

32.2.7. 校验

校验软件包比较从某软件包安装的文件和原始软件包中的同一文件的信息。它校验每个文件的大小、MD5 值、权限、类型、所有者、以及组群。

rpm -V 命令校验软件包。你可以查询任何软件包选择选项列举的条目来指定要校验的软件包。校验的最简单用法是rpm -V foo，它校验所有在foo 软件包内的文件是否和最初安装时一样。例如：

- 要校验包含某一特定文件的软件包：
  rpm -Vf /bin/vi
- 要校验所有安装了的软件包：
  rpm -Va
- 要根据RPM 软件包文件来校验安装了的软件包：
  rpm -Vp foo-1.0-1.i386.rpm

  如果你怀疑RPM 数据库已被损坏，该命令就会很有用。

如果一切都被校验正确，就不会有输出。如果出现矛盾，它们就会被显示。输出的格式为包括八个字符的字符串（c 代表配置文件），然后是文件名称。这八个字符的每个字符都代表一种文件属性的比较结果，所比较的是文件的属性和RPM 数据库中记录的属性。单用一个.（点）意味着测试通过。下列字符代表某类测试失败：

- 5 — MD5 校验和
- S — 文件大小
- L — 符号链接
- T — 文件修改时间
- D — 设备
- U — 用户
- G — 组群
- M — 模式（包括权限和文件类型）
- ? — 不可读文件

如果你看到任何输出，最好开动脑筋来判断是应该删除还是重新安装该软件包，或用另一种方法来解决这个问题。

32.3. 检查软件包的签名

如果你想校验某软件包是否被损坏或篡改过，只需检查md5sum。在shell 提示下键入下面的命令（把*coolapp* 换成RPM 软件包的文件名）：

```
rpm -K --nogpg <rpm-file>
```

你会看到消息“<*rpm-file*>: md5 OK”。这条消息意味着文件在下载中没有被损坏。要看到更详细的消息，把命令中的-K 换成-Kvv。

另一方面，创建软件包的开发者是不是值得信任？如果该软件包使用开发者的**GnuPG** 钥匙（*key*）被签名（*signed*），你就会知道这位开发者的身份确实如他们所言。

RPM 软件包可以使用**Gnu** 隐私卫士（或称**GnuPG**）来签名，从而帮助你肯定下载软件包的可信任性。

GnuPG 是安全通讯工具；它是PGP（一种电子隐私程序）加密技术的完全和免费的替换品。使用GnuPG，你可以验证文档的有效性，在其它通讯者之间加密或解密数据。GnuPG 还具有解密和校验PGP 5.*x* 文件的能力。

在Red Hat Linux 的安装过程中，GnuPG 被默认安装。这样，你便可以立即开始使用GnuPG 来校验你从Red Hat 收到的软件包。首先，你需要导入Red Hat 的公钥。

32.3.1. 导入钥匙

要校验Red Hat 软件包，你必须导入Red Hat GPG 公钥。要导入公钥，在shell 提示下执行以下命令：

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

要显示用来校验RPM 而安装的钥匙列表，执行以下命令：

```
rpm -qa gpg-pubkey*
```

对于Red Hat 公钥而言，其输出应包括：

```
gpg-pubkey-db42a60e-37ea5438
```

要显示关于某一指定钥匙的细节，使用rpm -qi，其后跟随前一命令的输出：

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

32.3.2. 校验软件包的签名

导入了建构者的GnuPG 公钥后，要检查RPM 文件的GnuPG 签名，使用以下命令（把<*rpm-file*> 换成RPM 软件包的名称）：

```
rpm -K <rpm-file>
```

如果一切顺利，你会看到这条消息：md5 gpg OK。这意味着软件包的签名已被校验，该软件包没有被损坏。


窍门

关于GnuPG 的详细信息，请参阅附录B。

32.4. 用RPM 在朋友面前大显身手

RPM 对于管理系统、诊断和修正问题都极有用途。要理解它的选项的最佳途径是通过示范。

- 可能你不小心删除了一些文件，却不能肯定删除了哪些文件。如果你想校验整个系统来看一看缺少哪些文件，你可以试一试下面的命令：
  ```
  rpm -Va
  ```
  如果缺少某些文件或它们似乎被损坏，你可能应该重新安装该软件包或删除安装然后再重新安装该软件包。
- 有时候，你可能会看到不认识的文件。要发现哪个软件包拥有它，你可以输入：
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  它的输出和以下相似：
  ```
  gv-3.5.8-22
  ```
- 我们可以在以下的假想情况下组合以上的两个例子。假设你的/usr/bin/paste 出了问题，你想校验拥有该程序的软件包，但是你不知道哪个软件包拥有paste。你只需输入以下命令就可以了：
  ```
  rpm -Vf /usr/bin/paste
  ```
  这样，适当的软件包就会被校验。
- 你想知道关于某一特定的程序的详细信息吗？你可以试用下面的命令来查找拥有该程序的软件包所附带的文档：
  ```
  rpm -qdf /usr/bin/free
  ```
  它的输出和以下相似：
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  /usr/share/man/man5/sysctl.conf.5.gz
  /usr/share/man/man8/sysctl.8.gz
  /usr/share/man/man8/vmstat.8.gz
  ```
- 你可能会发现一个新的RPM，但是你不知道它的用途。要寻找关于它的信息，使用下面的命令：
  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```
  它的输出看起来和以下相似：
  ```
  Name    : crontabs                  Relocations: (not relocateable)
  Version : 1.10                        Vendor: Red Hat, Inc.
  Release : 5                        Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)       Build Host: porky.devel.redhat.com
  Group   : System Environment/Base   Source RPM: crontabs-1.10-5.src.rpm
  Size    : 1004                         License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  ```

```
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

- 也许你想指定crontabs RPM 会安装哪些文件。你可以輸入下面的命令：
  `rpm -qlp crontabs-1.10-5.noarch.rpm`

  它的輸出看起来和下面相似：

