

21 世纪 高 职 高 专 规 划 教 材

网 络 专 业 系 列



# Linux服务器 配置与管理

冯 昊 编著

清华大学出版社



# 21 世纪高职高专规划教材

## 网络专业系列

计算机网络基础教程  
网络操作系统教程  
Windows 2003网络管理实训教程  
Linux入门教程  
网络安全技术  
计算机网络技术实训教程  
网站设计与管理  
网络工程与综合布线  
交换机/路由器的配置与管理  
**Linux服务器配置与管理**  
SQL Server数据库应用技术  
Oracle 9i数据库管理教程  
Java程序设计教程  
网页制作工具——Dreamweaver MX 2004  
C#应用开发  
Visual Basic.NET程序设计教程  
UML基础与应用  
VRML虚拟现实网页设计

ISBN 7-302-10854-4



9 787302 108542 >

定价: 32.00元

21 世纪高职高专规划教材

网络专业系列

# Linux服务器 配置与管理

冯昊 编著



清华大学出版社  
北京

## 内 容 简 介

Linux 是以 Intel x86 系列 CPU 为硬件平台的 32 位多用户多任务操作系统,具备强大的网络服务功能,是商用网络服务器首选的操作系统之一。

本书以目前使用最广泛、安装也最为方便的 Red Hat Linux 9 为例,结合作者多年的网络管理和教学经验,从初学者角度出发,通过大量具体应用实例,详细介绍了 Linux 的安装与启动、Linux 的磁盘文件管理、用户与用户组管理、服务与进程管理、软件包管理、网络连接配置、MySQL 数据库服务器、Web 服务器、FTP 服务器、DNS/DHCP、qmail 邮件服务器、防火墙和代理服务器、远程登录管理和 Linux 内核升级等实用内容,并配有大量的习题与上机指导。

本书可作为高职高专院校计算机教材,也可作为 Linux 爱好者的参考书和各种培训班教材。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。

### 图书在版编目(CIP)数据

Linux 服务器配置与管理/冯昊编著. - 北京:清华大学出版社,2005.6

(21 世纪高职高专规划教材,网络专业系列)

ISBN 7-302-10854-4

I. L… II. 冯… III. Linux 操作系统—高等学校:技术学校—教材 IV. TP316.89

中国版本图书馆 CIP 数据核字(2005)第 036606 号

出 版 者:清华大学出版社

<http://www.tup.com.cn>

社 总 机:010-62770175

地 址:北京清华大学学研大厦

邮 编:100084

客户服务:010-62776969

责任编辑:曾 妍

印 刷 者:清华大学印刷厂

装 订 者:三河市化甲屯小学装订二厂

发 行 者:新华书店总店北京发行所

开 本:185×230 印张:26.25 字数:538 千字

版 次:2005 年 6 月第 1 版 2005 年 6 月第 1 次印刷

书 号:ISBN 7-302-10854-4/TP·7218

印 数:1~5000

定 价:32.00 元



# 出版说明

高职高专教育是我国高等教育的重要组成部分,担负着为国家培养并输送生产、建设、管理、服务第一线高素质技术应用型人才的重任。

进入 21 世纪后,高职高专教育的改革和发展呈现出前所未有的发展势头,学生规模已占我国高等教育的半壁江山,成为我国高等教育的一支重要的生力军;办学理念上,“以就业为导向”成为高等职业教育改革与发展的主旋律。近两年来,教育部召开了三次产学研交流会,并启动四个专业的“国家技能型紧缺人才培养项目”,同时成立了 35 所示范性软件职业技术学院,进行两年制教学改革试点。这些举措都表明国家正在推动高职高专教育进行深层次的重大改革,向培养生产、服务第一线真正需要的应用型人才的方向发展。

为了顺应当前我国高职高专教育的发展形势,配合高职高专院校的教学改革和教材建设,进一步提高我国高职高专教育教材质量,在教育部的指导下,清华大学出版社组织出版“21 世纪高职高专规划教材”。

为推动规划教材的建设,清华大学出版社组织并成立“高职高专教育教材编审委员会”,旨在对清华版的全国性高职高专教材及教材选题进行评审,并向清华大学出版社推荐各院校办学特色鲜明、内容质量优秀的教材选题。教材选题由个人或各院校推荐,经编审委员会认真评审,最后由清华大学出版社出版。编审委员会的成员皆来源于教改成效大、办学特色鲜明、师资实力强的高职高专院校、普通高校以及著名企业,教材的编写者和审定者都是从事高职高专教育第一线的骨干教师和专家。

编审委员会根据教育部最新文件政策,规划教材体系,比如部分专业的两年制教材;“以就业为导向”,以“专业技能体系”为主,突出人才培养的实践性、应用性的原则,重新组织系列课程的教材结构,整合课程体系;按照教育部制定的“高职高专教育基础课程教学基本要求”,教材的基础理论以“必要、够用”为度,突出基础理论的应用和实践技能的培养。

本套规划教材的编写原则如下:

- (1) 根据岗位群设置教材系列,并成立系列教材编审委员会;
- (2) 由编审委员会规划教材、评审教材;
- (3) 重点课程进行立体化建设,突出案例式教学体系,加强实训教材的出版,完善教学服务体系;
- (4) 教材编写者由具有丰富教学经验和多年实践经验的教师共同组成,建立“双师

型”编者体系。

本套规划教材涵盖了公共基础课、计算机、电子信息、机械、经济管理以及服务等大类的主要课程,包括专业基础课和专业主干课。目前已经规划的教材系列名称如下:

#### • 公共基础课

公共基础课系列

#### • 计算机类

计算机基础教育系列

计算机专业基础系列

计算机应用系列

网络专业系列

软件专业系列

电子商务专业系列

#### • 电子信息类

电子信息基础系列

微电子技术系列

通信技术系列

电气、自动化、应用电子技术系列

#### • 机械类

机械基础系列

机械设计与制造专业系列

数控技术系列

模具设计与制造系列

#### • 经济管理类

经济管理基础系列

市场营销系列

财务会计系列

企业管理系列

物流管理系列

财政金融系列

#### • 服务类

旅游系列

艺术设计系列

本套规划教材的系列名称根据学科基础和岗位群方向设置,为各高职高专院校提供“自助餐”形式的教材。各院校在选择课程需要的教材时,专业课程可以根据岗位群选择系列;专业基础课程可以根据学科方向选择各类的基础课系列。例如,数控技术方向的专业课程可以在“数控技术系列”选择;数控技术专业需要的基础课程,属于计算机类课程可以在“计算机基础教育系列”和“计算机应用系列”选择,属于机械类课程可以在“机械基础系列”选择,属于电子信息类课程可以在“电子信息基础系列”选择。依此类推。

为方便教师授课和学生学习,清华大学出版社正在建设本套教材的教学服务体系。本套教材先期选择重点课程和专业主干课程,进行立体化教材建设;加强多媒体教学课件或电子教案、素材库、学习盘、学习指导书等形式的制作和出版,开发网络课程。学校在选用教材时,可通过邮件或电话与我们联系获取相关服务,并通过与各院校的密切交流,使其日臻完善。

高职高专教育正处于新一轮改革时期,从专业设置、课程体系建设到教材编写,依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议,并向我们推荐优秀选题。反馈意见请发送到 E-mail:gzgz@tup.tsinghua.edu.cn。清华大学出版社将对已出版的教材不断地修订、完善,提高教材质量,完善教材服务体系,为我国的高职高专教育出版优秀的高质量的教材。

高职高专教育教材编审委员会

# 前言

## Linux 服务器配置与管理

Linux 是在 1991 年发展起来的与 UNIX 兼容的操作系统,它以 Intel x86 系列 CPU 为硬件平台,遵循 POSIX(标准操作系统界面)标准的 32 位多用户多任务操作系统。

Linux 的开发和发行遵循 GPL(GNU general public license,GNU 通用公共许可证)版权协议,其源代码可以免费获得,用户可以根据自身的需求,对代码进行修改,但必须公开修改过的源代码,最初的作者拥有版权。Linux 的发行版本并不都是免费的,只要源代码保持公开,开发人员是可以要求获得适当的报酬,比如 Red Hat Enterprise Linux 发行版本目前是要收费的,以使 Linux 能有更好的发展。

Linux 是一个非常健壮和稳定的操作系统,其内核具有 Windows 无法比拟的稳定性和高效性,在不使用 X-Windows 图形界面的情况下,Linux 占用的系统资源很少,甚至可以使一台 Intel 486 成为一台高效的工作站。Linux 使用了最先进的内存管理技术,能很好地释放和管理内存及系统资源,系统可长时间稳定工作,而不需要经常重启操作系统。Linux 系统很少死机,可以随时终止那些有问题的进程,以保证操作系统正常的运行。而 Windows 2000 Server 由于不能很好地自动释放系统资源,必须每隔一段时间就重启一次系统。另外,Linux 几乎不受病毒的攻击,在安全性方面也比 Windows 系统好。

Linux 在经过 IBM、惠普、Novell 和红帽等公司专业开发人员的发展后,如今已经主宰了高性能计算机市场。目前,在全球超级计算机“500 强”中,有 301 台使用了 Linux 操作系统,有 189 台使用了 UNIX 操作系统,2 台使用了 UNIX 的改进型 FreeBSD 操作系统,1 台使用了微软的 Windows 操作系统,另有 7 台使用了其他操作系统。

目前,Linux 在我国也得到了较广泛的应用,但缺乏介绍 Linux 深层使用的书籍,阻碍了 Linux 的深层次应用和普及。目前,关于 Linux 方面的书虽然较多,但大多数都是介绍如何安装,以及如何使用像 KDE 和 GNOME 这类图形界面的,对 Linux 作为服务器应用介绍相对较少。大多数用户仍习惯将 Linux 当作一个桌面型操作系统来使用,而对于桌面型操作系统和办公应用,目前最好的选择仍是 Windows 平台,Linux 真正的优势和发展方向应是作为服务器操作系统。根据需要,Linux 可安装成各种各样的服务器,比如数据库服务器、Web 服务器、FTP 服务器、DNS 服务器、DHCP 服务器、邮件服务、代理服

务器、防火墙等,并且用 Linux 作为服务器操作系统比用 Windows 2000 Server 要稳定、安全得多,另外,在价格方面也要便宜很多。

全书共 13 章,在编写上力求语言简洁、条理清晰、实用性强。建议周课时 6 学时,注意培养学生实际动手和操作应用能力,以及独立思考和解决问题的能力。在进行上机实践时,可在 Windows 2000 系统中,安装 VMware Workstation 虚拟主机,然后在虚拟主机中安装 Linux,并进行 Linux 的相关操作。VMware Workstation 虚拟主机以及本书所用到的相关软件包,可通过访问作者网站(<http://www.pcnetedu.com>)来获得。

本书第 1~3 章由陈丹编写,第 4~5 章由杨海燕编写,第 6~13 章由冯昊编写。在编写过程中,得到了清华大学出版社的大力支持和帮助,在此一并致以衷心的感谢!

作 者

2005 年 5 月

# 目 录

Linux 服务器配置与管理

<b>第 1 章 Red Hat Linux 9 的安装与启动</b>	<b>1</b>
1.1 Linux 简介	1
1.1.1 什么是 Linux	1
1.1.2 Linux 的发展史	2
1.1.3 Linux 的优点与应用	2
1.1.4 Red Hat Linux 简介	3
1.2 Red Hat Linux 的安装方式	3
1.3 安装 Red Hat Linux 9	8
1.4 Linux 的启动与登录	22
1.4.1 Red Hat Linux 的启动	22
1.4.2 登录与注销	22
习题	25
实训 1-1 搭建 Linux 学习环境	27
实训 1-2 安装 Red Hat Linux 9	31
<b>第 2 章 Linux 磁盘文件管理</b>	<b>34</b>
2.1 Linux 文件系统类型	34
2.2 Linux 系统的目录结构	35
2.3 文件类型与文件属性	39
2.4 Linux 常用命令	45
2.4.1 Linux 命令基础	45
2.4.2 基本操作命令	46
2.4.3 目录操作命令	48
2.4.4 文件操作命令	49

2.4.5	查看系统信息 .....	55
2.4.6	使用 vi 编辑器 .....	59
2.5	建立与使用文件系统 .....	62
2.5.1	创建分区 .....	62
2.5.2	在分区建立文件系统 .....	63
2.5.3	挂载和使用文件系统 .....	65
2.6	在 Linux 中使用移动存储设备 .....	66
2.6.1	在 Linux 中使用软盘 .....	66
2.6.2	在 Linux 中使用 USB 存储设备 .....	68
2.7	制作与使用光盘镜像文件 .....	71
2.7.1	制作光盘镜像文件 .....	71
2.7.2	使用光盘镜像文件 .....	71
习题	.....	72
<b>第 3 章</b>	<b>管理用户和用户组 .....</b>	<b>75</b>
3.1	用户和用户组文件 .....	75
3.2	管理用户账户与密码 .....	77
3.2.1	用户账号管理 .....	77
3.2.2	用户密码管理 .....	80
3.3	用户组管理 .....	81
3.4	使用用户管理器管理用户和组 .....	84
习题	.....	87
实训 3	用户与用户组管理 .....	88
<b>第 4 章</b>	<b>Linux 的服务与进程管理 .....</b>	<b>90</b>
4.1	Linux 的启动过程 .....	90
4.1.1	Linux 启动过程概述 .....	90
4.1.2	inittab 配置文件 .....	90
4.2	Linux 的服务管理 .....	94
4.2.1	服务的启动脚本 .....	94
4.2.2	服务的启动与停止 .....	95
4.2.3	配置服务的启动状态 .....	96
4.3	Linux 的进程管理 .....	98
4.3.1	进程与作业 .....	98

4.3.2 进程的启动 .....	99
4.3.3 管理系统的进程 .....	101
习题 .....	103
实训 4 服务与进程管理 .....	104
<b>第 5 章 软件包管理 .....</b>	<b>106</b>
5.1 RPM 软件包管理 .....	106
5.1.1 RPM 简介 .....	106
5.1.2 使用 rpm 命令 .....	106
5.1.3 RPM 软件包管理工具 .....	110
5.2 TAR 包管理 .....	111
习题 .....	113
实训 5 Linux 软件包管理 .....	114
<b>第 6 章 配置网络连接 .....</b>	<b>116</b>
6.1 网络的基本配置 .....	116
6.1.1 配置主机名 .....	116
6.1.2 配置网卡 .....	117
6.1.3 配置客户端名称解析 .....	125
6.2 安装与配置 ADSL 拨号 .....	126
6.2.1 安装 PPPoE 拨号软件 .....	126
6.2.2 配置 ADSL 拨号 .....	127
6.3 常用网络调试命令 .....	131
6.4 网络故障排查的基本方法 .....	136
习题 .....	137
实训 6 配置网络接口卡 .....	138
<b>第 7 章 Linux 服务器的配置 .....</b>	<b>141</b>
7.1 安装与配置 MySQL 服务器 .....	141
7.1.1 MySQL 安装简介 .....	141
7.1.2 安装 MySQL 服务器 .....	142
7.1.3 MySQL 管理基础 .....	150
7.2 安装与配置 Web 服务器 .....	161
7.2.1 安装 Apache 服务器 .....	161



7.2.2	Apache 配置文件简介 .....	168
7.2.3	Apache 服务器基本配置 .....	168
7.2.4	配置虚拟主机 .....	179
7.2.5	安装与配置 PIIP 解释器 .....	189
7.2.6	安装与配置 Perl 解释器 .....	199
7.2.7	安装与配置 phpMyAdmin .....	200
习题	.....	202
实训 7-1	安装与配置 MySQL 服务器 .....	204
实训 7-2	安装与配置 WWW 服务器 .....	205
<b>第 8 章</b>	<b>配置 FTP 服务器 .....</b>	<b>206</b>
8.1	安装 vsftpd 服务器 .....	206
8.2	连接和访问 FTP 服务器 .....	208
8.3	配置 vsftpd 服务器 .....	214
8.4	用户磁盘配额管理 .....	221
8.5	vsftp 服务器配置示例 .....	226
8.6	FTP 常用命令 .....	230
习题	.....	232
实训 8	安装与配置 FTP 服务器 .....	233
<b>第 9 章</b>	<b>配置 DNS 与 DHCP 服务器 .....</b>	<b>234</b>
9.1	配置 DNS 服务器 .....	234
9.1.1	DNS 简介 .....	234
9.1.2	安装 DNS 服务器 .....	235
9.1.3	配置 DNS .....	238
9.2	安装与配置 DHCP 服务器 .....	249
9.2.1	DHCP 简介 .....	249
9.2.2	安装 DHCP 服务器软件包 .....	250
9.2.3	配置 DHCP 服务器 .....	251
习题	.....	255
实训 9-1	安装与配置 DNS 服务器 .....	256
实训 9-2	安装与配置 DHCP 服务器 .....	256

<b>第 10 章 配置 qmail 邮件服务器</b> .....	257
10.1 邮件服务系统简介 .....	257
10.2 qmail 工作流程简介 .....	259
10.3 安装 qmail 邮件服务器 .....	261
10.4 安装 qmailadmin .....	284
10.5 安装与配置 webmail .....	288
10.5.1 安装与配置 sqwebmail .....	288
10.5.2 安装与配置 igenus .....	292
10.6 邮件账户的 Web 注册 .....	296
10.7 qmail 服务进程的管理 .....	299
10.8 qmail 的配置文件 .....	304
10.9 qmail 防病毒与反垃圾邮件 .....	308
习题 .....	324
实训 10 安装与配置 qmail 服务器 .....	325
<b>第 11 章 配置防火墙与代理服务器</b> .....	326
11.1 配置 Linux 防火墙 .....	326
11.1.1 防火墙简介 .....	326
11.1.2 IP 包过滤与网络地址转换 .....	328
11.1.3 使内核支持防火墙 .....	331
11.1.4 iptables 命令用法 .....	334
11.1.5 防火墙配置实例 .....	344
11.2 安装与配置透明代理服务器 .....	348
11.2.1 代理服务器简介 .....	348
11.2.2 利用网络地址转换实现透明代理 .....	349
11.2.3 安装与配置 squid 缓存透明代理 .....	353
11.2.4 squid 的配置命令 .....	361
11.3 端口扫描与数据包捕获 .....	372
11.3.1 端口与端口扫描工具 .....	372
11.3.2 tcpdump 数据包捕获命令 .....	375
习题 .....	379
实训 11 配置防火墙与透明代理 .....	380

<b>第 12 章 Linux 的远程登录管理</b> .....	381
12.1 使用 telnet 远程登录 .....	381
12.2 使用 SSH 远程登录 .....	382
12.3 Windows 平台使用 SSH 客户端登录 .....	387
习题 .....	388
实训 12 远程登录 .....	389
<b>第 13 章 Linux 内核的升级</b> .....	390
13.1 Linux 2.6 内核新特性 .....	390
13.2 升级到 Linux 2.6 内核 .....	391
<b>参考文献</b> .....	405

## Red Hat Linux 9 的安装与启动

Linux 是在 1991 年发展起来的与 UNIX 兼容的操作系统,可以免费使用,其源代码还可自由传播,并允许修改、充实和发展。本章将对 Linux 作一些简单介绍,并以目前使用较广泛的 Red Hat Linux 为例,介绍 Linux 的安装方式和安装方法,以及 Linux 的启动与登录方法,以便对 Linux 有一个初步的认识。

### 1.1 Linux 简介

#### 1.1.1 什么是 Linux

Linux 是一个以 Intel x86 系列 CPU 为硬件平台、遵循 POSIX(标准操作系统界面)标准、完全免费而且可以自由传播的 UNIX 兼容系统。该系统是一个完整的 32 位多用户多任务操作系统,可直接安装使用,不需要预先安装其他操作系统。

Linux 的内核(kernel)版权属于 Linus Torvalds,在 GPL(GNU general public license,GNU 通用公共许可证)版权协议下发行,用户可以自由复制、修改、套装分发和销售,但是不可在分发时加入任何限制,而且所有源代码必须公开,因此任何人均可无偿取得所有执行文件和源代码。

对于用户和系统管理员而言,Linux 是指包含 Linux Kernel(系统内核)、utilities(系统工具程序)以及 application(应用软件)的一个完整的操作系统。Linux 的应用软件是由自由软件基金会(FSF)开发的,全世界许多热心的程序员为 Linux 开发或移植了很多应用程序,包括 X-Windows、Emacs、TCP/IP 网络等。Linux 源代码兼容绝大部分 UNIX 标准(如 IEEE POSIX、System V、BSD),UNIX 很多源程序拿到 Linux 下重新编译后就可以正常运行,对于 BSD UNIX 来说,其可执行文件还可直接在 Linux 环境下运行。

Linux 的吉祥物是企鹅,它是由 Linux 的创始人 Linus Torvalds 挑选的,代表他所创立的 Linux 操作系统。

### 1.1.2 Linux 的发展史

Linux 的历史最早可追溯到 1990 年,它是由一名叫 Linus Torvalds 的计算机爱好者开发的。当时他是芬兰赫尔辛基大学(Helsinki)的学生,最初用汇编语言写了一个 80386 保护模式下处理多任务切换的程序,后来从 Minix(受 UNIX 源代码版权限制,由一位名叫 Andrew Tannebaum 的计算机教授编写的可在 PC 机上运行,用于示范教学的 Mini UNIX 系统)中得到灵感,于是开始写一些硬件设备驱动程序和文件系统,随后就诞生了 0.0.1 版本的 Linux,但它必须在装有 Minix 的机器上编译以后才能运行。之后, Linus Torvalds 决定抛开 Minix 系统,重新开发一个全新的系统,该系统能运行在 386、486 个人计算机上,并且具有 UNIX 操作系统的全部功能,于是在 1991 年 10 月 5 日发布了 Linux 0.0.2 版,该版本可以运行 bash(一种用户与操作系统内核通信的软件)和 gcc(GNU C 编译器),并将其源代码发布在网上,随即就引起了爱好者的注意,他们通过互联网也加入了 Linux 内核的开发工作,一大批高水平程序员的加入,使得 Linux 得到了迅猛发展,到 1993 年底, Linux 1.0 终于诞生。此时的 Linux 已是一个功能完备的操作系统了,其内核紧凑高效,可以充分发挥硬件的性能,在 4MB 内存的 80386 机器上已有非常出色的表现。

Linux 加入 GNU 并遵循公共版权许可证(GPL)协议,由于不排斥商家对软件作进一步开发,不排斥在 Linux 上开发商业软件,从而使 Linux 又开始了一次飞跃,出现了很多 Linux 的发行版本,如 Red Hat、Slackware、Suse、TurboLinux、Red Flag、Blue Point、Xteam Linux、OpenLinux、Happy Linux、Xlinux 等,而且还在增加。一些公司也开始在 Linux 上开发商业软件或将其他 UNIX 平台上的软件移植到 Linux 上来,随着 Linux 的应用和发展前景的看好,目前 IT 界众多知名商家,如 IBM、Intel、Oracle、Informix、Sysbase、Novell、HP 等都宣布支持 Linux,并极力开发和推广 Linux 商业服务器和相关软件,众多商家的加盟弥补了纯自由软件的不足和发展障碍,使得 Linux 得以迅速普及和前所未有的大发展。

### 1.1.3 Linux 的优点与应用

Linux 的核心具有 Windows 无法比拟的稳定性和高效性,在不使用 X-Windows 的情况下, Linux 占用系统资源很少,甚至可以使一台 Intel 486 成为高效的工作站。一台 Linux 服务器可以长期高效、稳定地工作,而一台 Windows NT 服务器,由于系统不能很好地自动释放系统资源,必须每隔一段时间就重启系统一次。

在网络服务和安全性方面, Linux 也强于 Windows NT 服务器,目前各种操作系统在网络方面的性能比较,公认的优劣顺序是 BSD (UNIX)、Linux、Windows NT、Windows 9x。

Linux 主要用作服务器操作系统,具有强大的网络服务功能,可实现各种网络服务,如邮件服务、Web 服务、FTP、DNS、DHCP、防火墙、代理服务器、路由器等。对于个人桌

面操作系统,目前最好的选择仍是 Windows 系统。

Linux 在网络服务器市场增长非常强劲,UNIX 和 Linux 已成为目前最流行的中端服务器操作系统。据 IDC(international data corporation)公司 2003 年第三季度的市场调查,Linux 在全球服务器市场所占份额约为 26%,Windows 为 44%,但 Linux 保持着较高的增长率,据 2004 年 6 月份 IDC 的最新调查显示,2004 年第一季度全球 Linux 服务器的出货量增长了 46.4%,而 Windows 服务器的涨幅仅为 26.5%。

### 1.1.4 Red Hat Linux 简介

Linux 的不同发行版本,其区别主要在于安装和配置方式、捆绑软件以及技术支持方面存在差异。在众多的发行版本中,Red Hat Linux 是业内最负盛名,也是做得最出色的,本教材以 Red Hat Linux 9 为例进行介绍,其内核版本为 2.4.20-8。

Red Hat Linux 是目前使用最广泛、安装最方便的 Linux 版本,支持多种安装方式,著名的 RPM 套件安装程序也是 Red Hat 公司的首创。Red Hat Linux 9 可以在许多硬件平台上运行,与以前版本相比,对硬件的支持又有了很大的提高,并加入了最新的技术,同时弥补了以前版本中出现的 Bug。

目前,Red Hat 公司已将研发重心放在了 Linux 商用企业服务器(Red Hat Enterprise Linux)的开发上,原有的 Red Hat Linux 开发计划与 Fedora Linux 计划整合成新的 Fedora 项目,作为 Linux 免费发行的开发源代码的项目。该 Fedora 项目由 Red Hat 公司赞助,以社会群体主导、支持的方式来开发 Linux 新的发行版,目前该发行版的最新版本为 Fedora Core 2,它相当于是 Red Hat Linux 9 的后续版本,目前还处于测试阶段。

Fedora Core 2 采用了 Linux 2.6 版的内核(Kernel),具有更快的运行速度;能更好地支持即插即用设备,对硬件的支持更强,对数码相机、USB 等设备可实现无需任何配置,真正做到即插即用,并开始支持 USB 2.0 设备;全面支持 UTF-8,对中文具有更好的支持。

## 1.2 Red Hat Linux 的安装方式

### 1. 安装方式

Red Hat Linux 支持多种安装方式,根据安装时软件的来源,有光盘安装、硬盘安装、NFS 映像安装、FTP 安装和 HTTP 安装五种方式。

光盘和硬盘安装属于本地安装,NFS 映像安装、FTP 和 HTTP 安装则属于网络安装。不管采用哪种安装方式,都需要有安装启动盘。在 Red Hat Linux 的第一张安装光盘的 images 目录下,存放有制作启动盘和驱动程序盘所需的镜像文件:bootdisk.img 为启动软盘镜像文件,各种安装方式都需要该文件,drvnet.img 为网络安装时需要制作的

网卡驱动盘镜像文件, `drvblock.img` 为使用 SCSI 设备安装时需要制作的块设备驱动盘镜像文件, `pcmciaadd.img` 为使用笔记本安装时, 需要制作的 PCMCIA 设备驱动磁盘镜像文件, 各种安装方式下需要制作的启动软盘和驱动程序盘以及对应的镜像文件如表 1.1 所示。

表 1.1 各安装方式所需要制作的软盘以及对应的镜像文件

安 装 方 式	<code>bootdisk.img</code>	<code>drvnet.img</code>	<code>drvblock.img</code>	<code>pcmciaadd.img</code>
IDE 光盘	✓			
IDE 硬盘	✓			
USB 移动硬盘	✓			
网络安装	✓	✓		
SCSI 设备	✓		✓	
PCMCIA 设备	✓			✓

由于软盘容量小、速度慢、易损坏, Red Hat Linux 还提供了用于制作安装引导光盘所需的 `boot.iso` 镜像文件。该文件包括了所有相关的驱动程序, 引导系统后可实现从各种介质进行安装, 但不包括任何安装软件包, 常用于引导系统后从非光盘介质(如硬盘、网络)进行安装, 是软盘引导的一种较好替代方式。用光盘刻录软件, 把 `boot.iso` 镜像文件刻录到光盘即可获得具有引导功能的启动光盘。

Red Hat Linux 发行版安装光盘的第一张光盘, 自带有启动功能, 可直接利用光盘启动后进行安装, 不需要再制作启动软盘, 这是目前最简单也是最常用的一种安装方式。

对于没有光驱或无法从光盘引导的系统, 可采用从软盘引导来安装 Linux。软盘只负责引导系统并通过其他介质(如硬盘、光盘或网络)提供安装软件包来实现安装 Linux, 其本身并不包含任何要安装的软件包。对于通过网络、SCSI 设备或 PCMCIA 设备进行安装时, 还需要相应的设备驱动软盘配合引导软盘, 才能实现正常安装。

## 2. 制作启动软盘

在 Red Hat Linux 发行版安装光盘的第一张光盘的 `dosutils` 目录, 提供了制作启动软盘和驱动软盘的实用工具。

### (1) 在 Windows 平台制作启动软盘

在 `dosutils` 目录下面有一个 `rawwritewin` 子目录, 双击运行 `rawwritewin.exe` 程序, 即可启动制作程序, 如图 1.1 所示。

在 Image file 输入框中输入或单击输入框旁边带省略号的浏览按钮选择要制作启动软盘的镜像文件, 在 Number of copies 输入框中设置要制作的软盘张数, 最后单击 Write



按钮,即可开始制作启动软盘。驱动软盘制作方法与此相同。

### (2) 在 DOS 命令行制作启动盘

dosutils 目录下面的 rawwrite.exe 是命令行制作程序,可在纯 DOS 环境使用,也可在 Windows 的 MS-DOS 环境下运行。假设放有 Red Hat Linux 第一张光盘的光驱盘符为 G,则制作启动盘的命令为:

```
G:\>cd dosutils
G:\dosutils>rawwrite -f \images\bootdisk.
img -d a -n
```

或者在命令行中直接输入 rawwrite,然后按提示进行相应操作即可。

### (3) 在 Linux 环境下制作启动盘

可在任意一种 Linux 环境下制作,首先准备好一张格式化的 3.5 英寸软盘,插入到软驱中(先不要给 Linux 挂上软驱),然后按以下方式进行操作。Linux 的命令行提示符为 #,命令行注释符也为 #,在以下命令中,命令行之后的 # 及其文字为注释,用于对该命令的功能进行注解说明。

```
# mount /mnt/cdrom/           # 挂载光驱设备
# cd /mnt/cdrom/images/       # 进入光盘的 images 目录
# dd if=bootdisk.img of=/dev/fd0 bs=1440k # 运行 dd 命令,实现制作启动盘
# cd                           # 退出当前目录,并回到当前登录用户的宿主目录,因为接下来要卸载光驱
# umount /mnt/cdrom/          # 卸载光驱,这样才能取出光盘
# mdisk a:                     # 查看软盘文件清单
```

dd 是 Linux 系统的一个实用程序,是 disk dump 的缩写,if 是 input file 的缩写,of 是 output file 的缩写,bs 是 block size 的缩写。该命令是将 bootdisk.img 镜像文件的内容,输出到指定的 /dev/fd0 设备,并规定每次读、写磁盘所存取的块大小为 1440KB。在 Linux 系统中,第 1 个软驱的设备名为 /dev/fd0。

## 3. 准备 Red Hat Linux 安装文件

在进行安装 Red Hat Linux 之前,应准备好所需的安装文件。Red Hat Linux 9 的安装文件有安装光盘、光盘镜像文件(ISO)、安装文件目录树三种提供方式。

安装光盘可直接购买 Red Hat Linux 的发行版来获得,或从官方网站(www.redhat.com)下载光盘镜像文件,然后通过光盘刻录而获得。其光盘镜像文件有 3 个,文件名分

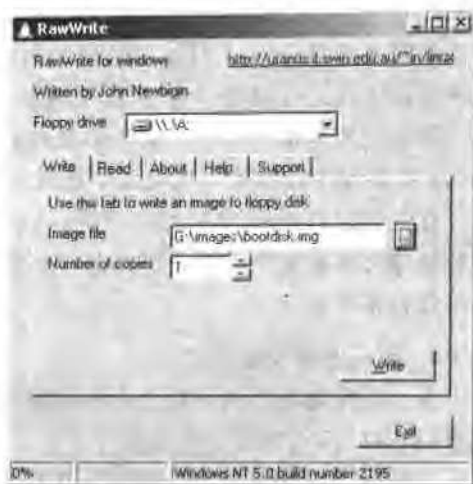


图 1.1 Linux 启动盘制作工具

别是 shrike-i386-disc1.iso、shrike-i386-disc2.iso 和 shrike-i386-disc3.iso。安装目录树是将 3 张安装光盘中 Red Hat 目录中的内容,全部复制到硬盘中而生成一个完整的安装文件目录树。进行网络安装时,需要提供安装文件目录树。

硬盘安装是指将 Linux 的安装文件放置在要安装 Linux 操作系统的主机的硬盘中, Linux 安装程序直接从本机硬盘中读取安装文件进行安装。

在安装时, Linux 安装程序只能识别 ext2、ext3 和 FAT 分区格式,因此应将 Linux 的安装镜像文件放置在该类分区的某个目录中。在安装时,再指定包含有镜像文件的目录,即可开始正常安装。

#### 4. 如何选择安装方式

无论采用哪种方式安装 Linux,都需要先引导并启动安装程序,其启动可以使用启动软盘,也可以采用安装引导光盘。

安装程序启动成功后,将出现图 1.2 所示的安装程序启动界面,在该界面中按 F2 键,就可进入 Option 界面,如图 1.3 所示。在该画面中提供了可供使用的启动选项,在启动提示符(boot:)后输入 linux askmethod,并按回车键,以进入询问安装方式界面,询问用户采用何种安装方式。



图 1.2 Linux 安装程序启动画面

接下来安装程序就会要求用户选择安装界面所使用的语言和键盘的类型(通常选择

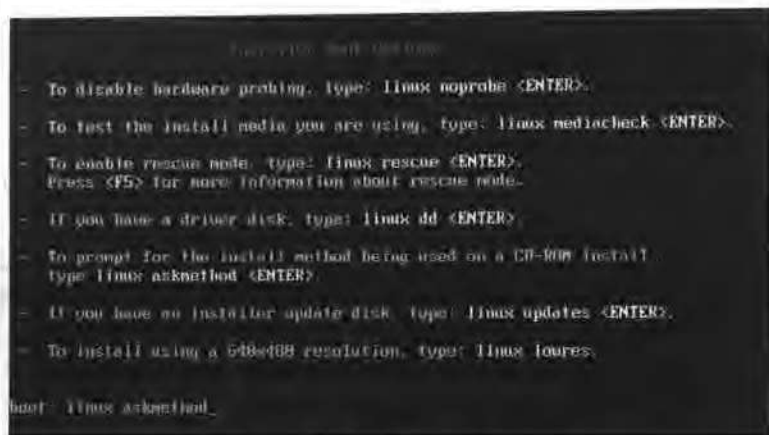


图 1.3 选择询问安装方式

us 类型), 可使用 Tab 键或 Alt+Tab 键在各元素间切换, 利用光标键在列表中进行选择。之后就会出现安装方式选择画面, 如图 1.4 所示。选择具体的安装方式后, 系统就会进入后续的安装。



图 1.4 选择安装方法

## 1.3 安装 Red Hat Linux 9

本节采用最常用的光盘安装方式,介绍 Red Hat Linux 9 的安装方法。Red Hat Linux 9 的安装,根据安装界面的不同,又可分为图形界面安装和文本字符界面安装两种方式。

图形界面安装可使用鼠标进行操作,安装速度较慢;文本字符界面安装只能使用键盘操作,安装速度快,适合于所有要安装 Linux 的主机。Red Hat Linux 9 安装程序支持简体中文、繁体中文和英文以及其他语系等,为使读者尽快适应英文界面,本节采用英文文本字符界面进行安装。

### 1. 启动安装程序

在 CMOS 中进行设置,确保光驱具有优先引导权,并将 Red Hat Linux 9 的第一张安装光盘放入光驱,然后启动计算机。引导程序加载成功后,就会出现安装程序的启动画面,如图 1.2 所示。

若要以图形界面安装,则直接按回车;若要以文本字符界面进行安装,则在安装提示符 boot:后输入 linux text,然后按回车,则开始进入文本字符界面安装方式。

### 2. 测试光盘介质

安装程序提供了测试光盘介质自身正确性的功能,通过该测试,可以检测出光盘是否有物理损坏,或是否有无法正确读取的文件,这样可避免由于某些文件无法读出,而造成安装无法继续的情况。另外,还可确保此光盘是 Red Hat 的官方发布版,而没有经过任何人的篡改,以保证安装程序的安全性。

强烈建议测试完每张安装光盘,Linux 不像 Windows 安装程序,可以跳过读不出的文件,Linux 在安装过程中,只要有一个文件无法读出,则整个安装将宣告失败。

利用 Tab 键,选中 OK 按钮,然后按回车,进入测试界面;若放弃测试,则选择 Skip 按钮,并回车,以跳过测试。在测试界面,选择 Test 按钮并回车,即开始测试当前光盘,测试完毕,将报告测试结果为 Pass(通过)或 Fail(失败)。在测试报告画面,选择 OK 按钮并回车,将弹出光盘,更换光盘后,选中 Test 按钮,继续测试下一张光盘。若不想测试或测试完毕后,放入第一张光盘到光驱,选择 Continue 按钮,然后回车,将结束测试,并进入后续的安装。

### 3. 显示说明信息

在说明信息显示界面,直接选中 OK 按钮,进入下一步。

### 4. 选择安装界面所使用的语言

Red Hat Linux 9 支持多种语言界面,可根据需要进行选择,此处选择默认的

English。若要选择简体中文,则用光标键将光亮条移动到 Chinese(Simplified)选项,再按 Tab 键,将光标移动到 OK 按钮,最后按回车键选中,并进入下一步的安装。

### 5. 选择键盘类型

键盘类型默认为 us,使用该默认值,选中 OK 按钮继续下一步的安装。

### 6. 选择鼠标类型

安装程序一般均能正确检测出系统所使用的鼠标类型,如图 1.5 所示,若不正确,可进行手工选择。Wheel Mouse(PS/2)代表滚轮 PS/2 鼠标,目前较新的主机一般使用的是该类鼠标。Emulate 3 Buttons 选项表示是否模拟 3 键鼠标。选中 OK 按钮继续下一步安装。

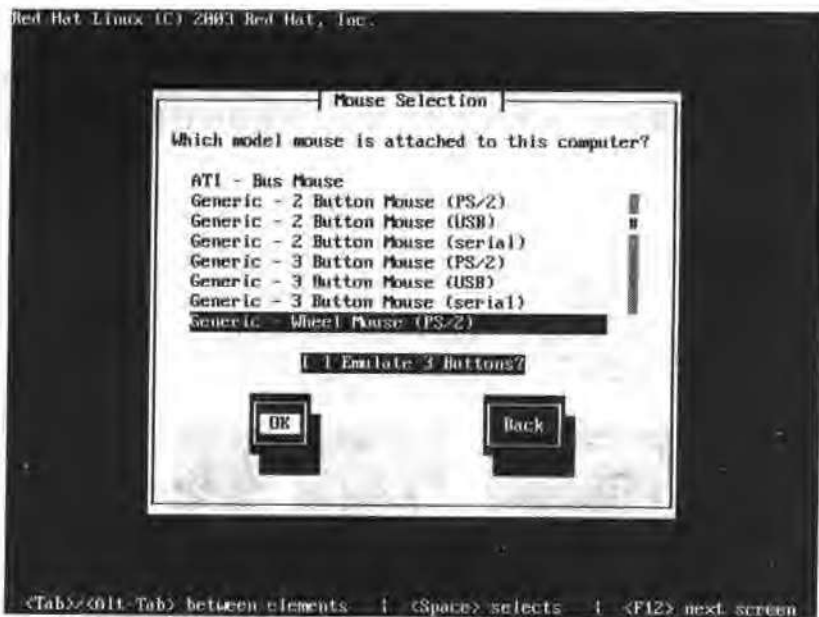


图 1.5 选择鼠标类型

### 7. 选择 Linux 系统安装类型

Red Hat Linux 有 4 种安装类型可供选择,分别是 Personal Desktop(个人桌面)、Workstation(工作站)、Server(服务器)和 Custom(定制)。

Personal Desktop 安装方式要安装图形化桌面环境和应用程序,但不安装服务器软件;Workstation 安装方式安装带有软件开发和系统管理用的图形化桌面环境;Server 为服务器安装,安装各类网络服务器,也可指定是否安装图形化桌面环境和应用程序;Custom 由用户选择要安装的软件包,通常由高级用户使用。

Linux 操作系统通常用作服务器,此处选择 Server 类型,然后选中 OK 按钮继续。

## 8. 为安装准备分区

在正式安装 Linux 系统之前,需要准备好相应的 Linux 分区,安装程序具有创建分区的功能。

### (1) Linux 文件系统类型简介

Linux 内核支持多种不同类型的文件系统,对于 Red Hat Linux 安装程序,能创建的文件系统类型主要是 ext2、ext3、swap 和 vfat。Red Hat Linux 9 默认使用的文件系统是 ext3 和 swap。ext3 是 ext2 的升级版,兼容 ext2,在 ext2 的基础上,增加了日志记录功能,从而提高了数据的安全性,称为日志式文件系统。swap 文件系统在 Linux 中用作交换分区,以提供虚拟内存。

### (2) 选择分区方法

硬盘分区设置界面如图 1.6 所示。Autopartition 为自动创建分区,由安装程序根据用户在第 7 步选择的安装类型自动进行分区的划分。自动分区将重新建立硬盘分区,硬盘中的现有数据将全部丢失。

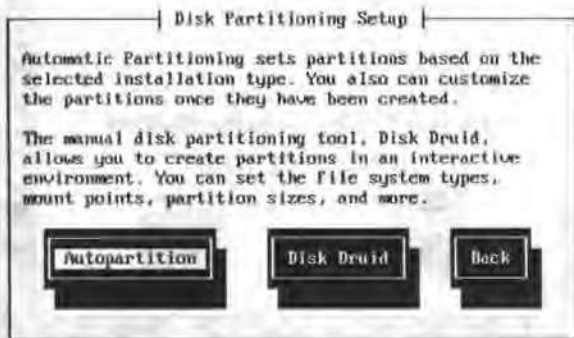


图 1.6 创建硬盘分区

Disk Druid 为手工分区,由用户使用安装程序提供的分区工具,手工创建分区并设置分区的大小。若要使用现有分区进行安装,或硬盘还有其他需要保留数据的分区,则只能选择该方法。

#### ① 自动创建分区

手工分区适合于有多次安装经验的用户,对于初学者或第一次安装 Linux 的用户来说,建议使用自动分区。选中 Autopartition 按钮后,将弹出分区警告信息,若确认要对整个硬盘进行重新分区,选中 Yes 按钮继续。此时将进入自动分区方案选择界面,如图 1.7 所示。

自动分区方案界面的各选项及对应的分区操作如表 1.2 所示。

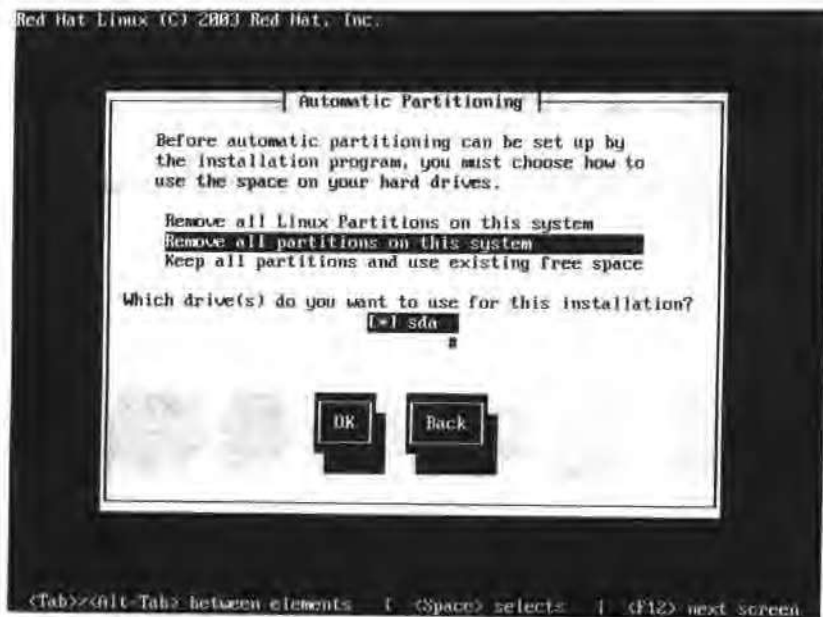


图 1.7 选择自动分区方案

表 1.2 自动分区方案操作表

选 项	分 区 动 作
Remove all Linux Partitions on this system	删除系统中所有 Linux 类型的分区
Remove all partitions on this system	删除系统中的所有分区
Keep all partitions and use existing free space	保留系统中现有的分区,在空闲空间建立 Linux 所需的分区

图 1.7 中,下面的选项是询问在哪个驱动器安装 Linux 操作系统,默认为 sda。sda 在 Linux 中代表第一个 SCSI 硬盘设备。

可根据实际情况选择合理的分区方案,此处选择默认的删除系统中的所有分区,然后选中 OK 按钮,开始自动创建分区。由于删除系统中的所有分区操作比较危险,系统会再次弹出确认操作的警告性对话框,按 Tab 键选择 Yes 按钮,并回车确认该操作。分区操作成功后,将显示如图 1.8 所示的分区信息。

DOS 和 Windows 系统是使用盘符来代表各分区,而在 Linux 操作系统中,则是使用设备文件来代表各分区。Linux 操作系统需要的分区通常有系统引导分区(/boot)、根分区(/)和交换分区.swap),这些对于 Linux 系统的正常启动和运行都是需要的。

Windows 系统使用交换文件来提供虚拟内存,而 Linux 则是使用交换分区来提供虚



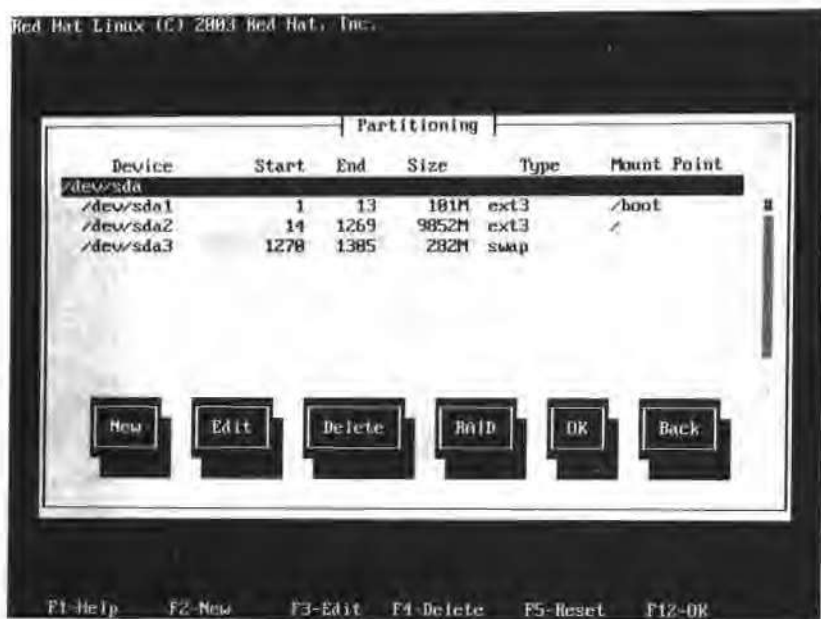


图 1.8 自动分区方案创建的硬盘分区

拟内存。

对 Linux 各分区的说明如表 1.3 的示。

表 1.3 Linux 分区说明

设备文件	分区类型	挂载点	分区说明
/dev/sda1	ext3	/boot	存储 Linux 系统启动时所需的文件,空间需求较少。100MB 左右即可
/dev/sda2	ext3	/	作为系统目录树的根节点,Linux 操作系统及用户文件均放在此处
	swap		交换分区没有挂载点,类型为 swap。大小通常是物理内存的 2 倍

分区自动创建好后,在图 1.8 所示的界面中,还可利用 New、Edit、Delete 按钮所提供的功能,添加分区,或对所选中的分区进行编辑修改或删除。

## ② 手工创建分区

在图 1.6 所示的界面中,选中 Disk Druid 按钮,即可采用手工方式来创建分区。此时将显示类似图 1.8 所示的界面,只是分区都还未创建。通过选中 New 按钮,即可分别创建出所需的根分区、引导分区和交换分区。手工创建分区的界面如图 1.9 所示。

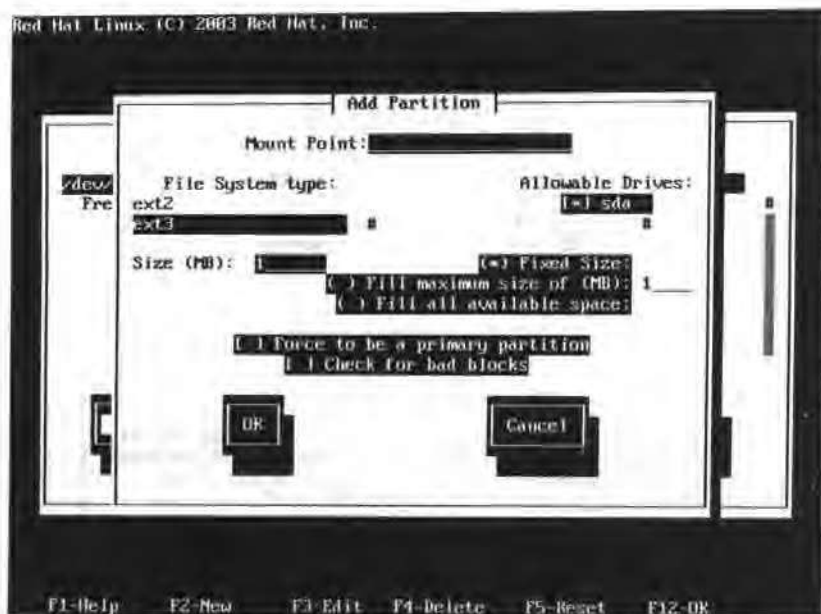


图 1.9 手工创建分区

Mount Point 用于输入分区的挂载点,对于根分区输入“/”,对于引导分区输入“/boot”,交换分区不需要输入。输入完挂载点后,按 Tab 键,选择 File System type(分区文件系统类型)选项,可利用上、下光标键进行选择,对于根和引导分区,通常选择 ext3,对于交换分区,则选择 swap。接下来再按 Tab 键,移到分区大小输入框,输入分区大小(以 MB 为单位),最后选中 OK 按钮,即可创建好该分区。重复该操作,可创建出所需要的各种分区。分区创建好后,选择 OK 按钮,回车继续下一步安装。

## 9. 启动引导器设置

### (1) 选择启动引导器

启动引导器用于引导并启动已安装的 Linux 操作系统。Red Hat Linux 9 提供有 GRUB 和 LILO 两种启动引导器,如图 1.10 所示。GRUB 功能强大,推荐选用该引导器;LILO 历史较长但功能简单,现在一般使用较少。No Boot Loader 表示不安装启动引导器,一般不应选择该选项,除非打算使用第三方的启动引导程序。选中 OK 按钮继续,此时将显示启动引导器参数设置界面,如图 1.11 所示。

### (2) 配置启动引导器参数

对于一些特殊的主机硬件,需要对启动引导器设置相应参数才能正常引导并启动系统。但对于大多数情况都是不需要的,可保持设置为空,直接选中 OK 按钮继续,此时将显示启动口令设置界面。

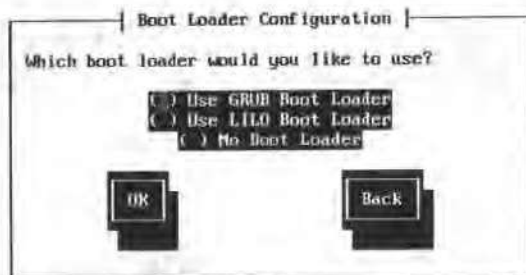


图 1.10 选择启动引导器

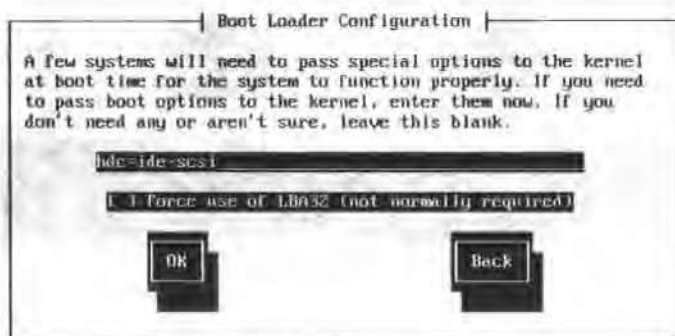


图 1.11 配置启动引导器

### (3) 设置启动引导器口令

GRUB 提供了口令保护功能,如果需要口令保护,则在图 1.12 所示的界面中,按 Tab 键选择 Use a GRUB Password 选项,然后按空格键,选中该选项,并在 Boot Loader

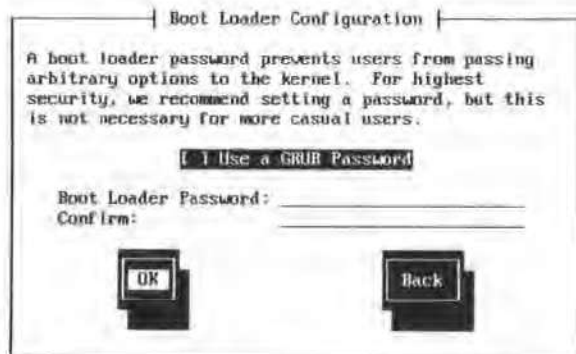


图 1.12 设置启动引导器口令

Password 输入框中输入口令,在 Confirm 输入框中再次输入要设置的口令。

设置口令后,再启动时,必须正确输入该口令后,启动引导器才能使用。

选中 OK 按钮继续,此时将显示配置启动菜单的界面,如图 1.13 所示。

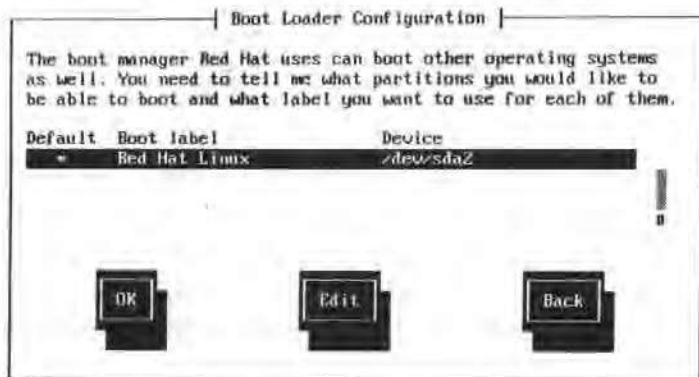


图 1.13 配置 GRUB 启动菜单

#### (4) 配置启动菜单

GRUB 支持多操作系统的引导启动,若在安装 Linux 操作系统时,硬盘中还安装有其他操作系统(如 Windows 9x 或 Windows 2000 等),Linux 安装程序会自动搜索这些已安装的操作系统,并将其添加到 GRUB 的启动菜单中,以后通过 GRUB 引导器,即可实现自由启动这些操作系统。

GRUB 提供了设置默认启动项的功能,默认启动项前面带有一“\*”号。其菜单项对应的操作系统设置为默认启动项后,系统再启动时,在经过一定的延时后,如用户未作出选择,则 GRUB 将自动引导并启动默认菜单项对应的操作系统。

本安装由于是全新安装,系统并未安装其他操作系统,因此启动菜单项中只有 Red Hat Linux 一项,并自动设置为默认启动项。

选择 Edit 按钮,可对启动菜单项进行编辑,以修改或设置菜单项的标题。设置好后选中 OK 按钮继续,此时将显示启动引导器安装位置的设置界面,如图 1.14 所示。

#### (5) 设置启动引导器的安装位置

启动引导器的安装位置有两种,通常情况应安装到硬盘的主引导扇区,即 Master Boot Record(MBR),以实现启动计算机时,就可以自动加载运行 GRUB 启动引导器。另外就是安装在启动分区中的第一个扇区,即 First sector of boot partition,这时需要借助安装在 MBR 中的其他引导程序的引导,才能启动该 GRUB 启动引导器。因此,通常应将 GRUB 安装到主引导扇区,这是系统的默认项,因此,直接选中 OK 按钮,结束对启动引导器的设置,继续后面的安装。

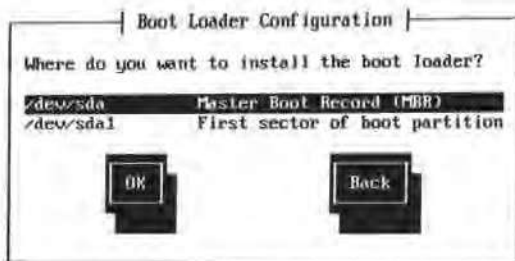


图 1.14 设置启动引导器的安装位置

## 10. 网络配置

Linux 操作系统通常用作服务器操作系统使用,对网络进行配置就十分必要。因此,在安装程序中,提供了对网络的基本配置,以使系统启动后能够进行正常的网络连接。

### (1) 对网卡的配置

在 Linux 操作系统中,第一个以太网卡的设备名为 eth0,第二个为 eth1,其余依次类推。一般情况下,安装程序能够自动检测出主机所使用的网卡类型,并给出配置界面,如图 1.15 所示。

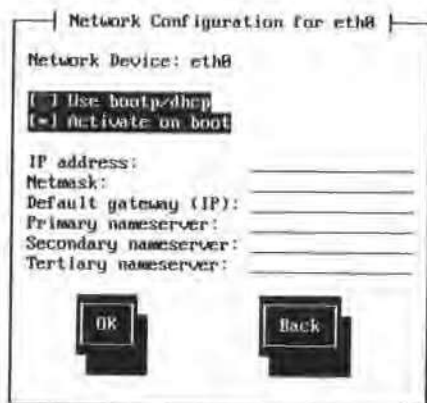


图 1.15 网卡配置界面

网卡 IP 地址的获取方式有自动获取和静态分配两种方式。Linux 默认使用 bootp/ddhcp 启动协议自动获取 IP 地址。若要静态分配,则将选中 Use bootp/dhcp 选项,然后按空格键,取消对该项的选中,再选中 Activate on boot 选项,就可在下面指定 IP 地址、子网掩码 (Netmask)、默认网关 (Default gateway)、主域名解析服务器地址 (Primary nameserver)、次域名解析服务器 (Secondary nameserver) 地址以及第三域名解析服务器地址 (Tertiary nameserver)。

本示例设置 IP 地址为 192.168.5.154、子网掩码为 255.255.255.0、默认网关为 192.168.5.1、主域名解析服务器为 192.168.252.253、次域名解析服务器地址为 61.128.128.68。

Activate on boot 表示是否在启动时激活网卡,让网卡有效。通常应选中该项。设置好后选 OK 按钮继续。

### (2) 设置 Linux 主机名

网卡配置好后,接下来将显示图 1.16 所示的界面,要求设置主机名,此处设置主机名为 rh9。

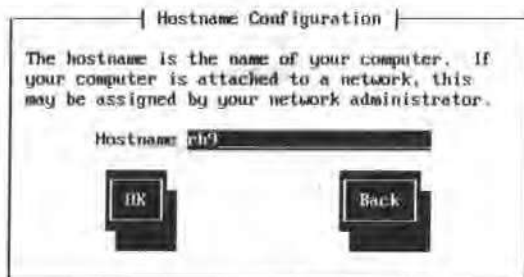


图 1.16 设置主机名称

### (3) 配置防火墙

Linux 内置防火墙功能,主要是通过 iptables 软件来实现的,在安装时,根据防火墙的安全级别,可简单设置为高、中或无防火墙三种情况,如图 1.17 所示。

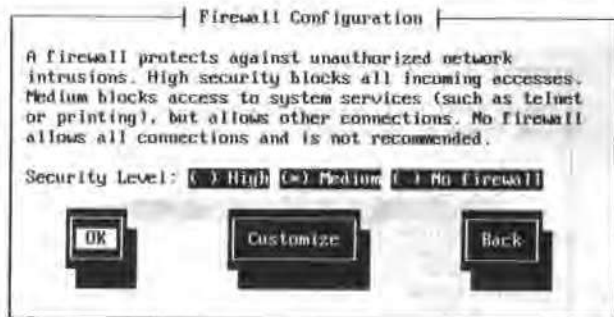


图 1.17 设置防火墙安全级别

默认安全级别为 Medium(中),按 Tab 键选中 Customize,可自定义防火墙的安全规则,此时将显示图 1.18 所示的设置界面。此处设置允许 DHCP、Telnet、WWW、Mail 和 FTP 服务数据包通过。

设置好后,选中 OK 按钮,返回图 1.17 所示的界面,然后再选中 OK 按钮,继续下面

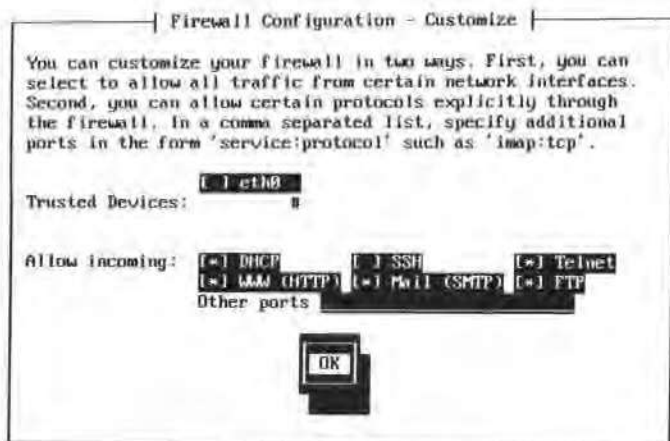


图 1.18 自定义防火墙规则

的安装设置。

### 11. 设置 Linux 操作系统支持的语言

Red Hat Linux 9 的图形界面支持多种语言,包括简体和繁体中文,但在控制台的文本方式下,仍只能使用英文。

可在语言列表中根据需要,选择多种语言,以后在使用时,就可实现各语言间的切换选择。如选择 English 和 Chinese (P. R. of China),如图 1.19 所示,然后选中 OK 按钮继续,接下来系统将显示图 1.20 所示的界面,要求设置图形界面启动时所采用的默认语言,此处设置默认语言为 English,然后选中 OK 按钮继续。

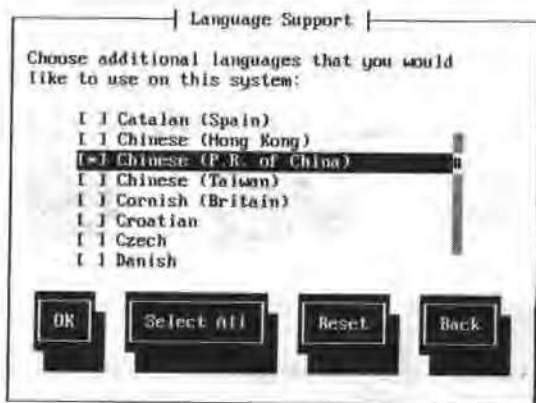


图 1.19 选择 Linux 图形界面支持的语言





图 1.20 设置图形界面启动时的默认语言



图 1.21 设置系统时区

## 12. 设置系统时区

在列表中选择设置时区为 Asia/Chongqing, 即亚洲中国重庆时区, 如图 1.21 所示, 然后选中 OK 按钮继续。

## 13. 设置 root 用户密码

Linux 操作系统的管理员账户为 root, 相当于 Windows 2000 Server 中的 Administrator 账户。此时安装程序将显示 root 用户密码设置界面, 如图 1.22 所示, 设置好密码后, 选中 OK 按钮继续。

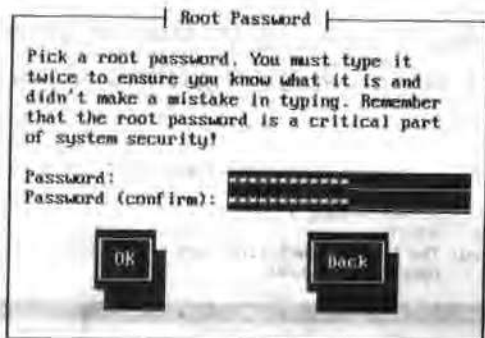


图 1.22 设置 root 用户密码

## 14. 选择要安装的软件包

此时将显示图 1.23 所示的界面, 要求选择要安装的软件包。通过 Tab 键、光标键和空格键相结合, 选中 Administration Tools, DNS Name Server, Development Tools, FTP Server, GNOME Desktop Environment, Graphical Internet, Network Servers, Printing Support, Server Configuration Tools, System Tools, Web Server, Windows File Server,

X-Windows System。Sound and Video 以及 KDE Desktop Environment, 作为对 Linux 的学习和了解, 也可以对其选中安装。



图 1.23 选择要安装的软件包

选择好要安装的软件包后, 选中 OK 按钮继续下一步的安装。此时将显示安装即将开始的提示画面, 并提示安装日志存放在 /root/install.log 文件中。选中 OK 按钮, 确认开始安装。

### 15. 复制并安装软件包

接下来安装程序开始格式化分区并传送安装镜像文件到硬盘, 之后, 便开始复制和安装软件包, 安装界面如图 1.24 所示。在此安装过程中, 会要求插入第二张光盘和第三张光盘。

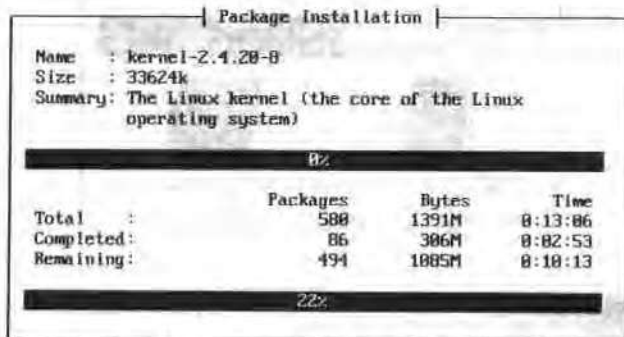


图 1.24 安装软件包

## 16. 制作 Linux 系统启动软盘

在软件包复制安装结束后,安装程序将提示制作一张用于启动 Linux 操作系统的软盘。当硬盘的主引导扇区中的引导程序损坏,无法引导时,可以改用软盘来引导启动 Linux 操作系统。

插入一张空白软盘到软驱中,选中 Yes 按钮,开始制作引导软盘。若不需要制作,则选中 No 按钮,继续下一步安装。

## 17. 配置视频卡

安装程序将开始检测系统安装的视频卡类型和显存的大小,如图 1.25 所示。



图 1.25 配置视频卡类型和显存大小

若检测结果不正确,可选中 Change 选项,在弹出的列表中,进行手工选择。设置好后选择 OK 按钮继续。

## 18. 设置显示器型号和性能参数

安装程序接下来将检测显示器的型号和性能参数,如图 1.26 所示。若不正确,可选中 Change 选项,在弹出的列表中进行手工设置。对于显示器性能,若不清楚,可使用其默认值。

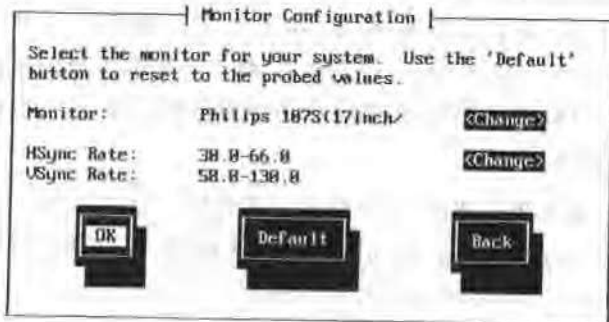


图 1.26 设置显示器类型及性能参数

### 19. 设置图形界面的分辨率及颜色深度

可根据显示器和显卡的性能,设置合理的分辨率和颜色深度。在该设置界面中还可设置系统登录时默认界面类型(图形或文本),此处选择文本方式登录。设置界面如图 1.27 所示。

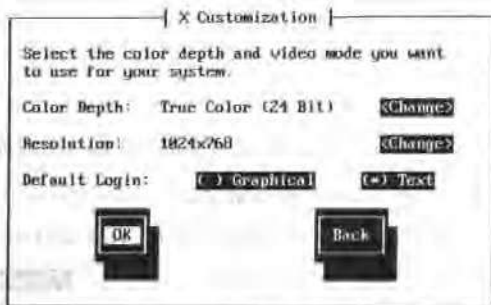


图 1.27 设置图形界面分辨率及颜色深度

选择 OK 按钮,并回车,此时将退出安装光盘,并显示安装完成的祝贺画面,并提示移除软盘,选择 OK 按钮,结束整个 Linux 的安装,并进入首次系统启动。

## 1.4 Linux 的启动与登录

Red Hat Linux 安装完毕,接下来就可启动了,启动成功后,系统将要求用户登录,只有登录成功,才能访问和使用系统。

### 1.4.1 Red Hat Linux 的启动

Linux 通过硬盘启动后,将进入 GRUB 的启动菜单画面,如图 1.28 所示。默认 10 秒等待用户选择要进入的操作系统,若没有选择,则自动进入默认系统。

选中 Red Hat Linux 操作系统后,或 10 秒过后,将自动开始引导 Red Hat Linux 操作系统,其引导过程如图 1.29 所示,引导完毕后,将进入文本虚拟控制台登录界面。若安装时设置的默认登录界面为图形界面,则将启动图形系统,并进入图形登录界面。

### 1.4.2 登录与注销

文本虚拟控制台登录界面如图 1.30 所示。首先输入登录者账户名,如 root,然后在 Password 提示行输入对应的密码,输入的密码不会回显,校验通过后就能登录到 Linux 系统,此时将出现 Linux 的命令行提示符#,在命令行中,通过键入命令,即可操作和使用 Linux 系统了。root 用户登录后,命令行提示符为#,普通用户登录后,命令行提示符为\$。Linux 是多用户多任务操作系统,任何用户要使用 Linux 系统,都必须登录。



图 1.28 Red Hat Linux 的启动菜单界面

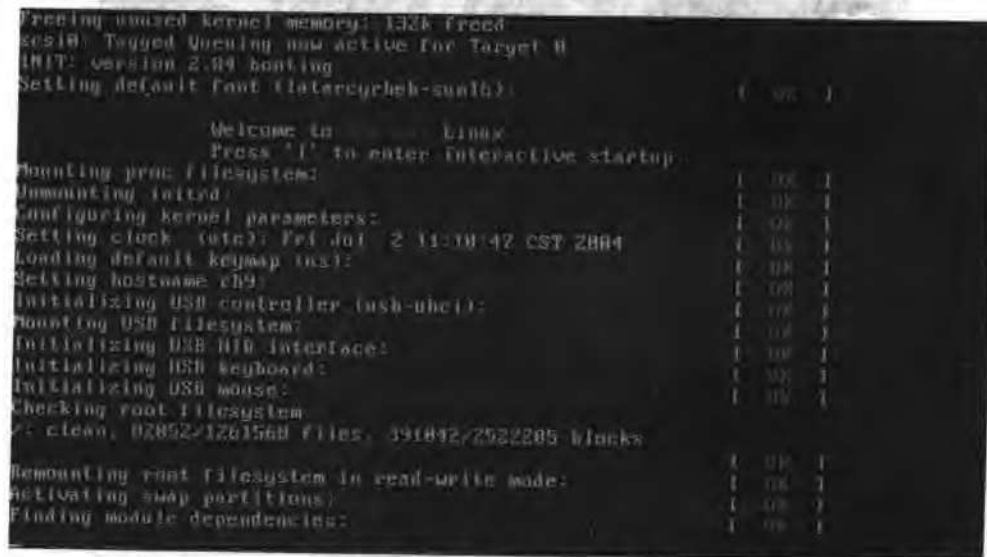


图 1.29 Red Hat Linux 引导过程

```
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8 on an i686

rh9 login: root
Password:
[root@rh9 root]#
```

图 1.30 Linux 的登录

在命令行提示符( # )的左边,显示有相关提示信息,各部分的含义如下:

```
[root@rh9 root]#
```

↓ 当前用户    
 ↓ Linux 主机名    
 ↓ 当前目录名

用户登录成功,会自动进入该用户的宿主目录,root 用户的宿主目录为 /root,所以当前目录名为 root。在任何位置,通过执行 cd 命令,可快速回到自己的宿主目录。清屏可使用 clear 命令。

在 # 提示行上输入“cd 目录名”命令可进入指定的目录,使用“cd ..”可返回上一级目录,使用“cd /”可返回根目录,使用 ls 或 ll 命令可查看目录文件清单。在命令行状态下键入 startx,即可启动进入 Red Hat Linux 的图形界面(X-Windows),图形界面与 Windows 极为类似,操作方式也类似,如图 1.31 所示。



图 1.31 Red Hat Linux 的图形界面

在文本虚拟控制台(tty)界面下,若要注销当前用户,以其他用户身份登录,则可键入 `logout` 或 `exit` 命令;若要重新启动系统,可键入 `reboot` 或 `shutdown -r`;若要关机退出,则键入 `shutdown -h now`;键入“命令?”或“命令 -help”可获得对该命令的详细用法帮助。

直接关掉电源可能引起严重的磁盘错误,这是不安全的做法,正确关闭系统是非常重要的。要使用 `shutdown` 命令,必须是 `root` 用户或者使用 `su` 命令切换到 `root` 身份。

在图形界面中,选择 `System Tools` 下面的 `Terminal` 菜单项,可打开仿真终端窗口,如图 1.32 所示。在该窗口中,可通过执行命令来完成相关操作。执行 `exit` 命令,关闭该终端窗口。

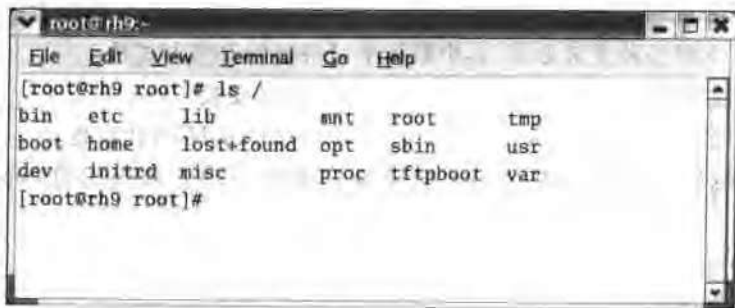


图 1.32 图形界面中的终端窗口

进入 X-Windows 图形界面系统后,按 `Ctrl+Alt+F2` 键可回到文本控制台界面,按 `Ctrl+Alt+F7` 键可返回 X-Windows 界面。

Linux 允许同时打开 6 个(`tty1~tty6`)文本虚拟控制台进行输入和操作。启动 Linux 后,默认使用 1 号虚拟控制台,按 `Alt+F1~F6` 的一个功能键,可以选择指定的虚拟控制台登录,也可用同样的方法在虚拟控制台之间进行自由切换。对于 X-Windows 界面下的仿真终端(`pts/0, pts/1, ...`)窗口,则用 `Shift+Alt+F1~F6` 进行选择或切换。利用虚拟控制台,可以实现以不同用户身份登录,或用于实现同时运行多个应用程序。

## 习题

1. 以下不属于服务器操作系统的是( ),其中公认的性能最好的服务器操作系统是( )。

- |               |                        |
|---------------|------------------------|
| A. Windows XP | B. Windows 2000 Server |
| C. Linux      | D. UNIX                |

2. 制作 Red Hat Linux 9 的安装启动软盘,需要使用的镜像文件是( )。

- |                 |               |
|-----------------|---------------|
| A. bootdisk.img | B. drvnet.img |
|-----------------|---------------|

- C. drvblock.img                      D. pcmciadd.img
3. 在 Windows 系统中,若要制作 Red Hat Linux 9 的安装启动盘,应使用( )实用程序来实现。
- A. rawwritewin      B. rawwrite              C. dd                      D. HD
4. 制作启动盘的实用程序,位于 Red Hat Linux 9 第一张安装光盘的( )目录中,制作启动软盘所需的镜像文件位于( )目录中。
- A. images              B. tools                      C. dosutils              D. Redhat
5. Linux 的管理员账户名为( ),登录成功后,其命令行提示符为( )。
- A. Administrator      B. root                      C. #                      D. \$
6. Linux 支持多种安装方式,其中最简单最快捷的安装方式是( )。
- A. 光盘安装                      B. 硬盘安装  
C. NFS 映像安装                      D. FTP 或 HTTP 安装
7. 若要选择安装方式,在 Linux 的安装启动画面的安装提示符(boot:)下,应键入( )。
- A. linux text  
B. 直接回车  
C. 按 F2,然后输入 linux askmethod  
D. linux dd
8. 以下对 Linux 的说法中,不正确的是( )。
- A. Linux 只能用作服务器操作系统,不能作为桌面操作系统使用,缺乏常用的办公字处理软件  
B. Linux 的应用主要在服务器操作系统领域  
C. Linux 是一种 32 位的多用户多任务操作系统,能运行在基于 Intel x86 系列 CPU 的计算机上  
D. UNIX 都不能运行在基于 Intel x86 系列 CPU 的计算机上  
E. Linux 正常运行至少要有“/”、“/boot”和“swap”三个分区
9. Red Hat Linux 9 默认使用的文件系统类型为( )。
- A. ext2                      B. ext3                      C. FAT                      D. swap
10. Linux 利用交换分区空间来提供虚拟内存,交换分区的文件系统类型必须是( )。
- A. ext2                      B. ext3                      C. FAT                      D. swap
11. 在 Linux 中,选择使用第 2 号虚拟控制台,应按( )功能键。
- A. F2                      B. Ctrl+F2                      C. Alt+F2                      D. Alt+2
12. 在 Linux 的 X-Windows 界面,若要退回到文本虚拟控制台界面,则应按( )功



能键。

- A. Ctrl+Alt+F2    B. Ctrl+Alt+F7    C. Ctrl+F2    D. F7
13. 在默认情况下,要重启 Linux 操作系统,以下方法中,不正确的是( )。
- A. 在#命令提示符下,键入 reboot 命令并回车  
B. 在\$命令提示符下,键入 reboot 命令并回车  
C. 在#命令提示符下,键入 shutdown -r 命令并回车  
D. 直接按 Ctrl+Alt+Del 键
14. 在 Linux 中,要查看目录文件清单,可使用( )命令;根目录采用( )表示;若要进入根目录下面的 mnt 目录,则实现命令为( );若要返回上一级目录,则应执行( )命令;若要返回根目录,则应执行( )命令。
- A. ls 或 ll    B. /    C. \    D. cd /mnt  
E. CD /mnt    F. cd \mnt    G. cd ..    H. cd /  
I. cd \
15. 以下命令中,只有 root 用户才有权执行的是( )。
- A. shutdown    B. logout    C. ls    D. reboot

## 实训 1-1 搭建 Linux 学习环境

**[实训目的]** 学习并掌握利用 VMware Workstation 软件来创建虚拟计算机的方法,并利用该虚拟计算机作为 Linux 的安装和运行环境。

### **[硬件要求]**

计算机硬件:一台具有光驱并具有光驱启动能力的计算机,硬盘自由空间不低于 2GB,内存不低于 256MB,有网卡并能正常工作。

操作系统:可使用 Windows 9x,但建议使用 Windows 2000 Server 或 Professional 版。

### **[Linux 运行环境说明]**

要安装和运行 Linux,可直接在计算机上进行安装和运行,Linux 支持在同一个硬盘上安装和运行多个不同的操作系统。要在计算机上同时安装多个不同的操作系统,一般应先安装其他操作系统,如 Windows 9x、Windows 2000,最后再安装 Linux 操作系统,这样就可利用 Linux 的 GRUB 启动菜单,来选择所要启动的操作系统。

对于 Linux 初学者,直接在硬盘上安装会冒极大的风险。在安装过程中,由于要创建 Linux 所需的分区,就要求硬盘上必须有还没有划分使用的空间(不是现有分区的可自由使用空间)。其次,在分区操作过程中,若操作不当,就会造成硬盘中原分区数据的全部丢失。因此,对于初学者,建议在原操作系统(如 Windows 2000)中安装虚拟主机,然后在虚

拟主机中安装和运行 Linux 操作系统,这样就不会对原操作系统和硬盘中的数据造成任何损害,本实训环境就采用该方式。

虚拟主机也称虚拟计算机,它是利用软件在原操作系统中,模拟出来的一台计算机,具有与真实计算机相同的特性,该计算机的内存使用部分现有计算机的内存,硬盘空间也是使用现有的部分硬盘空间。

能够用来在一个操作系统中模拟出虚拟计算机的软件,目前常用的主要是 VMware 和 Virtual PC。VMware 功能更强大,支持捕获虚拟计算机画面,该软件有两种版本,一种是运行于 Windows 9x 平台,另一种是运行于 Windows 2000 平台的 VMware Workstation,最新版本为 4.5.2。本实训环境以 VMware Workstation 为例,介绍虚拟主机的创建和使用方法。

### [创建虚拟计算机]

#### 1. 安装 VMware Workstation 软件

访问 <http://www.pcnetedu.com> 站点或官方站点 <http://www.vmware.com/download/>, 下载 VMware Workstation 软件,然后运行下载所得的 VMware-workstation-4.5.2-8848.exe,安装该软件。

#### 2. 创建虚拟计算机

在桌面双击 VMware Workstation 快捷键图标启动该软件,如图 3.33 所示。左边的 Favorites 栏用于显示当前已创建的虚拟主机名。在右边的 Home 页面显示有 New

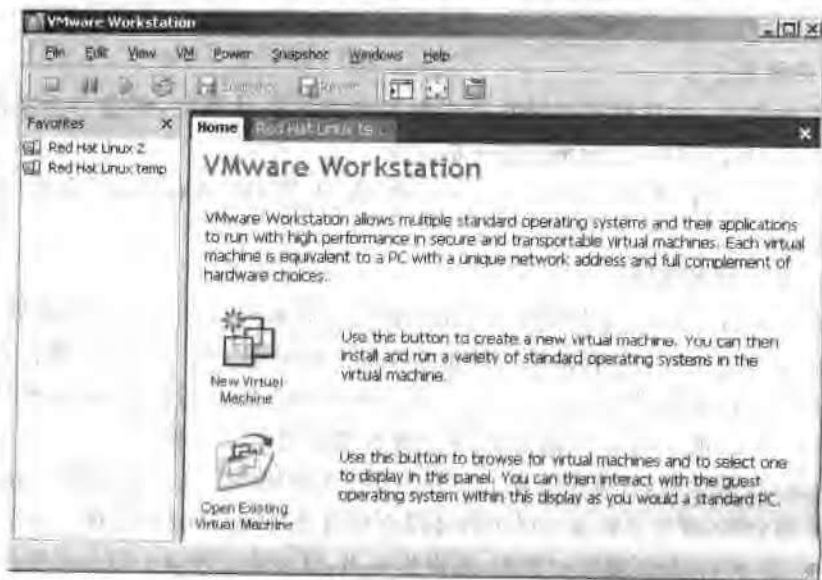


图 1.33 VMware Workstation 主界面

Virtual Machine 和 Open Existing Virtual Machine 两个功能图标,分别用于实现创建新的虚拟主机和打开已存在的虚拟主机。根据需要,可创建出多个虚拟主机,虚拟主机创建后,只有打开虚拟主机的电源(Power On),即启动虚拟主机后,系统才开始模拟出该虚拟主机的硬件环境。虚拟主机同时运行的数目受限于当前计算机的 CPU、内存和硬盘容量。