```
Name    : crontabs                  Relocations: (not relocateable)
Version : 1.10                        Vendor: Red Hat, Inc.
Release : 5                       Build Date: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)       Build Host: porky.devel.redhat.com
Group   : System Environment/Base   Source RPM: crontabs-1.10-5.src.rpm
Size    : 1004                       License: Public Domain
Signature : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager  : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary   : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

以上不过是几个例子。随着你的使用经验的增加，你会发现更多RPM 的用途。

32.5. 其它资料

RPM 是一个非常复杂的工具。它有许多查询、安装、升级、以及删除软件包的选项和方法。请参考下面的资料来进一步了解RPM 技术。RPM.

32.5.1. 安装了的文档

- `rpm --help` — 该命令显示RPM 参数的快速参考。
- `man rpm` — RPM 的说明书（man）页会给你提供比`rpm --help` 命令更详细的RPM 参数信息。

32.5.2. 有用的网站

- http://www.rpm.org/ — RPM 网站。
- http://www.redhat.com/mailing-lists/rpm-list/ — 邮件列表的归档位于此处。要订阅，给<rpm-list-request@redhat.com> 发送邮件，在主题行中注明subscribe。

32.5.3. 相关书籍

- *Maximum RPM*，作者Ed Bailey；Red Hat Press — 该书的在线版本可在http://www.rpm.org/ 和http://www.redhat.com/docs/books/ 中找到。

33. 软件包管理工具

在安装中，用户选择「工作站」或「服务器」之类的安装类型。软件包就是根据这个选择来安装的。因为用户使用计算机的方法、目的不同，它们可能在安装后想再安装或删除某些软件包。软件包管理工具允许用户执行这类操作。

运行软件包管理工具需要X 窗口系统。要启动这个程序，点击面板上的「主菜单」 => 「系统设置」 => 「添加/删除应用程序」，或在shell 提示下键入`redhat-config-packages` 命令。

如果你在计算机中插入了Red Hat Linux 光盘#1，你会看到相同的界面。

图**33-1.** 软件包管理工具

该程序的界面和安装中使用的相似。软件包被分成软件包组，每一组包含一列标准软件包（*standard packages*）和一列分享公用功能的额外软件包（*extra packages*）。例如，「图形化互联网」组包含万维网浏览器、电子邮件客户、以及其它用来连接到互联网的程序。你不能删除标准软件包，除非整个软件包组都要被删除。只要软件包组被选，其中的额外软件包是你能够选择要安装或删除的可选软件包。

主菜单显示了软件包组的列表。如果软件包组旁边的复选箱内有一个选择符号，这说明该组当前已被安装。要查看其中的单个软件包列表，点击它旁边的「细节」按钮。带有选择符号的单个软件包当前已被安装。

33.1. 安装软件包

要安装软件包组中目前尚未安装的标准软件包，选择它旁边的复选箱。要定制软件包组中要安装的软件包，点击它旁边的「细节」按钮。一个包含标准和额外软件包的列表会被显示，如图33-2所示。点击软件包名称会在窗口底部显示安装它所需的磁盘空间。选择它旁边的复选箱会把它标记为要安装的软件包。

你还可以从已安装的软件包组中选择单个软件包，方法是点击「细节」按钮，然后选择任意没有被安装的额外软件包。

图**33-2.** 单个软件包的选择

选择了要安装的软件包组和单个软件包后，点击主窗口上的「更新」按钮。然后，该程序会计算安装这些软件包所需的磁盘空间，以及软件包依赖关系，并显示一个总结窗口。如果软件包依赖关系存在，它们会被自动添加到要安装的软件包列表中。点击「显示细节」按钮来查看要安装的软件包的完整列表。

图**33-3.** 软件包安装总结

点击「继续」来启动安装进程。当它结束后，「更新完毕」消息会出现。

窍门

如果你使用**Nautilus** 来浏览计算机上的文件和目录，你还可以用它来安装软件包。在**Nautilus** 中，转到包含RPM 软件包（它们通常以 `.rpm` 结尾）的目录中，然后双击RPM 图标。

33.2. 删除软件包

要删除某个软件包组内的所有软件包，取消选择它旁边的复选箱。要删除单个软件包组，点击该软件包组旁边的「细节」按钮，然后取消选择单个软件包。

当你选定了要删除的软件包后，点击主窗口中的「更新」按钮。该程序会计算它会腾出的空闲空间以及软件包依赖关系。如果其它软件包依赖于你选择要删除的软件包，它们会被自动加入到要被删除的软件包列表中。点击「显示细节」按钮来查看要删除的软件包列表。

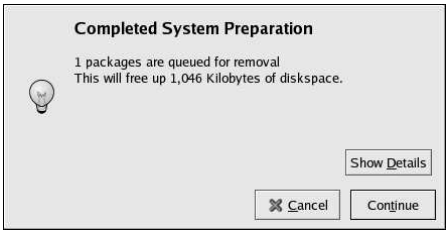


图33-4. 软件包删除总结

点击「继续」来启动删除进程。当它结束后，「更新完毕」消息会出现。


窍门

你可以同时进行软件包的安装和删除，方法是，选择要安装或删除的软件包或软件包组，然后点击「更新」。「系统筹备完毕」窗口会显示要安装和删除的软件包数量。

34. Red Hat 网络

Red Hat 网络是用来管理一个或多个Red Hat Linux 系统的互联网解决方案。所有的安全警告、错误修正警告、以及增进警告（通称勘误警告）可从Red Hat 上直接下载，你可以使用**Red Hat** 更新代理这个独立程序，也可以通过RHN 万维网界面来下载：http://rhn.redhat.com/.

图**34-1.** 你的**RHN**

Red Hat 网络为用户节省时间，因为在更新软件包一发行用户就会收到电子邮件通知。用户不必在万维网上苦寻更新的软件包或安全警告。按照默认设置，Red Hat 网络还安装这些软件包。用户不需要学习如何使用**RPM**，也不必为解决软件包依赖关系而搅尽脑汁；RHN 全盘包办。

每个Red Hat 网络帐号都带有：

- 勘误警告— 通过“基本”界面获悉用于你的网络中所有系统的安全警告、错误修正警告和增进警告在何时会被发出。

图**34-2.** 相关勘误

- 自动电子邮件通知— 向你的系统发出勘误警告时自动收到电子邮件通知
- 调度的勘误更新— 调度勘误更新的投递
- 安装软件包— 点击一个按钮就可以在一个或多个系统上调度软件包的安装
- **Red Hat** 更新代理 — 使用**Red Hat** 更新代理来为你的系统下载最新的软件包（还可以安装软件包）
- Red Hat 网络网站— 通过任何计算机上的安全万维网浏览器来管理多个系统、下载单个软件包，以及调度勘误更新之类的任务

要开始使用Red Hat 网络，请遵循下面三个基本步骤：

1. 使用以下方法之一来创建一个系统档案：
   - 在系统安装后的首次引导时运行的设置代理中把系统注册到RHN 中。
   - 在你的桌面上选择「主菜单」 => 「系统工具」 => 「**Red Hat** 网络」。
   - 从shell 提示下执行`up2date` 命令。
2. 在RHN 的网站http://rhn.redhat.com/ 上登录，并使系统有权获得所提供的服务。每个人都可以免费获得用于一个系统的Red Hat 网络账号。额外账号可以通过购买获得。
3. 开始通过RHN 网站来调度更新，或使用**Red Hat** 更新代理来下载并安装勘误更新。

要获得更详细的说明，请阅读*Red Hat Network User Reference Guide*，它位于 http://www.redhat.com/docs/manuals/RHNetwork/。


窍门

Red Hat Linux 包括了**Red Hat** 网络更新通知工具，它是一个方便的面板图标，当用于你的Red Hat Linux 系统的更新可用时，这个图标就会显示一个可视的警告。有关该插件的详细信息，请参见：http://rhn.redhat.com/help/basic/applet.html

VI. 附录

这个部分包含从Red Hat, Inc. 提供的源文件来建构定制内核的说明。它还包含关于Gnu Privacy Guard 这个用于安全通信的工具的信息。

目录

附录A.

建构定制内核

许多Linux 的新用户经常会问：“我为什么应该建构自己的内核？”鉴于在内核模块使用上的发展，对这个问题最恰当的回答应该是：“除非你已经知道你为什么需要建构自己的内核，你可能没必要这么做。”

Red Hat Linux 和通过Red Hat Linux 勘误系统所提供的内核提供了对多数现代硬件而支持以及内核功能。对多数用户来说，它不必被重新编译。本附录只是一个为想要重新编译他们的内核，并想进一步学习有关知识的用户以及想把试验性的功能编译入内核的用户而提供的指南。

要使用Red Hat, Inc. 发行的内核软件包来升级内核，请参阅第30章。


警告

建构定制内核不被Red Hat Linux 安装支持组所支持。要获得更多关于使用Red Hat, Inc. 发行的RPM 软件包来升级内核的信息，请参阅第30章。

A.1. 建构筹备

在建构定制内核之前，最重要的步骤是确定你有一张可运行的紧急引导盘，以防万一出错。要制作一个将会使用当前运行的内核来引导的引导盘，执行以下命令：

```
/sbin/mkbootdisk `uname -r`
```