### (1) 创建虚拟主机

单击 New Virtual Machine 图标,此时将打开虚拟主机创建向导,单击“下一步”按钮,将显示虚拟主机配置选择对话框,有 Typical 和 Custom 两种选择,直接单击“下一步”按钮,使用默认的 Typical 选项,此时将打开图 1.34 所示的对话框,要求选择虚拟主机要运行的操作系统类型和版本。此处选择 Linux,在下面的 Version 下拉列表框中,选择 Linux 的版本为 Red Hat Linux,然后单击“下一步”按钮,出现图 1.35 所示的对话框,在对话框中设置虚拟主机的标题,然后在 Location 输入框中输入或选择虚拟主机文件的存入位置。虚拟主机是用文件来模拟的,虚拟主机的硬盘占用了多少空间,则对应的模拟文件也要占用相应大小的物理硬盘空间,因此,最好将其指定到硬盘自由空间较大的分区中,此处指定为 D:\My Virtual Machines\Red Hat Linux,继续单击“下一步”按钮,此时要求选择网络的连接方式,使用默认的网桥方式,直接单击“下一步”按钮,此时弹出对话框,要求指定虚拟主机的硬盘空间大小,以 GB 为单位,默认为 4GB,可根据自己硬盘空间大小进行设置,若要指定为 10GB,则输入 10,最后单击“完成”按钮,就实现了虚拟主机的创建,如图 1.36 所示。



图 1.34 选择虚拟主机要运行的操作系统和版本

### (2) 编辑虚拟主机设置

虚拟主机创建后,在左边的 Favorites 收藏夹中选中该虚拟主机后,单击工具栏中带

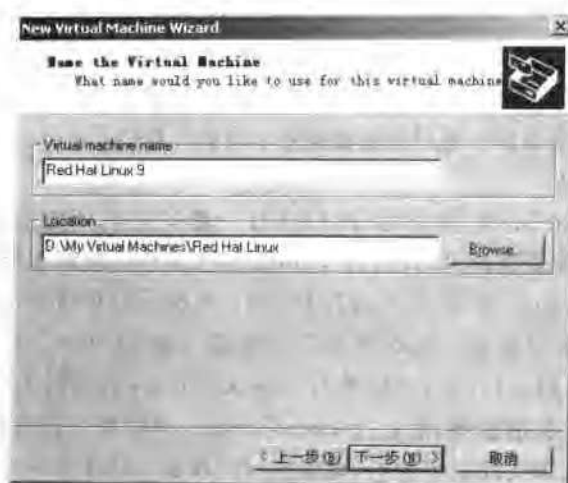


图 1.35 设置虚拟主机标题和虚拟主机文件的存放位置



图 1.36 创建好的虚拟主机

绿色箭头的按钮,即可给虚拟主机加电启动,或者单击 Start this virtual machine 图标。

首次运行时,系统一般会弹出图 1.37 所示的消息框,提示没有足够的物理内存供虚拟主机使用,并建议将虚拟主机的内存降低为 136MB。单击 OK 按钮,关闭消息框,然后单击 Edit virtual machine settings,对虚拟主机的硬件配置进行调整,将内存大小按提示要求设置为 136MB,在左边的硬件列表中单击选中 CD-ROM,然后在右边的“Connection”

选项中,选择 Use physical driver,即设置虚拟主机使用物理光驱。单击 Add 按钮,还可为该虚拟主机添加其他硬件配置,比如增加一个硬盘、光驱或软驱等,设置好后单击 OK 按钮退出。

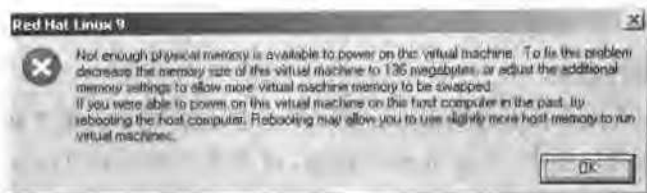


图 1.37 提示没有足够物理内存供虚拟主机使用

重新给虚拟主机加电启动,此时应可正常启动了。注意,此时的虚拟主机就相当于只有硬件系统的计算机,还没有安装任何软件,接下来就应安装相应的操作系统,操作系统安装完成后,该虚拟主机就可正常启动并能正常工作了。前面在创建虚拟主机时,选择操作系统类型,主要是让配置向导根据该操作系统的运行要求,合理配置该虚拟主机的硬件。

进入 D:\My Virtual Machines\Red Hat Linux 目录,将会发现几个虚拟主机所使用的文件,包含有硬盘图标的文件,是用来模拟虚拟主机的硬盘的,一个这样的文件对应着一个硬盘。

## 实训 1-2 安装 Red Hat Linux 9

[实训目的] 学习并掌握 Red Hat Linux 9 的安装、启动与关机方法。

[实训环境] 在前面“实训 1-1”搭建好的虚拟主机中安装和运行。

[实训内容]

### 1. 准备工作

首先检查当前计算机的首选启动设备是不是光驱,若不是,则在 CMOS 中设置光驱为首选的启动设备。重启时,注意先不要将 Red Hat Linux 9 的第一张安装光盘放入光驱中。

### 2. 安装 Linux

操作系统启动成功后,放入 Red Hat Linux 9 的第一张安装光盘到光驱中,然后启动 VMware Workstation 软件,在左边的收藏夹中选中 Red Hat Linux 9 虚拟主机,单击 Start this virtual machine 图标,启动虚拟主机,之后虚拟主机就能从光驱启动系统,并开始启动 Linux 系统的安装向导。然后按教材所讲步骤,完成 Linux 操作系统的安装。

### 3. Linux 的基本操作

基本操作练习：Linux 的启动、登录（包括选择不同的虚拟控制台进行登录）、查看 Linux 系统的目录文件、文本虚拟控制台与 X-Windows 界面的切换、注销、重启与关机等操作。

### 4. VMware 操作提示

注意：每次在虚拟主机中启动 Linux 时，应快速选择 VM 菜单下的 Install VMware Tools，并在弹出的对话框中，单击 Install 按钮，以安装 VMware Tools 工具。该工具可以增强虚拟主机的图形支持能力和鼠标性能，从而使虚拟主机上的操作系统能支持 16 位或以上的颜色，并使鼠标移动和操作灵活自如。该工具包只有在虚拟主机运行时才能安装。

虚拟主机上的操作系统启动成功后，当前的计算机上实际上同时运行了两个操作系统，用户的鼠标如何在这两个操作系统之间切换，以操作不同的系统呢？其方法如下：

若要从父操作系统进入客户操作系统（虚拟主机上的操作系统），可以用鼠标在虚拟主机屏幕上单击一下，此时鼠标就属于客户操作系统了，此时的键盘和鼠标均属于客户操作系统了。若要从客户操作系统中退出来操作父操作系统，则按 Ctrl+Alt 键即可。



图 1.38 在虚拟主机中运行 Linux 操作系统

Ctrl+Alt+Del 键是 Windows 2000 中定义的用于弹出任务管理器的快捷键,若要将 Ctrl+Alt+Del 键动作传递给客户操作系统 Linux,在 VMware 中,定义了一个替换键 Ctrl+Alt+Insert 键,按 Ctrl+Alt+Insert 键,就相当于在客户操作系统中按了 Ctrl+Alt+Del 键。

若要全屏幕运行客户操作系统,可按 Ctrl+Alt+Enter 键来实现,若要返回到 VMware 窗口界面,则按一下 Ctrl+Alt 键即可。

Linux 在虚拟主机中启动成功后的 X-Windows 界面如图 1.38 所示。

图 1.38

## 第 2 章

# Linux 磁盘文件管理

本章主要介绍 Linux 的文件系统、磁盘目录结构以及常用的磁盘文件操作命令,以进一步熟悉 Linux 的相关知识和操作环境,掌握常用的一些基本操作。

## 2.1 Linux 文件系统类型

不同的操作系统需要使用不同类型的文件系统,为了与其他操作系统兼容,以相互交换数据,通常操作系统都能支持多种类型的文件系统。比如 Windows 2000 Server,系统默认或推荐采用的文件系统是 NTFS,但同时也支持 FAT32 或 FAT16 文件系统;DOS 和 Windows 9x 一般采用 FAT16 或 FAT32,不支持 NTFS 文件系统。

Linux 内核支持十多种不同类型的文件系统,对于 Red Hat Linux,系统默认使用 ext2 或 ext3 和 swap 文件系统。下面对 Linux 常用的文件系统作一个简单介绍。

### 1. ext2 与 ext3 文件系统

ext 是第一个专门为 Linux 设计的文件系统类型,称为扩展文件系统,在 Linux 发展的早期,起过重要的作用。由于在稳定性、速度和兼容性方面存在许多缺陷,现已很少使用。

ext2 是为解决 ext 文件系统存在的缺陷而设计的可扩展、高性能的文件系统,称为二级扩展文件系统。ext2 于 1993 年发布,在速度和 CPU 利用率上具有较突出的优势,是 GNU/Linux 系统中标准的文件系统,支持 256 个字节的长文件名,文件存取性能极好。

ext3 是 ext2 的升级版本,兼容 ext2,在 ext2 的基础上,增加了文件系统日志记录功能,称为日志式文件系统,是目前 Linux 默认采用的文件系统。日志式文件系统在因断电或其他异常事件而停机重启后,操作系统会根据文件系统的日志,快速检测并恢复文件系统到正常的状态,并可提高系统的恢复时间,提高数据的安全性。若对数据有较高安全性要求,建议使用 ext3 文件系统。



日志文件系统是目前 Linux 文件系统发展的方向,除了 Red Hat Linux 采用的 ext3 外,常用的还有 reiserfs 和 jfs 等日志文件系统。

### 2. swap 文件系统

swap 文件系统用于 Linux 的交换分区。在 Linux 中,使用整个交换分区来提供虚拟内存,其分区大小一般应是系统物理内存的 2 倍。

在安装 Linux 操作系统时,就应创建交换分区,它是 Linux 正常运行所必需的,其类型必须是 swap。交换分区由操作系统自行管理。

### 3. vfat 文件系统

vfat 是 Linux 对 DOS、Windows 系统下的 FAT(包括 FAT16 和 FAT32)文件系统的统称。Red Hat Linux 支持 FAT16 和 FAT32 分区,也能在该系统中通过相关命令创建 FAT 分区。

### 4. NFS 文件系统

NFS 即网络文件系统,用于在 UNIX 系统间通过网络进行文件共享,用户可将网络中 NFS 服务器提供的共享目录,挂载到本地的文件目录中,从而实现操作和访问 NFS 文件系统的内容。

### 5. ISO 9660 文件系统

该文件系统是光盘所使用的标准文件系统,Linux 对该文件系统也有很好的支持,不仅能读取光盘和光盘 ISO 映像文件,而且还支持在 Linux 环境中刻录光盘。

Red Hat Linux 支持的文件系统很多,在此就不逐一介绍,要想了解其支持的文件系统类型,可通过以下命令来查看:

```
# ls /lib/modules/2.4.20-8/kernel/fs
```

## 2.2 Linux 系统的目录结构

Linux 安装后,由系统产生的目录比较多,初学者对这众多的目录,通常会感到很迷惑,不知这些目录有何作用,彼此间有何区别,用户自己的目录创建在哪个目录下比较合适,本节针对这些问题,介绍 Linux 的目录结构以及系统对目录的基本约定。

### 1. 目录结构简介

与 DOS 和 Windows 系统一样,Linux 也使用树形目录结构来组织和管理文件,所有的文件采取分级、分层的方式组织在一起,从而形成一个树型的层次结构。在整个树型结构中,只有一个根目录(树根)位于根分区,其他目录、文件以及外部设备(包括硬盘、软驱、光驱、调制解调器等)文件都是以根目录为起点,挂接在根目录下面的,即整个 Linux 的文

件系统,都是以根目录为起点的,其他所有分区都被挂载到目录树的某个目录中。通过访问挂载点目录,即可实现对这些分区的访问。

在 DOS 和 Windows 操作系统中,每个分区都有一个独立的根目录,各分区采用盘符进行区分和标识,而 Linux 操作系统只有一个根目录。Linux 的根目录用“/”表示,路径表示可采用绝对路径,也可采用相对路径。

## 2. Red Hat Linux 9 的目录结构

Red Hat Linux 9 采用标准 Linux 目录结构,从根目录开始的每个目录都用于存储某特定类型的文件,根目录下的目录如下所示:

```
[root@rh9 root]# ls /
bin    dev    home   lib          misc    opt     root   tftpboot  usr
boot  etc    initrd  lost+found  mnt     proc   sbin   tmp       var
```

下面分别介绍一些常用目录的功能与作用。

### (1) /bin 和/sbin

对 Linux 系统进行维护操作的实用命令基本上都包含在/bin 和/sbin 目录中。

/bin 目录通常存放用户最常用的一些基本命令,包括对目录和文件操作的一些实用程序、系统实用程序、压缩工具、RPM 包管理程序等,如 login、date、ping、netstat、mount、umount、su、vi、rpm 等。

/sbin 目录中存放的是只允许系统管理员(root)运行的一些系统维护程序,即只有用 root 账户登录后,才能执行/sbin 目录中的命令。如 fdisk、mkfs、ext3、mkfs、vfat、shutdown、dump、route、iptables 等。

### (2) /dev

dev 是 device(设备)的简写,/dev 目录是一个非常重要的目录,用于存放系统中所有设备的设备文件。

Linux 将每一个 I/O 设备都看成一个文件,与普通文件一样处理,这样可以使文件与设备的操作尽可能统一。从用户的角度来看,对 I/O 设备的使用和普通文件的使用一样,不必了解 I/O 设备的细节。设备文件可以细分为块设备文件和字符设备文件,前者的存取是以一个个字符块为单位的,后者则是以单个字符为单位的。

对设备文件进行操作,实际上是在操作该文件对应的物理设备,一些常用外部设备的名称需要牢记。

IDE 硬盘设备的设备文件名以 hd 开头,后面按设备的 ID 号顺序从英文字母 a 开始顺次命名。因此,第 1 个 IDE 硬盘的设备名为 hda,第 2 个 IDE 硬盘为 hdb;对于硬盘中的分区,则在设备文件名后增加相应的数字来代表相应的分区,主分区从 1 开始,逻辑分区从 5 开始(一个硬盘最多可建 4 个主分区)。第 1 个 IDE 硬盘中的第 1 个主分区的设备

文件名为 hda1,第2个主分区为 hda2,第1个逻辑分区为 hda5,第2个逻辑分区为 hda6。

SCSI 设备(如 SCSI 硬盘,USB 设备)的命名方法与 IDE 硬盘相同,只是设备名前两个字符为 sd。比如,第1个 SCSI 设备的设备名为 sda,第2个 SCSI 设备名为 sdb,第1个 SCSI 硬盘的第1个逻辑分区为 sda5。第1个 IDE 光驱的设备名为 hdc,第1个软驱的设备名为 fd0。在具体使用时,应注意表达出完整的设备文件名及路径,比如若要格式化软盘,则命令应表达为:

```
# mke2fs /dev/fd0
```

光驱常用的设备文件名为 /dev/cdrom,它实际上是一个符号链接文件,该文件指向实际的光驱设备。可用以下命令查看当前光驱的实际设备文件名。

```
# ll /dev/cdrom
```

```
lrwxrwxrwx 1 root root 8 Jun 14 12:01 /dev/cdrom -> /dev/hdc
```

另外,SCSI 磁带设备的设备文件用 /dev/st 来表示;计算机的串行接口用 /dev/ttyS 表示,其中的 COM1 的设备文件名为 /dev/ttyS0;调制解调器的设备名为 /dev/cua;空设备用 /dev/null 表示,任何输出到该设备的信息将有去无回,若以该设备作为输入,则会创建一个零长度的文件。鼠标常用的设备名为 /dev/mouse,它是指向鼠标实际连接设备的一个符号链接文件,若鼠标接在 COM1,则连接的实际鼠标设备为 /etc/ttyS0;若接在 PS2 接口上,则连接的实际设备名是 /dev/psaux;对于 USB 鼠标, /dev/mouse/ 指向的是 /dev/input/mice。

### (3) /home

系统中所有普通用户的宿主目录,系统默认放在 /home 目录中(通过在创建用户时使用 -d 参数,也可指定放在其他位置),root 用户的宿主目录为 /root。新建用户账户后,系统就会自动在该目录中创建一个与账户同名的子目录,作为该用户的宿主目录。普通用户只能访问自己的宿主目录,无权访问其他用户的宿主目录。

### (4) /lib

lib 是 library 的简写,用于存放系统的动态链接库,几乎所有的应用程序都会用到这个目录下的共享库。

### (5) /usr

/usr 目录一般用来存放与用户直接相关的程序或文件。用户安装的程序或要自行建立的目录,一般应放在该目录下面,它是占用硬盘空间最大的一个目录。其下一些比较重要的子目录,主要有:

/usr/bin 存放有一些实用程序。

/usr/etc 存放有许多各种各样的配置文件。

/usr/include 该目录及其子目录是存放 C 编译程序的所有包含文件。对编译

Linux 源程序至关重要。

/usr/lib 包含有程序编译后在连接时需要使用的各种库。

/usr/src 用于存放 Linux 源程序。

/usr/local/src 通常用来存放 Linux 的软件安装包源代码。

/usr/local 用户软件包通常安装在该目录中。

(6) /boot

/boot 目录用于存放与系统启动相关的各种文件,包括系统的引导程序和系统内核程序。不要轻易对该目录进行操作。

(7) /etc

/etc 目录也是 Linux 系统中一个非常重要的目录,用于存放系统管理时要用到的各种配置文件,包括网络配置、设备配置信息、X-Windows 系统配置、用户信息等。如 securetty,passwd,inittab,fstab。

(8) /lost+found

/lost+found 目录用于存放当系统非正常关机后重新启动系统时,不知道该向哪个文件恢复的碎片文件。

(9) /mnt

CD-ROM、软盘这类可移动介质的挂载点目录一般放在/mnt 目录下,通常有 cdrom 和 floppy 两个子目录,分别是光盘和软盘的挂载安装点。通过挂载光盘或软盘后,对应进入/mnt/cdrom 或/mnt/floppy 子目录,就可访问光盘或软盘中的内容。注意挂载点目录中不要有任何文件,否则将无法正确挂载。

例如:若要在 Linux 系统中,查看光盘中的内容,则应先将光盘放入光驱,然后利用以下命令将光盘挂载到/cdrom 目录:

```
# mount /mnt/cdrom
```

挂载成功后,进入/mnt/cdrom 目录,使用 ls 命令即可看到光盘中的内容。此时的 cdrom 中的内容,也即是光盘中的内容。对于软盘与此类似,只是挂载点换成/mnt/floppy。若要卸载光盘,则应先退出/mnt/cdrom 目录,然后再执行以下命令:

```
# umount /mnt/cdrom
```

另外,也可使用光盘的设备文件(/dev/cdrom)来挂载或卸载光盘,操作方法如下所示:

```
# mount /dev/cdrom      # 挂载光盘到/mnt/cdrom 目录
# cd /mnt/cdrom          # 进入挂载点目录
# ll                     # 查看光盘内容
# cd                     # 返回宿主目录,以退出挂载点目录
```

```
# umount /dev/cdrom    # 卸载光盘
```

#### (10) /proc

/proc 目录中的内容是系统自动产生的,其内容是当前系统运行的进程的一个虚拟镜像以及记录当前内存内容的 kernel 文件。可以在该目录中,看到一些由当前运行的进程号组成的子目录。

利用 cat 命令显示输出该目录下的一些特殊文件的内容,可查看到系统的一些特殊信息,例如:

```
cat /proc/cpuinfo    详细显示当前系统 CPU 的硬件信息。
cat /proc/interrupts 显示当前系统各设备所使用的中断信息。
cat /proc/meminfo    显示内存信息。
cat /proc/version    显示 Linux 的版本号。
```

#### (11) /tmp 与 /var

/tmp 目录用于存放临时文件,如程序执行期间产生的临时文件。/var 目录则用于存放经常变化的文件。对于存取频繁或内容经常变化的文件,可放在该目录中。

## 2.3 文件类型与文件属性

### 1. 文件的类型

Linux 支持长文件名,不论是文件名还是目录名,最长可以达到 256 个字节。Linux 的文件名中不能含有空格和一些对 shell 来说有特殊含义的字符,如:

```
! @ # $ % ^ & * ( ) [ ] { } ' " \ / | ; <
<< >> >
```

Linux 的文件和命令均要区分大小写。

Linux 的文件类型大致可分为普通文件、可执行文件、链接文件和设备文件。在 Linux 中,若文件名以“.”开头,则该文件就成为隐藏文件,需要使用 ls -a 命令才能看到。

在 Linux 中,文件是否是可执行文件,不是由扩展名来决定,而是由文件的属性来决定,这与 DOS 和 Windows 系统采用扩展名来标识可执行文件的做法是不相同的。

链接文件类似于 Windows 系统的快捷键文件。有时需要在多个不同的目录中,都需要存放某一个文件,为节省磁盘空间,可在某一个目录中存放该文件,然后在其他也需要该文件的目录,创建一个指向该真实文件的一个符号链接文件即可。访问该符号链接文件,实质也就是访问它所链接到的原始文件。

在文本控制台下使用 ls 或 ll 命令显示时,普通文件显示为白色,在图形界面中的仿真终端中,普通文件显示为黑色(背景为白色),目录显示为蓝色,可执行文件显示为绿色,

链接文件显示为青色。通过颜色,也可很快区分文件的类型。

## 2. 查看文件的类型

使用 `ls -l` 或 `ll` 命令,可列出文件和目录的详细信息。其显示格式及各列的含义如下所示。为便于讲解,以下所列的文件来源于不同目录,此处将其汇合在了一起。

lrwxrwxrwx	1	root	root	11	Jul	2	10:18	init.d->rc.d/init.d
drwxr-xr-x	3	root	root	4096	Jul	2	10:21	pcmcia
drwxr-xr-x	2	root	root	4096	Jul	2	10:42	vsftpd
-rw-r--r--	1	root	root	26940	Feb	25	2003	php.ini
-rwxr-xr-x	1	root	root	456108	Feb	12	2003	vi
lrwxrwxrwx	1	root	root	2	Jul	2	10:20	view->vi

↓	↓	↓	↓	↓	↓	↓	↓	↓
文件属性	文件数	拥有者	所属的组	文件大小	建档月份	日	年或时间	文件名

文件和目录的详细信息分为 7 列显示,其中第 6 列用于显示文档创建的日期或时间,下面分别作一个简单介绍:

(1) 第 1 列显示文件属性。文件属性占用 10 个字节,由 3 组权限属性和一个文件类型标识组成,其构成如图 2.1 所示。

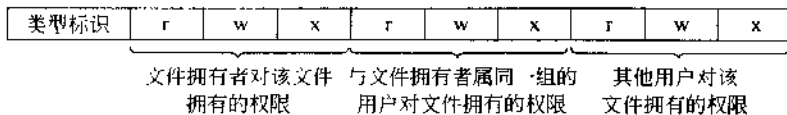


图 2.1 Linux 文件属性的构成

在 Linux 中,用户对文件的操作权限分为可读、可写、可执行三种,分别用 `r`、`w`、`x` 表示。若用户无某个权限,则在相应权限位置用“-”代表,表示无此权限。

若某文件具有 `x` 属性,则该文件就可执行,属于可执行文件。具有 `x` 属性的文件一般是二进制程序文件或可执行的脚本文件。二进制可执行程序是真正包含可执行代码的程序文件,可执行脚本文件本身仍是文本文件,但文件中包含有相应的脚本命令,它相当于 DOS 系统下的 `.bat` 批处理文件。

对于目录,若拥有可执行权限,则表示允许打开该目录中的文件,并且可用 `cd` 命令进入该目录。

类型标识用于说明该文件的类型是普通文件、链接文件还是目录。对于普通文件,第一个类型标识处显示为“-”,若是链接文件,则该位置的标识为 `l`(注:是 `L` 的小写,不是数字 1);若是目录,则该位置的标识为 `d`。

比如上面的 `vi` 文件,其文件属性为 `-rwxr-xr-x`,其第 1 个标识位为“-”,说明是一个文件,第 1 组权限为 `rwx`,说明该文件的拥有者对该文件具有可读、可写和执行权限;第 2 组权限为 `r-x`,则说明与文件拥有者属同一组的用户,对该文件具有读和执行权限,但不能对

该文件进行写操作;第3组权限为 r-x,说明其他用户对该文件具有读和执行权限,无写权限。其他用户是指文件拥有者和拥有者所属的组以外的用户。

另外,有一些程序命令文件的属性的执行部分不是 x,而是 s,这表示执行这个程序的使用者,临时可获得与该文件的拥有者一样的权力来运行该程序。这种情况,一般出现在系统管理类的命令程序中,如/bin 目录下的 ping、su、mount 和 umount,该类文件在显示时,其背景是红色显示的。

(2) 第2列表示文件个数。对于文件,其值为 1,若为目录,则表示该目录下的文件数。

(3) 第3列表示该文件或目录的拥有者。

(4) 第4列表示该文件所属的组。

(5) 第5列表示文件的大小。默认用 B 为单位,空目录一般为 1024B。

(6) 第6列表示文件创建的日期或时间。对于目录和链接文件,显示的是“月 日 时间”,对于普通文件,显示的是“月 日 年”。

(7) 第7列表示文件名。根据文件类型的不同,将显示成不同的颜色。

### 3. 修改文件的属性

对文件属性的修改包括修改文件的拥有者和修改用户对文件的权限两个方面。

#### (1) 修改文件或目录的拥有者

文件或目录的创建者,一般是该文件或目录的拥有者(所有者或称属主),拥有者对文件具有特别使用权。根据需要,文件或目录的所属关系是可以更改的,所有者或 root 用户可以将一个文件或目录的所有权转让给其他用户,使其他用户成为该文件或目录的拥有者或所有者。

在 Linux 中,使用 chown 命令可改变文件或目录的所有者(属主)和所属的用户组,利用参数-R,可递归设置指定目录下的全部文件(包括子目录和于目录中的文件)的所属关系;chgrp 命令只能更改指定文件或目录所属的用户组。其命令用法为:

chown [-R] 新所有者.新用户组 要改变的文件名或目录

chgrp 新用户组 要改变所属用户组的目录或文件

便于测试该命令,下而用 useradd 命令创建两个普通用户账户,并用 passwd 命令为新创建的用户设置登录密码,否则该用户将无法登录。

```
# groupadd student
```

```
# 创建一个名为 student 的用户组
```

```
# useradd -g student liyang
```

```
# 创建名为 liyang 的用户,并将其加入 student 用户组
```

```
# passwd liyang
```

```
# 设置 liyang 用户的登录密码
```

```
Changing password for user liyang.
```

```
New password:
```

```
Rctype new password:
```

```
passwd:all authentication tokens updated successfully.
# useradd -g student fengyuan      # 创建名为 fengyuan 的用户,并加入 student 用户组
# passwd liyang                    # 设置 fengyuan 用户的登录密码
Changing password for user fengyuan.
New password:
Retype new password:
passwd:all authentication tokens updated successfully.
```

用户创建好后,系统就会自动在/home 目录下,为用户创建一个与账户同名的主目录(home directory)。用户登录后,其当前目录就是该主目录。

键入 logout 注销 root 用户,用 liyang 用户重新登录,然后用以下命令新建一个名为 myfile.txt 的文件。

```
[liyang@rh9 liyang]$ touch myfile.txt
[liyang@rh9 liyang]$ ll myfile.txt
-rw-r--r-- 1 liyang student 11 Jul 0 05:39 myfile.txt
```

从以上输出可见,该文件的拥有者为 liyang,所属的组为 student。拥有者对该文件具有读和写的权限,其他用户仅有读的权限,由于文件不具有可执行性,因此不具有 x 属性。

若要将该文件的拥有者修改为 fengyuan,则操作命令为:

```
[root@rh9 root]# chown fengyuan /home/liyang/myfile.txt
[root@rh9 root]$ ll /home/liyang/myfile.txt
-rw-r--r-- 1 fengyuan student 11 Jul 0 05:42 myfile.txt
```

从上可见,尽管该文件仍位于 liyang 用户的主目录中,但文件的所有者已变为了 fengyuan 用户,此时的 fengyuan 用户对该文件有读和写的权限,而原来的 liyang 用户作为 student 组的成员,只有读的权限。

若要将 myfile.txt 文件所属的用户组修改为 nobody 组,则实现命令为:

```
[root@rh9 root]# chgrp nobody /home/liyang/myfile.txt
[root@rh9 root]# ll /home/liyang/myfile.txt
-rw-r--r-- 1 fengyuan nobody 11 Jul 0 05:45 myfile.txt
```

若要将 myfile.txt 文件的所有者和所属的用户组更改为 root 用户和 root 用户组,则实现命令为:

```
[root@rh9 root]# chown root,root /home/liyang/myfile.txt
[root@rh9 root]# ll /home/liyang/myfile.txt
-rw-r--r-- 1 root root 11 Jul 0 05:47 myfile.txt
```



chown 命令可同时更改所有者和所属的用户组,所有者和所属用户组之间可用小数点或冒号进行分隔表达。

## (2) 改变文件的权限

文件权限是与用户账户和用户组紧密联系在一起的,在 Linux 中,可使用 chmod 命令来重新设置或修改文件或目录的权限,但只有文件或目录的拥有者或 root 用户才有此更改权。

### ① 权限的表示方法

权限除了可用 r、w、x 来表示外,也可用一个 3 位的数字来表示,比如 644,其百位上的数代表拥有者的权限,十位上的数代表拥有者所属的组中的用户的权限,个位上的数,代表其他用户对该文件的权限。这种采用数字来表示权限的方法,称为绝对权限表示法。

由于用户的权限是用 rwx 来表示的,没有的权限对应位置上用“-”表示,因此可用一个 3 位的二进制数来表示用户的权限,有权限的位置用 1 表示,没有权限的位置用 0 表示,这样就会形成一个 3 位的二进制数编码,然后将该二进制数转换成对应的十进制数,这样就得到一个 0~7 的数,从而就可实现用十进制数来表示用户对文件的权限。

比如某一个文件的权限为:                      rw-      r--      r--  
若用二进制数表示,则为:                      110      100      100  
将每部分转换成对应的十进制,则为:      6              4              4  
因此,该文件的权限(rw-r--r-)用数字来表示,则为 644。  
rwx 表示的权限与用数字表示的权限对照如表 2.1 所示。

表 2.1 权限的表示形式

rwx 表示的权限	二进制数表示	权限的十进制数表示	权限含义
---	000	0	无任何权限
--x	001	1	可执行
-w-	010	2	可写
-wx	011	3	可写和可执行
r--	100	4	可读
r-x	101	5	可读和可执行
rw-	110	6	可读和可写
rwx	111	7	可读、可写和可执行

文件的权限除了 r、w 和 x 外,还有一种称为 s 的权限,具有 s 权限的文件一般是可执行文件,具有该权限的用户在执行该文件时,根据需要可获得与 root 用户相同的权限。

s 权限也可用数字来表达。由于文件的权限包括文件的所有者、所属的用户组和其他用户三个方面,因此可用一个三位的二进制数来表示这三类用户对 s 权限的拥有情况,有 s 权限的用 1 表示,没有的用 0 表示,如表 2.2 所示。

表 2.2 s 权限的表示形式

所有者有 s 权限	所属组有 s 权限	其他用户有 s 权限	s 权限对应的十进制数值
0	0	0	0
1	0	0	4
1	1	0	6
1	1	1	7

要表示各用户对 s 权限的拥有情况,可在原有的三位十进制数的前面,再增加一个数字来代表 s 权限,比如 4755 中的 4,就用来表达 s 权限,表示文件的所有者拥有 s 权限,所属的用户组和其他用户没有 s 权限。755 中的 7 代表文件的所有者具有读、写和执行权限,由于此时它同时拥有了 s 权限,因此在最后显示时,其权限将显示为 rws;755 中间的 5 代表所属的用户组的权限是具有读和执行权限,最后的 5 代表其他用户的权限,也是读和执行权限。

## ② 改变文件或目录的权限

由于权限有两种表示法,因此,改变权限的 chmod 命令的具体用法也有两种。

利用绝对权限表达法(即用权限对应的数值)来设置或改变文件或目录的权限,其用法为:

chmod [-R] 绝对权限值 要改变的文件或目录名

参数-R 代表递归设置指定目录下的所有文件的权限。

比如: myfile.txt 文件目前的权限为 rw-r--r--,若要更改为 rw-rw-r--,其实现的命令为:

```
[root@rh9 root]# chmod 664 /home/liyang/myfile.txt
[root@rh9 root]# ll /home/liyang/myfile.txt
-rw-rw-r-- 1 liyang student 11 Jul 4 05:39 myfile.txt
```

若要将 myfile.txt 设置为所有者具有读写和 s 权限,所属用户组和其他用户具有读和执行权限,则实现命令为:

```
chmod 4755 /home/liyang/myfile.txt
```

设置后,查看该文件的权限,其权限显示将会是: -rwsr-xr-x。若设置为 6755 权限,则显示的权限将会是: -rwsr-sr-x。若设置为 7755 权限,则显示的权限将会是: -rwsr-sr-s。

若通过 r、w、x、s 表示方式来更改权限,则只需在 chmod 命令中表达出权限需要改变的部分即可,该方法可视为是相对修改法。此时用 u 表示修改文件或目录的拥有者的权限,用 g 表示修改文件拥有者所属的用户组的权限,用 o 表示修改其他用户的权限。若要增加某项权限,则用“+”表示,若要去掉某项权限,则用“-”表示,若只赋予该项权限,则用“=”表示。

比如,假设 /home/liyang/myfile.txt 文件的权限为 rw-rw-r--,若要修改为 rw-r---,则更改命令为:

```
chmod g-w /home/liyang/myfile.txt
chmod o-r /home/liyang/myfile.txt
ll /home/liyang/myfile.txt
-rw-r--- 1 liyang student 11 Jul 4 05:39 myfile.txt
```

若要给其他用户增加读的权限,则实现命令为:

```
chmod o+r /home/liyang/myfile.txt
```

若要同时去掉用户组和其他用户对该文件的读权限,则实现命令为:

```
chmod go-r /home/liyang/myfile.txt
```

若文件拥有者、用户组和其他用户都只赋予读的权限,则实现命令为:

```
chmod ugo=r /home/liyang/myfile.txt
```

若要为文件的拥有者和所属的组增加 s 权限,则设置命令为:

```
chmod ug+s /home/liyang/myfile.txt
```

## 2.4 Linux 常用命令

### 2.4.1 Linux 命令基础

#### 1. 命令特点

Linux 区分大小写。在命令行(shell)中,可以使用 Tab 键来自动补全命令。即可以输入命令的前几个字母,然后按 Tab 键,系统将自动补全该命令,若不止一个,则显示出所有和输入字母相匹配的命令。

按 Tab 键时,如果系统只找到一个和输入相匹配的目录或文件,则自动补全;若没有匹配的内容或多个相匹配的名字,系统将发出警鸣声,再按一下 Tab 键将列出所有相匹配的内容(如果有的话),以供用户选择。比如在命令提示行上输入 mou,然后按 Tab

键,系统将自动补全该命令为 `mount`;若输入 `mo`,然后按 `Tab` 键,此时将警鸣一声,再次按 `Tab` 键,系统将显示出所有以 `mo` 开头的命令。

另外,利用向上或向下的光标键,可以翻查曾执行过的历史命令,并可再次执行。

要在一个命令行上输入和执行多条命令,可使用分号来分隔命令。比如 `cd /etc; ls -l`。

断开一个长命令行,可使用反斜杠“`\`”,以将一个较长的命令分成多行表达,增强命令的可读性。换行后,shell 自动显示提示符“`>`”,表示正在输入一个长命令,此时可继续在新行上输入命令的后续部分。

## 2. 后台运行程序

一个文本控制台或仿真终端在同一时刻只能运行一个程序或命令,在未执行结束前,一般不能进行其他操作,此时可采取将程序在后台运行,以释放控制台或终端,使其仍能进行其他操作。要使程序以后台方式运行,只需在要执行的命令后跟上一个 `&` 符号即可,比如 `# xcalc &`。

### 2.4.2 基本操作命令

Linux 最基本也是最常用的命令主要有 `ls`、`cd`、`clear`、`su`、`login`、`logout`、`exit`、`shutdown`、`reboot`、`mount`、`umount` 以及发送消息的 `write` 和 `mesg` 等命令,大部分命令在前面都已作介绍,此处对部分命令再作一个补充说明。

#### 1. su 命令

`su` 命令用于使当前普通用户临时切换到管理员(`root`)身份,使其成为具有与管理员同等权限的超级用户(`superuser`)。使用完毕后,可通过执行 `exit` 命令,回到原来的普通用户身份。执行 `su` 命令后,必须正确输入 `root` 账户密码后,才能切换成功。执行演示如下:

```
[liyang@rh9 liyang]$ su           # 执行 su 命令,临时切换到管理员身份
Password:                         # 输入 root 账户密码
[root@rh9 liyang]# exit           # 命令行提示符变为 #,切换成功。执行 exit 退出
[liyang@rh9 liyang]$             # 重新回到普通用户身份
```

`su` 命令适合于管理员使用,由于 `root` 用户权力很大,为防止误操作损坏系统,管理员通常以一个普通用户身份登录,进行日常维护,当需要操作一些只有管理员才有权操作的命令时,就可使用该命令,临时切换到管理员身份,以获得管理员级的权限。

#### 2. shutdown 命令

`shutdown` 命令用于重启或关闭 Linux 系统(关机),只能由 `root` 用户执行。常用的功能参数主要是 `-h` 和 `-r`,其中 `-h` 代表关机动作(`halt`),`-r` 代表重启动作(`reboot`),`now` 代表

立刻执行当前动作,比如:

```
# shutdown -h now          # 立刻关机
# shutdown -r now          # 立刻重新启动,相当于 reboot
# shutdown -h 17:30         # 系统将在今天的 17:30 关机,并广播内置消息给各用户
# shutdown -h t secs 2     # 系统在 2 分钟后关机,并广播内置消息给各用户
```

### 3. mount 与 umount 命令

mount 用于挂载系统可以识别的文件系统,通常用于挂载光盘、软盘、硬盘等存储设备。其用法格式为:

mount 设备文件名 挂载点目录名

其功能是将指定的设备挂载到指定的目录。用作挂载点的目录应是空目录,不能含有文件。比如挂载光盘,其命令为 mount /dev/cdrom /mnt/cdrom 或 mount -t iso9660 /dev/cdrom /mnt/cdrom。其中的 -t iso9660 参数用于指定挂载的文件系统的类型为 iso9660。

umount 用于卸载系统中不再需要使用的文件系统,其用法为:

umount 设备文件名或挂载点目录名

比如卸载光盘,则命令为 umount /dev/cdrom 或 umount /mnt/cdrom。

直接执行 mount 命令,可显示当前系统中已挂载的文件系统的相关信息。

### 4. write 与 mesg 命令

write 命令用于向登录系统的某用户发送信息。其命令用法为:

write 接收消息的用户账号 [用户所使用的终端名称]

接收消息的用户所使用的终端名称为可选项,若不知道,也可不指定,命令中只要指定接收消息的用户账户即可。执行该命令后,即进入消息发送状态,输入要发送的消息按回车后,消息即会传送给指定的用户,在其终端屏幕上将会显示出该消息。对方也可用相同的方法回复消息。在发送状态,可实现连续发送,若要退出发送状态,则按 Ctrl+C 组合键。

例如,假设 root 用户在虚拟终端 1, vodup 用户在虚拟终端 2, root 用户若要给 vodup 发送消息,则实现的操作命令为:

```
[root@rh9 root]# write vodup tty2      或 # write vodup
```

执行该命令后,直接输入要发送的消息,按回车即可,此时 vodup 用户就可收到消息了。

mesg 命令用于设定是否允许其他用户用 write 命令给自己发送信息。如果允许别

人给自己发送信息,则执行 `mesg y` 命令,否则执行 `mesg n` 命令。直接执行 `mesg` 命令,可查询当前的允许状态,若显示的是 `y`,则表示允许。用户执行 `mesg n` 命令后,就不会收到其他普通用户发送给自己的消息,同时也不能向外发送消息,但仍能接收到来自 `root` 用户的消息。

### 2.4.3 目录操作命令

#### 1. mkdir 与 rmdir

`mkdir` 用于建立新目录,对应于 DOS 的 `md` 命令;`rmdir` 用于删除目录,对应于 DOS 的 `rd` 命令,用 `rmdir` 删除目录时,目录必须是空目录,且必须在上级目录进行删除操作。用法为:

```
# mkdir 新目录名
# rmdir 要删除的目录名
```

另外,`mkdir` 命令与 `-p` 参数结合使用,可快速创建出目录结构中指定的每个目录,对于已存在的目录不会被覆盖。比如要在 `/usr` 目录下面创建一个子目录 `mydoc`,然后在 `mydoc` 下面再创建一个 `liyang` 目录,则操作命令为:

```
# mkdir -p /usr/mydoc/liyang
```

#### 2. pwd

`pwd` 是 `print working directory` 的缩写,该命令用于显示当前工作目录。用法示例:

```
[root@rh9 root]# pwd
/root
```

#### 3. cd

`cd` 命令用于改变当前目录,基本用法为“`cd 目录名`”,表示进入指定的目录,使该目录成为当前目录。在 Linux 中,直接执行 `cd`,不跟任何参数或跟“`~`”参数,则表示进入当前用户对应的宿主目录,若“`~`”后面跟一用户名,则进入到该用户的宿主目录。特殊用法如下:

<code># cd ..</code>	# 返回上一级目录
<code># cd ../../</code>	# 返回上二级目录
<code># cd /</code>	# 进入根目录
<code># cd -</code>	# 在最近访问过的两个目录之间快速切换
<code>[root@rh9 ~]# cd ~</code>	# 进入到 root 用户的主目录
<code>[root@rh9 ~]# cd ~snbj</code>	# 进入到 snbj 用户的主目录

其中的“`..`”代表上一级目录,“`.`”代表当前目录,这与 DOS 系统相同。

## 2.4.4 文件操作命令

### 1. ls 命令

ls 命令用于列出一个或多个目录下的内容(目录或文件),该命令支持很多参数,以实现更详细的控制。默认情况下,ls 命令按列显示目录下的内容,垂直排序。常用参数及功能如表 2.3 所示。

表 2.3 ls 命令参数选项

选项	说 明
-d	列出目录名,不列出目录内容
-l	按长格式显示(包括文件大小、日期、权限等详细信息)
-li	按长格式显示,同时还要显示文件的 i 节点(inode)值
-m	文件名之间用逗号隔开
-x	按水平方向对文件名进行排序
-a	列出所有文件(包括“.”和“..”文件以及其他以“.”开始的隐藏文件)
-A	列出所有文件,但不列出“.”和“..”文件
-C	按垂直方向对文件名进行排序
-F	区分目录、链接和可执行文件。文件后将附加显示表示文件类型的符号,*表示可执行,/表示目录,@表示链接文件
-R	循环列出目录内容,即列出所有子目录下的文件
-S	按大小对文件进行排序
--color	启用彩色显示方案,利用颜色区分不同类型的文件。目前 ls 命令已内置该功能

ll 命令的功能等价于 ls -l,ll 实际上是 Linux 系统中定义的一个针对 ls -l 命令的一个别名,利用别名,可简化命令的输入。查看系统中所定义的别名,可执行 alias 命令来实现。

若要定义别名,其命令用法为:

```
alias 别名='要代表的命令'
```

比如要定义别名 lsa 代表 ls -a 命令,则定义命令为 alias lsa='ls -a'。

若要删除所定义的别名,可通过 unalias 命令来实现,其用法为:

```
unalias 要删除的别名
```

比如要删除 lsa 别名,则操作命令为 unalias lsa。

## 2. cp 命令

cp 是 copy 的缩写,可用于目录或文件的复制。其用法为:

cp [参数选项] 源文件 目标文件

默认情况下,cp 命令会直接覆盖已存在的目标文件,若要求显示覆盖提示,可使用-i 参数。

利用 cp 命令复制目录时,参数选项可使用-r,以实现将源目录下的文件和子目录一并复制到目标目录中,其命令用法为:

cp -r 源目录 目标目录

例如,要将/mnt/cdrom/linux\_soft 目录及其子目录中的文件全部复制到/root/linux\_soft 目录中,则实现命令为:

```
[root@rh9 root]# cp -r /mnt/cdrom/linux_soft linux_soft
```

## 3. rm 命令

rm(remove)命令用于删除文件或目录。在命令行中可包含一个或多个文件名(各文件间用空格分隔)或通配符,以实现删除多个文件。其用法为:

rm [参数选项] 文件名或目录名

在 Linux 系统中,文件一旦被删除,就无法再挽回了,因此删除操作一定要小心,为此可在执行该命令时,选用-i 参数,以使系统在删除之前,显示删除确认询问。目前新版的 Linux 都定义了 rm -i 命令的别名为 rm,因此执行时,-i 参数就可省略了。若不需要提示,则使用-f(force)选项,此时将直接删除文件或目录,而不显示任何警告消息,使用时应备加小心。

例如,要直接删除当前目录下的 myfile.txt 文件,则执行如下命令:

```
# rm -f myfile.txt
```

rm 命令本身主要用于删除文件,若要用来删除目录,则必须带-r(recursive)参数,否则该命令的执行将失败,带上-r 参数后,该命令将删除指定目录及其目录下的所有文件和子目录。

例如,要删除当前目录下面的 test 目录及其目录下的全部内容,则执行如下命令:

```
# rm -r test
```

执行过程中,会逐一询问是否要删除某文件,若要系统不逐一询问,而直接删除,则可再加上-f 参数,此时的命令应为:



```
# rm -rf test
```

由于命令将直接删除整棵子目录树,以 root 身份执行带-rf 参数的 rm 命令时,一定要特别小心。rmdir 虽也可删除目录,但要求被删除的目录必须是空目录。

#### 4. mv 命令

mv 是 move 的缩写,该命令用于移动或重命名目录或文件。Linux 系统没有重命名命令,因此,可利用该命令来间接实现。其用法为:

```
mv [-参数选项] 源目录或文件名 目标目录或文件名
```

使用该命令可将文件移动到另一个目录之下,若目标文件已存在,则会自动覆盖,除非使用-i 选项。mv 命令若使用-b(backup)参数,则在覆盖已存在的文件前,系统会自动创建原已存在文件的一个备份,备份文件名为原名称后附加一个“~”符号。

mv 命令也可移动整个目录。如果目标目录不存在,则重命名源目录;若目标目录已存在,则将源目录连同该目录下面的子目录,移动到目标目录之中。

比如执行命令 mv liyang liyan,其结果就有两种情况:若目标目录 liyan 不存在,则该命令的功能就是重命名;若 liyan 目录存在,则 liyang 目录将被移到 liyan 目录之下。

#### 5. touch 命令

touch 命令用于更新指定的文件或目录被访问和修改时间为当前系统的日期和时间。查看当前系统日期和时间,使用 date 命令。

若指定的文件不存在,则该命令将以指定的文件名自动创建一个空文件。这也是快速创建文件的一个途径,比如要创建两个没有内容的空文件 file1 和 file2,则操作命令为:

```
# touch file1 file2
```

各文件间用空格进行分隔。

#### 6. ln 命令

ln 命令用于创建链接文件。链接是将已存在的文件或目录链接到位置或名字更便捷的文件或目录。

当需要在不同的目录中,用到相同的某个文件时,不需要在每一个目录下都放一个该文件,这样会重复占用磁盘空间,也不便于同步管理,为此,可在某个固定的目录中放置该文件,然后在其他需要该文件的目录中,利用 ln 命令创建一个指向该文件的链接(link)即可,所生成的文件即为链接文件或称符号链接文件。

在 Linux 中,链接的方式有硬链接(hard link)和软链接(soft link)两种。

##### (1) 软链接

将会生成一个很小的链接文件,该文件的内容是要链接到的文件的路径。原文件删

除后,软链接文件也就失去了作用,删除软链接文件,对原文件无任何影响。类似于 Windows 操作系统的快捷方式。软链接可以跨越各种文件系统和挂载的设备。

创建软链接,使用带-s(symbolic link)选项的 ln 命令,其用法为:

ln -s 原文件或目录名 要链接的文件或目录名

假设在/home/liyang 目录下有一个 myfile.txt 文件,现要创建该文件的一个软链接文件 newfile.txt,则操作命令为:

```
# cd /home/liyang
# ln -s myfile.txt newfile.txt
# ll
-rw-r--r- 1 liyang student 11 Jul 5 02:00 myfile.txt
lrwxrwxrwx 1 root root 10 Jul 5 02:58 newfile.txt -> myfile.txt
```

此时若执行 more newfile.txt 命令,看到的实际上是 myfile.txt 文件中的内容。

## (2) 硬链接

文件都是被写到硬盘上的某个物理位置,该物理位置称作 i 节点(inode),它是获得文件内容的一个入口地址,而每个 i 节点都有一个编号。利用 ls -li 命令可以查看每个文件对应的 i 节点值。创建硬链接,实质就是创建了另外一个指向同一 i 节点的文件。硬链接使用不带-s 参数的 ln 命令来创建,其用法为:

ln 原文件 要链接的文件名

硬链接无法跨越不同的文件系统、分区和挂载的设备,只能在原文件所在的同一磁盘的同一分区上创建硬链接,而且硬链接只针对文件,不能用于目录。

比如要再创建一个 myfile.txt 文件的硬链接文件 hardlink.txt,则操作命令为:

```
# ln myfile.txt hardlink.txt
# ll -li
508545 -rw-r--r- 2 liyang student 11 Jul 5 02:00 hardlink.txt
508545 -rw-r--r- 2 liyang student 11 Jul 5 02:00 myfile.txt
508569 lrwxrwxrwx 1 root root 10 Jul 5 02:58 newfile.txt -> myfile.txt
```

对照输出结果,可以看到,硬链接文件与原始文件除了文件名不同外,其余属性都相同。第一列是该文件在磁盘中的存储位置。

## 7. 查看文本文件的内容

### (1) 利用 cat 命令查看

cat 是 concatenate 的缩写,该命令用于将文件的内容打印输出到显示器或终端窗口上,常用于查看内容不多的文本文件的内容,长文件会因滚动太快而无法阅读。相当于

DOS 系统的 Type 命令。

在 cat 命令后面可指定多个文件,或使用通配符实现依次显示多个文件的内容。比如:

```
# cat file1.txt file2.txt
```

使用 -n 参数选项,在显示时将为各行加上行编号。

(2) 使用 more 或 less 命令查看

对于内容较多的文件,不适合于用 cat 命令来查看,此时可用 more 或 less 命令来查看。more 命令可实现分屏显示文件内容,按任意一键后,系统会自动显示下一屏的内容,到达文件末尾后,命令执行即结束。cat 是连续滚动显示的。

less 比 more 功能更强大,除了有 more 的功能外,还支持用光标键向上或向下滚动浏览文件的功能,对于宽文档还支持水平滚动,当到达文件末尾时,less 命令不会自动退出,需要输入 q 来结束浏览。

less 和 more 命令后可同时指定多个文件(文件间用空格分隔),或使用通配符以实现同时浏览或查看多个文件的内容。

(3) head 与 tail 命令

head 命令用来查看一个文件前面部分的信息,默认显示前面 10 行的内容,也可指定要查看的行数,其用法为:

head -n 要查看的行数 文件名

比如要查看 /boot/grub/grub.conf 文件中前 10 行的内容,则操作命令为:

```
# head /boot/grub/grub.conf
```

若要查看前 20 行的内容,则操作命令为:

```
# head -n 20 /boot/grub/grub.conf
```

注: grub.conf 是 GRUB 引导器的配置文件,不要随便修改其中的内容。其中的 timeout=10 用于设置启动菜单等待用户选择的时间(秒),title 后面的内容是启动菜单项显示的标题,这两方面的内容,可根据需要进行修改。

tail 命令的功能与 head 相反,用于查看文件的最后若干行的内容,默认为最后 10 行,用法与 head 相同。另外,tail 命令若带上 -f 参数,则可实现不停地读取和显示文件的内容,以监视文件内容的变化。

## 8. grep 命令

grep 命令用于在指定的文件中,查找并显示含有指定字符串的行。其用法为:

grep 要找的字符串 文本文件名

比如要在 `/etc/fstab` 文件中,查找显示含有 `cdrom` 的行的内容,则操作命令为:

```
# grep cdrom /etc/fstab
```

## 9. diff 命令

`diff` 命令用于比较两个文件或两个目录的不同之处,其用法为:

`diff [-r] 文件或目录名1 文件或目录名2`

若是对目录进行比较,则应带 `-r` 参数,比如:

```
# diff file1 file2          # 比较文件 file1 与 file2 内,各行的不同之处
# diff -r dir1 dir2         # 比较目录 dir1 与 dir2 内,各文件的不同之处
```

## 10. >、>>与<、<<重定向操作符

(1) >、>>输出重定向符

输出重定向符能实现将一个命令的输出重定向到一个文件中,而不是显示屏幕。比如,要将 `last` 命令的输出结果,传输到 `mylog.txt` 文件中,则实现命令为:

```
# last >mylog.txt
# less mylog.txt
```

该重定向符通常也与 `cat` 命令结合使用,从而实现文件的创建与合并等操作。比如要将 `file1.txt` 和 `file2.txt` 的内容合并,并将合并后的内容传输给 `file3.txt` 文件保存,此时就可使用标准输出重定向符“>”来实现,其操作命令为:

```
# cat file1.txt file2.txt >file3.txt
```

利用 `cat >file.txt` 命令格式,还可实现将键盘输入的内容添加到指定的 `file.txt` 文件中,输入完毕后按 `Ctrl+D` 组合键存盘退出,此时就会自动产生 `file.txt` 文件,其内容就是刚才输入的内容,该用法等价于 DOS 系统的 `copy con file.txt` 命令。若要放弃存盘,则按 `Ctrl+C` 组合键终止退出。

若 `file.txt` 文件已存在,执行 `cat >file.txt` 命令后,将覆盖原文件的内容,若要不覆盖,以追加的方式添加,则换成“>>”(追加)重定向符即可,此时用法为 `cat >>file.txt`。

(2) <、<<输入重定向符

“<”为标准输入重定向符,用于改变一个命令的输入源。比如 `cat <file1.txt` 命令,它读取 `file1.txt` 文件中的内容,并显示输出在屏幕上。

“<<”为此处操作符(here operator),该操作符在从键盘读取内容时,读到指定的字符串时,便停止读取动作,然后将所读的内容输出。其与 `cat` 命令相结合使用时的用法为:

cat <<结束读取的标识字符串

例如,执行命令: cat <<end >file.txt,然后从键盘输入一些字符串,当输入的字符串含有 end 时,其读取动作就会结束,并开始输出刚才所读的字符串,此处由于使用“>”定向符将输出重新指向了 file.txt 文件,因此,刚才所读的内容将保存在 file.txt 文件中,使用 more file.txt 命令即可看到其内容。

### 11. 管道操作

管道操作可以实现将一个命令的输出当作另一个命令的输入,后者的输出又可作为第三条命令的输入,以此类推,这样,管道命令行中最后一条命令的输出才会显示输出在屏幕上。因此,利用管道操作,可实现将多条相关的命令连接起来。管道操作符为“|”。例如 ls -l /etc | grep ftp。

以上命令将 ls -l /etc 的输出作为后面一条命令 grep 的输入,grep 命令就在输入的内容中查找包含 ftp 关键字的行,并将这些包含有 ftp 关键字的行的内容输出。

当输出的内容比较多,要浏览查看时,可将输出的内容通过管道操作符传递给 less 命令来实现浏览。比如 ls -l /etc | less。

## 2.4.5 查看系统信息

### 1. 查看 Linux 内核版本

查看 Linux 内核版本可使用 uname -r 或 uname -a 命令。

### 2. df 命令

利用 df 命令,可以查看已安装的文件系统的空间大小和剩余空间的大小。磁盘空间大小的单位为数据块,1 数据块=1024 字节。

### 3. du 命令

利用 du 命令可显示出当前目录以及其下各子目录的大小。du -a 则可详细显示当前目录以及其下的各子目录和各文件的大小,du -s 显示当前目录和其下的各子目录的大小总和(summary)。利用“>”或“>>”重定向符,可将显示结果保存到某文件,然后再用 more 或 less 命令进行详细查看。

利用 du -s | sort -n 命令,可按目录占用空间的大小,由小到大排序显示。

### 4. free 命令

free 命令用于查看当前系统内存的使用情况,包括系统中剩余和已用的物理内存和交换内存,以及共享内存和被核心使用的缓冲区大小等。其用法为 free [-b | -k | -m]。

参数-b 表示以字节为单位显示,-k 以 KB 为单位显示,-m 表示以 MB 为单位显示。

```
[root@rh9 root]# free
```

	total	used	free	shared	buffers	cached
Mem:	125992	122264	3728	0	29240	64784
+/+ buffers/cache:		28320	97672			
Swap:	289160	460	288692			

## 5. uptime 命令

uptime 命令用于显示系统已经运行了多长时间,将依次显示:现在时间、系统已经运行了多长时间,目前有多少登录用户、系统在过去的 1 分钟、5 分钟和 15 分钟内的平均负载。

## 6. 查询 CPU 信息

要查询 CPU 硬件信息,可使用命令 `cat /proc/cpuinfo` 来实现,该命令可显示有关 CPU 的详细硬件信息。

## 7. 查看 CPU 和进程的状况

要详细了解 CPU 的使用状况和正在运行的进程的状况,可执行 `top` 命令来实现,其显示结果如图 2.2 所示,该命令显示的信息会自动周期性刷新,另外也可利用“d delay”参数来指定刷新的间隔时间,其中 delay 代表间隔的秒数。若要手工立即刷新,可按空格键。该命令相当于 Windows 2000 Server 的任务管理器。

```

12:05:34 up 3:59, 1 user, load average: 0.00, 0.00, 0.00
37 processes: 36 sleeping, 1 running, 0 zombie, 0 stopped
CPU states: 0.0% user 0.5% system 0.0% nice 0.0% iowait 99.4% idle
Mem: 125992k av, 122344k used, 3648k free, 0k shrd, 29332k buff
      81564k actv, 0k in_d, 2268k in_c
Swap: 289168k av, 468k used, 288692k free 64684k cached

```

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	CPU	COMMAND
8529	root	15	0	1052	1052	852	R	0.3	0.0	0:00	0	top
1733	root	15	0	108	108	68	S	0.1	0.0	0:00	0	gpm
1	root	15	0	144	136	96	S	0.0	0.1	0:05	0	init
2	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	keventd
3	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	kajmnd
4	root	34	19	0	0	0	SUM	0.0	0.0	0:00	0	ksoftirqd_CPU
9	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	bdflush
5	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	kswapd
6	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	kscand/DMA
7	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	kscand/Normal
8	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	kscand/HighMe
18	root	15	0	0	0	0	SW	0.0	0.0	0:00	0	kupdated

图 2.2 CPU 使用状况

`top` 命令还提供了一些用于交互操作的子命令,执行该命令后,键入 `h`,系统将显示该命令可用的交互操作子命令。利用子命令,可改变显示结果的排序方式、监视指定用户产生的进程以及删除特定的进程。键入子命令 `q`,可退出 `top` 命令。

### (1) 各行信息的含义

第 1 行显示的信息与 `uptime` 命令显示的结果相同。

第2行显示当前系统有37个进程,其中36个处于睡眠(sleeping)状态,1个处于运行状态(running),0个僵尸进程(zombie process),0个处于停止状态(stopped)。

一个子进程终止后,需要父进程对其进行善后工作(获取子进程的结束状态,释放它仍占用的资源)。在子进程结束后,父进程对其进行善后处理之前的这段时间,该子进程就称为僵尸进程。

第3行显示CPU的使用率,其中0.0%的时间用于处理用户操作;0.5%用于处理系统的工作,即系统占用的CPU时间率;0.0%的时间用于处理系统的nice命令的工作;0.0%的时间处理I/O等待;99.4%的时间处于闲置状态(idle),该值越大,说明目前CPU的负荷越低,越有时间处理系统的各种响应。

第4~6行显示物理内存和交换分区的使用情况,与free命令显示的内容差不多。其中的av(available)表示有效内存。

第7行显示的是各进程列表的各栏标题,其内容如下:

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	CPU	COMMAND
-----	------	-----	----	------	-----	-------	------	------	------	------	-----	---------

下面对各栏代表的含义作简要说明:

**PID** 代表程序的进程号(Process ID),系统中执行的每一个程序都会有一个唯一的标识号ID。

**USER** 指该进程属于哪位用户。

**PRI** 代表进程执行的优先级别。

**NI** NI是nice的缩写,代表进程的优先级别值,即进程对CPU的使用权值。默认的标准优先级值为0,取值范围为-20~19,数值越小获得CPU的优先权就越高。只有root用户有权调高优先权,普通用户只能调低优先权。可使用nice命令来调整一个进程的nice值。

**SIZE** 进程的程序代码大小加上堆栈(stack)空间的大小(KB)。

**RSS** 进程所使用的物理内存的大小(KB)。

**SHARE** 进程所使用的共享内存空间大小(KB)。

**STAT** 进行目前的状态。S表示sleeping,D表示uninterrupting sleep,R表示running,Z表示zombies,T表示stoped,"<"表示nice值为负,N表示nice值为正,W表示进程因异常而被置换出内存。

**%CPU** 画面更新时,进程所使用的CPU时间百分比。

**%MEM** 画面更新时,进程所使用的物理内存百分比。

**TIME** 进程启动后所使用的CPU的时间。

**CPU** CPU的ID号,一般为0。

COMMAND 产生该进程的程序名。

## (2) 排序结果

默认情况下,根据使用 CPU 时间的多少来排序,另外还可按以下命令键来改变排序方式:

按 P(注意是大写字母,应按 Shift+P)键,按 CPU 的使用率降序排序,即按 %CPU 列排序。

按 M 键,按内存用量降序排序,即按 %MEM 列降序排序。

按 T 键,按 TIME 列降序排序。

按 N 键,按 PID 列升序排序。

## (3) 监视特定用户

top 命令可以监视指定用户产生的进程。按 u 键,然后输入要监视的用户名即可。

## (4) 删除特定的进程

在监视过程中,若发现某进程占用的系统资源太多,影响到系统的正常运行,可以将该进程终止并删除,方法是:按 k 键,之后将显示提示信息“PID to kill:”,输入要删除的进程的 ID,然后回车,此时系统又将显示类似“Kill PID with signal[15]:”的提示信息,输入 signal 号码,默认为 15,直接按回车就可将其终止并删除。若遇到某些无法终止并删除的进程,则输入 9,来强制终止并删除该进程。

## 8. 查看登录日志信息

要查看登录日志,可使用 last 命令来实现。该命令显示的实际上是 /var/log/wtmp 文件中的内容。该命令采用滚屏显示方式,通常可将其内容重定向传输到一个文本文件中,然后再利用该文本文件来查看。

## 9. 查看登录用户的信息

对于系统管理员,若想了解当前登录用户的相关信息(比如当前用户正在运行什么程序或命令),可执行 w 命令来查看,w 命令将显示出所有登录用户的相关信息,若只想查看某个登录用户的信息,则在 w 命令后面指定该用户名,比如若想查看 liyang 用户正在做什么,则可执行命令:w liyang。

w 命令的显示输出如图 2.3 所示。

```

[root@rh9 root]# w
13:24:41 up 5:10, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
root      tty1     ~              11:27am  0.00s  0.59s  0.04s  w

```

图 2.3 w 命令输出结果



第1行依次显示的是当前系统的时间、主机已开机多长时间、目前登录用户数、系统在过去的1、5、10分钟的平均负载情况,数字越接近0.00,则表示负载越低。

第2行显示列表的各列的标题,其含义如下:

USER 登录的用户。

TTY 用户登录的虚拟终端。

FROM 若用户从本机登录,则该列显示为“-”;若是从远程登录,则显示对方远程主机的IP地址或主机名称。

LOGIN@ 用户登录的时间。

IDLE 用户没有进行任何操作的时间。

JCPU 用户登录后,执行的所有程序消耗的CPU时间。

PCPU 当前正在执行的程序所消耗的CPU时间。

WHAT 用户现在正在运行的命令。

另外,如果仅是查看当前有哪些用户登录,也可使用 `users` 命令来查看。

## 10. 显示月历或年历

若要显示当前月的月历,则可执行 `cal` 命令;若要显示某一年的年历,则执行“`cal 4 位年号`”命令,如 `cal 2004`。

显示当前日期和时间,可使用 `date` 命令。若要设置当前系统的日期或时间,可使用 `date -s` 命令,其用法为 `date -s 日期(mm/dd/yy)` 或时间 `(hh:mm:ss)`,最后再使用 `clock -w` 命令将修改后的日期或时间信息强制写入 CMOS 中。

## 2.4.6 使用 vi 编辑器

`vi`(visual interface)是Linux和UNIX中功能最为强大的全屏幕文本编辑器,本节介绍该编辑器的一些常用操作。

### 1. 启动 vi 编辑器

在提示符状态下,键入 `vi` 文件名或 `vi`,则可启动 `vi` 编辑器,并自动进入命令模式。`vi` 命令后若指定了文件名,则打开该文件或创建该文件(若指定的文件不存在)。若未指定文件名,则创建一个未命名的新文件。

### 2. vi 的工作模式

`vi` 编辑器具有命令模式(command mode)、插入模式(insert mode)和末行模式(last line mode)三种。

#### (1) 命令模式

不管用户当前处于何种模式,只要按 `Esc` 键,则立即进入命令模式。在命令模式下,

允许输入 vi 命令,以对文档进行管理,若输入的不是合法的 vi 命令,则会蜂鸣告警。

### (2) 插入模式

插入模式也称输入模式,在该模式下,用户输入的内容当作文档的内容,并显示在屏幕上。在命令模式下输入 i、a、o 命令都可进入插入模式,实现文档内容的输入或对文档进行编辑修改。

### (3) 末行模式

命令模式下输入的 vi 命令通常是单个字母,所输的命令都不回显。但有些控制命令表达比较复杂,比如要将文档内容保存到指定的文件,或将指定的文件内容读入到当前位置,此时就需要回显,为此 vi 提供了末行工作模式。

在命令模式下按 Shift+“:”键,即可切换到末行模式,此时在编辑器屏幕的最末一行将显示冒号提示符,在此行中,就可输入 vi 命令,按回车键后即开始执行,执行完毕,又自动回到命令模式。

在末行模式的命令输入过程中,若改变主意放弃执行,则可按 Esc 键退回到命令模式。或用退格键将所输入的命令全部删除之后,再按一下退格键,来实现返回命令模式。

## 3. vi 的常用命令

vi 编辑器常用的命令见表 2.4。

表 2.4 vi 编辑器常用的命令

分 类	命令模式输入	功 能 说 明
存盘与退出 vi	:wq 回车	以当前文件名存盘并退出 vi 编辑器
	:w 文件名 回车	以指定的文件名存盘,不退出 vi
	:w! 文件名 回车	以指定的文件强制存盘,不管文件是否存在
	:q	退出 vi 编辑
	:q!	强制退出 vi,不管是否完成文档的保存工作
vi 的文件存取操作	:n,mw 文件名 回车	将第 n 行至 m 行的内容写入指定的文件
	:n,mw>>文件名 回车	将第 n 行至 m 行的内容以追加方式添加到指定文件的末尾
	:r 文件名 回车	读取指定的文件内容,并插到当前光标所在的行的下面
显示行号	:. =	显示当前光标所在的行的行号

续表

分 类	命令模式输入	功 能 说 明
进入插入编辑模式的命令	i	在当前光标前插入
	a	在当前光标之后插入
	O	在当前光标的下面插入新的一行并接受输入
	O	在当前光标的上面插入新的一行并接受输入
	A	在当前光标所在行的末尾插入
	I	在当前光标所在行的最开头插入
光标移动命令 (在命令模式下输入)	k j h l	分别用于向上、向下、向左、向右移动光标
	G	光标移到文件的最后一行
	\$	光标移到行尾
	nG	移动光标到第 n 行
非 vi 命令在 插入编辑模式 下,直接对内容 进行编辑操作	按 Backspace 键	向左删除一个字
	按 Delete 键	删除当前光标位置的一个字
	按 Page Down 键	向下翻页
	按 Page Up	向上翻页
	按 Home 键	光标移到行首
	按 End 键	光标移到行尾
	按 Insert 键	内容插入与替换模式转换
	上、下、左、右光标键	实现光标的向上、向下、向左、向右的移动
删除指令	ndd	向下删除 n 行内容,当前行包含在内
	nx	向后删除 n 个字
字符串查找	/字符串 回车	向后查找指定的字符串
	?字符串 回车	向前查找指定的字符串
字符串查找与 替换	:n,ms/str1/str2/opt	从第 n 列搜寻到第 m 列,搜索 str1 字符串用 str2 字符串取代, opt 选项若为 g 则自动全部替换,为 c 表示确认后再替换
	:1,\$s/str1/str2/g	从头到尾自动用 str2 替换 str1

## 2.5 建立与使用文件系统

在 Linux 安装过程中,会自动创建分区和文件系统,但在 Linux 的使用和管理中,经常会因硬盘空间不够,需要通过添加硬盘来扩充可用空间。此时就必须熟练掌握手工创建分区和文件系统以及文件系统的挂载方法。在硬盘中建立和使用文件系统,通常应遵循以下步骤:

(1) 为便于管理,首先应对硬盘进行分区。

(2) 对分区进行格式化,以建立相应的文件系统。

(3) 将分区挂载到系统的相应目录(挂载点目录必须为空),通过访问该目录,即可实现在该分区进行文件的存取操作。

### 2.5.1 创建分区

Red Hat Linux 9 提供了 fdisk 和 parted 两个命令用于对硬盘进行分区,fdisk 命令简单易用,parted 命令功能虽强大一些,但使用较复杂,此处主要介绍利用 fdisk 命令来进行分区。

键入不带任何参数的 mount 命令,可查看了解当前系统已挂载的设备。键入不带参数的 fdisk 命令,将显示该命令的用法提示,其基本用法为:

```
# fdisk 设备名
```

第 1 个 IDE 设备的设备名为 hda,第 2 个为 hdb,第 1 个 SCSI 硬盘设备为 sda,第 2 个 SCSI 硬盘为 sdb。若要对第 2 个 IDE 硬盘创建分区,则操作命令就应为 fdisk /dev/hdb。

fdisk 命令是以交互方式进行操作的,在 Command(m for help): 状态下,键入 m 子命令,可查看所有的子命令及对应的功能解释。fdisk 的交互操作于命令均为单个字母,常用的主要是以下几个:

a 设置可引导标志	b 设置卷标	d 删除一个分区	n 新建分区
p 显示分区信息	v 校验分区表	q 不存盘退出	w 存盘退出

服务器硬盘一般多采用 SCSI 硬盘,现假设在服务器中增加了一个 10GB 的 SCSI 硬盘,现要将整个硬盘划分成一个分区,则操作方法如下(“//”后面的文字为操作注解):

```
[root@rh9 root]# fdisk /dev/sdb
Command (m for help): p // 键入 p,查看是否有分区
Disk /dev/sdb: 10.7GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

```

Device Boot      Start          End      Blocks      Id      System
// 无输出,说明没有分区

Command (m for help): n          // 键入 n,新建分区
Command action                    // 提示选择下一步的动作,e代表创建扩展分区,p为主分区
   e    extended
   p    primary partition (1-4)
p                                  // 键入 p,选择创建主分区
Partition number (1-4):1          // 提示选择创建第几个分区.此处要创建的是第 1 个,输入 1
First cylinder (1-1305, default 1):1 // 分区使用磁盘空间的开始柱面号
Last cylinder or + size or - sizeM or + sizeK (1-1305, default 1305): 1305
//分区使用到的最后一个柱面号
//注此处是将整个硬盘创建一个分区。若要以分区的大小方式指定,则键入+10240M。
Command (m for help): p          // 查看新创建的分区
Disk /dev/sdb: 10.7GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start          End      Blocks      Id      System
/dev/sdb1              1          1305     10482381      83      Linux

Command (m for help): w          // 键入 w 存盘退出
The partition table has been altered!
Calling ioctl() to re-read partition table.
SCSI device sdb: 20971520 512-byte hdwr sectors (10737MB)
SCSI device sdb: 20971520 512-byte hdwr sectors (10737MB)
Syncing disks.
[root@rh9 root]#

```

至此,分区创建成功。

### 2.5.2 在分区建立文件系统

分区创建后,接下来就要根据要创建的文件系统类型,选择相应的命令来格式化分区,从而实现在分区创建相应的文件系统。只有建立了文件系统后,该分区才能用于存取文件。

在 Red Hat Linux 9 中,对于不同类型的文件系统,提供了不同的格式化命令,如表 2.5 所示。

为了与以前版本相兼容,Red Hat Linux 9 对于同一文件系统的创建命令,提供了多个命令名,比如 mkfs、ext3、mkfs.ext2 和 mke2fs,虽然名称不同,但实质调用的都是 mke2fs 这个命令程序。Red Hat Linux 9 默认采用 ext3 文件系统。

表 2.5 建立文件系统的命令

命令名 1	命令名 2	命令名 3	功 能
mkfs, ext3	mkfs, ext2	mke2fs	建立 ext3 文件系统
mkfs, vfat	mkfs, msdos	mkdosfs	建立 vfat 文件系统
mkfs, reiserfs		mkreiserfs	建立 reiser 文件系统
		mkjfs, jfs	建立 jfs 文件系统
		mkswap	建立 swap 文件系统

若要对刚才分好区的硬盘进行格式化,创建 ext3 文件系统,则操作命令为:

```
[root@rh9 root]# mkfs, ext3 /dev/sdb1
```

格式化过程的输出信息如图 2.4 所示。

```

[root@rh9 root]# mkfs, ext3 /dev/sdb1
mke2fs 1.32 (09-Nov-2002)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1310720 inodes, 2620595 blocks
131029 blocks (5.00%) reserved for the super user
First data block=8
38 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
    32768, 90384, 163848, 229376, 294912, 819200, 804736, 1685632

Writing inode tables: sorted: Tagged Quering now active for Target 1
done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 39 mounts or
188 days, whichever comes first. Use tune2fs -c or -i to override.
[root@rh9 root]#

```

图 2.4 格式化硬盘分区

另外, Linux 还提供了几个用于对分区进行维护的实用命令。

### 1. e2label 命令

用于为指定的分区设置一个卷标,用法为“e2label 分区设备名 [卷标名]”。

比如设置/dev/sdb1分区的标卷为vodftp,则操作命令为e2label /dev/sdb1 vodftp。

若默认卷标参数,采用“e2label 分区设备名”的用法,则提示输入该分区的标卷名称。

### 2. findfs 命令

findfs 命令用于查找并输出指定卷标所在的文件系统的设备名,其用法为 findfs LABEL=卷标。

比如要查找卷标为 vod 的文件系统对应的设备名,则命令为 `findfs LABEL=vod`。

### 3. e2fsck 命令

该命令用于检测指定分区中 ext2/ext3 文件系统,并进行错误修复。注意,该命令不能用于检测系统中已经挂载的文件系统,否则将造成文件系统的损坏。

用法: `e2fsck 分区设备名`

比如: `e2fsck /dev/sdb1`

## 2.5.3 挂载和使用文件系统

为了将分区挂载到 Linux 文件系统中,需要先创建一个挂载点目录,或利用某个现成的空目录。假设要求将硬盘分区挂载到 /usr 目录下面的 myvod 目录,则操作命令为:

```
[root@rh9 root]# mkdir /usr/myvod           # 创建挂载点目录
[root@rh9 root]# mount /dev/sdb1 /usr/myvod   # 挂载/dev/sdb1 设备到/usr/myvod 目录
[root@rh9 root]# mount                       # 查看当前已挂载的设备
```

从输出的内容中,就会看到下面一行的内容,表明挂载成功。

```
/dev/sdb1 on /usr/myvod type ext3 (rw)
```

以后存取 /usr/myvod 目录中的文件,实际上就是存取第 2 个 SCSI 硬盘中的文件。

若要卸载该硬盘分区,则执行命令 `umount /dev/sdb1` 即可。

以上对硬盘的挂载仅对本次操作有效,系统重启后又需要重新挂载。由于硬盘是长期要使用的设备,因此希望在系统启动时能自动进行挂载,要实现该功能,可利用 /etc/fstab 配置文件来实现,该配置文件类似于 DOS 系统的自动批处理文件的功能,fstab 配置文件主要用来设置在 Linux 启动时需要执行的一些操作,通常是文件系统和外部设备的挂载操作。

在 Red Hat Linux 9 启动过程中,init 进程会自动读取 /etc/fstab 配置文件中的内容,并挂载相应的文件系统,因此,只需将要自动挂载的设备和挂载点信息加入到 fstab 配置文件中即可。

要查看 fstab 配置文件中的内容,可使用 `more /etc/fstab` 命令。

fstab 配置文件中第 5 列中的 1 代表在系统出问题时需要导出(dump),第 6 列中的 1 表示在开机启动时,需要用 fsck 命令来检查其文件系统。

fstab 配置文件非常重要,若配置错,就有可能造成系统不能正常启动,为防止误操作损坏原配置文件,可将 /etc/fstab 配置文件复制一份到 /root 目录,然后再利用 vi 编辑器,在 /etc/fstab 配置文件最后增加一行如下的内容,用于自动挂载该硬盘分区。

```
/dev/sdb1          /usr/myvod        ext3
```

其操作命令为:

```
[root@rh9 root]# cp /etc/fstab fstab_bak  
[root@rh9 root]# vi /etc/fstab
```

另外,也可不使用 vi 编辑器,而直接使用“>>”追加定向符,向/etc/fstab 文件中添加挂载信息,其操作命令为:

```
[root@rh9 root]# echo "/dev/sdb1          /usr/myvod          ext3">>/etc/fstab
```

注意:不要使用“>”定向符,否则将覆盖掉/etc/fstab 配置文件中的原有内容。

修改/etc/fstab 配置文件后,利用 reboot 重启 Linux,然后再用 mount 命令查看,可以看到系统已自动挂载了 sdb1 分区。

## 2.6 在 Linux 中使用移动存储设备

移动存储设备常见的主要是软盘和 USB 存储设备(包括 U 盘和 USB 移动硬盘),目前常用的主要是 USB 存储设备。

### 2.6.1 在 Linux 中使用软盘

#### 1. 制作软盘文件系统

软盘在使用前应先建立文件系统,可通过格式化操作来完成。对于软盘,Red Hat Linux 9 支持 ext2 和 FAT 格式的文件系统。

##### (1) 建立 ext2 文件系统

命令格式: ext2 软盘设备文件名

命令功能:在指定驱动器设备的软盘上建立 ext2 文件系统。

目前计算机的软驱设备一般只有一个,其设备名为/dev/fd0,因此要在软盘上建立文件系统,则命令为:

```
[root@rh9 root]# mke2fs /dev/fd0
```

文件系统建立好以后,就可利用 mount/mnt/floppy 命令挂载软盘,进入/mnt/floppy 目录,存取软盘中的文件。

对于新建的 ext2 和 ext3 文件系统,会自动创建 lost+found 目录。

##### (2) 建立 FAT 文件系统

要建立可在 DOS 系统使用的 FAT 文件系统,可用 mkdosfs 命令来完成,其命令用法为:

```
mkdosfs 软盘设备文件名
```

FAT 文件系统创建后,不需要挂载,采用与 DOS 系统相同的做法,通过存取访问 A 盘来实现。



在 Linux 系统中,提供了许多以 m 开头的命令,这些命令与 DOS 系统的磁盘文件操作命令相对应,只是在原 DOS 命令的基础上前缀了一个 m,其功能与用法也与 DOS 命令相同。比如,若要查看 A 盘中的文件,则可执行 `mmdir a;` 命令来实现。

Linux 提供的类 DOS 命令常用的主要有: `mattrib`、`mcd`、`mmd`、`mrd`、`mmove`、`mren`、`mtype`、`mcopy`、`mdel`、`mdeltree`、`mdir`、`mformat`、`mlabel` 等,这些命令适用于操作 FAT 文件系统,通常用于操作软盘。

### (3) 用图形界面格式化软盘

在 X-Windows 图形界面主菜单下面的 System Tools 中,提供了 Floppy Formatter 实用工具,利用该工具也可实现对软盘的格式化,其界面如图 2.5 所示。



图 2.5 软盘格式化实用程序

## 2. 制作 Linux 系统启动盘

准备一张 Linux 系统启动盘是必要的,当系统不能从硬盘启动时,可利用启动软盘来启动系统。要建立启动软盘,可使用 `mkbootdisk` 命令来实现,其用法为:

`mkbootdisk -device 软盘设备文件名 Linux 内核版本号`

Linux 内核版本号可通过 `uname -r` 命令来自动获得,因此,该命令的实际用法格式为:

```
mkbootdisk -device /dev/fd0 `uname -r`
```

## 3. 制作软盘镜像文件

软盘易于损坏,通常可将重要的软盘内容,制作成软盘镜像文件,保存在硬盘或光盘

中。在 Linux 中,制作和使用软盘镜像文件比较方便,可使用 cp 命令来实现,其用法为:

```
cp /dev/fd0 镜像文件名
```

该命令的功能即是把/dev/fd0 设备中的内容复制到镜像文件中,镜像文件扩展名通常命名为.img。

比如要制作启动盘的镜像文件,并将镜像文件命名为 myboot.img,则操作命令为:

```
[root@rh9 root]# cp /dev/fd0 myboot.img
```

要查看镜像文件的类型,可使用“file 镜像文件名”命令来查看。

#### 4. 从镜像文件制作软盘

在需要时,可将镜像文件中的内容恢复到软盘中,其操作命令为:

```
cp 镜像文件名 /dev/fd0
```

#### 5. 挂载使用镜像文件

Linux 支持直接挂载软盘镜像文件,并可读取其中的内容,这与直接挂载软盘具有同样的效果,由于软盘读取速度慢,这是一种较好的替换使用软盘的方式,其挂载方法为:

```
mount -o loop 软盘镜像文件 挂载点路径
```

比如要将 myboot.img 镜像文件挂载到/mnt/floppy 目录中,则操作命令为:

```
[root@rh9 root]# mount -o loop myboot.img /mnt/floppy
```

```
[root@rh9 root]# ls /mnt/floppy
```

### 2.6.2 在 Linux 中使用 USB 存储设备

USB 存储设备具有存取速度快、稳定性高、即插即用和携带方便的特点,目前应用已十分普遍。USB 存储设备常用的主要是 U 盘和 USB 移动硬盘两种。

在 Linux 中,将 USB 存储设备当作 SCSI 设备来对待,对于 U 盘,如果没有进行分区,则使用相应的 SCSI 设备文件名来挂载使用,如果 U 盘中存在分区,则使用相应分区的设备文件名来进行挂载。USB 硬盘,则使用对应分区的设备文件名来进行挂载即可。

USB 存储设备不使用时,要先 umount,然后再移除 USB 设备。下面以一个 16MB 的 U 盘和一个外置 USB 2.0 接口的移动硬盘为例,介绍 USB 存储设备在 Linux 中的用法。

#### 1. 在 Linux 中使用 U 盘

##### (1) 连接 U 盘

将 U 盘插入计算机的 USB 接口,之后,Linux 将检测到该设备,并显示出相关信息,如下所示。

```
usb, c: USB device 2 (vend/prod 0xea0/0x6803) is not claimed by any active driver.
```

```
Vendor: PINGYU      Model: ADP      Rev: 1.11
Type:   Direct-Access      ANSI SCSI revision: 02
Attached scsi removable disk sdb at scsi2, channel 0, id 0, lun 0
SCSI device sdb: 32256 512-byte hdwr sectors (17MB)
sdb: Write Protect is off
```

从输出的信息中,可获知该 USB 的容量大小、存取方式以及在当前 Linux 系统中的设备名称(sdb)。获得 USB 设备的设备名称,这是最重要的,因为下面要利用该设备名来挂载 USB 盘。根据系统所安装的 SCSI 设备的不同,具体使用时,U 盘的设备名会有所不同。查看完所输出的信息后,按回车,回到 Linux 的命令提示符状态。

### (2) 创建挂载点目录

为了能挂载使用 U 盘,还需在/mnt 目录下,创建一个用于挂载 USB 盘的目录,如 usb-disk。

```
[root@rh9 root]# mkdir /mnt/usb-disk
```

### (3) 挂载和使用 U 盘

当前 U 盘只有一个 FAT 分区,因此使用 sdb1 设备名来挂载,实现命令为:

```
[root@rh9 root]# mount -t vfat /dev/sdb1 /mnt/usb-disk/
```

执行挂载命令时,只要未输出错误信息,则意味着挂载成功,进入/mnt/usb-disk 目录,就可存取访问 U 盘中的内容了。

若挂载时所使用的设备名错误,比如使用/dev/sdb 来进行挂载,此时将显示类似以下的错误信息:

```
FAT: bogus logical sector size 20487
VFS: Can't find a valid FAT filesystem on dev 08:10
or too many mounted file systems
```

若挂载点目录未创建,则会显示如下所示的错误提示信息:

```
mount: mount point /mnt/usb-disk/ does not exist
```

若 U 盘容量较大,还有第 2 个分区,则可使用/dev/sdb2 来进行挂载,挂载前同样要先创建挂载点目录。

### (4) 卸载 U 盘

当不再使用 U 盘时,应卸载该设备,然后再从物理上移除设备。若要卸载刚才挂载使用的 U 盘,则实现命令为:

```
[root@rh9 root]# umount /mnt/usb-disk
```

## 2. 使用 USB 移动硬盘

USB 移动硬盘是指外置接口为 USB 的硬盘,所使用的硬盘一般分为笔记本硬盘和普通 IDE 硬盘两种,前者比较小巧,便于携带,后者一般采用普通的 IDE 硬盘,体积相对较大,可以选择具有很大容量的硬盘,以用作系统备份。

下面以外置 USB 2.0 接口的移动硬盘为例介绍其用法。该移动硬盘自带电源接口,采用的是普通的 IDE 硬盘,容量为 120GB,共有 3 个主分区,第 1 个主分区为 NTFS 文件系统,第 2 个主分区为 FAT32 文件系统,第 3 个主分区为 NTFS 文件系统。内核为 2.4、20-8 的 Red Hat Linux 9 还无法直接识别 NTFS 分区,因此 Linux 只能识别该移动硬盘中的第 2 个分区。

### (1) 连接移动硬盘

打开移动硬盘的电源开关,并将 USB 移动硬盘连接线插入计算机的 USB 接口。之后 Linux 将检测到该设备,并显示以下信息:

```
usb.c:USB device 2 (vend/prod 0x402/0x5621) is not claimed by
any active driver.
Vendor: USB 2.0      Model:Storage Device  Rev:0100
Type:   Direct-Access      ANSI SCSI revision: 02
Attached scsi disk sdb at scsi2, channel 0, id 0, lun 0
SCSI device sdb:234441648 512-byte hdwr sectors (120034MB)
```

从第 5 行输出信息可知,该移动硬盘被 Linux 系统识别为第 2 个 SCSI 设备,其设备名为 sdb。

### (2) 挂载硬盘分区

硬盘的设备名当前为 sdb,由于只有第 2 个分区(FAT32)Linux 可以识别,因此,下面挂载第 2 个分区到/mnt/usb-disk 目录中。实现命令为:

```
[root@rh9 root]# mount -t vfat /dev/sdb2 /mnt/usb-disk
[root@rh9 root]# cd /mnt/usb-disk
[root@rh9 usb-disk]# ll                                # 此时应可看到硬盘分区中的内容
```

假设在当前硬盘分区中有一个名为 linux\_soft 的目录,现要求将该目录下的子目录及所有软件,复制到/root/linux\_soft 目录中,则实现的操作为

```
[root@rh9 usb-disk]# cp -r linux_soft /root/linux_soft
[root@rh9 usb disk]# cd
[root@rh9 root]# ll linux_soft                        # 查看复制得到的目录和文件
```

### (3) 卸载 USB 硬盘

卸载命令为: umount /mnt/usb-disk。

## 2.7 制作与使用光盘镜像文件

### 2.7.1 制作光盘镜像文件

#### 1. 从光盘制作镜像文件

光盘的文件系统为 ISO 9660, 光盘镜像文件的扩展名通常命名为 .iso, 其制作方法与软盘相同, 使用 cp 命令来完成, 其命令用法为:

```
cp /dev/cdrom 镜像文件名
```

例如, 要将当前光盘的内容制作一个光盘镜像文件, 其文件名为 mybook.iso, 则操作命令为:

```
[root@rh9 root]# cp /dev/cdrom mybook.iso
[root@rh9 root]# file mybook.iso          # 查看镜像文件的类型
mybook.iso: ISO 9660 CD-ROM filesystem data
```

#### 2. 使用目录文件制作镜像文件

除了可将整张光盘制作成一个镜像文件外, Linux 还支持将指定的目录及目录下的文件和子目录, 制作生成一个 ISO 镜像文件。对目录制作镜像文件, 使用 mkisofs 命令来实现, 其用法为:

```
mkisofs -r -o 镜像文件名 目录路径
```

例如, 要将/etc 目录下的文件制作生成一个名为 mylinuxetc.iso 镜像文件, 则操作命令为:

```
[root@rh9 root]# mkisofs -r -o mylinuxetc.iso /etc
```

### 2.7.2 使用光盘镜像文件

ISO 镜像文件可以直接挂载使用, 也可利用它来刻录制作对应的光盘。

#### 1. 挂载使用光盘镜像文件

光盘镜像文件的挂载和使用方法与软盘类似, 实现挂载的命令为:

```
mount -o loop ISO 镜像文件名 挂载点目录
```

挂载成功后, 进入挂载点目录, 即可访问 ISO 镜像文件中的内容。使用镜像文件, 可减少光盘的读取, 提高访问速度。

比如要将 mylinuxetc.iso 镜像文件挂载到 /mnt/cdrom 目录, 则操作命令为:

```
[root@rh9 root]# mount -o loop mylinuxetc.iso /mnt/cdrom
[root@rh9 root]# cd /mnt/cdrom
[root@rh9 root]# ll
```

## 2. 刻录光盘

在 Linux 中,使用 `cdrecord` 命令,利用 ISO 镜像文件可刻录对应的光盘。要刻录光盘,计算机还必须配置有光盘刻录光驱,刻录光驱在 Linux 系统中被当作 SCSI 设备对待。

### (1) 检测刻录光驱的设备 ID 号

在刻录光盘之前,可使用 `cdrecord -scanbus` 命令检测系统中光盘刻录机的相关参数,从而获得该光驱设备的设备号,在正式刻录时,其操作命令中需要指定该设备的设备号。

### (2) 刻录光盘

刻录光盘可使用 `cdrecord` 命令实现,其命令用法为:

`cdrecord -v speed=刻录速度 dev=刻录光驱设备号 ISO 镜像文件名`

例如:

`cdrecord -v speed=12 dev=0,0 /root/mylinuxetc.iso`

## 习题

1. Linux 交换分区必须使用的文件系统类型是( ), Red Hat Linux 9 的根分区默认使用的文件系统类型为( )。

- A. ext2                      B. ext3                      C. swap                      D. jfs

2. 光盘所使用的文件系统类型为( )。

- A. ext2                      B. ext3                      C. swap                      D. ISO 9660

3. 以下对 Linux 的说法,不正确的是( )。

- A. Red Hat Linux 9 不支持 NTFS 文件系统,但可通过升级内核来实现对 NTFS 文件系统的支持
- B. Red Hat Linux 支持很多种不同的文件系统,但默认使用的是 ext2 或 ext3 文件系统
- C. 要创建不同的文件系统, Linux 需要使用不同的命令,通过格式化操作来实现
- D. 安装 Linux 操作系统,只需要一个分区即可,因此 Linux 只有一个根目录,用“/”来表示

4. 以下命令中,可以将用户身份临时改变为 root 的是( )。

- A. Su                      B. su                      C. login                      D. whoami
5. 在以下设备文件中,代表第2个 SCSI 硬盘的第1个逻辑分区的设备文件是( )。
- A. /etc/sdb              B. /etc/sda              C. /etc/sdb5              D. /etc/sdb1
6. 以下设备文件中,代表空设备的是( )。
- A. /etc/ttyS1              B. /etc/null              C. /etc/Null              D. /etc/empty
7. 在 Red Hat Linux 中,在#命令行提示符状态下执行 cd 命令后,其当前目录为( )。
- A. /                      B. /home                      C. /root                      D. /home/root
8. 对 Linux 文件系统的自动挂载,其配置工作是在( )文件中完成的。
- A. /etc/inittab              B. /etc/fstab              C. /usr/etc/fstab              D. /usr/etc/inittab
9. 以下挂载光盘的方法中,不正确的是( )。
- A. mount /mnt/cdrom  
B. mount /dev/cdrom  
C. mount -t iso9660 /dev/cdrom /mnt/cdrom  
D. umount /dev/cdrom
10. 以下关于 Linux 文件的描述,不正确的是( )。
- A. Linux 的文件命名中不能含有空格字符  
B. Linux 的文件名区分大小写,且最多可有 256 个字符  
C. Linux 的文件类型不由扩展名决定,而由文件的属性决定  
D. 若要将文件暂时隐藏起来,可通过设置文件的相关属性来实现
11. 若要改变一个文件的拥有者,可通过( )命令来实现。
- A. chmod                      B. chown                      C. usermod                      D. file
12. 若要设置/usr/myprog 文件的拥有者有读、写和可执行权限,用户组和其他用户均没有对该文件的操作权限,以下操作命令中,正确的是( )。
- A. chmod 700 /usr/myprog              B. chown 700 /usr/myprog  
C. chmod u=rwx /usr/myprog              D. chmod u=rwx go-r-w-x /usr/myprog
13. Linux 命令的续行符使用( )。
- A. /                      B. \                      C. ;                      D. &
14. 若要让 Linux 系统在 5 分钟后重新启动,以下命令中正确有效的是( )。
- A. reboot -t 5                      B. shutdown -r -t 5  
C. shutdown -r -t secs 5                      D. shutdown -h -t 5
15. 在 Linux 中,若要返回上三级目录,则应使用( )命令。
- A. cd /                      B. cd ../../                      C. cd ../../..                      D. cd -
16. 以下命令用法中,功能与 ll 相同的是( )。
- A. ls -a                      B. ls -l                      C. ls -la                      D. ls -F
17. 若要删除/usr/mytest 目录及其下的子目录和文件,以下操作正确的是( )。

- A. rmdir /usr/mytest                      B. rm /usr/mytest  
C. rm -f /usr/mytest                      D. rm -r /usr/mytest

18. 在对目录进行复制、删除或移动操作时,如果要对整棵目录树进行操作,应在命令中选择使用( )参数。

- A. -r                      B. -f                      C. -b                      D. -i

19. 以下命令中,可用于更新文件或目录的访问日期和时间的命令是( )。

- A. date                      B. update                      C. touch                      D. uptime

20. 以下命令中,不能用来查看文本文件内容的命令是( )。

- A. less                      B. cat                      C. tail                      D. diff

21. 若要在指定的文件中查找并显示目标字符串所在行的内容,可使用( )命令来实现。

- A. diff                      B. grep                      C. head                      D. more

22. 假设 file1.txt 文件不存在, file2.txt 存在,则内容不为空,执行以下命令后,生成的文件内容不为空的是( )。

- A. touch file1.txt  
B. 执行 cat >file1.txt 命令后,立即按 Ctrl+D  
C. cat file2.txt>file1.txt  
D. cat /dev/null>file1.txt

23. 若要列出/etc 目录下所有以 vsftpd 开头的文件,以下命令中,不能实现的是( )。

- A. ls /etc |grep vsftpd                      B. ls /etc/vsftpd  
C. ls /etc/vsftpd \*                      D. ll /etc/vsftpd \*

24. 在 Linux 系统中,若要查看当前文件系统的剩余空间,则可使用( )命令。

- A. df                      B. du                      C. free                      D. uptime

25. 目前正处于 vi 的插入编辑模式,若要切换到末行模式,以下操作方法中,正确的是( )。

- A. 按 Esc 键                      B. 按 Esc 键,然后按“:”键  
C. 直接按“:”键                      D. 直接按 Shift+“:”键

26. 假设当前处于 vi 的命令模式,现要进入插入模式,以下命令按键中,无法实现的是( )。

- A. I                      B. A                      C. O                      D. l

27. 以下命令不能用于创建 ext3 文件系统的是( )。

- A. mkfs.ext3                      B. mkfs.ext2                      C. mke2fs                      D. mkefs.ext3

28. 若要对一个已挂载的文件系统进行检查,应使用( )命令。

- A. fsck                      B. e2fsck                      C. check                      D. scandisk



## 管理用户和用户组

Linux 是一个多用户、多任务的服务器操作系统,作为一个系统管理员,掌握用户和用户组的创建与管理至关重要。在 Linux 中,可通过命令来创建和管理用户与用户组,也可在图形界面利用用户管理器来管理。

### 3.1 用户和用户组文件

在 Linux 中,用户账号、用户密码、用户组信息和用户组密码均是存放在不同的配置文件中的,本节将对这些配置文件作一个简单介绍,以便对 Linux 系统有更深入的了解。

#### 1. 用户账号文件

在 Linux 系统中,所创建的用户账号及其相关信息(密码除外)均是存放在一个名叫 `passwd` 的配置文件中的,该文件位于 `/etc` 目录。由于所有用户对 `passwd` 文件均有读取的权限,因此密码信息并未保存在该文件中,而是保存在了另外一个名叫 `shadow` 的配置文件中。

Linux 的配置文件均是文本文件,因此可使用文本文件内容查看命令来查看。在 `passwd` 文件中,一行定义一个用户账号,每行均由多个不同的字段构成,各字段值间用“:”分隔,每个字段均代表该账户某方面的信息。

在刚安装完成的 Linux 系统中,`passwd` 配置文件已有很多账户信息了,这些账户是由系统自动创建的,它们是 Linux 进程或部分服务程序正常工作所需要使用的账户,这些账户的最后一个字段的值一般为 `/sbin/nologin`,表示该账户不能用来登录 Linux 系统。

由于 `passwd` 配置文件内容较多,下面仅显示前 10 行的内容,其显示结果如图 3.1 所示。

在 `passwd` 配置文件中,从左至右各字段的对应关系及其含义如表 3.1 所示。

```

[root@rh9 root]# head /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
[root@rh9 root]#

```

图 3.1 passwd 用户文件部分内容

表 3.1 passwd 配置文件各字段的对应关系

用户账号	用户密码	用户 ID	用户组 ID	用户名全称	用户主目录	用户所使用的 Shell
root	x	0	0	root	/root	/bin/bash
bin	x	1	1	bin	/bin	/sbin/nologin
⋮	⋮	⋮	⋮	⋮	⋮	⋮

由于 passwd 不再保存密码信息,所以用 x 占位代表。用户 ID 是一个惟一代表该用户的一个数字,用户组 ID 代表该用户所属的私有组的组号,也是一个惟一代表该用户组的一个数字。

Shell 是用户登录后所使用的一个命令行界面。输入的命令由 Shell 进行解释,并发送给 Linux 内核,由内核进行具体操作,以实现命令所体现的功能。Linux 系统自带有许多种 Shell,系统默认使用的是 /bin/bash。若在配置文件中,该字段的值为空,则默认使用“/bin/sh”Shell。在 /etc 目录下的 shells 文件中,列出了系统可以使用的 Shell 列表,可使用 more /etc/shells 或 chsh -l 命令来查看。

若要使某个用户账户不能登录 Linux,只需设置该用户所使用的 Shell 为 /sbin/nologin 即可。比如,对于 FTP 账户,一般只允许登录和访问 FTP 服务器,不允许登录 Linux 操作系统。若要让某用户没有 telnet 权限,即不允许该用户利用 telnet 远程登录和访问 Linux 操作系统,则设置该用户所使用的 Shell 为 /bin/true 即可。若要让用户没有 telnet 和 ftp 登录权限,则可设置该用户的 Shell 为 /bin/false。

在 /etc/shells 文件中,若没有 /bin/false 或 /bin/true,则可使用以下命令将其添加进去。

```

[root@rh9 root]# echo "/bin/false" >> /etc/shells
[root@rh9 root]# echo "/bin/true" >> /etc/shells

```

在第 2 章介绍文件的拥有者时,创建了两个用户账户,下面查看一下这两个账户在 passwd 文件中相关信息。新建账户的记录保存在 passwd 文件的末尾。

```
[root@rh9 root]# tail -2 /etc/passwd           # 显示最后 2 行的内容
liyang:x:500:500:;/home/liyang:/bin/bash
fengyuan:x:501:500:;/home/fengyuan:/bin/bash
```

普通用户账户的用户 ID 是从 500 开始编号的,系统账号小于 500。

## 2. 用户密码文件

为安全起见,用户真实的密码采用 MD5 加密算法加密后,保存在/etc/shadow 配置文件中,该文件只有 root 用户可以读取。

与 passwd 文件类似,shadow 文件也是每行定义和保存一个账户的相关信息。第 1 个字段为账户名,第 2 个字段为该账户的密码。

```
[root@rh9 root]# tail -2 /etc/shadow
liyang: $1$fkjLp5zp$lBqVILqHKFywT0OEjgzPN/:12602:0:99999:7:::
fengyuan: $1$sqUt/Cu$egGTKs.9cFQk41xuhfZWt/:12602:0:99999:7:::
```

## 3. 用户组账号文件

用户组账户信息保存在/etc/group 配置文件中,任何用户均可以读取。用户组的真实密码保存在/etc/gshadow 配置文件中。

在 group 文件中,第 1 个字段代表用户组的名称,第 2 列为 x,第 3 列为用户组的 ID 号,第 4 列为该组中的用户成员列表,各用户名间用逗号分隔。

# 3.2 管理用户账户与密码

## 3.2.1 用户账号管理

### 1. 添加用户

#### (1) 命令用法

在 Linux 中,创建或添加新用户使用 useradd 命令来实现,其命令用法为:

```
useradd [option] username
```

该命令的 option 可选项较多,常用的主要有:

- c 注释 用于设置对该账户的注释说明文字。
- d 主目录 指定用来取代默认的/home/username的主目录。
- m 若主目录不存在,则创建它。-r 与-m 相结合,可为系统账户创建主目录。
- M 不创建主目录。
- e expire\_date 指定账户过期的日期。日期格式为 MM/DD/YY。
- f inactive\_days 账号过期几日后永久停权。若指定为 0,则立即被停权;为-1,

则关闭此功能。

**-g 用户组** 指定将该用户加入到哪一个用户组中。该用户组在指定时必须已存在。

**-G 用户组列表** 指定用户同时也是其中成员的其他用户组列表,各组用逗号分隔。

**-n** 不为用户创建私有用户组。

**-s shell** 指定用户登录时所使用的 Shell,默认为/bin/bash。

**-r** 创建一个用户 ID 小于 500 的系统账户,默认不创建对应的主目录。

**-u 用户 ID** 手工指定新用户的 ID 值,该值必须惟一,且大于 499。

**-p password** 为新建用户指定登录密码。此处的 password 是对登录密码经 MD5 加密后所得到的密码值,不是真实密码原文,因此在实际应用中,该参数选项使用较少,通常单独使用 passwd 命令来为用户设置登录密码。

## (2) 应用示例

例如,若要创建一个名为 zhangyan 的用户,并作为 student 用户组的成员,则操作命令为:

```
[root@rh9 root]# useradd -g student zhangyan
[root@rh9 root]# tail -1 /etc/passwd           # 显示最后 1 行的内容
zhangyan:x:502:500:./home/zhangyan:/bin/bash
```

添加用户时,若未用 -g 参数指定用户组,则系统默认会自动创建一个与用户账号同名的私有用户组。若不需要创建该私有用户组,则可选用 -n 参数。

比如,添加一个名为 lijie 的账户,但不指定用户组,其操作结果为:

```
[root@rh9 root]# useradd lijie
[root@rh9 root]# tail -1 /etc/passwd
lijie:x:503:503:./home/lijie:/bin/bash
[root@rh9 root]# tail -2 /etc/group          # 显示最后 2 行的内容
student:x:500:
lijie:x:503:                                # 系统自动创建了名为 lijie 的用户组, ID 号为 503
```

创建用户账户时,系统会自动创建该账户对应的主目录,该目录默认放在 /home 目录下,若要改变位置,可利用 -d 参数指定;对于用户登录时所使用的 Shell,默认为 /bin/bash,若要更改,则使用 -s 参数指定。

例如,若要创建一个名为 vodup 的账户,主目录放在 /var 目录下,并指定登录 Shell 为 /sbin/nologin,则操作命令为:

```
[root@rh9 root]# useradd -d /var/vodup -s /sbin/nologin vodup
[root@rh9 root]# tail -1 /etc/passwd
```

```
vodup:x:504:504:./var/vodup:/sbin/nologin
[root@rh9 root]# tail -1 /etc/group
vodup:x:501:
```

在 Linux 中,对于新创建的用户,在没有设置密码的情况下,账户密码是处于锁定状态的,此时用户账户将无法登录系统。在创建新用户时,对于没有指定的属性,其默认设置位于/etc/default/useradd 文件中。

## 2. 设置账户属性

对于已创建好的账户,可使用 usermod 命令来修改和设置账户的各项属性,包括登录名、主目录、用户组、登录 Shell 等,该命令的用法为:

```
usermod [option] username
```

命令参数选项 option 大部分与添加用户时所使用的参数相同,参数的功能也一样,下面按用途介绍该命令新增的几个参数。

### (1) 改变用户账户名

若要改变用户名,可使用 -l(L 的小写)参数来实现,其命令用法为:

```
usermod -l 新用户名 原用户名
```

例如,若要将用户 lijie 更名为 lijunjie,则操作命令为:

```
usermod -l lijunjie lijie
[root@rh9 root]# usermod -l lijunjie lijie
[root@rh9 root]# tail -1 /etc/passwd
lijunjie:x:503:503:./home/lijie:/bin/bash
```

从输出结果可见,用户名已更改为了 lijunjie。主目录仍为原来的/home/lijie,若也要将其更改为/home/lijunjie,则可通过执行以下命令来实现。

```
[root@rh9 root]# usermod -d /home/lijunjie lijunjie # 注意指定要修改属性的用户名
[root@rh9 root]# tail -1 /etc/passwd
lijunjie:x:503:503:./home/lijunjie:/bin/bash # 主目录更改成功
[root@rh9 root]# mv /home/lijie /home/lijunjie # 注意将实际的目录也相应更改为 lijunjie
```

若要将 lijunjie 加入 student 用户组(用户组 ID 为 500),则实现的命令为:

```
usermod -g student lijunjie 或 usermod -g 500 lijunjie
[root@rh9 root]# usermod -g student lijunjie
[root@rh9 root]# tail -1 /etc/passwd
lijunjie:x:503:500:./home/lijunjie:/bin/bash # 用户组已更改为了 500,操作成功
```

### (2) 锁定账户

若要临时禁止用户登户,可将该用户账户锁定。锁定账户可利用 -L 参数来实现,其

命令用法为：

`usermod -l` 要锁定的账户

比如，若要锁定 lijunjie 账户，则操作命令为 `usermod -L lijunjie`。

Linux 锁定账户，是通过在密码文件 shadow 的密码字段前加“!”来标识该用户被锁定。

### (3) 解锁账户

要解锁账户，可使用带-U 参数的 `usermod` 命令来实现，其用法为：

`usermod -U` 要解锁的账户

比如，若要解除对 lijunjie 账户的锁定，则操作命令为 `usermod -U lijunjie`。

## 3. 删除账户

要删除账户，可使用 `userdel` 命令来实现，其用法为：

`userdel [-r]` 账户名

-r 为可选项，若带上该参数，则在删除该账户的同时，一并删除该账户对应的主目录。

比如，若要删除 vodup 账户，并同时删除其主目录，则操作命令为 `userdel -r vodup`。

若要设置所有用户账户密码过期的时间，则可通过修改 `/etc/login.defs` 配置文件中的 `PASS_MAX_DAYS` 配置项的值来实现，其默认值为 99999，代表用户账户密码永不过期。其中的 `PASS_MIN_LEN` 配置项用于指定账户密码的最小长度，默认为 5 个字符。

## 3.2.2 用户密码管理

### 1. 设置用户登录密码

Linux 的账户必须设置密码后，才能登录系统。设置账户登录密码，使用 `passwd` 命令，其用法为：

`passwd` [账户名]

若指定了账户名称，则设置指定账户的登录密码，原密码自动被覆盖。只有 root 用户才有权设置指定账户的密码，一般用户只能设置或修改自己账户的密码，使用不带账户名的 `passwd` 命令来实现设置当前用户的密码。

例如，若要设置 lijunjie 账户的登录密码，则操作命令为：

```
[root@rh9 root]# passwd lijunjie
Changing password for user lijunjie.
New password:                               # 键入密码
Retype new password:                         # 重输密码
passwd: all authentication tokens updated successfully.
```

账户登录密码设置后,该账户就可登录系统了。按 Alt+F2 键,选择第 2 号虚拟控制台(tty2),然后利用 lijunjie 账户登录,以检验能否登录。

## 2. 锁定账户密码

在 Linux 中,除了用户账户可被锁定外,账户密码也可被锁定,任何一方被锁定后,都将导致该账户无法登录系统。只有 root 用户才有权执行该命令。锁定账户密码使用带-l 参数的 passwd 命令,其用法为:

```
passwd -l 账户名
```

例如,若要锁定 lijunjie 账户的密码,则操作命令为 passwd -l lijunjie。

## 3. 解锁账户密码

用户密码被锁定后,若要解锁,使用带-u 参数的 passwd 命令,该命令只有 root 用户才有权执行,其用法为:

```
passwd -u 要解锁的账户
```

## 4. 查询密码状态

要查询当前账户的密码是否被锁定,可使用带-S 参数的 passwd 命令来实现,其用法为:

```
passwd -S 账户名
```

若账户密码被锁定,将显示输出“Password locked.”,若未加密,则显示“Password set,MD5 crypt.”。

## 5. 删除账户密码

若要删除账户的密码,使用带-d 参数的 passwd 命令来实现,该命令也只有 root 用户才有权执行,其用法为:

```
passwd -d 账户名
```

账户密码被删除后,将不能登录系统,除非重新设置密码。

# 3.3 用户组管理

用户组是用户的集合,通常将用户进行分类归组,便于进行访问控制。用户与用户组属于多对多的关系,一个用户可以同时属于多个用户组,一个用户组可以包含多个不同的用户。

## 1. 创建用户组

创建用户组使用 groupadd 命令,其命令用法为:

groupadd [-r] 用户组名称

若命令带有-r 参数,则创建系统用户组,该类用户组的 GID 值小于 500;若没有-r 参数,则创建普通用户组,其 GID 值大于或等于 500。在前面创建的 student 用户组,由于是所创建的第 1 个普通用户组,故其 GID 值为 500。

若要创建一个名为 sysgroup 的系统用户组,则操作命令为:

```
[root@rh9 root]# groupadd -r sysgroup
[root@rh9 root]# tail -1 /etc/group
sysgroup:x:101:                                #该用户组的 ID 为 101
```

## 2. 修改用户组属性

用户组创建后,根据需要可对用户组的相关属性进行修改。对用户组属性的修改,主要是修改用户组的名称和用户组的 GID 值。

### (1) 改变用户组名称

若要对用户组进行重命名,可使用带-n 参数的 groupmod 命令来实现,其用法为:

groupmod -n 新用户组名 原用户组名

对用户组更名,不会改变其 GID 的值。

比如,若要将 sysgroup 用户组更名为 teacher 用户组,则操作命令为:

```
[root@rh9 root]# groupmod -n teacher sysgroup
[root@rh9 root]# tail -1 /etc/group
teacher:x:101:
```

### (2) 重设用户组的 GID

用户组的 GID 值可以重新进行设置修改,但不能与已有用户组的 GID 值重复。对 GID 进行修改,不会改变用户名的名称。

要修改用户组的 GID,使用带-g 参数的 groupmod 命令,其用法为:

groupmod -g new\_GID 用户组名称

例如,若要将 teacher 组的 GID 更改名为 501,则操作命令为:

```
[root@rh9 root]# groupmod -g 501 teacher
[root@rh9 root]# grep teacher /etc/group    #在/etc/group 文件中查找并显示含有 teacher 的行
teacher:x:501:
```

## 3. 删除用户组

删除用户组使用 groupdel 命令来实现,其用法为:

groupdel 用户组名



比如,若要删除 teacher 用户组,则操作命令为 groupdel teacher。

在删除用户组时,被删除的用户组不能是某个账户的私有用户组,否则将无法删除,若要删除,则应先删除引用该私有用户组的账户,然后再删除用户组。操作演示如下:

```
[root@rh9 root]# groupadd teacher          # 新建 teacher 用户组
[root@rh9 root]# useradd -g teacher wj      # 创建 wj 用户,并将 teacher 组作为其私有用户组
[root@rh9 root]# groupdel teacher
groupdel: cannot remove user's primary group. # 提示不能删除用户的私有组
[root@rh9 root]# userdel -r wj              # 删除 wj 用户
[root@rh9 root]# groupdel teacher
[root@rh9 root]# grep teacher /etc/group    # 没有输出,说明 teacher 用户组已不存在,删除成功
```

#### 4. 添加用户到指定的组

可以将用户添加到指定的组,使其成为该组的成员。其实现命令为:

gpasswd -a 用户账户 用户组名

例如,现创建一个名为 ftpusers 的用户组,然后将 liyang 用户添加到 ftpusers 用户组,其操作命令为:

```
[root@rh9 root]# groupadd ftpusers          # 新建 ftpusers 用户组
[root@rh9 root]# gpasswd -a liyang ftpusers # 将 liyang 用户添加到 ftpusers 用户组
Adding user liyang to group ftpusers
[root@rh9 root]# groups liyang              # 用 groups 命令查看 liyang 用户所属的组
lyiang : student ftpusers                  # liyang 同时属于 student 和 ftpusers 用户组
```

#### 5. 从指定的组中移除某用户

若要从用户组中移除某用户,其实现命令为:

gpasswd -d 用户账户名 用户组名

比如,若要从 ftpusers 用户组中,移除 liyang 用户,则操作命令为:

```
[root@rh9 root]# gpasswd -d liyang ftpusers
Removing user liyang from group ftpusers
[root@rh9 root]# groups liyang
lyiang : student
# liyang 用户已不再属于 ftpusers 用户组
```

#### 6. 设置用户组管理员

添加用户到组和从组中移除某用户,除了 root 用户可以执行该操作外,用户组管理员也可以执行该操作。本章的命令,只要未特别申明,都只有 root 用户才有权执行这些管理性操作。

要将某用户指派为某个用户组的管理员,可使用以下命令来实现:

```
gpasswd -A 用户账户 要管理的用户组
```

命令功能: 将指定的用户设置为指定用户组的用户管理员。用户管理员只能对授权的用户组进行用户管理(添加用户到组或从组中删除用户),无权对其他用户组进行管理。

比如,若要设置 liyang 为 ftpuser 用户组的用户管理员,则操作命令为:

```
[root@rh9 root]# gpasswd -A liyang ftpusers
```

之后 liyang 用户就可对 ftpusers 用户组进行管理,但无权对 student 用户组进行管理,操作演示如下:

```
[liyang@rh9 liyang]$ gpasswd -a fengyuan ftpusers      # 将 fengyuan 添加到 ftpusers 用户组
Adding user fengyuan to group ftpusers                # 操作成功,说明可以对 ftpusers 用户组进行管理
[liyang@rh9 liyang]$ gpasswd -d fengyuan student
                                                         # 试图将 fengyuan 用户从 student 用户组中移除
Permission denied.                                     # 操作被拒绝,说明无权对其他用户组进行管理
```

另外, Linux 还提供了 id、whoami 和 groups 等命令,用来查看用户和组的状态。id 命令用于显示当前用户的 uid、gid 和所属的用户组的列表;whoami 用于查询当前用户的名称;“groups 用户账户”用于查看指定的用户所隶属的用户组。

### 3.4 使用用户管理器管理用户和组

在 Red Hat Linux 9 的 X-Windows 图形系统中,提供了用户管理器,利用该管理器,可实现用户和用户组的创建与管理。其操作方式与 Windows 系统相同,因此本节仅作简单介绍。

#### 1. 启动用户管理器

依次单击“开始按钮(红帽子)”→System Settings→Users and Groups,即可启动用户管理器,如图 3.2 所示。

在用户管理器窗口显示有 Users 和 Groups 两个选项卡,分别用于显示当前的用户账户和用户组。可单击选项卡的标题栏,进行选项卡的切换。

利用工具栏中的 Add User、Add Group、Properties 和 Delete 按钮,可分别实现添加用户、添加用户组、修改用户账户属性、删除用户或用户组等功能。

#### 2. 添加用户

单击 Add User 按钮,将显示图 3.3 所示的对话框,在对话框中分别输入要添加的用户的相关信息,然后单击 OK 按钮,即可实现用户的添加。

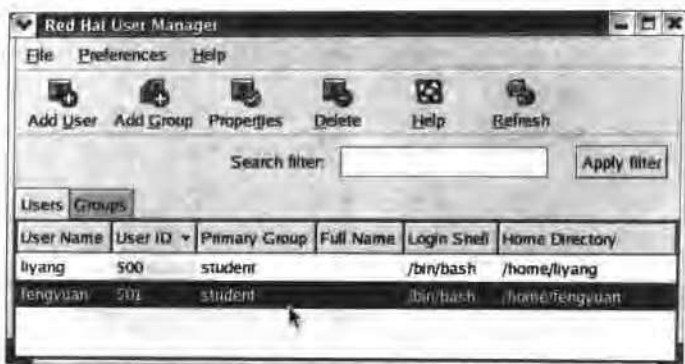


图 3.2 用户管理器

### 3. 添加用户组

单击 Add Group 按钮,将显示图 3.4 所示的对话框,在输入框中输入用户组的名称,最后单击 OK 按钮即可。

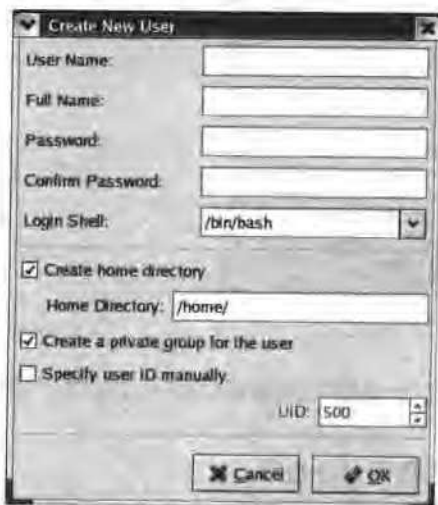


图 3.3 创建新用户

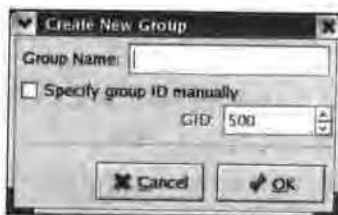


图 3.4 创建用户组

### 4. 修改用户属性

在用户列表中,首先选中要修改属性的用户,然后单击 Properties 工具按钮,此时将打开图 3.5 所示的对话框。在该设置界面中,可对账户的各项属性进行设置和修改。

单击 Account Info 选项卡,切换到账户信息设置对话框,在该对话框中,可设置账户过期的日期以及账户是否加锁。



图 3.5 用户属性设置对话框

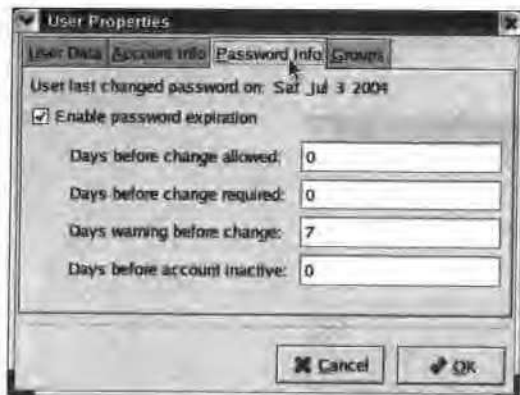


图 3.6 设置账户口令信息

单击 Password Info 选项卡,将显示图 3.6 所示的设置对话框,该对话框用于设置与口令过期相关的信息,其中:

“Enable password expiration”用于设置是否启用口令过期。

“Days before change allowed”用于设置口令有效的最多天数,用户口令过期后,在使用该账号前就必须改变口令,若设置为 0,则口令不过期。

“Days before change required”用于设置用户必须改变口令所间隔的天数。若设置为 0,则口令不会过期。

“Days warning before change”用于设置口令过期前要警告用户的天数。

“Days before account inactive”用于设置口令过期后,账号被锁前不活跃的天数。若设置为 0,账号在口令过期后不被锁定。

单击 Groups 选项卡,切换到图 3.7 所示的对话框,在列表框中,可选择当前用户要加入的用户组。Primary Group 组合框用于选择或输入当前用户的主要用户组(私有用户组)。

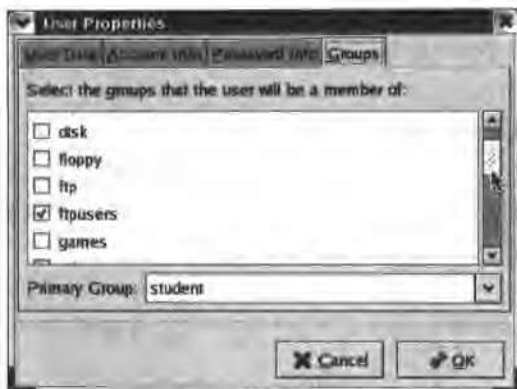


图 3.7 添加用户到用户组

### 5. 删除用户或用户组

首先在用户列表框中选中要删除的用户,然后单击 Delete 工具按钮,此时将弹出对话框,询问是否要删除该用户的主目录,若单击 Yes 按钮,则同时删除当前用户的主目录。

若要删除用户组,单击 Groups 选项卡,切换到用户组列表,选中要删除的用户组,然后单击 Delete 工具按钮即可删除。

若读者对英文界面不习惯,可在 System Settings 菜单下面选择 Language 菜单项,在打开的对话框中,设置图形界面默认使用的语言为简体中文,然后重新启动 Linux 操作系统,之后图形界面就是中文版的了。

## 习题

- 以下文件中,只有 root 用户才有权存取的是( )。
  - passwd
  - shadow
  - group
  - password
- 以下对 Linux 用户账户的描述,正确的是( )。
  - Linux 的用户账户和对应的密码,均是存放在 passwd 文件中的
  - passwd 文件只有系统管理员才有权存取
  - Linux 的用户账户必须设置了密码后,才能登录系统
  - Linux 的用户密码存放在 shadow 文件中,每个用户对它有读的权限

3. 若要创建一个 webadmin 用户,该用户属于 ftpusers 用户组的成员,不允许该用户登录 Linux 系统,以下创建方法中,正确的是( )。

- A. useradd -g ftpusers webadmin
- B. useradd -G ftpuser webadmin
- C. useradd -g ftpusers -s /sbin/nologin webadmin
- D. useradd -G ftpusers -s /bin/nologin webadmin

4. usermod 命令无法实现的操作是( )。

- A. 账户重命名
- B. 删除指定的账户和对应的主目录
- C. 加锁与解锁用户账户
- D. 对用户密码进行加锁或解锁

5. 对用户组进行重命名,应使用的命令参数是( )。

- A. -n
- B. -l
- C. -L
- D. -r

6. 要将用户添加到指定的用户组,应使用( )命令来实现。

- A. groupadd
- B. groupmod
- C. gpasswd
- D. groupuser

7. 以下关于用户组的描述,不正确的是( )。

- A. 要删除一个用户的私有用户组(primary group),必须先删除该用户账户
- B. 可以将用户添加到指定的用户组,也可以将用户从某用户组中移除
- C. 用户组管理员可以进行用户账户的创建、设置或修改账户密码等一切与用户和组相关的操作
- D. 只有 root 用户才有权创建用户和用户组

## 实训 3 用户与用户组管理

**[实训目的]** 掌握用户与用户组的创建与管理。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 利用 more 命令查看用户账户文件的内容,注意观察账户信息在该文件中的存储格式,以及各账户所使用的 shell。另外注意查看 root 账户所使用的 shell 是什么,用户 ID 和用户组 ID 是不是都为 0。

注: /etc/passwd 文件中的很多账户都是系统自动创建的,用户不要随意更改或删除,否则将引起某些服务无法正常启动或工作。在实际操作时,用户尽量只对自己所创建的用户或用户组进行操作。

2. 查看/etc/shadow 文件中的内容,注意观察其存储格式和用于保存密码信息的第 2 个字段的内容。

3. 创建一个名为 vodup 的用户账户,然后使用 grep vodup /etc/passwd 命令查看新

创建的账户在 `passwd` 文件中的存储内容,注意查看该账户对应的主目录。然后使用“`grep vodup /etc/shadow`”命令查看该账户此时在密码文件中存储的内容,第2个字段的内容应为“!!”,说明该账户还未设置密码,被禁用。查看 `/home` 目录,看是否自动创建了一个与用户名相同的目录,该目录即为该用户的主目录,当用户登录系统后,当前目录即为该目录。

使用 `grep vodup /etc/group` 命令查看系统在创建 `vodup` 用户的同时,是否也创建了一个名为 `vodup` 的用户组。若在创建用户时,不创建该用户组,则在创建用户时,应使用什么命令参数?

4. 设置 `vodup` 用户的密码为“`myvod24361#`”,并在 `/etc/shadow` 文件重新查看该账户的密码存储字段的内容。然后按 `Alt+F2` 键切换到第2个虚拟终端,用 `vodup` 账户和密码登录系统,看能否正常登录。登录成功后,注意观察命令行提示符是“`#`”还是“`$`”,以及默认的当前目录是什么。

5. 按 `Alt+F1` 键,重新回到虚拟终端1,对 `vodup` 用户的密码加锁,然后在 `/etc/shadow` 文件中,查看密码加锁后,其存储内容有何变化(其存储的密码前增加了两个“!”)。

按 `Alt+F2` 键再切换回虚拟终端2,使用 `logout` 注销原有的登录,然后再用 `vodup` 账户登录,看此时还能否再登录。

按 `Alt+F1` 键切换回虚拟终端1,对密码解锁,然后对 `vodup` 账户加锁,并查看 `/etc/shadow` 文件中,密码存储内容此时有何变化(存储的密码前增加了一个“!”)。

从中可见,Linux 对账户或密码加锁后,用户账户均无法再登录系统。对账户和密码加锁所使用的命令和参数有所不同,学习中应注意归纳、总结。

6. 创建一个名为 `ftpmanager` 的普通用户组,然后创建一个名为 `webftp` 的用户,并将该用户添加到 `ftpmanager` 用户组中。

将 `vodup` 用户添加到 `ftpmanager` 用户组中,然后用“`groups vodup`”命令查看 `vodup` 所隶属的用户组。

7. 删除 `webftp` 账户并同时删除该账户的主目录。

8. 使用 `startx` 命令切换到 X-Windows 图形界面,然后启动用户管理器,在用户管理器中练习用户组和用户的创建和管理。

## 第 4 章

# Linux 的服务与进程管理

### 4.1 Linux 的启动过程

系统的引导和初始化是操作系统实现控制的第一步,了解 Linux 系统的启动和初始化过程,对于进一步理解和掌握 Linux 是十分有益的。Linux 系统的初始化包含内核部分和 init 程序两部分,内核部分主要完成对系统硬件的检测和初始化工作,init 程序部分则主要完成对系统的各项配置。

#### 4.1.1 Linux 启动过程概述

Linux 的启动大体经历以下五个阶段:

① 主机加电并进行硬件自检后,读取并加载硬盘 MBR 中的启动引导器(GRUB 或 LILO),供用户选择要启动的操作系统。

② 用户选择启动 Linux 操作系统后,启动引导器从/boot 分区读取并加载 Linux 内核程序(vmlinuz-2.4.20-8 和 initrd-2.4.20-8.img),然后由内核程序负责初始化系统硬件和设备驱动程序。

③ 之后内核将启动执行 init 程序,以启动系统的 init 进程。该进程是 Linux 系统中运行的第一个进程,其进程号(PID)始终为 1,该进程将根据/etc/inittab 配置文件的要求执行相应的启动程序,以引导运行系统所需的其他进程,并进入指定的系统运行级别。init 进程是其他进程的父进程。

④ 在不同的运行级别,根据系统的设置启动相应的服务程序(不同的运行级别,启动的服务程序有所不同)。

⑤ 在启动过程的最后,运行 Shell 程序,并显示登录信息。

#### 4.1.2 inittab 配置文件

init 程序位于/sbin 目录中,它负责在系统启动时运行一系列程序和脚本文件。init 程序一旦被内核调用后,便成为系统的第1号进程,它将根据/etc/inittab配置文件的要求



求执行相应的启动程序,并进入指定的系统运行级别。

### 1. inittab 配置文件的内容

inittab 配置文件的内容如下,其中的“#”为注释说明符,“//”后面的内容为便于读者理解而加的说明文字。

```
# Default runlevel. The runlevels used by RHS are: //默认的运行级,RHS 用到的级别如下:
# 0 - halt (Do NOT set initdefault to this) //停机(不要把 initdefault 设置为 0)
# 1 - Single user mode //单用户模式,仅用于 root 用户对系统进行维护
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
//多用户,但不支持 NFS
# 3 - Full multiuser mode //完全多用户模式,即多用户文本界面模式,是标准的运行级
# 4 - unused //未使用,保留
# 5 - X11 //X-Windows,即多用户图形界面
# 6 - reboot (Do NOT set initdefault to this) //重新启动系统
#
id:3:initdefault; //定义默认进入的运行级别,此处为 3

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit //调用/etc/rc.d/rc.sysinit 脚本文件实现对系统的初始化
l0:0:wait:/etc/rc.d/rc 0 //在运行级别 0,将调用执行的脚本
l1:1:wait:/etc/rc.d/rc 1 //在运行级别 1,将调用执行的脚本
l2:2:wait:/etc/rc.d/rc 2 //在运行级别 2,将调用执行的脚本
l3:3:wait:/etc/rc.d/rc 3 //在运行级别 3,将调用执行的脚本
l4:4:wait:/etc/rc.d/rc 4 //在运行级别 4,将调用执行的脚本
l5:5:wait:/etc/rc.d/rc 5 //在运行级别 5,将调用执行的脚本
l6:6:wait:/etc/rc.d/rc 6 //在运行级别 6,将调用执行的脚本

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now //定义按 Ctrl+Alt+Del 键时要执行的命令

# When our UPS tells us power has failed, assume we have a few minutes
# of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
//UPS 断电时的动作

# If power was restored before the shutdown kicked in, cancel it.
```

```
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

//UPS 供电恢复时的动作

```
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1           //在 2345 级别,均要启动虚拟控制台 1(tty1)
2:2345:respawn:/sbin/mingetty tty2           //在 2345 级别,均要启动虚拟控制台 2(tty2)
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6           //在 2345 级别,均要启动虚拟控制台 6(tty6)

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/xdm -nodaemon           //在运行级别 5 时,启动 X-Windows
```

## 2. inittab 配置文件解析

inittab 是 init 进程的配置文件,用于指定系统启动时和正常运行时将要运行哪些进程。其中的每一配置命令行都由四个字段(域)构成,各字段间用冒号分隔,共同确定某进程在哪些运行级别以何种方式运行。配置命令行的格式如下:

```
id:runlevels:action:command
```

### (1) id

id 字段用于惟一标识一条配置命令,可以由 1~4 个字符组成。

### (2) runlevels

runlevels 字段用于指定该配置命令在哪些运行级别中运行。运行级别是操作系统当前正在运行的功能级别,Linux 的运行级别有 7 级,分别用 0~6 的数字代表,各级别的功能含义参见 inittab 配置文件前面部分的注解说明。

runlevels 字段可以是某一个运行级别,也可以是多个运行级别的一个列表。比如,以下配置命令表示在 2、3、4、5 运行级别中,都要运行该配置命令(/sbin/mingetty tty1)。

```
1:2345:respawn:/sbin/mingetty tty1
```

在 inittab 配置文件中,有 6 条这样的配置命令,从而实现启动 tty1~tty6 这 6 个虚拟文本控制台(终端)。Linux 最多支持 23 个虚拟终端,可根据需要在配置文件中添加,但要注意不要定义第 7 个虚拟终端,X-Windows 系统使用该虚拟终端,配置文件修改好后,使用命令“telinit q”让新添加的虚拟终端生效,以后就可使用左 Alt+Fn 键在 1~6 和 8~12 间切换,使用右 Alt+Fn 键在 13~24 之间进行切换。

在 Linux 正常运行时,也可通过手工执行“init 运行级别”命令,来进入相应的级别。

比如,执行 `init 6` 命令,将进入运行级别 6,从而实现 Linux 系统的重新启动。

运行 `runlevel` 命令,可查看当前运行的级别,该命令将显示上一次的运行级别和当前的运行级别。

### (3) action

该字段用于描述执行哪种类型的动作。该字段的常见取值及功能如下:

#### ① initdefault

用于指定系统启动后默认进入哪个运行级别,此时 `command` 字段被忽略。应用示例:

```
id:3:initdefault:           //定义默认进入运行级别 3
```

若 `inittab` 配置文件中,无该配置命令,init 进程会在控制台询问要进入的运行级别。

#### ② sysinit

`sysinit` 类型的配置命令用于实现对系统的初始化,此时 `runlevels` 字段将被忽略。应用示例:

```
si::sysinit:/etc/rc.d/rc.sysinit
```

`/etc/rc.d/rc.sysinit` 脚本文件用于实现对系统进行初始化,如激活交换分区、检查并挂载文件系统、装载部分模块等。

#### ③ wait

`wait` 类型的配置命令将在进入指定的运行级别后运行一次,init 进程将等待其结束。应用示例:

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
:
l6:6:wait:/etc/rc.d/rc 6
```

该组配置命令分别定义了 0~6 的运行级别上,将要调用执行的脚本文件。若当前运行级别为 N,则在该运行级别将调用执行 `/etc/rc.d/rcN.d` 目录下的脚本程序。在 `/etc/rc.d` 目录下,有 `rc0.d`、`rc1.d`、`...`、`rc6.d` 这样 7 个目录,每个目录下均有类似 `Knnxxxx` 和 `Snnxxxx` 的文件,`nn` 是 00~99 之间的一个整数,用于确定同类脚本的执行顺序,当系统进入某运行级别时,将按照序号从小到大的顺序执行脚本以启动该服务。`xxxx` 代表系统提供的某种服务。以 S 开头的文件用于启动(start)服务进程,以 K 开头的文件用于终止(kill)服务进程,当离开某运行级别时,该运行级别对应目录下的以 K 开头的文件将依次被执行,以结束该服务进程。

#### ④ ctrlaltdel

用于指定当用户按了 `Ctrl+Alt+Del` 键时,系统所要进行动作。应用示例:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

以上配置命令定义了当用户按 Ctrl+Alt+Del 键时,系统的动作是重新启动系统。

对于 Windows 2000 Server,通常采用按 Ctrl+Alt+Del 键来实现对系统加锁,对于 Linux 管理员,为防止误操作,通常需要将 Ctrl+Alt+Del 键失效,为此可在该配置命令前加“#”,将其注释掉。

#### ⑤ powerfail 和 powerokwait

powerfail 用于指定当 UPS 发来断电信号时,系统所要运行的命令;powerokwait 用于指定当 UPS 供电恢复时所要运行的命令。应用示例:

```
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

#### ⑥ respawn

该类配置命令在结束后会重新启动运行。在 inittab 配置文件中,在 2、3、4、5 运行级别都会启动 6 个虚拟控制台,当用户在虚拟控制台中注销后,系统会重新运行 mingetty,以等待新的登录。该类配置命令如下:

```
1:2345:respawn:/sbin/mingetty tty1
```

#### (4) command

用于指定启动该进程所要执行的命令。

## 4.2 Linux 的服务管理

Linux 的服务分为独立运行的服务和受 xinetd 服务管理的两类。xinetd 本身也是一个独立运行的服务,它负责管理系统中不频繁使用的服务,当这些服务被请求时,由 xinetd 服务负责启动运行,完成服务请求后,再结束该服务的运行,以减少对系统资源的占用。

### 4.2.1 服务的启动脚本

在 Linux 中,每个服务都会有相应的服务器启动脚本,该脚本可用于实现启动服务、重启服务、停止服务和查询服务等功能。在服务器启动脚本中,一般还有对该脚本功能的简要说明和使用方法,可利用 head 命令来查看。

所有的服务器启动脚本都放在 /etc/rc.d/init.d 目录中,脚本名称与服务名称相对应。该目录中有哪些脚本与当前系统中所安装的服务有关。

/etc/rc.d/rc.local 文件相当于 DOS 系统的 autoexec.bat 文件的功能,放入该文件中的脚本或命令,在其他初始化脚本执行完后,将自动被执行。

```
[root@rh9 root]# ls /etc/rc.d
init.d    rc0.d    rc2.d    rc4.d    rc6.d    rc.sysinit
rc        rc1.d    rc3.d    rc5.d    rc.local

[root@rh9 root]# ls /etc/rc.d/init.d
aep1000    firstboot    kderotate    nfslock    rhnsd    sshd    yppasswdd
anacron    functions    keytable    nsd        saslauthd    syslog    ypserv
apmd       gpm          killall      ntpd       sendmail  tux      ypxfrd
atd        halt         kudzu        pcmcia     single    vsftpd
autofs     httpd        named        portmap    smb       winbind
bcm5820    iptables     netfs        pxe        snmpd     xfs
crond      irda         network      random     snmptrapd  xinetd
cups       isdn         nfs          rawdevices  squid     ypbind
```

系统的各运行级别有独立的脚本目录,其目录名分别为 rc0.d~rc6.d,当系统启动或进入某运行级别时,对应脚本目录中用于启动服务的脚本将自动被运行,当离开该级别时,用于停止服务的脚本也将自动运行,以结束在该级别中运行的这些服务。

各运行级别对应的脚本目录下的脚本,都是指向服务器脚本目录(/etc/rc.d/init.d)下面某个服务启动脚本的符号链接。比如,在 rc0.d 和 rc6.d 目录中的 s00killall 脚本,其实质就是指向/etc/rc.d/init.d/killall 服务脚本的一个符号链接,它用于停止所有系统进程。

#### 4.2.2 服务的启动与停止

Linux 的服务在系统启动或进入某运行级别时会自动启动或停止,另外在系统运行过程中,也可使用相应的命令来实现对某服务的启动、停止或重启服务。

##### 1. 通过服务启动脚本来管理服务

在 Linux 中,启动、停止或重启服务可通过执行相应的服务启动脚本来实现。若直接执行相应的服务启动脚本,系统将显示用法帮助,其用法为:

```
# /etc/rc.d/init.d/服务启动脚本名 {start|stop|status|restart|condrestart|reload}
```

服务启动脚本名后面的启动参数若为 start,则启动该服务;若为 stop,则停止该服务;若为 restart,则为重启该服务;若为 status,则为查询该服务的启动状态。

比如,若要查询 xinetd 服务的启动状态,则执行命令:

```
[root@rh9 root]# /etc/rc.d/init.d/xinetd status
xinetd (pid 1694) is running...
```

说明该服务已经启动,其进程号为 1694。若要重启该服务,则执行命令:

```
[root@rh9 root]# /etc/rc.d/init.d/xinetd restart
```

Stopping xinetd: [OK]

Starting xinetd: [OK]

若要停止该服务,则执行命令:

```
[root@rh9 root]# /etc/rc.d/init.d/xinetd stop
```

Stopping xinetd: [OK]

若要启动该服务,则执行命令:

```
[root@rh9 root]# /etc/rc.d/init.d/xinetd start
```

Starting xinetd: [OK]

## 2. 使用 service 命令管理服务

利用服务启动脚本来启动或停止服务时,每次都要输入脚本的全路径,使用起来比较麻烦,为此,Red Hat Linux 专门提供了 service 命令来解决该问题,使用时只需要指定要启动或停止的服务名即可,其用法为:

service 服务名称 要执行的动作(start|stop|restart)

用户在任何路径下均可通过该命令来实现启动或停止服务,service 命令会自动到/etc/rc.d/init.d 目录中查找并执行相应的服务启动脚本。

比如,若要重启 xinetd 服务,实现命令为 service xinetd restart。

若要停止 xinetd 服务,实现命令为 service xinetd stop。

xinetd 服务的配置文件为/etc/xinetd.conf,该配置文件中的“includedir /etc/xinetd.d”用于设置 xinetd 服务管理的服务的启动配置文件所在的目录为/etc/xinetd.d。在/etc/xinetd.d 目录中,xinetd 管理的每个服务都有独立的配置文件,配置文件对 xinetd 服务将如何启动该服务进行了设置。配置文件的名称与服务名相同。

### 4.2.3 配置服务的启动状态

在对 Linux 系统的管理中,经常需要设置或调整某些服务在某运行级别中自动启动或不启动,这可通过配置服务的启动状态来实现,为此 Linux 提供了 ntsysv 和 chkconfig 命令来实现该功能。

#### 1. ntsysv 命令

ntsysv 命令是一个基于文本字符界面的实用程序,操作简单、直观,但只能设置当前运行级别下各服务的启动状态。若要设置其他运行级别下各服务的启动状态,则需要转换到相应的运行级别,然后再运行 ntsysv 命令来进行设置。

在命令行状态下键入并执行 ntsysv 命令,此时将出现如图 4.1 所示的设置界面,在服务列表框中,可利用向上或向下的光标键或 PageUp 键或 PageDown 键,来实现向上或

向下滚动显示服务列表。将光亮条移动到要设置的服务列表上,按空格键,可设置为自动启动,此时被选中的方括号中会显示一个“\*”。若要取消自动启动,则再按一次空格键,此时方括号中的“\*”将消失,表示不设置为自动启动。设置完毕,按 Tab 键将光亮条移动到 OK 按钮,然后按回车键退出。



图 4.1 设置服务启动状态

## 2. chkconfig 命令

chkconfig 命令可以设置系统中所有服务在各运行级别中的启动状态。下面根据该命令功能的不同,分别介绍其用法。

### (1) 查看服务的启动状态

命令用法: `chkconfig -list [服务名称]`

chkconfig 命令带 `-list` 参数,用于查看服务的启动状态。若缺省服务名称参数,则显示所有服务的启动状态;若指定了要查看的服务,则只显示该服务的启动状态。

比如,若要查看当前系统中各服务的启动状态,则执行命令:

```
[root@rh9 root]# chkconfig -list
kudzu      0:off    1:off    2:off    3:on     4:on     5:on     6:off
syslog     0:off    1:off    2:on     3:on     4:on     5:on     6:off
netfs      0:off    1:off    2:off    3:on     4:on     5:on     6:off
network    0:off    1:off    2:on     3:on     4:on     5:on     6:off
:
vsftpd     0:off    1:off    2:off    3:off    4:off    5:off    6:off
xinetd based services:
  chargen-udp:  off
```

```
rsync:          off
:
cups-lpd:       off
sgi_fam:        on
```

若要单独查看 vsftpd 服务的启动状态,则实现命令为 `chkconfig --list vsftpd`。

各服务的启动状态改变后,在系统下一次启动时才会生效。

## (2) 设置独立运行的服务的启动状态

命令用法: `chkconfig --level <运行级别列表> <服务名称> <on|off|reset>`

命令功能: 设置指定服务在指定运行级别中的启动状态。参数 on 代表设置为启动, off 为不启动, reset 代表恢复为系统的默认启动状态。

例如,若要设置 vsftpd 服务在 2、3、5 运行级别启动,则实现命令为:

```
[root@rh9 root]# chkconfig --level 235 vsftpd on
[root@rh9 root]# chkconfig --list vsftpd
vsftpd      0:off    1:off    2:on     3:on     4:off    5:on     6:off
```

## (3) 设置非独立运行的服务的启动状态

命令用法: `chkconfig <服务名称> <on|off|reset>`

非独立运行的服务受 xinetd 服务的管理,因此不存在运行级别启动状态的问题。非独立运行的服务的启动状态改变后,需要重新启动 xinetd 服务,才能使设置立即生效。

比如,若要设置 rsync 服务的自启动状态为 on,并让其立即生效启动,则实现命令为:

```
[root@rh9 root]# chkconfig --list rsync
rsync              off
[root@rh9 root]# chkconfig rsync on
[root@rh9 root]# chkconfig --list rsync
rsync              on
[root@rh9 root]# service xinetd restart
```

## 4.3 Linux 的进程管理

### 4.3.1 进程与作业

#### 1. 进程的概念

Linux 是一个多用户、多任务的操作系统,在同一时间允许有许多用户向操作系统发出各种操作命令。当运行一个命令时,系统至少会建立一个进程来运行该命令,通常将一个开始执行但是还没有结束的程序的实例称为进程。程序是一种包含可执行代码的文件。



进程由程序产生,是一个运行着的、要占用系统运行资源的程序,但进程并不等于程序,进程是动态的,而程序是静态的文件,多个进程可以并发调用同一个程序,一个程序可以启动多个进程。每一个进程还可以有许多子进程,依次循环下去,从而产生子孙进程。当程序被系统调用到内存以后,系统会给程序分配一定的资源(如内存、设备等),然后进行一系列的复杂操作,使程序变成进程以供系统调用。

为了充分利用系统资源,系统对进程区分了不同的状态,将进程分为新建、运行、阻塞、就绪和完成五个状态。新建表示进程正在被创建,运行表示进程正在运行,阻塞表示进程正在等待某一事件发生,就绪是表示系统正在等待 CPU 来执行命令,而完成则表示进程已经结束,系统正在回收资源。

进程在运行期间,会用到很多资源,如内存资源和 CPU 资源,当某一个进程占用 CPU 资源时,别的进程必须等待正在运行的进程空闲 CPU 后才能运行,通常会存在很多进程在等待,内核通过调度算法来决定将 CPU 分配给哪个进程。

系统在刚刚启动时,运行于内核方式,此时只有一个初始化进程在运行,该进程首先做系统的初始化,然后执行初始化程序(一般是/sbin/init)。初始化进程是系统的第一个进程,以后的所有进程都是初始化进程的子进程。在 Shell 下执行程序启动的进程就是 Shell 进程的子进程,一般情况下,只有子进程结束后,才能继续父进程,若是从后台启动的,则不用等待子进程结束。

为了区分不同的进程,系统给每一个进程都分配了一个惟一的进程标识符(进程号)。Linux 是一个多进程的操作系统,每一个进程都是独立的,都有自己的权限及任务,当某一进程失败时不会导致别的进程失败。

Linux 系统的进程大体可分为交互进程、批处理进程和监控进程(守护进程)三种。交互进程是在 Shell 下通过执行程序所产生的进程,可在前台运行,也可在后台运行;批处理进程是一个进程序列;监控进程通常也称为守护进程,它是 Linux 系统启动时就自动启动产生的进程,并在后台运行。

## 2. 作业的概念

正在执行的一个或多个相关进程称为一个作业,即一个作业可以包含一个或多个进程,比如,在执行使用了管道和重定向操作的命令时,该作业就包含了多个进程。使用作业控制,可以同时运行多个作业,并在需要时在作业之间进行切换。

作业控制指的是控制正在运行的进程的行为。比如,用户可以挂起一个进程,等一会儿再继续执行该进程。Shell 将记录所有启动的进程情况,在每个进程过程中,用户可以任意地挂起进程或重新启动进程。作业控制是许多 Shell(包括 bash 和 tcsh)的一个特性,使用户能在多个独立作业间进行切换。

### 4.3.2 进程的启动

在键入需要运行的程序名来执行一个程序时,此时也就启动了一个进程。每个进程

都有一个进程号,用于系统识别和调度该进程。启动进程有两个主要途径,即手工启动和调度启动。

### 1. 手工启动

由用户在 Shell 命令行下输入要执行的程序来启动一个进程,即为手工启动进程。其启动方式又分为前台启动和后台启动,默认为前台启动。若要在要执行的命令后面跟随一个“&”,则为后台启动,此时进程在后台运行,Shell 可继续运行和处理其他程序。

### 2. 调度启动

调度启动是事先设置好在某个时间要运行的程序,当到了预设的时间后,由系统自动启动。在对 Linux 系统进行维护和管理的过程中,有时需要进行一些比较费时而且占用资源较多的操作,为了不影响正常的服务,通常将其安排在深夜由系统自动运行。此时就可以采用调度启动要运行的程序,并事先设置好任务运行的时间,到时系统就会自动完成指定的操作。

在指定的时间运行指定的程序,可使用 at 或 crontab 命令来实现。

#### (1) at 命令

命令用法: at [-f 文件名] [-m] 时间

该命令至少需要指定一条要执行的命令、一个计划执行时间才能正常运行。

参数说明:

-f 文件名 用于指定计划执行的命令序列存放在哪一个文件中。若缺省该参数,执行 at 命令后,将出现“at>”提示符,此时用户可在该提示符下,输入所要执行的命令,输入完每一行命令后按回车,所有命令序列输入完毕后,按 Ctrl+Z 键结束 at 命令的输入。

-m 作业结束后发送邮件给执行 at 命令的用户。

时间参数用于指定任务执行的时间,可包含日期信息,其表达方式可采用绝对时间表达法,也可采用相对时间表达法。

#### ① 绝对时间表达

绝对时间表达分为“hh:mm”和“hh:mm 日期”两种形式。其中时间一般采用 24 小时制,也可采用 12 小时制,然后再加上 am(上午)或 pm(下午)来说明是上午还是下午;日期的格式可表达为“month day”、“mm/dd/yy”和“dd. mm. yy”三种形式,但应注意日期必须放在时间之后。另外还可用 today 代表今天的日期,tomorrow 代表明天的日期。

比如若要表达 2004-8-1 下午 1:30,则表达形式可以是:

1:30pm 8/1/04

13:30 1.8.04

13:30 August 1

## ② 相对时间表达

相对时间表达法适合于安排后不久就要执行的情况,该表达法以当前时间 now 为基准,然后递增若干个时间单位,其时间单位可以是 minutes(分钟)、hours(小时)、days(天)、weeks(星期),表达格式为“now + num 时间单位”。

比如若要表达 5 小时后,则表达方法为 now + 5 hours。

假设要计划执行的命令都事先写入了/tmp/myjob 文件中,现要求在今天晚上 11:30 执行,则实现命令为:

```
[root@rh9 root]# at -f /tmp/myjob 23:30 today
```

在任何情况下,root 用户均可以执行该命令,对于其他用户是否有权执行该命令,取决于/etc/at.allow 和/etc/at.deny 两个配置文件。如果/etc/at.allow 文件存在,则只有在该文件中列表的用户才有权执行 at 命令;如果该文件不存在,则检查/etc/at.deny 文件是否存在,在该文件中列表的用户均不能执行 at 命令;若这两个文件均不存在,则只有 root 用户可以执行。Linux 默认一个空的/etc/at.deny 配置文件,即所有用户均可以执行 at 命令。

## (2) crontab 命令

crontab 计划调度服务可在指定的日期和时间执行预定的命令,其计划任务的表达方式为:

minute hour day month day of the week command

前面 5 个域用空格分隔,分别表示执行后面 command 命令的分钟数(0~59)、小时数(0~23)、天数(0~31)、月份(0~12)和星期数(0~7,0 或 7 代表星期天)。每个域均可用“\*”代表任意的值,可用“~”来表达一个范围,用逗号分隔来表达一个值的列表。

例如,若要在每天晚上的 23 点,自动检查并升级 Clam 杀毒软件的病毒库,则设置方法为:

```
[root@rh9 bin]# crontab -c
```

执行该命令后,将调用 vi 编辑器供用户输入计划要执行的任务。

```
* 23 * * * /usr/local/bin/freshclam --quiet -l /var/log/update_clam.log
```

输入完后,存盘退出 vi 即可。

## 4.3.3 管理系统的进程

### 1. 查看系统的进程

Linux 系统中每个运行着的程序都是系统中的一个进程,要查看系统当前的进程,可使用 ps 命令来实现。其用法为“ps 命令选项”。

该命令的命令选项很多,可执行 `ps -help` 命令来查看,其参数有的要加“-”,有的不加。此处仅介绍几个常用的参数。

若缺省参数,直接执行 `ps` 命令,则仅显示当前控制台的进程,如:

```
[root@rh9 root] # ps
PID  TTY          TIME     CMD
1874  tty1          00:00:01 bash
2050  tty1          00:00:00 ps
```

`u` 参数表示输出进程用户所属的信息。带上 `u` 参数后,将显示更详细的信息。例如:

```
[root@rh9 root] # ps u
USER  PID  %CPU %MEM VSZ  RSS  TTY  START  START  TIME  COMMAND
root  1874  0.0   1.0  5204 1424  tty1  S      17:42   0:01  -bash
root  2053  0.0   0.4  2596  644  tty1  R      19:00   0:00  ps u
```

参数 `a` 表示显示系统中所有用户的进程;参数 `x` 用于显示没有控制台的进程及后台进程。参数 `a` 与 `x` 同时使用,可用于显示系统中的所有进程,另外要显示系统中的所有进程,也可直接使用 `-e` 参数来实现。通常情况下,系统中运行的进程很多,可使用管道操作符和 `less` 命令来查看,其实现命令为 `ps -e u|less` 或 `ps aux|less`。

主机运行的服务越多,被攻击者入侵的可能性就会加大,作为管理员应经常查看系统运行的进程和服务,对于异常的和不要的进程和服务,应及时将其结束,并通过修改系统的自启动服务,来关闭不需要的自启动服务。作为服务器,应坚持服务够用的原则,所提供的服务越少越好,不要安装和开启一些与所提供服务无关的服务。

另外,若要查看各进程的继承关系,可使用 `ps tree` 命令或 `ps tree|less` 或 `ps tree -pu|less` 命令来实现,该命令以树状结构方式列出系统中正在运行的各进程之间的继承关系。

## 2. 结束进程的运行

在 Linux 系统的运行过程中,有时某个进程由于异常情况,对系统停止了反应,此时就需要停止该进程的运行。另外,当发现一些不安全的异常进程时,也需要强行终止该进程的运行,为此,Linux 提供了 `kill` 和 `killall` 命令来结束进程的运行。

### (1) kill 命令

该命令使用进程号来结束指定进程的运行。可使用 `ps` 命令获得该进程的进程号,然后再使用 `kill` 命令将该进程“杀死”,其用法为“`kill [-9] 进程号`”。

`kill` 命令向指定的进程发送终止运行的信号,进程在收到信号后,会自动结束本进程,并处理好结束前的相关事务,属于安全结束进程,不会导致 Linux 系统的崩溃或不稳定。

参数 `-9` 用于强行结束指定进程的运行,适合于结束已经“死掉”而没有能力自动结

束的进程。带上该参数后,该命令属于非正常结束进程。

为了查看指定进程的进程号,可使用管道操作和 `grep` 命令相结合的方式来实现,比如,若要查看 `xinetd` 进程对应的进程号,则实现命令为:

```
[root@rh9 root]# ps -e|grep xinetd
1665 ?    00:00:00 xinetd
```

从其输出信息中,可知该进程的进程号为 1665,若要结束该进程,则执行命令:

```
[root@rh9 root]# kill 1665
```

## (2) killall 命令

该命令使用进程名来结束指定进程的运行。若系统存在同名的多个进程,则这些进程将全部结束运行,其用法为“`killall [-9] 进程名`”。

参数 `-9` 用于强行结束指定进程的运行,属于非正常结束。

例如,若要结束 `xinetd` 进程的运行,则实现命令为 `killall xinetd`。

## 习题

- Linux 用于启动系统所需加载的内核程序位于( )。
  - /
  - /lib/modules/2.4.20-8/kernel
  - /boot
  - /proc
- `init` 进程对应的配置文件名为( ),该进程是 Linux 系统的第一个进程,其进程号 PID 始终为 1。
  - /etc/fstab
  - /etc/init.conf
  - /etc/inittab.conf
  - /etc/inittab
- 在 Linux 运行的 7 个级别中,具有全部功能的多用户文本模式,其运行级别为( ),X-Windows 图形系统的运行级别为( )。
  - 2
  - 3
  - 5
  - 6
- 当前为多用户文本模式,要切换到 X-Windows 图形系统,能实现的命令有( )。
  - `init 5`
  - `startx`
  - `init 6`
  - `init 3`
- 在 Linux 的 `inittab` 配置文件中,用于定义系统启动时默认进入的运行级别的配置命令是( );用于启动时实现对系统初始化的配置命令是( );用于定义按 `Ctrl+Alt+Del` 键时系统所执行的操作的配置命令是( )。Linux 支持多达 23 个虚拟终端(vt),在 `inittab` 配置文件中,默认定义了 6 个,若要定义下一个可使用的虚拟终端,则实现的配置命令应为( )。
  - `ca::ctrlaltdel:/sbin/sbutdown -t3 -r now`

- B. id;3:initdefault:
  - C. si::sysinit:/etc/rc.d/rc.sysinit
  - D. 7:2345:respawn:/sbin/mingetty tty7
  - E. 8:2345:respawn:/sbin/mingetty tty8
6. 若要重新启动 Linux 操作系统,以下操作命令中,不正确的是( )。
- A. reboot      B. restart      C. init 6      D. shutdown -r now
7. Linux 所有服务的启动脚本均存放在( )目录中。
- A. /etc/rc.d/init.d      B. /etc/rc.d
- C. /etc/rc.d/rc      D. /etc/rc.d
8. 若要重新启动 network 服务,则以下启动命令中,正确的有( )。
- A. /etc/rc.d/init.d/network start
- B. /etc/rc.d/init.d/network-server restart
- C. /etc/rc.d/init.d/network restart
- D. service network restart
9. 若要取消 sendmail 服务在第 2、3、4、5 运行级别的自启动,则实现的操作命令为( )。
- A. ntsysv      B. chkconfig sendmail off
- C. chkconfig --level 2345 off      D. chkconfig --level 2345 sendmail off
10. telnet 服务不是一个独立运行的服务,现要求在 Linux 系统启动时,能自动启动该服务,则实现的操作命令为( )。
- A. 执行 ntsysv 命令,在服务列表中,选中 telnet 服务,下次系统启动时,就可自动启动了
- B. chkconfig --level 2345 telnet on
- C. chkconfig telnet on
- D. service xinetd start
11. 若要使用进程名来结束进程,应使用( )命令,以树形结构显示进程间的继承关系,可使用命令( )。
- A. kill      B. killall      C. ps      D. pstree

## 实训 4 服务与进程管理

【实训目的】 了解 Linux 的启动过程,掌握 init 进程的配置文件的功能和修改方法,掌握 Linux 服务的启动与停止方法以及设置服务的自启动方法,掌握进程的查看与结束进程的方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 利用 vi 编辑器修改 `/etc/inittab` 配置文件, 将 “`id:3:initdefault:`” 更改为 “`id:5:initdefault:`”, 然后重新启动 Linux 操作系统, 观察有何变化。

2. 在 Linux 的图形界面系统中, 选择红帽子开始菜单 → System Tools → Terminal, 打开终端窗口, 在终端窗口的命令行中, 利用 vi 编辑器修改 `/etc/inittab` 配置文件, 将 “`id:5:initdefault:`” 再次改为 “`id:3:initdefault:`”, 并在 “`ca::ctrlaltdel:/sbin/shutdown -t3 -r now`” 配置命令前添加一个 “#”, 将该语句注释掉, 在 “`6:2345:respawn:/sbin/mingetty tty6`” 配置命令后再添加一行配置命令:

```
8:2345:respawn:/sbin/mingetty tty8
```

保存内容, 退出 vi, 然后键入 `exit` 命令关闭终端窗口。最后按 `Ctrl+Alt+Del` 键, 然后在弹出的关闭对话框中, 选择重新启动, 并同时选中 “Save Current Setup”, 观察重启后, 系统是否再次回到文本登录方式, 此时再按 `Ctrl+Alt+Del` 键, Linux 系统是否会被重启。按左边的 `Alt+F8` 键, 观察是否会出现虚拟终端, 若按 `Alt+F8` 键后, 出现文本登录画面, 则说明该虚拟终端添加成功, 登录后即可进入 Linux 系统。

3. 使用 `ls /etc/rc.d/init.d` 命令, 查看当前系统有哪些服务启动脚本。

使用 `/etc/rc.d/init.d/vsftpd status` 命令查看 `vsftpd` 服务的启动状态。若没有启动, 则使用 `/etc/rc.d/init.d/vsftpd start` 命令启动, 然后再次查询该服务的启动状态; 若已启动, 使用 `/etc/rc.d/init.d/vsftpd restart` 命令重启该服务, 观察重启过程。

使用 `/etc/rc.d/init.d/vsftpd stop` 命令停止该服务, 并查询是否停止成功。最后用 `service vsftpd start` 命令启动该服务, 观察启动效果是否与直接使用服务启动脚本相同。

4. 使用 `chkconfig --list|less` 命令浏览了解各服务在不同运行级别的启动状态, 并查看有哪些服务是受 `xinetd` 服务监控的。

用 `chkconfig` 命令修改 `vsftpd` 服务在 2、3、5 运行级别时自动启动。重启 Linux 系统, 然后使用 `/etc/rc.d/init.d/vsftpd status` 命令查询, 看该服务是否自启动成功。

5. 使用 `ps -e|less` 或 `ps aux|less` 浏览查看当前系统的所有进程, 然后使用 `ps -e|grep vsftpd` 命令在所有进程中搜索 `vsftpd` 服务对应的进程, 并记下其进程号, 然后使用 `kill` 命令结束该进程, 最后再用 `/etc/rc.d/init.d/vsftpd status` 命令查询该服务是否已结束。

重新启动 `vsftpd` 服务, 然后再使用 `killall vsftpd` 命令来结束该进程, 然后再查询 `vsftpd` 服务的启动状态, 观察使用 `kill` 和 `killall` 来结束进程的效果是否相同。

# 第 5 章

## 软件包管理

在对系统的使用和维护过程中,安装和卸载软件是必须掌握的操作。Red Hat Linux 为便于软件包的安装、更新或卸载,提供了 RPM 软件包管理器,本章将详细介绍 rpm 命令和 Linux/UNIX 系统中标准的 TAR 包管理命令。

### 5.1 RPM 软件包管理

#### 5.1.1 RPM 简介

RPM(Redhat package manager)是由 Red Hat 公司提出的一种软件包管理标准,可用于软件包的安装、查询、更新升级、校验、卸载已安装的软件包,以及生成 rpm 格式的软件包等,其功能均是通过 rpm 命令结合使用不同的命令参数来实现的。由于功能十分强大,RPM 已成为目前 Linux 各发行版本中应用最广泛的软件包格式之一。

RPM 软件包的名称具有特定的格式,其格式为:

软件名称-版本号(包括主版本和次版本号). 软件运行的硬件平台.rpm

比如,Telnet 服务器程序的软件包名称为 telnet-server-0.17-25.i386.rpm,其中的 telnet-server 为软件的名称,0.17-25 为软件版本号,i386 是软件运行的硬件平台,最后的 rpm 是文件的扩展名,代表文件是 rpm 类型的软件包。

RPM 软件包中的文件以压缩格式存储,并拥有一个定制的二进制头文件,其中包含有关于本软件包和内容的相关信息,便于对软件包信息进行查询。

#### 5.1.2 使用 rpm 命令

Red Hat Linux 使用 rpm 命令实现对 RPM 软件包进行维护和管理,由于 rpm 命令功能十分强大,因此,rpm 命令的参数选项也特别多,通过在 Shell 命令行中键入 rpm 命令,可查看其用法提示,其中详细列出了该命令的全部参数选项,本节将按其功能用途,介



绍最常用的几个参数选项。当命令中同时选用多个参数时,这些参数可合并在一起表达。

### 1. 查询 RPM 软件包

查询 RPM 软件包使用 -q 参数,要进一步查询软件包中的其他方面的信息,可结合使用一些相关的参数。

#### (1) 查询系统中已安装的全部 RPM 软件包

若要查看系统中已安装了哪些 RPM 软件包,可使用 rpm -qa 命令来实现,其中 a 参数代表全部(all)。一般系统安装的软件包较多,为便于分屏浏览,可结合管道操作符和 less 命令来实现,其命令用法为:

```
[root@rh9 root]# rpm -qa | less
```

若要查询包含某关键字的软件包是否已安装,可结合管道操作符和 grep 命令来实现。比如,若要在已安装的软件包中,查询包含 ftp 关键字的软件包的名称,则实现的命令为:

```
[root@rh9 root]# rpm -qa | grep ftp
```

#### (2) 查询指定的软件包是否安装

命令用法: rpm -q 软件包名称列表

该命令可同时查询多个软件包,各软件包名称之间用空格分隔,若指定的软件包已安装,将显示该软件包的完整名称(包含有版本号信息),若没有安装,则会提示该软件包没有安装。

比如,若要查询 vsftpd 软件包是否已安装,则操作命令为:

```
[root@rh9 root]# rpm -q vsftpd  
vsftpd-1.1.3-8
```

若要查询 telnet-server 服务的软件包是否安装,则操作命令为:

```
[root@rh9 root]# rpm -q telnet-server  
package telnet-server is not installed
```