制作了磁盘后，请测试它以确定它能够引导系统。

要重新编译内核，你必须安装了`kernel-source` 软件包。启用命令：

```
rpm -q kernel-source
```

来判定它是否被安装。如果它没有被安装，从Red Hat Linux 光盘、Red Hat FTP 站点（ftp://ftp.redhat.com，其镜像列表位于http://www.redhat.com/mirrors.html）或Red Hat 网络中安装它。关于安装RPM 软件包的详情，请参阅第V 部分。

A.2. 建构内核

本节的说明应用于建构定制的模块化内核。要建构单一化内核，请参阅第A.3 节来获得关于建构和安装单一化内核的各方面的解释。


注记

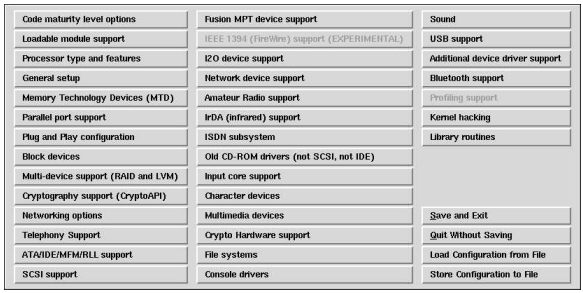
这个例子使用2.4.20-2.47.1 作为内核版本（内核版本可能会有所不同）。要判定内核版本，键入`uname -r` 命令，然后用返回的内核版本来代替2.4.20-2.47.1。

要建构用于x86 体系的内核，遵循以下步骤（已根用户身份执行）：

1. 打开一个shell 提示，改换到目录/usr/src/linux-2.4 下。从此以后的命令都必须在该目录下执行。
2. 你应该明确建构内核所使用的源码树的状况，这一点至关重要。因此，建议你从命令make mrproper 开始着手。它会删除所有的配置文件，以及散落在源码树周围的从前建构的版本遗迹。如果你已有一个存在的配置文件/usr/src/linux-2.4/.config，在运行这项命令前把它备份到另一个目录中，命令运行后再把它复制回来。
3. 推荐你从默认Red Hat Linux 内核的配置着手。其步骤是，把系统体系的配置文件从/usr/src/linux-2.4/configs/ 目录中复制到/usr/src/linux-2.4/.config 目录中。如果系统的内存大于4GB，复制包含bigmem 的文件。
4. 下一步，定制设置。如果X 窗口系统可用，建议的方法是使用make xconfig 命令来运行**Linux Kernel Configuration**。

注记

要使用make xconfig 命令所启动的图形化工具，你必须安装提供了wish 命令的tk 软件包。关于安装RPM 软件包的详情，请参阅第V 部分。



图**A-1.** 配置内核组件的类别

如图A-1所示，点击一个类别来选择它。在每个类别中包含的是组件。选择组件旁的**y**（是）、**m**（模块）、或**n**（否）来把它编译入内核、编译成内核模块、或不编译它。要进一步了解某组件，点击它旁边的**help**按钮。

点击**Main Menu**来返回到类别列表。

完成了配置后，点击主菜单中的**Save and Exit**按钮来创建配置文件/usr/src/linux-2.4/.config 并退出**Linux Kernel Configuration** 程序。

即便没有对设置进行任何改变，在继续前你也需要运行make xconfig 命令（或其它内核配置方法）。

其它可用的内核配置方法包括：

- make config — 互动文本程序。组件以线形格式出现，并被一个一个地回答。这种方法不需要运行X 窗口系统，而且不允许你改变对前面问题的回答。
- make menuconfig — 文本模式、菜单驱动的程序。组件以类别菜单的格式被显示；使用和文本模式Red Hat Linux 安装程序所用的同样方法来选择想要的组件。双态切换和要包括的项目相对应的标签：**[*]**（内建）、**[ ]**（排除）、<**M**>（模块）、或< >（具备模块能力）。这种方法不需要X 窗口系统。
- make oldconfig — 这是一个非互动的脚本。它设置配置文件来包含默认的设置。如果系统使用的是默认Red Hat Linux 内核，它会为用于该体系的Red Hat Linux 包括的内核创

建一个配置文件。这能够帮助你按照已知的工作默认值来设置内核，然后关闭你不想使用的功能。

注记

要使用kmod 和内核模块，在配置中对kmod support 和module version (CONFIG_MODVERSIONS) support 回答**Yes**。

5. 创建了/usr/src/linux-2.4/.config 文件后，使用make dep 命令来正确设置依赖关系。
6. 使用make clean 命令来准备要建构的源码树。
7. 推荐你给定制内核添加一个修改版本号码，因此现存内核不会被覆盖。此处描述的方法是从意味事件中恢复的最简易方法。关于其它可能性，请参阅http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html 或/usr/src/linux-2.4 中的Makefile 的详情。

   按照默认设置，/usr/src/linux-2.4/Makefile 在以EXTRAVERSION 开头的行的结尾处包括custom 这个词。后补这个词会允许系统同时拥有原有的工作内核和新内核（版本2.4.20-2.47.1custom）。