根据输出的提示信息,说明该软件包还没有被安装。

#### (3) 查询软件包的描述信息

命令用法: rpm -qi 软件包名称

例如,若要查看 vsftpd 软件包的描述信息,则实现命令为:

```
rpm -qi vsftpd
```

#### (4) 查询软件包中的文件列表

命令用法: rpm -ql 软件包名称

命令中的 `l` 参数是 `list` 的缩写, 可用于查询显示已安装软件包中所包含文件的文件名以及安装位置。

例如, 若要查询 `vsftpd` 软件包包含有哪些文件, 以及这些文件都安装在什么位置, 则实现的命令为:

```
[root@rh9 root]# rpm -ql vsftpd
```

#### (5) 查询某文件所属的软件包

命令用法: `rpm -qf 文件或目录的全路径名`

利用该命令, 可以查询显示某个文件或目录是通过安装哪一个软件包产生的, 但要注意并不是系统中的每一个文件都一定属于某个软件包, 比如用户自己创建的文件, 就不属于任何一个软件包。

例如, 若要查询显示 `/etc/mail` 目录是安装哪一个软件包产生的, 则实现的命令为:

```
[root@rh9 root]# rpm -qf /etc/mail  
sendmail-8.12.8-4
```

#### (6) 查询未安装的软件包信息

在安装一个软件包前, 通常需要了解一下有关该软件包的相关信息, 比如该软件包的描述信息、文件列表等, 此时可增加使用 `p` 参数来实现。

查询软件包的描述信息, 命令用法: `rpm -qpi 软件包文件全路径名`

查询软件包的文件列表, 命令用法: `rpm -qpl 软件包文件全路径名`

查询软件包所安装的软件包的名称, 命令用法:

`rpm -qp 软件包文件全路径名`

例如, `telnet-server-0.17-25.i386.rpm` 软件包位于 Red Hat Linux 9 安装光盘的第 3 张的 `RedHat/RPMS` 目录中, 在安装前想了解一下该软件包的文件列表及安装的位置, 则实现的操作命令为:

```
[root@rh9 root]# mount /mnt/cdrom  
[root@rh9 root]# rpm -qpl /mnt/cdrom/RedHat/RPMS/telnet-server-0.17-25.i386.rpm  
/etc/xinetd.d/telnet  
/usr/sbin/in.telnetd  
/usr/share/man/man5/issue.net.5.gz  
/usr/share/man/man8/in.telnetd.8.gz  
/usr/share/man/man8/telnetd.8.gz  
[root@rh9 root]# umount /mnt/cdrom
```

## 2. 安装 RPM 软件包

安装 RPM 软件使用 `-i` 参数, 通常还结合使用 `v` 和 `h` 参数。其中 `v` 参数代表 `verbose`,

使用该参数在安装过程中将显示较详细的安装信息；h 参数代表 hash，在安装过程中将通过显示一系列“#”来表示安装的进度。因此安装 RPM 软件包的通常用法为“rpm -ivh 软件包全路径名”。

例如，若要安装 telnet-server-0.17-25.i386.rpm 软件包，则操作命令为：

```
[root@rh9 root]# mount /mnt/cdrom
[root@rh9 root]# rpm -ivh /mnt/cdrom/RedHat/RPMS/telnet-server-0.17-25.i386.rpm
[root@rh9 root]# rpm -q telnet server
telnet-server-0.17-25
```

根据查询的输出信息，说明 Telnet 服务器的软件包安装成功。telnet 服务受 xinetd 服务的管理，默认情况下并未启用该服务，若要启用该服务，则执行以下命令即可。

```
[root@rh9 root]# chkconfig telnet on
[root@rh9 root]# service xinetd restart
```

telnet 服务启动后，以后在 Windows 系统中就可使用“telnet Linux 主机 IP 地址”命令，登录到 Linux 服务器，并可对 Linux 服务器进行远程管理和操作了。

在安装软件包时，若要安装的软件包中某个文件已在安装其他软件包时安装，此时系统会报错，提示该文件不能被安装，若要 let rpm 命令忽略该错误信息，可在命令中增加使用“--replacefiles”参数选项。

有时一个软件包可能还依赖于其他软件包，即只有在安装了所依赖的特定软件包后，才能安装该软件包，此时，只需按系统给出的提示信息，先安装所依赖的软件包，然后再安装所要安装的软件包即可。

### 3. 删除 RPM 软件包

删除 RPM 软件包使用 -e 参数，命令用法：

rpm -e 软件包名

例如，若要删除 telnet-server 软件包，则实现命令为：

```
rpm -e telnet-server
```

### 4. 升级 RPM 软件包

若要将某软件包升级为较高版本的软件包，此时可采用升级安装方式。升级安装使用 -U 参数来实现，该参数的功能是先卸载旧版，然后再安装新版软件包。为了更详细地显示安装过程，通常也结合 v 和 h 参数使用，其用法为“rpm -Uvh 软件包文件全路径名”。

若指定的 RPM 包并未安装，则系统直接进行安装。

### 5. 软件包的验证

对软件包进行验证可保证软件包是安全的、合法有效的。若验证通过，将不会产生任

何输出,若验证未通过,将显示相关信息,此时应考虑删除或重新安装。

验证软件包是通过比较从软件包中安装的文件和软件包中原始文件的信息来进行的,验证主要是比较文件的大小、MD5 校验码、文件权限、类型、属主和用户组等。

验证软件包使用 -V 参数,要验证所有已安装的软件包,使用命令 `rpm -Va`。

若要根据 RPM 文件来验证软件包,则命令用法为“`rpm -Vp rpm 包文件名`”。

### 5.1.3 RPM 软件包管理工具

在 X-Windows 图形界面中,也提供了一个图形化的 RPM 软件包管理工具,利用该管理工具,也可实现软件包的添加或删除。

单击 X-Windows 的主菜单,然后单击 System Settings,在其下选择 Add/Remove Applications,即可打开 RPM 软件包管理工具,如图 5.1 所示。

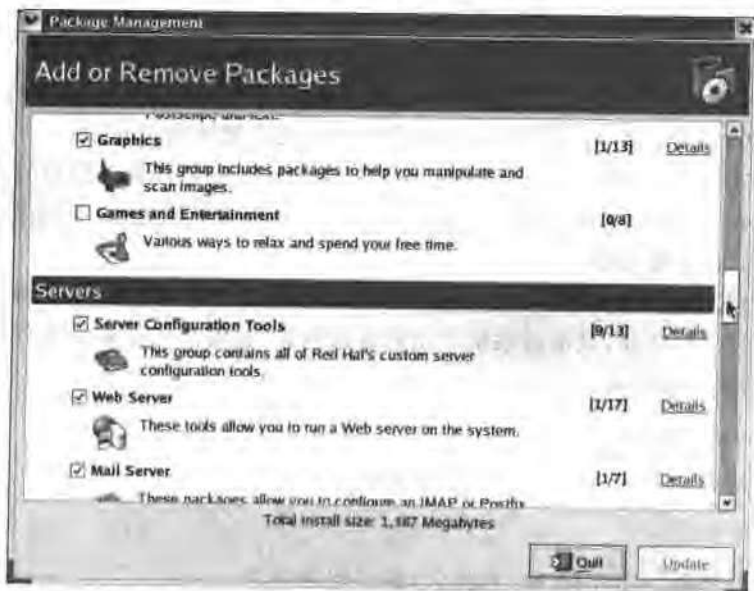


图 5.1 软件包管理工具

在该管理工具中,软件包被分成软件包组,单击该软件包组右边的 Details(细节),将打开一个新的窗口,在该窗口的列表中,将显示可供安装的 Standard Packages(标准软件包)和 Extra Packages(额外软件包),单击 Standard Packages 或 Extra Packages 前面的箭头图标,将进一步展开显示可供选择安装的软件包,在要安装的软件包前面的单选框中单击,让其出现一个打钩标志,即可选中要安装该软件包。设置完要安装的软件包后,单击 Update 按钮,即开始计算安装这些软件包所需的磁盘空间以及软件包的依赖关系,并会显示一个总结窗口,如果要安装的软件包存在所依赖的软件包,这些软件包将自动添加

到安装列表中,单击 Show details 按钮,可查看将要安装的软件包的完整列表,单击 Continue 按钮,即可开始安装。

## 5.2 TAR 包管理

TAR 是一种标准的文件打包格式,利用 tar 命令可将要备份保存的数据打包成一个扩展名为 .tar 的文件,以便于保存。需要时再从 .tar 文件中恢复即可。

使用 tar 命令来实现 TAR 包的创建或恢复,生成的 TAR 包文件的扩展名为 .tar,该命令只负责将多个文件打包成一个文件,但并不压缩文件,因此通常的做法是再配合其他压缩命令(如 gzip 或 bzip2),来实现对 TAR 包进行压缩或解压缩,为方便使用,tar 命令内置了相应的参数选项,来实现直接调用相应的压缩解压缩命令,以实现 TAR 文件的压缩或解压。该命令的基本用法为:

```
tar option file-list
```

option 为 tar 命令的功能参数,根据需要可同时选用多个,执行“tar --help”命令可获得用法帮助。其常用的主功能参数有:

- t 查看包中的文件列表;
- x 释包;
- c 创建包;
- r 增加文件到包文档的末尾。

另外,该命令还有一些辅助的功能参数,如 -z 代表 .gz 格式的压缩包,-j 代表 .bz 或 .bz2 格式的压缩包,-f 用于指定包文件名,-v 表示在命令执行时显示详细的提示信息,C 用于指定包解压释放到的目录路径,用法为: -C 目录路径名。

file-list 为要打包的文件名列表(文件名之间用空格分隔)或目录名,或者是要解压缩的包文件名。下面分别介绍该命令的详细用法。

### 1. 创建 TAR 包

命令用法: tar -cvf tar 包文件名 要备份的目录或文件名

命令功能: 将指定的目录或文件打包成扩展名为 .tar 的包文件。其中的参数 -c 代表创建 TAR 包文件。

例如,若要将 /etc 目录下的文件打包成 mylinux\_etc.tar,则实现命令为:

```
[root@rh9 root]# tar -cvf mylinux_etc.tar /etc/
```

命令执行后,在 /root 目录中就会生成一个名为 mylinux\_etc.tar 的文件。

### 2. 创建压缩的 TAR 包

直接生成的 TAR 包没有压缩,所生成的文件一般较大,为节省磁盘空间,通常需要

生成压缩格式的 TAR 包文件,此时可在 TAR 命令中增加使用-z 或-j 参数,以调用 gzip 或 bzip2 程序对其进行压缩,压缩后的文件扩展名分别为 .gz、.bz 或 .bz2,其命令用法为:

```
tar [-z | j]cvf 压缩的 tar 包文件名 要备份的目录或文件名
```

例如,若要将/etc 目录下的文件打包并压缩为 mylinux\_etc.tar.gz,则实现的命令为:

```
[root@rh9 root]# tar -zcvf mylinux_etc.tar.gz /etc/
```

最后在/root 目录中就会生成 mylinux\_etc.tar.gz 文件。

若要打包并压缩为 .bz2 格式的压缩包,则实现命令为:

```
[root@rh9 root]# tar -jcvf mylinux_etc.tar.bz2 /etc/
```

若要将/root/目录下的 install.log 和 myfile.txt 文件打包并压缩成 test.tar.bz2,则命令为:

```
[root@rh9 root]# tar -jcvf test.tar.bz2 install.log myfile.txt
```

```
[root@rh9 root]# file test.tar.bz2
```

# 查看文件的类型

```
test.tar.bz2: bzip2 compressed data, block size = 900k
```

### 3. 查询 TAR 包中文件列表

在释放解压 TAR 包文件之前,有时需要了解一下 TAR 包中的文件目录列表,此时可使用带-t 参数的 tar 命令来实现,其用法为“tar -t [-z | j][v]f tar 包文件名”。

例如,若要查询 mylinux\_etc.tar 中的文件目录列表,则实现命令为:

```
[root@rh9 root]# tar -tf mylinux_etc.tar
```

若要显示文件列表中每个文件的详细情况,可增加使用-v 参数,此时的文件列表方式类似于“ls -l”命令。比如:

```
[root@rh9 root]# tar -tvf mylinux_etc.tar
```

若要查看 .gz 压缩包中的文件列表,则还应增加使用-z 参数;若要查看 .bz 或 .bz2 格式的压缩包的文件列表,则应增加-j 参数。例如:

```
[root@rh9 root]# tar -tjvf mylinux_etc.tar.bz2
```

```
[root@rh9 root]# tar -tzvf mylinux_etc.tar.gz
```

### 4. 释放 TAR 包

释放 TAR 包使用-x 参数,其命令用法为“tar -xvf tar 包文件名”。

对 .gz 格式的压缩包,增加-z 参数,.bz 或 .bz2 压缩包,增加-j 参数,此时的命令用法为“tar [-z | j]xvf 压缩的 tar 包文件名”。

例如,若要释放软件包 `httpd-2.0.50.tar.gz`,则实现的命令为:

```
[root@rh9 root]# tar -zxvf httpd-2.0.50.tar.gz
```

若要释放软件包 `iptables-1.2.8.tar.bz2`,则实现的命令为:

```
[root@rh9 root]# tar -jxvf iptables-1.2.8.tar.bz2
```

`tar` 命令的参数也可不要“-”,比如释放 `iptables-1.2.8.tar.bz2` 软件包的命令也可以表达为 `tar jxvf iptables-1.2.8.tar.bz2`。

`tar` 命令在释放软件包时,将按原备份路径释放和恢复,若要将软件包释放到指定的位置,可使用“-C 路径名”参数来指定要释放到的位置。

比如,假设在当前目录下名为 `iptables-1.2.8.tar.bz2` 的软件包,现要将其释放到 `/usr/local/src` 目录下,则释放命令为:

```
[root@rh9 root]# tar -jxvf iptables-1.2.8.tar.bz2 -C /usr/local/src
```

另外,如果要将 `.gz` 文件分割成数个 1.44MB 大小的文件,可采用以下命令来实现。把 `.gz` 文件分割到软盘,实现命令:

```
tar -cvfm /dev/fd0 file.tar.gz
```

将软盘上的文件合并恢复到硬盘,实现命令:

```
tar -xvfm /dev/fd0
```

对于没有用 `tar` 打包而直接用 `gunzip` 压缩的文件,可使用“`gunzip filename.gz`”的格式来进行解压。对于 `zip` 格式的压缩文件,Linux 提供了 `/usr/bin/unzip` 解压程序。

## 习题

1. Red Hat Linux 所提供的安装软件包,默认的打包格式为( )。  
A. `.tar`                      B. `.tar.gz`                      C. `.rpm`                      D. `.zip`
2. 以下对 Linux 包管理方式的描述正确的是( )。  
A. `.rpm` 格式的软件包相当于 Windows 系统的安装程序,因此可以直接在命令行中键入软件包的名称来安装该软件包  
B. `.tar` 格式的软件包,在打包时已经过压缩处理  
C. `tar` 命令本身不具有压缩功能,但可以通过指定参数来调用其他压缩程序,实现对包的压缩  
D. 要查看 `vsftpd` 软件包的描述信息,可使用命令 `rpm -i vsftpd` 来实现
3. 若要查询 `vsftpd` 软件包在当前 Linux 系统中是否安装,则实现的命令为( )。

- A. rpm -qa      B. rpm -q vsftpd      C. rpm -i vsftpd      D. rpm -qi vsftpd
4. 若要查询系统当前都安装有哪些包含 ssh 关键字的软件包,则实现的命令为( )。
- A. rpm -qa|grep ssh      B. rpm -q ssh  
C. rpm -qi ssh      D. rpm -ql ssh
5. 在安装一个软件包之前,若想查看该软件包将安装哪些文件以及安装位置,此时 rpm 命令的功能选项参数应使用( )。
- A. -ql      B. -qpi      C. -qpl      D. -qp
6. 利用 rpm 安装软件包时,应使用的命令选项参数为( ),删除某软件包,应使用( ),升级某个已安装的软件包,应使用( )。
- A. -i      B. -u      C. -e      D. -U
7. 若要对 myfile.txt.tar.gz 包进行解压还原,则应使用命令( )来实现。
- A. tar -xvf myfile.txt.tar.gz      B. tar -cvf myfile.txt.tar.gz  
C. tar -zcvf myfile.txt.tar.gz      D. tar -zxvf myfile.txt.tar.gz
8. 若要将当前目录中的 myfile.txt 文件压缩成 myfile.txt.tar.gz,则实现的命令为( )。
- A. tar -cvf myfile.txt myfile.txt.tar.gz  
B. tar -zcvf myfile.txt myfile.txt.tar.gz  
C. tar -zcvf myfile.txt.tar.gz myfile.txt  
D. tar -cvf myfile.txt.tar.gz myfile.txt
9. 现有 httpd-2.0.50.tar.bz2 软件包,现要将其释放到/usr/local/src 目录中,以下释放方法中,正确的是( )。
- A. tar zxvf httpd-2.0.50.tar.bz2  
B. tar -zxvf httpd-2.0.50.tar.bz2  
C. tar -jxvf httpd-2.0.50.tar.bz2  
D. tar jxvf httpd-2.0.50.tar.bz2 -C /usr/local/src

## 实训 5 Linux 软件包管理

**[实训目的]** 掌握 Linux RPM 软件包的查询、安装和删除方法,掌握 tar.gz 包的创建与解压方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 执行 rpm -qa|less 命令,查询了解当前系统所安装的软件包程序,查看完后用 q



命令退出 less 命令。

2. 查询显示当前所安装的软件包中,包含 tel 关键字的软件包。
3. 查询已安装的 telnet-0.17-25 软件包所包含的文件及其安装位置。
4. 查询当前系统是否安装 telnet-server 服务器软件包,若没有安装,则安装 telnet-server-0.17-25.i386.rpm 软件包,然后查询 telnet-server 软件包安装是否成功。
5. 使用 chkconfig 命令设置 telnet 服务在 Linux 系统启动时自启动,并重启 xinetd 服务,以让 telnet 服务立即启动生效。
6. 在 Windows 系统的命令行状态下,使用“telnet Linux 主机 IP 地址”命令登录 Linux 服务器,以测试能否利用 Telnet 服务器,进行远程登录和访问 Linux 主机。

注:在组织学生上机操作时,所设置的网关地址应是真实可以 ping 通的地址,否则宿主操作系统(如 Windows 2000)将无法访问虚拟主机。

7. 将整个/etc 目录打包并压缩成 myetc.tar.gz 文件,并保存在/root 目录中。
8. 将整个/etc 目录的文件列表保存到/root/myfile.txt 文件中,然后将该文件打包压缩成 myfile.txt.tar.bz2,接下来删除 myfile.txt 文件,最后对 myfile.txt.tar.bz2 包进行解压还原,并观察是否生成了 myfile.txt 文件。

## 第 6 章

# 配置网络连接

Linux 主机要与其他主机进行连接和通信,必须进行正确的网络配置。网络配置通常包括配置主机名、网卡 IP 地址、子网掩码、默认网关(默认路由)、DNS 服务器等方面。

在 Linux 系统中,TCP/IP 网络的配置信息是分别存储在不同的配置文件中的,需要编辑、修改这些配置文件来完成联网工作。相关的配置文件主要有/etc/sysconfig/network、网卡配置文件,以及和名称解析相关的/etc/resolv.conf、/etc/hosts 和/etc/nsswitch.conf 配置文件。

### 6.1 网络的基本配置

对网络的基本配置一般包括配置主机名、配置网卡和设置客户端名称解析服务三方面。

#### 6.1.1 配置主机名

主机名用于标识一台主机的名称,在网络中主机名具有惟一性。要查看当前主机的名称,可使用 hostname 命令,若要临时设置主机名,可使用“hostname 新主机名”命令来实现,该命令不会将新主机名保存到/etc/sysconfig/network 配置文件中,因此,重新启动系统后,主机名将恢复为配置文件中所设置的主机名。

```
[root@rh9 root]# hostname  
rh9
```

若要临时设置主机名为 mylinux,则实现命令为:

```
[root@rh9 root]# hostname mylinux  
[root@rh9 root]# hostname  
mylinux
```

在设置了新的主机名后,“#”左边的提示符还不能同步更改,使用 logout 注销重新登录后,就可显示出新的主机名来。

若要使主机名更改长期生效,则应直接在/etc/sysconfig/network 配置文件中进行修改,系统启动时,会从该配置文件中获得主机名信息,并进行主机名的设置。network 配置文件中的内容如下:

```
[root@rh9 root]# more /etc/sysconfig/network
NETWORKING= yes           //系统是否使用网络服务功能
HOSTNAME=rh9              //设置主机名
GATEWAY=192.168.168.1     //默认网关
FORWARD_IPV4=false       //是否开启 IP 数据包的转发,单网卡时一般为 false
```

### 6.1.2 配置网卡

对网卡(网络接口卡)设备和网卡 IP 地址、子网掩码、默认网关的配置,是主机网络配置的主要方面,直接关系着当前主机能否正常连接和通信。对网卡的配置包括对网卡硬件驱动的配置、IP 地址及网关配置两方面。

#### 1. 网络配置文件

网络配置文件/etc/sysconfig/network 用于对网络服务进行总体配置,如是否启用网络服务功能,是否开启 IP 数据包转发服务等。在没有配置或安装网卡时,也需要设置该文件,以使本机的回环设备(lo)能够正常工作,该设备是 Linux 内部通信的基础。常用的设置项主要有:

(1) NETWORKING 用于设置系统是否使用网络服务功能。一般应设置为 yes,若设置为 no,则将不能使用网络,而且很多系统服务程序也将无法启动。在配置文件中的设置方法为:

```
NETWORKING=yes|no
```

(2) FORWARD\_IPV4 用于设置是否开启 IPv4 的包转发功能。在只有一块网卡时,一般设置为 false,若安装有两块网卡,并要开启 IP 数据包的转发功能,则设置为 true,如在利用双网卡代理上网或连接两个网段进行通信时。

```
FORWARD_IPV4=false|true
```

另外也可编辑修改/etc/sysctl.conf 配置文件,将其中的 net.ipv4.ip\_forward=0 语句更改为 net.ipv4.ip\_forward=1,来打开内核的包转发功能。

(3) HOSTNAME 用于设置本机的主机名,/etc/hosts 中设置的主机名要注意与此处的设置相同。

(4) DOMAINNAME 用于设置本机的域名。

(5) GATEWAY 用于设置本机的网关 IP 地址。

(6) GATEWAYDEV 用于设置与此网关进行通信时,所使用的网卡的名称。

network 的典型配置如下:

```
NETWORKING=yes
FORWARD_IPV4=false
GATEWAY=192.168.168.1
GATEWAYDEV=eth0
HOSTNAME=rh9
DOMAINNAME=localdomain
```

## 2. 配置网卡的设备驱动模块

要使网卡正常工作,必须首先正确配置网卡的设备驱动模块,这类似于在 Windows 系统中要正确安装网卡的驱动程序。

按总线类型的不同,目前使用的以太网卡主要有 ISA 网卡、PCI 网卡和 PCMCIA 网卡。为使网卡正常工作,需要在模块配置文件(/etc/modules.conf)中设置网卡设备的别名(如 eth0 或 eth1 等),以及该网卡所要使用的驱动模块名,这样内核在需要使用驱动程序时,会由内核服务 kmod 使用系统命令 modprobe(insmod)自动装载该驱动模块,以使设备能正常工作。

在 Linux 系统中,模块配置文件用于在系统启动时,加载系统所需的硬件驱动模块,如网卡、声卡、USB 等设备的驱动模块。一般情况下,Linux 的安装程序均能自动检测和识别到网卡,并能自动在模块配置文件中对网卡进行配置。不同硬件的网卡所需加载的网卡驱动模块是不同的,若系统中存在多块网卡,则对每块网卡都要指定所要加载的驱动模块。

以太网卡的设备名用 ethN 来表示,其中 N 为一个从 0 开始的数字,代表网卡的序号,第一块以太网卡的设备名为 eth0,第二块以太网卡的设备名为 eth1,其余依次类推。若要查看在 modules.conf 文件中,对网卡驱动模块的配置情况,则可使用以下命令来实现:

```
[root@rh9 root]# grep eth /etc/modules.conf
alias eth0 pcnet32
```

可见,当前系统的 eth0 网卡所加载使用的网卡驱动模块为 pcnet32。

配置文件中的“alias usb-controller usb-uhci”用于指定 USB 设备的别名(usb-controller)和所使用的桥接器驱动模块(usb-uhci)。进行该项配置后,系统启动时就会自动检测 USB 设备,当检测到系统支持的 USB 设备时,就会自动加载所需的模块。

## 3. 网卡配置文件

网卡的设备名、IP 地址、子网掩码以及默认网关等配置信息是保存在网卡的配置文

件中的,一块网卡对应一个配置文件,该配置文件位于/etc/sysconfig/network-scripts目录中,其配置文件名具有以下格式:

ifcfg-网卡类型以及网卡的序号

以太网卡的类型为 eth,因此,第一块网卡的配置文件名为 ifcfg-eth0,第二块网卡的配置文件名为 ifcfg-eth1,其余依次类推。其他网卡的配置文件可用 cp 命令复制 ifcfg-eth0 配置文件获得,然后根据需要进行适当的修改即可。

Linux 也支持一块物理网卡绑定多个 IP 地址,此时对于每个绑定的 IP 地址,需要一个虚拟网卡,该网卡的设备名为 ethN:M,对应的配置文件名的格式为 ifcfg-ethN:M,其中 N 和 M 均为从 0 开始的数字,代表其序号。如第 1 块以太网卡上绑定的第 1 个虚拟网卡(设备名为 eth0:0)的配置文件名为 ifcfg-eth0:0,绑定的第 2 块虚拟网卡(设备名为 eth0:1)的配置文件名为 ifcfg-eth0:1。Linux 最多支持 255 个 IP 别名,对应的配置文件可通过复制 ifcfg-eth0 配置文件,并通过修改其配置内容来获得。

在网卡配置文件中,每一行为一个配置项目,左边为项目名称,右边为当前设置值,中间用“=”连接。配置文件中各项目的功能与含义如表 6.1 所示。

表 6.1 网卡配置文件各项目的功能与含义

项目名称	设置值	功 能
DEVICE	eth0	代表当前网卡设备的设备名称
BOOTPROTO	static 或 dhcp	设置 IP 地址的获得方式,static 代表静态指定 IP 地址,dhcp 为动态分配 IP 地址
BROADCAST	192.168.168.255	广播地址
IPADDR	192.168.168.154	为该网卡的 IP 地址
NETMASK	255.255.255.0	该网卡的子网掩码
NETWORK	192.168.168.0	该网卡所处网络的网络地址
GATEWAY	192.168.168.1	网卡的默认网关地址(默认路由)
ONBOOT	yes 或 no	用于设置在系统启动时,是否启用该网卡设备。若为 yes,则启用

在 Linux 安装程序的最后,会要求对网卡的 IP 地址、子网掩码、默认网关以及 DNS 服务器进行指定和配置,正常安装的 Linux 系统,其网卡已配置并可正常工作。根据需要也可重新对其进行配置和修改。

若要查看 eth0 网卡的配置文件的内容,则操作命令为:

```
[root@rh9 root]# more /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.168.255
IPADDR=192.168.168.154
NETMASK=255.255.255.0
NETWORK=192.168.168.0
GATEWAY=192.168.168.1
ONBOOT=yes
```

若要在 eth0 网卡上再绑定一个 192.168.168.13 的 IP 地址,则绑定方法为:

```
[root@rh9 root]# cd /etc/sysconfig/network-scripts/
[root@rh9 network-scripts]# cp ifcfg-eth0 ifcfg-eth0:0
[root@rh9 network-scripts]# vi ifcfg-eth0:0
DEVICE=eth0:0
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.168.13
NETMASK=255.255.255.0
```

**注意:**更改网卡的设备名(DEVICE)为 eth0:0,以后绑定有 192.168.168.13 IP 地址的这块虚拟网卡的设备名称就是 eth0:0。另外,网卡配置文件中的 NETWORK 和 BROADCAST 地址可以不指定,利用子网掩码,系统可以自动计算出来。

若要临时给网卡绑定一个 IP 地址,可使用以下命令来实现:

```
ifconfig eth0 add 192.168.168.150 netmask 255.255.255.0
```

#### 4. 网卡的配置方法

对网卡的配置有两种方法,一是直接利用 vi 编辑器,编辑修改网卡的配置文件,二是利用 netconfig 配置工具来配置网络,netconfig 实质上也是通过修改网卡的配置文件来实现的。

netconfig 网络配置工具采用基于字符的窗口界面,来完成对 IP 地址、子网掩码、默认网关和 DNS 域名服务器的设置。在 Shell 命令行上键入并执行 netconfig 命令,即可启动该配置工具。在启动界面单击 Yes 按钮,即可进入网络配置界面,如图 6.1 所示。设置好后,单击 OK 按钮退出,其配置结果将写回到网卡的配置文件中。

使用 netconfig 配置工具进行网络配置后仅是修改了网络配置文件,并未立即生效。为使所作的配置立即生效,需要使用 service network restart 命令重启网络服务。

```
[root@rh9 root]# service network restart
Shutting down interface eth0:
```

[OK]

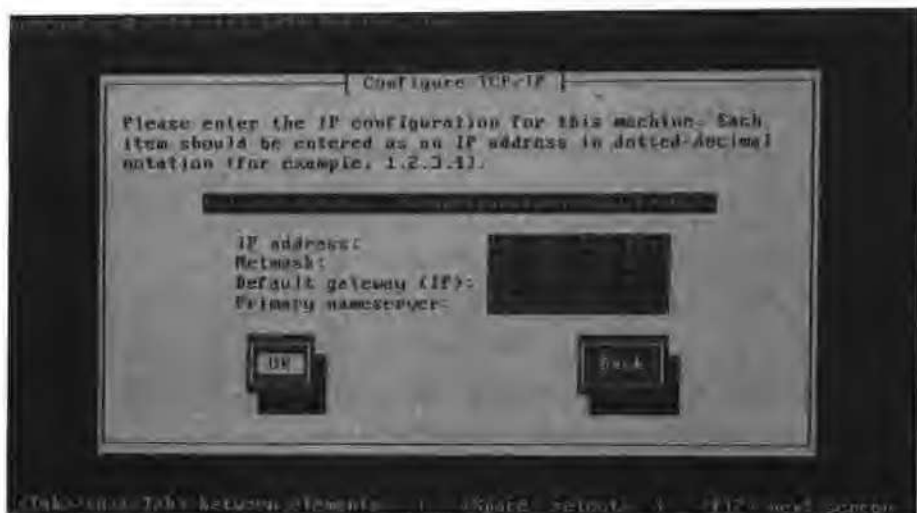


图 6.1 网络配置主界面

Shutting down loopback interface:	[OK]
Setting network parameters:	[OK]
Bringing up loopback interface:	[OK]
Bringing up interface eth0:	[OK]

## 5. 网卡的常用操作命令

Linux 系统还提供了一些命令,用于查看网卡的设置信息或实现对网卡的管理。

### (1) 显示网卡的设置信息

要显示网卡的设置信息,可使用 `ifconfig` 命令来实现,其通常用法有以下几种。

显示当前活动的网卡(未被禁用的)的设置,命令用法为 `ifconfig`。

显示系统中所有网卡的设置信息,命令用法为 `ifconfig -a`。

显示指定网卡的设置信息,命令用法为“`ifconfig 网卡设备名`”。

例如,若要查看系统中所有网卡的设置信息,则执行命令:

```
[root@rh9 root]# ifconfig -a
eth0:  Link encap:Ethernet  HWaddr 00:0C:29:03:F3:75
        inet addr:192.168.168.154    Bcast:192.168.168.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  METRIC:1
        RX packets:154 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:28030(27.3Kb)  TX bytes:336 (336.0 b)
```

```

    Interrupt:10 Base address:0x1080
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP BROADCAST RUNNING MTU:16436 METRIC:1
        RX packets:10 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:700(700.0 b)  TX bytes:700(700.0 b)

```

UP BROADCAST RUNNING 表示该网卡处于活动状态,没有被禁用。lo 是 loopback 的缩写,代表 loopback 接口,计算机使用 loopback 接口来连接自己,该接口同时也是 Linux 内部通信的基础,其接口 IP 地址始终为 127.0.0.1,默认情况下 lo 网络接口已自动配置好,用户不需对其进行修改或重新配置。

### (2) 设置网卡的 IP 地址

要设置或修改网卡的 IP 地址,可使用以下命令用法来实现:

ifconfig 网卡设备名 IP 地址 netmask 子网掩码

例如,若要将当前网卡 eth0 的 IP 地址设置为 192.168.168.156,子网掩码为 255.255.255.0,则实现命令为:

```

[root@rh9 root]# ifconfig eth0 192.168.168.156 netmask 255.255.255.0
[root@rh9 root]# ifconfig eth0

```

从输出信息的第 2 行的“inet addr:192.168.168.156”可知,网卡的 IP 地址已被重设为 192.168.168.156。

该命令不会修改网卡的配置文件,所设置的 IP 地址仅对本次有效,重启系统或网卡被禁用后又重启,其 IP 地址将设置为网卡配置文件中指定的 IP 地址。

### (3) 禁用网卡

若要禁用网卡设备,可使用以下命令来实现:

ifconfig 网卡设备名 down

或 ifdown 网卡设备名

这两条命令功能相同,通常后者使用较多。

例如,若要临时禁用 eth0 网卡,则实现命令为 ifdown eth0 或 ifconfig eth0 down。

### (4) 重新启用网卡

网卡被禁用后,若要重新启用网卡,其命令为:

ifconfig 网卡设备名 up

或 ifup 网卡设备名



例如,若要重新启动 eth0 网卡,则实现命令为 ifup eth0 或 ifconfig eth0 up。

#### (5) 设置默认网关

网关是将当前网段中的主机与其他网络的主机相连接并实现通信的一个设备。设置了主机的 IP 地址和子网掩码后,就可与同网段的其他主机进行通信了,但此时无法与其他网段的主机进行通信,为了实现能与不同网段的主机进行通信,必须设置默认网关地址。网关地址必须是当前网段的地址,不能是其他网段的地址。

设置默认网关也即设置默认路由,可使用 Linux 系统提供的 route 命令来实现,该命令主要用于添加或删除路由信息。下面分别介绍该命令的功能和用法:

##### ① 查看当前路由信息

若要查看当前系统的路由信息,其实现命令为 route。

```
[root@rh9 root]# route
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.168	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo

##### ② 添加/删除默认网关

若要添加默认网关,其命令用法为:

```
route add default gw 网关 IP 地址 dev 网卡设备名
```

删除默认网关,命令用法为:

```
route del default gw 网关 IP 地址
```

例如,若要设置网卡 eth0 的默认网关地址为 192.168.168.1,则实现命令为:

```
[root@rh9 root]# route add default gw 192.168.168.1 dev eth0
[root@rh9 root]# route
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.168	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.168.1	0.0.0.0	UG	0	0	0	eth0

若要删除默认网关,则实现命令为:

```
route del default gw 192.168.168.1
```

##### ③ 添加/删除路由信息

在系统当前路由表中添加路由记录,其命令用法为:

```
route add -net 网络地址 netmask 子网掩码 [dev 网卡设备名] [gw 网关]
```

若要删除某条路由记录,则命令用法为:

```
route del -net 网络地址 netmask 子网掩码
```

为便于演示路由的删除和添加,下面先对 eth0 网卡绑定一个 192.168.167.155 的 IP 地址,其操作命令为:

```
[root@rh9 root]# ifconfig eth0:0 192.168.4.155
```

```
[root@rh9 root]# route
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.168.0	*	255.255.255.0	U	0	0	0	eth0
192.168.167.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.168.1	0.0.0.0	UG	0	0	0	eth0

从中可见,系统自动添加 192.168.167.0 网络的路由记录。若要删除该条路由记录,则实现的操作命令为:

```
[root@rh9 root]# route del -net 192.168.167.0 netmask 255.255.255.0
```

```
[root@rh9 root]# route
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.168.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.168.1	0.0.0.0	UG	0	0	0	eth0

若要再次将该条路由添加到当前路由表中,则实现的操作命令为:

```
[root@rh9 root]# route add -net 192.168.167.0 netmask 255.255.255.0 dev eth0
```

```
[root@rh9 root]# route
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.168.0	*	255.255.255.0	U	0	0	0	eth0
192.168.167.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.168.1	0.0.0.0	UG	0	0	0	eth0

假设要为 192.168.0.0/16 网络添加一条路由,其网关地址为 192.168.252.254,则实现命令为 `route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.252.254`。

## 6. 绑定 IP 和 MAC 地址

将 IP 与 MAC 地址绑定,可防止 IP 地址的盗用。其实现方法如下。

首先创建/etc/ethers 文件,其内容为“ip 地址 空格 mac 地址”。

然后运行 arp -f 命令,使绑定生效。

例如,若要将 192.168.168.154 与 MAC 地址为 00:0C:29:03:F3:75 的网卡绑定,则实现命令为:

```
[root@rh9 root]# echo "192.168.168.154 00:0C:29:03:F3:75" >> /etc/ethers
[root@rh9 root]# arp -f
```

### 7. 修改网卡的 MAC 地址

首先停用要修改的网卡设备,然后使用以下命令格式进行设置修改:

ifconfig 网卡设备名 hw ether MAC 地址

例如,若要将 eth0 网卡的 MAC 地址修改为 00:0C:29:03:F3:76,则实现命令如下:

```
[root@rh9 root]# ifdown eth0
[root@rh9 root]# ifconfig eth0 hw ether 00:0C:29:03:F3:76
[root@rh9 root]# ifup eth0
[root@rh9 root]# ifconfig eth0
```

# 查看新的 MAC 地址

## 6.1.3 配置客户端名称解析

### 1. 设置 DNS 服务器

正确设置了 IP 地址和网关地址后,就可用 IP 地址与其他主机通信了,但此时还无法用域名与其他主机进行通信,为此,必须为当前主机指定至少一个 DNS 服务器的 IP 地址,以便当前主机能用该 DNS 服务器来进行域名解析。在 Linux 中,最多可同时指定 3 个 DNS 服务器的 IP 地址。

/etc/resolv.conf 配置文件用于配置 DNS 客户,该文件包含了主机的域名搜索顺序和 DNS 服务器的 IP 地址。在配置文件中,使用 nameserver 配置项来指定 DNS 服务器的 IP 地址,查询时就按 nameserver 在配置文件中的顺序进行,且只有当第一个 nameserver 指定的域名服务器没有反应时,才用下面一个 nameserver 指定的域名服务器来进行域名解析。

```
[root@rh9 root]# more /etc/resolv.conf
nameserver 192.168.252.253
```

若还要添加可用的 DNS 服务器地址,则利用 vi 编辑器在其中添加即可。比如若要再添加 61.128.128.68 和 61.128.192.68 这两个 DNS 服务器,则在配置文件中添加以下两行内容:

```
nameserver 61.128.128.68
```

```
nameserver 61.128.192.68
```

另外还可用 domain 来指定当前主机所在域的域名。

## 2. hosts 文件

/etc/hosts 是早期实现主机名称解析的一种方法,其中包含了 IP 地址和主机名之间的对应关系。进行名称解析时系统会直接读取该文件中设置的 IP 地址和主机名的对应记录。文件中“#”开头的行为注释行,其余每一行为一条记录,IP 地址在左,主机名、主机全域名以及主机的别名在右。该配置文件的默认内容如下:

```
[root@rh9 root]# more /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          rh9    localhost,localdomain localhost
```

在没有指定域名服务器时,网络程序一般通过查询该文件来获得某个主机对应的 IP 地址。利用该文件,可实现在本机上的域名解析,比如,若要将域名为 www.mytest.com 的主机的 IP 地址指向 192.168.168.154,则只需在该文件中添加如下一行内容即可。

```
192.168.168.154    www.mytest.com
[root@rh9 root]# ping www.mytest.com          #测试域名解析是否生效
```

## 3. 指定名称解析顺序

要设置名称解析的先后顺序,可利用/etc/nsswitch.conf 配置文件中的“hosts:”配置项来指定,其默认解析顺序为 hosts 文件、DNS 服务器。对于 UNIX 系统,还可用 NIS 服务器来进行解析。

```
[root@rh9 root]# grep hosts /etc/nsswitch.conf
# hosts:  db files nisplus nis dns
hosts:    files dns          #其中的 files 代表用 hosts 文件来进行名称解析
```

# 6.2 安装与配置 ADSL 拨号

## 6.2.1 安装 PPPoE 拨号软件

PPP(Point to Point Protocol,点对点协议)是 TCP/IP 协议的一个扩展,增加了通过串行接口传输 TCP/IP 包和安全登录的功能。以前的 MODEM 拨号上网采用的就是 PPP 协议,由于串行通信速度很慢,目前使用较少。

PPPoE(Point-to-Point Protocol Over Ethernet,以太网点对点协议)支持通过以太网来传输 TCP/IP 包,从而大大提高了网络的传输速度。PPPoE 也支持使用用户登录来确

保通信的安全并测量每个用户的数据流量。

ADSL 拨号上网可使用 PPPoE 拨号软件来实现,该软件的最新源代码软件包的下载地址为 [http://www.roaringpenguin.com/penguin/open\\_source\\_rp-pppoe.php](http://www.roaringpenguin.com/penguin/open_source_rp-pppoe.php),3.5 版的下载地址为 <http://www.roaringpenguin.com/penguin/pppoe/rp-pppoe-3.5.tar.gz>。

### 1. 下载软件包

使用如下命令可下载软件包:

```
[root@rh9 root]# cd /usr/local/src
[root@rh9 src]# wget http://www.roaringpenguin.com/penguin/pppoe/rp-pppoe-3.5.tar.gz
```

### 2. 安装软件包

安装软件包的操作命令如下:

```
[root@rh9 src]# tar -zxvf rp-pppoe-3.5.tar.gz
[root@rh9 src]# cd rp-pppoe-3.5/src
[root@rh9 src]# ./configure
[root@rh9 src]# make
[root@rh9 src]# make install
```

编译安装后,默认安装在 `/usr` 目录中,提供的可执行程序安装在 `/usr/sbin` 目录中,常用的可执行程序有 `adsl-setup`、`adsl-connect`、`adsl-start`、`adsl-stop`、`adsl-status`。配置文件安装在 `/etc/ppp` 目录中,主配置文件为 `pppoe.conf`,与防火墙相关的配置文件为 `/etc/ppp/firwall-standalone` 和 `/etc/ppp/firewall-masq`。`adsl` 服务启动脚本为 `/etc/rc.d/init.d/adsl`,帮助文档安装在 `/usr/man/man8` 和 `/usr/man/man5` 目录中。

另外,在 PPPoE 的源代码安装目录下,还提供了 `go` 和 `go-gui` 两个快速安装和配置向导,`go` 是一个基于文本界面的安装配置向导,`go-gui` 是一个基于图形界面的安装配置向导。

## 6.2.2 配置 ADSL 拨号

在使用 ADSL 之前,应先到 ISP 服务商处申请 ADSL 账户。安装 PPPoE 拨号软件后,接下来就应对 ADSL 拨号进行相关配置。配置可通过手工修改 `pppoe.conf` 配置文件来实现,也可使用 `adsl-setup` 配置向导来实现。

### 1. 配置 ADSL 拨号

使用 `adsl-setup` 配置向导来配置 ADSL 护号的步骤如下:

```
[root@rh9 root]# cd /usr/sbin
[root@rh9/sbin]# ./adsl-setup                                # 开始配置 ADSL
Welcome to the Roaring Penguin ADSL client setup. First, I will run some checks on your system to
```

```
make sure the PPPoE client is installed properly...
```

```
Looks good! Now, please enter some information:
```

```
USER NAME
```

```
>>>Enter your PPPoE user name (default bxxxxnxx@sympatico.ca): adsl628xxxxx
```

输入 ADSL 账户名称, 中国电信的 ADSL 直接输入账户名, 账户名一般是 ADSL 加电话号码。对于中国网通以太网宽带接入, 应在账户名后面输入! Internet。

```
INTERFACE
```

```
>>>Enter the Ethernet interface connected to the ADSL modem
```

```
For Solaris, this is likely to be something like /dev/hme0.
```

```
For Linux, it will be ethn, where 'n' is a number.
```

```
(default eth0): eth0
```

此时输入与 ADSL MODEM 相连的网卡的名称, 即用于连接 Internet 的网卡的名称。

```
Do you want the link to come up on demand, or stay up continuously?
```

```
If you want it to come up on demand, enter the idle time in seconds after which the link should be  
dropped. If you want the link to stay up permanently, enter 'no' (two letters, lower-case.)
```

```
NOTE: Demand-activated links do not interact well with dynamic IP addresses. You may have  
some problems with demand-activated links.
```

```
Enter the demand value (default no):
```

此段是询问是否启用闲时断开拨号连接。若回答 yes, 接下来将设置断开拨号连接的闲置时间, 在这段时间内若没有数据流, 将断开拨号连接。默认为 no, 不启用该项功能。由于目前 ADSL 基本上是包月制, 因此输入 no 或直接按回车。

```
DNS
```

```
Please enter the IP address of your ISP's primary DNS server.
```

```
If your ISP claims that 'the server will provide dynamic DNS addresses', enter 'server' (all lower-  
case) here.
```

```
If you just press enter, I will assume you know what you are doing and not modify your DNS setup.
```

```
Enter the DNS information here: 61.128.128.68
```

```
Please enter the IP address of your ISP's secondary DNS server.
```

```
If you just press enter, I will assume there is only one DNS server.
```

```
Enter the secondary DNS server address here: 61.128.192.68
```

如果 ADSL 服务提供商提供有动态的 DNS 服务器地址, 则输入全部小写的 server, 若没有提供, 则直接指定首选 DNS 服务器和备用 DNS 服务器的地址。

```
PASSWORD
```

```
>>>Please enter your PPPoE password:
```

>>>Please re-enter your PPPoE password:

此时输入 ADSL 账户的密码。

#### FIREWALLING

Please choose the firewall rules to use. Note that these rules are very basic. You are strongly encouraged to use a more sophisticated firewall setup; however, these will provide basic security. If you are running any servers on your machine, you must choose 'NONE' and set up firewalling yourself. Otherwise, the firewall rules will deny access to all standard servers like Web, e-mail, ftp, etc. If you are using SSH, the rules will block outgoing SSH connections which allocate a privileged source port.

The firewall choices are:

- 0 - NONE: This script will not set any firewall rules. You are responsible for ensuring the security of your machine. You are **STRONGLY** recommended to use some kind of firewall rules.
  - 1 - STANDALONE: Appropriate for a basic stand-alone web-surfing workstation
  - 2 - MASQUERADE: Appropriate for a machine acting as an Internet gateway for a LAN
- Choose a type of firewall (0-2): 2

此处选择防火墙类型,0 表示不使用防火墙,对于单机上网,可选择 1,若要将该台计算机作为企业内网用户上网的网关,可选择 2,使用 IP 伪装方式代理内网用户访问 Internet。

```
** Summary of what you entered **  
Ethernet Interface: eth0  
User name: adsl628xxxxx  
Activate-on-demand: No  
Primary DNS: 61.128.128.68  
Secondary DNS: 61.128.192.68  
Firewalling: MASQUERADE  
>>>Accept these settings and adjust configuration files (y/n)? y
```

此时显示了配置信息的一个摘要,回答 y,确认配置,系统将配置信息写入相关的文件中。

```
Adjusting /etc/ppp/pppoe.conf  
Adjusting /etc/resolv.conf  
Adjusting /etc/ppp/pap-secrets and /etc/ppp/chap-secrets  
(But first backing it up to /etc/ppp/pap-secrets-bak)  
(But first backing it up to /etc/ppp/chap-secrets-bak)
```

Congratulations, it should be all set up!

Type 'adsl-start' to bring up your ADSL link and 'adsl-stop' to bring it down.  
Type 'adsl-status' to see the link status.

系统提示配置成功,并提示可使用 adsl-start 进行拨号,使用 adsl-stop 来断开拨号连接。使用 adsl-status 命令查看连接状态。

与 ADSL 拨号相关的配置文件主要是/etc/ppp/pppoe.conf、pap-secrets 和 chap-secrets,其中 pap-secrets 和 chap-secrets 配置文件中均存储有拨号用户的账户和密码,分别用于支持 pap 和 chap 用户认证方式。

## 2. ADSL 拨号测试

在拨号之前,应先检查/etc/sysconfig/network 文件和网卡配置文件中是否设置了默认网关,若设置了,应在配置文件中将其删除,让 ADSL 拨号成功后自动获得,然后利用“service network restart”命令重启网络服务。

ADSL 拨号成功后,会增加拨号适配器 ppp0,系统就会自动将其作为默认的网关地址,这样才能访问 Internet 网。

```
[root@rh9 sbin]# ./adsl-start          # 开始 ADSL 拨号
.. Connected!                          # 连接成功!
```

拨号适配器的网络接口卡的名称为 ppp0,拨号成功后,会增加该网络接口。如果拨号不成功,应检查网线连接、ADSL MODEM 设备以及账户和密码设置是否正确,并可通过查看 /var/log/messages 日志文件,来了解拨号不成功的原因。

```
[root@rh9 sbin]# ifconfig ppp0          # 查 ppp0 网络接口
ppp0  Link encap:Point-to-Point Protocol
       inet addr:222.182.112.180  P-t-P:172.17.1.1 Mask:255.255.255.255
       UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
       RX packets:44 errors:0 dropped:0 overruns:0 frame:0
       TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:3
       RX bytes:2006 (1.9 Kb) TX bytes:30 (30.0 b)

[root@rh9 sbin]# route                  # 查看默认网关,应设置为 ppp0
Kernel IP routing table
Destination    Gateway      Genmask      Flags    Metric    Ref    Use    Iface
172.17.1.1     *           255.255.255.255 UH       0         0      0      ppp0
192.168.168.0  *           255.255.255.0  U        0         0      0      eth0
127.0.0.0      *           255.0.0.0     U        0         0      0      lo
default       172.17.1.1  0.0.0.0      UG       0         0      0      ppp0

[root@rh9 sbin]# ping 61.128.128.68    # 通过 ping DNS 服务器来测试对 Internet 的访问
```

若要停止 ADSL 连接,则操作命令为:



```
[root@rh9 sbin]# ./adsl-stop  
Killing pppd (7918)  
Killing adsl-connect (6679)
```

### 3. 设置 ADSL 自动拨号

若要在开机时自动拨号接入网络,可设置 ADSL 服务在 2、3、4、5 运行级别时,自动启动,其实现命令为:

```
[root@rh9 root]# chkconfig --add adsl --level 2345
```

## 6.3 常用网络调试命令

在网络的使用过程中,经常会出现由于某种原因,导致网络无法正常通信,为便于查找网络故障,Linux 系统提供一些网络诊断测试命令,以帮助用户找出故障原因并最终解决问题。本节将介绍一些常用的网络调试诊断命令。由于造成网络故障的原因一般较多,还需要用户在实践中不断总结和积累经验,以提高排错能力。

### 1. ping 命令

命令用法: `ping [-c count] [-s packetsize] [-W timeout]`

命令功能: ping 命令常用来检测网络是否连通以及连通的质量,是使用最频繁的一条网络检测命令。该命令通过向被测试的目的主机地址发送 ICMP 报文并收取回应的报文,来测试当前主机到目的主机的网络连接状态。

参数说明:

`-c count` 该选项用于指定向目的主机地址发送多少个报文,count 代表发送报文的数目。默认情况下,ping 命令会不停地发送 ICMP 报文,若要让 ping 命令停止发送 ICMP 报文,则可按 Ctrl+C 组合键来实现,最后还会显示一个总结信息。

`-s packetsize` 该选项用于指定发送 ICMP 报文的大小,以字节为单位。默认情况下,发送的报文数据大小为 56B(字节),加上每个报文头的 8B,共 64B 数据。有时网络会出现 ping 小包正常,而 ping 较大的数据包时,出现严重丢包现象,此时,就可利用该参数选项来发送一个较大的 ICMP 包,以检测网络在大数据流量的情况下,工作是否正常。

`-W timeout` 该选项用于设置等待接收回应报文的间隔时间,以秒为单位。当 ping 一个目标主机时,若全部出现“Destination Host Unreachable”(目标主机不可到达)的提示信息,则说明网络不通或目标主机被禁止 ping。在目标主机未被禁止 ping 的情况下,为了进一步确定是否真的是网路不通,此时就可利用 -i 选项,调大等待的时间间隔,然后再 ping。若仍全是目标主机不可到达,则说明当前主机到目的主机的网路确实不通;若有部分报文可到达,则说明网络线路是通的,可能比较繁忙或带宽较窄,导致丢包严重。

例如,若要检测当前主机到目标主机 192.168.168.155 的网路是否通畅,则实现的操作命令为:

```
[root@rh9 root]# ping -c 4 192.168.168.155
PING 192.168.168.155 (192.168.168.155) 56 (84) bytes of data.
64 bytes from 192.168.168.154: icmp_seq=1 ttl=128 time=0.624 ms
64 bytes from 192.168.168.154: icmp_seq=2 ttl=128 time=0.325 ms
64 bytes from 192.168.168.154: icmp_seq=3 ttl=128 time=0.297 ms
64 bytes from 192.168.168.154: icmp_seq=4 ttl=128 time=0.290 ms

--- 192.168.168.155 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.290/0.384/0.624/0.139 ms
```

从输出信息可知,当前主机到目标主机的网路是通畅的,可以正常通信。time 项的值代表目标主机的响应时间,单位是毫秒(ms),该值越小,说明响应越快,网络连接质量越高。

若出现“Destination Host Unreachable”信息,则说明此次发送的 ICMP 报文未能到达目标主机。网路存在丢包现象。

若要向目标主机 192.168.168.155 发送 2K 的 ping 测试包,则操作命令为:

```
[root@rh9 root]# ping -c 4 -s 2048 192.168.168.155
PING 192.168.168.155 (192.168.168.155) 2048 (2076) bytes of data.
2056 bytes from 192.168.168.154: icmp_seq=1 ttl=128 time=11.5 ms
2056 bytes from 192.168.168.154: icmp_seq=2 ttl=128 time=0.612 ms
2056 bytes from 192.168.168.154: icmp_seq=3 ttl=128 time=0.663 ms
2056 bytes from 192.168.168.154: icmp_seq=4 ttl=128 time=0.626 ms

--- 192.168.168.155 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.612/3.364/11.555/4.729 ms
```

若要测试当前主机能否访问 192.168.168.240 主机,则操作命令为:

```
[root@rh9 root]# ping 192.168.168.240
PING 192.168.168.240 (192.168.168.240) 56(84) bytes of data.
From 192.168.168.154 icmp_seq=1 Destination Host Unreachable
From 192.168.168.154 icmp_seq=2 Destination Host Unreachable
From 192.168.168.154 icmp_seq=3 Destination Host Unreachable
From 192.168.168.154 icmp_seq=4 Destination Host Unreachable
From 192.168.168.154 icmp_seq=5 Destination Host Unreachable
```

```
/ 按 Ctrl+C 组合键停止 ping
192.168.168.240 ping statistics --
6 packets transmitted, 0 received, +6 errors, 100% packet loss, time 9001ms, pipe 3
```

所发送的 ICMP 报文全部未能到达目标主机,说明当前主机无法访问目标主机(应排除目标主机禁止 ping 的情况)。

当前主机与目标主机间的网络连接正常的情况下,若目标主机安装了防火墙软件并在防火墙规则中禁止了 ICMP 报文通过,或者在到达目标主机的网路中的某个三层交换机或路由器的 ACL(存取访问控制列表)中,不允许 ICMP 报文到达目标主机,则在 ping 目标主机时,也会出现报告“Destination Host Unreachable”的现象,这是因为该网路禁止了 ping 包通过。

## 2. netstat 命令

该命令可用来显示网络连接、路由表和正在侦听的端口等信息。通过网络连接信息,可以查看了解当前主机已建立了哪些连接,以及有哪些端口正处于侦听状态,从而发现一些异常的连接和开启的端口。“木马”程序通常会建立相应的连接并开启所需的端口,有经验的管理人员,通过该命令,可用来检查并发现一些可能存在的“木马”等后门程序。

该命令的用法: netstat 命令选项

该命令的命令选项较多,执行 netstat --help 命令可查看详细帮助说明。此处仅介绍几个常用的命令选项参数。

-l 显示正在侦听的服务或端口。

-a 该命令选项可用来显示当前主机所开放的所有端口,包括 TCP 端口和 UDP 端口,以及当前已建立的连接和正在侦听的端口。

-n 不进行名称解析。端口采用端口号来显示,而不转换为 service 文件中定义的端口名;IP 地址采用数字式地址显示,不转换成主机名或网络名显示。

-p 显示端口是由哪个进程和程序在监听。使用该参数后,会增加显示 PID/Program name 项目。

-c 动态显示网络连接和端口侦听信息。带上该参数后,所显示的信息将动态刷新,按 Ctrl+C 键可结束该命令。

-i 显示网络接口卡的相关信息。

-r 显示当前主机的路由表信息。netstat -r 或 netstat -nr 命令与 route 命令功能相同。

例如,若要显示当前主机正在侦听的端口,不进行名称解析,则实现命令为:

```
[root@rh9 root]# netstat -ln
```

若要显示当前主机所开放的所有端口,并显示各端口是由哪个进程在监听,则实现命

令为：

```
[root@rh9 root]# netstat -ap
```

### 3. traceroute 命令

该命令用于实现路由跟踪,命令用法：

```
traceroute IP 地址
```

利用该命令可跟踪从当前主机到指定的主机所经过的路径,从而分析出网络的故障点。

### 4. nslookup 命令

nslookup 命令主要用于检测指定的 DNS 服务器工作是否正常,该命令有交互查询方式和命令行查询方式两种用法。

#### (1) 交互查询方式

命令用法：nslookup

直接执行该命令,则进入域名的交互查询方式,并可指定域名服务器,以实现用指定的域名服务器来解析域名,以检查该域名服务器能否正常解析域名或某个域名。

nslookup 交互环境的命令行提示符为“>”,在该状态行上直接输入域名或 IP 地址,可进行域名到 IP 地址的解析或 IP 地址到域名的解析;使用“server DNS 服务器 IP 地址”子命令,可设置用来解析域名的 DNS 服务器;使用 exit 子命令可退出 nslookup 命令的交互状态。

对于网络管理员,通常应熟记几个本地的域名服务器的 IP 地址,如 61.128.128.68 和 61.128.192.68,这样可便于调试和检测网络故障。当无法用域名访问某个网站时,可先 ping 一下当地的 DNS 服务器,以检查当前计算机能否正常访问 Internet,若能 ping 通,则可用 nslookup 命令检查当前的 DNS 服务器能否正常解析该域名,若不能,则更换一个域名服务器再试,若多个域名服务器均无法解析,则一般说明该网站的域名过期或未注册。

例如,若要检查 61.128.192.68 这个域名服务器能否解析 www.tsinghua.edu.cn 和 www.pcnctedu.com 这两个域名,并查看 pcnctedu.com 域的 MX 记录,则操作方法如下：

```
[root@rh9 root]# nslookup
```

```
Note: nslookup is deprecated and may be removed from future releases.
```

```
Consider using the 'dig' or 'host' programs instead. Run nslookup with
```

```
the '-sil[ent]' option to prevent this message from appearing.
```

```
>server 61.128.192.68
```

# 指定用来解析域名的域名服务器

```

Default server: 61.128.192.68
Address: 61.128.192.68 # 53
> www.tsinghua.edu.cn
Server:        61.128.192.68
Address:       61.128.192.68 # 53

```

# 测试域名解析

```

Non-authoritative answer:
Name:   www.tsinghua.edu.cn
Address: 166.111.4.100
> www.pcnnetedu.com
Server:        61.128.192.68
Address:       61.128.192.68 # 53

```

# 测试域名解析

```

Non-authoritative answer:
Name:   www.pcnnetedu.com
Address: 61.186.170.104
> set type=mx
> pcnnetedu.com
Default server: 61.128.128.68
Address: 61.128.128.68 # 53

```

# 该域名对应的 IP 地址

# 设置查看的记录类型为 MX 记录

# 输入要查看的域名

```

Non-authoritative answer:
pcnnetedu.com mail exchanger= 10 mail.

```

authoritative answer can be found from:

pcnnetedu.com nameserver= ns.xinnet.cn.

# 该域名所注册的域名服务器

pcnnetedu.com nameserver= ns.xinnetdns.com.

mail.pcnnetedu.com internet address= 61.186.170.104

# 所查域的邮件服务器主机的 IP 地址

ns.xinnet.cn internet address= 202.106.124.195

# 域名服务器的 IP 地址

ns.xinnetdns.com internet address= 210.51.170.66

&gt; exit

# 退出 nslookup

[root@rh9 root] #

## (2) 命令行查询方式

该查询方式使用当前系统所设置的域名服务器来进行域名解析,其使用用法:

nslookup 域名

例如,若要检查能否解析 www.pcnnetedu.com 域名,则实现命令为:

```
[root@rh9 root] # nslookup www.pcnnetedu.com
```

```
Note: nslookup is deprecated and may be removed from future releases.  
Consider using the 'dig' or 'host' programs instead. Run nslookup with  
the '-silent' option to prevent this message from appearing.
```

```
Server:      192.168.252.253  
Address:     192.168.252.253#53
```

```
Non-authoritative answer:  
Name:   www.penetedu.com  
Address: 61.186.170.109
```

## 6.4 网络故障排查的基本方法

网络出现故障导致无法通信的原因多种多样,这需要管理员利用自己的网络理论知识,结合网络诊断调试命令,逐一分析和排查,找出故障点和故障原因,并最终解决问题。目前局域网中的用户,多采用网关和透明代理方式来访问互联网,当局域网中的用户出现无法访问互联网中的某个网站时,一般情况下,可采用以下步骤和方法,来逐一排查故障。

### 1. 检查本机 IP 地址及网关地址是否正确

当出现主机无法访问 Internet 网时,可先检查一下当前主机的 IP 地址、网关和域名服务器设置是否正确。较大型的局域网一般均采用划分网段的方法来减小冲突和广播域,不同的主机划分在不同的网段中,其内网 IP 地址和网关是不相同的,因此应先检查 IP 地址和网关设置是否正确,另外还应检查网卡本身工作是否正常,网线连接是否有问题。

对于动态分配的 IP 地址,可使用 `ipconfig /all` 命令(Windows 系统)检查当前主机是否正确获得了 IP 地址、网关地址和域名服务器地址。若发现未能正确获得,可以 ping DHCP 服务器,看能否访问 DHCP 服务器。若不能,则检查 DHCP 服务器工作是否正常;若正常,则说明到 DHCP 服务器间的网路不通。

对于 Linux 主机,可使用 `ifconfig` 命令来获得当前主机的 IP 地址,另外还可使用 `route` 命令查看当前主机路由表中的路由是否正确,特别要注意查看是否有默认路由,以及默认路由的地址是否正确。若没有默认路由,则主机将无法访问其他网段的主机或 Internet 网。

### 2. 检查到网关和代理的网路是否通畅

IP 地址和网关设置获取正确后,接下来可以 ping 网关地址,网关是该网段内的计算机的一个出口地址,若不通,则说明到网关的网路有问题。若能 ping 通,则下一步可以 ping 代理服务器地址,看访问代理服务器是否正常。若 ping 不通,则应检查代理服务器本身工作是否正常。

### 3. 检查与 DNS 服务器的连接

若代理服务器访问正常,接下来可以 ping 一下位于 Internet 网中的某个 DNS 服务器的 IP 地址,以检查能否访问互联网。若某个 DNS 服务器 ping 不通,则可以换一个再试,如 211.154.211.88 和 211.154.211.89,一般不会出现几个 DNS 服务器都同时出现故障的情况。

若 DNS 服务器都 ping 不通,则说明当前主机无法访问 Internet 网,很可能是网关接入互联网部分出现了问题。

### 4. 测试域名解析是否正确

若当前主机能 ping 通互联网中的 DNS 服务器,则意味着当前主机能访问互联网了。若此时仍出现某个网站无法访问的情况,此时可通过 nslookup 命令,测试当前主机使用的 DNS 服务器是否能够正确解析域名,若不能,还可换一个域名服务器再试,若都不能解析,则说明该网站的域名注册过期。若域名解析正常,主机又能访问其他网站,则说明该网站可能停机。

另外在访问不是使用 80 端口的网站或其他需要使用特殊端口的服务时,若出现无法连接的情况,此时应首先考虑该访问连接所要使用的端口,是不是被路由器或防火墙给关闭了,若是,则根据需要打开相应的端口即可。对于网管员,应了解一些常用服务器软件所使用的端口或端口范围,便于在做 ACL 控制列表时,打开需要使用的端口,关闭掉不需要使用的端口,以提高系统的安全性。

## 习题

1. 在 Linux 系统中,主机名保存在( )配置文件中。  
A. /etc/hosts  
B. /etc/modules.conf  
C. /etc/sysconfig/network  
D. /etc/network
2. 用于指定网卡、声卡等硬件驱动模块的配置文件是( )。  
A. /etc/modules.conf  
B. /etc/sysconfig/modules.conf  
C. /etc/conf.modules  
D. /etc/sysconfig/network-scripts/modules.conf
3. 第二块以太网卡的配置文件全路径名应是( )。  
A. /etc/sysconfig/network/ifcfg-eth0  
B. /etc/sysconfig/network/ifcfg-eth1  
C. /etc/sysconfig/network-scripts/ifcfg-eth0

- D. /etc/sysconfig/network-scripts/ifcfg-eth1
4. 在 Linux 系统中,用于设置 DNS 客户的配置文件是( )。  
A. /etc/hosts  
B. /etc/resolv.conf  
C. /etc/dns.conf  
D. /etc/nis.conf
5. 以下对网卡配置的说法中,正确的是( )。  
A. 可以利用 netconfig 命令来设置或修改网卡的 IP 地址、默认网关和域名服务器,该方法所设置的 IP 地址会立即生效  
B. 可以利用 vi 编辑器,直接修改网卡对应的配置文件,达到设置或修改网卡的名称、IP 地址以及默认网关等内容  
C. 利用 vi 编辑器修改网卡配置文件后,必须重新启动 Linux 系统,新的设置才会生效  
D. 在 Linux 系统中,多块网卡是共用同一个配置文件
6. 若要暂时禁用 eth0 网卡,以下命令中,可以实现的有( )。  
A. ifconfig eth0  
B. ifup eth0  
C. ifconfig eth0 up  
D. ifconfig eth0 down
7. 若要重新启用 eth0 网卡,以下命令中,可以实现的有( )。  
A. ifconfig eth0  
B. ifup eth0  
C. ifdown eth0  
D. ifconfig eth0 down
8. 若要查看当前主机的路由表信息,可使用的命令是( )。  
A. nslookup  
B. Router  
C. route  
D. router
9. 若要用指定的域名服务器来解析某个域名,则应使用( )命令。  
A. ping  
B. nslookup  
C. nslookup 要测试的域名  
D. netstat
10. 要重新启动 Linux 的网络服务功能,以下命令中,正确有效的有( )。  
A. server network restart  
B. service network restart  
C. /etc/rc.d/init.d/network restart  
D. /etc/rc.d/init.d/network start

## 实训 6 配置网络接口卡

**〔实训目的〕** 了解网卡的驱动模块配置文件,掌握网卡 IP 地址、网关和域名服务器的配置方法。

**【实训环境】** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。



### [实训内容]

1. 启动虚拟 PC 的 Linux 操作系统并用 root 用户登录。用 `ifconfig -a` 查看当前主机的网络接口卡,并从输出信息中,找到当前网卡的 IP 地址和 MAC 地址以及该网卡所使用的中断号。

2. 用 `ifdown eth0` 或 `ifconfig eth0 down` 命令禁用 `eth0` 网卡,然后再用 `ifconfig` 命令查看当前活动的网卡,此时 `eth0` 网卡的信息应不会显示出来。使用 `ifconfig -a` 命令查看所有网络接口卡的状态信息,注意查看当 `eth0` 网卡被禁用时,所输出的状态信息。

3. 用 `ifup eth0` 或 `ifconfig eth0 up` 命令重新启用 `eth0` 网卡,然后再用 `ifconfig` 命令查看。

4. 利用 `more /etc/modules.conf` 命令查看驱动模块配置文件,从中找出当前 `eth0` 网卡所使用的驱动模块名。

5. 利用 vi 编辑器编辑修改 `/etc/sysconfig/network-scripts/ifcfg-eth0` 配置文件,对网卡的 IP 地址进行修改(若改变了网段,则还应更改相应的网关),然后保存配置退出。利用 `service network restart` 命令重启 Linux 系统的网络服务功能,使更改生效。

用 `ifconfig eth0` 命令查看当前网卡的 IP 地址是否为所更改的 IP 地址,并用 `ping` 命令去 ping 该地址,检查能否 ping 通,最后用 `ping` 命令再 ping 一下位于相同网段的其他主机的 IP 地址,看能否 ping 通。

注:在组织学生上机操作时,各 Linux 主机以及虚拟 PC 的宿主操作系统的 IP 地址最好都设置为同一网段的地址,便于相互通信和进行 ping 测试。

为了使虚拟 PC 和宿主操作系统间能相互 ping 通,在宿主操作系统的网络和拨号连接中,应将 VMware Network Adapter VMnet1 和 VMware Network Adapter VMnet8 网络适配器禁用。

6. 利用 `netconfig` 命令来设置或修改网卡的 IP 地址、网关和域名服务器地址,更改后查看网卡的配置文件和 `/etc/resolv.conf` 配置文件,看是否在配置文件中作了对应的修改。最后用 `service network restart` 重启网络服务功能,使配置生效。

7. 下面为 Linux 主机再添加一块网卡并对该网卡进行必要的配置。利用双网卡可实现连接两个不同的网段,让其能相互通信。在实际应用中,代理服务器通常都是采用双网卡,一块网卡(如 `eth0`)用于连接内部局域网,另一块网卡(如 `eth1`)用于连接 Internet 网,在进行必要的配置后,就可以代理上网。有关代理服务器的详细配置方法,将在后续章节详细介绍,此处的实验,主要学习如何配置第 2 块。

(1) 利用 vi 编辑器,在驱动模块配置文件 `/etc/modules.conf` 中添加第 2 块网卡的驱动模块。一般情况下,最好使用与第一块网卡相同型号的网卡。添加方法参照第 1 块网卡,注意更改网卡设备名为 `eth1`,如: `alias eth1 pcnet32`。

(2) 进入 `/etc/sysconfig/network-scripts` 目录,利用 `cp ifcfg-eth0 ifcfg-eth1` 命令复

制生成第 2 块网卡的配置文件 `ifcfg-eth1`。然后利用 `vi` 编辑器修改该配置文件,注意修改第 2 块网卡的设备名为 `eth1`,第 2 块网卡的 IP 地址和相应的网关,比如 IP 地址设置为 192.168.167.156,网关设置为 192.168.167.1。在 `/etc/sysconfig/network` 配置文件中,添加以下配置项:

```
FORWARD_IPV4=true
```

(3) 使用 `shutdown -h now` 命令关闭 Linux 操作系统,然后安装第 2 块网卡到计算机中。此处的实验由于是在虚拟机中进行的,因此不需要实际安装第 2 块网卡,但需要利用虚拟机管理器,为该虚拟主机再添加一块网卡,添加方法如下:

单击“Edit virtual machine settings”,然后在虚拟机控制面板窗口中,单击 Add 按钮,此时将打开硬件添加向导,单击“下一步”按钮,在硬件类型列表中选择“Ethernet Adapter”,然后单击“下一步”按钮,在随后出现的网络连接方式窗口中,选择默认的网桥(Bridged: Connected directly to the physical network)方式,直接单击“完成”按钮完成第 2 块网卡的添加。

(4) 重新启动 Linux 系统,用 `ifconfig` 命令查看,检查 `eth1` 网卡是否生效。若输出了 `eth1` 网卡的信息,则说明 `eth1` 网卡安装成功,可以用 `ping` 命令 `ping` 一下该网卡绑定的 IP 地址,看能否 `ping` 通,最后再 `ping` 一下第 1 块网卡的 IP 地址,正常情况下都应能 `ping` 通。

8. 按 6.2 节所讲述的步骤和方法,配置 ADSL 拨号,并进行拨号连接和 `ping` 测试,以检查能否正常访问 Internet 网。

## Linux 服务器的配置

Linux 的网络服务功能十分强大,这是 Linux 系统的突出优点,本章将详细介绍 Linux 常用服务的安装和配置方法。

### 7.1 安装与配置 MySQL 服务器

MySQL 是一个小巧的、真正的多用户、多线程 SQL 数据库服务器软件,支持标准的数据库查询语言 SQL(Structured Query Language),使用 SQL 语句,可以很方便地实现数据库、数据表的创建,数据的插入、编辑修改和查询等操作,功能十分强大,且安全性好,并支持跨平台运行,能很好地运行在 Windows 9x、Windows 2000 和 Linux/UNIX 等平台。

#### 7.1.1 MySQL 安装简介

##### 1. 软件包安装简介

Red Hat Linux 软件包的安装一般有 RPM 包安装和源代码安装两种方式。利用 RPM 包安装操作较简单,不需要编译源代码,但只能安装在软件包所指定的位置,并只能安装固定的模块。利用源代码安装,需要事先对软件包进行必要的配置(如指定安装位置、要安装的模块等)和编译,然后再安装,该方式比较灵活,可以指定软件要安装到的位置以及所要安装的模块。

若要让 Linux 系统支持软件包源代码安装方式,则在安装 Linux 系统时,应注意安装 Linux 的开发工具,以提供编译源代码所需的编译器和相关的函数库。

要安装的软件包源代码通常放在 `/usr/local/src` 目录中,获得软件包的下载地址后,在 Linux 中,也可直接在命令行使用“`wget 下载地址`”命令来下载软件包。

##### 2. 查询 MySQL 服务器

在安装一个服务器软件之前,应先查询当前系统是否已安装了该服务。比如,要查询当前系统是否已安装了 MySQL 服务器,则操作命令为:

```
[root@rh9 root]# rpm -q mysql
package mysql is not installed
```

从输出信息可知,目前 MySQL 服务器尚未安装。若输出 mysql-3.23.52-3,则说明已安装,它是 Red Hat Linux 9 自带的版本。

若已安装 MySQL 服务,则可直接配置使用。若要安装新版的 MySQL,则可以使用 rpm -e 命令先删除原来安装的 MySQL,然后再安装新版的 MySQL,或者采用升级安装方式来升级 MySQL 服务器。

### 3. 获得 MySQL 服务器软件

MySQL 服务器软件的最新版本可到 <http://www.mysql.com> 官方网站下载,对于 Linux 平台,提供了 RPM 软件包和 tar.gz 格式的源代码软件包,这两种软件包的安装方法会有所不同。另外,在 Red Hat Linux 9 的安装光盘中,也自带 MySQL 的 rpm 安装软件包,该软件包的名称为 mysql-3.23.52-3.i386.rpm。

## 7.1.2 安装 MySQL 服务器

本节将分别介绍 MySQL 数据库服务器的 RPM 软件包安装方法和源代码安装方法,以及 MySQL 服务器的运行测试方法。

### 1. RPM 软件包安装方式

#### (1) 下载 MySQL 的 RPM 软件包

MySQL 3.23.58 版本的 RPM 软件包分为服务器和客户端两个软件包,其文件名分别为 MySQL-3.23.58-1.i386.rpm 和 MySQL-client-3.23.58-1.i386.rpm。客户端软件包用于提供 MySQL 的一些实用程序,比如用于连接 MySQL 服务器的 mysql 程序,及管理 mysql 的 mysqladmin 程序。

可将 RPM 软件包下载或复制到 /root/mylinuxsoft 目录中,并在安装前,先查询并了解软件包的文件列表及安装位置。其操作命令如下:

```
[root@rh9 root]# mkdir mylinuxsoft
[root@rh9 root]# cd mylinuxsoft
[root@rh9 mylinuxsoft]# rpm -qpl MySQL-3.23.58-1.i386.rpm | less # 查询包中文件安装列表
:
/etc/rc.d/init.d/mysql
:
/usr/bin/mysql_install_db
/usr/bin/mysqltest
/usr/bin/safe_mysqld
:
/usr/sbin/mysqld
:
```

从中可见,MySQL 的实用程序安装在/usr/bin 和/usr/sbin 目录中,/etc/rc.d/init.d/mysql 为 MySQL 服务器的启动和停止脚本。

```
[root@rh9 mylinuxsoft]# rpm -qpl MySQL-client-3.23.58-1.i386.rpm # 查询客户端文件列表
/usr/bin/msql2mysql
/usr/bin/mysql
/usr/bin/mysql_find_rows
/usr/bin/mysqlaccess
/usr/bin/mysqladmin
/usr/bin/mysqlbinlog
/usr/bin/mysqlcheck
/usr/bin/mysqldump
/usr/bin/mysqldimport
/usr/bin/mysql/show
/usr/share/man/man1/mysql.1.gz
:
/usr/share/man/man1/mysqlshow.1.gz
```

从中可见,MySQL 的客户端实用程序也默认安装在/usr/bin 目录下。

## (2) 安装 MySQL 服务器与客户端

```
[root@rh9 mylinuxsoft]# rpm -ivh MySQL-3.23.58-1.i386.rpm # 安装 MySQL 服务器软件包
```

执行该命令后,将显示软件的安装进度,并显示相关的提示信息。

MySQL 服务器安装成功后,将会产生/etc/rc.d/init.d/mysql 服务器启动脚本,同时还会创建 mysql 用户和名为 mysql 的用户组,并完成 MySQL 数据库的初始化工作。mysql 用户属于 mysql 用户组,mysql 服务器默认使用 mysql 用户来启动服务,它是 mysql 服务器正常工作所必需的一个系统账户。

```
[root@rh9 mylinuxsoft]# grep mysql /etc/passwd
mysql:x:100:101:MySQL server:/var/lib/mysql:/bin/bash
[root@rh9 mylinuxsoft]# grep mysql /etc/group
mysql:x:101:
```

从上可知,mysql 用户的宿主目录为/var/lib/mysql,该目录实际上就是 MySQL 数据库服务器存放数据库的位置。

```
[root@rh9 mylinuxsoft]# ll /var/lib/mysql/
drwx--x--x      2  mysql  root    4096  Aug  7  19:00  mysql
srwxrwxrwx      1  mysql  mysql    0     Aug  7  19:00  mysql.sock
-rw-rw----      1  mysql  root      72   Aug  7  19:00  rh9.err
-rw-rw--        1  mysql  mysql     4     Aug  7  19:00  rh9.pid
```

```
drwxr-xr-x      2  mysql  root    4096  Aug   7   19:00  test
```

MySQL 的一个数据库对应着一个目录,该数据库的数据表均存放在该目录下,每个数据表对应着三个文件,这三个文件的主名与数据表名相同,扩展名分别为 .frm、.MYD 和 .MYI。从以上输出可见,MySQL 服务器软件包安装后,系统自动创建了 mysql 数据库和 test 数据库,mysql 数据库是 MySQL 数据库服务器的系统数据库,包含名为 columns\_priv、tables\_priv、db、func、host 和 user 的数据表,其中的 user 数据表用于存放用户的账户和密码信息。test 数据库是一个空的数据库,没有任何数据表,用于测试,不用时也可将其删除。

如果要在命令行连接登录 MySQL 服务器,则还应安装 MySQL 的客户端软件包,其安装方法为:

```
[root@rh9 mylinuxsoft]# rpm -ivh MySQL-client-3.23.58-1.i386.rpm
Warning: MySQL-client-3.23.58-1.i386.rpm: V3 DSA signature: NOKEY, KEY ID 5072e1f5
Preparing...                               ##### [100%]
   1: MySQL-client                          ##### [100%]
[root@rh9 mylinuxsoft]# rpm -q mysql
MySQL-client-3.23.58-1
```

### (3) 启动 MySQL 服务器

MySQL 软件包安装完成后,默认情况下,MySQL 服务器已经启动。

若要启动 MySQL 服务器,实现的操作命令为:

```
[root@rh9 root]# /etc/rc.d/init.d/mysql start      # 或使用命令: service mysql start
Starting mysqld daemon with databasc from /var/lib/mysql
```

若要停止 MySQL 服务器启动,则操作命令为:

```
[root@rh9 root]# /etc/rc.d/init.d/mysql stop      # 或使用命令: service mysql stop
Killing mysqld with pid 3109
040807 20:02:17 mysqld ended
```

### (4) 设置 root 账户的密码

MySQL 服务器软件包安装时会自动初始化数据库,另外也可用 /usr/bin/mysql\_install\_db 命令来初始化和建立系统数据库。对于刚安装的 MySQL 服务器,其用户数据表中的 root 账户密码为空,即没有设置密码。出于安全考虑,一定要为 root 用户设置密码,因为该账户是 MySQL 数据库服务器的管理员账户,具有全部操作权限。

设置 root 账户的密码可使用 mysqladmin 命令来实现,该命令用于设置密码时的用法:

```
# /usr/bin/mysqladmin -u root -h 主机名 [-p] password '新密码'
```

其中, -u 参数用于指定用户名, -h 参数用于指定 MySQL 服务器所在的主机名或 IP 地址, 若 root 用户已有密码, 则必须选用 -p 参数, 并在提示输入密码时, 输入原密码, 若没有, 则不要使用 -p 参数。

在 user 用户数据表中, root 用户默认有两条记录, 其主机名字段 host 的值分别为 localhost 和 rh9。host 字段用于存储主机的名称或 IP 地址, 代表该用户可以从哪台主机登录 MySQL 服务器。localhost 代表本地主机, rh9 是当前 MySQL 服务器的主机名, 因此, 默认情况下, root 账户只能在 MySQL 服务器的本地机上登录, 对这两条记录均应设置密码。

例如, 要将 root 账户的密码设置为 snbj0814 # %baby, 则实现的命令为:

```
[root@rh9 root]# /usr/bin/mysqladmin -u root -h localhost password 'snbj0814 # %baby'
[root@rh9 root]# /usr/bin/mysqladmin -u root -h rh9 password 'snbj0814 # %baby'
[root@rh9 root]# /usr/bin/mysqladmin -u root flush-privileges      # 让密码立即生效
```

对 localhost 主机记录设置密码时, -h localhost 参数可以缺省。

#### (5) 连接和访问 MySQL 服务器

要存取访问 MySQL 服务器中的数据库, 必须首先登录连接到 MySQL 服务器。利用 MySQL 客户端软件包所提供的 mysql 程序, 可实现在 Linux 的命令行来连接和登录 MySQL 服务器, 登录成功后, 将出现 MySQL 的命令行提示符 mysql>, 在该命令中, 就可利用 MySQL 提供的命令和标准的 SQL 语句来操作和访问 MySQL 服务器了。

除了可在命令行访问 MySQL 服务器外, 也可在 PHP 网页中, 利用 PHP 脚本所提供的连接函数来连接和登录 MySQL 服务器, 登录成功后, 就可利用 PHP 所提供的相关函数, 结合 SQL 语句, 来实现利用网页存取和访问 MySQL 后台数据库服务器中的数据。

利用客户端连接程序 mysql 登录 MySQL 数据库服务器的命令用法:

mysql -u 用户名 -h 主机名 -p 用户密码

在命令行中, 用户密码可不指定, 但 -p 参数必须指定(若有密码), 系统会自动提示输入密码, 这是比较安全的用法, 用户密码不会记录在日志文件中。下面以 root 用户登录为例。