   如果系统包含不止一个定制的内核，区别它们的好办法是在后面添加日期（或其它标识符号）。
8. 使用make bzImage 来建构内核。
9. 建构使用make modules 所配置的模块。
10. 使用make modules_install 命令来安装内核模块（即便事实上什么也没有建构）。请留心命令中的下划线（_）。这会把内核模块安装入/lib/modules/<*KERNELVERSION*>/kernel/drivers 目录（*KERNELVERSION* 是Makefile 中指定的版本）。在这个例子里是/lib/modules/2.4.20-2.47.1custom/kernel/drivers/。
11. 使用make install 来把新内核和相关文件复制到正确的目录中。

    除了在/boot 目录中安装内核文件，这个命令还执行/sbin/new-kernel-pkg 脚本。该脚本会建构一个新的initrd 映像，并在引导装载程序的配置文件中添加一个新项目。

    如果系统有一个SCSI 适配器，而SCSI 驱动程序被作为模块编译了；或在建构内核时把ext3 支持作为模块（Red Hat Linux 的默认设置）编译入，你就需要initrd 映像。
12. 即便initrd 映像和引导装载程序被修改了，你也应该校验这些修改的正确性，并确定使用定制的内核版本而不是2.4.20-2.47.1。关于校验这些修改的信息，请参阅第30.5 节和第30.6 节。

A.3. 建构单一化内核

要建构单一化内核，除了几个例外以外，其步骤和和建构模块化内核相同。

- 当配置内核时，不要把一切都编译成模块。换一句话说，只对问题回答**Yes** 或**No**。还有，你应该对kmod support 和module version (CONFIG_MODVERSIONS) support 回答**No**。
- 省略下面几个步骤：
  make modules
  make modules_install
- 在grub.conf 文件中的kernel 行后补nomodules 或编辑lilo.conf 来包括append=nomodules 行。

A.4. 其它资料

要获取更多关于Linux 内核的信息，请参考下面的资料。

A.4.1. 安装了的文档

- `/usr/src/linux-2.4/Documentation` — 关于Linux 内核和它的模块的高级文档。这些文档是为那些理解内核运行并打算对内核源码做些贡献的用户编撰的。

A.4.2. 有用的网站

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — 来自Linux 文档计划的*The Linux Kernel HOWTO*。
- http://www.kernel.org/pub/linux/docs/lkml/ — linux-kernel 邮件列表。

redhat.

附录B.

Gnu Privacy Guard 入门

你有没有自问过，电子邮件在传输过程中会不会被别人读取？不幸的是，即便是陌生人也可以不动声色地截取甚至篡改你的电子邮件。

在传统的邮寄方式（又称“蜗牛”）中，信件通常是封在信封内，贴上邮票，然后在邮局间传递，直到它们到达其目的地。通过互联网来邮寄信件没有传统方式安全；电子邮件通常在服务器间明文传输，没有采取任何特别措施来防止通信被别人偷看或篡改。

要帮助你保护个人隐私权，Red Hat Linux 9 包括了GnuPG - *GNU Privacy Guard*（GNU 隐私卫士）- 它在典型Red Hat Linux 安装中被默认安装。它又称为*GPG*.

GnuPG 是用于安全通信的工具；它是对PGP（Pretty Good Privacy，一种广受欢迎的加密程序）加密技术的完全和免费的代替。使用GnuPG，你可以给你的数据和通信加密，并可以使用数码签名（*digitally signing*）来验证你的通信。GnuPG 还能够解密及校验PGP 5.*x*。

因为GnuPG 和其它加密标准兼容，你的安全通信可能会与其它操作系统（如Windows和Macintosh）上的电子邮件程序兼容。

GnuPG 使用公钥加密术（*public key cryptography*）来为用户提供安全的数据交换。在公钥加密术方案中，你生成两把钥匙：公钥和密钥。你和通信对方或钥匙服务器互换你的公钥，你决不应该出示你的密钥。

加密依赖于对钥匙的使用。在传统的或对称的加密术中，传输双方都有相同的钥匙，他们可以使用这把相同的钥匙来给彼此的传输解密。在公钥加密术中，两把钥匙并存：一把公钥，一把密钥。个人或组织把他们的密钥保密，但是公布他们的公钥。用公钥加密的数据只能用密钥才能解密；用密钥加密的数据只能用公钥才能解密。


重要

记住，你可以把公钥送给任何你想与之进行安全通信的人，但是你决不能向任何人提供你的密钥。

加密术的多数知识已超出本书涉及的范围；关于它的著述比比皆是。在本章中，我们只希望你对GnuPG 有足够的了解，因而能在你自己的通信中开始使用加密术。关于GnuPG、PGP 和加密技术的详细信息，请参见第B.8 节。

B.1. 配置文件

在你第一次运行GnuPG 命令的时候，你的主目录中会创建一个`.gnupg` 目录。从版本1.2 起，其配置文件名已从`.gnupg/options` 改为`.gnupg/gpg.conf`。如果在你的主目录中找不到`.gnupg/gpg.conf`，`.gnupg/options` 文件就会被使用。如果你只使用版本1.2 或更高，推荐你使用以下格式重新命名你的配置文件：

```
mv ~/.gnupg/options ~/.gnupg/gpg.conf
```

如果你从1.0.7 以前的版本中升级，你可以在你的钥匙圈中创建签名缓存来减短钥匙圈的访问时间。要执行这一操作，执行一次以下命令：

```
gpg --rebuild-keydb-caches
```

B.2. 警告消息

在执行GnuPG 命令时，你可能会看到这条消息：

```
gpg: Warning: using insecure memory!
```

出现该警告是由于非根用户无法锁定内存页。如果用户无法锁定内存页，他们可以执行内存外的“拒绝服务”（DoS）攻击；这就可能会造成安全问题。有关细节请参阅http://www.gnupg.org/(en)/documentation/faqs.html#q6.1。

你可能会看到以下消息：

```
gpg: WARNING: unsafe permissions on configuration file "/home/username/.gnupg/gpg.conf"
```

如果你的配置文件的权限被设置为允许其他人读取，这则消息就会被显示。如果你看到这条警告，推荐你执行以下命令来改变文件的权限：

```
chmod 600 ~/.gnupg/gpg.conf
```

另一条常见的警告消息是：

```
gpg: WARNING: unsafe enclosing directory permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

如果你的配置文件所在的目录的权限被设置为允许其他人读取，这则消息就会被显示。如果你看到这条警告，推荐你执行以下命令来改变文件的权限：

```
chmod 700 ~/.gnupg
```

如果你从以前的版本中升级GnuPG，你可能会看到以下消息：

```
gpg: /home/username/.gnupg/gpg.conf:82: deprecated option "honor-http-proxy"
gpg: please use "keyserver-options honor-http-proxy" instead
```

出现该警告是因为你的~/.gnupg/gpg.conf 文件包含以下行：

```
honor-http-proxy
```

版本1.0.7 和更高喜欢使用另一种语法。把以上行改成：

```
keyserver-options honor-http-proxy
```

B.3. 生成钥匙对

要开始使用GnuPG，你必须首先生成一组新的钥匙对：一把公钥和一把密钥。

要生成钥匙对，在shell 提示下，键入以下命令：

```
gpg --gen-key
```

因为你使用最频繁的是你的用户帐号，你应该登录到你的用户帐号（而不是根帐号）时执行该命令。

你会看到一个介绍屏幕，其中有钥匙选项，包括一个推荐的选项（默认），该屏幕类似：

```
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
```

```
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
  (1) DSA and ElGamal (default)
  (2) DSA (sign only)
  (5) RSA (sign only)
Your selection?
```

多数要求你选择选项的屏幕会在括号内列出默认选项。你可以按[Enter]键来接受默认选项。

在第一个屏幕上，你应该接受默认选项：(1) DSA and ElGamal。该选项会允许你生成数码签名，并用两种技术来加密（和解密）。键入**1**然后按[Enter]键。

下一步，选择钥匙大小或长短。通常，钥匙越长，你的消息抵御攻击的能力就越强。默认的1024位对多数用户来说已足够强劲，因此按[Enter]键来接受默认。

下一个选项请你指定钥匙的有效期，通常，使用默认值（0 = key does not expire）就可以。如果你想设立一个过期日期，请记住，你需要通知和你互换公钥的人员这个过期日期并向他们提供一把新公钥。如果你不设立过期日期，你会被要求确认这个决定。按[y]来确认你的决定。

你的下一个任务是提供用户ID，这包括你的姓名、电子邮件地址，以及其它可选注解。当你结束后，你的面前就会出现你输入的信息的摘要。

一旦你接受了你的选择，你还必须输入一个口令句。


窍门

和你的帐号口令一样，好的词组口令是GnuPG安全保障的基本条件。譬如，你可以在口令中混和大小写字母、数字或标点符号。

输入并校验口令句之后，你的钥匙就生成了。你会看到一条和以下相仿的消息：

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++
+++.++++++++++++++++++++++++++++++++++++++.........................++++
```

当屏幕活动停止后，你的新钥匙就制作成功并被放置在你的主目录下的.gnupg目录中。要列举你的钥匙，使用下面的命令：

```
gpg --list-keys
```

你会看到和以下相似的输出：

```
/home/username/.gnupg/pubring.gpg
---------------------------------------
pub 1024D/B7085C8A 2000-06-18 Your Name <you@example.com>
sub 1024g/E12AF9C4 2000-06-18
```

如果你使用低于1.0.6的版本来生成GnuPG钥匙，把你的密钥导出后又导入一个新钥匙，你必须具体信任你自己的密钥来给使用高于1.0.7版本的项目签名。要信任你的钥匙，键入以下的命令（请替换<*user-id*>）：

```
gpg --edit-key <user-id>
```

在Command>提示后键入**trust**，然后选择5 = I trust ultimately来信任你自己的密钥。

B.4. 生成一份废弃证书

在你生成了钥匙对之后，你应该为你的公钥创建一份废弃证书。如果你忘记了你的口令句，或该口令句已被窃取，你应该公布这份证书来通知用户你的公钥不应该再被使用。

注记

在你生成废弃证书时，你不是在废弃你刚刚生成的钥匙，相反，你给自己提供了一种停止钥匙被继续公开使用的安全方法。在你忘记了口令、更换了ISP（地址），或硬盘驱动器崩溃的情况下，这份废弃证书就可以用来宣告你原来的公钥无效。