```
[root@rh9 root]# mysql -u root -h localhost -p
Enter password: *****
Welcome to the MySQL monitor. Commands end with; or \g.
Your MySQL connection id is 1 to server version: 3. 23. 58
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql>
```

登录成功后, 将显示一些提示信息, 如提示 MySQL 的命令结束符使用分号或 \g、当

前登录者的 id 号等,最后将出现 MySQL 的命令提示符 `mysql>`,在该命令行中,就可输入 MySQL 命令或 SQL 语句进行操作了。

比如,要显示当前 MySQL 数据库服务器中都有哪些数据库,则操作命令为:

```
mysql>show databases;
```

从输出可知,当前 MySQL 服务器有 `mysql` 和 `test` 两个数据库。

数据是直接存储在数据表中的,相关的多个数据表又是存放在某个数据库中的,在访问数据表中的数据之前,应先打开所要使用的数据库,在 MySQL 中,打开数据库使用 `use` 命令。比如要打开 MySQL 的系统数据库 `mysql`,则操作命令为:

```
mysql>use mysql;
```

若要显示该数据库中都有哪些数据表,则操作命令为:

```
mysql>show tables;
```

若要查看其中的 `user` 数据表中,每条记录的 `host`、`user` 和 `password` 字段的值,则操作命令为:

```
mysql>select host,user,password from user;
```

该命令执行后的输出如图 7.1 所示。

```
mysql> select host,user,password from user;
+-----+-----+-----+
| host      | user  | password |
+-----+-----+-----+
| localhost | root  | 5dc7875657dfa47a |
| rh9       | root  | 5dc7875657dfa47a |
| localhost |      |          |
| rh9       |      |          |
+-----+-----+-----+
4 rows in set (0.00 sec)

mysql>
```

图 7.1 查询 user 用户表的内容

从输出可见,刚才设置的密码在保存时,已经过加密(MD5)处理,保证了密码的安全性。若要查看 `user` 数据表中的全部字段的内容,则操作命令为:

```
mysql>select * from user;
```

若要退出 `mysql`,关闭当前连接,则执行 `quit` 或 `exit` 命令,此时将关闭与 MySQL 数据库服务器的连接,并退回到 Linux 的命令提示符状态。有关 MySQL 的其他用法,参见后面的 MySQL 管理基础。



### (6) 设置 MySQL 服务器的自启动

使用 `chkconfig --list|grep mysql` 命令可查询 mysql 服务器的自启动状态。

```
[root@rh9 root]# chkconfig --list|grep mysql
mysql      0:off    1:off    2:on     3:off    4:on     5:off    6:off
```

从输出可见,在运行级别为 3 和 5,mysql 服务器被设置为不自动启动,现将其改为自动启动即可,实现命令为:

```
[root@rh9 root]# chkconfig --level 35 mysql on
[root@rh9 root]# chkconfig --list|grep mysql
mysql      0:off    1:off    2:on     3:on     4:on     5:on     6:off
```

### (7) 复制生成 MySQL 服务器的配置文件

在 `/usr/share/mysql` 目录下,有 `my-huge.cnf`、`my-large.cnf`、`my-medium.cnf` 和 `my-small.cnf` 四个 MySQL 样本配置文件,可根据服务器自身的硬件配置情况,选择一个合适的使用。只需将其复制到 `/etc` 目录下,并更名为 `my.cnf` 即可,该配置文件用于设置 MySQL 服务器的一些全局环境变量,这些变量将影响 MySQL 服务器的性能。

`my-small.cnf` 配置文件适用于内存小于或等于 64MB 的服务器,`my-medium.cnf` 适用于内存为 32~64MB 的服务器,`my-large.cnf` 配置文件适用于内存为 512MB 及以上的服务器,`my-huge.cnf` 配置文件适用于内存为 1~2GB 的服务器使用,这类服务器一般主要运行 MySQL 服务。

假如当前 MySQL 服务器的内存为 1GB,则可使用 `my-huge.cnf` 文件作为 MySQL 服务器的配置文件,操作命令为:

```
[root@rh9 root]# cp /usr/share/mysql/my-huge.cnf /etc/my.cnf
```

若服务器配置比较高档,还可利用 `vi` 编辑器修改 `/etc/my.cnf` 配置文件,在 `[mysqld]` 段中添加 `max_connections` 全局环境变量,该变量用于设置 MySQL 服务器允许的最大并发连接数,默认为 100,若要设置最大并发连接数为 250,则在配置文件中添加如下行的内容:

```
set-variable = max_connections=250
```

在 `/usr/share/mysql` 目录下还有一个很重要的文件,其文件名为 `mysql.server`,该文件实质是 mysql 服务器的启动与停止脚本,与 `/etc/rc.d/init.d/mysql` 文件内容相同,若在 `/etc/rc.d/init.d` 目录下没有 mysql 启动脚本,则可通过更名复制 `mysql.server` 文件来生成。

## 2. 源代码安装方式

MySQL 的源代码包文件名为 `mysql-3.23.58.i386.tar.gz`,安装前应先解压,然后进

行配置、编译,最后再安装。Linux 使用 gcc 编译器实现对源代码进行编译,在编译前应确保当前 Linux 系统安装了 gcc 编译器,可使用命令 `gcc -v` 来检查,若输出了以下信息,则说明已安装。

```
gcc version 3.2.2 20030222 (Red Hat Linux 3.2.2-5)
```

利用源代码安装时,可指定安装位置,下面以将 MySQL 安装在 `/usr/local/mysql` 目录中为例,介绍 MySQL 的源代码安装方法。

### (1) 安装 MySQL 服务器

将 `mysql-3.23.58.i386.tar.gz` 源代码包下载或复制到 `/usr/local/src` 目录中,源代码中包含了 MySQL 的服务器和客户端程序的源代码,经过配置、编译之后,就可安装。

```
[root@rh9 root]# cd /usr/local/src
[root@rh9 src]# tar zxvf mysql-3.23.58.i386.tar.gz
[root@rh9 src]# cd mysql-3.23.58
[root@rh9 mysql-3.23.58]# groupadd -r mysql           # 创建 mysql 用户组
[root@rh9 mysql-3.23.58]# useradd -m -r -g mysql -d /var/lib/mysql -s /bin/bash \
> -c "MySQL Server" mysql                          # 创建 mysql 用户
[root@rh9 mysql-3.23.58]# ./configure --prefix=/usr/local/mysql \
> --sysconfdir=/etc --localstatedir=/var/lib/mysql --enable-local-infile
```

注: `--prefix` 配置项用于指定 `mysql` 的安装目录; `--sysconfdir` 用于指定 MySQL 配置文件的存放目录; `--localstatedir` 配置项用于指定 MySQL 的数据库存放目录; `--enable-local-infile` 用于激活 `load data local infile` 语句,使 MySQL 支持使用该语句。

```
[root@rh9 mysql-3.23.58]# make                      # 编译(需要较长时间)
[root@rh9 mysql-3.23.58]# make install               # 安装
```

### (2) 初始化系统数据库

使用源代码编译安装后,必须手工初始化系统数据库,其实现操作为:

```
[root@rh9 mysql-3.23.58]# cd /usr/local/mysql
[root@rh9 mysql]# ./bin/mysql_install_db             # 初始化系统数据库
[root@rh9 mysql]# ls /var/lib/mysql                  # 查看存放数据库的目录的内容
mysql test
```

### (3) 设置修改数据库目录的所有者

对 MySQL 的数据库存放目录及其下面的文件,必须设置其所有者为 `mysql` 账户,否则会因为 `mysql` 账户无法存取访问 `mysql` 数据库而无法启动 MySQL 服务。实现的操作命令为:

```
[root@rh9 mysql]# chown -R mysql:mysql /var/lib/mysql
```

若出现 MySQL 服务器无法启动的情况,可查看/var/lib/mysql 目录下面扩展名为 .err 的错误日志文件(如 rh9.err),该文件记录了服务器无法启动的原因。若未执行以上语句,MySQL 服务器将无法启动,此时的错误日志为:

```
040808 08:49:46 mysqld started
040808 8:49:46 /usr/local/mysql/libexec/mysqld: Can't find file: './mysql/host.frm' (errno:13)
040808 08:49:46 mysqld ended
```

host.frm 文件是 mysql 数据库中名为 host 的数据表的一个组成文件,此处的信息说明了 mysql 账户无法存取访问 host 数据表。

(4) 复制 MySQL 的配置文件到/etc 目录中,并更名为 my.cnf。操作命令为:

```
[root@rh9 mysql]# cp /usr/local/mysql/share/mysql/my-large.cnf /etc/my.cnf
```

(5) 复制生成 MySQL 服务器的启动与停止脚本

/usr/local/mysql/share/mysql/mysql.server 文件实质是 MySQL 服务器的启动和停止脚本,源代码安装方式不会自动将其安装到/etc/rc.d/init.d 目录下,需要手工操作,可将其复制到/etc/rc.d/init.d 目录下,并更名为 mysql。

```
[root@rh9 mysql]# cp /usr/local/mysql/share/mysql/mysql.server /etc/rc.d/init.d/mysql
```

(6) 将 mysql 服务添加到服务管理器中,并设置自启动状态

源代码安装方式不会自动添加 mysql 服务到服务管理器中,可采用如下命令添加。

```
[root@rh9 mysql]# chkconfig --list|grep mysql      # 查询当前是否有 mysql 服务
[root@rh9 mysql]# chkconfig --add mysql             # 添加 mysql 服务到服务管理器中
[root@rh9 mysql]# chkconfig --list|grep mysql       # 查询此时 mysql 服务的启动状态
mysql        0:off    1:off    2:on     3:off    4:on     5:off    6:off
[root@rh9 mysql]# chkconfig --level 35 mysql on     # 设置在 3、5 运行级别也自启动
[root@rh9 mysql]# chkconfig --list|grep mysql
mysql        0:off    1:off    2:on     3:on     4:on     5:on     6:off
```

(7) 启动 MySQL 服务器

启动 MySQL 服务器,实现命令如下:

```
service mysql start 或 /etc/rc.d/init.d/mysql start
```

停止 MySQL 服务器,实现命令如下:

```
service mysql stop 或 /etc/rc.d/init.d/mysql stop
```

输出以下提示信息,说明 MySQL 服务器启动成功,按回车可回到 Linux 的命令行提示符状态。

```
[root@rh9 mysql]# service mysql start
Starting mysqld daemon with databases from /var/lib/mysql
```

### (8) 测试 MySQL 服务器

MySQL 服务器启动成功后,在登录之前,可使用以下命令测试服务器能否正常登录和访问。

```
[root@rh9 mysql]# /usr/local/mysql/bin/mysqladmin version
Server version      3.23.58-log
Protocol version    10
Connection          Localhost via UNIX socket
UNIX socket         /tmp/mysql.sock
Uptime:             4 min 42 sec
```

若输出以上信息,则说明 MySQL 服务器能正常登录。另外,也可使用以下命令来测试 MySQL 服务器是否已启动。

```
[root@rh9 mysql]# /usr/local/mysql/bin/mysqladmin ping
mysqld is alive
```

### (9) 设置 root 账户密码

刚安装的 MySQL 服务器其 root 账户密码未设置,直接使用 `mysql -u root` 命令就可登录,没有安全可言,因此一定要设置该账户的密码,其设置方法与前面相同。

由于是将 MySQL 安装在 `/usr/local/mysql` 目录中,因此 `mysql` 的实用程序均位于 `/usr/local/mysql/bin` 目录中,而利用 RPM 软件包安装时,默认实用程序是安装在 `/usr/bin` 目录中的,应注意区分。

设置好密码后,就可使用以下命令登录访问 MySQL 服务器了。

```
[root@rh9 mysql]# /usr/local/bin/mysql -u root -h localhost -p
```

此处将 MySQL 安装在 `/usr/local/mysql` 目录中,这有助于对文件进行归类管理,但这样做又使得 MySQL 的库文件和头文件被安装到了非标准的位置。由于在编译 PHP 源代码时,会使用到部分 MySQL 的库文件和头文件,若服务器还需提供 PHP 动态网页服务,会导致找不到相应的文件,解决的办法是为目录创建一个符号链接,其实现的操作命令如下:

```
[root@rh9 mysql]# ln -s /usr/local/mysql/lib/mysql /usr/lib/mysql
[root@rh9 mysql]# ln -s /usr/local/mysql/include/mysql /usr/include/mysql
```

## 7.1.3 MySQL 管理基础

MySQL 具有十分优秀的数据库服务功能,并支持标准的 SQL 语句,利用 SQL 语句、

MySQL 的命令和函数,可实现强大的数据库操作。对于 MySQL 数据库管理员,了解并掌握常用的 MySQL 操作与维护命令是必要的,本节将简单介绍 MySQL 的常用操作、维护与管理命令。

### 1. MySQL 的命令特点

MySQL 的命令和函数不区分大小写,在 Linux/UNIX 平台,数据库、数据表、用户名和密码要区分大小写。

MySQL 的命令以分号或\g 作为命令的结束符,因此,一条 MySQL 命令可表达成多行。若键入 MySQL 命令忘了在末尾加分号,按回车键后,此时的操作提示符将变为以下形式:

—>

该提示符表示系统正等待接收命令的剩余部分,此时输入分号并回车,系统就可执行所键入的命令了。

### 2. MySQL 的数据类型

若要创建数据表,则必须了解 MySQL 可使用的数据类型,以及这些类型的表达方法。

MySQL 支持的数据类型较多,对数据类型也分得比较细,总体上可分为三大类,即数值型、日期时间型和字符串类型。

#### (1) 数值类型

在 MySQL 中,属于数值型的数据类型有 8 种,分别是 tinyint、smallint、mediumint、int、bigint、float、double、decimal。

#### (2) 日期和时间类型

日期和时间类型在 MySQL 中细分为 5 种具体的类型,分别是 date、datetime、timestamp、time 和 year 类型。

#### (3) 字符串类型

MySQL 的字符串类型细分为 8 种具体的数据类型,常用的主要是 char、varchar、tinyblob 或 tinytext、blob 或 text、mediumblob 或 mediumtext、longblob 或 longtext、enum、set。

### 3. MySQL 常用操作命令

#### (1) 登录与注销

登录 MySQL,使用如下命令:

```
mysql -u 用户名 -h 服务器主机名或 IP 地址 -p 密码
```

断开与 MySQL 服务器的连接,使用如下命令: quit 或 exit。

## (2) 查询数据库与数据表

查询当前服务器中有哪些数据库,使用命令: show database;

选择所使用的数据库,使用命令: use 数据库名;

显示当前数据库中有哪些数据表,使用命令: show tables;

显示数据表的结构信息,使用命令: describe 数据表名。

## (3) 数据库操作

① 创建数据库,使用命令: create database 数据库名称;

② 在数据库中创建数据表,使用 create table 命令,命令用法:

```
create table 表名(字段名1 字段类型[(宽度[.小数位数])] [,字段名2 字段类型[(宽度[.小数位数])]...);
```

说明: [ ] 所括的部分为可选项。用法如下所示。

```
mysql>create table Customer (name varchar(10),sex char(2),company varchar(60),  
-->work varchar(20),mony double(9,2),checkout date);
```

## ③ 向表添加记录

- 成批添加记录 将要添加的数据保存在一文本文件中,一行为一条记录的数据,各数据项间用 Tab 定位符分隔,空值项用 \N 表示。然后利用 MySQL 的 load data 命令将文本文件中的数据自动添加到指定的数据表中。命令用法:

```
mysql>load data local infile "文本文件名" into table 数据表名;
```

- 一次添加一条记录 使用 insert into 可实现向数据表添加一条记录的功能,语句用法:

```
insert into 表名 [( '字段名1,字段名2,...,字段名n) ] values(值1,值2,...,值n);
```

## ④ 查询数据使用 select 语句,语句用法:

```
select 字段列表/* from 表名 [where 检索条件] [order by 排序关键字段 [ASC/ DESC]] [group  
by 分类关键字段];
```

## ⑤ 修改数据,使用 update 语句,语句用法:

```
update 表名 set '字段名1 新值1[,字段名2=新值2...]' [where 条件表达式];
```

## ⑥ 删除数据,使用 delete 语句,语句用法:

```
delete from 表名 where 条件表达式;
```

## ⑦ 删除数据表与数据库

- 删除数据表,使用命令: drop table 数据表名;

- 删除数据库,使用命令: drop database 数据库名。

#### (4) mysqladmin 命令

mysqladmin 是一个功能很强大的数据库管理工具,其功能是通过一系列特定的命令行参数来实现的,比如 password、flush-privileges、shutdown、extended-status 等。mysqladmin 命令默认使用 root 用户身份来运行后面所指定的命令,在执行前,mysqladmin 命令会试着用 root 用户登录连接 MySQL 服务器,登录成功后,再自动执行后面命令行参数所代表的操作。当 root 用户有密码时,在 mysqladmin 命令行中必须增加使用 -p 参数,以便能正确登录服务器。下面介绍该命令常用的一些命令行参数及其用法。

##### ① password 用于设置或修改用户密码。

若当前 root 用户的密码为 snbj0814 # %baby,现要更改为 mybaby0814,则操作命令为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysqladmin -u root -h rh9 -psnbj0814 # %baby \
> password 'mybaby0814'
[root@rh9 root]# /usr/local/mysql/bin/mysqladmin -u root -h localhost \
> -psnbj0814 # %baby password 'mybaby0814'
[root@rh9 root]# /usr/local/mysql/bin/mysqladmin -u root -psnbj0814 # %baby \
> flush-privileges # 由于刚才设置的密码还未生效,故仍使用原密码
```

② flush-privileges 用于刷新用户权限表。当添加或删除了用户,设置或修改了用户密码以及用户的权限后,应让系统重新装载权限表,以使修改立即生效。其用法为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysqladmin -u root -p flush-privileges
Enter password: # 输入 root 用户登录 MySQL 服务器的密码
```

##### ③ shutdown 用来关闭 MySQL 数据库服务器。

比如要利用 mysqladmin 命令来停止 MySQL 服务器,则操作命令为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysqladmin -u root -psnbj0814 # %baby shutdown
040808 18:21:12 mysqld ended # 说明执行成功,服务被停止
```

##### ④ extended status 用于显示 MySQL 服务器的运行状态统计信息。

```
[root@rh9 root]# /usr/local/mysql/bin/mysqladmin -u root -pmybaby0814 \
> extended-status | less
```

## 4. MySQL 的用户与权限管理

MySQL 数据库服务器具有很高的安全性,但这种高安全性是需要对用户账户和用户权限进行合理设置的。mysql 数据库是 MySQL 服务器的系统数据库,用于存储用户账户和账户的权限设置,该数据库中有 columns\_priv、db、func、host、tables\_priv 和 user

六个数据表。

### (1) MySQL 的用户及权限表

MySQL 的用户账户及对应的权限保存在 mysql 数据库的相关数据表中,根据权限作用范围的不同,MySQL 的用户权限级别分为全局权限、数据库级别权限、表权限和列权限四种。

① 全局权限作用于当前服务器上的所有数据库,该种权限存储在 user 数据表中,即 user 数据表中的用户及其权限设置,是全局性的,对所有数据库和数据表均有效。

查看 user 数据表的结构可使用 describe user 命令,其表结构如图 7.2 所示,除了前 3 个字段外,后面 14 个字段均用于设置该用户在某方面的权限,其值为 Y 或 N,代表用户有或无这方面的权限,默认值为 N,各字段所代表的权限及含义如表 7.1 所示。

```
mysql> describe user;
```

Field	Type	Null	Key	Default	Extra
Host	char(60) binary		PRI		
User	char(16) binary		PRI		
Password	char(16) binary				
Select_priv	enum('N','Y')			N	
Insert_priv	enum('N','Y')			N	
Update_priv	enum('N','Y')			N	
Delete_priv	enum('N','Y')			N	
Create_priv	enum('N','Y')			N	
Drop_priv	enum('N','Y')			N	
Reload_priv	enum('N','Y')			N	
Shutdown_priv	enum('N','Y')			N	
Process_priv	enum('N','Y')			N	
File_priv	enum('N','Y')			N	
Grant_priv	enum('N','Y')			N	
References_priv	enum('N','Y')			N	
Index_priv	enum('N','Y')			N	
Alter_priv	enum('N','Y')			N	

17 rows in set (0.01 sec)

图 7.2 user 数据表结构

表 7.1 user 表权限字段及其含义

字段名	字段值	代表的权限	含义描述	权限类别
Select_priv	Y 或 N	select	是否允许使用 select 语句检索数据	数据库,数据表操作类权限
Insert_priv	Y 或 N	insert	是否允许向数据表添加记录	
Update_priv	Y 或 N	update	是否允许更新修改表中数据	
Delete_priv	Y 或 N	delete	是否允许删除表中记录	
Create_priv	Y 或 N	create	是否允许创建数据库或数据表	
Drop_priv	Y 或 N	drop	是否允许删除数据库或数据表	
Index_priv	Y 或 N	index	是否允许创建或删除索引	
Alter_priv	Y 或 N	alter	是否允许使用 alter table 语句修改表结构	



续表

字段名	字段值	代表的权限	含义描述	权限类别
Reload_priv	Y 或 N	reload	是否允许重载权限表(flush-privileges)	管理类权限, 允许用户控制服务器的某些动作, 对安全影响很大, 应慎重授权
Shutdown_priv	Y 或 N	shutdown	是否允许停止 MySQL 服务器(shutdown)	
Process_priv	Y 或 N	process	是否允许查看或结束服务器进程	
File_priv	Y 或 N	file	是否允许在服务器上进行文件读写操作	
Grant_priv	Y 或 N	grant	是否允许将该用户的权限授予给别的用户	
References_priv	Y 或 N	references	保留未用	

Host 字段的值为主机名或 IP 地址, 允许使用“%”和“\_”通配符, 用于指定该用户可以从哪台或哪些主机登录访问 MySQL 服务器。比如 192.168.168.% , 代表可以从 192.168.168 网段的任何一台主机登录访问, 另外也可用“网段/子网掩码长度”来表示, 如表示为 192.168.168.0/24。Host 字段值为“%”或空, 则表示可从任何一台主机登录; 若设置为 192.168.168.154, 则表示该用户只能从 IP 地址为 192.168.168.154 的主机登录访问。

User 字段用于存储用户账户, 用户名最多 16 个字符。该字段的值若为空白, 则代表任意用户, 登录时任意指定的用户均可与该字段值匹配, 利用该方法可实现匿名登录访问 MySQL 服务器。比如 Host 字段值为 192.168.168.% 或 192.168.168.0/24, User 字段的值为空白, password 字段的值也为空白, 则 192.168.168 网段中的主机用户, 都可使用“mysql -u 任意的一个用户名”来实现匿名登录 MySQL 服务器。

默认的用户数据表中有两条记录的用户和 Password 字段的值均为空白, 主机名分别为 localhost 和 rh9(当前服务器的主机名), 该记录用于支持匿名登录。若要禁止匿名登录, 可使用以下语句将其删除。

```
mysql>delete * from user where user="" and password="";
```

Password 字段用于存储用户的密码, 其值是经过加密后所得到的值, 不是原始的密码。若该字段的值为空白, 则代表登录时不使用密码。

这三个字段的值用于登录连接 MySQL 服务器时, 进行用户身份的验证。验证时不仅要验证用户名和密码, 同时还要验证登录所用的主机与 Host 字段的设定是否匹配。

当有连接请求时, MySQL 会对 user 数据表按 Host 字段和 User 字段进行排序, Host 为主排序关键字, 当有两条记录的 Host 字段值相同时, 再按 User 字段进行排序。排序的先后顺序是最具体的主机名或 IP 地址排在前面, 不太明确或不太具体的排在后, 最不明确的“%”一般排在最后。然后再从头开始查找并使用第一个与主机匹配的记录,

并利用该条记录进行用户名与密码的校验。若没有与主机匹配的记录,将显示类似以下的错误信息,提示该主机不允许连接 MySQL 服务器。

```
ERROR 1130: Host '192.168.168.65' is not allowed to connect to this MySQL Server.
```

管理类权限不要轻易授权给普通用户,否则将给服务器的安全带来很大的隐患。

reload 权限允许用户通过执行 `mysqladmin flush-privileges` 命令来重载权限表。

shutdown 权限允许用户通过执行 `mysqladmin shutdown` 命令来停止 MySQL 服务器。

process 权限允许用户查看或结束进程。

file 权限允许用户在服务器上进行文件操作,一切允许读或写的文件,均可以读写。比如一个具有 file 权限的用户,可以完成以下操作:

```
Create table mypass (pwd text);  
load data infile "/etc/passwd" into table mypass;  
select * from mypass;
```

通过以上操作,就可获得 Linux 系统的用户列表,因此安全隐患很大,一定要慎重授权。

grant 权限允许用户对别的用户授权,授权范围为该用户所拥有的权限(包括 grant 权限本身)。若有两个权限不同的用户,但其中某个用户有 grant 权限,则他们可互相实现权限合并,因此,这是一个极其危险的权限,不要轻易授权。

另外,alter 权限虽不属于管理类权限,但也不要轻易授权,否则用户可通过更改表名来颠覆原来的权限设置。

② 数据库权限作用于一个指定的数据库中的所有数据表。数据库权限存储在 db 数据表中,db 表决定用户能从哪台主机存取访问哪个数据库,对数据库具有哪些访问权限。

具有数据库级别权限的用户,除了在 db 表中的相关记录外,在 user 表中也有记录,该用户的密码信息仍是存储在 user 表中的,只不过该用户没有全局权限。

若要让用户能从多台主机存取访问某数据库,此时可在 db 数据表中,让 Host 字段的值为空白,然后在 host 数据表中,添加允许访问该数据库的主机名。host 表常与 db 表配合使用。

db 表和 host 表的结构如图 7.3 和图 7.4 所示。

③ 表权限作用于一个指定表的所有列,该种权限存储在 tables\_priv 数据表中。

④ 列权限作用于一个指定表的单个列,该种权限存储在 columns\_priv 数据表中。

## (2) 用户的创建与权限管理

创建用户与设置用户的权限可同时完成,也可单独设置或修改。对用户权限的设置,MySQL 提供了 grant 和 revoke 命令,grant 用于创建和设置用户的权限,revoke 则用于

```
mysql> describe db;
```

Field	Type	Null	Key	Default	Extra
Host	char(60) binary		PRI		
Db	char(64) binary		PRI		
User	char(16) binary		PRI		
Select_priv	enum('N','Y')			N	
Insert_priv	enum('N','Y')			N	
Update_priv	enum('N','Y')			N	
Delete_priv	enum('N','Y')			N	
Create_priv	enum('N','Y')			N	
Drop_priv	enum('N','Y')			N	
Grant_priv	enum('N','Y')			N	
References_priv	enum('N','Y')			N	
Index_priv	enum('N','Y')			N	
Alter_priv	enum('N','Y')			N	

13 rows in set (0.00 sec)

图 7.3 db 数据表结构

```
mysql> describe host;
```

Field	Type	Null	Key	Default	Extra
Host	char(60) binary		PRI		
Db	char(64) binary		PRI		
Select_priv	enum('N','Y')			N	
Insert_priv	enum('N','Y')			N	
Update_priv	enum('N','Y')			N	
Delete_priv	enum('N','Y')			N	
Create_priv	enum('N','Y')			N	
Drop_priv	enum('N','Y')			N	
Grant_priv	enum('N','Y')			N	
References_priv	enum('N','Y')			N	
Index_priv	enum('N','Y')			N	
Alter_priv	enum('N','Y')			N	

12 rows in set (0.00 sec)

图 7.4 host 数据表结构

撤销用户的某些授权。另外,也可利用 insert into 或 update 语句,直接通过修改用户权限表来实现。

#### ① grant 命令

命令用法:

```
grant priv_type [(column_list)] [, priv_type [(column_list)] ...]
on {tbl_name | *.* | db_name.*}
to username [identified by 'password'] [, username [identified by 'password'] ...]
[with grant option];
```

参数说明:

priv\_type 代表要授予给用户的权限列表,各权限名称之间用逗号分隔。其中,all 与 all privileges 同义,代表全部权限,usage 代表没有权限,即全部权限均没有。

column\_list 是要设置权限的列的列表,为表中的列设置权限。列权限只有 select、insert、update 和 references。各权限级别所允许的权限种类,可通过查看相应的权限表的结构来获得。

on 子句用于指定权限的级别类型。\*. \* 代表任意数据库中的任意数据表,代表全局权限;db\_name. \* 代表某数据库中的全部数据表,即代表设置数据库级别的权限;tbl\_name 代表要设置权限的某数据表,即用于设置表级别的权限。

to 子句用于指定为哪一个或哪几个用户设置该权限,to 后面可同时指定多个用户,各用户间用逗号分隔。在用户名之后,可利用 identified by 'password' 子句设置该用户的密码,其中的 password 代表密码的明文,grant 语句会自动对密码进行加密存储。若指定的用户不存在,则会自动创建该用户,另外,在指定用户时,采用“用户名@主机名”的格式指定,在创建用户时,@后面的主机名将存入到 Host 字段中。

with grant option 子句用于为用户设置 grant 权限。

[例 7.1] 试创建一个名为 webadmin 的用户,该用户只允许在服务器本地机上登录,有 select、insert、update 和 delete 的全局权限,用户密码为 purelove0814。

实现的操作命令为:

```
mysql> grant select,insert,update,delete on *. * to webadmin@localhost \
--> identified by 'purelove0814';
```

执行该命令后,若指定的用户不存在,则会自动创建,若已存在,则会授予相应的权限。grant 命令所设置的权限立即生效。

若要查询所创建的用户及相关字段的内容,可使用以下命令:

```
mysql> select host,user,password,select_priv,insert_priv,update_priv,delete_priv from user \
--> where user='webadmin';
```

以上操作也可使用 insert into 语句通过直接操作 user 权限表来实现,其实现命令为:

```
mysql> insert into user (host,user,password,select_priv,insert_priv,update_priv,delete_priv) \
--> values('localhost','webadmin',password('purelove0814'),'Y','Y','Y','Y');
mysql> flush privileges;
```

使用 insert into 或 update 语句在权限表中添加记录或修改记录的权限设置后,不会立即生效,需要使用 flush privileges 语句让系统重新装载权限表后,才能生效。flush privileges 命令让 MySQL 重新装载用户权限数据表中的设置,该命令在 mysql> 状态下执行。另外,在 Linux 的命令行状态下,利用 mysqladmin 命令结合 flush-privileges 参数,也可实现相同的功能。

```
mysql>quit
[root@rh9 root]# /usr/local/mysql/bin/mysql u webadmin -ppurelove0814
mysql>                                     #新建用户登录成功
```

当在 p 参数后指定登录密码时, p 与密码之间不要留空格。

若要为 webadmin 账户授予全部权限, 则实现的操作命令为:

```
mysql>grant all on *.* to webadmin@localhost with grant option;
```

执行该语句后, webadmin 账户就拥有了与 root 账户相同的权限。注意以上语句需以 root 账户身份登录后才能执行成功。

**[例 7.2]** 试创建一个名为 news 的数据库, 然后创建一个 webshow 用户和 webup 用户, webshow 仅对 news 数据库有 select 权限, webup 用户仅对 news 数据库有 select、insert、update 和 delete 权限, 两个用户只允许在服务器本地机上登录。webshow 用户的密码为 RxO% \* 24361, webup 用户的密码为 Qj # 354Rzt。

实现的操作命令为:

```
mysql>create database news;
mysql>grant select on news.* to webshow@localhost identified by 'RxO% * 24361';
mysql>grant select,insert,update,delete on news.* to webup@localhost \
-> identified by 'Qj # 354Rzt';
mysql>select host,user,password,select_priv,insert_priv,update_priv,delete_priv from user;
mysql>select host,db,user, select_priv,insert_priv,update_priv,delete_priv from db;
```

另外, 也可直接使用 insert into 语句, 分别在 user 和 db 表中添加用户记录来实现数据库级别的授权。从授权后的查询输出可知, 拥有数据库权限的用户, 在 user 表中也有记录, 只不过没有全局权限, 其数据库权限是记录在 db 表中的。

## ② revoke 命令

revoke 命令用于撤销授予用户的某些权限, 可同时撤销多个用户的权限。其命令用法为:

```
revoke priv_type [(column_list)] [, priv_type [(column_list)] ...]
on {tbl_name | *.* | db_name.*} from username [, username ...];
```

若要全部撤销授予给 webadmin 用户的权限, 则实现的操作命令为:

```
mysql>revoke all on *.* from webadmin@localhost;
mysql>select * from user where user='webadmin';
```

从查询输出可知, 用户权限被全部撤销后, 该用户的记录不会被删除, 此时该用户仍可以登录 MySQL 服务器, 但无法进行数据库操作。

## 5. MySQL 数据的导入与导出

作为数据库管理员,对数据库数据进行导入导出等备份操作是经常的事,为此,MySQL 也提供了用于数据导出的 `mysqldump` 命令,对备份数据的恢复(导入),仍使用 `mysql` 程序来实现。

命令用法:

```
mysqldump [options_ database_name [table_name]
```

命令功能:将指定的数据库或数据库表的数据导出。该命令将数据转换成 SQL 语句(一系列创建库和表结构的 `create` 语句和用于向表添加数据的 `insert into` 语句),然后输出到标准的输出设备(显示器)。因此在导出数据时,通常与“>”定向输出符配合使用,以实现将数据导出到指定的文件中。

参数说明:

`database_name` 要导出备份的数据库,若缺省 `tables_name`,则导出整个数据库。

`table_name` 要导出备份的数据库表名。

`options` 参数项较多,可使用 `mysqldump -help` 命令查看,下面仅介绍几个常用的选项:

`--add-drop table` 在每个 `create` 语句之前增加一个 `drop table`。

`--add-locks` 在每个表导出之前增加 `lock table`,在完成之后添加 `unlock table`。

`--opt` 与 `--quick` 同义,将数据直接导出。默认情况下, `mysqldump` 会将全部数据先装载到内容中,然后再导出。如果要导出的数据库很大,会导致内存不够,通常使用该参数。

`-t` 与 `--no-create-info` 同义,在导出数据时,不导出表结构信息,即不添加 `create table` 语句。使用该参数后,所导出的内容仅有表数据,无表结构信息。

`-d` 与 `--no-data` 同义,在导出数据时,不导出表数据,仅有表结构信息。

例如,要将名为 `webdata` 的数据库整体导出备份为 `/root/database_bak/webdata_bak.sql`,则实现的操作命令为:

```
[root@rh9 root]# mkdir database_bak
[root@rh9 root]# /usr/local/mysql/bin/mysqldump -u root -p --add-drop-table \
> --opt webdata > /root/database_bak/webdata_bak.sql
[root@rh9 root]# ll /root/database_bak/webdata_bak.sql
```

若数据库很大,导出时可进行压缩处理,实现命令为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysqldump -u root -p --add-drop-table \
> --opt webdata | gzip > /root/database_bak/webdata_bak.sql.gz
```

若要将全部数据库导出备份,则实现的操作命令为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysqldump -u root -p --add-drop-table \  
> --opt --all databases > /root/database_bak/alldatabases.sql
```

若要仅导出备份 webdata 数据库中的 news 数据表,则实现的命令为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysqldump -u root -p --add-drop-table \  
> --opt webdata news > /root/database_bak/webdata_tbl_news.sql
```

导出备份文件中的内容全部是 SQL 语句,只需利用标准输入重定向符“<”将其输入给 mysql 程序执行,即可恢复出原数据库、数据表以及表中的记录内容。其命令格式为:

```
# mysql -u root -p database_name < backupfilename.sql
```

例如,要从备份文件 webdata\_tbl\_news.sql 中恢复 news 数据表,则实现的操作命令为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysql -u root -p webdata < webdata_tbl_news.sql
```

## 7.2 安装与配置 Web 服务器

Web 服务是目前 Internet 应用最流行、最受欢迎的服务之一, Linux 平台使用最广泛的 Web 服务器是 Apache,它是目前性能最优秀、最稳定的 Web 服务器之一。

Apache 1.3 与 Apache 2.0 在安装和配置上存在很大的差异, Apache 2.0 在功能上得到了很大的增强,新增了一些实用的功能模块(如 mod\_ssl、mod\_dav、mod\_deflate 等),并简化了部分配置,本节以最新的 Apache 2.0 为例,介绍 Apache Web 服务器的安装与配置方法,及支持动态网页的 PHP 解释器的安装与配置方法。

### 7.2.1 安装 Apache 服务器

对 Apache Web 服务器的安装,同样可采取 RPM 软件包安装和源代码安装两种方式,另外也可在 Linux 的图形界面,利用软件包管理器来自动安装 Apache 服务器和相关的软件包,该安装方式实质仍属于 RPM 软件包安装方式。

RPM 软件包将配置文件和实用程序安装在固定位置,不需要编译;源代码安装需要先配置、编译,然后再安装,但可选择要安装的模块和安装路径。

Red Hat Linux 9 安装光盘自带 Apache 服务器的 RPM 软件包,其版本为 2.0.40-21,如果在安装 Linux 时已选择安装 Apache,则可以直接配置使用。另外,也可到官方网站下载安装最新的 Apache 软件包。Apache 的最新源代码安装包可到 <http://www.apache.org> 网站下载; Apache 的 RPM 软件包可到 <http://updates.redhat.com> 网站

下载。

### 1. 利用软件包管理器安装

若当前 Linux 系统安装了 X-Windows 图形界面系统,则可利用软件包管理器来直接安装 Apache Web 服务器,同时还可安装与 Web 服务应用紧密相关的 PHP 解释器、Perl 解释器和支持 PHP 访问连接 MySQL 数据库的软件包,该安装方式简单直观。

启动进入 Linux 的图形界面,依次单击“红帽子”→System Settings→Add/Remove Applications,打开 Linux 的软件包管理器,然后在 Servers 栏目中选中 Web Server 服务,然后单击右边的 Details,打开 Web Server 服务软件包的详细选项,其中的 standard packages 用于安装 Apache 服务器,extra packages 选项用于安装与 Web 服务紧密相关的 PHP、Perl 和 MySQL 的支持包,单击 extra packages 左边的箭头,展开选项列表,一般可选择安装 mod\_auth\_mysql、mod\_perl、php、php\_mysql 和 php\_odbc 等软件包,如图 7.5 所示。

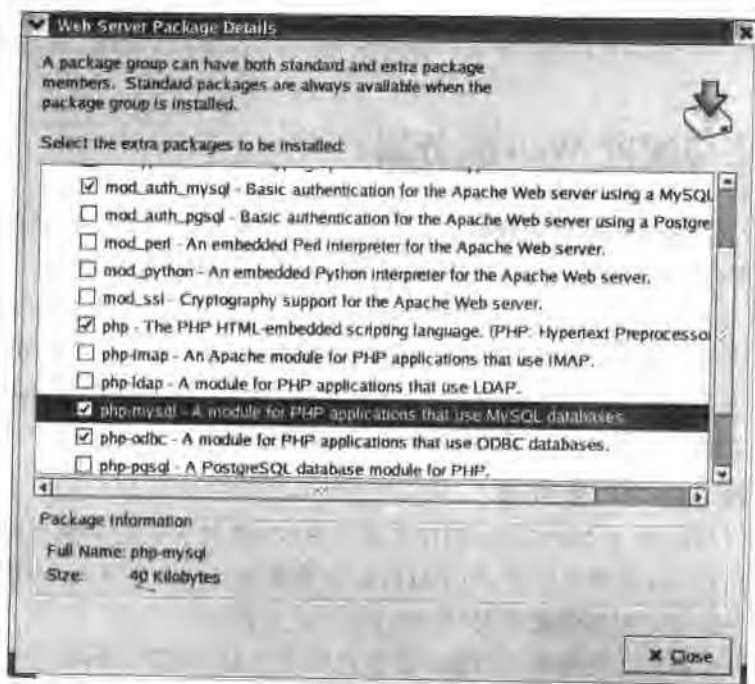


图 7.5 选择安装与 Web 服务相关的 PHP 和 MySQL 支持包

软件包安装过程中,将提示插入相应的 Red Hat Linux 9 安装光盘到光驱中。安装完成后,可在 System tools 下面选择 terminal,启动虚拟终端,然后在虚拟终端中设置 Apache 服务在 2、3、5 运行级别的自动启动。



```
[root@rh9 root]# chkconfig --level 235 httpd on
[root@rh9 root]# chkconfig --list httpd      # 查询该服务的启动状态
httpd 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

重新启动 Linux 系统,或使用以下命令立即启动 Apache 服务。

```
[root@rh9 root]# service httpd start
```

单击“红帽子”→Internet→Mozilla Web Browser,启动 Linux 的浏览器,然后在地址栏键入 `http://127.0.0.1` 或 `http://localhost`,若能看到如图 7.6 所示的页面,则说明 Apache 服务器启动成功,工作正常。图 7.6 所示的页面,是 Apache 安装后在默认 Web 站点中的默认主页。

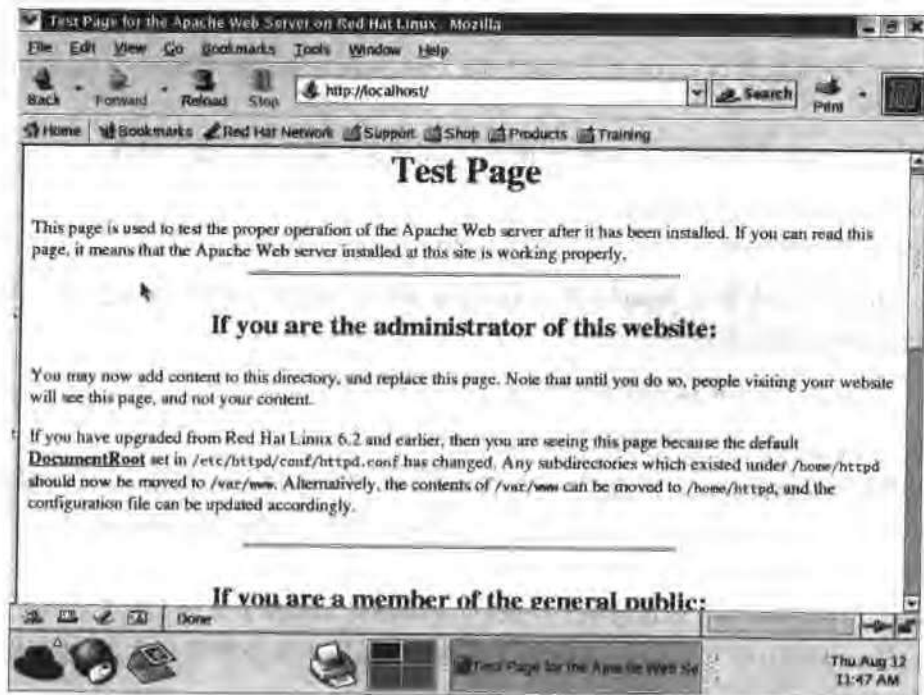


图 7.6 访问 Apache 服务器默认站点

## 2. 利用 RPM 软件包安装

专门用作服务器的 Linux 系统一般不安装 X-Windows 图形界面,因此,作为 Linux 系统管理员,还必须掌握直接利用 RPM 软件包和源代码来安装 Apache Web 服务器的方法。

### (1) 查询 Apache 服务是否安装

在安装 Apache 服务器软件包之前,可先查询一下当前 Linux 系统,看是否已安装了

该软件包。

```
[root@rh9 root]# rpm -q httpd
httpd-2.0.40-21
```

若有输出信息,则说明 Apache 服务已经安装,其版本号为 2.0.40-21。

```
[root@rh9 root]# chkconfig --list httpd           # 查询该服务的启动状态
httpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Apache 服务器安装后,默认情况下不会自动启动。

### (2) 安装 Apache RPM 软件包

若经查询当前 Linux 系统还未安装或者要强制安装 Apache 服务器,则可使用以下方法来安装。

首先将 RPM 软件包 httpd-2.0.40-21.11.i386.rpm 下载或复制到 /root/mylinuxsoft 目录中。

若当前 Linux 系统未安装 Apache 服务器,则可采用以下命令进行安装。

```
[root@rh9 root]# cd mylinuxsoft
[root@rh9 mylinuxsoft]# rpm -ivh httpd-2.0.40-21.11.i386.rpm
```

若当前系统已安装了 Apache 服务器,也可采用以下命令来进行升级安装。升级安装会保留原来的配置文件。

```
[root@rh9 mylinuxsoft]# rpm -Uvh httpd-2.0.40-21.11.i386.rpm
```

### (3) Apache 软件包安装位置

采用图形界面的软件包管理器,或者直接采用 RPM 软件包来安装 Apache 服务器,软件包会将 Apache 服务器的配置文件、日志文件和实用程序安装在固定的目录下,下面对此作一个简单的介绍。

/etc/httpd/conf      该目录用于存放 Apache 服务器的配置文件 httpd.conf。

/etc/rc.d/init.d/      Apache 服务器的服务启动脚本安装在该目录下,其文件名为 httpd。

/var/www/html      该目录为 Apache 服务器默认的 Web 站点根目录。网站的网页文件及其相关文件可放在该目录下。

/usr/bin      Apache 软件包提供的可执行程序安装在该目录下。

/etc/httpd/logs      Apache 服务器默认情况下,将日志文件(access\_log 和 error\_log)放在该目录下。

有关 Apache 服务器配置文件中各配置项的功能与含义将在后面部分详细介绍。

### (4) 启动和关闭 Apache 服务器

Apache RPM 软件包安装后会自动在 `/etc/rc.d/init.d` 目录下创建 Apache 服务器的启动脚本 `httpd`, 可使用以下方法来对 Apache 服务进行管理。

启动 Apache 服务器, 实现命令: `service httpd start`

重启 Apache 服务器, 实现命令: `service httpd restart`

重新装载 `httpd.conf` 配置文件的内容, 让修改在不重启服务器进程的情况下立即生效, 实现命令为: `service httpd reload`

停止 Apache 服务器, 实现命令: `service httpd stop`

### 3. 利用源代码安装 Apache 服务器

#### (1) Apache 模块简介

Apache 是一个模块化的 Web 服务器, 其内核仅包含了最基本最常用的功能模块, 默认情况下, 只有 `base` 组的模块被编译进了服务器, 扩展功能由其他模块提供, 需要在编译配置时, 指定所要使用的功能模块。

Apache 对模块的使用有两种方法, 一种是将其永久性地编译进 Apache 内核中, 即采用静态编译; 另一种是采取动态编译, 将其编译成 DSO (dynamic shared object, 动态共享对象) 模块, DSO 模块的存储是独立于内核的, 可被内核在需要时调用, 具体是由 `mod_so` 模块提供的运行时刻配置指令 (`LoadModule`) 来实现的, 若在编译中包含有任何动态模块, 则 `mod_so` 模块会被自动包含进内核。若仅希望内核能够支持装载 DSO 模块, 但不实际编译任何动态模块, 则在编译配置时应明确指定 `--enable-so` 配置参数。

除了标准模块组外, Apache 2.0 还提供了多道处理模块 MPMs (multi-processing modules), 编译过程中必须包含一个且只能有一个 MPM, 编译时系统会根据平台类型自动选择使用默认的 MPM, 也可在 `configure` 命令行中, 利用以下配置项指定。

`--with-mpm=Name`

其中 `Name` 为要使用的 MPM 类型。Linux/UNIX 平台为 `Prefork`, Windows 平台为 `mpm_winnt`。

有关 Apache 可使用的模块和 MPM 可使用类型的更详细介绍, 可访问官方网站 <http://httpd.apache.org/docs-2.0/mod/>。

#### (2) 模块的指定方法

在编译配置时, 可指定所要额外使用的模块以及该模块的编译使用方法。

##### ① 静态编译模块到内核中

`--enable-MODULE`

`MODULE` 代表要编译并包含的模块名称。在 <http://httpd.apache.org/docs-2.0/mod/> 页面, 显示了 Apache 可使用的模块, 此处的 `MODULE` 应是文档中的模块名去掉 `mod_` 后的名称。比如要编译包含 `mod_rewrite` 模块, 则指定方法为: `--enable-rewrite`。

--enable-modules=MODULE-LIST 方法用于指定要编译并包含的多个模块。其中的 MODULE-LIST 为模块列表,各模块名间用空格分隔。比如要编译包含 mod\_ssl 和 mod\_rewrite 模块,则指定方法为:

```
./configure --enable-modules="ssl rewrite"
```

或者表达为:

```
./configure --enable-ssl --enable-rewrite
```

## ② 动态编译模块为 DSO

```
--enable-MODULE=shared
```

MODULE 代表要编译的模块名。例如:--enable-rewrite=shared。

```
--enable-mods-shared=MODULE-LIST
```

将模块列表(MODULE-LIST)中的模块编译为 DSO 模块。

另外,若要排除或禁用可能被编译并包含的模块,则可使用--disable-MODULE。

## (3) 安装 Apache 服务器

从 Apache 的官方网站 <http://httpd.apache.org> 下载 Apache 的源代码软件包。目前最新版本的软件包为 httpd-2.0.50.tar.gz,将其下载或复制到/usr/local/src 目录中,然后采用以下步骤和方法进行配置、编译和安装。

mod\_deflate 模块是 Apache 2.0 新增的一个模块,该模块允许支持此功能的浏览器,在请求的页面内容发送前进行压缩,以节省网络带宽,编译时可将该模块编译进内核中。

mod\_vhost\_alias 模块支持虚拟主机的动态配置,可编译进内核中。

```
[root@rh9 root]# cd /usr/local/src
[root@rh9 src]# tar -zxvf httpd-2.0.50.tar.gz
[root@rh9 src]# cd httpd-2.0.50
[root@rh9 httpd-2.0.50]# ./configure --prefix=/usr/local/apache2 --enable-so \
> ..with-mpm=prefork --enable-modules="setenvif rewrite deflate vhost_alias"
[root@rh9 httpd-2.0.50]# make                # 编译,将耗时约 7 分钟左右
[root@rh9 httpd-2.0.50]# make install        # 安装
```

采用源代码安装方式,与 Apache 软件包相关的文档均安装在了指定的/usr/local/apache2 目录下面。其中,Apache 的配置文件存放在/usr/local/apache2/conf 目录下面;HTML 网页文件存放在/usr/local/apache2/htdocs 目录中,它是默认 Web 站点的根目录,该目录可通过配置文件 httpd.conf 进行设置或更改;日志文件存放在/usr/local/apache2/logs 目录中;CGI 脚本存放在/usr/local/apache2/cgi-bin 目录中;Apache 提供的实用程序、Apache 的 httpd 守护进程程序(httpd)和 Apache 服务器启动脚本(apachectl)均存放在/usr/local/apache2/bin 目录中,执行以下命令可查看目前已包含在

httpd 程序中的模块。

```
[root@rh9 root]# /usr/local/apache2/bin/httpd -l
```

#### (4) 启动、停止与重启 Apache 服务器

Apache 服务器的 Web 服务功能,是由 httpd 守护进程来实现的,该进程在后台不断处理用户的 http 请求。httpd 守护进程由 Apache 提供的 httpd 程序来启动,但最好不通过直接执行 httpd 程序来启动该守护进程,而要利用系统提供的 apachectl 启动脚本来启动该守护进程。apachectl 启动脚本会自动设置在某些操作系统下,正常运行 httpd 所需的环境变量。

httpd 程序被调用后所做的第一件事就是读取 httpd.conf 配置文件,并根据其配置项来配置当前 Web 服务器。如根据 Listen 80 配置项,将 Web 服务器绑定在 80 端口,并通过创建很多子进程,来完成侦听和回应客户端的 http 请求;通过 DocumentRoot 配置项来设置 Web 站点的根目录等。httpd 的主进程以 root 用户的权限运行,而其子进程则以一个较低权限的用户运行,这由多道处理模块自动进行控制。

启动 Apache 服务器,其实现命令为 /usr/local/apache2/bin/apachectl start。

```
[root@rh9 root]# /usr/local/apache2/bin/apachectl start
httpd: Could not determine the server's fully qualified domain name, using 127.0.0.1
for ServerName
```

在默认的配置文件中,没有配置 ServerName,因此在启动时找不到服务器域名,系统提示采用 127.0.0.1 来作为服务器名。

重启 Apache 服务器,实现命令为 /usr/local/apache2/bin/apachectl restart。

停止 Apache 服务器,实现命令为 /usr/local/apache2/bin/apachectl stop。

#### (5) 测试 Web 服务器

Apache Web 服务器启动成功后,在 Linux 服务器的 Mozilla 浏览器中,键入 http://127.0.0.1 或 http://localhost 并回车,即可看到 Apache 默认站点的内容了,如图 7.6 所示。对于其他主机,可通过“http://服务器 IP 地址”的方式来访问该 Web 站点。

另外,也可采用以下命令自行创建一个简单的测试页面 index.html,来检查 Web 服务器是否工作正常。

```
[root@rh9 root]# vi /usr/local/apache2/htdocs/index.html
```

然后输入以下内容并存盘保存:

```
<.html>
<head><title>homepage test</title></head>
<body>
hello,apache web server.
```

```
</body>
</html>
```

假如当前 Linux 服务器的 IP 地址为 192.168.168.154,则在浏览器中键入 `http://192.168.168.154/index.html` 并回车,此时若在页面中输出 `hello,apache web server.` 信息,则说明 Apache Web 服务器工作正常。

#### (6) 设置 Apache 服务自启动

若要使 Apache Web 服务器随 Linux 操作系统的启动而自动启动,可将启动 Apache 服务器的命令添加到 `/etc/rc.d/` 目录下的 `rc.local` 文件中,实现的操作命令为:

```
[root@rh9 root]# echo "/usr/local/apache2/bin/apachectl start">>/etc/rc.d/rc.local
```

### 7.2.2 Apache 配置文件简介

Apache 的配置文件是包含了若干指令的纯文本文件,其文件名为 `httpd.conf`,在 Apache 启动时,会自动读取配置文件中的内容,并根据配置指令影响 Apache 服务器的运行。配置文件改变后,只有在下次启动或重新启动后才会生效。

在 `/usr/local/apache2/conf` 目录中,除了提供标准的 `httpd.conf` 配置文件外,还提供了一些样本配置文件,可根据需要进行选择使用。利用 `less/usr/local/apache2/conf/httpd.conf` 命令,可查看配置文件的内容,对于每个配置项,通常还附有一些简要的配置说明。

配置文件中的内容分为注释行和服务器配置命令行。行首有“#”的即为注释行,注释不能出现在指令的后边,除了注释行和空行外,服务器会认为其他的行都是配置命令行。

配置文件中的指令不区分大小写,但指令的参数通常是对大小写敏感的。对于较长的配置命令,行末可使用反斜杠“\”换行,但反斜杠与下一行之间不能有任何其他字符(包括空白)。

可以使用 `apachectl configtest` 或者 `httpd` 的命令行参数 `-t` 来检查配置文件中的错误,而无需启动 Apache 服务器。

整个配置文件总体上划分为三部分(section),第一部分为全局环境设置,主要用于设置 `ServerRoot`、主进程号的保存文件、对进程的控制、服务器侦听的 IP 地址和端口以及要装载的 DSO 模块等;第二部分是服务器的主要配置指定位置;第三部分用于设置和创建虚拟主机。

### 7.2.3 Apache 服务器基本配置

Apache 的配置命令由内核和模块共同提供,配置命令很多,下面主要介绍一些常用的配置命令。

## 1. 常规配置命令

### (1) ServerRoot

用于设置服务器的根目录,默认设置为/usr/local/apache2,一般不需要修改。服务器根目录是 Apache 配置文件和日志文件的基础目录,也是所有和 Apache 服务器相关的文件的根目录。若 Apache 的安装位置发生改变,则应更改,该配置命令用法为:

```
ServerRoot apache 安装路径
```

### (2) ServerName

设置服务器用于辨识自己的主机名和端口号,该设置仅用于重定向和虚拟主机的识别。该指令取代了 Apache 1.3 中的 Port 命令。命令用法为:

```
ServerName 完整的域名[:端口号]
```

对于 Internet Web 服务器,应保证该名称是 DNS 服务器中的有效记录。默认配置文件中对此没有设置,应根据服务器的实际情况进行设置。

比如当前 Web 服务器的域名为 www.pcnetedu.com,则可设置为:

```
ServerName www.pcnetedu.com
```

或设置为

```
ServerName www.pcnetedu.com:80
```

当没有指定 ServerName 时,服务器会尝试对 IP 地址进行反向查询来获得主机名。如果在服务器名中没有指定端口号,服务器会使用接受请求的端口。为了加强可靠性和可预测性,应使用 ServerName 显式地指定一个主机名和端口号。

### (3) Listen

Listen 命令告诉服务器接受来自指定端口或者指定地址的某端口的请求。如果 Listen 仅指定了端口,则服务器会监听本机的所有地址;如果指定了地址和端口,则服务器只监听来自该地址和端口的请求。利用多个 Listen 指令,可以指定要监听的多个地址和端口,比如,在使用虚拟主机时,对不同的 IP、主机名和端口需要作出不同的响应,此时就必须明确指出要监听的地址和端口。其命令用法为:

```
Listen [IP 地址] 端口号
```

Web 服务器使用标准的 80 号端口,若要对当前主机的 80 端口进行侦听,则配置命令为:

```
Listen 80
```

假设当前服务器绑定了 61.186.160.104 和 61.186.160.105 IP 地址,现需要对其 80

端口和 8080 端口进行监听,则配置命令为:

```
Listen 61.186.160.104:80
Listen 61.186.160.104:8080
Listen 61.186.160.105:80
Listen 61.186.160.105:8080
```

#### (4) ServerAdmin

用于设置 Web 站点管理员的 E-mail 地址。当服务器产生错误时(如指定的网页找不到),服务器返回给客户端的错误信息中将包含该邮件地址,以告诉用户该向谁报告错误。其命令用法为:

ServerAdmin E-mail 地址

#### (5) DocumentRoot

用于设置 Web 服务器的站点根目录,其命令用法为:

DocumentRoot 目录路径名

默认设置为:DocumentRoot /usr/local/apache2/htdocs

设置时注意,目录路径名的最后不能加“/”,否则将会发生错误。

#### (6) ErrorDocument

用于定义当遇到错误时,服务器将给客户端什么样的回应,通常是显示预设置的一个错误页面。其命令用法为:

ErrorDocument 错误号 所要显示的网页

在默认的配置文件中,预定义了一些对不同错误的响应信息,但都注释掉了,若要开启,只需去掉前面的“#”号即可。使用以下命令可查看这些定义。

```
[root@rh9 root]# grep ErrorDocument /usr/local/apache2/conf/httpd.conf
```

#### (7) DirectoryIndex

用于设置站点主页文件的搜索顺序,各文件间用空格分隔。

例如,要将主页文件的搜索顺序设置为 index.php、index.htm、index.html、default.htm,则配置命令为:

```
DirectoryIndex index.php index.htm index.html default.htm
```

#### (8) User 与 Group

User 用于设置服务器以哪种用户身份来响应客户端的请求。Group 用于设置将由哪一组来响应用户的请求。可用“#”加用户 ID 号或组 ID 号来表达,默认设置为:

```
User nobody
```



Group # -1

nobody 用户权限较小,对系统安全威胁不大。千万不要将 User 或 Group 设置为 root。

#### (9) AddDefaultCharset

用于指定默认的字符集。在 HTTP 的回应信息中,若在 HTTP 头中未包含任何关于内容字符集类型的参数时,此指令将指定的字符集添加到 HTTP 头中,此时将覆盖网页文件中,通过 META 标记符所指定的字符集。命令用法为:

AddDefaultCharset 字符集名称

Apache 默认的字符集为 ISO-8859-1,对于含有中文字符的网页,若网页中没有指定字符集,则在显示中文的时候会出现乱码,解决的办法就是将默认字符集设置为 GB2312,其配置命令为:

AddDefaultCharset GB2312

## 2. 性能配置命令

### (1) 持续连接配置

一般情况下,每个 HTTP 请求和响应都使用一个单独的 TCP 连接,服务器每次接受一个请求时,都会打开一个 TCP 连接并在请求结束后关闭该连接。若能对多个处理重复使用同一个连接,则可减小打开 TCP 连接和关闭 TCP 连接的负担,从而提高服务器的效能。

① Timeout 用于设置连接请求超时的时间,单位为秒。默认设置值为 300,超过该时间,连接将断开。若网速较慢,可适当调大该值。

② KeepAlive 用于启用持续的连接或者禁用持续的连接。其命令用法: KeepAlive On|Off。配置文件中的默认设置为 KeepAlive On。

③ MaxKeepAliveRequests 用于设置在一个持续连接期间允许的最大 HTTP 请求数目。若设置为 0,则没有限制;默认设置为 100,可以将该值适当加大,以提高服务器的性能。

④ KeepAliveTimeout 用于设置在关闭 TCP 连接之前,等待后续请求的秒数。一旦接受请求建立了 TCP 连接后,就开始计时,若超出该设定值还没有接受到后续的请求,则该 TCP 连接将被断开。默认设置为 10 秒。

### (2) 控制 Apache 进程

对于使用 prefork 多道处理模块的 Apache 服务器,对进程的控制,可在 prefork.c 模块中进行设置或修改。配置文件的默认设置为:

<IfModule prefork.c>

```
StartServers          5
MinSpareServers       5
MaxSpareServers       10
MaxClients            150
MaxRequestsPerChild   0
</IfModule>
```

在配置文件中,属于特定模块的指令要用<IfModule>指令包含起来,使之有条件地生效。<IfModule prefork.c>表示如果 prefork.c 模块存在,则在<IfModule prefork.c>与</IfModule>之间的配置指令将被执行,否则不会被执行。下面分别介绍各配置项的功能。

① StartServers 用于设置服务器启动时启动的子进程的个数。

② MinSpareServers 用于设置服务器中空闲子进程(即没有 HTTP 处理请求的子进程)数目的下限。若空闲子进程数目小于该设置值,父进程就会以极快的速度生成子进程。

③ MaxSpareServers 用于设置服务器中空闲子进程数目的上限。若空闲子进程超过该设置值,则父进程就会停止多余的子进程。一般只有在站点非常繁忙的情况下,才有必要调大该设置值。

④ MaxClients 用于设置服务器允许连接的最大客户数,默认值为 150,该值也限制了 httpd 子进程的最大数目,可根据需要进行更改,比如更改为 500。

⑤ MaxRequestsPerChild 用于设置子进程所能处理请求的数目上限。当到达上限后,该子进程就会停止。若设置为 0,则不受限制,子进程将一直工作下去。

### 3. 日志配置命令

对于 Web 站点,日志文件必不可少,它记录着服务器处理的所有请求、运行状态和一些错误或警告等信息。要了解服务器上发生了什么,就必须检查日志文件,虽然日志文件只记录已经发生的事件,但是它会让管理员知道服务器遭受的攻击,并有助于判断当前系统是否提供了足够的安全保护等级。

#### (1) ErrorLog

用于指定服务器存放错误日志文件的位置和文件名,默认设置为 ErrorLog logs/error\_log。

此处的路径是相对于 ServerRoot 目录的路径。在 error\_log 日志文件中,记录了 Apache 守护进程 httpd 发出的诊断信息和服务器在处理请求时所产生的出错信息。在启动 Apache 服务器出现故障时,应查看该文件以了解出错原因。

#### (2) LogLevel

用于设置记录在错误日志中的信息的详细程度。依照重要性降序排列,其记录级别如下所示:

emerg	紧急,系统将无法使用	warn	警告情况
alert	必须立即采取措施	notice	一般重要情况
crit	致命情况	info	普通信息
error	错误情况	debug	出错级别信息

当指定了某特定级别后,所有级别高于它的信息也将被记录在日志文件中。配置文件中的默认设置级别为 warn,可根据需要进行调整。级别设置过低,将会导致日志文件急剧增大。

### (3) LogFormat、CustomLog

access\_log 日志文件用于记录服务器处理的所有请求。CustomLog 用于指定 access\_log 日志文件的位置和日志记录的格式;LogFormat 则用于定义日志的记录格式。

LogFormat 命令的用法如下:

LogFormat 日志格式字符串 日志格式名称

在配置文件中,预定义了四种日志格式,分别是:

- LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined;
- LogFormat "%h %l %u %t \"%r\" %>s %b" common;
- LogFormat "%{Referer}i ->%U" referer;
- LogFormat "%{User-agent}i" agent。

日志格式主要用于指定要记录的信息以及彼此间的排列顺序。要记录的信息采用一系列以“%”开头的变量来表示,每个变量代表某一方面的内容,如表 7.2 所示。整个日志格式字符串用双引号括起来,在其中要使用双引号的地方,采用“\”转义字符表示。

表 7.2 LogFormat 使用的变量

变 量 名	输出的内容	变 量 名	输出的内容
%a	远程主机 IP 地址	%b	发送的字节数,不包括 HTTP 标题
%A	本地主机 IP 地址	%t	请求的时间
%h	远程主机名	%r	HTTP 请求的第一行的内容
%H	请求协议	%s	HTTP 响应状态码
%l	远程登录名	%m	请求方法
%u	来自 auth 的远程用户	%v	服务于该请求的服务器的 ServerName
%U	请求的 URL 路径	%V	服务器的名字,取决于 UseCanonicalName 的设置
%{User-agent}i	用户浏览器类型	%{Host}i	返回 HTTP 请求的主机头信息,可能含端口号信息

若要采用预定义的 common 日志格式来记录访问日志,则配置命令为:

```
CustomLog logs/access_log common
```

采用该种日志格式的记录的格式如下:

```
192.168.168.154 - - [16/Aug/2004:13:04:46 +0800] "GET /index.html HTTP/1.1" 200 88
```

倒数第三项的 GET /index.html HTTP/1.1 是由 %r 变量输出的,代表 HTTP 请求的第一行的内容,GET 说明是 HTTP 请求,/index.html 代表所请求的文件。

倒数第二项的 200,是由 %>s 变量输出的,代表 HTTP 响应的状态码。200 代表访问成功,404 代表文件未找到,403 代表禁止访问,401 代表未授权访问,400 代表错误请求。

最后一项的 88 代表所请求的数据大小为 88B,它是由 %b 变量输出的。

#### (4) PidFile

用于指定存放 httpd 主(父)进程号的文件名,便于停止该服务。其默认设置为:

```
PidFile logs/httpd.pid
```

### 4. 容器与访问控制指令

#### (1) 容器指令简介

容器指令通常用于封装一组指令,使其在容器条件成立时有效,或者用于改变指令的作用域。容器指令通常成对出现,具有以下格式特点:

```
<容器指令名 参数>
```

```
:
```

```
</容器指令名>
```

比如:

```
<IfModule mod_ssl.c>
```

```
    Include conf/ssl.conf
```

```
</IfModule>
```

<IfModule> 容器用于判断指定的模块是否存在,若存在(被静态地编译进服务器,或是被动态装载进服务器),则包含于其中的指令将有效,否则会被忽略。此处的配置指令的含义是:若 mod\_ssl 模块存在,则用 Include 指令,将 conf/ssl.conf 配置文件包含进当前的配置文件中。

<IfModule> 容器可以嵌套使用。若要使模块不存在时所包含的指令有效,只需在模块名前加一个“!”即可。比如配置文件中的以下配置:

```
<IfModule ! mpm_winnt.c>
```

```
<IfModule ! mpm_netware.c>
```

```
User nobody
Group # - 1
</IfModule>
</IfModule>
```

除了<IfModule>容器外,Apache 还提供了<Directory>、<Files>、<Location>、<VirtualHost>等容器指令。其中,<VirtualHost>用于定义虚拟主机;<Directory>、<Files>、<Location>等容器指令主要用来封装一组指令,使指令的作用域限制在容器指定的目录、文件或某个以 URL 开始的地址。在容器中,通过使用访问控制指令,可实现对这些目录、文件或 URL 地址的访问控制。

### (2) 访问控制指令

访问控制指令由 Apache 的内建模块 mod\_access 提供,它能实现基于 Internet 主机名的访问控制,其主机名可以是域名,也可以是一个 IP 地址,建议尽量使用 IP 地址,以减少 DNS 域名解析。相关的指令主要有 Allow、Deny 和 Order。

#### ① Allow

命令用法: Allow from host-list

命令功能: 指定允许访问的主机。host-list 代表主机名列表,各主机名间用空格分隔。该指令常用于<Directory>、<Files>、<Location>等容器中,以设置允许访问指定目录、文件或 URL 地址的主机。

比如允许 61.186.160.104 主机访问,则实现命令为: Allow from 61.186.160.104

若要允许所有的主机访问,则实现命令可表达为: Allow from all

#### ② Deny

命令用法: Deny from host-list

命令功能: 该命令与 Allow 刚好相反,用于指定禁止访问的主机名。

#### ③ Order

命令用法: Order allow,deny | deny,allow | mutual-failure

命令功能: 用于指定 allow 和 deny 语句,哪一个被先执行。其具体用法有以下三种。

- Order deny,allow deny 在 allow 之前进行控制。若主机没有被特别指出拒绝访问,则该资源将被允许访问。
- Order allow,deny allow 语句在 deny 语句之前执行。若主机没有被特别指出允许访问,则该主机将被拒绝访问该资源。
- Order mutual-failure 只有那些在 allow 语句中被指定,同时又没有出现在 deny 语句中的主机,才允许访问。若主机在两条指令中都没有出现,则将被拒绝访问。

### (3) 对目录、文件和 URL 操作的容器

#### ① <Directory>容器

<Directory>容器用于封装一组指令,使其对指定的目录及其子目录有效。该指令不能嵌套使用,其命令用法:

```
<Directory 目录名>
:
</Directory>
```

容器中所指定的目录名可以采用文件系统的绝对路径,也可以是包含通配符的表达式。比如要设置所有主机均能访问/usr/local/apache2/htdocs 目录,则容器指令应表达为:

```
<Directory /usr/local/apache2/htdocs>
    Order allow,deny
    Allow from all
</Directory>
```

若要禁止所有主机通过 Apache 服务访问文件系统的根目录,则配置指令为:

```
<Directory />
    Order deny,allow
    Deny from all
</Directory>
```

目录名可使用“\*”或“?”通配符,“\*”代表任意个字符,但不能通配“/”符号。“?”代表一个任意的字符。比如要对所有普通用户的主目录下的 public\_html 子目录进行配置,则此时的容器指令应表达为:

```
<Directory /home/* /public_html>
    Order allow,deny
    Allow from all
</Directory>
```

如果有多个<Directory>容器配置段符合包含某文档的目录(或其父目录),那么指令将以最短目录、最先应用的规则进行应用。

另外,还提供了一个名为<DirectoryMatch>的容器,其用法与<Directory>相同,只是在指定目录名时,可直接使用正则表达式。<Directory>若要使用正则表达式,则需要在正则表达式前加“~”符号。

## ② <Files> 容器

<Files>容器作用于指定的文件,而不管该文件实际存在于哪个目录。其命令用法:

```
<Files 文件名>
```

```

:
</Files>

```

文件名可以是一个具体的文件名,也可以使用“\*”和“?”通配符。另外,还可使用正则表达式来表达多个文件,此时要在正则表达式前多加一个“~”符号。

比如配置文件中的以下配置,将拒绝所有主机访问位于任何目录下的以.ht开头的文件,如.htaccess和.htpasswd等系统重要文件。

```

<Files ~ "\.ht">
Order allow,deny
Deny from all
</Files>

```

该容器通常嵌套在<Directory>容器中使用,以限制其所作用的文件系统范围。比如:

```

<Directory /usr/local/apache2/htdocs>
<Files private.html>
Order allow,deny
Deny from all
</Files>
</Directory>

```

以上配置将拒绝对htdocs目录及其所有子目录下的private.html文件进行访问。

<FilesMatch>容器与<Files>用法相同,只是可以直接使用正则表达式来通配多个文件。

### ③ <Location>容器

Location容器是针对URL地址进行访问限制的,而不是Linux的文件系统。其命令用法:

```

<Location URL>
:
</Location>

```

比如要拒绝除61.186.160.105以外的主机,对URL以/assistant开头的访问,则配置命令为:

```

<Location /assistant>
Order deny,allow
Deny from all
Allow from 61.186.160.105

```

```
</Location>
```

在<Location>容器中,/assistant 代表 Web 站点根目录下的 assistant 目录。而在<Directory>容器中,最左边的“/”代表的是 Linux 文件系统的根目录。

通过以上设置后,除 61.186.160.105 主机外,对 Web 站点根目录下的 assistant 目录,以及对其下子目录中的页面访问,都将被禁止。

## 5. 其他配置命令

### (1) .htaccess 文件

.htaccess 文件也称为分布式配置文件,在该文件中也可放置一些配置指令,以作用于该文件所在的目录以及其下的所有子目录。该文件可位于多个目录中,以分别对这些目录进行控制。功能上类似于<Directory>容器,但<Directory>和<Location>容器不能用在.htaccess 文件中,<Files>容器可以用于该文件。

.htaccess 文件是在 httpd.conf 配置文件中,由以下命令配置指定的。

```
AccessFileName .htaccess
```

在配置文件指定分布式配置文件.htaccess 后,若站点的根目录为/usr/local/apache2/htdocs,当用户在浏览器中请求/index.html 页面时,服务器会在该文档的各个路径中去查找第一个存在的.htaccess 配置文件,即 Apache 会试图打开/.htaccess、/usr/.htaccess、/usr/local/.htaccess、/usr/local/apache2/.htaccess、/usr/local/apache2/htdocs/.htaccess。

对系统的配置均可在 httpd.conf 文件中实现,搜寻.htaccess 文件会降低系统性能,可通过在<Directory />中使用 AllowOverride None 命令,来禁止系统查找该文件。

```
<Directory />
```

```
AllowOverride None
```

```
</Directory>
```

AllowOverride 命令用于设置原来设定的权限是否可以被.htaccess 文件中的权限所覆盖,其选项有 All 和 None 两个。若设置为 None,则不受.htaccess 的权限覆盖,此时系统就不再寻找和读取.htaccess 文件中的配置内容。

### (2) Options 命令

Options 命令控制在特定目录中将使用哪些服务器特性,通常用在<Directory>容器中,其命令用法为“Options 功能选项列表”。

可用的选项及功能如表 7.3 所示。

对于 Linux 系统的根目录和 Web 站点根目录的访问控制,通常可设置为以下形式:



表 7.3 Options 命令可用的选项

选 项	功 能 描 述
None	不启用任何额外特性
All	除 MultiViews 之外的所有特性,默认设置
ExecCGI	允许执行 CGI 脚本
FollowSymLinks	服务器允许在此目录中使用符号连接。在<Location>段中无效
Includes	允许服务器端包含 SSI(Server-side includes)
IncludesNOEXEC	允许服务器端包含,但禁用 #exec 和 #exec CGI 命令。但仍可以从 ScriptAlias 目录使用 #include 虚拟 CGI 脚本
Indexes	如果一个映射到目录的 URL 被请求,而此目录中又没有 DirectoryIndex (例如:index.html),那么服务器会返回一个格式化后的目录列表
MultiViews	允许内容协商的多重视图
SymLinksIfOwnerMatch	服务器仅在符号连接与其目的目录或文件拥有者具有同样的用户 id 时,才使用它

```

<Directory />
Options FollowSymLinks
AllowOverride None
Order allow,deny
Deny from all
</Directory>
<Directory "/usr/local/apache2/htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>

```

#### 7.2.4 配置虚拟主机

虚拟主机(virtual host)是指在一台主机上运行的多个 Web 站点,每个站点均有自己独立的域名,虚拟主机对用户是透明的,就好像每个站点都在单独的一台主机上运行一样。

如果每个 Web 站点拥有不同的 IP 地址,则称为基于 IP 的虚拟主机;若每个站点的 IP 地址相同,但域名不同,则称为基于名字或主机名的虚拟主机,使用这种技术,不同的虚拟主机可以共享同一个 IP 地址,以解决 IP 地址缺乏的问题。

要实现虚拟主机,首先必须用 Listen 指令告诉服务器需要监听的地址和端口,然后为特定的地址和端口建立一个<VirtualHost>段,并在该段中配置虚拟主机。

在配置虚拟主机时,可使用以下命令来检查虚拟主机的配置,看是否存在语法错误。

```
/usr/local/apache2/bin/httpd -S
```

### 1. 基于主机名的虚拟主机

基于主机名(域名)的虚拟主机是根据客户端提交的 HTTP 头中,关于主机名部分决定的。配置虚拟主机之前,应首先配置 DNS 服务器,让每个虚拟主机的域名,都能解析到当前服务器所使用的 IP 地址,然后再配置 Apache 服务器,使其能辨识不同的主机名即可。

由于 SSL 协议自身的原因,基于主机名的虚拟主机不能做成 SSL 安全服务器。

#### (1) 虚拟主机的创建步骤

① 在 DNS 服务器中为每个虚拟主机所使用的域名进行注册,让其能解析到服务器所使用的 IP 地址。

② 在配置文件中使⽤ Listen 指令,指定要监听的地址和端口。Web 服务器使用标准的 80 号端口,因此一般可配置为 Listen 80,让其监听当前服务器的所有地址上的 80 端口。

③ 使用 NameVirtualHost 指令,为一个基于域名的虚拟主机指定将使用哪个 IP 地址和端口来接受请求。如果对多个地址使用了多个基于域名的虚拟主机,则对每个地址均要使用此指令。

命令用法: NameVirtualHost 地址[:端口]

端口号为可选项,若虚拟主机使用的是非标准的 80 号端口,则应明确指定所使用的端口号。

比如,若基于域名的虚拟主机使用 61.186.160.104 这个 IP 地址,则指定方法为:

```
NameVirtualHost 61.186.160.104
```

另外也可表达为 NameVirtualHost \*。此处的“\*”通配任意的 IP 地址。当 IP 地址无法确定时,使用“\*”是很方便的,比如,若服务器使用的是动态 IP 地址,而域名也是使用动态域名解析系统时,因为“\*”匹配任何 IP 地址,无论 IP 地址如何变化,都不需要修改虚拟主机的配置。

若希望在一个 IP 地址上运行一个基于域名的虚拟主机,而在另外一个地址上运行一个基于 IP 的或是另外一套基于域名的虚拟主机,此时就必须使用具体的 IP 地址,而不能使用“\*”。

④ 使用<VirtualHost>容器指令定义每一个虚拟主机。<VirtualHost>容器的参

数必须与 NameVirtualHost 后面所使用的参数保持一致。

在<VirtualHost>容器中至少应指定 ServerName 和 DocumentRoot,另外可选的配置还有 ServerAdmin、DirectoryIndex、ErrorLog、CustomLog、TransferLog、ServerAlias、ScriptAlias 等,大部分的配置命令都可用在<VirtualHost>容器中,但与进程控制相关的 PidFile、TypesConfig、ServerRoot、Listen 和 NameVirtual 不能使用。

### (2) 虚拟主机的匹配方式

当一个请求到达时,服务器会首先检查它是否使用了一个能和 NameVirtualHost 相匹配的 IP 地址。如果匹配,就会查找每个与这个 IP 地址相对应的<VirtualHost>配置段,并尝试找出一个 ServerName 或 ServerAlias 配置项与请求的主机名(域名)相同的,若找到,则使用该虚拟主机的配置,并响应其访问请求,否则将使用符合这个 IP 地址的第一个列出的虚拟主机。从中可见,排在最前面的虚拟主机成为默认虚拟主机。

当请求的 IP 地址与 NameVirtualHost 指令中的地址匹配时,主服务器中的 DocumentRoot 将永远不会被用到,因此,若要在现有的 Web 服务器上增加虚拟主机,必须也要为主服务器提供的 Web 站点,创建一个<VirtualHost>配置块,在该虚拟主机中 ServerName 和 DocumentRoot 的内容应该与全局的 ServerName 和 DocumentRoot 保持一致,还要把这个虚拟主机放在所有<VirtualHost>的最前面,让其成为默认主机。

**[例 7.3]** 假设当前服务器的 IP 地址为 192.168.168.154,现要在该服务器创建两个基于域名的虚拟主机,使用端口为标准的 80,其域名分别为 www.myweb1.com 和 www.myweb2.com,站点根目录分别为/var/www/myweb1 和/var/www/myweb2,日志文件分别放在/var/vhlogs/myweb1/和/var/vhlogs/myweb2/目录下,Apache 服务器原来的主站点采用域名 www.myweb.com 进行访问。

服务器配置步骤如下:

#### ① 注册虚拟主机所要使用的域名。

对于测试,可直接使用/etc/hosts 名称解析文件来进行域名的注册。对于 Internet 的虚拟主机域名,则应在位于 Internet 的 DNS 服务器上进行注册登记。

```
[root@rh9 root]# vi /etc/hosts
```

编辑/etc/hosts 文件,在文件中添加以下内容:

```
192.168.168.154      www.myweb1.com  www.myweb2.com  www.myweb.com
[root@rh9 root]# ping www.myweb1.com      # 检测域名解析是否正常
[root@rh9 root]# ping www.myweb2.com
[root@rh9 root]# ping www.myweb.com
```

若能 ping 通,则域名解析正常。

#### ② 创建所需的目录。

```
[root@rh9 root]# mkdir -p /var/www/myweb1
[root@rh9 root]# mkdir -p /var/www/myweb2
[root@rh9 root]# mkdir -p /var/vhlogs/myweb1
[root@rh9 root]# mkdir -p /var/vhlogs/myweb2
```

③ 编辑 httpd.conf 配置文件, 设置 Listen 指令侦听的端口。

```
Listen 80
```

④ 在 httpd.conf 配置文件的第三部分中, 添加对虚拟主机的定义。添加的配置内容为:

```
NameVirtualHost 192.168.168.154
<VirtualHost 192.168.168.154>
    ServerName www.myweb.com
    DocumentRoot /usr/local/apache2/htdocs
    ServerAdmin webmaster@myweb.com
</VirtualHost>

<VirtualHost 192.168.168.154>
    ServerName www.myweb1.com
    DocumentRoot /var/www/myweb1
    DirectoryIndex index.php index.php3 index.html index.htm default.html default.html
    ServerAdmin webmaster@myweb1.com
    ErrorLog /var/vhlogs/myweb1/error_log
    TransferLog /var/vhlogs/myweb1/access_log
</VirtualHost>

<VirtualHost 192.168.168.154>
    ServerName www.myweb2.com
    DocumentRoot /var/www/myweb2
    DirectoryIndex index.php index.php3 index.htm index.html default.htm default.html
    ServerAdmin webmaster@myweb2.com
    ErrorLog /var/vhlogs/myweb2/error_log
    TransferLog /var/vhlogs/myweb2/access_log
</VirtualHost>
```

利用 DirectoryIndex 可为每个虚拟主机独立设置各主页文件的解析顺序。

⑤ 对用于存放 Web 站点的目录, 设置访问控制。

```
<Directory /var/www>
    Options FollowSymLinks
```

```
AllowOverride None
Order deny,allow
Allow from all
</Directory>
```