在钥匙被废弃之前，你的签名对那些阅读你发出的信件的人有效，并可以被他们用来解密收到的消息。要生成废弃证书，使用--gen-revoke 选项：

```
gpg --output revoke.asc --gen-revoke <you@example.com>
```

注意，如果你在上面省略了--output revoke.asc 选项，你的废弃证书就会被显示在标准输出，即显示屏幕上。虽然你可以使用文本编辑器来把它们剪贴到一个文本文件中，但是直接把输出转写入登录目录中的文件可能更加简易可行。这样，你就可以保存证书以备将来之用，或将其移到软盘中，存放在一个安全之处。

其输出会类似：

```
sec 1024D/823D25A9 2000-04-26 Your Name <you@example.com>

Create a revocation certificate for this key?
```

按[Y] 来创建列出钥匙的废弃证书。下一步，你会被要求选择废弃原因或提供描述。确认了原因后，输入你用来生成钥匙的口令句。

废弃证书（revoke.asc）创建完毕后，它会位于你的登录目录中。你应该把它复制到一张软盘中，并存放在一个安全的地方。（如果你不知道如何在Red Hat Linux 中把文件复制到软盘上，请参阅《*Red Hat Linux* 入门指南》。）

B.5. 导出公钥

在你使用公钥加密术之前，其他人必须有一份你的公钥。要把你的公钥提供给通信对方或钥匙服务器，你必须导出（*export*）这把钥匙。

你需要导出公钥才能在网页上显示它或在电子邮件中粘贴它，键入以下命令：

```
gpg --armor --export <you@example.com> > mykey.asc
```

你不会看到任何输出，因为你在导出公钥的同时还把输出转写入另一个文件，譬如一个叫做mykey.asc 的文件。（若命令中不加> mykey.asc，钥匙就会被显示在标准输出即屏幕上。）

现在，mykey.asc 文件就可以被插入电子邮件或导出到钥匙服务器中。要查看这把钥匙，键入less mykey.asc 来在分页器中打开该文件（键入[q] 来退出换页器）。它应该与下面的输出相似：

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
```

```
tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
SW0jCH+pIQH5lerV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAe+pzdyX9vS+Pnf8osu7W3j60WprQkUGF1bCBHYWxs
YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
/uXVS0a5KoN7J61/1vEwx11poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQ1bD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV0lX0OSvsTyMG9wEB
vSNZk+Rl+phA55r1s8cAAwUEAJjqazvk0bgFrw1OPG9m7fEeDlvPSV6HSA0fvz4w
c7ckfpuxg/URQNf3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK5l1luGdk+l0M85FpT
/cen2OdJtToAF/6fGnIkeCeP1O5aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
iLyPH1QAoI33Ft/0HBqLtqdtP4vWYQRbibjW
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

B.5.1. 导出到钥匙服务器

如果与你通信的人寥寥无几，你可以导出公钥后逐一地发送给他们。可是，如果你的朋友遍布四海，逐一发送公钥就非常费时费力了，你可以使用钥匙服务器来解决这个问题。

钥匙服务器是一个在互联网上为任何人贮存和传递公钥的仓库。可用的钥匙服务器有很多，多数都试图保持彼此同步；向一个钥匙服务器发送公钥就如同向所有钥匙服务器发送公钥一样。通信人可以从钥匙服务器中请求你的公钥，把它导入到他们的钥匙圈上，然后他们就可以和你进行安全通信了。


穷门

因为多数钥匙服务器是同步的，向一个钥匙服务器发送你的公钥和向所有钥匙服务器发送公钥的效果一样。不过，你可以找一找不同的钥匙服务器。要搜寻它的最佳起点是*Keyserver.Net*，它位于http://www.keyserver.net。

你可以从shell 提示或浏览器中发送你的公钥；显然，你必须在线才能发送或从钥匙服务器接收钥匙。

- 在shell 提示下，键入以下命令：
  `gpg --keyserver search.keyserver.net --send-key` *`you@example.com`*
- 在浏览器中，转到Keyserver.Net（http://www.keyserver.net），然后选择来添加你自己的PGP 公钥。

  你的下一个任务是把公钥复制并粘贴到网页上恰当的位置中。如果你需要这个过程的说明，使用下列步骤：

  - 使用分页器打开你导出的公钥文件（如第B.5 节中创建的*`mykey.asc`*）— 譬如，使用`less mykey.asc` 命令。
  - 用鼠标突出显示从`BEGIN PGP` 到`END PGP` 之间的所有行并复制它们（参见图B-1）。
  - 把*`mykey.asc`* 文件的内容粘贴到Keyserver.Net 网页上的恰当位置中，方法是点击鼠标的中间按钮（若使用两键鼠标，则同时按左右两个按钮）。然后在钥匙服务器网页上按**Submit** 按钮。（如果你出了错，按该网页上的**Reset** 按钮来清除粘贴的钥匙。）

图**B-1.** 复制公钥

注意，如果你向另一个基于网站的钥匙服务器提交公钥，方法和以上步骤基本上相同。

至此你便大功告成。不管你使用的是shell 提示还是万维网，你都会看到一条消息通知你钥匙已被成功提交— 或在shell 提示下，或在钥匙服务器的网站上。从现在起，想和你安全通信的用户就可以导入你的公钥并把它添加到他们的钥匙圈上了。

B.6. 导入公钥

钥匙互换的另一方面是把别人的公钥导入到你的钥匙圈上— 它和导出公钥一样简单。当你导入别人的公钥时，你就可以用它来解密他们发来的邮件并根据你钥匙圈上他们的公钥来检查他们的数码签名。

导入钥匙的最简单的方法之一是从网站上下载或保存它。

公钥被下载并保存到*key.asc* 文件后，使用下列命令来把它添加到你的钥匙圈上。

```
gpg --import key.asc
```

另一种保存钥匙的方法是使用浏览器的「**Save As**（另存为）」功能。如果你使用**Mozilla** 之类的浏览器，你可以在钥匙服务器中找到某钥匙，把该网页存为文本文件（点击**File => Save Page As**）。在**Files of Type** 旁边的下拉菜单中，选择**Text Files (*.txt)**。然后，你就可以导入该钥匙— 但是别忘了你储存的文件名。譬如，如果你把钥匙存为叫做*newkey.txt* 的文本文件，要导入文件，在shell 提示下，键入下面的命令：

```
gpg --import newkey.txt
```

它的输出会与下面相似：

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
gpg:       imported: 1
```

要检查该过程是否成功，使用gpg --list-keys 命令；你应该看到你的钥匙圈上列出了一把新导入的钥匙。

当你导入公钥后，你把它添加到你的钥匙圈（*keyring*）上，它是一个保存公钥和密钥的文件。然后，当你从该实体中下载文档或文件时，你可以根据添加到你的钥匙圈上的钥匙来校验那个文档。

B.7. 数码签名在哪里?

数码签名可以用来和你手写的签名做比较。和传统的通信方式不同，传统签名有可能被伪造，数码签名却无法被伪造。这是因为该签名是用你的独特密钥制作的，收信人可以使用你的公钥来校验它。

数码签名会给文档加注时间戳；这意味着你在给文档签名时的时间也是签名的一部分。因此，如果某人企图修改文档，签名校验就会失败。某些电子邮件程序，如**Exmh** 或KDE 的**KMail**，在程序的界面中包括了使用**GnuPG** 来给文档签名的功能。

两种有用的数码签名是：净签（*clearsigned*）文档和分离签名（*detached signatures*）。这两类签名都使用同样的验证保安，不要求收信人给你的整条消息解密。

在净签消息中，你的签名会在信件主体内以文本块形式出现；分离签名是和你的通信一起发出的一个分开的文件。

B.8. 其它资料

加密技术中可以研究讨论之处极多，这里只对**GnuPG** 蜻蜓点水地介绍了一下。如果你想深入了解这方面的知识，可以参看下面的资料。

B.8.1. 安装了的文档

- `man gpg` 和`info gpg` — GnuPG 命令和选项的快捷参考。

B.8.2. 有用的网站

- http://www.gnupg.org — GnuPG 网站，其中有到最新GnuPG 发行版本、通俗易懂的用户指南、以及其它加密资源的链接。
- http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html — 访问Webmonkey 的*Encryption Tutorial* 来进一步学习加密技术以及如何应用这项技术。
- http://www.eff.org/pub/Privacy — 电子前沿基金会（Electronic Frontier Foundation），“Privacy, Security, Crypto, & Surveillance”的归档。

B.8.3. 相关书籍

- *The Official PGP User's Guide*，作者Philip R. Zimmerman；MIT Press 出版
- *PGP: Pretty Good Privacy*，作者Simson Garfinkel；O'Reilly & Associates, Inc. 出版
- *E-Mail Security: How to Keep Your Electronic Messages Private*，作者Bruce Schneier；John Wiley & Sons 出版

索引

汉字和符号

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

后记

Red Hat Linux 指南手册使用DocBook SGML v4.1 格式编写。HTML 和PDF 格式使用定制的DSSSL 风格表单和定制的jade 会绕脚本来编写。

Marianne Pecci <goddess@ipass.net> 创建了警诫图形（注记、窍门、重要、小心、和警告）。在获得Marianne Pecci 和Red Hat, Inc. 的书面许可后，它们可以被重新发行。

Red Hat Linux 产品文档组的成员如下：

Sandra A. Moore —《*Red Hat Linux x86* 安装指南》 的主要撰写人和维护者；《*Red Hat Linux* 入门指南》 的参与撰写人

Tammy Fox —《*Red Hat Linux* 定制指南》 的主要撰写人和维护者；《*Red Hat Linux* 入门指南》的参与撰写人；DocBook 的定制风格表和脚本的编写人和维护者

Edward C. Bailey —《*Red Hat Linux x86* 安装指南》 的参与撰写人

Johnray Fuller —《*Red Hat Linux* 参考指南》的主要撰写人和维护者；《*Red Hat Linux* 安全指南》的参与撰写人和维护者

John Ha —《*Red Hat Linux* 入门指南》的主要撰写人和维护者；《*Red Hat Linux* 安全指南》的参与撰写人和维护者

Sarah Smith（王赛英） —《*Red Hat Linux x86* 安装指南》、《*Red Hat Linux* 入门指南》、和《*Red Hat Linux* 定制指南》 的简体中文翻译者