⑥ 保存 `httpd.conf` 配置文件,利用 `apachectl -S` 命令检查虚拟主机配置是否正确。

```
[root@rh9 root]# /usr/local/apache2/bin/apachectl -S
VirtualHost configuration:
192.168.168.154:80          is a NameVirtualHost
    default server www.myweb.com
    port 80  namevhost www.myweb.com
    port 80  namevhost www.myweb1.com
    port 80  namevhost www.myweb2.com
Syntax OK
```

从输出信息可知,虚拟主机配置正确。利用以下命令重启 Apache 服务器,以使配置生效。

```
[root@rh9 root]# /usr/local/apache2/bin/apachectl restart
```

⑦ 测试虚拟主机。

利用 vi 编辑器,在虚拟主机的站点根目录,分别创建 `index.html` 页面文件,并在页面的 `<body>` 与 `</body>` 之间输入不同的正文内容,以示区别。

在命令行中键入 `startx`,切换到 X-Windows 图形界面,启动浏览器,然后在地址栏中键入 `http://www.myweb1.com` 并回车,若能看到 `index.html` 页面的内容,则虚拟主机创建成功。

分别键入 `http://www.myweb.com` 和 `http://www.myweb2.com` 并回车,查看虚拟主机对应的 Web 站点工作是否正常。

若服务器有两个 IP 地址,也可将一个 IP 地址用于主站点(main host),而将另一个 IP 地址用于虚拟主机。

在 `<VirtualHost>` 配置段中,可以单独为每个虚拟主机指定日志文件,若未指定,则日志统一记录在主日志文件中。主日志文件默认位于 `/usr/local/apache2/logs/` 目录下,文件名分别为 `error_log` 和 `access_log`。

当虚拟主机很多,而且每个主机又都使用了不同的日志文件时,Apache 可能会遇到耗尽 file handles 的情况,从而无法创建文件。Linux/UNIX 操作系统限制了每个进程可以使用的 file handles 的数量,典型上限为 64 个,但可以扩充,直至到达一个很大的硬限制为止。

若服务器上的虚拟主机很多,为防止日志文件过多,也可在 `<VirtualHost>` 配置段

中不指定,而统一记录在系统的主日志文件中,此时为了记录该日志是哪一个虚拟主机产生的,应修改日志的记录内容和格式,并在日志内容的最开头添加“%v”变量,以记录虚拟主机的名称(即 ServerName 的内容)。比如:

```
LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost
CustomLog logs/vhost_log vhost
```

当需要分析阅读日志文件时,可使用以下命令,将日志按虚拟主机名分组,拆分成一个个独立的日志文件,每个日志文件采用“虚拟主机名.log”形式命名,其中包含了该虚拟主机所产生的日志记录。

```
split-logfile < /usr/local/apache2/logs/vhost_log
```

split-logfile 程序可在 Apache 发行版的 support 目录找到。

**[例 7.4]** 现有某企业的服务器,配有两块网卡,IP 地址分别为内网的 192.168.168.10 和外网地址 61.186.160.104,在 Internet 网中,企业域名 www.example.com 指向 61.186.160.104 地址,在企业内网的 DNS 服务器中,同样的域名指向 192.168.168.10。现要求为来自内网和外网的请求提供同样的 Web 服务。

实现方法:

在企业内网中应配置一个 DNS 服务器,并对 www.example.com 域名进行注册,使其解析到 192.168.168.10 地址。对于不能解析的域名,该 DNS 服务器应向上级 DNS 服务器提交域名解析请求。内网中的主机应配置 DNS 客户为内网的 DNS 服务器的地址,以便在请求域名 www.example.com 时,能优先解析为 192.168.168.10,以通过内网访问服务器。

在 httpd.conf 配置文件中,添加以下虚拟主机配置。

```
NameVirtualHost 192.168.168.10
NameVirtualHost 61.186.160.104
<VirtualHost 192.168.168.10 61.186.160.104>
    DocumentRoot /www/server1
    ServerName www.example.com
</VirtualHost>
```

**[例 7.5]** 当前服务器的 IP 地址为 192.168.168.154,现要在该服务器上创建两个基于域名(主机名)的虚拟主机,域名分别为 www.myweb3.com 和 www.myweb4.com,每个虚拟主机的 80 端口和 8080 端口,分别服务一个 Web 站点,其站点根目录分别为 /var/www/myweb3-80、/var/www/myweb3-8080、/var/www/myweb4-80、/var/www/myweb4-8080。www.myweb3.com 的 80 端口作为默认 Web 站点。

服务器配置步骤如下:

① 在 /etc hosts 文件中注册虚拟主机所使用的域名。

② 创建所需的目录。

```
[root@rh9 root]# mkdir -p /var/www/myweb3-80
[root@rh9 root]# mkdir -p /var/www/myweb3-8080
[root@rh9 root]# mkdir -p /var/www/myweb4-80
[root@rh9 root]# mkdir -p /var/www/myweb4-8080
```

③ 编辑 httpd.conf 配置文件, 设置 Listen 指令侦听的端口为 80 和 8080。

```
Listen 80
Listen 8080
```

④ 在 httpd.conf 配置文件的第三部分中, 添加对虚拟主机的定义。添加的配置内容

```
NameVirtualHost 192.168.168.154:80
NameVirtualHost 192.168.168.154:8080
```

```
<VirtualHost 192.168.168.154:80>
ServerName www.myweb3.com
DocumentRoot /var/www/myweb3-80
</VirtualHost>
<VirtualHost 192.168.168.154:8080>
ServerName www.myweb3.com
DocumentRoot /var/www/myweb3-8080
</VirtualHost>
```

```
<VirtualHost 192.168.168.154:80>
ServerName www.myweb4.com
DocumentRoot /var/www/myweb4-80
</VirtualHost>
<VirtualHost 192.168.168.154:8080>
ServerName www.myweb4.com
DocumentRoot /var/www/myweb4-8080
</VirtualHost>
```

⑤ 保存 httpd.conf 配置文件, 然后重启 Apache 服务器。

⑥ 利用 vi 编辑器, 在各站点根目录分别创建一个内容不同的 index.html 文件。

⑦ 测试各 Web 站点。

在浏览器中分别键入以下地址, 访问各自的主页, 检查能否正常访问。

```
http://www.myweb3.com
http://www.myweb3.com:8080
http://www.myweb4.com
http://www.myweb4.com:8080
```

利用域名虚拟主机,结合使用不同的端口,同一个 IP 地址,可以创建出很多 Web 站点。在目前实际应用的虚拟主机服务中,对于同一个域名,通常开放了几个端口,80 端口服务于该域名的主 Web 站点,而将 8080 或其他端口提供的网站,用作对主网站的后台管理或用于提供该域名的基于 Web 的 E-mail 服务。

## 2. 基于 IP 地址的虚拟主机

基于 IP 的虚拟主机拥有不同的 IP 地址,这就要求服务器必须同时绑定多个 IP 地址。这可通过在服务器上安装多块网卡,或通过虚拟 IP 接口(Red Hat Linux 将其称为 IP 别名)来实现,即在一张网卡上绑定多个 IP 地址。

有两种配置方法使 Apache 支持基于 IP 地址的虚拟主机,一是为每个主机运行一个 httpd 守护进程,各守护进程的配置文件不同,分别以不同的 User、Group、Listen 和 ServerRoot 来运行,并通过 Listen 指令来指定为哪个 IP 地址和端口的虚拟主机服务。该方法适合于虚拟主机彼此间安全性要求很高的场合。

启动 httpd 守护进程时,可使用以下方法来指定所要加载的配置文件:

```
[root@rh9 root]# ./usr/local/apache2/bin/httpd -f 配置文件名及路径
```

另一种方法是使用一个 httpd 守护进程来支持所有的虚拟主机。在服务器需要为大量请求服务的情况下,该方法可以获得较高的性能。下面主要针对该方法介绍基于 IP 地址的虚拟主机的实现方法。

(1) 为服务器安装多块网卡或为现有网卡绑定多个 IP 地址

**[例 7.6]** 当前服务器有两张网卡 eth0 和 eth1,eth0 的 IP 地址为 192.168.168.154,eth1 网卡的 IP 地址为 192.168.168.156。eth0 网卡用作了基于主机名的虚拟主机,现在用 eth1 网卡,通过 IP 别名方式,为其绑定多个 IP 地址,用于提供基于 IP 地址的虚拟主机。

eth1 网卡的配置文件为/etc/sysconfig/network-scripts/ifcfg-eth1,eth1 绑定的第一张虚拟网卡的设备名为 eth1:0,对应的配置文件为 ifcfg-eth1:0,通过修改配置文件中的设备名和 IP 地址,即可实现 IP 地址的绑定,具体操作步骤如下:

```
[root@rh9 root]# cd /etc/sysconfig/network-scripts
[root@rh9 network-scripts]# cp ifcfg-eth1 ifcfg-eth1:0
[root@rh9 network-scripts]# vi ifcfg-eth1:0
```

注意:修改该虚拟网卡的设备名为 eth1:0,网卡地址设置为需要的地址,比如:



```
DEVICE=eth1:0
IPADDR=192.168.167.157
[root@rh9 network-scripts]# ifdown eth1
[root@rh9 network-scripts]# ifup eth1:0
[root@rh9 network-scripts]# ifup eth1
[root@rh9 network-scripts]# ping 192.168.167.157
[root@rh9 network-scripts]# ping 192.168.167.156
```

若能 ping 通,则说明 IP 地址绑定成功。

## (2) 配置基于 IP 地址的虚拟主机

首先利用 Listen 指令设置要侦听的 IP 地址和端口,然后在配置文件中直接利用 <VirtualHost> 容器配置虚拟主机即可。在配置段中 ServerName 和 DocumentRoot 仍是必选项,可选有配置项有 ServerAdmin、ErrorLog、TransferLog 和 CustomLog 等。

单一的 httpd 守护进程将伺服所有对主服务器和虚拟主机的 HTTP 请求。

**[例 7.7]** 当前服务器有 192.168.167.156 和 192.168.167.157 两个 IP 地址,对应的域名分别为 www.example2.com 和 www.example3.com,试为其创建基于 IP 地址的虚拟主机,端口使用 80。这两个站点的根目录分别为 /var/www/example2 和 /var/www/example3。

服务器配置步骤如下:

### ① 注册虚拟主机所要使用的域名。

编辑 /etc/hosts 文件,在文件中添加以下两行内容:

```
192.168.167.156      www.example2.com
192.168.167.157      www.example3.com
```

### ② 创建 Web 站点根目录。

```
[root@rh9 root]# mkdir -p /var/www/example2
[root@rh9 root]# mkdir -p /var/www/example3
```

### ③ 编辑 httpd.conf 配置文件,保证有以下 Listen 指令。

```
Listen 80
```

### ④ 配置虚拟主机。

```
<VirtualHost 192.168.167.156>
ServerName www.example2.com
DocumentRoot /var/www/example2
</VirtualHost>
<VirtualHost 192.168.167.157>
```

```
ServerName www.example3.com
DocumentRoot /var/www/example3
</VirtualHost>
```

⑤ 在 /var/www/example2 和 /var/www/example3 目录中, 利用 vi 编辑器创建 index.html 主页文件。

⑥ 重启 Apache 服务器, 然后测试虚拟主机。

若键入 `http://localhost`, 返回的将是服务器的主站点的主页内容。基于 IP 地址的虚拟主机, 可以使用域名访问, 也可使用 IP 地址访问。基于主机名的虚拟主机, 应采用域名访问, 若使用 IP 地址, 则访问的是服务器的主站点。

**[例 7.8]** 在例 7.7 的基础上, 为这两个域再增加 8080 端口, 使其也能在 8080 端口发布另外的 Web 站点。在 8080 端口的 Web 站点根目录, 分别为 /var/www/example2-8080 和 /var/www/example3-8080。

服务器配置步骤如下:

① 创建所需的站点根目录。

```
[root@rh9 root]# mkdir -p /var/www/example2-8080
[root@rh9 root]# mkdir -p /var/www/example3-8080
```

② 编辑修改 `httpd.conf` 配置文件, 保证有以下 `Listen` 指令。

```
Listen 80
Listen 8080
```

③ 编辑修改配置文件, 将例 7.7 的虚拟主机配置, 更改为以下形式。

```
<VirtualHost 192.168.167.156:80>
ServerName www.example2.com
DocumentRoot /var/www/example2
</VirtualHost>
<VirtualHost 192.168.167.156:8080>
ServerName www.example2.com
DocumentRoot /var/www/example2-8080
</VirtualHost>

<VirtualHost 192.168.167.157:80>
ServerName www.example3.com
DocumentRoot /var/www/example3
</VirtualHost>
<VirtualHost 192.168.167.157:8080>
ServerName www.example3.com
```

```
DocumentRoot /var/www/example3-8080
```

```
</VirtualHost>
```

④ 在 `/var/www/example2-8080` 和 `/var/www/example3-8080` 目录创建 `index.html` 文件。然后重启 Apache 服务器。

⑤ 测试虚拟主机。

分别键入以下地址进行测试。

```
http://www.example2.com
```

```
http://www.example2.com:8080
```

```
http://www.example3.com
```

```
http://www.example3.com:8080
```

另外,在同一台服务器上,还可混用基于域名的虚拟主机和基于 IP 地址的虚拟主机。

### 7.2.5 安装与配置 PHP 解释器

到目前为止,Apache Web 服务器已能实现对 HTML 静态网页进行解析和提供网站服务了。由于静态网页无法存取访问后台数据库,功能上受到很多限制,目前网站使用动态技术已比较普遍,在 Linux/UNIX 平台,支持的动态网页技术主要有 PHP 和 JSP。

PHP 是一种服务器端的脚本语言,支持跨平台运行,脚本的语法与 C 语言很类似,其功能主要由自身和其他扩展库所提供的大量函数来实现,支持访问各种符合 ODBC 标准的大中型数据库,最常用的主要是 MySQL。JSP 使用 Java 编程语言来实现对网页内容的动态生成,支持访问各种大中型数据库,功能很强大,采用预编译运行,运行速度较 PHP 快。

#### 1. 获得 PHP 及相关软件包

PHP 源代码软件包可从官方网站 (<http://www.php.net>) 下载,目前最新版本为 5.0.1,软件包名称为 `php-5.0.1.tar.gz`。可将该软件包下载或复制到 `/usr/local/src` 目录中。

为使 PHP 支持绘图处理并支持常见的图形文件格式 (`.jpg`、`.jpeg`、`.png`、`.tif`),需要为 PHP 安装 GD 扩展库和其他相关的支持库,以增强 PHP 的功能。

在 Red Hat Linux 9 的第一张安装光盘 `RedHat/RPMS` 目录下,提供了 RPM 安装包格式的 GD 库和相关的支持包,目前在网上也可找到更新版本的源代码包,其文件名(含版本号)和软件包的作用如表 7.4 所示。

若采用 RPM 包安装,还应安装含有 `devel` 的软件包,用于提供支持库和头文件。

软件的官方网站分别为:

```
zlib          http://www.gzip.org/zlib
```

```
freetype      http://www.freetype.org
```

表 7.4 PHP 扩展使用的 GD 库及相关支持包

Red Hat Linux 9 安装光盘	较新版本	作 用
gd-devel-1.8.4-11.i386.rpm gd-1.8.4-11.i386.rpm	gd-2.0.28.tar.gz	使 PHP 支持绘图处理,实现用代码绘图
libjpeg-6b-26.i386.rpm	jpegsrc.v6b.tar.gz	使 PHP 在绘图时支持 jpeg 和 jpg 格式
libpng-devel-1.2.2-16.i386.rpm libpng-1.2.2-16.i386.rpm	libpng-1.2.5.tar.gz	使 PHP 在绘图时支持 png 图形格式
freetype-devel-2.1.3-6.i386.rpm freetype-2.1.3-6.i386.rpm		使 PHP 支持 TrueType 字库
zlib-devel-1.1.4-8.i386.rpm zlib-1.1.4-8.i386.rpm	zlib-1.2.1.tar.gz	zlib 是一个通用的压缩与解压缩支持库

gd 库 <http://www.boutell.com/gd>

libpng <http://www.libpng.org/pub/png>

RPM 格式的包安装很简单,支持库默认安装在 /usr/lib 目录中。若从安装简单角度出发,可直接使用 Red Hat Linux 9 安装光盘所提供的 RPM 包来安装,在 PHP 的安装配置时,相关支持库的位置,指定为 /usr/lib 即可。若要追求安装最新版,则可下载相关的 .gz 包来安装。本例使用以下软件包来进行安装。

```
jpegsrc.v6b.tar.gz      libpng-1.2.5.tar.gz      freetype-2.1.3-6.i386.rpm
gd-2.0.28.tar.gz        zlib-1.2.1.tar.gz        mm-1.3.0.tar.gz
libxml2-2.5.11.tar.gz(支持 XML2)
```

将以上软件包复制到 /usr/local/src 目录中。

## 2. 安装 PHP 的相关支持包

安装扩展支持包的目的是增强 PHP 的功能,可根据需要选择所要安装的扩展包。gz 格式的软件包此处统一将其安装在 /usr/local/gdlibforphp 目录中。

### (1) 安装 libjpeg 库

```
[root@rh9 root]# cd /usr/local/src
[root@rh9 src]# tar -zxvf jpegsrc.v6b.tar.gz
[root@rh9 src]# cd jpeg-6b
[root@rh9 src]# mkdir -p /usr/local/gdlibforphp/jpeg
[root@rh9 jpeg-6b]# ./configure --help |less          # 获得配置帮助
[root@rh9 jpeg-6b]# ./configure --prefix=/usr/local/gdlibforphp/jpeg \
:> --enable-static --enable-shared
```

注:该软件包存在 bug,不能自动创建安装目录树,需要手工创建以下安装目录树。

在执行 make install 时,将出现错误信息,根据此信息可判断出需要创建以下目录。

```
[root@rh9 jpeg-6b]# mkdir -p /usr/local/gdlibforphp/jpeg/bin
[root@rh9 jpeg-6b]# mkdir -p /usr/local/gdlibforphp/jpeg/man/man1
[root@rh9 jpeg-6b]# mkdir -p /usr/local/gdlibforphp/jpeg/include
[root@rh9 jpeg-6b]# mkdir -p /usr/local/gdlibforphp/jpeg/lib
[root@rh9 jpeg-6b]# make
[root@rh9 jpeg-6b]# make install
```

下面将该软件包的库文件添加到/etc/ld. so. conf 文件中,以便其他需要使用该共享库的程序找到这些支持库。

```
[root@rh9 jpeg-6b]# echo "/usr/local/gdlibforphp/jpeg/lib">>/etc/ld. so. conf
[root@rh9 jpeg-6b]# ldconfig # 重新装载
[root@rh9 jpeg-6b]# ldconfig -p | grep "/usr/local/gdlibforphp/jpeg/lib" # 查看所添加的共享库
```

**注意:** 使用“>>”重定向符,千万不要用成“>”,否则将覆盖掉/etc/ld. so. conf 文件中的原内容。

## (2) 安装 zlib 库

```
[root@rh9 src]# tar -zxvf zlib-1.2.1.tar.gz
[root@rh9 src]# cd zlib-1.2.1
[root@rh9 zlib-1.2.1]# mkdir -p /usr/local/gdlibforphp/zlib
[root@rh9 zlib-1.2.1]# ./configure --help | less # 获得配置帮助
[root@rh9 zlib-1.2.1]# ./configure --shared --prefix=/usr/local/gdlibforphp/zlib \
> --libdir=/usr/lib --includedir=/usr/include
[root@rh9 zlib-1.2.1]# make
[root@rh9 zlib-1.2.1]# make install
```

此处将 zlib 的库和 include 头文件放在了标准的/usr/lib 和/usr/include 目录中。

## (3) 安装 libpng 库

```
[root@rh9 src]# tar -zxvf libpng-1.2.5.tar.gz
[root@rh9 src]# cd libpng-1.2.5
[root@rh9 libpng-1.2.5]# ./configure --help | less # 获得配置帮助
[root@rh9 libpng-1.2.5]# less INSTALL # 按提示查看安装帮助
[root@rh9 libpng-1.2.5]# cp scripts/makefile.gcc makefile
```

**提示:** libpng 没有使用 autoconf 技术,针对不同平台需要使用不同的 makefile。对于 Linux 平台应使用 scripts 目录下的 makefile. linux 或 makefile. gcc, 其中后者是针对 CPU 的 MMX 指令优化的文件。

```
[root@rh9 libpng-1.2.5]# make
```

```
[root@rh9 libpng 1.2.5]# make install-headers
[root@rh9 libpng-1.2.5]# make install
```

从输出的提示信息可知,libpng 的头文件安装在/usr/local/include/libpng12 目录中,库文件安装在/usr/local/lib 目录中。

```
[root@rh9 libpng-1.2.5]# echo "/usr/local/lib">> /etc/ld.so.conf
[root@rh9 libpng-1.2.5]# ldconfig
```

#### (4) 安装 freetype

```
[root@rh9 src]# rpm -qpl freetype-2.1.3-6.i386.rpm | less      # 查看库的安装位置
```

从输出的前 4 行可知是安装在/usr/lib 目录中。

```
[root@rh9 src]# rpm -ivh freetype-2.1.3-6.i386.rpm
```

#### (5) 安装 GD 库

```
[root@rh9 src]# tar -zxvf gd-2.0.28.tar.gz
[root@rh9 src]# cd gd-2.0.28
[root@rh9 gd-2.0.28]# mkdir -p /usr/local/gdlibforphp/gd
[root@rh9 gd 2.0.28]# ./configure --help
[root@rh9 gd-2.0.28]# ./configure --prefix=/usr/local/gdlibforphp/gd \
> - with-png = /usr/local/lib --with-jpeg = /usr/local/gdlibforphp/jpeg/lib --with-freetype -- /
usr/lib
```

**提示:** 还可使用“--libdir”和“--includedir”来指定库文件和头文件的安装位置,此处将其放在安装目录下面。

在配置过程中,会显示以下提示信息:

```
** Configuration summary for gd 2.0.28:
  Support for PNG library:      yes
  Support for JPEG library:     yes
  support for Freetype 2.x library: yes
  support for Xpm library:      no
  Support for pthreads:         yes
```

其中的 Xpm 是为 X-Windows 图形界面系统所使用的一个 pixmap 库,一般可不安装。

```
[root@rh9 gd-2.0.28]# make
[root@rh9 gd-2.0.28]# make install
```

安装完毕后,GD 的支持库和头文件位于/usr/local/gdlibforphp/gd/目录下,目录名

分别为 lib 和 include。最后还应将 gd.h 文件复制到 GD 的支持库目录下,编译 PHP 时需要该文件。

```
[root@rh9 gd-2.0.28]# cp gd.h /usr/local/gdlibforphp/gd/lib
[root@rh9 gd-2.0.28]# echo "/usr/local/gdlibforphp/gd/lib">>/etc/ld.so.conf
[root@rh9 gd-2.0.28]# ldconfig
```

#### (6) 安装 mm

mm-1.3.0.tar.gz 软件包为 PHP 提供 session storage 服务。

```
[root@rh9 src]# tar -zxvf mm-1.3.0.tar.gz
[root@rh9 src]# cd mm-1.3.0
[root@rh9 mm-1.3.0]# mkdir /usr/local/gdlibforphp/mm
[root@rh9 mm-1.3.0]# ./configure --prefix=/usr/local/gdlibforphp/mm
[root@rh9 mm-1.3.0]# make
[root@rh9 mm-1.3.0]# make install
```

安装完毕后,mm 的共享支持库安装在 /usr/local/gdlibforphp/mm/lib 目录中。

```
[root@rh9 mm-1.3.0]# echo "/usr/local/gdlibforphp/mm/lib">>/etc/ld.so.conf
[root@rh9 mm-1.3.0]# ldconfig
```

#### (7) 安装 libxml2

libxml2-2.5.11.tar.gz 软件包提供对 XML2 的支持。

```
[root@rh9 src]# tar -zxvf libxml2-2.5.11.tar.gz
[root@rh9 src]# cd libxml2-2.5.11
[root@rh9 libxml2-2.5.11]# mkdir /usr/local/gdlibforphp/xml2
[root@rh9 libxml2-2.5.11]# ./configure --prefix=/usr/local/gdlibforphp/xml2
[root@rh9 libxml2-2.5.11]# make
[root@rh9 libxml2-2.5.11]# make install
[root@rh9 libxml2-2.5.11]# echo "/usr/local/gdlibforphp/xml2/lib">>/etc/ld.so.conf
[root@rh9 libxml2-2.5.11]# ldconfig
```

### 3. 安装 PHP 软件包

#### (1) 编译方式简介

PHP 可以编译成两种方式运行,一种是编译成 Apache 的动态模块,将 PHP 作为 Apache 服务器的一个模块来运行,此时的配置方式应为: ./configure --with-apxs2=/usr/local/apache/bin/apxs。

参数“--with-apxs2”表示将 PHP 编译成 Apache 2.0 的模块。它调用 Apache 提供的实现程序 apxs(apache extension)来实现将其编译成 DSO 动态模块。

另一种是编译成 php.exe 和 php5apache2.dll 文件,以单独的 shell 方式来运行,此时的编译配置方式为: ./configure --prefix=/usr/local/php。

### (2) 编译时可选参数简介

在 PHP 的源代码目录执行“./configure -help”命令,可查看当前配置可使用的参数。常用的配置选项及功能如下:

--enable-track-vars	使 PHP 能追踪 HTTP_GET_VARS、HTTP_POST_VARS、HTTP_COOKIE_VARS 三个变量。
--enable-safe-mode	激活安全模式,为默认设置。
--enable-debug	打开内建的 PHP 调试器,便于 PHP 开发调试。
--enable-ftp	激活 FTP 功能支持。即让 PHP 支持 FTP 函数。
--enable-memory-limit	激活内存限制功能。
--enable-bcmath	使 PHP 支持 bcmath 高精度函数。
--enable-gd-native-ttf	使 PHP 支持 TrueType 函数。
--disable-xml	关闭对 XML 功能的支持。
--enable-wddx	激活对 WDDX 功能的支持。
--enable-sockets	激活对 sockets 功能的支持。
--enable-magic-quotes	让程序执行时自动加入反斜线的引入符号,为默认设置。
--enable-url-includes	让 PHP 程序能包含远程(HTTP 或 FTP)服务器的文件。
--with-openssl-dir< [= dir]>	用于指定 openssl 的安装目录,使系统支持 Open SSL。
with-openssl[ = dir]	功能与上相同,要求 OpenSSL 的版本号大于或等于 0.9.6。
with-mm[ = dir]	指定 mm 的安装位置。为 PHP 提供 session storage 服务。
--with-mysql-sock[ = dir]	MySQL 的 mysql.sock(Socket 套接字)安装位置。
--with-mysql[ = dir]	指定 MySQL 的安装目录。
--with-apxs2[ = file]	指定 Apache 的 apxs 程序的位置。
--with-freetype-dir[ = dir]	指定 FreeType 2 功能库的安装目录。与 PHP 的绘图功能相关。
--with-ttf[ = dir]	指定 FreeType 1.X 功能库的安装目录。
--with-png-dir[ = dir]	指定 libpng 功能库的安装目录,使 PHP 支持 png 格式的图形。
--with-jpeg-dir[ = dir]	指定 libjpeg 功能库的安装目录,使 PHP 支持 jpeg 图形。
with-gd[ = dir]	指定 gd 功能库的安装目录,使用 PHP 支持绘图功能。
--with-zlib-dir[ = dir]	指定 zlib 功能库的安装目录。要求 zlib 库的版本 >= 1.0.9。
--with-zlib[ = dir]	与 --with-zlib-dir 参数项功能相同。
--with-tif-dir[ = dir]	指定 libtiff 功能库的安装目录。
--with-libxml-dir[ = dir]	指定 libxml2 功能库的安装目录。
--with-config-file-path <[dir]>	指定 PHP 配置文件 php.ini 的存放位置。

### (3) 编译安装 PHP

下面采取将 PHP 编译成 Apache 2.0 的动态模块,PHP 的编译配置方法为:

```
[root@rh9 root]# cd /usr/local/src
[root@rh9 src]# tar -zxvf php-5.0.1.tar.gz
[root@rh9 src]# cd php-5.0.1
```



```
[root@rh9 php-5.0.1]# ./configure --with-apxs2=/usr/local/apache2/bin/apxs \
> --enable-track-vars --enable-debug --enable-url-includes --enable-ftp --enable-safe-mode \
> --enable-sockets --with-mysql-sock=/tmp/mysql.sock --enable-bcmath \
> --enable-wddx --enable-magic-quotes --enable-memory-limit --enable-gd-native-ttf \
> --with-config-file-path=/usr/local/apache2/conf --with-mysql=/usr/local/mysql \
> --with-zlib-dir=/usr --with-png-dir=/usr/local --with-freetype-dir=/usr \
> --with-gd=/usr/local/gdlibforphp/gd --with-jpeg-dir=/usr/local/gdlibforphp/jpeg \
> --with-mm=/usr/local/gdlibforphp/mm --with-libxml-dir=/usr/local/gdlibforphp/xml2
[root@rh9 php-5.0.1]# make # 编译需要约 10 分钟左右
[root@rh9 php-5.0.1]# make install
[root@rh9 php-5.0.1]# ll /usr/local/apache2/modules/
-rwxr-xr-x 1 root root 11215172 Aug 20 13:37 libphp5.so # 若存在, 则编译成功
```

#### (4) 复制获得 PHP 的配置文件

PHP 是作为 Apache 的一个模块来运行的, 为配置方便, 此处编译配置时将其指定在了与 Apache 配置文件相同的位置。

PHP 的配置文件为 php.ini, 可从 PHP 的源代码目录中, 通过更名复制获得。

```
[root@rh9 php-5.0.1]# cp php.ini-recommended /usr/local/apache2/conf/php.ini
```

#### 4. 配置 Apache 使其支持 PHP 解析

PHP 模块编译好后, 接下来就可修改 Apache 的配置文件, 装载 PHP 模块, 以使 PHP 支持对 PHP 页面的解析。

```
[root@rh9 php-5.0.1]# vi /usr/local/apache2/conf/httpd.conf
```

① 在配置文件第一部分的末尾 (Listen 指令的下面), 有一个用于装载动态模块的位置, 在空白地方添加以下命令行, 装载 PHP 5 的 Apache 2.0 动态模块。

```
LoadModule php5_module modules/libphp5.so
```

② 然后在配置文件的 AddType 位置的空白地方, 添加以下命令行, 以增加 .php 和 .php3 等文件类型。

```
AddType application/x-httpd-php .php .phtml .php3
```

```
AddType application/x-httpd-php-source .phps
```

③ 最后在 DirectoryIndex 指令中增加 PHP 类型的主页文件, 比如设置为:

```
DirectoryIndex index.php index.php3 index.htm index.html default.htm default.html
```

#### 5. 配置 PHP

对 PHP 的配置通过 php.ini 配置文件来实现, 下面简单介绍一些常用的配置项。

```
[root@rh9 php-5.0.1]# vi /usr/local/apache2/conf/php.ini
```

<code>register_globals=Off On</code>	是否允许注册全局变量,默认为 Off,为安全起见,请设置为 Off。
<code>display_errors Off On</code>	是否显示脚本执行错误。PHP 开发调试阶段可开启,正式运行时,应关闭,否则将影响 PHP 的安全。根据错误信息,可获得服务器相关信息。
<code>log_errors= On Off</code>	是否允许记录错误日志。
<code>error_log - /usr/local/apache2/logs/php_error.log</code>	设置错误日志存放的位置。
<code>error_reporting=E_ALL</code>	用于设置脚本出错时的报告格式。
<code>safe_mode = Off On</code>	是否使用安全模式。
<code>max_execution_time -30</code>	脚本最大执行时间。
<code>max_input_time 60</code>	脚本最大输出时间。
<code>memory_limit = 8M</code>	PHP 脚本允许使用的内存限制。
<code>post_max_size 8M</code>	PHP 最大传递数据。
<code>default_charset "iso-8858-1"</code>	设置默认字符集,请更改设置为 GB 2312。默认未启用。
<code>file_uploads On Off</code>	是否允许 HTTP 文件传输。
<code>upload_tmp_dir -</code>	文件上传到服务器的临时存放位置。
<code>upload_max_filesize=2M</code>	文件上传大小限制。
<code>allow_url_fopen= On Off</code>	是否允许 PHP 使用 http 或 ftp 打开远程文件。
<code>SMTP=localhost</code>	PHP 中利用 mail() 函数发送邮件时使用的 SMTP 服务器地址。
<code>smtp_port = 25</code>	SMTP 服务所使用的端口。此为默认值,不需要更改。
<code>mysql.default_port=</code>	设置 MySQL 服务器所使用的端口号。默认为 3306。
<code>mysql.default_socket=</code>	设置 MySQL 通信所使用的 socket,对于采用源代码安装的 MySQL 服务器,请设置为 /tmp/mysql.sock。
<code>session.save_path="/tmp"</code>	session 对应文件的存放位置。默认未启用,若要使用 session 功能,请启用该设置项。
<code>session.save_handler=mm</code>	若编译时加上了 mm 的共享内存支持,请修改成 mm。
<code>disable_functions =phpinfo, get_cfg_var</code>	设置要禁止的函数 (phpinfo, get_cfg_var)。

## 6. 测试 PHP 解析

在修改完 Apache 和 PHP 的配置文件后,重新启动 Apache 服务器。

在 www.myweb.com 站点的根目录 (/usr/local/apache2/htdocs) 下,创建一个名为 index.php 的网页。

```
[root@rh9 root]# vi /usr/local/apache2/htdocs/index.php
```

然后输入以下网页文件内容:

```
<html>
<head><title>PHP TEST</title></head>
<body>
<? phpinfo();? >
</body>
```

</html>

在浏览器中键入 `http://www.myweb.com` 并回车,若出现如图 7.7 所示的页面内容,则说明 PHP 解析正常。

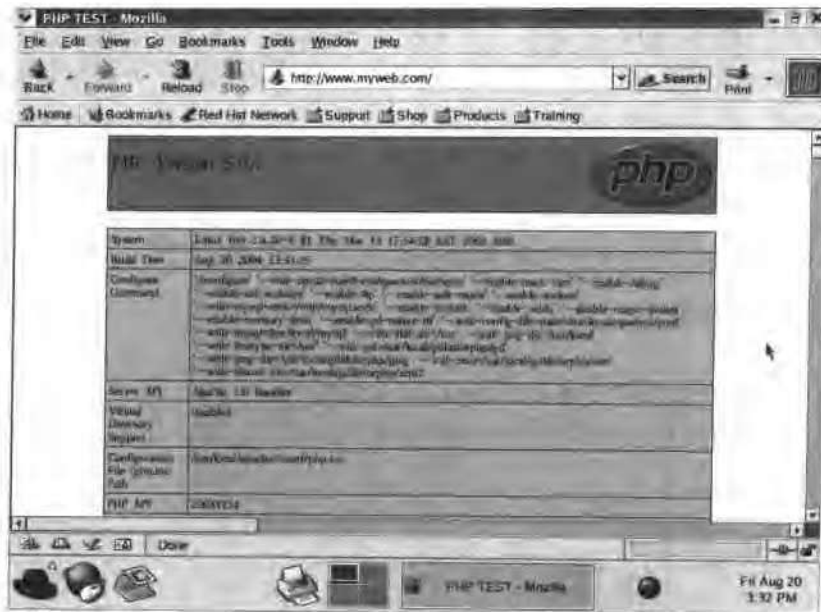


图 7.7 测试 PHP 解析

另外也可在宿主操作系统或其他主机的 IE 浏览器中,通过键入 `http://192.168.168.154` 来访问该 Web 站点。

PHP 解析正常了,下面测试 PHP 访问 MySQL 数据库,看是否正常。

首先以 root 用户身份登录 MySQL 服务器,以命令行方式创建名为 mywebdata 的数据库和名为 counter 的数据表,该数据表用作网站的访问计数。然后创建一个名为 webuser 的用户,以后利用该用户来实现基于网页访问后台数据库 MySQL,设置该账户只能在服务器本机登录,并只能访问 mywebdata 数据库,有 select、insert 和 update 权限。

```
[root@rh9 root]# cd /usr/local/mysql/bin
[root@rh9 bin]# ./mysql -u root -h localhost -p
Enter Password: *****
mysql> create database mywebdata;
mysql> use mywebdata;
mysql> create table counter(id int(11) not null auto_increment primary key, \
-> hits bigint(20) default 0);
```

```
Query OK, 0 rows affected (0.00 sec)
mysql> grant Select, Insert, Update on mywebdata. * to webuser@localhost \
--> identified by 'purelove0814';
mysql> quit
```

在前面创建虚拟主机时, 创建了一个域名为 www.myweb1.com 的 Web 站点, 该站点的根目录为 /var/www/myweb1, 先在该站点的根目录中创建一个名为 index.php 的页面。

注意: 在 httpd.conf 配置文件中设置 index.php 优先于 index.htm 或 index.html 解析。

```
[root@rh9 root]# vi /var/www/myweb1/index.php
```

然后输入以下内容:

```
<html>
<head><title>测试 PHP 与数据库 MySQL 的连接</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</head>
<body>
<? php
    if(! mysql_connect("localhost","webuser","purelove0814"))
    {
        echo "无法连接数据库."; exit(); //若无法连接, 则退出 PHP 脚本的执行
    }
    $query="select * from counter order by id asc"; // PHP 的变量以 $ 开头
    $result=mysql_db_query("mywebdata", $query); // 执行查询
    if(mysql_num_rows($result) != 0) //若返回的行数不为 0
    {
        $recValue=mysql_fetch_array($result); //将返回的记录保存在 recValue 数组中
        // 获取首记录的 hits 字段的值, 并加 1 输出。小数点为 PHP 的字符串连接符
        echo "访问次数: " . ($recValue["hits"]+1);
        $query="update counter set hits=hits+1"; //将计数器递增 1
        $result=mysql_db_query("mywebdata", $query); //执行 SQL 查询, 实现计数递增
    }
    else{
        $query="insert into counter (hits) values(1)"; //添加 1 条记录, 注意表名与括号间有空格
        $result=mysql_db_query("mywebdata", $query); //执行 SQL 查询, 实现添加记录
        echo "首次访问.";
    }
    // mysql_free_result($result);
    mysql_close(); //关闭连接
```

```
? >  
</body>  
</html>
```

保存文件,然后在浏览器中键入 `http://www.mywebl.com` 并回车,此时应看到有计数输出,刷新页面,计数值应递增。若 PHP 无法连接访问 MySQL 服务器,将显示相应的提示信息。

## 7.2.6 安装与配置 Perl 解释器

Perl 脚本可用于编写动态网页,很多基于 Web 的邮件客户端软件和管理性页面,以及一些论坛等,都是用 Perl 脚本编写的,为了使 Apache 服务器能支持解析 Perl 编写的 CGI 脚本,需要安装 Perl 脚本解释器。

一般在安装 Linux 系统时,通常已安装了该解释器,若未安装,可利用安装光盘提供的 RMP 安装包,或到官方网站下载最新的源代码软件包。

### 1. 检查是否安装 Perl 解释器

要检查当前 Linux 系统是否安装了 Perl 解释器,可使用以下命令来实现:

```
[root@rh9 root]# rpm -q perl  
perl-5.8.0-88
```

若输出了 Perl 的版本信息,则说明已安装。若未安装,可在 Red Hat Linux 9 的第一张安装光盘中,找到 Perl 的 RPM 安装包文件 `perl-5.8.0-88.i386.rpm`,然后利用以下命令即可实现安装。

```
[root@rh9 root]# rpm -ivh /mnt/cdrom//RedHat/RPMS/perl-5.8.0-88.i386.rpm
```

### 2. 利用源代码安装 Perl 解释器

从 `http://www.perl.org` 网站可下载到 Perl 的最新源代码软件包(`perl-5.8.5.tar.gz`),然后将其放在 `/usr/local/src` 目录中,其安装方法如下:

```
[root@rh9 root]# cd /usr/local/src  
[root@rh9 src]# tar -zxvf perl-5.8.5.tar.gz  
[root@rh9 src]# cd perl-5.8.5  
[root@rh9 perl-5.8.5]# sh Configure -de          # 使用默认配置  
[root@rh9 perl-5.8.5]# make                      # 编译  
[root@rh9 perl-5.8.5]# make test                 # 安装测试,也可不进行测试  
[root@rh9 perl-5.8.5]# make install              # 安装 Perl
```

在安装一次后,若要重新配置安装或升级安装之前,应使用“`rm -f config.sh Policy.sh`”命令,删除以前安装时的配置文件。

安装完成后,Perl 所在目录为 /usr/local/lib/perl5,Perl 的可执行文件(perl)放在 /usr/local/bin 目录中。

### 3. 修改 httpd.conf 配置文件,使 Apache 支持 Perl 脚本解析

在配置文件中保证有以下配置项,该配置项用于添加 Perl 脚本文件类型(扩展名为.cgi 或.pl)。

```
AddHandler cgi-script .cgi .pl
```

对存放 Perl 脚本的目录,要保证该目录有 ExecCGI 执行权限,这通常在<Directory>中进行设置,如下所示:

```
<Directory "/usr/local/apache2/htdocs">
    Indexes Includes FollowSymLinks ExecCGI SymLinksIfOwnerMatch MultiViews
    Option Indexes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

对存放 Perl 脚本的目录,利用 ScriptAlias 语句定义一个别名,以便于访问。通常定义别名为/cgi-bin/,表示站点根目录下的 cgi-bin 目录。这有点类似于在 IIS 中创建虚拟目录。

比如,若 Perl 脚本安装在/usr/local/apache2/cgi-bin/目录中,则可定义为:

```
ScriptAlias /cgi-bin/ "/usr/local/apache2/cgi-bin/"
```

以后在浏览器中键入“http://网站 URL 地址/cgi-bin”,即可访问用 Perl 脚本编写的网页了。

## 7.2.7 安装与配置 phpMyAdmin

phpMyAdmin 是一个用 PHP 编写的基于网页的 MySQL 数据库管理工具。利用该工具,可实现对 MySQL 数据库的管理、包括数据库、数据表的创建、数据的添加、编辑修改和删除等数据库操作,功能十分强大。

phpMyAdmin 软件包可从“http://sourceforge.net/projects/phpmyadmin/”网站下载,目前最新版本为 phpMyAdmin-2.6.0-rc1.tar.gz,下面介绍其安装、配置与使用方法。

### 1. 安装 phpMyAdmin 软件包

```
[root@rh9 src]# mkdir /usr/local/apache2/htdocs/phpMyAdmin
[root@rh9 src]# tar -zxvf phpMyAdmin-2.6.0-rc1.tar.gz
[root@rh9 src]# cp -a phpMyAdmin-2.6.0-rc1/* /usr/local/apache2/htdocs/phpMyAdmin/
```

```
[root@rh9 src]# cd /usr/local/apache2/htdocs/phpMyAdmin/
```

## 2. 修改 phpMyAdmin 配置文件

```
[root@rh9 phpMyAdmin]# vi config.inc.php
```

然后根据实际情况,修改配置文件中以下几行的相关内容:

```
$cfg['PmaAbsoluteUri'] = 'http://网站域名/phpMyAdmin/';
$cfg['Servers'][$i]['socket'] = '/tmp/mysql.sock';
$cfg['Servers'][$i]['controluser'] = 'root';
$cfg['Servers'][$i]['controlpass'] = 'yourpassword';
$cfg['Servers'][$i]['auth_type'] = 'config';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'yourpassword';
$cfg['DefaultLang'] = 'zh';
$cfg['DefaultCharset'] = 'gb2312';
```

## 3. 运行 phpMyAdmin

phpMyAdmin 用于对 MySQL 数据库进行全面的管理,功能很强大,应注意限制用户随意访问。

在浏览器地址栏中键入“http://192.168.168.154/phpMyAdmin”,即可访问 phpMyAdmin 页面了,如图 7.8 所示。

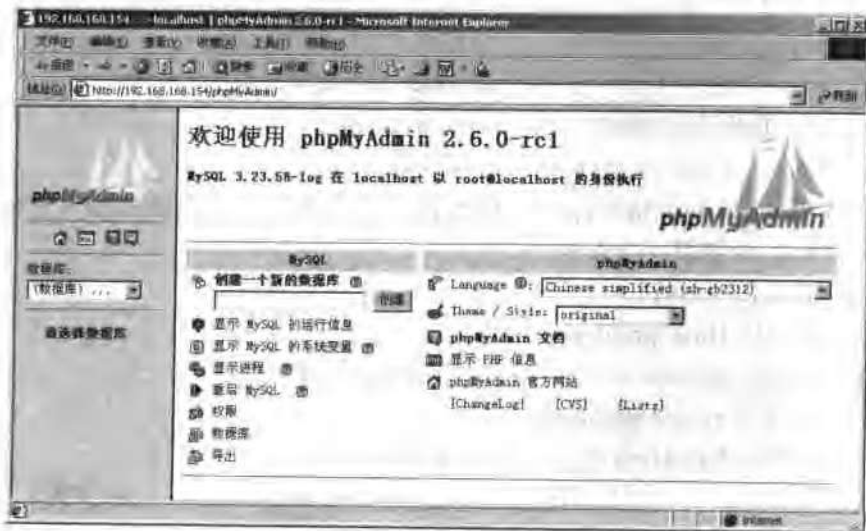


图 7.8 phpMyAdmin 主界面

## 习题

1. 利用 RPM 软件包安装的 MySQL 数据库服务器,其数据库默认存放在( )。  
A. /var/lib/mysql  
B. /usr/local/mysql  
C. /usr/local/mysql/data  
D. /usr/local/mysql/share/mysql
2. 若要设置 MySQL 的 root 用户的密码为“ner \* 24361 #”,以下命令中正确的是( )。  
A. mysql -u root -p "ner \* 24361 #"  
B. mysql -u root -h localhost password "ner \* 24361 #"  
C. mysqladmin -u root -p "ner \* 24361 #"  
D. mysqladmin -u root password "ner \* 24361 #"
3. 在 MySQL 中,若要选择使用名为 mysql 的数据库,则实现命令为( )。  
A. show databases;  
B. use database mysql;  
C. use mysql;  
D. select \* from mysql;
4. 若 MySQL 启动失败,可通过查看( )错误日志文件来了解启动失败的原因。  
A. /var/lib/mysql/rh9.err  
B. /var/log/rh9.log  
C. /var/log/mysql.log  
D. /var/lib/mysql/mysql/rh9.err
5. 若要备份名为 MySQL 的数据库,可使用( )命令来实现,若要从备份文件中恢复数据,则应使用( )命令。  
A. mysqladmin  
B. mysqldump -u root -p --opt mysql > /mysqlbak.sql  
C. mysqladmin -u root -p < /mysqlbak.sql  
D. mysql -u root -p mysql < /mysqlbak.sql
6. 若使用 insert into 语句直接在 MySQL 数据库的 user 表中添加用户,为使所添加的用户立即生效,应使用( )命令。  
A. mysql>fresh;  
B. mysql>flush privileges;  
C. mysql>mysqladmin -u root -p flush-privileges;  
D. mysql>reload privileges;
7. Linux 操作系统中,最常用的 Web 服务器是( )。  
A. Apache  
B. IIS  
C. Tomcat  
D. PWS
8. 启动 Apache 服务器的命令是( )。  
A. service apache start  
B. server http start



- C. service httpd start                      D. service httpd reload
9. 使用 RPM 软件包安装的 Apache 服务器,其配置文件位于( ),默认的站点根目录是( )。
- A. /etc/httpd.conf                      B. /etc/httpd/conf/httpd.conf  
C. /var/www/html                      D. /var/www
10. 对于采用源代码安装的 Apache 服务器,假设安装在/usr/local/apache2 目录中,其最正确的启动方法是( )。
- A. service apachectl start  
B. /usr/local/apache2/bin/apachectl start  
C. server apachectl start  
D. /usr/local/apache2/bin/httpd start
11. 若要设置 Web 站点根目录的位置,应在配置文件中通过( )配置语句来实现。
- A. ServerRoot                      B. ServerName  
C. DocumentRoot                      D. DirectoryIndex
12. 若要设置网页默认使用的字符集为简体中文,则应在配置文件中添加( )配置项。
- A. DefaultCharset GB2312                      B. AddDefaultCharset GB2312  
C. DefaultCharset ISO-8859-1                      D. AddDefaultCharset GB5
13. 若要设置 Apache 服务器允许持续连接,则设置命令为( )。
- A. KeepAlive On                      B. KeepAliveTimeout 10  
C. MaxKeepAliveRequests 100                      D. KeepConnect On
14. 设置站点的默认主页,可在配置文件中通过( )配置项来实现。
- A. RootIndex                      B. ErrorDocument  
C. DocumentRoot                      D. DirectoryIndex
15. 以下描述中,不正确的是( )。
- A. Apache 服务器,可支持 .htm、.html 和 .php 网页的解析  
B. 以模块方式编译安装 PHP 解释器后,必须在 httpd.conf 配置文件中加载 PHP 模块并增加 .php 文件类型,Apache 服务器才能支持对 .php 页面的解析  
C. 对 .php 页面的解析是由客户端浏览器负责的,因此,服务器端可以不安装 PHP  
D. 对 mysql 数据库的管理,可使用 phpmyadmin 管理工具来实现

## 实训 7-1 安装与配置 MySQL 服务器

**[实训目的]** 了解 Linux 软件包的安装方法,掌握 MySQL 服务器的安装与配置,掌握常用的 MySQL 操作命令与用户权限管理方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 在 VMware Workstation 未启动的情况下,将 Red Hat Linux 虚拟主机工作目录下的文件进行备份,以备份一个未安装 MySQL 服务器的 Linux 系统,以供练习 MySQL 源代码安装方式。一般应有 4 个文件,其文件名分别为 nvram、Red Hat Linux.vmdk、Red Hat Linux 2.vmx 和 vmware.log。

2. 启动 Linux 虚拟主机,并按教材所讲的步骤和方法,采用 RPM 软件包方式,安装 MySQL 服务器。

3. 登录 MySQL 服务器,并练习 show database、use mysql、show tables、describe user、select host、user、password from user、exit 和 quit 命令,掌握其功能和用法。

4. 练习不同的登录方法。分别练习以下登录方式,查看效果是否相同。假设 Linux 的主机名为 rh9,root 用户的密码为 mybaby,若不同,练习时请换成实际的主机名和密码。

```
[root@rh9 root]# /usr/bin/mysql -u root -p -h localhost
[root@rh9 root]# /usr/bin/mysql -u root -p -h rh9
[root@rh9 root]# /usr/bin/mysql -uroot -pmybaby -hrh9
[root@rh9 root]# /usr/bin/mysql -u anybody
```

5. 关闭 Linux 操作系统,退出虚拟主机管理器,将还未安装 MySQL 时的虚拟主机备份文件,重新复制到虚拟主机的工作目录,并覆盖相同的文件,以使 Linux 恢复到未安装 MySQL 服务器的状态。

6. 重新启动虚拟主机,按本书所讲的步骤和方法,采用源代码方式安装 MySQL 服务器。

7. 在 MySQL 数据库的 user 数据表中,添加一个名为 admin 的用户,用户密码为 linux,该用户可从任意地方登录 MySQL 服务器,拥有 select、insert、delete 和 update 权限。然后利用该用户登录 MySQL 服务器,看能否访问 MySQL 数据库和 webdata 数据库。

8. 创建一个名为 webadmin 的用户,用户密码为 anyone,该用户只能访问 webdata 数据库,有 select、insert、delete 和 update 权限。然后利用该用户登录,看能否访问 MySQL 数据库,然后再访问 webdata 数据库,并进行 select、insert、delete 和 update 等操作。

作,看操作能否成功。

9. 练习用不同的主机远程登录 MySQL 服务器。假设当前宿主操作系统(即用来安装虚拟主机的操作系统)是 Windows 2000,IP 地址为 192.168.168.65, Linux 虚拟主机的 IP 地址为 192.168.168.154。利用 Windows 2000 开始菜单的“运行”功能,执行 cmd 命令,进入 MS-DOS 方式,然后登录访问 MySQL 服务器。但 Windows 2000 系统中应安装 MySQL 的客户端程序,可到 MySQL 站点下载安装 Windows 版本的 MySQL。

## 实训 7-2 安装与配置 WWW 服务器

**[实训目的]** 熟悉并掌握在 Linux 平台,Web 服务器和 PHP 解释器的配置步骤与方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实作。

**[实训内容]**

1. 安装并配置 Apache 2.0 服务器,在默认站点根目录/usr/local/apache2/htdocs 中,利用 vi 创建一个简单网页文件 index.htm,然后访问该默认站点,以检查 web 服务器工作是否正常。

2. 按本书例 7.3~例 7.8 所讲步骤和方法,配置并测试虚拟主机。

3. 按本书所讲步骤和方法,安装 PHP 解释器,并创建一个简单的 PHP 网页,测试 Web 服务器能否正常解析 PHP 脚本。

## 第 8 章

# 配置 FTP 服务器

FTP(file transfer protocol,文件传输协议)服务器利用文件传输协议实现文件的上传与下载服务,从而实现文件存储和交换的目的。FTP 服务也是目前 Internet 应用很广泛的服务之一,利用 FTP 服务,可实现将 Web 站点所需的文件上传到远程的 Web 服务器,或者从服务器下载到本地。

Red Hat Linux 9 自带 vsftpd FTP 服务软件包,其名称为 vsftpd-1.1.3-8.i386.rpm,位于第 3 张安装光盘中。vsftp(very security FTP)意为非常安全的 FTP 服务器,vsftpd 是 vsftp 服务器的一个守护进程,用于具体实现 FTP 服务器的功能。

除了使用 vsftpd 作 FTP 服务器,也可选择另一个很优秀的 ProFTP 作为 FTP 服务器,相应的软件包可到官方网站(<http://www.proftp.org>)下载。

本章以 vsftpd 为例,介绍 FTP 服务器的安装、配置与使用方法。

### 8.1 安装 vsftpd 服务器

若在安装 Linux 系统时,已选择安装了 FTP 服务,则 vsftpd 服务器已安装好了;若未安装,则可使用 vsftpd-1.1.3-8.i386.rpm 软件包来安装。

#### 1. 检查是否安装 vsftpd 服务器

在使用或安装 vsftpd 服务器之前,应先检测当前系统是否已安装了该服务。其方法为:

```
[root@rh9 root]# rpm -q vsftpd
vsftpd-1.1.3-8                                #说明当前系统已安装
```

若未安装,则可采用以下命令来安装:

```
[root@rh9 root]# rpm -ivh /mnt/cdrom/RedHat/RPMS/vsftpd-1.1.3-8.i386.rpm
```

## 2. 设置 vsftpd 服务的自启动

vsftpd 服务安装后,默认情况下,该服务并未启动,可采用以下命令来检查其启动状态:

```
[root@rh9 root]# chkconfig list vsftpd
vsftpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

若要设置该服务在 3 和 5 运行级别时自动启动,则设置命令为:

```
[root@rh9 root]# chkconfig --level 35 vsftpd on
[root@rh9 root]# chkconfig --list vsftpd
vsftpd 0:off 1:off 2:off 3:on 4:off 5:on 6:off
```

## 3. vsftpd 的配置与访问控制文件

对 vsftpd 服务器的配置,通过 vsftpd.conf 配置文件来完成,该配置文件位于/etc/vsftpd 目录中。在/etc 目录下面还有两个 vsftpd 的用户访问控制文件,其文件名分别为 vsftpd.user\_list 和 vsftpd.ftpusers。vsftpd.ftpusers 用于定义不允许登录 FTP 服务器的用户列表;vsftpd.user\_list 用于定义允许或不允许登录的用户列表,这由 userlist\_deny 的设置进一步确定。

## 4. vsftpd 服务器的启动脚本

vsftpd 服务器在/etc/rc.d/init.d 目录下,有一个名为 vsftpd 的服务启动脚本,利用该脚本,可实现 vsftpd 服务器的启动、重启、状态查询、停止等操作。

- 启动 vsftpd 服务器的实现命令: /etc/rc.d/init.d/vsftpd start 或 service vsftpd start。
- 重启 vsftpd 服务器的实现命令: /etc/rc.d/init.d/vsftpd restart 或 service vsftpd restart。
- 查询 vsftpd 服务器状态的实现命令: /etc/rc.d/init.d/vsftpd status 或 service vsftpd status。
- 停止 vsftpd 服务器的实现命令: /etc/rc.d/init.d/vsftpd stop 或 service vsftpd stop。

## 5. 测试 vsftpd 服务器

vsftpd 服务器安装并启动服务后,用其默认配置,就可以正常工作了。vsftpd 默认的匿名用户账户为 ftp,密码也为 ftp,默认允许匿名用户登录,登录后所在的 FTP 站点根目录为/var/ftp 目录。下面使用 ftp 命令登录 vsftpd 服务器,以检测该服务器能否正常工作。

```

[root@rh9 root]# service vsftpd start
Starting vsftpd for vsftpd: [OK]
[root@rh9 root]# ftp 192.168.168.154 # ftp 是用于连接 FTP 服务器的命令
Connected to 192.168.168.154 (192.168.168.154)
220 (vsFTPd 1.1.3)
Name (192.168.168.154:root):ftp # 输入登录者的用户名
331 Please specify the password.
Password: # 输入用户密码
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> # 登录成功, 出现 FTP 的命令行提示符

```

FTP 登录成功后, 将出现 FTP 的命令行提示符 `ftp>`。在命令行中, 键入 FTP 命令, 可实现相关的操作, 比如, 用 `ls` 命令查看当前目录的文件目录列表, `mkdir` 建立目录, `rm` 删除目录, 用 `get` 或 `mget` 实现下载文件, `put` 或 `mput` 实现上传文件, `cd` 或 `lcd` 切换服务器端或本地的目录, 用 `quit` 或 `exit` 退出 `ftp` 登录等。在 `ftp>` 状态下键入 `?`, 可获得可用的 `ftp` 命令帮助, 有关 `ftp` 命令的具体用法, 将在 8.6 节介绍。

## 8.2 连接和访问 FTP 服务器

### 1. 创建 FTP 账户

对于有较高安全要求的 FTP 服务器一般不允许匿名访问, 或给匿名用户很低的访问权限。一般应以本地用户账户来登录和访问 FTP 服务器, 因此在使用和访问 FTP 服务器之前, 应根据需要, 创建好所需的 FTP 账户。作为 FTP 登录使用的账户, 其 Shell 应设置为 `/sbin/nologin`, 以使用户账户只能用来登录 FTP, 而不能用来登录 Linux 系统。

`vsftpd` 在安装时会自动创建 FTP 系统用户组和属于该组的 FTP 系统用户, 该用户的主目录为 `/var/ftp`, 默认作为 FTP 服务器的匿名账户。

```

[root@rh9 root]# grep ftp /etc/passwd
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
[root@rh9 root]# grep ftp /etc/group
ftp:x:50:

```

在默认配置下, 本地用户登录 FTP 服务器后, 所在的 FTP 目录为该用户的主目录, 因此在创建用户时, 还应指定该用户的主目录。若未指定, 系统默认将主目录放在 `/home` 目录下, 目录名与账户名相同。

利用不同账户登录 FTP 服务器后, 其 FTP 站点根目录不同的特点, 可将用户 Web

站点根目录与该用户的FTP站点根目录设置为相同,这样用户就可利用FTP连接远程管理Web站点下的目录和文件,实现对站点文件的删除、更名、上传和下载等操作,以实现对Web服务器的远程管理。

若要求各FTP用户登录后,其站点根目录均为同一个目录,比如,用于提供软件下载的FTP站点,此时可将各用户的主目录都设置为FTP站点的根目录即可。

## 2. 登录和访问FTP服务器

FTP服务器启动并创建好FTP账户后,登录和访问FTP服务器有3种方法。

(1) 在Linux的文本模式或Windows平台的MS-DOS方式下,利用“ftp 服务器IP地址”命令,以文本方式通过ftp命令来连接和访问FTP服务器。

(2) 在浏览器中,利用ftp协议来访问FTP服务器,访问格式为:

ftp://用户名:用户密码@网站域名 或 ftp://用户名@网站域名

(3) 使用图形化的FTP客户端软件来连接和访问FTP服务器,以简化操作。在Windows平台,推荐使用CuteFTP Pro软件;在Linux的图形界面,可使用gftp命令或gFTP开始菜单项,来启动Linux的图形化FTP客户端软件。另外,gftp也可在Linux的文本模式下运行,此时的界面和操作方式与ftp类似。

下面用示例分别介绍连接和访问FTP服务器的方法,以及gftp客户端软件的使用。

**[例 8.1]** 试创建一个名为webftp1的系统用户,属于ftp组,不允许登录Linux系统,其上目录为/var/www/myweb1,然后利用该账户以文本方式登录FTP服务器(192.168.168.154),并查看所在目录的路径和当前目录下的文件列表,接着新建一个名为downloads的目录,并将本地/usr/local/src目录下的php-5.0.1.tar.gz文件,上传到downloads目录中,并查看上传结果。

操作步骤:

① 创建用户和用户组。由于ftp组是已存在的组,因此不再需要创建,下面直接创建用户账户。

```
[root@rh9 root]# useradd webftp1 -r -m -g ftp -d /var/www/myweb1 -s /sbin/nologin -c "FTP User"
[root@rh9 root]# passwd webftp1                                     # 设置账户密码
Changing password for user webftp1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@rh9 root]# grep webftp1 /etc/passwd                             # 查看账户记录
webftp1:x:101:50:FTP User:/var/www/myweb1:/sbin/nologin
```

## ② 设置用户主目录的所有者、所属的组和权限。

在创建用户账户时,若主目录不存在,利用-m 参数,可自动创建所需的主目录,此时主目录的所有者和所属组是正确的,不需要设置和修改。若在创建用户之前,指定的主目录已存在,则应检查并设置和修改所有者和所属的组。

```
[root@rh9 root]# ll /var/www/
drwxr-xr-x 2 root root 4096 Aug 22 09:59 myweb1
[root@rh9 root]# chown webftp1 /var/www/myweb1
[root@rh9 root]# chgrp ftp /var/www/myweb1
[root@rh9 root]# ll /var/www/
drwxr-xr-x 2 webftp1 ftp 4096 Aug 22 09:59 myweb1
```

设置用户对主目录的权限。主目录的所有者默认有 rwx,对于 Web 站点,所属组和其他用户有读和执行权限即可。在 Linux 系统中,用户对目录必须有执行权限,这样才能进入和访问该目录下的文件和子目录。设置命令为:

```
[root@rh9 root]# chmod 755 /var/www/myweb1
[root@rh9 root]# ll /var/www
drwxr-xr-x 2 webftp1 ftp 4096 Aug 22 09:59 myweb1
```

## ③ 使用 ftp 命令登录 FTP 服务器,然后进行所要求的操作。

```
[root@rh9 root]# ftp 192.168.168.154
Connected to 192.168.168.154 (192.168.168.154)
220 (vsFTPd 1.1.3)
Name (192.168.168.154:root):webftp1          # 输入用户名 webftp1
331 Please specify the password.
Password:                                   # 输入用户密码
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>ls                                     # 查看当前目录的文件列表
227 Entering Passive Mode (192.168.168.154,156,131)
150 Here comes the directory listing.
-rw-r--r--      1    0    0    105   Aug  18 03:24      index.html
-rwxr-xr-x      1    0    0   1188   Aug  20 09:33      index.php
226 Directory send OK.
ftp>pwd                                     # 查询当前目录路径
257 "/var/www/myweb1"
ftp>mkdir downloads                         # 创建子目录
257 "/var/www/myweb1/downloads" created
```



```

ftp>ls
227 Entering Passive Mode (192,168,168,154,21,174)
150 Here comes the directory listing.
drwxr-xr-x  2 101  50  4096  Aug  22 03:04  downloads
-rw-r--r--  1   0   0   105  Aug  18 03:24  index.html
-rwxr-xr-x  1   0   0  1188  Aug  20 09:33  index.php
226 Directory send OK.
ftp>put /usr/local/src/php-5.0.1.tar.gz  downloads/php-5.0.1.tar.gz      # 上传文件
local: /usr/local/src/php-5.0.1.tar.gz  remote: downloads/php-5.0.1.tar.gz
227 Entering Passive Mode (192,168,168,154,221,139)
150 OK to send data.
226 File receive OK.
5619589 bytes sent in 0.579 secs (9.5e+03 Kbytes/sec)
ftp>cd downloads                    # 进入 downloads 目录
250 Directory successfully changed.
ftp>ls                              # 查看所上传的文件
227 Entering Passive Mode (192,168,168,154,52,102)
150 Here comes the directory listing.
-rw-r--r--  1 101  50    5619589  Aug 22 03:16  php-5.0.1.tar.gz
226 Directory send OK.
ftp>cd ..
250 Directory successfully changed.
ftp>quit
221 Goodbye.
[root@rh9 root]# startx              # 启动 X-Windows 界面,在浏览器中检验文件下载

```

④ 启动 mozilla 浏览器,在地址栏中键入以下地址,下载 php-5.0.1.tar.gz 软件包,检查下载能否成功。

http://www.myweb1.com/downloads/php-5.0.1.tar.gz

键入以上地址并回车后,应出现如图 8.1 所示的提示对话框。

选择 Save this file to disk,单击 OK 按钮,就会弹出文件另存为对话框,选择要保存到的目录位置,就开始下载软件了,这种下载方式是通过 HTTP 协议来实现的。另外,也可利用 FTP 客户端软件来下载。

[例 8.2] www.myweb1.com 网站的管理员账户为 webftp1,试利用浏览器来访问该网站的 FTP 站点,并下载 downloads 目录下的 php-5.0.1.tar.gz 软件包。

操作步骤:

① 单击红帽子右边的图标,启动 Mozilla 浏览器。

② 为安全起见,最好不要在地址中包含账户密码信息。因此,在浏览器地址栏中输入地址 ftp://webftp1@www.myweb1.com,然后按回车键,此时将弹出图 8.2 所示的对

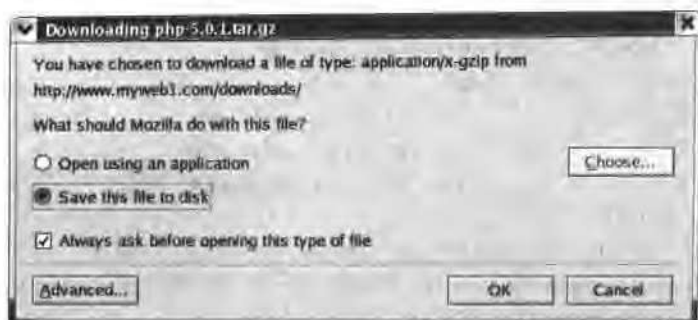


图 8.1 下载对话框

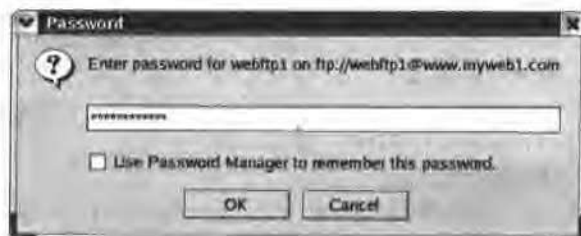


图 8.2 登录密码对话框

话框,要求输入该账户的密码。

输入账户密码并单击 OK 按钮后,浏览器将以文件列表的形式,显示出该站点的目录和文件列表。单击 downloads 目录,将进入到该目录中,并显示该目录的文件列表,最后单击 php-5.0.1.tar.gz 文件,即可实现软件的下载。

以上是在 Linux 平台利用 Mozilla 浏览器来实现的,也可在 Windows 平台,利用 IE 浏览器用同样的方法来访问。由于 IE 浏览器的功能比 Mozilla 要强大得多,因此,在 IE 浏览器中,除可实现下载外,还可实现上传,以及对文件或目录的更名或删除等操作,其操作方式与 Windows 的资源管理器相同,建议使用 IE 浏览器来访问 FTP 站点。

### 3. Linux 的 FTP 客户端软件

Linux 提供了 FTP 客户端软件 gFTP,其界面和操作方式与 Windows 平台的 CuteFTP Pro 很类似,功能强大,使用简单、方便。

#### (1) 启动 gFTP

在 Linux 图形界面,依次单击“红帽子”→Internet→More Internet Applications→gFTP,就可启动 gFTP 软件,如图 8.3 所示。另外,也可在命令行执行 `gftp&` 命令来启动。

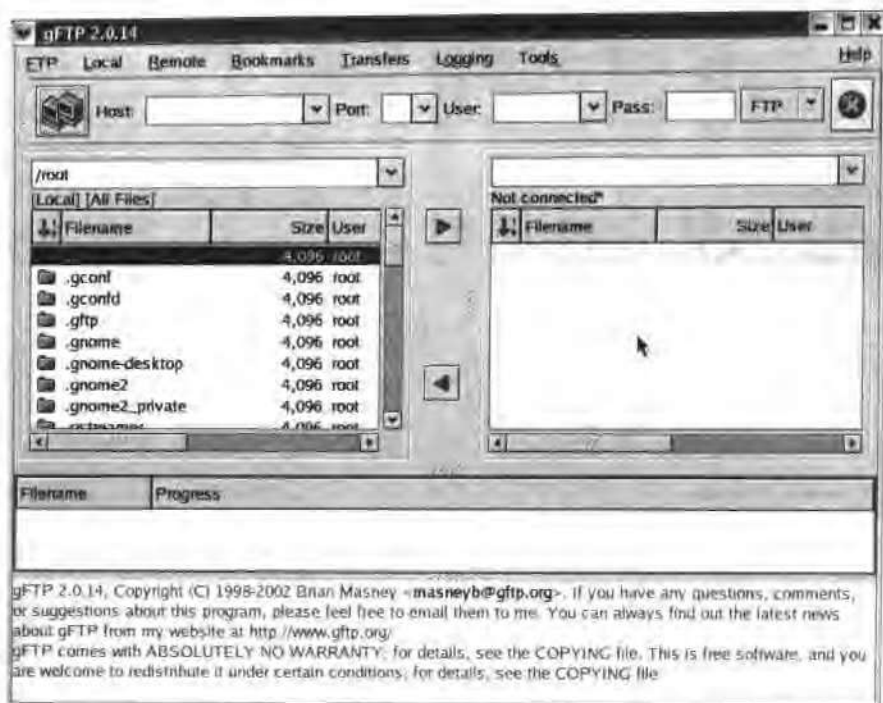


图 8.3 gFTP 主界面

### (2) 连接 FTP 服务器

在 gFTP 主界面顶部的 Host 输入框中输入要登录的 FTP 服务器的 IP 地址,在 Port 中输入 FTP 服务器所使用的端口,标准端口为 21,在 User 中输入要登录的 FTP 账户,在 Pass 输入框中,输入 FTP 账户对应的密码,然后单击 Host 左边的按钮,即可实现与 FTP 服务器的连接,连接后的 gFTP 主界面如图 8.4 所示。在 Remote 菜单中选择 Disconnect 可断开连接。

### (3) gFTP 主界面组成简介

主界面最底部是状态显示栏,显示各操作对应的命令及命令执行的状态。图 8.4 中,鼠标指针所指的区域为正在上传或下载的文件列表;中间部分左边一栏上面的组合框用于输入本地目录的路径;下面的列表框,则用于显示刚才所输入目录中的文件和子目录列表;右边一栏用于显示远程 FTP 服务器上的目录和目录下的文件及子目录列表。

### (4) gFTP 操作

利用 gFTP 可实现文件的上传、下载、更名或删除文件,创建目录等操作。对本地文件的操作,相关操作命令由 Local 菜单提供,对于远程 FTP 服务器中的文件目录操作,则通过 Remote 菜单提供的相关命令来实现。

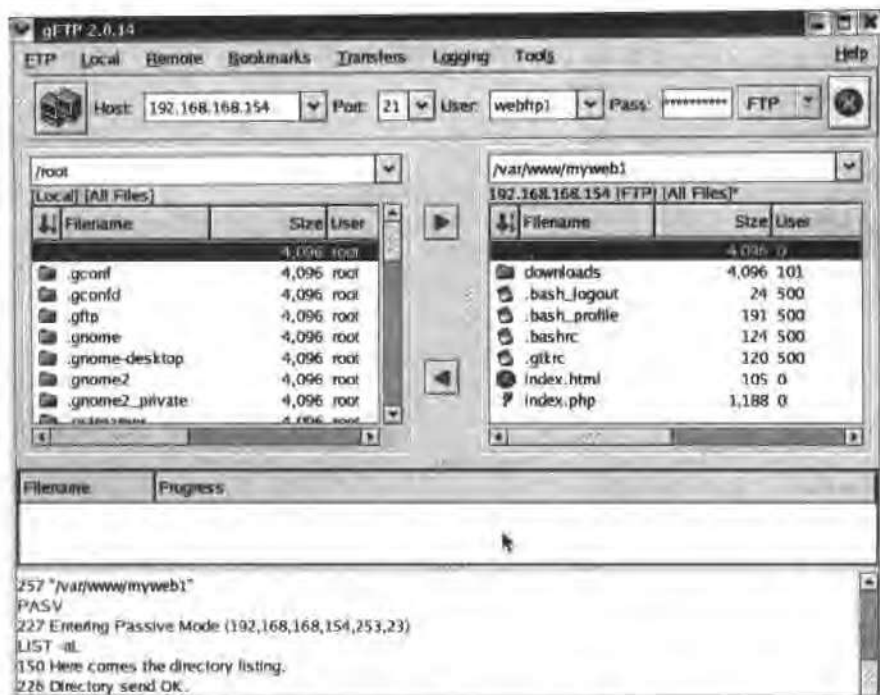


图 8.4 登录成功的 gFTP 主界面

在左边的组合框中输入 `/usr/local/src` 并回车,就可在本地(Local)文件列表框中显示出 `/usr/local/src` 目录中的文件目录列表,选中要上传的文件,将其拖动到右边的远程文件列表框中的某目录上,然后释放鼠标按键,即可实现将这些文件上传到指定的目录中。另外,在选中文件后,也可单击列表框旁边带右箭头的按钮。下载则向相反方向拖动,或单击带有向左箭头的按钮实现下载。

gFTP 的操作方式与 Windows 系统类似,就不再详细介绍。

### 8.3 配置 vsftpd 服务器

为了让 FTP 服务器能更好地按要求提供服务,就需要对 FTP 服务器的配置文件进行合理、有效地配置。vsftpd 提供的配置命令较多,默认配置文件只列出了最基本的配置命令,很多配置命令在配置文件中并未列出来。下面介绍一些常用的配置命令。

vsftpd 配置文件采用“#”作为注释符,以“#”开头的行和空白行在解析时将被忽略,其余的行被视为配置命令行,每个配置命令的“=”两边不要留有空格。对于每个配置命令,在配置文件中还列出了相关的配置说明,利用 vi 编辑器可实现对配置文件的编辑

修改。

```
[root@rh9 root]# vi /etc/vsftpd/vsftpd.conf
```

### 1. 登录和对匿名用户的设置

- `write_enable=YES` 是否对登录用户开启写权限。属于全局性设置。
- `local_enable=YES` 是否允许本地用户登录FTP服务器。
- `anonymous_enable=YES` 设置是否允许匿名用户登录FTP服务器。
- `ftp_username=ftp` 定义匿名用户的账户名称,默认值为ftp。
- `no_anon_password=YES` 匿名用户登录时是否询问口令。设置为YES,则不询问。
- `anon_world_readable_only=YES` 匿名用户是否允许下载可阅读的文档,默认为YES。
- `anon_upload_enable=YES` 是否允许匿名用户上传文件。只有在`write_enable`设置为YES时,该配置项才有效。
- `anon_mkdir_write_enable=YES` 是否允许匿名用户创建目录。只有在`write_enable`设置为YES时有效。
- `anon_other_write_enable=NO` 若设置为YES,则匿名用户会被允许拥有多于上传和建立目录的权限,还会拥有删除和更名权限。默认值为NO。

### 2. 设置欢迎信息

用户登录FTP服务器成功后,服务器可向登录用户输出预设置的欢迎信息。

```
ftpd_banner=Welcome to blah FTP service.
```

该配置项用于设置比较简短的欢迎信息。若欢迎信息较多,则可使用`banner_file`配置项。

- `banner_file=/etc/vsftpd/banner` 设置用户登录时,将要显示输出的文件。该设置项将覆盖`ftpd_banner`的设置。
- `dirmessage_enable=YES` 设置是否显示目录消息。若设置为YES,则当用户进入目录时,将显示该目录中的由`message_file`配置项指定的文件(.message)中的内容。
- `message_file=.message` 设置目录消息文件。可将要显示的信息存入该文件。

### 3. 设置用户登录后所在的目录

- `local_root=/var/ftp` 设置本地用户登录后所在的目录。默认配置文件中没有设置该项,此时用户登录FTP服务器后,所在的目录为该用户的主目录,对于

root 用户,则为 /root 目录。

- anon\_root=/var/ftp 设置匿名用户登录后所在的目录。若未指定,则默认为 /var/ftp 目录。

#### 4. 控制用户是否允许切换到上级目录

在默认配置下,用户可以使用“cd ..”命名切换到上级目录。比如,若用户登录后所在的目录为 /var/ftp,则在“ftp>”命令行下,执行“cd ..”命令后,用户将切换到其上级目录 /var,若继续执行该命令,则可进入 Linux 系统的根目录,从而可以对整个 Linux 的文件系统进行操作。若设置了 write\_enable=YES,则用户还可对根目录下的文件进行改写操作,会给系统带来极大的安全隐患,因此,必须防止用户切换到 Linux 的根目录,相关的配置项如下:

- chroot\_list\_enable=YES 设置是否启用 chroot\_list\_file 配置项指定的用户列表文件。
- chroot\_list\_file=/etc/vsftpd.chroot\_list 用于指定用户列表文件,该文件用于控制哪些用户可以切换到 FTP 站点根目录的上级目录。
- chroot\_local\_user=YES 用于指定用户列表文件中的用户,是否允许切换到上级目录。

具体情况有以下几种:

当 chroot\_list\_enable=YES, chroot\_local\_user=YES 时,在 /etc/vsftpd.chroot\_list 文件中列出的用户,可以切换到上级目录;未在文件中列出的用户,不能切换到站点根目录的上级目录。

当 chroot\_list\_enable=YES, chroot\_local\_user=NO 时,在 /etc/vsftpd.chroot\_list 文件中列出的用户,不能切换到站点根目录的上级目录;未在文件中列出的用户,可以切换到上级目录。

当 chroot\_list\_enable=NO, chroot\_local\_user=YES 时,所有用户均不能切换到上级目录。

当 chroot\_list\_enable=NO, chroot\_local\_user=NO 时,所有用户均可以切换到上级目录。

当用户不允许切换到上级目录时,登录后 FTP 站点的根目录(/)是该 FTP 账户的主目录。

#### 5. 设置访问控制

##### (1) 设置允许或不允许访问的主机

tcp\_wrappers=YES 设置 vsftpd 服务器是否与 tcp wrapper 相结合,进行主机的访问控制。默认设置为 YES, vsftpd 服务器会检查 /etc/hosts.allow 和 /etc/hosts.deny

中的设置,以决定请求连接的主机,是否允许连接访问该FTP服务器。这两个文件可以起到简易的防火墙功能。

比如,若要仅允许192.168.168.1~192.168.168.254的用户,可以访问连接vsftpd服务器,则可在/etc/hosts.allow文件中添加以下内容:

```
vsftpd:192.168.168. : allow  
all :all :deny
```

## (2) 设置允许或不允许访问的用户

对用户的访问控制由/etc目录下的vsftpd.user\_list和vsftpd.ftpusers文件来控制实现。相关配置命令如下:

- userlist\_enable=YES 决定vsftpd.user\_list文件是否启用生效。YES则生效,NO不生效。
- userlist\_deny=YES 决定vsftpd.user\_list文件中的用户是允许访问还是不允许访问。若设置为YES,则vsftpd.user\_list文件中的用户将不允许访问FTP服务器;若设置为NO,则只有vsftpd.user\_list文件中的用户,才能访问FTP服务器。

vsftpd.ftpusers文件则专门用于定义不允许访问FTP服务器的用户列表。默认情况下,这两个文件中已预设置了一些不允许访问FTP服务器的系统内部账户。若要在vsftpd.user\_list文件中定义允许访问FTP服务器的用户,则应注意将vsftpd.user\_list文件中原定义的不允许访问的用户列表删除或移到vsftpd.ftpusers文件中。

## 6. 设置访问速度

anon\_max\_rate=0 设置匿名用户所能使用的最大传输速度,单位为B/s。若设置为0,则不受速度限制,此为默认值。

local\_max\_rate=0 设置本地用户所能使用的最大传输速度。默认为0,不受限制。

## 7. 定义用户配置文件

在vsftpd服务器中,不同用户还可使用不同的配置,这通过用户配置文件来实现。

user\_config\_dir=/etc/vsftpd/userconf 用于设置用户配置文件所在的目录。

设置了该配置项后,当用户登录FTP服务器时,系统就会到/etc/vsftpd/userconf目录下,读取与当前用户名相同的文件,并根据文件中的配置命令,对当前用户进行更进一步的配置。比如,利用用户配置文件,可实现对不同用户进行访问速度的控制,在各用户配置文件中,定义local\_max\_rate配置,以决定该用户允许的访问速度。

## 8. 与连接相关的设置

- listen=YES 设置vsftpd服务器是否以standalone模式运行。以standalone

模式运行是一种较好的方式,此时 listen 必须设置为 YES,此为默认值,建议不要更改,很多与服务器运行相关的配置命令,需要此运行模式才有效。若设置为 NO,则 vsftpd 不是以独立的服务运行,要受 xinetd 服务的管理控制,功能上会受限制。

- max\_clients=0 设置 vsftpd 允许的最大连接数,默认为 0,表示不受限制。若设置为 150 时,则同时允许有 150 个连接,超出的将拒绝建立连接。只有在以 standalone 模式运行时才有效。
- max\_per\_ip=0 设置每个 IP 地址允许与 FTP 服务器同时建立连接的数目。默认为 0,不受限制。通常可对此配置进行设置,防止同一个用户建立太多的连接。只有在以 standalone 模式运行时才有效。
- listen\_address=IP 地址 设置在指定的 IP 地址上侦听用户的 FTP 请求。若不设置,则对服务器所绑定的所有 IP 地址进行侦听。只有在以 standalone 模式运行时才有效。对于只绑定了一个 IP 地址的服务器,不需要配置该项,默认情况下,配置文件中没有该配置项。若服务器同时绑定了多个 IP 地址,则应通过该配置项,指定在哪个 IP 地址上,提供 FTP 服务,即指定 FTP 服务器所使用的 IP 地址。
- accept\_timeout=60 设置建立 FTP 连接的超时时间,单位为秒,默认值为 60。
- connect\_timeout=120 PORT 方式下建立数据连接的超时时间,单位为秒。
- data\_connection\_timeout=120 设置建立 FTP 数据连接的超时时间,默认为 120 秒。
- idle\_session\_timeout=600 设置多长时间不对 FTP 服务器进行任何操作,则断开该 FTP 连接,单位为秒,默认为 600 秒。即设置发呆的逾时时间,在这个时间内,若没有数据传送或指令的输入,则会强行断开连接。
- pam\_service\_name=vsftpd 设置在 PAM 所使用的名称,默认值为 vsftpd。
- setproctitle\_enable=NO|YES 设置每个与 FTP 服务器的连接,是否以不同的进程表现出来,默认值为 NO,此时只有一个名为 vsftpd 的进程。若设置为 YES,则每个连接都会有一个 vsftpd 进程,使用“ps -ef|grep ftp”命令可查看到详细的 FTP 连接信息。

## 9. FTP 工作方式与端口设置

### (1) FTP 工作方式简介

FTP 的工作方式有两种,一种是 PORT FTP,另一种是 PASV FTP。下面分别介绍其工作方式。

PORT FTP 是常用的 FTP 工作方式,当客户端的连接请求到来时,FTP 服务器会使用默认的 21 端口与客户端建立连接,该连接属于命令通道,利用该通道来下达控制指令;



接下来服务器便会在 20 端口接受客户端的数据传输连接请求,并建立数据传输通道,开始传送数据,数据传送完毕后,便会关闭该次的数据连接,接着又会在 20 端口等待接受数据连接。从中可见,基于端口的工作方式下,服务器的数据端口始终使用 20,建立 ftp 连接使用的是标准的 21 端口。根据需要,在配置文件中可以重新设置所使用的端口。

PASV FTP 在工作的第一步,与 PORT FTP 相同,会首先利用 21 端口,建立控制连接;但在第二步,是由 FTP 客户端主动发起建立数据传输连接的请求,并由客户端选择和指定建立数据传输连接所使用的端口号,因此,每次建立的数据传输连接通道,所使用的端口号都是不相同的。

二者的区别在于,PORT FTP 的数据传输端口是由 FTP 服务器指定的,而 PASV FTP 则是由 FTP 客户端指定的,而且每次数据连接所使用的端口号都不同。正因为如此,所以在 CuteFTP 等 FTP 客户端软件中,其连接类型设置项中有 PORT 和 PASV 两种选择。

当 FTP 服务器设置为 PASV 工作模式时,客户端也必须设置为 PASV 连接类型。若客户端连接类型设置为 PORT,则能建立 FTP 连接,但在执行 ls 或 get 等需要数据请求的命令时,将会出现无响应并最终报告无法建立数据连接。

#### (2) 与端口相关的配置

- listen\_port=21 设置 FTP 服务器建立连接所侦听的端口,默认值为 21。
- connect\_from\_port\_20=YES 默认值为 YES,指定 FTP 数据传输连接使用 20 端口。若设置为 NO,则进行数据连接时,所使用的端口由 ftp\_data\_port 指定。
- ftp\_data\_port=20 设置 PORT 方式下 FTP 数据连接所使用的端口,默认值为 20。
- pasv\_enable=YES|NO 若设置为 YES,则使用 PASV 工作模式;若设置为 NO,使用 PORT 模式。默认为 YES,即使用 PASV 模式。在前面的例 7.8 中,当执行 ls 命令时,服务器会返回以下类似提示信息:

```
227 Entering Passive Mode (192,168,168,154,52,102)
```

其中,227 是 FTP 服务器返回的代码,表示现在进入 PASV 模式,后面括号中的前 4 个数字是服务器的 IP 地址,后 2 个是建立数据连接时双方所使用的端口号。

- pasv\_max\_port=0 设置在 PASV 工作方式下,数据连接可以使用的端口范围的上界。默认值为 0,表示任意端口。
- pasv\_min\_port=0 设置在 PASV 工作方式下,数据连接可以使用的端口范围的下界。默认值为 0,任意端口。

#### 10. 设置传输模式

FTP 在传输数据时,可使用二进制方式,也可使用 ASCII 模式来上传或下载数据。

- `ascii_download_enable=YES` 设置是否启用 ASCII 模式下载数据。默认为 NO。
- `ascii_upload_enable=YES` 设置是否启用 ASCII 模式上传数据。默认为 NO。

## 11. 设置上传文档的所属关系和权限

### (1) 设置匿名上传文档的属主

- `chown_uploads=YES` 用于设置是否改变匿名用户上传的文档的属主。默认为 NO。

若设置为 YES, 则匿名用户上传的文档的属主将被设置为 `chown_username` 配置项所设置的用户名。

- `chown_username=whoever` 设置匿名用户上传的文档的属主名。建议不要设置为 root 用户。

### (2) 新增文档的权限设定

- `local_umask=022` 设置本地用户新增文档的 umask, 默认为 022, 对应的权限为 755。umask 为 022, 对应的二进制数为 000 010 010, 将其取反为 111 101 101, 转换成十进制数, 即为权限值 755, 代表文档的所有者(属主)有读写执行权, 所属组有读和执行权, 其他用户有读和执行权。022 适合于大多数情况, 一般不需要更改。若设置为 077, 则对应的权限为 700。
- `anon_umask=022` 设置匿名用户新增文档的 umask。
- `file_open_mode=755` 设置上传文档的权限。权限采用数字格式。

## 12. 日志文件

- `xferlog_enable=YES` 是否启用上传/下载日志记录。
- `xferlog_file=/var/log/vsftpd.log` 设置日志文件名及路径。
- `xferlog_std_format=YES` 日志文件是否使用标准的 xferlog 格式。

## 13. 其他设置

- `text_userdb_names=NO` 设置在执行 ls 命令时, 是显示 UID、GID 还是显示出具体的用户名或组名称。默认为 NO, 以 UID 和 GID 方式显示, 若希望显示用户名和组名称, 则设置为 YES。在前面例 7.8 中执行 ls 命令时, 所显示出来的 101 和 50 即分别代表 UID 和 GID 值。
- `ls_recurse_enable=NO` 若设置为 YES, 则允许执行“ls -R”这个命令, 默认值为 NO。在配置文件中该配置项被注释掉了, 与此类似的还有一些配置, 需要启用时, 将注释符去掉并进行 YES 或 NO 的设置即可。

## 8.4 用户磁盘配额管理

### 1. 磁盘配额简介

磁盘配额(disk quota)用于限制各用户或用户组所允许使用的磁盘空间的大小。Linux是一个多用户系统,有必要限制各用户允许使用的磁盘空间,以防止恶意用户用垃圾数据塞满服务器磁盘空间,Linux操作系统为此提供了磁盘配额管理。

启动磁盘配额后,当某用户使用了过多的磁盘空间或分区,可用空间将尽时,系统管理员就会收到警告信息。磁盘配额可限制用户可使用的磁盘空间,也可限制用户可以创建的文件数目。

### 2. 使 Linux 支持磁盘配额

Linux系统支持磁盘配额,但必须要安装支持配额管理的 quota 软件包。Red Hat Linux 9 提供了 quota 软件包,在安装 Linux 系统时一般都安装了,可使用以下命令检查是否安装。

```
[root@rh9 root]# rpm -q quota
quota-3.06-9
```

若未安装,可在安装光盘中找到 quota-3.06-9.i386.rpm 软件包安装。

### 3. 配置磁盘配额

(1) 修改/etc/fstab 配置文件,指定要进行磁盘配额管理的文件系统。

对于要启用磁盘配额的文件系统,要在/etc/fstab 配置文件中指定,指定方法即是在该文件系统配置行的第4列中,添加 usrquota 和 grpquota。usrquota 表示启用用户磁盘配额功能,grpquota 表示启用用户组磁盘配额功能。

Linux 的主要磁盘空间位于根分区,若要对 Linux 的根目录文件系统启用用户和用户组磁盘配额,则启用方法如下:

用 vi 编辑/etc/fstab 文件,将“LABEL= /”这行的第4列,添加 usrquota 和 grpquota,添加后的内容如下所示:

```
[root@rh9 root]# vi /etc/fstab
```

LABEL= /	/	ext3	defaults,usrquota,grpquota	1	1
LABEL= /boot	/boot	ext3	defaults	1	2
/dev/sda3	swap	swap	defaults	0	0
none	/proc	proc	defaults	0	0
none	/dev/pts	devpts	gid=5,mode=620	0	0
/dev/fd0	/mnt/floppy	auto	noauto,owner,kudzu	0	0

修改后存盘退出 vi。

(2) 重新启动 Linux 或者直接执行以下命令,重新挂载根分区文件系统,让修改生效。

```
[root@rh9 root]# mount -o remount,defaults,usrquota,grpquota /
```

(3) 建立磁盘配额文件

对文件系统启用磁盘配额后,接下来就可使用 quotacheck 命令,检查启用了磁盘配额的文件系统,并为每个文件系统建立一个当前磁盘用量表,并创建出磁盘配额文件。

quotacheck 命令的用法为: quotacheck [-cvbugm] -a | filesystem。

参数说明:

- c 创建新的磁盘配额文件,对于已存在的磁盘配额文件,将被覆盖重写。
- b 在创建磁盘配额文件时,对已存在的配额文件先备份,备份文件名多一个“~”符号。

- v 在检查过程中显示检查进度和检查结果等详细信息。

- u 创建用户磁盘配额文件(aquota. user),该文件位于根目录下面。为默认值,可缺省。

- g 创建用户组磁盘配额文件(aquota. group),位于根目录下面。

- m 强行进行检查。对根目录文件系统检查时,由于正在使用,会报错,可使用-m 参数,强行进行检查。

- a 对所有启用了磁盘配额的 filesystem 进行检查。

filesystem 代表指定要检查的文件系统名。比如根目录文件系统,则表示为“/”。

要对根目录文件系统进行磁盘配额检查,并生成用户和用户组磁盘配额文件,则实现的操作命令为:

```
[root@rh9 root]# quotacheck -acugvm
quotacheck: Scanning /dev/sda2 [/] done
quotacheck: Checked 5673 directories and 101540 files
```

命令执行成功后,将在 Linux 的根目录下生成用户磁盘配额文件 aquota. user 和用户组磁盘配额文件 aquota. group。

```
[root@rh9 root]# ll / |grep quota
-rw----- 1 root root 9216 Aug 22 20:19 aquota.group
-rw----- 1 root root 10240 Aug 22 20:19 aquota.user
```

以后若磁盘配额文件被损坏,或要重新检查,可使用不带-c 参数的该命令来实现。若使用-c 参数,则原有的配置将丢失,因为-c 参数是重新创建磁盘配额文件。

(4) 为用户和用户组设置磁盘配额

设置磁盘配额使用 `edquota` 命令,该命令将调用 `vi` 编辑,来完成用户磁盘配额的显示和设置,其命令用法为: `edquota [-u | -g] [-f 文件系统] 用户名`

其中, `-u` 表示编辑用户的磁盘配额,此为默认值,可以缺省; `-g` 代表编辑用户组的磁盘配额; `-f` 用于指定要进行磁盘配额的文件系统名。

例如,若要对 `webftp1` 用户设置磁盘配额限制,则操作命令为:

```
[root@rh9 root]# edquota -u webftp1 -f / # 也可表达为 edquota webftp1
Disk quotas for user webftp1(uid 101):
Filesystem      blocks      soft      hard      inodes      soft      hard
/dev/sda2       12272        0        0         5          0        0
```

执行命令后,系统进入 `vi` 编辑器,并在编辑器中显示出以上内容。其中,第1列是启用了磁盘配额的文件系统的设备名;第2列显示了该用户当前已使用的磁盘块数;第3和第4列分别用来设置用户在该文件系统上的软、硬磁盘块数限制,设置为0,表示不受限制; `inodes` 列显示了用户当前已使用的 `i` 节点的数量,用户每创建或上传一个文件或目录将占用一个 `i` 节点,对 `i` 节点数的限制实质是对允许创建的文件数的限制;最后两列分别用来设置用户在该文件系统上的软、硬 `i` 节点数的限制,设置为0,表示不受限制。一般不要限制 `i` 节点数。

硬限制是指用户或组群可以使用的磁盘空间块数或 `i` 节点数的绝对最大值,达到该限度后,磁盘空间或 `i` 节点数就不能再被用户或组增加使用了。软限制是定义可被使用的最大磁盘空间量或 `i` 节点数,与硬限制不同的是,软限制可以在一段时期内被超过使用,这段时期被称为过渡期(`grace period`)。过渡期可以用秒、分、小时、天数、周数或月数来表示。

比如,若要设置用户软限制可使用的磁盘块数为55000,硬限制块数为52000,可使用的 `i` 节点数不受限制,则将其修改为以下形式,并存盘退出。

```
Filesystem      blocks      soft      hard      inodes      soft      hard
/dev/sda2       12272     55000     52000        5          0        0
```

对于一个用户组进行磁盘配额限制后,则该组中的成员,都将受此限制,便于统一控制。例如,对于提供个人 Web 服务的虚拟主机,假设每个用户 Web 站点可使用的空间为100MB,对站点文件的上传和下载使用 FTP 服务来实现,每个 FTP 账户均属于 `ftp` 用户组,则此时只需对 `ftp` 用户组进行磁盘配额设置,即可实现对各 Web 站点的磁盘配额管理。

对 `ftp` 用户组设置磁盘配额,其操作命令为:

```
[root@rh9 root]# edquota -g ftp -f /
Disk quotas for group ftp (gid 50):
```

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/sda2	12372	0	0	9	0	0

根据需要,设置好允许使用的软、硬磁盘空间块数,比如,将软块数设置为 110000,硬块数设置为 100000,然后存盘退出。

#### (5) 设置或修改过渡期

为软限制设置过渡期,可使用带-t 参数的 edquota 命令来实现,其命令用法为 edquota -t。

```
[root@rh9 root]# edquota -t
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/sda2        7days                7days
```

设置好后保存配置,然后退出 vi。

#### (6) 查看用户或用户组的磁盘配额

使用 quota 命令,可查看用户或用户组当前的磁盘配额设置,其命令用法如下:

```
quota [-u | -g] 用户名或组名
```

其中,-u 参数代表查看用户的用户配额,为默认值,可缺省。-g 代表查看用户组的磁盘配额。

例如,若要查看 webftp1 用户的磁盘配额情况,则操作命令为:

```
[root@rh9 root]# quota -u webftp1          # 或表达为: quota webftp1
Disk quotas for user webftp1 (uid 101):
Filesystem      blocks      quota      limit  grace  files      quota      limit  grace
/dev/sda2        12272      55000      52000          5         0         0
```

grace 列通常是空白的,若软限被超出,这一列将显示过渡期中的剩余时间,若过渡期已超过,则显示 none。

若要查看 webftp2 的磁盘配额情况,则操作命令如下:

```
[root@rh9 root]# quota webftp2
Disk quotas for user webftp2 (uid 102): none      # 说明该用户还未设置磁盘配额
```

对于 root 用户,可使用“repquota -a”或“repquota /”命令,检查并输出所有用户的配额情况,其中参数-a 表示检查并输出所有文件系统的磁盘配额情况;“repquota /”命令表示检查并输出根目录文件系统的磁盘配额情况。可结合管道操作符和 less 命令来查看,具体用法如下:

```
[root@rh9 root]# repquota -a | less
```

显示效果如图 8.5 所示。显示在每个用户后面的“-”可用于快速判断该用户是否超出块限制或节点数限度。第一个“-”代表块限制,第二个“-”代表节点数限制,若超出限制,则“-”将由“\_”代替显示。

```
*** Report for user quotas on device /dev/sda2
Block grace time: 7days; Inode grace time: 7days
```

User		Block limits			grace	File limits			grace
		used	soft	hard		used	soft	hard	
root	--	1744212	0	0		85128	0	0	
daemon	--	12	0	0		3	0	0	
lp	--	1484	0	0		19	0	0	
rpm	--	26336	0	0		187	0	0	
rcsa	--	8	0	0		128	0	0	
rpcuser	--	16	0	0		4	0	0	
smmsp	--	56	0	0		7	0	0	
xfs	--	4	0	0		2	0	0	
named	--	8	0	0		2	0	0	
ntp	--	12	0	0		4	0	0	
gdm	--	52	0	0		2	0	0	
mysql	--	276	0	0		68	0	0	
webftp1	--	24	55888	52888		7	0	0	
webftp2	--	28	0	0		6	0	0	
yangjunhao	--	28	0	0		8	0	0	
u200	--	2464	0	0		95	0	0	
u301	--	2472	0	0		146	0	0	
u500	--	53844	0	0		4756	0	0	
u581	--	1828	0	0		188	0	0	

图 8.5 用户磁盘配额报告

若要查看 ftp 用户组的磁盘配额设置,则操作命令为:

```
[root@rh9 root]# quota -g ftp
```

Disk Quotas for group ftp (gid 50):

Filesystem	blocks	quota	limit	grace	files	quota	limit	grace
/dev/sda2	12372	110000	100000		9	0	0	

### (7) 启用与禁用磁盘配额

用户或用户组的磁盘配额设置好后,应打开启用,以便让磁盘配额生效。以后一旦用户所占用的磁盘空间超过了硬限制所设定的值,便会得到警告信息,此时仍可继续增加所使用的空间,达到软限制所设定的容量,但不能超过软限制的空间,在过渡期过了后,将被限制在硬限制所允许的空间内。

启用磁盘配额,使用 `quotaon` 命令,其命令用法为:

```
quotaon -vug -a | filesystem
```

参数说明: `-u` 代表启用用户磁盘配额,为默认值,可缺省; `-g` 代表用户组。

若要启用根目录文件系统的用户和用户组磁盘配额,则操作命令为:

```
[root@rh9 root]# quotaon -vlt /          # 或 quotaon -avug
/dev/sda2 [/]: group quotas turned on
/dev/sda2 [/]: user quotas turned on
```

若要禁用文件系统的磁盘配额,则可使用 quotaoff 命令来实现,其命令用法为:

```
quotaoff -vug -a | filesystem
```

例如,若要关闭所有文件系统的用户和用户组磁盘配额,则操作命令为:

```
[root@rh9 root]# quotaoff -avug
/dev/sda2 [/]: group quotas turned off
/dev/sda2 [/]: user quotas turned off
```

禁用后,需要时可用 quotaon 再度启用。在启用前,最好先用 quotacheck -avug 或 quotacheck -avugm 命令,重新检查一下文件系统,以刷新用户和用户组的磁盘用量表。

在学习时,可将用户的磁盘配额设置小一点,以便查看当 FTP 用户上传的数据超过限制的空间时的效果。此时用户应无法再上传文件,FTP 会报告无法写文件等类似错误信息。

## 8.5 vsftp 服务器配置示例

### 1. 配置要求

现有某提供虚拟主机 Web 和 FTP 服务的服务器,服务器的 IP 地址为 192.168.168.154,虚拟主机采用基于域名(主机名)的虚拟主机,各用户的 Web 站点根目录统一放在 /var/www 目录中,目录名为域名的名称,比如,若某网站的域名为 pcnetedu.com,则站点根目录为 /var/www/pcnetedu.com。每个网站的管理员有一个 FTP 账户,利用该账户 FTP 登录后,可对 Web 站点根目录下的文件进行上传、下载、创建子目录、更名和删除操作,用户只能对自己的 Web 站点根目录及其下面的目录文件操作,不允许切换到上级目录,不允许匿名用户登录和访问。

FTP 服务器采用 PASV 工作模式,允许 ASCII 模式来上传或下载数据,允许最多同时连机 350 用户,每个客户 IP 允许同时与服务器建立 5 个连接,每个用户的访问速度限制为 512K。FTP 日志文件存放在 /var/vhlogs/vsftpd.log 文件中。

/var/www 目录位于 Linux 的根分区,对根分区文件系统启用用户和用户组的磁盘配额,然后对每个 FTP 用户启用磁盘配额,每个 FTP 用户允许使用磁盘空间的软限制块数为 150000,硬限制块数为 130000,i 节点数不受限制。

### 2. 配置方法

下面假设给一个名为 yangjunhao 的新用户配置 Web 站点(http://www.pcnetedu.com)和对应的 FTP 站点为例,介绍其配置步骤和方法。



分析：由于FTP账户登录后所在的FTP站点的根目录也就是Web站点的根目录，因此，Web站点的根目录可在创建该用户账户时一并创建。

配置步骤：

① 创建新用户账户，并设置密码。该账户仅用作登录FTP服务器。

```
[root@rh9 root]# useradd yangjunhao -r m -g ftp -d /var/www/pcnetedu.com \
> -s /sbin/nologin -c "vHost FTP User"
[root@rh9 root]# passwd yangjunhao
Changing password for user yangjunhao.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

② 检查并设置站点根目录的所属关系和权限。

```
[root@rh9 root]# ll /var/www | grep pcnetedu.com          # 查询所属关系及权限
drwx----- 2 yangjunhao ftp 4096 Aug 23 11:49 pcnetedu.com
[root@rh9 root]# chmod 755 /var/www/pcnetedu.com
[root@rh9 root]# ll /var/www | grep pcnetedu.com
drwxr-xr-x 2 yangjunhao ftp 4096 Aug 23 11:49 pcnetedu.com
```

③ 为根目录文件系统打开磁盘配额功能，并为ftp用户组配置磁盘配额。配置步骤和方法参见8.4节，此处略。

④ 修改/usr/local/apache2/conf/httpd.conf配置文件，添加www.pcnetedu.com虚拟主机。添加方法参见前面虚拟主机配置部分，此处略。

⑤ 配置FTP服务器。

对FTP服务器的配置，是对整个FTP服务器生效的，因此，只需配置一次即可。配置好后，以后添加新用户时，就不再需要配置了。

利用vi编辑器编辑修改/etc/vsftpd/vsftpd.conf配置文件，将配置项设置为以下形式：

```
write_enable=YES
# 对匿名用户的设置
anonymous_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
# 对本地用户设置
local_enable=YES
local_umask=022
file_open_mode=755
```

```
# 欢迎信息设置
dirmessage enable= NO
ftpd_banner= Welcome to pcnnetedu.com Virtual Host FTP Service.
# 日志文件
xferlog_enable= YES
xferlog_file= /var/vhlogs/vsftpd.log
xferlog_std_format= YES
# 允许以 ASCII 方式上传或下载文件
ascii_upload_enable= YES
ascii_download_enable= YES
# 仅允许 vsftpd.chroot_list 文件中的用户,可以切换到上级目录。
chroot_local_user= YES
chroot_list_enable= YES
chroot_list_file= /etc/vsftpd.chroot_list
# 访问控制,拒绝 vsftpd.user_list 和 vsftpd.ftppusers 文件中的用户登录 FTP 服务器。
userlist_enable= YES
userlist_deny= YES
tcp_wrappers= YES
# 设置 vsftpd 以单进程方式工作
setproctitle_enable= NO
pam_service_name= vsftpd
# 与连接相关的设置
listen= YES
listen_address= 192.168.168.154
listen_port= 21
ftp_data_port= 20
connect_from_port_20= YES
pasv_enable= YES
pasv_max_port= 0
pasv_min_port= 0
idle_session_timeout= 600
data_connection_timeout= 120
max_clients= 350
max_per_ip= 5
local_max_rate= 512000
# anon_max_rate= 51200
```

保存配置,然后退出 vi 编辑器。

⑥ 创建/etc/vsftpd.chroot\_list 配置文件,然后重新启动 vsftpd 服务器即可。

```
[root@rh9 root]# touch /etc/vsftpd, chroot_list
[root@rh9 root]# service vsftpd restart
```

### ⑦ 访问FTP站点。

利用 yangjunhao 账户登录FTP服务器,然后再创建两个名为 downloads 和 images 的目录。检测访问是否正常。

```
[root@rh9 root]# ftp 192.168.168.154
Connected to 192.168.168.154 (192.168.168.154).
220 Welcome to pcnetedu.com Virtual Host FTP service.
Name (192.168.168.154:root): yangjunhao
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>mkdir downloads                                # 创建 downloads 目录
257 "/downloads" created
ftp>mkdir images                                    # 创建 images 目录
257 "/images" created
ftp>pwd                                              # 检查当前在FTP服务器中的位置
257 "/"                                              # 说明位于FTP站点的根目录
ftp>ls                                              # 查询文件目录列表
227 Entering Passive Mode (192,168,168,236,27)
150 Here comes the directory listing.
drwxr-xr-x  2   103    50  4096  Aug 23 04:53      downloads
drwxr-xr-x  2   103    50  4096  Aug 23 04:52      images
226 Directory send OK.
ftp>quit
Goodbye.
[root@rh9 root]#
```

在“ftp>”命令行下执行“cd ..”命令,虽然提示目录切换成功,但实际上仍在FTP站点的根目录之下,无法切换到上级目录,说明配置成功。每个FTP用户登录FTP服务器后,其对应的FTP站点根目录,是该用户的主目录。对于 yangjunhao 用户而言,其FTP站点的根目录实际对应的是Linux文件系统的/var/www/pcnetedu.com目录。

到此为止,一个完整的FTP服务器配置成功。以后增加新用户时,只需要创建用户,并在Apache的配置文件中,为该用户配置基于域名的虚拟主机即可。

## 8.6 FTP 常用命令

FTP 命令用于登录连接远程 FTP 站点,实现对远程 FTP 站点的文件操作和对文件的上传和下载等功能。熟悉并掌握 FTP 命令,可大大方便远程维护和管理 FTP 站点或 Web 服务器。Linux 平台和 Windows 平台均提供有 ftp 命令,其命令功能和用法均相同。

本节以 Linux 平台为例,介绍一些常用的 FTP 命令及用法,对于 Windows 平台,只需在 MS-DOS 提示符下,键入 ftp 命令,即可进入 ftp 命令行状态(ftp>)。

### 1. 登录 FTP 站点

要对远程 FTP 站点进行操作,就必须先登录连接 FTP 站点。对 FTP 站点的访问有授权访问和匿名访问两种。匿名访问时,系统自动使用预设的匿名账户和密码来登录,不需要特定的授权账户;而授权访问,必须用授权的账户和密码来登录 FTP 站点,登录成功后,才能访问 FTP 站点。

在 ftp 命令行状态下,可用 open 命令来登录连接 FTP 服务器。比如,若要连接 192.168.168.154 FTP 服务器,则操作命令为:

```
[root@rh9 root]# ftp
ftp>open 192.168.168.154
```

接下来会提示输入用户名和密码,校验成功后,即可登录上 FTP 服务器,从而可以访问服务器中的文件。

### 2. 对 FTP 站点进行文件操作

#### (1) 查询站点的目录文件列表

要查看站点的目录和文件列表,可执行 dir 或 ls 命令来实现,命令支持“\*”和“?”通配符。

#### (2) 删除站点文件

若要删除远程站点中的某个或某些文件,则可使用 delete 或 mdelete 命令来实现。delete 用于删除单个文件,mdelete 用于一次删除多个文件,支持“\*”和“?”通配符。

#### (3) 更名站点文件

若要对远程站点的文件更名,可使用 rename 命令来实现,命令用法为:

```
ftp>rename 源文件名 新文件名
```

### 3. 对站点进行目录操作

#### (1) 改变当前目录

改变当前目录分为改变远程站点的当前目录和改变本地当前目录两种情况。改变远

程站点的当前目录使用 `cd` 命令,改变本地的当前目录使用 `lcd` 命令。`lcd` 命令中的 `l` 是 `Location` 的缩写,意为本地的,两个语句的用法相同。

#### (2) 建立目录

在远程站点建立目录,使用 `mkdir` 命令,命令用法为: `ftp>mkdir 目录名`

#### (3) 删除目录

要删除远程站点的目录,使用 `rmdir` 命令,命令用法为: `ftp>rmdir 目录名`

### 4. 上传与下载文件

#### (1) 设置文件的传输模式

文件的传输模式有二进制方式和 ASCII 方式。设置为二进制传输模式,执行 `binary` 命令;设置为 ASCII 模式,执行 `ascii` 命令。

#### (2) 设置多个文件传输时的交互提示

在上传或下载多个文件时,默认情况下系统对每个文件都要进行询问是否要进行该操作。若要关闭该提示或重新开启交互提示,可使用 `prompt` 命令,该命令没有参数,第一次执行时关闭,第二次执行时就开启。

#### (3) 传输时显示进度

在上传或下载较大文件时,为动态显示传输的进度,可通过执行 `hash` 命令来开启,若要关闭,只需再执行一次即可。开启后,每传输 2048 个字节,就显示一个“\*”,以示传输的进度情况。

#### (4) 上传文件

将本地文件上传到远程的站点,可使用 `put` 或 `mput` 来实现,`put` 用于传输单个文件,`mput` 用于一次传输多个文件,支持“\*”和“?”通配符。上传前,可事先设置目标目录为当前目录,这样上传时就可缺省路径。

#### (5) 下载文件

从远程站点将文件下载到本地,可使用 `get` 或 `mget`。`get` 用于下载单个文件,`mget` 用于一次下载多个文件。用法格式如下:

```
ftp>get 远程文件名 本地文件名
```

### 5. 中断与远程站点的会话

要断开与远程站点的会话连接,可使用 `close` 或 `disconnect` 命令,两个命令功能相同。该命令与 `open` 功能相反。

### 6. 退出 ftp 会话

若要退出 `ftp` 会话,使用 `quit` 或 `bye` 命令,这两个命令的功能相同。

## 习题

1. 以下文件中,不属于 vsftpd 的配置文件的是( )。  
A. /etc/vsftpd/vsftp.conf      B. /etc/vsftpd/vsftpd.conf  
C. /etc/vsftpd.ftpusers      D. /etc/vsftpd.user\_list
2. 安装 vsftpd FTP 服务器后,若要启动该服务,则正确的命令是( )。  
A. server vsftpd start      B. service vsftd restart  
C. service vsftd start      D. /etc/rc.d/init.d/vsftpd restart
3. 若使用 vsftpd 的默认配置,使用匿名账户登录 FTP 服务器,所处的目录是( )。  
A. /home/ftp      B. /var/ftp      C. /home      D. /home/vsftpd
4. 以下命令或软件中,不能用来登录 FTP 服务器的是( )。  
A. ftp      B. CuteFTP Pro  
C. gftp      D. http://FTP 服务器地址
5. 以下对 vsftp 的描述,不正确的是( )。  
A. Linux 系统组建 FTP 服务器可使用 vsftpd 或者 ProFTP  
B. 在默认配置下,匿名登录 vsftpd 服务器后,在服务器端的位置是/var/ftp  
C. 客户端可使用 ftp 或 gftp 命令或 FTP 客户端软件来登录 FTP 服务器  
D. vsftp 服务器不能对用户的上传或下载速度进行控制
6. 在 vsftpd.conf 配置文件中,用于设置不允许匿名用户登录 FTP 服务器的配置命令是( )。  
A. anonymous\_enable=NO      B. no\_anonymous\_login=YES  
C. local\_enable=NO      D. anonymous\_enable=YES
7. 在 vsftpd.conf 配置文件中,用于设置普通用户登录后,其 FTP 站点根目录的配置项是( )。  
A. local\_root      B. local\_ftproot      C. anon\_root      D. anon\_ftproot
8. 若要禁止所有 ftp 用户登录 FTP 服务器后,切换到 FTP 站点根目录的上级目录,则相关的配置应是( )。  
A. chroot\_local\_user=NO      B. chroot\_local\_user=YES  
    chroot\_list\_enable=NO      chroot\_list\_enable=NO  
C. chroot\_local\_user=YES      D. chroot\_local\_user=NO  
    chroot\_list\_enable=YES      chroot\_list\_enable=YES
9. 以下对磁盘配额的描述,错误的是( )。  
A. Linux 系统支持对用户和用户组的磁盘配额管理,但应安装 quota 软件包,并

要进行相应配置

- B. 若要进行用户和用户组的磁盘配额,必须修改/etc/fstab文件,对需要启用配额管理的分区,在第4列的defaults之后,添加usrquota,然后重新启动系统即可实现
- C. 查看一个用户或用户组的磁盘配额情况,可使用quota命令
- D. 设置用户或用户组的磁盘配额,使用edquota命令来实现

## 实训8 安装与配置FTP服务器

**【实训目的】** 掌握vsftpd FTP服务器的配置和FTP服务器的登录与访问方法。掌握磁盘配额的配置与管理。

**【实训环境】** 在虚拟PC机的Linux操作系统中进行实际操作。

**【实训内容】**

1. 安装并启动vsftpd FTP服务器,然后设置vsftpd服务在运行级别3和5时自动启动。
2. 在Linux或Windows 2000的命令行提示符下,使用“ftp FTP服务器IP地址”命令,并使用匿名账户登录连接vsftpd FTP服务器。然后使用pwd命令查询当前所处的目录位置,使用mkdir命令创建一个上级子目录,然后使用ls命令显示当前目录下的文件列表,使用quit命令退出并断开对FTP服务器的登录连接。
3. 按本书例8.1所示的步骤和方法,创建并测试FTP服务器。
4. 为Linux的根文件系统打开用户和用户组磁盘配额功能,并为ftp用户组配置硬盘空间为51200个数据块(1数据块=1024字节),i节点数不受限制。
5. 按本书8.5节所讲的步骤和方法,创建并配置FTP服务器。

## 第 9 章

# 配置 DNS 与 DHCP 服务器

DNS 和 DHCP 服务器也是很常用的服务器,本章将详细介绍在 Linux 平台,如何安装和配置 DNS 和 DHCP 服务器。

## 9.1 配置 DNS 服务器

### 9.1.1 DNS 简介

#### 1. DNS 的作用

DNS(domain name server,域名服务器)用于实现域名和 IP 地址的相互转换。有了域名服务系统,就可将网络中的每个主机名当作一个符号地址,来使用网络所提供的资源,对用户而言,使用主机名比使用数字式的 IP 地址更为直观、方便和易于记忆,而对于资源的提供者,也更容易把自己的品牌和服务内容反映在主机名(域名)之中,从而起到更好的宣传作用。

当在客户机的浏览器中键入要访问的主机名时,就会触发一个 IP 地址的查询请求,该请求会自动发送到默认的 DNS 服务器,DNS 服务器就会从数据库中查询该主机名所对应的 IP 地址,并将找到的 IP 地址作为查询结果返回。浏览器获得 IP 地址后,就根据 IP 地址,在 Internet 网中定位所要访问的资源。

DNS 服务器分为 3 种,高速缓存服务器(cache-only server)、主服务器(primary name server)和辅助服务器(second name server)。

#### 2. DNS 的查询模式

按照 DNS 搜索区域的类型,DNS 的区域可分为正向搜索区域和反向搜索区域。正向搜索是 DNS 服务器要实现的主要功能,它根据计算机的 DNS 名称(即域名),解析出相应的 IP 地址;而反向搜索则是根据计算机的 IP 地址解析出它的 DNS 名称(主机名)。



### (1) 正向查询

正向查询就是根据域名,搜索出对应的 IP 地址,其查询方法为:

当 DNS 客户机(也可以是 DNS 服务器)向首选 DNS 服务器发出查询请求后,如果首选 DNS 服务器中不含所需的数据,则会将查询请求转发给另一台 DNS 服务器,依此类推,一直找到所需的数据为止,如果到最后一台 DNS 服务器中也没有所需的数据,则通知 DNS 客户机查询失败。

### (2) 反向查询

反向查询与正向查询刚好相反,它是利用 IP 地址查询出对应的域名。

## 9.1.2 安装 DNS 服务器

### 1. 获得 BIND 软件包

Red Hat Linux 9 自带有版本号为 9.2.1 的 BIND(berkeley internet name domain)服务器软件,它是目前使用最广泛的域名服务器软件,使用 named 守护进程提供域名解析服务。

在第 1 张安装光盘提供了 BIND 服务的主要安装软件包 bind-9.2.1-16.i386.rpm,另一部分与 DNS 相关的实用程序(dig、host、nslookup 和 nsupdate)由 bind-utils-9.2.1-16.i386.rpm 软件包提供。BIND 的主配置文件(named.conf)、本地域文件和根域文件(named.ca)等重要配置文件,则由第 2 张安装光盘中的 caching-nameserver-7.2-7.noarch.rpm 软件包提供。

BIND 软件是由 Nominum 公司开发,由 ISC(internet software consortium)负责维护,其最新软件包采用源代码方式发布,可访问 <http://www.isc.org/products/bind/> 网站下载。bind 9.2.2 源代码软件包的下载地址为 <ftp://ftp.isc.org/isc/bind9/9.2.2/bind-9.2.2.tar.gz>。

### 2. 安装 BIND 软件包

#### (1) 检查是否已安装 BIND 软件包

在准备配置 DNS 服务器之前,应首先检查当前 Linux 系统是否安装了 BIND 软件包,检查方法为:

```
[root@rh9 root]# rpm -q bind  
bind-9.2.1-16
```

通过输出的 bind-9.2.1-16,说明当前系统已安装了该软件包。BIND 的主配置文件为 named.conf,默认位置在/etc 目录,默认的工作目录为/var/named,相关的主要实用程序默认安装在/usr/sbin 目录中。bind-utils-9.2.1-16.i386.rpm 软件包提供的实用程序默认安装在/usr/bin 目录中。

对于一个新的软件包,若不知其安装位置,可通过查询其 RPM 安装软件包的文件列表来获得。

检查 BIND 的样本配置文件和区文件是否安装。检查/etc/目录下是否有 named.conf 文件,/var/named 目录下面是否有本地域文件和根域文件,若都没有,则说明未安装,可使用以下方法安装:

```
[root@rh9 root]# cd /usr/local/src # 进入存放有软件包的目录
[root@rh9 src]# rpm -qpl caching-nameserver-7.2-7.noarch.rpm # 查询将要安装的文件列表
/etc/named.conf
/usr/share/doc/caching-nameserver-7.2
/usr/share/doc/caching-nameserver-7.2/Copyright
/var/named/localhost.zone
/var/named/named.ca
/var/named/named.local
[root@rh9 src]# rpm -ivh caching-nameserver-7.2-7.noarch.rpm # 安装配置文件软件包
```

(2) 若 BIND 软件包未安装,可采用以下方法安装。

#### ① RPM 软件包安装

```
[root@rh9 src]# rpm -qpl ivh bind-9.2.1-16.i386.rpm | less # 查询 BIND 软件包
/etc/logrotate.d/named
/etc/rc.d/init.d/named # named 守护进程启动脚本
/etc/rndc.conf # rndc 的配置文件
/etc/rndc.key # 存储有验证需要的 DNS 密钥
/etc/sysconfig/named
/usr/lib/libisc.so.0
:
/usr/sbin/dns-keygen
/usr/sbin/dnssec-keygen # DNS 密钥生成器
/usr/sbin/dnssec-makekeyscrt # 利用 dnssec-keygen 生成的一个或多个密钥创建密钥集
/usr/sbin/dnssec-signkey # 为区域文件密钥集生成签名
/usr/sbin/dnssec-signzone # 生成带有签名的区域文件
/usr/sbin/lwresd
/usr/sbin/named # BIND 的守护进程
/usr/sbin/named-bootconf # 用于生成 named.conf 配置文件
/usr/sbin/named-checkconf # 检查 named.conf 文件的语法
/usr/sbin/named-checkzone # 检查区域文件的合法性
/usr/sbin/rndc # BIND 管理工具
/usr/sbin/rndc-confgen # 生成 rndc.conf 配置文件
/usr/share/doc/bind-9.2.1
```

```

:
/var/named                                # BIND 守护进程的工作目录
/var/run/named                            # 用于存放 BIND 进程号文件的目录,进程号文件可放于此
[root@rh9 src] # rpm -ivh bind-9.2.1-16.i386.rpm          # 安装 BIND 软件包
[root@rh9 src] # rpm -ivh caching-nameserver-7.2-7.noarch.rpm
[root@rh9 src] # rpm -qpl bind-utils-9.2.1-16.i386.rpm
/usr/bin/dig                             # 可用于更新根名称服务器的列表
/usr/bin/host                             # DNS 查找工具
/usr/bin/nslookup                         # 检查域名解析是否正常
/usr/bin/nsupdate                         # 域名动态更新的命令行程序,可提交 DNS 更新请求
/usr/lib/libdns.so.5
:
[root@rh9 src] # rpm -ivh bind-utils-9.2.1-16.i386.rpm

```

BIND 软件包安装后,还将创建名为 named 的用户和用户组,并自动设置相关目录的权属关系。named 守护进程默认使用 named 用户身份运行。

```

[root@rh9 root] # grep named /etc/passwd
named:x:25:25:Named:/var/named:/sbin/nologin
[root@rh9 root] # grep named /etc/group
named:x:25:

```

/var/named 工作目录和/var/run/named 目录的所有者和权限设置为:

```

[root@rh9 root] # ll /var/ | grep named          # /var/named 目录
drwxr-xr-x  2 named named      4096 Aug 24 12:28 named
[root@rh9 root] # ll /var/run | grep named        # /var/run/named 目录
drwxr-xr-x  2 named named      4096 Jan 26 2003 named

```

若是利用源代码软件包安装,应手工创建 named 用户和用户组,并按以上所示,设置好工作目录和用于存放进程号文件的目录(/var/run/named)的所属关系和权限设置。

## ② 利用源代码软件包安装

```

[root@rh9 src] # tar -zxvf bind-9.2.2.tar.gz
[root@rh9 src] # cd bind-9.2.2
[root@rh9 bind-9.2.2] # ./configure --prefix=/usr --sysconfdir=/etc
[root@rh9 bind-9.2.2] # make
[root@rh9 bind-9.2.2] # make install

```

另外也可通过指定--prefix=/usr/local/bind,将其安装在/usr/local/bind 目录中。若未指定--prefix(安装位置),则默认安装在/usr/local/bin、/usr/local/lib 等相关目录中。

### 9.1.3 配置 DNS

对 DNS 服务器的配置,是通过相关的配置文件来实现的。

#### 1. BIND 配置文件简介

BIND 的配置文件包括主配置文件/etc/named.conf、根域文件(named.ca)、区域文件以及用于管理 BIND 守护进程的 rndc 程序的配置文件/etc/rndc.conf。

根域文件用于提供位于顶层的根域名服务器的列表,根域文件 named.ca、rndc.conf 和用于保存密钥的 rndc.key 文件,在安装好 BIND 软件包后已提供,用户一般不需要编辑或修改,配置 DNS 服务器,主要是对 named.conf 和区域文件进行配置和编辑修改。

named.conf 主配置文件由若干配置段构成,在配置文件中每行以分号作为结束符,行注释可使用“#”或“//”,对一段文字的注释采用/\*...\*/。

#### 2. 主配置文件(named.conf)

BIND 软件包安装后提供了一个样本配置文件,可在此基础上进行删除、添加和修改,来实现对 DNS 服务器的配置。下面以该样本配置文件为例,介绍主配置文件的格式和常用配置命令。

##### (1) named.conf 配置文件的内容

```
[root@rh9 root]# cat /etc/named.conf | less
options {                                # 全局设置
    directory "/var/named";              # 设置 BIND 的工作目录,域数据文件存放于此
    // query-source address * port 53;
};
controls {                               # 声明一个控制通道,用于 rndc 实用程序管理 named 守护进程
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
# zone 用于声明一个区
zone "." IN {                             # 定义根区域(root zone),让 DNS 服务器能获得根服务器的地址
    type hint;                            # 以便初始化 DNS 缓冲区。type 用于定义区域的类型为 hint
    file "named.ca";                     # 指定要读的根域文件
};
zone "localhost" IN {                     # 定义 localhost 的正向搜索区域
    type master;                          # 定义为主域名服务器的区域
    file "localhost.zone";                # 指定要读的区域文件,该文件具体实现正向域名解析
    allow-update { none; };               # 不允许域名动态更新
};
zone "0.0.127.in-addr.arpa" IN {          # 定义 127.0.0 网段的反向搜索区域
    type master;                          # 定义为主域名服务器的区域
```

```

file "named.local":           # 指定要读的区域文件,该文件具体实现反向域名解析
allow-update { none; };      # 不允许域名动态更新
;
include "/etc/rndc.key";      # 将/etc/rndc.key 文件包含进当前配置文件

```

## (2) 配置文件详解

### ① options 配置段

该配置段属于全局性的设置,常用配置项命令及功能如下:

- **directory** 用于指定 named 守护进程的工作目录,各区域正反向搜索解析文件和 DNS 根服务器地址列表文件(named.ca)应放在该配置项指定的目录中。若指定为/var/named 目录,则配置命令为“directory “/var/named”;”。
- **pid-file** 指定创建用于保存 named 守护进程号的文件名及路径。守护进程号文件一般保存在/var/run 目录中,BIND 软件包安装时在/var/run 目录下创建了一个 named 目录,因此,可将进程号文件保存在该目录中,相应的配置命令为“pid-file “/var/run/named/named.pid”;”。
- **statistics-file** 用于指定记录状态信息的文件的位置。若将其保存在与进程号文件相同的位置,则相应的配置命令为“statistics-file “/var/run/named/named.stats”;”。
- **allow-recursion{}** 指定允许查询该 DNS 服务器的 IP 地址或网络。在{}中可指定允许查询的 IP 地址或网络地址列表,地址间用分号分隔。若不配置该项,则默认所有主机均可以查询。allow-query{}与此功能相同。另外,还可使用地址匹配符来表达允许的主机。比如,any 可匹配所有的 IP 地址,none 不匹配任何 IP 地址,localhost 匹配本地主机使用的所有 IP 地址,localnets 匹配同本地主机相连的网络中的所有主机。

比如若仅允许 127.0.0.1 和 192.168.168.0/24 网段的主机查询该 DNS 服务器,则命令为:

```
allow-recursion{127.0.0.1;192.168.168.0/24;};
```

或表达为: allow query{127.0.0.1;192.168.168.0/24;};

若地址列表较多,还可在 options 段之前,用 acl 定义一个访问控制列表,然后再在 allow-query{}中引用该访问控制列表。

比如若要定义一个名为 red-hats 的访问控制列表,则定义和引用方法如下:

```

acl red hats {
127.0.0.1;
192.168.168.0/24;

```

```
};  
options{  
allow-query{red-hats:};  
};
```

- **transfer-format** 用于控制在发送的每个信息中包含一个资源记录,还是包含多个资源记录。若每个信息包中包含多个资源记录,则效率更高,但只有 8.1 或以上版本的 BIND 域名服务器才支持,默认为 `one-answer`。

若要配置成每个信息包含多个资源记录,则命令为“`transfer-format many-answers;`”。

若要配置成每个信息包含一个资源记录,则命令为“`transfer-format one-answer;`”。

- **listen-on** 设置 `named` 守护进程监听的 IP 地址和端口。若未指定,默认监听 DNS 服务器的所有 IP 地址的 53 号端口。当服务器安装有多块网卡,有多个 IP 地址时,可通过该配置命令指定所要监听的 IP 地址。对于只有一个地址的服务器,不必设置。

若要设置 DNS 服务器监听 192.168.168.154 这个 IP 地址,端口使用标准的 53 号,则配置命令为“`listen-on {192.168.168.154;};`”。

若要使用 5353 号端口,则配置命令为“`listen-on port 5353 {192.168.168.154;};`”。

- **forwarders{}** 与 **forward** **forwarders{}** 用于定义 DNS 转发器。当设置了转发器后,所有非本域的和在缓存中无法找到的域名查询,可由指定的 DNS 转发器来完成解析工作并做缓存。

**forward** 用于指定转发方式,仅在 **forwarders** 的转发器列表不为空时有效,其用法为:“`forward first | only;`”。

**forward first** 为默认方式,DNS 服务器会将用户的域名查询请求,先转发给 **forwarders** 设置的转发器,由转发器来完成域名的解析工作,若指定的转发器无法完成解析或无响应,则再由 DNS 服务器自身来完成域名的解析。

若设置为“`forward only;`”,则 DNS 服务器仅将用户的域名查询请求,转发给转发器,若指定的转发器无法完成域名解析或无响应,DNS 服务器自身也不会试着对其进行域名解析。

例如,某地区的 DNS 服务器为 61.128.192.68 和 61.128.128.68,若要将其设置为 DNS 服务器的转发器,则配置命令为:

```
options{  
forwarders {61.128.192.68;61.128.128.68;};  
forward first;  
};
```

另外,forward 也用于定义转发区(forward zone),此时的 forward 代表区(zone)的类型。利用转发区,可将 DNS 配置成只有查找特定域的时候,才使用转发器。

例如,若要配置在查找 pcnetedu.com 域时,才使用 DNS 转发器,则配置命令为:

```
zone "pcnetedu.com" {
    type forward;                # 定义转发区
    forward first;
    forwarders{61.128.192.68;61.128.128.68;};
};
```

### ② controls 声明段

BIND 软件包提供了一个 rndc 工具,通过该工具,使用命令行参数可实现本地或远程管理 named 守护进程,为了使 rndc 能够连接 named 守护进程,在 named.conf 配置文件中必须添加 controls 声明段,用于指定控制通道,以允许管理员在本地执行 rndc 命令,实现对 named 进程的管理。

在进行身份验证时所需的密钥信息,默认存放在/etc/rndc.key 文件中,因此在 named.conf 配置文件的末尾,使用“include “/etc/rndc.key” ;”语句将其包含进来了。

rndc.key 文件中的内容为:

```
key "rndckey" {
    algorithm hmac-md5;
    secret "yxog7FPTOI9YMDJtVgOTv3BGLvXMm0fa9bpmSwP394T137Tu4rkQUS1GhSum";
};
```

rndc.conf 配置文件中的内容为:

```
options {
    default-server localhost;
    default-key "rndckey";
};
server localhost {
    key "rndckey";
};
include "/etc/rndc.key";
```

### ③ 区域声明

区域声明使用 zone,主域名服务器的正向解析区域声明格式为:

```
zone "区域名称" IN {
    type master;
    file "实现正向解析的区域文件名";
```

```
allow-update {none};
};
```

从域名服务器的正向解析区域声明格式为:

```
zone "区域名称" IN {
    type slave;
    file "实现正向解析的区域文件名";
    masters{主域名服务器的 IP 地址;};
};
```

反向解析区域的声明格式与正向相同,只是 file 所指定要读的文件不同,另外就是区域的名称不同。若要反向解析 x. y. z 网段的主机,则反向解析的区域名称应设置为:

```
z. y. x. in-addr. arpa
```

一个网段通常应声明一组正反向解析区域。对于主域名服务器或从域名服务器而言,第一次配置好后,以后对配置文件的改动主要是增加、删除或修改区域。在区域中还可使用一些配置指令,这些指令作用于该区域。比如为某区域设置转发器,利用 allow-update 指定允许 DNS 动态更新的 IP 地址等。

根区的声明格式一般为:

```
zone "." IN {
    type hint;
    file path_name;
};
```

转发区的声明格式为:

```
zone domain_name IN{
    type forward;
    [forward only | first;]
    forwarders {[ip_addr;[ip_addr;... ]];
};
```

named.conf 样本配置文件仅是一个基本的结构,对于用户自己要解析的域,则要按照此声明格式手工添加,并创建正反解析区域文件。

### 3. DNS 根服务器文件

DNS 根服务器文件中包含了 DNS 根服务器的地址列表,利用该文件,以让 DNS 服务器能找到根服务器,并初始化 DNS 的缓冲区。通过安装 caching-nameserver-7. 2-7 . noarch. rpm 软件包,可获得根服务器文件 named.ca,该文件名可任意命名,但要与根区



声明中所引用的文件名保持一致。

根服务器的地址一般不会有太大变化,但部分根服务器地址发生改变也是有可能的,另外也有可能添加了新的根服务器,因此,更新根服务器的最新地址列表,对 DNS 服务器的正常解析,是很有必要的。

named.ca 文件内容较多,通过查看前 12 行的说明文字,可获知到什么地方,可以获得其最新版本,以及该文件的最近更新时间。

```
[root@rh9 root]# head - 12 /var/named/named.ca
```

#### 4. 正向解析文件

正向解析用于实现域名到 IP 地址的转换。主机名 localhost 到 IP 地址的正向解析文件为 localhost.zone,该文件不需要修改,可直接使用,用于将 localhost 解析成 IP 地址 127.0.0.1。下面以该文件为例,介绍正向解析区文件的格式和各部分的含义。

```
[root@rh9 root]# cat /var/named/localhost.zone
$TTL      86400
$ORIGIN localhost.
@          IN SOA      @ root (
                                42      ; serial (d. adams)
                                3H       ; refresh
                                15M      ; retry
                                1W       ; expire
                                1D )     ; minimum
          IN NS       @
          IN A         127.0.0.1
```

下面依次介绍各行的含义:

① \$TTL 86400

从 BIND 8.2 开始,需要在区域文件的最前面加一条 \$TTL 语句,用来设置域的默认生存时间 TTL(time to live),时间单位为秒。86400 秒即为 1 天,也可等价表达为 \$TTL 1D。

② \$ORIGIN localhost.

设置该域被添加到一个绝对的记录中。\$ORIGIN 后面为域的名称。

③ @ IN SOA @ root (

@符号代表当前的域,1D 代表 1 天(day),下面的 3H 代表 3 小时(hour),15M 代表 15 分钟(minute),1W 代表 1 周(week);

IN 代表地址类别;SOA 是主域名服务器区域文件中一定要设置的,用于开始权威的域名信息记录,宣布该服务器具有权威性的名字空间。

SOA 之后应填写该域的名称,并且要在名称的最后附加上一个小数点“.”;域名之后,应填写域名服务器管理员的 E-mail 地址,E-mail 地址中的“@”符号在此处用小数点代替,在 E-mail 地址的最后,也要附加一个小数点。

在该区域文件中,由于在前面使用了 \$ORIGIN 语句进行定义,因此,此处的域名和域管理员 E-mail 就简约表达为 @ root,root 名字不是以点结尾,系统会用 \$ORIGIN 定义的域结尾,扩展后就变成了 root.localhost.。

下面即将介绍的反向解析区域文件中,没有定义 \$ORIGIN 语句,其表达法就符合该规定,其表达形式为“localhost. root.localhost.”。

④ 接下来的括号中的值,其含义是:

分号为注释符,之后的文字用于对该行的数值进行注解说明。serial 行前面的值,代表该区域文件的版本号或序列号。每当修改了该文件的内容后,应记住更改此序列号,以便让其他服务器从该服务器检索信息时,知道发生了更改,从而执行更新操作。序列号可以是任意的数字,但不能多于 10 位。

refresh 行前面的值代表更新的时间周期。此处设置为 3H。

retry 行前面的值代表在更新出现通信故障时的重试时间。此处设置为 15M,即 15 分钟。

expire 行前面的值代表重新执行更新动作后仍然无法完成更新任务而终止更新的时间。

minimum 行前面的值代表客户域名查询的记录,在域名服务器上放置的时间,即设置记录的缓存时间(Time To Live)。

⑤ 1D IN NS @

用于添加一条 NS(名称服务器)记录,用于指定权威的名称服务器。即该语句用于指定域名服务器,NS 之后应放置当前域名服务器的名称。

⑥ 1D IN A 127.0.0.1

用于添加一条 A(Address)记录,即地址记录。用于指定一个名称所对应的 IP 地址。域名的正向解析就是通过添加 A 记录来实现的,有多少个域名需要解析,就添加多少条 A 记录。

该条记录的含义就是将 localhost 解析为 127.0.0.1。

## 5. 反向解析文件

反向解析文件用于实现 IP 地址到域名的转换。反向解析文件 named.local 的内容为:

```
[root@rh9 root]# cat /var/named/named.local
$TTL      86400
```

```

@      IN      SOA      localhost. root. localhost. (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
      IN      NS       localhost.
1      IN      PTR      localhost.

```

在该文件中,时间全部采用的是以秒为单位进行表达,也可以D、H、M、W为单位来表达,两种表达法等效。

最后一行的PTR用于定义一个PTR记录,即定义一条反向解析记录。该行前面的1代表当前两段(127.0.0.)内的第1台主机,即IP地址为127.0.0.1的主机,最后的localhost,代表将该IP地址解析为localhost域名。

## 6. DNS服务器配置实例

**【例9.1】** 现要为某校园网配置一台DNS服务器,该服务器的IP地址为192.168.168.254,DNS服务器的域名为dns.schoolname.edu.cn,DNS转发器设置为61.128.192.68和61.128.128.68。要求为以下域名提供正反向解析服务:

dns.schoolname.edu.cn	←→	192.168.168.254	
mail.schoolname.edu.cn	←→	192.168.168.240	MX记录
www.schoolname.edu.cn	←→	192.168.168.241	
press.schoolname.edu.cn	←→	192.168.168.242	
pt.schoolname.edu.cn	←→	192.168.168.243	
vod.schoolname.edu.cn	←→	192.168.168.244	

配置步骤:

- ① 配置DNS服务器网卡的IP地址为192.168.168.254。
- ② 利用vi编辑/etc/named.conf配置文件,添加区域。

```

[root@rh9 root]# vi /etc/named.conf
options {
    directory "/var/named";
    pid-file "/var/run/named/named.pid";
    statistics-file "/var/run/named/named.state";
    forwarders {61.128.192.68;61.128.128.68;};
    forward first;
    listen-on {192.168.168.254;};
};

```

```

controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
include "/etc/rndc.key";
zone "." IN {
    type hint;
    file "named.ca";
};
zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
};
//下面为添加的区域
zone "schoolname.edu.cn" IN {
    type master;
    file "schoolname.edu.cn.zone";
    allow-update { none; };
};
zone "168.168.192.in-addr.arpa" IN {
    type master;
    file "192.168.168.zone";
    allow-update { none; };
};

```

③ 利用 vi 编辑器, 创建 /var/named/schoolname.edu.cn.zone 区域文件, 实现正向解析。

```

[root@rh9 root]# cd /var/named
[root@rh9 named]# cp localhost.zone schoolname.edu.cn.zone
[root@rh9 named]# vi schoolname.edu.cn.zone
$ TTL      86400
@          IN      SOA      schoolname.edu.cn. root.schoolname.edu.cn. (
                                43          ; serial (d. adams)
                                3H         ; refresh

```

```

                                15M      ; retry
                                1W       ; expiry
                                1D )    ; minimum
                                IN       NS      dns.schoolname.edu.cn.
                                IN       MX 10    mail.schoolname.edu.cn.
dns      IN       A    192.168.168.254
mail     IN       A    192.168.168.240
www      IN       A    192.168.168.241
press    IN       A    192.168.168.242
pt       IN       A    192.168.168.243
vod      IN       A    192.168.168.244

```

编辑好后,存盘退出 vi。

其中,语句“IN MX 10 mail.schoolname.edu.cn.”用于为 schoolname.edu.cn 域定义一条邮件地址交换记录(MX),10 代表优先级,数字越小,优先级越高。当定义了两个或多个 MX 记录时,优先级高的服务器,将首先获得发来的邮件,只有定义了域的 MX 记录后,邮件服务器才能收到该域的邮件,以后域名 mail.schoolname.edu.cn 就可作为邮件服务器的 SMTP 和 POP3 服务器的地址来使用。

④ 利用 vi 编辑器,创建/var/named/192.168.168.zone 区域文件,以实现反向解析。

```

[root@rh9 named]# cp named.local 192.168.168.zone
[root@rh9 named]# vi 192.168.168.zone
$TTL      86400
@         IN      SOA      schoolname.edu.cn.  root.schoolname.edu.cn. (
                                1997022701 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
                                IN      NS      dns.schoolname.edu.cn.
                                IN      MX 10    mail.schoolname.edu.cn.
254       IN      PTR      dns.schoolname.edu.cn.
240       IN      PTR      mail.schoolname.edu.cn.
241       IN      PTR      www.schoolname.edu.cn.
242       IN      PTR      press.schoolname.edu.cn.
243       IN      PTR      pt.schoolname.edu.cn.
244       IN      PTR      vod.schoolname.edu.cn.

```

编辑好后,存盘退出 vi。

⑤ 由于 named 守护进程以 named 用户身份运行,为了能读取区域文件,必须设置区

域文件的所有者为 named 用户和 named 用户组。

```
[root@rh9 named]# chown named,named /var/named/ *
```

⑥ 配置 DNS 客户端,使用该 DNS 服务器。

```
[root@rh9 named]# vi /etc/resolv.conf
search schoolname.edu.cn
nameserver 192.168.168.254
```

⑦ 启动 named 守护进程,开始域名解析服务。

```
[root@rh9 named]# service named start           #或/etc/rc.d/init.d/named start
[root@rh9 named]# service named status          #检查服务器状态
number of zones:6
debug level:0
xfers running:0
xfers deferred:0
soa queries in progress:0
query logging is OFF
server is up and running
```

此时执行 netstat -ln 命令,若能发现以下两行信息,则说明 DNS 服务器启动正常,53 号端口处于监听服务状态。

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	192.168.168.254:53	0.0.0.0:*	LISTEN
udp	0	0	192.168.168.254:53	0.0.0.0:*	

⑧ 另外还可使用 ping 或 nslookup 命令,来进一步检查域名解析是否生效。

```
[root@rh9 named]# ping dns.schoolname.edu.cn
```

```
[root@rh9 named]# nslookup
```

Note: nslookup is deprecated and may be removed from future releases.

Consider using the 'dig' or 'host' programs instead. Run nslookup with the '-sil[ent]' option to prevent this message from appearing.

```
>server 192.168.168.254
```

# 设置使用 192.168.168.254 DNS 服务器来解析域名

```
Default server: 192.168.168.254
```

```
Address: 192.168.168.254 # 53
```

```
>www.schoolname.edu.cn
```

# 查询域名

```
Server: 192.168.168.254
```

# 系统提示当前所使用的 DNS 服务器

```
Address: 192.168.168.254 # 53
```

```

Name:    www.schoolname.edu.cn
Address: 192.168.168.241          # 域名解析得出的 IP 地址
>192.168.168.213                 # 测试反向域名解析
Server:   192.168.168.254
Address:  192.168.168.254 # 53

243.168.168.192.in-addr.arpa    name = pt.schoolname.edu.cn      # 反向解析的结果
>set type=mx                    # 设置查看 MX 记录
>schoolname.edu.cn             # 查询该域的 MX 记录
Server:   192.168.168.254
Address:  192.168.168.254 # 53
schoolname.edu.cn      mail    exchanger  10  mail.schoolname.edu.cn.
>set type=a             # 重新设置查看 A 记录
>mail.schoolname.edu.cn # 查询该域名对应的 IP 地址
>Server:   192.168.168.254
Address:  192.168.168.254 # 53

Name:    mail.schoolname.edu.cn
Address: 192.168.168.240          # 查询获得的 IP 地址
>exit                               # 退出 nslookup

```

## 9.2 安装与配置 DHCP 服务器

DHCP 服务器用于为客户机动态分配 IP 地址,便于对网络的 IP 地址进行管理。本节将详细介绍 DHCP 服务器的安装与配置方法。

### 9.2.1 DHCP 简介

DHCP(dynamic host configuration protocol)称为动态主机配置协议。在使用 TCP/IP 协议通信的网络中,每台计算机都必须至少有一个 IP 地址,这样才能与其他计算机通信。对于一个较大规模的网络,逐个地为每台计算机分配和设置 IP 地址,是一件很麻烦的事情,也不便于管理和维护,于是 DHCP 应运而生。

DHCP 服务器利用租约机制,实现了对整个网络 IP 地址的自动统一分配和集中管理。当客户机向 DHCP 服务器请求分配 IP 地址时,DHCP 服务器会自动从地址池中找出一个未使用的 IP 地址,分配给客户机,从而实现 IP 地址的动态分配。在分配 IP 地址给客户机的同时,还可为客户机指定默认网关(路由)和域名服务器等信息,以便客户机能与其他网段的计算机通信或实现访问 Internet 网。

DHCP 服务器应至少配置一个作用域,各作用域的 IP 地址范围(IP 地址池)不能发

生重叠。作用域是指 DHCP 服务器可分配租用给 DHCP 客户机的 IP 地址范围。

在安装配置好 DHCP 服务器后,对于 Windows 系统的 DHCP 客户,只需在 TCP/IP 协议的属性对话框中,设置为“自动获得 IP 地址”,然后重启系统,即可从 DHCP 服务器的 IP 地址池中自动分配到 IP 地址。对于 Linux 系统的 DHCP 客户机,则应安装配置 DHCP 客户程序(dhclient),以便能动态分配到 IP 地址。

### 9.2.2 安装 DHCP 服务器软件包

## 1. 获得 DHCP 软件包

Red Hat Linux 自帶有 DHCP 的安裝軟件包,相關文件共有三個,分別是:

dhcp-3.0pl1-23.i386.rpm DHCP 服务器安装软件包,位于第 2 张光盘。

dhclient-3.0p1-23.i386.rpm DHCP 客户端安装软件包,位于第 1 张光盘。

dhcp-devel-3.0p11-23.i386.rpm DHCP 开发包。位于第 2 张光盘,提供库和头文件。一般不需要安装。

DHCP 的最新源代码软件包可访问 <http://www.isc.org> 网站获得。源代码软件包提供了 DHCP 服务器程序、客户端程序和相关库和头文件。

## 2. 检查是否安装了 DHCP 服务器

在准备安装 DHCP 服务器前,应先检查当前系统是否已安装了 DHCP 服务器,检查方法如下:

```
[root@rh9 root]# rpm -q dhcpd
dhcp-3.0pl1-23
```

若输出了 DHCP 软件包的名称,则说明已安装。若未安装,则可利用软件包来直接安装。

### 3. 安装 DHCP 服务器软件包

```
[root@rh9 root]# rpm -q /usr/local/src/dhcp-3.0p11-23.i386.rpm      # 查询安装文件列表
# rpm -q dhcp-3.0p11-23.i386.rpm

/etc/rc.d/init.d/dhcpd                # DHCP 服务器的启动脚本
/etc/rc.d/init.d/dhcrelay             # dhcrelay(DHCP 中继器)服务启动脚本
/etc/sysconfig/dhcpd
/etc/sysconfig/dhcrelay
/usr/bin/omshell
/usr/sbin/dhcpd                        # DHCP 守护进程程序
/usr/sbin/dhcrelay                    # DHCP 中继服务程序
:
```



```

/var/lib/dhcp
/var/lib/dhcp/dhcpd.leases # DHCP 守护进程启动必须的文件
[root@rh9 root]# rpm -ivh /usr/local/src/dhcp-3.0p11-23.i386.rpm # 安装 DHCP 服务器软件包

```

DHCP 中继服务 (dchrelay) 可以在没有 DHCP 服务器的子网上, 接收 DHCP 和 BOOTP (Internet Bootstrap Protocol) 网络地址请求, 并将其转发给另一个有 DHCP 服务器的子网。

### 9.2.3 配置 DHCP 服务器

#### 1. DHCP 服务器启动脚本

DHCP 服务器的启动脚本为 /etc/rc.d/init.d/dhcpd, 利用该脚本可实现 DHCP 服务器的启动、状态查询和停止等操作。在启动 DHCP 服务器之前, 应先完成对 DHCP 服务器的配置, DHCP 服务器的配置文件为 /etc/dhcpd.conf。通过查看阅读启动脚本, 可知 DHCP 服务器正常启动所必须满足的一些条件。

```

[root@rh9 root]# cat /etc/rc.d/init.d/dhcpd | less
:
# Check that newworking is up.
[ ${NETWORKING} = "no" ] && exit 0 # 网络服务必须启动
[-f /usr/sbin/dhcpd ] || exit 0 # 必须要有 dhcpd 守护进程程序文件
[-f /etc/dhcpd.conf ] || exit 0 # 必须要有该配置文件
[-f /var/lib/dhcp/dhcpd.leases ] || exit 0 # 必须要有该文件
RETVAL=0
prog="dhcpd"
:

```

若是采用源代码软件包安装, 则 /var/lib/dhcp/dhcpd.leases 文件很可能没有被创建, 此时可用以下命令创建一个内容为空白的文件, 该文件是 dhcpd 守护进程正常启动所必需的, dhcpd 将客户的地址租用信息保存在该文件中, 可查到 IP 地址的分配情况。

```

[root@rh9 root]# touch /var/lib/dhcp/dhcpd.leases

```

#### 2. 配置 DHCP 服务器

##### (1) DHCP 的配置文件

对 DHCP 服务器的配置, 是通过 /etc/dhcpd.conf 配置文件来实现的。可用以下命令复制一个样本配置文件到 /etc 目录中, 然后根据需要, 对配置文件进行修改即可。

```

[root@rh9 root]# cp /usr/share/doc/dhcp-3.0p11/dhcpd.conf.sample /etc/dhcpd.conf

```

DHCP 配置文件具有以下格式特点:

## 全局配置项设置

# 利用 subnet 定义 DHCP 作用域, 一个网段应定义一个作用域

```

subnet 子网 1 netmask 子网掩码 {
    option routers 默认网关地址;
    range [dynamic-bootp] low-address [high address];    # 指定可分配的 IP 地址池范围
    [其他可选设置]
}
subnet 子网 2 netmask 子网掩码 {
    option routers 默认网关地址;
    range [dynamic-bootp] low-address [high-address];    # dynamic-bootp 可缺省
    [其他可选设置]
}
:
subnet 子网 n netmask 子网掩码 {
    option routers 默认网关地址;
    range [dynamic-bootp] low-address [high-address];
    [其他可选设置]
}
group {
    组配置项设置
    host 主机名 1 {
        hardware ethernet 网卡物理地址;
        对该主机的设置;
    }
    host 主机名 2 {
        hardware ethernet 网卡物理地址;
        对该主机的设置;
    }
    :
}

```

利用 host 配置语句, 可以对指定的主机进行特别配置, 比如为某些主机分配固定的 IP 地址等。多台主机中的共同配置项, 可放在组配置项中指定, 比如默认网关、域名服务器的指定等。

## (2) 配置实例

DHCP 服务器的配置比较简单, 下面以一个具体的实例, 介绍 DHCP 服务器的配置方法, 配置过程中常用的一些配置项, 采用注释介绍其作用与功能。

部分配置项 (如 default lease-time) 可放在 subnet 段之外, 成为全局设置, 若放在 subnet 段内, 则作用域为该子网。

**[例 9.2]** 假设要为某局域网安装配置一台 DHCP 服务器,为 192.168.168.0/24 网段和 192.168.167.0/24 网段的用户提供 IP 地址动态分配服务。192.168.168.0/24 网段用于动态分配的 IP 地址池范围为 192.168.168.60~192.168.168.240,默认网关(路由)为 192.168.168.1,该网段的其余地址保留或用于静态分配,另外物理地址为 00:0C:29:04:FB:E2 的网卡,固定分配的 IP 地址为 192.168.168.100,物理地址为 00:0C:29:04:ED:35 的网卡,固定分配到的 IP 地址为 192.168.168.101。

192.168.167.0/24 网段的默认网关为 192.168.167.1,用于动态分配的 IP 地址池范围为 192.168.167.20~192.168.167.100 和 192.168.167.140~192.168.167.240,各网段默认的域名服务器为 61.128.192.68 和 61.128.128.68。物理地址为 00:0C:29:1E:2F:4A 的网卡,固定分配到的 IP 地址为 192.168.167.100。

分析:

根据需求可知,要提供动态 IP 地址分配的网段有两个,因此,在 DHCP 服务器中,需要定义两个 DHCP 作用域。对于各作用域都相同的域名服务器,可将其定义为默认域名服务器,在各作用域中就可不再单独配置了。

实现以上要求的配置文件为:

```
[root@rh9 root]# vi /etc/dhcpd.conf           # 创建 DHCP 服务器配置文件
# 全局设置
ddns-update-style interim;                    # 设置 DNS 的动态更新方式(interim 或 ad-hoc)
# 以下设置是否允许动态更新 DNS。若允许,则设置为 allow client-updates;
deny client-updates;                          # 或 ignore client-updates; 不允许更新
default-lease-time 604800;                    # 设置默认的 IP 租用期,以秒为单位
max-lease-time 864000;                       # 设置默认的最长租用期
option subnet-mask 255.255.255.0;             # 设置默认的子网掩码
# option domain-name "yourdomain.com";        # 设置默认域名
option domain-name-servers 61.128.192.68,61.128.128.68; # 设置默认的域名服务器
option time-offset -18000;                    # Eastern Standard Time
# option netbios-name-servers 192.168.252.253; # 设置默认的 WINS 服务器,用于主机名称
# 解析

# 下面分别定义 DHCP 的作用域
subnet 192.168.168.0 netmask 255.255.255.0 {
    range 192.168.168.60 192.168.168.240;    # 指定可分配的 IP 地址范围
    option broadcast-address 192.168.168.255; # 指定该网段的广播地址,可不设置
    option routers 192.168.168.1;             # 指定该网段的默认网关
```

```

    subnet 192.168.167.0 netmask 255.255.255.0 {
        range 192.168.167.20 192.168.167.100;    # 指定第 1 段 IP 地址范围
        range 192.168.167.140 192.168.167.240;    # 指定第 2 段 IP 地址范围
        option broadcast-address 192.168.167.255;    # 指定该网段的广播地址
        option routers 192.168.167.1;                # 指定该网段的默认网关
    }
    # 以下对特殊的主机进行设置
    group{
        default-lease-time 259200;                    # 可为该组的客户机单独设置租用期
        option routers 192.168.168.1;                # 为该组设置默认网关
    host staticiphost1 {
        hardware ethernet 00:0C:29:04:FB:E2;        # 指定网卡的物理地址
        fixed-address 192.168.168.100;                # 指定所固定分配到的 IP 地址
    }
    host staticiphost2 {
        hardware ethernet 00:0C:29:04:ED:35;
        fixed-address 192.168.168.101;
    }
    host staticiphost3 {
        hardware ethernet 00:0C:29:1E:2F:4A;
        fixed-address 192.168.167.100;
        option routers 192.168.167.1;                # 为该主机特别指定默认网关
    }
}

```

当要设置的主机较多时,可使用 group 归为一组,便于集中设置共同的项,若要特别设置的主机较少,也可不使用 group,而直接利用 host 语句来指定。编辑完后,存盘退出 vi。

### 3. 启动 DHCP 服务器

对 DHCP 服务器配置好后,接下来就可启动 DHCP 服务器了,其启动方法如下:

```

[root@rh9 root]# service dhcpd start                # 或 /etc/rc.d/init.d/dhcpd start
Starting dhcpd:                                     [OK]

```

若要重新启动该服务,则实现命令为 service dhcpd restart。

若要查询该服务的启动状态,则实现命令为 service dhcpd status。

若要停止该服务,则实现命令为 `service dhcpd stop`。

#### 4. 测试 DHCP 服务器

DHCP 服务器安装并启动服务后,可找台安装有 Windows 系统的计算机,将 IP 地址设置为自动获得,并在指定的网段接入网络并启动计算机,然后在 MS-DOS 状态下执行 `ipconfig /all` 命令,此时若能看到所分配到的 IP 地址、默认网关和 DNS 服务器地址,则说明 DHCP 服务器工作正常,配置成功。对于 Windows 98 系统,则可运行 `winipcfg` 来查看。

## 习题

1. 要检查当前 Linux 系统是否安装有 DNS 服务器,以下命令中,正确的是( )。  
A. `rpm -q dns`                      B. `rpm -q bind`  
C. `ps -aux |grep bind`              D. `ps -aux | grep dns`
2. 以下对 DNS 服务器的描述,正确的是( )。  
A. DNS 服务器的主配置文件为 `/etc/named/dns.conf`  
B. 配置 DNS 服务器,只需配置好 `/etc/named.conf` 文件即可  
C. 配置 DNS 服务器,通常需要配置 `/etc/named.conf` 和相应的区域文件  
D. 配置 DNS 服务器时,正向和反向区域文件都必须配置才行
3. 设置 DNS 的转发器,可在主配置文件中通过( )语句来实现。  
A. `forward`                              B. `forwards`  
C. `forwarders`                          D. 通过定义转发区来实现
4. 启动 DNS 服务器的命令是( )。  
A. `service bind restart`              B. `service bind start`  
C. `service named start`                D. `server named start`
5. 检验 DNS 服务器配置是否成功,解析是否正确,最好采用( )命令来实现。  
A. `ping`                                  B. `netstat`  
C. `ps -aux | bind`                      D. `nslookup`
6. 对 DHCP 服务器的配置,以下描述中错误的是( )。  
A. 启动 DHCP 服务器的命令是: `service dhcpd start`  
B. 对 DHCP 服务器的配置,均可通过 `/etc/dhcp.conf` 配置文件来实现  
C. 在定义作用域时,一个网段通常应定义一个作用域,可通过 `range` 配置语句来指定可分配的 IP 地址范围,使用 `option routers` 配置语句来指定默认网关  
D. DNS 服务器的地址通常可放在全局设置中来定义,其设置语句是 `option domain-name`

## 实训 9-1 安装与配置 DNS 服务器

**[实训目的]** 掌握 DNS 服务器的配置与测试方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 查询当前系统是否安装了 BIND 软件包,若未安装,则使用安装光盘中的 RPM 软件包,安装 bind-9. 2. 1-16. i386. rpm、bind-utils-9. 2. 1-16. i386. rpm 和 caching-nameserver-7. 2-7. noarch. rpm 软件包。

2. 按照例 9.1 所讲的步骤与方法,配置 DNS 服务器,然后使用 nslookup 命令,测试 DNS 服务器解析是否正常。

## 实训 9-2 安装与配置 DHCP 服务器

**[实训目的]** 掌握 DHCP 服务器的配置与使用方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 查询当前系统是否安装 DHCP 服务器软件包,若未安装,则利用安装光盘,安装 DHCP 的服务器软件包 dhcp-3. 0pl1-23. i386. rpm。

2. 按照例 9.2 所示的步骤与方法,配置 DHCP 服务器,然后启动 DHCP 服务器,并测试 DHCP 服务器工作是否正常。

## 配置 qmail 邮件服务器

电子邮件服务也是互联网中最受欢迎、应用最广泛的一种服务,能实现电子邮件收发服务的服务器,即称为邮件服务器。本章以 Linux/UNIX 平台最优秀的 qmail 邮件服务器为例,介绍 Linux 系统中,邮件服务器的安装、配置与使用方法。

### 10.1 邮件服务系统简介

电子邮件服务系统包括邮件传输代理(mail transfer agent,MTA)和邮件用户代理(mail user agent,MUA)两部分构成。邮件传输代理属于服务器端应用程序,用于处理邮件的发送和接收以及邮件的转发等功能,它就是通常所说的邮件服务器,其具体职责为:

- 接收和传递(转发)由客户端发送的邮件。
- 为需要发送的邮件进行排队。
- 接收从其他邮件服务器转发来的用户邮件,并将邮件放置在一个指定的存储区域,直到用户连接本邮件服务器收回邮件。
- 根据设定的条件,有选择地转发或拒绝转发用户的邮件,或有选择地拒绝接收用户的邮件(邮件过滤)。

邮件的传输是通过 SMTP(simple mail transfer protocol,简单邮件传输协议)协议来实现的,是最基本的 Internet 邮件服务协议,该协议使用 TCP 25 号端口。ESMTP 称为扩展的 SMTP,增加了发件认证功能。

POP3(post office protocol,邮局协议)是允许用户从邮件服务器接收邮件的协议,常与 SMTP 协议相结合使用,POP3 是目前最常用的电子邮件服务协议。该协议使用 TCP 110 和 UDP 110 号端口。

IMAP 是 Internet Message Access Protocol 的缩写,称为 Internet 消息访问协议,目前常用的是版本 4,即 IMAP4,为用户提供了有选择性地从邮件服务器接收邮件、基于服务器的信息处理和共享邮箱等功能。

MIME 协议是多用途 Internet 邮件扩展 (Multipurpose Internet Mail Extensions), 作为对 SMTP 协议的扩展, MIME 规定了通过 SMTP 协议传输非文本电子邮件附件的标准。

邮件用户代理是邮件系统的客户端程序, 为用户提供邮件接收和发送服务。常用的客户端程序主要有 Foxmail、Outlook 和 Netscape Messenger。另外还有基于 Web 页面的邮件客户程序, 支持利用 Web 页面来实现邮件的收发服务。

Linux/UNIX 平台常用的邮件传送代理 MTA 主要有 Sendmail、Postfix 和 qmail, Sendmail 和 Postfix 是 Red Hat Linux 自带和默认安装的邮件服务器。Sendmail 在 UNIX 系统中属元老级的邮件传送代理, 但配置比较麻烦, 安全性较差。

qmail 可运行在 UNIX/Linux 系统, 是面向安全面设计的, 其目标是比 Sendmail 更容易使用, 并且运行更快速、高效和更安全, 是目前最受欢迎的一种邮件服务器之一, 它具有以下特点:

- 安全性更高 qmail 采用模块化设计, 将邮件处理分为多个过程, 采用不同的进程来分别实现, 并尽量避免使用 root 用户运行。

qmail 支持第三方的 vpopmail 软件包, 实现对虚拟域的管理。利用该软件包提供的 - 一个称为 vchkpw 的插件来支持虚拟 POP 域, 这样 POP3 邮件用户就不再需要系统的正式账户, 从而实现了邮件账户与 Linux 系统账户的分离, 进一步增强了安全性。

- 可靠性更高 为了保证可靠性, qmail 只有在邮件被正确地写入到磁盘才返回处理成功的结果, 这样即使在磁盘写入中发生系统崩溃或断电等情况, 也可以保证邮件不被丢失, 而是重新投递。另外, qmail 使用一种新的更可靠的邮箱格式 Maildir, 保证已经接收的新邮件不被丢失。
- 运行更高效 qmail 比其他实现同样功能的 MTA 都要小, 能更高速和高效地收发邮件。qmail 在一个中等规模的系统中每天可以投递大约百万封邮件。qmail 支持邮件的并行投递, 默认配置情况下, 能够达到 20 个并行邮件同时传送。qmail 的作者提出了 QMTP (quick mail transfer protocol) 来加速邮件的投递, 并在 qmail 中得到支持 (qmail-qmtpd), 若要启用 qmail 独有的快速邮件投递, 则使用 qmail-qmtpd 进程取代传统的 qmail-smtpd 进程即可。另外, 利用 qmail 还可实现分布式的邮件服务器。



Postfix 具有运行快速、安全和易于管理等优点,也是一个相当优秀的邮件服务器程序,Red Hat Linux 9 也自带该邮件程序。

## 10.2 qmail 工作流程简介

qmail 是采用模块化设计的邮件服务器,提供本地和远程邮件的传送和转发,每一个子功能都是由一个程序(进程)来实现的,每个程序的运行方式,则是由一个或多个配置文件和环境变量来共同控制的。有些进程常驻内存,有些仅在工作时才驻留内存,工作结束后就会被释放。利用 `ps -auxw | grep qmail` 命令,可查看到驻留在内存中的 qmail 进程。

qmail 的进程由相应的程序启动,这些程序位于 `/var/qmail/bin` 目录中,为便于理解 qmail 的工作方式,本节先介绍 qmail 的几个主要进程的功能与作用。

### 1. qmail-smtpd 与 qmail-inject

qmail-smtpd 进程以 `qmaild` 用户身份运行,用于接收/拒收通过 SMTP 传递的邮件,若允许发送,则将邮件传递给 `qmail-queue` 进程处理。`qmail-smtpd` 并不常驻内存,可用 `tcpserver` 或 `xinetd` 服务管理器来激活。`tcpserver` 可监视系统的 IP 连接请求,若侦听到 SMTP 连接请求,`tcpserver` 就会启动 `qmail-smtpd` 进程,然后将连接请求交由 `qmail-smtpd` 处理,SMTP 连接建立后,远端主机就可将邮件投递到本邮件服务器了。

qmail 采用模块化设计,通过使用不同的认证模块,可以支持多种用户认证方案。增加发件认证后,对于 Linux 系统账户,使用 `checkpassword` 程序来验证用户账户和密码;对于虚拟邮件域账户,则应使用 `vpopmail` 提供的 `vchkpw` 和第三方的 `cmd5checkpw` 程序来验证,即 CRAM-MD5 认证类型使用 `cmd5checkpw` 程序来验证。

`qmail-inject` 进程则用于接收本地域邮件用户投递的邮件,并将邮件传递给 `qmail-queue` 进程处理。

### 2. qmail-queue

该进程处理从 `qmail-smtpd` 和 `qmail-inject` 传递过来的邮件,并将这些邮件传递到邮件队列中。

### 3. qmail-send

该进程以 `qmails` 用户身份运行,用于投递来自消息队列的邮件。当一个邮件被放入邮件队列之后,`qmail send` 就开始对该邮件进行处理,它会检查邮件队列中的每一个邮件

的状态,对于没有投递过的和投递暂时失败的邮件,qmail-send 会将目标地址是本地主机的传递给 qmail-lspawn,目标地址是远端主机的传递给 qmail-rspawn,对于投递永久失败的邮件,qmail-send 将该邮件传递给 qmail-clean,让其永久删除该邮件。

qmail-send 常驻内存,若使用 killall qmail-send 结束该进程,则与之相关的 qmail-lspawn、qmail-rspawn 和 qmail-clean 进程也将被自动结束。以后若要重启这些进程,可通过执行“/var/qmail/rc &.”命令来启动。

#### 4. qmail-rspawn 与 qmail-lspawn

qmail-rspawn 进程常驻内存,以 qmailr 用户身份运行,其作用是调度邮件投递的时间和顺序,然后启动 qmail-remote 进程完成与目标邮件服务器的连接和邮件的投递。qmail-lspawn 与 qmail rspawn 功能相似,它启动 qmail-local 进程,来完成目标地址是本地域的邮件的投递,以 root 身份运行该进程。

#### 5. qmail-clean

该进程也是常驻内存,其作用是从邮件队列中删除投递永久失败的邮件,以 qmailq 用户身份运行。

#### 6. qmail-remote 与 qmail-local

qmail-remote 进程通过 SMTP 协议将邮件投递给远端的用户,默认允许运行 20 个 qmail remote 并发进程。一个 qmail-remote 进程每次只能同一个远端主机(目标邮件服务器)连接,在连接时,可以同时投递在这个远端主机上的多个接收者的邮件。

qmail-local 进程用于投递目标地址是本地邮件服务器的邮件,并负责将邮件投递到本地邮件用户的邮箱中,默认允许运行 10 个 qmail-local 并发进程。

qmail 邮件服务器发信的工作流程如图 10.1 所示。

#### 7. qmail-popup 与 qmail-pop3d

qmail-popup 进程用于通过网络获取客户端提交的 pop 账户和密码,然后调用 vchkpw 程序对用户身份进行验证,并设置相应的环境变量,验证通过后,再交给 qmail-pop3d 进程处理,实现用户邮件的读取或删除。qmail-pop3d 是 POP3 的后台服务程序,是 qmail 自带的 POP 服务器。

qmail-popup 进程通常用 tcpserver 或 xinetd 服务管理器来对其进行管理,并在 110 端口进行监听 POP 连接请求。

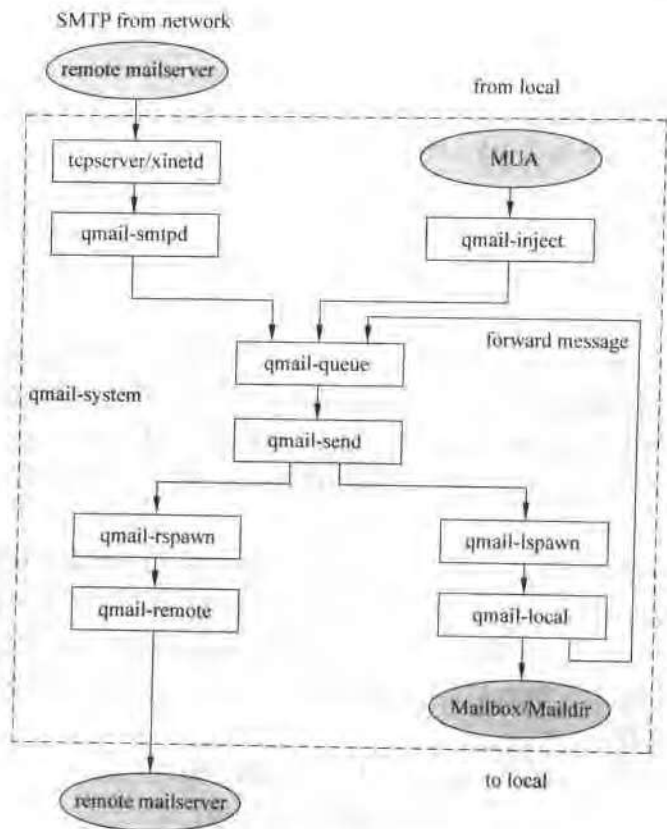


图 10.1 qmail 邮件服务器工作流程

### 10.3 安装 qmail 邮件服务器

qmail 的软件包仅实现了基本的邮件收发功能,若要创建虚拟邮件域并对其进行管理,提供邮件账户的在线申请和管理,以及提供基于 Web 的邮件收发功能,则需要另外安装基于 qmail 的一些配套软件包。

本节创建的 qmail 示例邮件服务器,具备以下功能:

- 支持 Foxmail 和 Outlook 等邮件客户端软件收发邮件,并支持发件认证 (ESMTP)。
- 支持 webmail,即支持用户通过 Web 页面进行邮件的收发。
- 支持利用 Web 页面申请注册邮件账户。

- 支持邮件虚拟域的创建和管理。
- 具备防病毒和反垃圾邮件的能力。

### 1. qmail 服务器的相关软件包

安装 qmail 邮件服务器常用的软件包及功能如下:

- netqmail-1.05.tar.gz qmail 1.05 基本系统软件包,内含 qmail-1.03.tar.gz 和升级到 1.05 的补丁以及一些相关的补丁。
- qmail-smtpd-auth-0.31.tar.gz SMTP 发信认证补丁程序,使 qmail 支持 ESMTP。
- ucspi-tcp-0.88.tar.gz 提供 tcpserver 服务,它是一个类似 inetd 的服务管理工具。该服务监视系统的 IP 连接请求,当检测到有 SMTP 连接请求时,tcpserver 就会自动地激活 qmail-smtpd,然后将 IP 连接的控制权交给 qmail-smtpd 处理。
- checkpassword-0.90.tar.gz pop 用户验证程序,用于验证 Linux 系统账户邮件。
- cmd5checkpw-0.22.tar.gz pop 用户验证程序,用于对虚拟域用户进行验证。
- vpopmail-5.4.6.tar.gz 基于 qmail 的虚拟邮件域创建和管理程序。
- sqwebmail-4.0.7.tar.bz2 一个 Web 界面的邮件客户端,使用 CGI 实现。
- igenus\_2[1].0.1\_20040713\_release.tgz 另一个 Web 界面的邮件客户端,使用 PHP 实现。
- vqsignup-0.5.tar.gz 提供 Web 方式的邮件用户注册。
- ezmlm-0.53.tar.gz 提供用户邮件列表管理。
- autorespond-2.0.4.tar.gz 邮件自动回复程序。
- qmailadmin-1.2.2.tar.gz 提供 Web 界面来管理 vpopmail 邮件域。
- daemontools-0.76.tar.gz 守护进程管理工具,用于对 qmail 进程进行管理。借助该管理工具所提供的命令,通过编写服务器控制脚本,可实现 qmail 各服务进程的启动、重启、查询服务状态或停止服务等功能。
- courier-imap-3.0.7.tar.bz2 使 qmail 支持 IMAP4 服务的软件包。

qmail 相关软件包的下载网址为 <http://cr.yp.to/qmail.html>、<http://www.inter7.com>、<http://sourceforge.net/projects/qmailadmin> 和 <http://www.igenus.org>,另外也可直接到作者的网站下载(<http://www.pcnetedu.com>)。可将相关的软件包下载或复制到 `/usr/local/src/qmail` 目录中。

### 2. 安装前的准备工作

(1) 申请注册域名,并设置该域的 MX 记录

在准备安装和组建 qmail 邮件服务器之前,应首先申请注册一个域名,并设置该域的

MX(邮件交换)记录指向邮件服务器主机。邮件服务器主机还必须拥有一个固定的公网 IP 地址。若邮件服务器主机有固定 IP 地址,但没有一个域的 MX 记录指向该服务器,则邮件服务器将无法接收到邮件。

此处假设已申请了 pcnetedu.com 域名,www.pcnetedu.com 用于 Web 服务,mail.pcnetedu.com 作为邮件服务器的主机名。

要检查所申请的域名是否生效,可直接利用 ping 命令去 ping 域名即可,对于 MX 记录是否生效,可采用如下方法来检查:

```
[root@rh9 root]# host -t mx pcnetedu.com      # 查询该域的 MX 记录指向的邮件服务器主机
pcnetedu.com mail is handled by 10 mail.pcnetedu.com.
[root@rh9 root]# host -t a mail.pcnetedu.com   # 查询 mail.pcnetedu.com 主机的 A 记录
mail.pcnetedu.com has address 61.186.170.104
```

另外,也可利用 nslookup 来检查,该命令在 Windows 和 Linux 平台均提供有。

## (2) 卸载 sendmail

Red Hat Linux 9 默认安装了 sendmail,有的可能还安装了 postfix 邮件服务器,在决定安装使用 qmail 之前,应先卸载已安装的邮件服务器,其实现命令为:

```
[root@rh9 root]# rpm -e sendmail - nodeps      # 删除 sendmail 邮件服务器
[root@rh9 root]# rpm -e postfix --nodeps       # 删除 postfix 邮件服务器
[root@rh9 root]# rm -rf /var/mail              # 删除邮件目录
```

在卸载软件包时,若有其他软件包要依赖于所卸载的软件包,卸载时会产生错误提示信息,若要忽略该提示信息,继续卸载,可使用“--nodeps”命令选项。

## (3) 创建 qmail 和 vpopmail 所需的用户和用户组

qmail 的工作目录(home directory)默认为/var/qmail,若要更改,可在编译 qmail 之前,编辑源代码目录中的 conf-qmail 文件。

qmail 工作时将要用到名为 qmail 和 nofiles 的用户组,以及一些用户账户,这些所需的用户组 and 用户账户,在编译安装 qmail 之前必须事先创建好。用户和组的创建可参阅源代码目录中的 INSTALL.ids 文档,内有各平台创建方法的详细说明。对于 Linux 系统,其创建方法如下:

```
[root@rh9 root]# mkdir /var/qmail              # 创建 qmail 工作目录
[root@rh9 root]# groupadd -g 91 nofiles
[root@rh9 root]# useradd -g nofiles -u 91 -s /bin/false -d /var/qmail/alias alias
[root@rh9 root]# useradd -g nofiles -u 92 -s /bin/false -d /var/qmail qmaild
[root@rh9 root]# useradd -g nofiles -u 93 -s /bin/false -d /var/qmail qmailf
[root@rh9 root]# useradd -g nofiles -u 94 -s /bin/false -d /var/qmail qmailp
[root@rh9 root]# groupadd -g 92 qmail
```

```
[root@rh9 root]# useradd -g qmail -u 95 -s /bin/false -d /var/qmail qmailq
[root@rh9 root]# useradd -g qmail -u 96 -s /bin/false -d /var/qmail qmailr
[root@rh9 root]# useradd -g qmail -u 90 -s /bin/false -d /var/qmail qmails
```

qmail 所使用的用户和用户组,若要更改,可在编译前编辑源代码目录中的 conf-users 和 conf-groups 文件,但建议用户一般不要更改。此处为用户和用户组指定了 UID 和 GID,主要是为了安全。

vpopmail 是与 qmail 配合使用的虚拟域管理软件, vpopmail 进程运行时需要名为 vpopmail 的用户,所属的用户组为 vchkpw,默认工作目录为/home/vpopmail,其用户和用户组的创建方法如下:

```
[root@rh9 root]# groupadd -g 89 vchkpw
[root@rh9 root]# useradd -g vchkpw -u 89 vpopmail
```

最后检查/etc/shells 文件中是否有/bin/false,若没有,则利用以下命令添加进去。

```
[root@rh9 root]# echo "/bin/false">>/etc/shells
```

### 3. 安装 qmail 1.05 软件包

#### (1) netqmail-1.05 软件包介绍

netqmail-1.05.tar.gz 是 qmail 的基本系统软件包,内含 qmail 1.03 的源代码软件包和将其升级到 1.05 的补丁,另外在 other-patches 目录下还提供了与 qmail 紧密相关的几个软件包的补丁:ucspi-tcp-0.88.errno.patch,ucspi-tcp-0.88.a\_record.patch,ucspi-tcp-0.88.nodfaulttbl.patch,checkpassword-0.90.errno.patch,daemontools-0.76.errno.patch。

Red Hat Linux 9 使用了新的 2.3.1 版的 GLIBC 库,在编译 qmail-1.03 和一些其他软件包时,会出现“undefined reference to 'errno'”编译错误,此时必须对源代码做修正打补丁,才能正常编译。对应的补丁在命名上通常含有.errno.patch 关键字。qmail 官方提供的推荐补丁可访问 <http://www.qmail.org/moni.csi.hu/pub/glibc-2.3.1/>。

netqmail-1.05.patch 补丁已包含了解决 errno 错误的补丁,对 qmail-1.03.tar.gz 打 1.05 的补丁后,即可正常编译了。

netqmail-1.05.tar.gz 解压后,在目录中有一个名为 collate.sh 的可执行文件,直接执行该文件,即可实现对 qmail-1.03.tar.gz 的解压,并利用 netqmail-1.05.patch 对其打补丁,然后将 qmail-1.03 目录更名为 netqmail-1.05,在 netqmail-1.05 目录就可编译安装 qmail 了。

#### (2) qmail 的其他补丁

qmail 本身并不支持发信认证,即不支持 ESMTP,但可通过给源代码打认证补丁来

实现认证功能,其认证补丁为 qmail-smtpd-auth-0.31.tar.gz,此处使用 qmail-toaster-0.6-1.patch.bz2 补丁集,该补丁集包括以下几个重要的补丁:

- smtp-auth-0.4.2 SMTP 认证补丁。
- qmail-queue (to allow for virus scanners) 允许杀毒和反垃圾邮件的软件扫描队列的补丁。
- netqmail-mailldir++.patch Maildir 邮箱补丁,使邮箱支持磁盘限额。
- support-oversize-dns-packets (not necessary if you use dns-cache) 超大 DNS 查询响应补丁。

DNS 的查询响应一般被限制在 512B 以内,但一些大型站点由于有多个 MX 记录,其 DNS 查询响应可能会多于 512B,此时 qmail 在处理时就会出现错误,导致无法向这些域发送邮件,该补丁可解决该问题。

- qmail-1.03-mfcheck.3.patch (check that the envelope sender has a dns entry) 该补丁用于检查发送信封中是否有一个合法的 DNS 域名,以避免收到无法回复的邮件。
- tarpit-delay。
- qregex (regular expression matching in badmailfrom and badmailto) 允许在 badmailfrom 和 badmailto 配置文件中正则表达式来匹配邮箱或邮件域。
- big-concurrency (set the spawn limit above 255) 该补丁使对 spawn 的限制突破 255,从而可以使用更多 qmail-remote 和 qmail-local 进程。

另外,该补丁集还提供了 IMAP 服务器需要使用的 TLS(SSL)支持,但需要事先安装好 openssl。

### (3) 编译安装 qmail

```
[root@rh9 root]# cd /usr/local/src/qmail
[root@rh9 qmail]# tar -zxvf netqmail-1.05.tar.gz
[root@rh9 qmail]# cd netqmail-1.05
[root@rh9 netqmail-1.05]# ls
[root@rh9 netqmail-1.05]# ./collate.sh #打补丁,将 1.03 升级到 1.05
[root@rh9 netqmail-1.05]# ls
[root@rh9 netqmail-1.05]# bunzip2 -c ../qmail-toaster-0.6-1.patch.bz2 | patch -p0
[root@rh9 netqmail-1.05]# cd netqmail-1.05
```

下面为 TLS(SSL)补丁所需的 include 文件创建符号连接,需要系统安装有 openssl。

```
[root@rh9 netqmail-1.05]# ln -s /usr/kerberos/include/com_err.h /usr/kerberos/include/krb5.h \
/usr/kerberos/include/profile.h /usr/include/
```

下面编译 qmail, 并创建 qmail 安装目录树。WITH\_QMAILQUEUE\_PATCH=yes 配置项表示以后将使用 qmail-queue 扫描器, 该扫描器可调用防病毒和反垃圾邮件引擎, 实现对邮件的防病毒检查和反垃圾过滤。

```
[root@rh9 netqmail-1.05]# make WITH_QMAILQUEUE_PATCH=yes setup check
```

若要对进出的邮件进行监控, 将其发送到指定的邮箱, 则在编译前可对 extra.h 文件进行修改。文件中的 QUEUE\_EXTRA 是一个编译时的配置参数, 用于确定每个邮件传送的一个附加的接收者, 并使用 "Trecipient\0" 格式来指定附加接收者。其中 recipient 代表接收者的邮件用户名。

QUEUE\_EXTRALEN 用于设置 QUEUE\_EXTRA 的字符长度, "\0" 算一个字符, 比如, 若要设置将所有进出的邮件都向 mailclone 邮箱发送一份, 则修改方法如下:

```
# vi extra.h
# define QUEUE_EXTRA "Tmailclone\0"
# define QUEUE_EXTRALEN 11
```

最后还要记得创建名为 "mailclone@域名" 的邮箱, 以便接收进出该邮件服务器的邮件。

#### (4) 配置邮件域名

```
[root@rh9 qmail-1.03]# ./config-fast mail.penetedu.com
Your fully qualified host name is mail.penetedu.com
Putting mail.penetedu.com into control/me...
Putting penetedu.com into control/defaultdomain...
Putting penetedu.com into control/plusdomain...
Putting mail.penetedu.com into control/locals...
Putting mail.penetedu.com into control/rcpthosts...
Now qmail will refuse to accept SMTP messages except to mail.penetedu.com.
Make sure to change rcpthosts if you add hosts to locals or virtualdomains!
```

下面启用邮件发送者信封域名检查, 以检查邮件的信封中是否有合法的 DNS 域名, 以防止垃圾邮件。

```
[root@rh9 netqmail-1.05]# echo 1 >> /var/qmail/control/mfcheck
```

#### (5) 建立 qmail 需要的系统别名

对别名的创建要求和创建方法可参阅源代码目录中的 INSTALL.alias 文档。别名的创建方法如下:

```
[root@rh9 qmail-1.03]# cd ~alias
```



```
[root@rh9 alias]# touch .qmail-postmaster .qmail-mailer-daemon .qmail-root
[root@rh9 alias]# chmod 2755 ~alias
[root@rh9 alias]# chmod 644 ~alias/.qmail *           # 或 chmod 644 .qmail *
```

postmaster 代表邮件系统管理员, mailer-daemon 为反弹邮件的标准接收者, root 代表 Linux 系统的管理者。若要让本地邮件用户 mailmaster 能接收到发送给邮件系统管理员和系统管理员的邮件, 则只需将该账户添加到相应的别名文件中即可。

```
[root@rh9 alias]# echo mailmaster > /var/qmail/alias/.qmail-postmaster
[root@rh9 alias]# echo mailmaster > /var/qmail/alias/.qmail-root
```

#### (6) 创建 sendmail 的符号连接

很多程序默认调用 sendmail 来发送邮件, 在删除 sendmail 邮件服务器后, 需要利用 qmail 提供的 sendmail 程序, 在原 sendmail 所在的位置, 创建一个 sendmail 的符号链接, 其创建方法如下:

```
ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
```

若不创建该链接, 原来依赖于 sendmail 发信的程序, 可能无法正常发送邮件。sendmail 是一个通用的发信接口, 为了兼容, qmail 也提供了一个 sendmail 程序, 但该程序仅是 qmail-inject 的一个外壳程序, 真正用来实现发信的程序是 qmail-inject。比如, 利用以下语句, 可实现给 mailmaster@pcnnetedu.com 发送一封空白邮件。

```
[root@rh9 qmail]# echo To: mailmaster@pcnnetedu.com | /var/qmail/bin/qmail-inject
```

#### (7) 设置 qmail 使用 Maildir 邮箱格式

qmail 支持三种邮件存储格式, 分别是传统的 UNIX 邮箱格式(/var/spool/mail)、最常见的~user/Mailbox 和新型的~user/Maildir 格式, 前两种使用较普遍, 但均存在安全上的隐患, Maildir 格式可使运行更安全更高效。

/var/qmail/boot 目录包含了不同配置的 qmail 启动脚本示例, 对于这三种邮件存储格式的创建方法如下:

/var/spool/mail 格式, 实现操作为: cp /var/qmail/boot/proc /var/qmail/rc  
Mailbox 和 Maildir 格式, 实现操作为: cp /var/qmail/boot/home /var/qmail/rc  
下面设置 qmail 使用 Maildir 邮箱格式:

```
[root@rh9 qmail]# cp /var/qmail/boot/home /var/qmail/rc
[root@rh9 qmail]# vi /var/qmail/rc           # 编辑 rc, 将默认的 Mailbox 更改为 Maildir
# ! /bin/sh
# Using splogger to send the log through syslog.
```

```
# Using qmail-local to deliver messages to ~'Maildir by default.
exe env -PATH " var/qmail/bin: $PATH" \
qmail-start . /Maildir/ splogger qmail
```

修改后存盘退出 vi。qmail-start 用于启动激活 qmail 的邮件投递服务, splogger 用于启动 splogger 进程, 该进程以 qmail 用户身份运行, 用于控制日志。整个命令启动的进程有 qmail-send、splogger、qmail-lspawn、qmail-rspawn 和 qmail-clean。

```
[root@rh9 qmail]# chmod 755 /var/qmail/rc # 设置为可执行文件
```

以后就可通过执行 /var/qmail/rc 来启动 qmail 的守护进程了, 启动时注意带 & 符号, 让其以后台方式运行, 其启动方法如下:

```
[root@rh9 qmail]# /var/qmail/rc &
[1] 11146
[root@rh9 qmail]# ps -auxw | grep qmail # 查看所启动的守护进程
qmails  11146  0.2  0.2  1392  328  tty1    S  23:45  0:00 [qmail-send]
qmail  11147  0.0  0.2  1360  400  tty1    S  23:45  0:00 [splogger]
root    11148  0.0  0.2  1368  284  tty1    S  23:45  0:00 qmail-lspawn . /Maildir/
qmailr  11149  0.0  0.2  1368  288  tty1    S  23:45  0:00 [qmail-rspawn]
qmailq  11150  0.0  0.2  1348  284  tty1    S  23:45  0:00 [qmail-clean]
root    11152  0.0  0.4  4436  620  tty1    S  23:45  0:00 grep qmail
```

到此为止, qmail 服务器的基本系统就安装完毕, 但 qmail 的 SMTP 和 POP3 服务进程还未启动, 因此, 目前还无法发送和接收邮件。qmail 的 SMTP 服务进程 qmail-smtpd 和 POP3 服务的进程 qmail-popup 通常采用 tcpserver 服务管理器来管理。

#### 4. 安装 checkpassword 和 cmd5checkpw 软件包

对邮件账户密码的校验, 若使用 Linux 系统账户来作为邮件账户, 则密码校验使用 checkpassword 程序; 若使用虚拟域的邮件账户, 则使用 cmd5checkpw 程序来验证。若不用 Linux 的系统账户来作为 E-mail 账户, 则不用安装 checkpassword, 可通过安装 vpopmail 来支持虚拟域, 从而实现用非系统账户来作为 E-mail 账户, 这样可大大提高系统的安全性。下面介绍一下这两个软件包的安装方法。

##### (1) 安装 checkpassword

```
[root@rh9 root]# cd /usr/local/src/qmail
[root@rh9 qmail]# mv ./netqmail-1.05/other-patches/* . # 将补丁移到 qmail 目录
[root@rh9 qmail]# tar -zxvf checkpassword-0.90.tar.gz
[root@rh9 qmail]# cd checkpassword-0.90
[root@rh9 checkpassword-0.90]# patch -p1 < ../checkpassword-0.90.errno.patch
[root@rh9 checkpassword-0.90]# make
[root@rh9 checkpassword-0.90]# make setup check
```

```
[root@rh9 checkpassword-0.90]# chmod 4755 /bin/checkpassword
[root@rh9 checkpassword-0.90]# ll /bin/checkpassword
-rwsr-xr-x 1 root root 7716 Aug 30 17:01 /bin/checkpassword
```

## (2) 安装 cmd5checkpw

```
[root@rh9 qmail]# tar -zxvf cmd5checkpw-0.22.tar.gz
[root@rh9 qmail]# mkdir /usr/man
[root@rh9 qmail]# mkdir /usr/man/man8
[root@rh9 qmail]# cd cmd5checkpw-0.22
[root@rh9 cmd5checkpw-0.22]# make
[root@rh9 cmd5checkpw-0.22]# make install
cp cmd5checkpw /bin/; cp cmd5checkpw.8 /usr/man/man8/
```

## 5. tcpserver 与邮件中继

tcpserver 是一个类似 inetd 的服务器管理程序,可用于控制对 qmail 邮件服务器的连接和邮件的中继(relay)。qmail 的 SMTP 服务进程 qmail-smtpd,通常作为 tcpserver 的一个子进程来运行,在进程列表中,通常看到的是 tcpserver,而不是 qmail-smtpd。

### (1) 安装 tcpserver 软件包

```
_root@rh9 qmail]# tar -zxvf ucspi-tcp-0.88.tar.gz
[root@rh9 qmail]# cd ucspi-tcp-0.88
[root@rh9 ucspi-tcp-0.88]# patch -p1 < ../ucspi-tcp-0.88.a_record.patch
[root@rh9 ucspi-tcp-0.88]# patch -p1 < ../ucspi-tcp-0.88.errno.patch
[root@rh9 ucspi-tcp-0.88]# patch -p1 < ../ucspi-tcp-0.88.nobase.patch
[root@rh9 ucspi-tcp-0.88]# make
[root@rh9 ucspi-tcp-0.88]# make setup check
```

其可执行文件安装在/usr/local/bin/目录中,常用的主要有 tcpserver 和 tcprules。

### (2) qmail 的邮件中继控制

#### ① 邮件中继简介

邮件中继是指服务器接受客户端的 smtp 发信请求,并将客户端发往第三方(非本域邮件用户)的邮件进行转发。当邮件服务器开放中继功能后,若不对允许中继的用户进行有效控制,邮件服务器将成为垃圾邮件转发的中继站。qmail 可使用发件认证和中继规则来防止邮件中继被滥用。

qmail 服务器启动后,其 qmail-smtpd 进程将监听 25 号端口,等待并接受用户的发信请求,网络上的其他 mail 服务器或发送邮件的 MUA 程序,也会主动连接 qmail 服务器的 25 号端口,通过 SMTP 会话,即可建立连接,并实现发送邮件。对于具有发信认证功能的 ESMTP,在会话过程中,将验证用户的身份(利用邮件账户和密码),只有身份验证通过后,才允许该用户发送邮件。发件认证是目前防止转发垃圾邮件的常用手段之一,对于拥

有合法身份的邮件发送者,若要禁止其中继或者要禁用某个或某些用户对邮件服务器的访问,则可进一步使用中继规则来进行控制。

## ② 设置 relay 规则

qmail 有一个名为 rcpthosts 的配置文件,它决定是否接受一个发信请求。只有当邮件接收者地址的域名存在于 rcpthost 文件中时,该发信请求才会被接收,否则将拒绝发送该邮件。若该文件不存在,则接受所有的发送请求,此时相当于完全开放了邮件中继。

qmail 的 qmail-smtpd 进程用于接收用户的发信请求,并将其传递给邮件队列处理,但该进程并不常驻内存,因此需要使用 tcpserver 进程来监听 SMTP 连接请求。当有 SMTP 连接请求时,tcpserver 会根据中继规则,决定是否允许该用户连接,若允许,则为其设置相关环境变量,然后启动激活 qmail-smtpd 进程,并将 SMTP 请求交给 qmail-smtpd 进程处理。若当前 RELAYCLIENT 环境变量被设置,则 rcpthost 文件将被忽略,此时允许用户中继;若 RELAYCLIENT 环境变量未被设置,则将拒绝中继。因此,利用中继控制文件,可实现 SMTP 的访问控制。

对中继规则的设置,使用 tcpserver 的配置文件 tcp.smtp 来实现,其配置命令用法如下:

```
IP 地址或网络号:deny | [allow [, RELAYCLIENT=""]]
```

deny 表示拒绝连接;allow 表示允许连接;RELAYCLIENT="" 用于设置环境变量,以决定是否允许中继。

比如,若允许转发本地主机用户所发送的邮件,则配置命令为:

```
127.0.0.1:allow, RELAYCLIENT=""
```

若要禁止 61.186.170.230 用户连接访问邮件服务器,则配置命令为:

```
61.186.170.230:deny
```

中继规则是使用 SMTP 请求者的 IP 地址来进行控制的,一般适合于 IP 地址相对固定的情况。对于未明确设定的 IP 地址,中继规则默认为 deny。

假设局域网用户通过代理访问 Internet,代理服务器的 IP 地址为 61.186.170.130,允许内网用户的邮件转发(中继),则中继控制文件的创建方法为:

建议将 tcp.smtp 文件存放/home/vpopmail/etc 目录中,vpopmail 也需要使用该文件。

```
[root@rh9 root]# mkdir -p /home/vpopmail/etc
[root@rh9 root]# vi /home/vpopmail/etc/tcp.smtp
127.0.0.1:allow, RELAYCLIENT=""
61.186.170.130:allow,RELAYCLIENT=""
```

```
;allow
```

tcpserver 并不直接使用 tcp.smtp 文件,中继规则设置好后,需要将其编译转换为 cdb 格式的中继控制文件,才能被 tcpserver 识别和使用。转换方法为:

```
[root@rh9 root]# cd /home/vpopmail/etc
[root@rh9 etc]# /usr/local/bin/tcprules tcp.smtp.cdb tcp.smtp.tmp<tcp.smtp
[root@rh9 etc]# chmod 644 /home/vpopmail/etc/tcp.smtp.cdb
```

生成的 tcp.smtp.cdb 文件,将在后面启动 SMTP 服务的命令行中通过 -x 参数引用。

## 6. 安装 vpopmail

vpopmail 是一个以 qmail 为基础的虚拟邮件域管理软件,利用 vpopmail 可创建多达 2300 个虚拟邮件域,每个域可创建 2300 个邮件用户,并可实现对这些域和域中的用户进行管理。另外也可使用 qmailadmin 管理工具,利用 Web 页面实现对域和域中用户的远程管理。

### (1) 安装前的准备工作

vpopmail 要使用 MySQL 数据库,因此在安装 vpopmail 之前,应先安装好 MySQL 数据库服务器。

#### ① 创建 vpopmail 所需的数据库和用户

vpopmail 使用名为 vpopmail 的数据库来存储邮件服务器域和用户账户等信息。另外还要创建两个 MySQL 用户账户,账户名可任意指定,一个只有读(select)的权限,另一个有 select、insert、update、delete、create、drop 权限,权限级别为数据库级,只能对 vpopmail 数据库进行操作,创建方法为:

```
[root@rh9 root]# /usr/local/mysql/bin/mysql -u root -h localhost -p
mysql>create database vpopmail;
mysql>show databases;
mysql>grant select on vpopmail. * to vpoonlyreaduser@localhost identified by 'password';
mysql>grant select,insert,update,delete,create,drop on vpopmail. * to vpopmailuser@localhost
identified by 'yourpassword';
mysql>quit
```

**注意:** 为 vpoonlyreaduser 和 vpopmail 用户设置登录密码。这两个账户用于 vpopmail 进程对 vpopmail 数据库进行连接和操作。

#### ② 创建 vpopmail.mysql 配置文件

vpopmail 进程使用名为/home/vpopmail/etc/vpopmail.mysql 的配置文件,来提供用于连接 MySQL 数据库的登录连接信息,这些信息包括 MySQL 服务器的主机名,端口号,MySQL 用户名、密码和要访问的数据库,该配置文件的表达格式为:

```
read_MySQLServer|read port|read_user|read_password|database_name
update_MySQLServer|update port|update_user|update_password|database_name
```

MySQL 服务器与 qmail 服务器由于是安装在同一台计算机中,因此通常用 localhost 来表示。MySQL 默认使用的端口为 3306,也可直接用 0 表示,代表使用默认端口。

vpopmail, mysql 配置文件的创建方法为:

```
[root@rh9 qmail]# mkdir ~vpopmail/etc
[root@rh9 qmail]# vi ~vpopmail/etc/vpopmail, mysql
localhost 0|vpoponlyreaduser|password|vpopmail
localhost 0|vpopmailuser|yourpassword|vpopmail
```

保存并退出 vi,然后设置属主和权限。

```
[root@rh9 qmail]# chown vpopmail, vchkpw ~vpopmail/etc/vpopmail, mysql
[root@rh9 qmail]# chmod 640 ~vpopmail/etc/vpopmail, mysql
```

该配置文件在编译安装 vpopmail 之前,应事先创建好。注意该文件的权限设置,不要为其他用户分配权限,否则对 MySQL 数据库服务器有很大的安全影响。

## (2) 编译安装 vpopmail

### ① 解压并查看配置选项

```
[root@rh9 root]# cd /usr/local/src/qmail
[root@rh9 qmail]# tar -zxvf vpopmail-5.4.6.tar.gz
[root@rh9 qmail]# cd vpopmail-5.4.6
[root@rh9 vpopmail 5.4.6]# ./configure --help | less      # 查看配置功能选项
```

### ② vpopmail 配置选项简介

--enable-auth-module=mysql 用于指定如何存储 vpopmail 的账户信息。vpopmail 支持 cdb、mysql、pgsql、ldap、oracle、sysbase、oracle 等数据库。若使用 mysql 数据库来存储,则指定为 mysql。

若 MySQL 采用的是源码安装,include 头文件若没有在标准的 /usr/include/mysql 目录或 /usr/local/include/mysql 目录下,则应使用 --enable-incdir 配置项指定其路径;对于 lib 库文件,若没有在 /usr/lib/mysql 或 /usr/local/lib/mysql 目录下,则也应使用 --enable-libdir 配置项进行指定。

--enable-incdir=path 指定 MySQL 的 include 文件的安装目录路径。

--enable-libdir=path 指定 MySQL 的 lib 文件的安装目录路径。

--enable-domainquotas 激活域用户的邮箱配额管理。启动该功能后,就可使用 /home/vpopmail/domains/yourdomain.com/.qmailadmin-limits 配置文件,来对整个域中的用户的邮箱容量和允许接收的邮件数进行限制。若要禁用配额,则使用 --disable-

domain-quotas 配置项。

`--enable-mysql-limits` 使用 MySQL 的数据表(limits)存储邮箱配额信息,用以取代 `qmailadmin-limits` 配置文件。

在启用配额管理的情况下,若 `qmailadmin limits` 文件不存在,limits 数据表也没有,则使用 `~vpopmail/etc/vlimits.default` 文件指定邮箱配额信息。可编辑修改该文件,但不能删除。

`--enable-qmaildir=DIR` 指定 qmail 的控制文件(配置文件)和用户目录的安装目录,默认为 `/var/qmail`。

`--enable-vpopuser=USER` 指定运行 vpopmail 进程的用户名。

`--enable-vpopgroup=GROUP` 运行 vpopmail 进程的用户所属的用户组。

`--enable-roaming-users` 激活 POP-before-SMTP 功能,即收信后,用户才能使用邮件中继功能,向其他域的用户转发邮件。

`--enable-tcprules-prog=PATH` tcprules 程序的全路径名。默认为 `/usr/local/bin/tcprules`。

`--enable-tcpsrvr-file=PATH` 指定中继控制文件(tcp.smtp)的文件名及路径。默认为 `/home/vpopmail/etc/tcp.smtp`。

`--enable-relay-clear-minutes=#` 指定中继过期的时间。即用户在收信后的多长时间内,允许中继邮件,超过之后,将不再允许中继转发邮件。默认为 180 分钟。

`--disable-rebuild-tcpsrvr file` 禁止对 tcp.smtp.cdb 文件进行重建。

`--disable-many-domains` 对每一个虚拟域创建一个数据表来存储。默认方式是将所有虚拟域的用户信息,全部存储在一个数据表中。仅对 mysql 和 postgresSQL 数据库有效。

`--enable-valias` 在 mysql 中存储 email 别名。

`--enable-passwd` 将 `/etc/passwd(or shadow)` 中的账户添加到虚拟域中。为安全起见,qmail 的邮件账户一般不使用 Linux 系统账户,此时可使用 `--disable-passwd` 配置项。

`--enable-qmail-ext` 激活 E-mail 地址扩展支持。

`--enable-logging=OPT` 设置日志记录的级别。n 表示不记录,e 代表只记录错误日志,此为默认值,y 记录所有的操作日志,p 代表记录口令错误日志,v 代表除口令错误日志外的所有其他日志信息。

`--enable-log-name=vpopmail` 指定系统日志名,默认为 vpopmail。

`--enable-auth-logging` 激活认证日志。

`--disable-auth-logging` 关闭认证日志。

`--enable-mysql-logging` 激活 mysql 认证日志。

`--enable-learn-passwords` 激活口令学习。即对于一个账户,若没有存储对应的口令,则在第一次认证时,记住对应的口令。

`--enable-sqwebmail-pass` 存储用户口令到日用的 maildir 目录中,以供 3.0 版本以前的 sq webmail 使用。

`--enable-ip-alias-domains` 启用该选项后,若用户提供的邮件账户没有包含域名信息,则会触发一个对用户连接的服务器的 IP 地址的反向查询,如果服务器的 IP 地址能解析到一个域名,则 vpopmail 将使用那个域名作为邮件域。

### ③ 编译安装 vpopmail

`/home/vpopmail/etc` 是 vpopmail 的配置文件的目录,邮件默认域保存在 `defaultdomain` 文件中,默认邮件域的用户账户在身份认证时,可直接使用用户名,而不需要指定域名信息。下面先将 `pcnetedu.com` 设置为默认邮件域,然后再编译安装 vpopmail。

```
[root@rh9 vpopmail-5.4.6]# mkdir /home/vpopmail/etc
[root@rh9 vpopmail-5.4.6]# echo "pcnetedu.com" > /home/vpopmail/etc/defaultdomain
[root@rh9 vpopmail-5.4.6]# chown -R vpopmail.vchkpw /home/vpopmail/etc
[root@rh9 vpopmail-5.4.6]# ./configure --prefix=/home/vpopmail --enable-valias \
> --enable-auth-module=mysql --enable-incdir=/usr/local/mysql/include/mysql \
> --enable-libdir=/usr/local/mysql/lib/mysql --disable-passwd \
> --enable-vpopuser=vpopmail --enable-vpopgroup=vchkpw \
> --enable-domainquotas --disable-mysql-limits --enable-auth-logging \
> --enable-mysql-logging --enable-logging=e --enable-roaming-users \
> --enable-tcprules-prog=/usr/local/bin/tcprules --enable-relay-clear-minutes=40 \
> --enable-tcpsrvr-file=/home/vpopmail/etc/tcp.smtp \
> --disable-ip-alias-domains --enable-default-domains=pcnetedu.com
[root@rh9 vpopmail-5.4.6]# make
[root@rh9 vpopmail-5.4.6]# make install-strip
```

vpopmail 提供的对域的管理命令均存放在 `/home/vpopmail/bin` 目录中。

### (3) 创建虚拟域

vpopmail 提供了对虚拟域的创建与删除、邮件用户的创建、修改和删除等操作。

#### ① 复制 MySQL 共享库到 `/usr/lib` 目录

若 MySQL 的共享库未安装在标准的 `/usr/lib` 目录中,则在执行 `vaddomain` 命令前,应将 `libmysqlclient.so.10` 共享库复制到 `/usr/lib` 目录中,否则在运行 `vaddomain` 命令时,将出现以下错误提示信息:

```
./vaddomain: error while loading shared libraries: libmysqlclient.so.10: cannot open shared object
file: No such file or directory
```



将 libmysqlclient. so. 10 共享库复制到 /usr/lib 目录的实现命令为:

```
[root@rh9 root]# cp /usr/local/mysql/lib/mysql/libmysqlclient. so. 10 /usr/lib
```

## ② 创建与删除虚拟域

使用 vaddomain 命令创建邮件虚拟域,其命令的用法为:

```
vaddomain 域名 域管理员密码
```

域管理员密码实际上设置的是该域的 postmaster 邮件账户的密码,该账户属于管理员账户。在安装了 qmailadmin 软件包后,就可利用 postmaster 邮件账户和此处设置的密码登录,并实现对该域的管理。

比如,若要创建一个名为 pcnetedu. com 的邮件虚拟域,则创建命令为:

```
[root@rh9 root]# cd /home/vpopmail/bin
[root@rh9 bin]# ./vaddomain pcnetedu. com snbj20010814
```

执行该命令后,将在 MySQL 的 vpopmail 数据库中,自动生成 4 个数据表,其表名分别为 dir\_control、lastauth、vlog 和 vpopmail,其中 vpopmail 数据表用于存储所有邮件虚拟域的邮件账户信息。

在前面编译配置 vpopmail 时,若使用 --disable-many-domains 配置项,则每创建一个虚拟域,就会添加一个与该域对应的数据表,其表名就是域名中的小数点替换为下划线后的名称。比如创建名为 pcnetedu. com 的虚拟域,则对应的表名为 pcnetedu\_com,以后就用该数据表来存储该域的用户账户等信息。若未使用 --disable-many-domains 配置项,则将所有域的用户信息,存储在名为 vpopmail 的数据表中,在第一次创建虚拟域时,就会创建该数据表。

查看虚拟域对应的数据表的操作命令为:

```
[root@rh9 bin]# /usr/local/mysql/bin/mysql -u root -p
Enter password:
mysql>show databases;
mysql>use vpopmail;
mysql>show tables;
mysql>select * from vpopmail;          # 表中已创建出 postmaster 邮件账户
mysql>quit
```

执行添加域的命令后,还会在 ~vpopmail/domains 目录下面,创建出一个与域相同名称的文件夹,该文件夹用于存放该域的用户邮箱目录 Maildir。

若要删除指定的虚拟域,则可使用 vdeldomain 命令,其用法为“vdeldomain 域名”。

## ③ 创建与删除邮件用户

邮件虚拟域创建好后,就可使用 vadduser 命令,为域添加邮件用户。为了表达该用

户是属于哪一个域的,用户名中必须包含域名信息,即要采用“用户名@虚拟域名”的方式来表达,其命令用法为“vadduser 用户名 用户密码”。

例如,若要在 pcnetedu.com 虚拟域,创建名为 answer 和 mailmaster 的邮件账户,并设置邮箱空间限额分别为 20MB 和 50MB,则创建命令为:

```
[root@rh9 bin]# ./vadduser -q 20971520S answer@pcnetedu.com snbjkl
[root@rh9 bin]# ./vadduser -q 52428800S mailmaster@pcnetedu.com hys0814
```

执行以上命令后,将在 vpopmail 数据表中添加两条对应的记录,磁盘配额信息存储在 pw\_shell 字段中。与此同时,该命令还会在 ~vpopmail/domains/pcnetedu.com 文件夹下面创建出该用户的邮箱目录,其邮箱目录路径分别为:

```
/home/vpopmail/domains/pcnetedu.com/answer/Maildir
/home/vpopmail/domains/pcnetedu.com/mailmaster/Maildir
```

在 Maildir 目录中还会有名为 cur、new 和 tmp 的三个子文件夹,new 用于存储未读邮件;cur 存储已读邮件,tmp 用于正在传送过程中的邮件使用。Maildir 邮箱格式可保证邮件传输的安全,即使在不锁定情况下,不同邮件代理同时更新邮件,也能保证传输的可靠性。

若要删除某邮件用户,则可使用 vdeluser 命令来实现,其命令用法为:

vdeluser 用户名

修改用户账户的属性,可使用 vmoduser 命令来实现,比如若要为 mailmaster 账户设置一个描述信息,则设置方法为:

```
[root@rh9 bin]# ./vmoduser -c "for mail master." mailmaster@pcnetedu.com
```

账户的描述信息存储在 pw\_gecos 字段中。

#### (4) 设置 vchkpw 的属性和权限

设置 vchkpw 程序的属主具有读写和 s 权限,所属组和其他用户具有读和执行权限。s 权限可使用户在需要时临时具有 root 用户的权限。

```
[root@rh9 root]# chmod 4755 /home/vpopmail/bin/vchkpw
[root@rh9 root]# ll /home/vpopmail/bin/vchkpw
-rwsr-xr-x 1 vpopmail vchkpw 64684 Aug 31 13:40 /home/vpopmail/bin/vchkpw
```

#### (5) 设置邮箱容量限额与限额警告信息

##### ① 设置邮箱容量限额

对邮箱容量的配额,可通过 vpopmail 的配置文件来实现。设置默认邮箱空间的大小,以及定义整个邮件域允许使用的磁盘空间和允许的邮件消息数,可通过编辑修改配置

文件~vpopmail/etc/vlimits.default 来实现,该文件仅在.qmailadmin-limits 文件不存在时生效。

```
[root@rh9 vpopmail]# vi ~vpopmail/etc/vlimits.default
# Default limits file. This file is used for domains without a .qmailadmin-limits file.
# maximums for each account type, -1 = unlimited
maxpopaccounts      -1
maxforwards         -1
maxautoresponders   -1
maxmailinglists     -1

# quota for entire domain, in megabytes
# example shows a domain with a 100MB quota and a limit of 10000 messages
# quota              100
# maxmsgcount        10000

# default quota for newly created users (in bytes)
# example shows a user with a 10MB quota and a limit of 1000 messages
# default_quota      10485760
# default_maxmsgcount 1000
# uncomment the following lines to disable certain features
# disable_pop
# disable_imap
# disable_dialup
# disable_password_changing
# disable_external_relay
# disable_smtp
# disable_webmail
# Set bitflags on account management for non-postmaster admins.
# To disable certain features, add the following bits:
#   Create = 1, Modify = 2, Delete = 4
# So, to allow modification but not creation or deletion of
# POP/IMAP accounts, set perm_account to 5.

perm_account        0
perm_alias           0
perm_forward         0
perm_autoresponder   0
perm_maillist        0
perm_quota           0
```

```
perm_defaultquota 0
```

根据需要进行设置修改后,存盘退出 vi。该配置文件已包含了对整个邮件域的设置,因此,.qmailadmin-limits 文件通常就不再使用。

default\_quota 和 default\_maxmsgcount 配置项用于设置默认的邮箱空间大小和允许的消息数,该设置是对每一个邮件账户的,设置好该配置项后,以后所创建的新用户将自动应用该规则。默认配置文件中该配置项前面加了“#”,进行了注释,并未启用,可去掉前面的“#”来启用,并需要根据需要修改默认邮件空间的大小和允许的邮件数。启用邮件空间限额后,在用户的邮箱目录 Maildir 目录,就会增加一个 maildirsize 文件,该文件记录着该用户允许使用的磁盘空间和允许的邮件数等信息。

vpopmail 5.1.1 或以上版本,支持两种磁盘限额表达法,下面是对 1MB 的磁盘限额表达。

旧版 vpopmail 表达法: 1048576 或 1MB 或 1024KB

maildirquota 表达法: 1048576S 或 1048576S,1000C

1048576S,1000C 代表 1MB 的磁盘空间限额和 1000 封邮件的限制。maildirquota 表达法同时支持对邮件数的限制,仅 5.1.1 或以上版本才支持。

除可在配置文件中设置限额以外,另外还可利用 vmoduser -q 或 vsetuserquota 命令来设置或修改用户的邮箱容量配额。vsetuserquota 后面若指定一个具体的邮件账户,则对该账户设置配额,若指定的是一个邮件域名,则对该邮件域进行设置。

例如,现添加一个名为 webmaster@pcnetedu.com 的邮件账户,密码为 webhys,并设置邮箱容量为 20MB,允许的邮件数为 500 封,则实现的操作命令为:

```
[root@rh9 root]# ./bin/vadduser -q 20971520S,500C webmaster@pcnetedu.com webhys
[root@rh9 root]# cat /home/vpopmail/domains/pcnetedu.com/webmaster/Maildirs/maildirsize
20971520S,500C
0 0
```

另外也可使用 vsetuserquota 命令来设置,下面先创建一个测试用户,然后进行操作。

```
[root@rh9 root]# ~vpopmail/bin/vadduser test@pcnetedu.com 123
[root@rh9 root]# ~vpopmail/bin/vsetuserquota test@pcnetedu.com 20971520S,500C
[root@rh9 root]# cat ~vpopmail/domains/pcnetedu.com/test/Maildirs/maildirsize
20971520S,500C
0 0
[root@rh9 root]# ~vpopmail/bin/vdeluser test@pcnetedu.com
```

vadduser -q 常用于创建新用户时,对其进行设置,vsetuserquota 用于对已存在的用户进行设置或修改。

~vpopmail/etc/.qmailadmin-limits 文件用于对整个域允许使用的磁盘空间和允许的邮件数进行设置和限制,其创建方法为:

```
[root@rh9 vpopmail]# vi ~vpopmail/etc/.qmailadmin-limits
quota 500
maxmsgcount 2000
```

编辑好后,存盘退出 vi。quota 用于设置整个邮件域允许使用的磁盘空间,单位为 MB。

## ② 设置限额警告信息

在设置邮箱的容量限额后,默认情况下,当达到或超过限额的 90% 时,系统会自动将限额警告信息文件中的内容,发送到该用户的邮箱中。若要更改限额报警触发的邮箱容量百分比,可编辑 vdelivermail.c 源文件中的 QUOTA\_WARN\_PERCENT 变量的值,然后重新编译 vpopmail。

在 vpopmail 的源代码中有限额警告消息文件 quotawarn.msg 的样本,可将其复制成 ~vpopmail/domains/.quotawarn.msg 文件,然后根据需要进行适当的修改即可。

```
[root@rh9 root]# cd /usr/local/src/qmail/vpopmail-5.4.6
[root@rh9 vpopmail-5.4.6]# cp quotawarn.msg ~vpopmail/domains/.quotawarn.msg
[root@rh9 vpopmail-5.4.6]# chown vpopmail.vchgrp ~vpopmail/domains/.quotawarn.msg
[root@rh9 vpopmail-5.4.6]# vi ~vpopmail/domains/.quotawarn.msg
From: mailmaster@pcnetedu.com
Reply-To: mailmaster@pcnetedu.com
To: Valued Customer
Subject: Mail quota warning
Mime-Version: 1.0
Content-Type: text/plain; charset=gb2312
Content-Transfer-Encoding: base64
Your mailbox on the server is now more than 90% full. So that you can continue to receive mail you
need to remove some messages from your mailbox.
```

您的邮箱空间已经达到 90%,如果想继续使用,请删除一些信件。如果需要帮助,请联系邮箱管理员。E-mail: mailmaster@pcnetedu.com。

编辑修改好后,存盘退出 vi。另外还可添加一个邮箱已满的警告信息,对应的警告文件为 ~vpopmail/domains/.over-quota.msg,创建方法为:

```
[root@rh9 vpopmail]# vi ~vpopmail/domains/.over-quota.msg
Message rejected. Not enough storage space in your mailbox to accept message.
```

您的邮箱空间已满,邮件将被拒绝。请删除信件。

如果需要帮助,请联系邮箱管理员。E-mail: mailmaster@pcnetedu.com。

编辑修改好后,存盘退出 vi。

## 7. 编写 SMTP 和 POP3 服务启动脚本

### (1) tcpserver 命令简介

qmail 的 SMTP 和 POP3 服务,采用 tcpserver 服务管理器进行管理。tcpserver 用于接收请求的 TCP 连接,并将请求交给指定的进程处理,基本用法为:

```
tcpserver opts host port prog
```

其中,opts 参数-c 用于指定允许运行多少个 prog 子进程,默认为 40;-v 显示错误和状态消息;-x /etc/tcp.smtp.cdb 用于指定中继规则控制文件;-H 不通过 DNS 反向查询获得远程主机的主机名;-R 不查询远程主机的信息,若不指定该参数,qmail 发完信后,会试图连接客户端的 113 号端口,会使发信过程显得缓慢;-l localname 表示不通过 DNS 查询本地主机名,localname 通常设置为数字 0,即-l 0,设置使用-H -R -l 0,可加快发信过程;-u 和-g 用于设置运行指定进程的用户名和用户组。

主机名 host 若设置为 0,则代表侦听本机的所有 IP 地址。主机名也可用点分的 IP 地址来表达。

端口 port 若设置为 0,表示自动选择没有被使用的 TCP 端口,端口也通常用在/etc/services 文件中定义的端口别名来表达,比如 smtp 代表 SMTP 服务使用的 TCP 25 号端口,pop3 代表 POP3 服务所使用的 TCP 110 号端口。

prog 为要启动和管理的进程程序,程序后面可带所需的参数。

### (2) /var/qmail/rc 启动脚本

该启动脚本在前面已完成,它用于启动 qmail 邮件发送的一系列守护进程。

### (3) 编辑 smtp 服务启动脚本(/var/qmail/startsmtp)

qmail-smtpd 进程以 qmaild 用户身份运行,因此需要使用-u 和-g 参数为其指定用户名和所属的用户组,该进程用于接收用户的 SMTP 发信请求。

```
[root@rh9 root]# vi /var/qmail/startsmtp
#! /bin/sh
QMAILDUID=qmaild
NOFILESGID=nofiles
/usr/local/bin/tcpserver -H -R -t 1 -l 0 -c 80 -v -x /home/vpopmail/etc/tcp.smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 smtp /var/qmail/bin/qmail-smtpd mail.pcnetedu.com \
/home/vpopmail/bin/vchkpw /bin/truc /bin/cmd5checkpw /bin/true &
```

编辑好后存盘退出 vi。另外,在前面创建用户和用户组时,qmaild 用户的 UID 为 92,nofiles 用户组的 GID 为 91,启动 SMTP 服务的语句也可直接表达为:

```
/usr/local/bin/tcpserver -H -R -t 1 -l 0 -c 80 -v -x /home/vpopmail/etc/tcp.smtp.cdb \
-u 92 -g 91 0 smtp /var/qmail/bin/qmail-smtpd mail.pcnetedu.com \
/home/vpopmail/bin/vchkpw /bin/true /bin/cmd5checkpw /bin/true &
```

使用以上启动脚本启用 SMTP 服务后,SMTP 的连接信息将动态显示输出在屏幕上,若要让其不输出,直接记录在日志文件中,则可采用以下方式表达:

```
/usr/local/bin/tcpserver -H -R -t 1 -l 0 -c 80 -v -x /home/vpopmail/etc/tcp.smtp.cdb \
-u 92 -g 91 0 smtp /var/qmail/bin/qmail-smtpd mail.pcnetedu.com \
/home/vpopmail/bin/vchkpw /bin/true \
/bin/cmd5checkpw /bin/true 2>&1 | /var/qmail/bin/splogger smtpd 3 &
```

其中 splogger 使用 syslog 日志记录系统给日志消息打时间戳,然后将消息送往 syslog 后台服务程序,发送给 syslog 的消息拥有功能和优先级属性,syslog 按照在配置文件/etc/syslog.conf 中的定义,将消息发往指定的 log 日志文件,默认为/var/log/maillog。

利用 grep 命令在 syslog.conf 文件中查找“mail”关键字,可获得 mail 日志的存储文件。

```
[root@rh9 root]# grep mail /etc/syslog.conf
mail. * /var/log/maillog
```

#### (4) 编辑 POP3 服务启动脚本(/var/qmail/startpop3)

qmail-popup 进程用于通过网络从客户端读取用户的 pop 账户和口令,然后交给 vchkpw 进行身份验证,验证通过后,再交给 qmail-pop3d 服务进程处理,该进程负责用户邮件的具体读取和删除等操作。qmail-pop3d 由 qmail-popup 进程调用,而 qmail-popup 进程通常用 tcpserver 服务管理来管理,作为它的一个子进程来运行,因此,启动 POP3 服务的命令基本格式为:

```
tcpserver [options] qmail-popup hostname vchkpw qmail-pop3d Maildir
```

下面创建启动 qmail 的 POP3 服务的启动脚本 startpop3:

```
[root@rh9 root]# vi /var/qmail/startpop3
#!/bin/sh
/usr/local/bin/tcpserver -H -R -U -v -t 1 -c 80 0 pop3 \
/var/qmail/bin/qmail-popup mail.pcnetedu.com \
/home/vpopmail/bin/vchkpw /var/qmail/bin/qmail-pop3d Maildir 2>&1
```

#### (5) 设置启动脚本为可执行文件

```
[root@rh9 root]# chmod 755 /var/qmail/startsmtp
```

```
[root@rh9 root]# chmod 755 /var/qmail/startpop3
```

若要实现 qmail 服务器在开机时自动启动,可将这 3 个启动脚本放入/etc/rc.local 文件中。

```
[root@rh9 root]# vi /etc/rc.local
#! /bin/sh
/var/qmail/rc &
/var/qmail/startsmtp
/var/qmail/startpop3
```

#### (6) 启动 qmail 邮件服务器

依次执行以下启动脚本,启动 qmail 邮件服务器。

```
[root@rh9 root]# /var/qmail/rc &           # 启动 qmail。注意 & 不能少,以后台方式运行
[root@rh9 root]# /var/qmail/startsmtp
tcpserver: status:0/80
[root@rh9 root]# /var/qmail/startpop3
[root@rh9 root]# ps -auxw | grep qmail      # 查看 qmail 进程
```

#### (7) 测试 qmail 邮件服务器

测试有两种方法,一种方法是利用 Foxmail 或 Outlook 等客户端邮件收发软件,来测试能否正常收发邮件。另一种方法是直接利用 SMTP 和 POP 命令来测试。下面介绍利用命令来测试,这样可直接在服务器上完成测试。

SMTP 服务使用 TCP25 号端口,因此,可使用利用 telnet 去连接服务器的 25 号端口,然后通过发布相关的 SMTP 命令来进行测试。

按 Alt+F2 键切换到虚拟终端 2(tty2)进行操作,由于在启动 qmail-smtpd 进程时,使用了-v 参数,当有客户连接时,屏幕上会输出 tcpserver 的相应提示信息,这会与 telnet 的操作输出信息一起输出,因此,选择使用另一个终端来进行 telnet 的操作。

```
[root@rh9 root]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
220 mail.pcnctedu.com ESMTP
HELO localhost           # 查询服务器支持的功能
250-mail.pcnctedu.com
250-STARTTLS             # 支持 IMAP 服务器使用的 TLS(SSL)
250-PIPELINING           # 支持流水服务扩展
250 8BITMIME             # 支持全 8-bit 字符
```



```

250-AUTH LOGIN PLAIN CRAM-MD5      # 支持 PLAIN 和 CRAM-MD5 认证类型
HELO snbj                           # 以邮件用户名作参数,成功返回 250 代码
250 mail.pcnnetedu.com
MAIL FROM:snbj@pcnnetedu.com        # 指定发件人的邮件地址
250 ok
RCPT TO:webmaster@pcnnetedu.com     # 指定收件人的邮件地址
250 ok
DATA                                # 执行 DATA 命令,开始邮件内容的书写
354 go ahead
Subject: mail test.                 # 邮件主题
From:snbj                           # 指定发件人
This is a test!
.                                    # 邮件书写完毕,以小数点加回车结束
250 ok 321622537 qp 2108            # 命令执行成功,ok 之后为邮件的 ID 号
QUIT                                 # 退出并断开 SMTP 连接
221 mail.pcnnetedu.com
Connection closed by foreign host.

```

下面测试接收邮件:

```

[root@rh9 root]# telnet localhost 110
Trying 127.0.0.1...
Connected to mail.pcnnetedu.com.
Escape character is '^]'.
+OK <1969.1094395346@mail.pcnnetedu.com>
USER webmaster@pcnnetedu.com        # USER 后跟邮件账户
+OK
PASS webhys                          # PASS 后指定该账户的密码
+OK
STAT                                # 查询当前用户邮件总数和邮件总大小
+OK 1 374                            # 显示共有 1 封邮件,邮件共有 374B
LIST                                 # 显示邮件列表。将显示各邮件的序号和大小
+OK 1 messages (374 octets)
1 374
.
RETR 1                               # 接收邮件,后跟邮件序号作参数
+OK 374 octets
Received: from mail.pcnnetedu.com [61.186.170.104] by pcnnetedu.com with ESMTP

```

```
(SMTPD32-7.00) id A52D24F701B6; Tue, 07 Sep 2004 15:37:17 +0800
Received: (qmail 2640 invoked from network); 7 Sep 2004 07:38:04 -0000
Received: from unknown (HELO snbj) (127.0.0.1)
  by 0 with SMTP; 7 Sep 2004 07:38:04 -0000
Subject: mail test
from: snbj
this is a test!
X-UIDL 321622537
.
DELE 1      # 删除邮件, 以邮件序号为参数, 该命令仅给邮件作删除标记, 结束会话时才正式删
            除。若要取消删除, 可执行 RSET 命令, 该命令没有参数
+OK msg deleted
QUIT                                     # 结束会话, 断开 POP 连接
+OK
Connection closed by foreign host.
```

若邮件收发正常, 则 qmail 邮件服务器安装成功。客户端就可使用 Foxmail 或 Outlook 来收发邮件了。由于 vpopmail 支持虚拟域名, 因此用户账户应使用全名称, 即用户名后面要加上所在的域名。对于默认域的用户, 可以直接使用用户名。

## 10.4 安装 qmailadmin

qmailadmin 是一个基于 qmail 的虚拟域管理软件包, 提供了基于 Web 页面的虚拟域管理方式。在安装之前, 应先安装好 Web 服务器的 CGI 支持, vpopmail, autorespond 和 ezmlm 软件包。

### 1. 安装 autorespond

autorespond 用于实现自动回复邮件, 最新软件包为 autorespond-2.0.4.tar.gz。

```
[root@rh9 qmail]# tar -zxvf autorespond-2.0.4.tar.gz
[root@rh9 qmail]# cd autorespond-2.0.4
[root@rh9 autorespond-2.0.4]# make
[root@rh9 autorespond-2.0.4]# make install
```

### 2. 安装 ezmlm

ezmlm 用于提供用户邮件列表管理, 最新的软件包为 ezmlm-0.53.tar.gz, ezmlm-idx-0.40.tar.gz 是对 ezmlm 的一个功能扩展, ezmlm-idx-0.53.400.unified\_41.patch 是 ezmlm 的“undefined reference to 'errno'”编译错误补丁, 其安装方法为:

```
[root@rh9 qmail]# tar -zxvf ezmlm-0.53.tar.gz
[root@rh9 qmail]# tar zxvf ezmlm-idx-0.40.tar.gz # 解压补丁
[root@rh9 qmail]# cp -rf ezmlm-idx-0.40/* ezmlm-0.53/
[root@rh9 qmail]# cd ezmlm-0.53
[root@rh9 ezmlm-0.53]# patch < idx.patch
[root@rh9 ezmlm-0.53]# patch -p1 < ../ezmlm-idx-0.53.400.unified_41.patch
[root@rh9 ezmlm-0.53]# make
[root@rh9 ezmlm-0.53]# make mysql # 添加对 mysql 的支持
[root@rh9 ezmlm-0.53]# make man
[root@rh9 ezmlm-0.53]# make ch_GB
[root@rh9 ezmlm-0.53]# make setup
```

ezmlm 的可执行文件默认安装在 /usr/local/bin 目录中。

### 3. 安装与运行 qmailadmin

#### (1) 安装 qmailadmin 软件包

qmailadmin-1.2.2 支持中文语系,安装后会自动检测并使用对应的语言系统来显示管理网页。

```
[root@rh9 qmail]# tar -zxvf qmailadmin-1.2.2.tar.gz
[root@rh9 qmail]# cd qmailadmin-1.2.2
[root@rh9 qmailadmin-1.2.2]# ./configure --help | less # 获得配置选项帮助,主要看 optional 项
[root@rh9 qmailadmin-1.2.2]# ./configure --enable-htmldir=/usr/local/apache2/htdocs \
> --enable-cgibindir=/usr/local/apache2/cgi-bin --enable-qmaildir=/var/qmail \
> --enable-ezmlmdir=/usr/local/bin --enable-vpopmaildir=/home/vpopmail \
> --enable-vpopuser=vpopmail --enable-vpopgroup=vchkpw \
> --enable-maxusersperpage=15 --enable-maxaliasessperpage=15 \
> --enable-modify-quota --enable-domain-autofill --disable-help \
> --enable-ezmlm-mysql

qmailadmin 1.2.2
Current setting
```

```
-----
cgi-bin dir = /usr/local/apache2/cgi-bin
html dir = /usr/local/apache2/htdocs
image dir = /usr/local/apache2/htdocs/images/qmailadmin
image URL = /images/qmailadmin
template dir = /usr/local/share/qmailadmin
```

```

qmail dir = /var/qmail
vpopmail dir = /home/vpopmail
autorespond dir = /usr/local/bin
ezmlm dir = /usr/local/bin
ezmlm idx = no
mysql for ezmlm = yes
help = no
modify quota = yes
domain autofill = yes
modify spam check=no
[root@rh9 qmailadmin-1.2.2]# make
[root@rh9 qmailadmin 1.2.2]# make install-strip

```

qmailadmin 编译安装后,网页文件安装在/usr/local/share/qmailadmin/html 目录中,语系文件安装在/usr/local/share/qmailadmin/lang 目录中,网页所使用的图形文件安装在/usr/local/apache2/htdocs/images/qmailadmin 目录中。qmailadmin 文件安装在/usr/local/apache2/cgi-bin 目录中。

## (2) 运行 qmailadmin

qmailadmin 是一个基于 Web 页面的虚拟域管理工具。可在浏览器中使用以下地址来访问 qmailadmin 管理页面。

<http://服务器主机域名或 IP 地址/cgi-bin/qmailadmin>

在客户机的 IE 浏览器中键入 <http://mail.pcnetedu.com/cgi-bin/qmailadmin> 并回车,其登录界面如图 10.2 所示。

postmaster 是域管理员的账户名,密码就是利用 vaddomain 命令创建虚拟域时所设置的密码。输入域名称 pcnetedu.com 和域管理员的密码 snbj20010814,然后单击“登录”按钮。登录成功后,将出现图 10.3 所示的管理主界面。

单击“新建邮箱账号”链接,可实现新邮件用户的创建,其界面如图 10.4 所示。

单击“邮箱账号”链接,可显示和管理当前域的用户账户,其界面如图 10.5 所示。

由于软件是国外公司中文化的,在用语上不够准确,图 10.3 主菜单中的“邮件机器人”,实际上是指定邮件自动回复账户。

单击“新建转发”,可创建邮件转发账户,其创建界面如图 10.6 所示。



图 10.2 qmailadmin 登录界面



图 10.3 qmailadmin 管理主界面

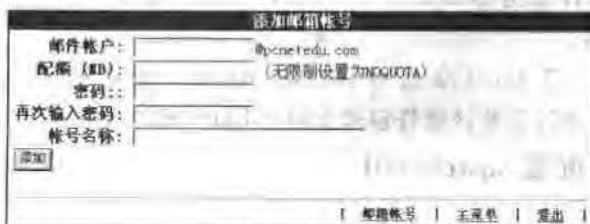


图 10.4 创建新邮件用户



图 10.5 qmailadmin 的邮件账户管理

图 10.6 创建邮件转发账号

## 10.5 安装与配置 webmail

webmail 是指 Web 界面的邮件客户端,可利用网页来实现邮件的收发。对于 qmail 邮件服务器,常用的 webmail 主要有 sqwebmail 和 igenus,前者采用 CGI 脚本实现,后者是采用 PHP 脚本实现的,它们均通过直接读写用户的邮箱目录,来实现邮件的收发。另外,通过给 qmail 邮件服务器添加安装 IMAP4 服务,也可使用 squirrelmail(小松鼠) webmail 邮件客户端。

courier-imap-3.0.7.tar.bz2 是一个支持 Maildirs 格式的 IMAP 服务器软件包, qmail 邮件服务器可通过安装该软件包来支持 IMAP4 邮件服务。

### 10.5.1 安装与配置 sqwebmail

#### 1. 安装 sqwebmail

```
[root@rh9 qmail]# tar -jxvf sqwebmail-4.0.7.tar.bz2
[root@rh9 qmail]# cd sqwebmail-4.0.7
[root@rh9 sqwebmail-4.0.7]# ./configure --help | less      # 获得配置选项帮助
[root@rh9 sqwebmail-4.0.7]# ./configure \                # 编译配置,将耗时约 12 分钟
> --without-authpwd --without-authshadow --without-authpam \
> --without-authuserdb --without-authldap --without-authdaemon \
> --with-authvchkpw --with-fcgi --with-cachedir --without-gzip \
> --enable-cgibindir=/usr/local/apache2/cgi-bin \
> --enable-imagedir=/usr/local/apache2/htdocs/webmail \
> --enable-mimetypes=/usr/local/apache2/conf \
> --enable-unicode --with-defaultlang=zh \
> --with-maxformargsize=8388608 --with-maxargsize=10485760 \
> --enable-hardtimeout=7200 --enable-softtimeout=1200
[root@rh9 sqwebmail-4.0.7]# make
[root@rh9 sqwebmail-4.0.7]# make install                # 安装 sqwebmail
```

```
[root@rh9 sqwebmail-4.0.7]# make install-configure      # 安装配置文件
```

sqwebmail 编译安装完成后,网页文件默认安装在/usr/local/share/sqwebmail/html 目录下,也可使用--prefix 配置项指定其安装的位置(PREFIX/share/sqwebmail),网页所需要的图形文件安装在/usr/local/apache2/htdocs/webmail 目录中,sqwebmail cgi 程序安装在/usr/local/apache2/cgi-bin 目录中。

配置选项说明:

--with-fcgi 带 fastcgi 支持编译 sqwebmail。

--enable-unicode 包含全部字符集。若仅指定编译包含部分字符集,可用等号列表指定,各字符集间用逗号分隔。

--with-defaultlang 指定默认语言。

--with-maxformargsize=8388608 指定利用 sqwebmail 发送邮件时,每封信允许的邮件附件大小,单位为字节,此处设置为允许上传附件 8MB。

--with-maxargsize=10485760 指定 sqwebmail 的每封邮件允许的最大容量,即附件与正文的总大小,单位为字节,此处设置为 10MB。

--enable-hardtimeout 和--enable-softtimeout 用于设置 sqwebmail 操作超时的时间,单位为秒。

## 2. sqwebmail 界面的中文化

sqwebmail 默认使用英文界面,软件包中并不包含中文界面的网页模块,在编译配置时,考虑到要使用中文界面,通过--with-defaultlang 配置项将默认语言设置为中文(zh),编译安装后,需要利用英文的网页模板,通过复制的方式产生中文界面的网页模板,然后再对这些网页模板进行中文化处理即可实现界面的中文化。

```
[root@rh9 root]# cd /usr/local/share/sqwebmail/html
[root@rh9 html]# cp -a en-us zh-cn      # 复制产生中文界面的网页模板
[root@rh9 html]# ln -s zh-cn zh        # 创建一个链接
[root@rh9 html]# cd zh-cn
```

下面对相关的配置文件进行修改,设置为中文语系。

```
[root@rh9 zh-cn]# echo cn50 zh-cn > LANGUAGE_PREF
[root@rh9 zh-cn]# echo zh_CN > LOCALE
[root@rh9 zh-cn]# echo gb2312 > CHARSET
[root@rh9 zh-cn]# echo chinese > ISPELLDICT
```

最后逐一对 zh-cn 目录下面的网页进行中文化处理即可。另外,还可对这些页面,根据需要进行样式和风格的修改,以使界面更美观。

### 3. 启动 authdaemon 守护进程

在利用网页访问 sqwebmail 页面之前,还需要启动 authdaemon 守护进程,其启动脚本文件是 /usr/local/share/sqwebmail/libexec/sqwebmaild.rc,该脚本的用法为:

启动 authdaemon 进程,实现命令: sqwebmaild.rc start

重启 authdaemon 进程,实现命令: sqwebmaild.rc reload

停止 authdaemon 进程,实现命令: sqwebmaild.rc stop

下面启动 authdaemon 守护进程:

```
[root@rh9 zh-cn]# cd /usr/local/share/sqwebmail/libexec
```

```
[root@rh9 libexec]# ./sqwebmaild.rc start
```

若不启动该服务进程,访问 sqwebmail 页面时,将出现以下错误提示信息:

Internal Error. The webmail system is temporarily unavailable. An error occured in function write:  
Transport endpoint is not connected.

### 4. 访问 sqwebmail 页面

在浏览器中键入地址 <http://mail.pcnetedu.com/cgi-bin/sqwebmail> 并回车,此时就可进入 sqwebmail 的登录界面,如图 10.7 所示。此处显示的是还未经中文化处理的英文界面。

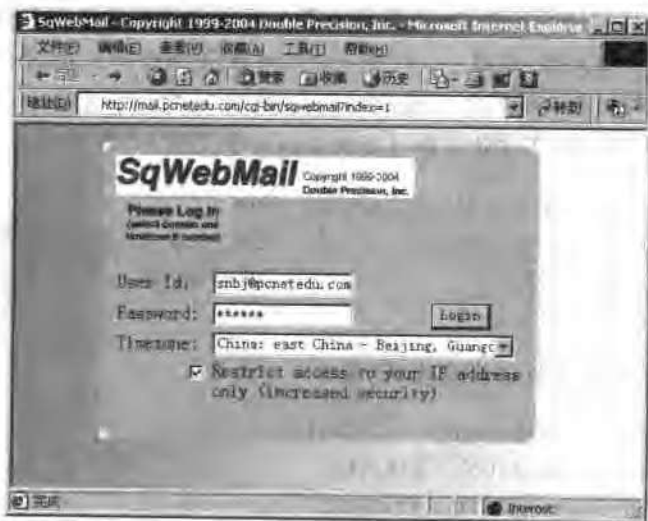


图 10.7 sqwebmail 登录界面

在登录界面中输入邮件用户账户号和密码,并选择时区,然后单击 Login 按钮,即可



进入 sqwebmail 的主界面,如图 10.8 所示。在该界面中,即可实现用户邮件的收发工作。

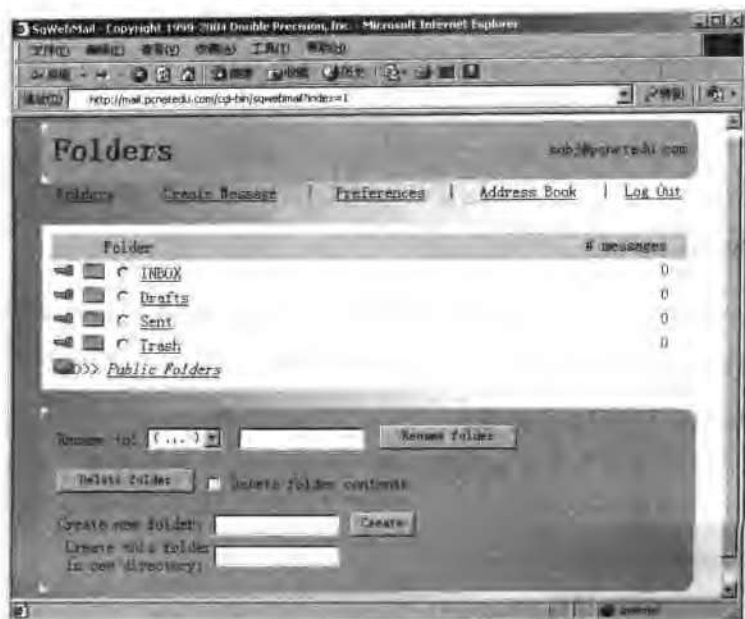


图 10.8 sqwebmail 主界面

单击 Create Message 链接,可实现新邮件的书写和发送;单击 Preferences 链接,可对当前账户属性进行设置或修改,并可修改用户的密码。

sqwebmail 默认的界面效果较差,但用户可自行编辑和修改网页模板,来美化界面。

### 5. 简化对 sqwebmail 的访问

访问 sqwebmail 时,每次都要输入较长的地址,很不方便,为此可在站点根目录下面创建一个主页文件,让其自动跳转到 sqwebmail 的访问地址。

若主页文件设置为 index.htm 或 index.html,则设置方法是在页面的<head>与</head>之间添加以下语句:

```
<meta http-equiv="refresh" content="0;URL=http://mail.pcnetedu.com/cgi-bin/sqwebmail">
```

若主页文件设置为 index.php 或 default.php,则设置方法是在该页面中添加以下脚本:

```
<? header("location:http://mail.pcnetedu.com/cgi-bin/sqwebmail"); ?>
```

设置好后,用户只需在浏览器地址栏中键入 http://mail.pcnetedu.com 就可访问了。

### 10.5.2 安装与配置 igenus

igenus 是一套基于 qmail + vpopmail + mysql 平台的邮件客户端程序,采用 PHP 脚本语言开发,采用直接读写 qmail 的 Maildir 目录结构,速度快,是很好的一个邮件客户端程序。

只需将软件包解压到运行目录,然后对 MySQL 的 vpopmail 数据库中的数据表做适当修改,并添加所需的数据表,最后配置好 Apache 服务器和 php.ini,就可正常运行了。

#### 1. 安装 igenus 软件包

```
[root@rh9 qmail]# tar -zxvf igenus_2[1].0.1_20040713_release.tgz -C /usr/local/apache2/htdocs
```

软件包中的文件将解压到 /usr/local/apache2/htdocs/igenus 目录中。

#### 2. 创建 igenus 所使用的临时目录

igenus 需要一个临时目录来存放邮件列表或邮件正文的编码等。此处将其创建在 /tmp 目录下面,其创建方法为:

```
[root@rh9 qmail]# mkdir /tmp/igenus
[root@rh9 qmail]# cd /tmp
[root@rh9 tmp]# chmod -R 0755 igenus
[root@rh9 tmp]# chown -R vpopmail:vchkpw igenus
```

#### 3. 修改 igenus 的配置文件

igenus 的配置文件位于 igenus 目录下的 config 目录中,文件名为 config\_inc.php。需要修改该配置文件,以设置 igenus 的安装目录,存取 MySQL 服务器的账户和密码信息。

```
[root@rh9 igenus]# vi ./config/config_inc.php
<? php
$CFG_BASEPATH="/usr/local/apache2/htdocs/igenus"; //指定 igenus 的安装目录
//Mysql
$CFG_MYSQL_HOST = 'localhost';           //MySQL 服务器主机名
$CFG_MYSQL_USER = 'vpopmailuser';        //设置对 vpopmail 数据库有较大操作权的用户
$CFG_MYSQL_PASS = 'yourpassword';        //设置该账户的密码
$CFG_MYSQL_DB = 'vpopmail';              //设置要存取的数据库
//vpopmail configure
$CFG_VPOPMAIL_MYSQL_LARGE_SITE=0;
//default for Language
$CFG_LANGUAGE=gb;                        //定义默认语言为中文
:
//default for web page Themes
$CFG_THEMES = "generic";                  //设置页面的风格样式
```

```

$CFG_TEMPLATE-"";
//Temp directory for maildir listing,mail body decoding etc.
$CFG_TEMP="/tmp/igenus";           //设置临时目录
$CFG_TEMP_MOD=0755;
$CFG_MAILBOX_MOD=0700;
:
$CFG_NETDISK_DEFAULT_QUOTA=10; //默认限额为 10MB
//MB
:
? >

```

#### 4. 修改 Apache 配置文件

修改 Apache 的配置文件,让 Internet 用户以 vpopmail 的用户身份运行网页,修改方法为:

```

[root@rh9 igenus]# vi /usr/local/apache2/conf/httpd.conf
:
User vpopmail
Group vchkpw
:

```

即将用户名设置为 vpopmail,用户组设置为 vchkpw。然后重新启动 Apache 服务。

```

[root@rh9 igenus]# /usr/local/apache2/bin/apachectl restart

```

#### 5. 修改 php.ini 配置文件

igenus 的 PHP 脚本使用了注册全局变量的功能,必须在 PHP 的配置文件中开启该项功能,否则 PHP 脚本将无法正常运行。其修改方法为:

```

[root@rh9 igenus]# vi /usr/local/apache2/conf/php.ini
max_execution_time=60           ;允许脚本执行的时间,单位为秒,默认为 30 秒
memory_limit=20M                ;允许脚本使用的内存空间大小,默认为 8MB
post_max_filesize=10M
file_uploads=On                 ;允许文件上传
upload_max_filesize=10M         ;默认为 2MB。允许上传文件的最大大小
register_globals = On           ;默认为 Off,将其设置为 On,允许注册全局变量
post_max_size=10M               ;默认为 8MB,更改为 10MB。PIIP 允许提交的最大数据容量
default_charset="gb2312"       ;设置默认字符集为 gb2312
session.save_path="/tmp"       ;默认未设置
session.bug_compat_42=0        ;默认为 0
session.bug_compat_warn=0      ;默认值为 1
Sendmail=/var/qmail/bin/qmail-inject;指定发送邮件的程序

```

#### 6. 修改并添加 igenus 所需的表

igenus 的脚本在 vpopmail 数据表中,使用 pw\_id 字段来标识用户的惟一性,而在原

vpopmail 数据表中没有 pw\_id 字段, 只有一个 pw\_uid 字段, 因此需要添加一个 pw\_id 字段, 并设置为主关键字段。

另外, igenus 还提供了个人通讯录(address)、名片夹(card)、收藏夹(stow)、内部通知(message)和日程安排(scheduler)、个人资料(personal)、日志记录(logs)等管理功能, 因此还需要添加一些相应的数据表, 最后还要添加一个用于管理的 admin 数据表。

#### (1) 修改 vpopmail 数据表结构, 添加 pw\_id 字段

```
[root@rh9 igenus]# 'usr/local/mysql/bin/mysql -u root -p
Enter password:
mysql> use vpopmail;
mysql> describe vpopmail;
mysql> alter table vpopmail drop primary key;
mysql> alter table vpopmail add column pw_id int(5) not null primary key auto_increment;
mysql> describe vpopmail;
mysql> quit
```

#### (2) 创建 igenus 所需要的其他 8 个数据表

在 igenus 安装目录下的 docs 目录中, 提供了一个数据表的 sql 创建脚本, 该文件名为 iGENUS.sql, 其中包含了 igenus 所需的 10 个数据表的创建脚本(包含 vpopmail 和 lastauth 数据表)。

由于 vpopmail 和 lastauth 数据表已经有了, 因此需对 iGENUS.sql 脚本文件进行编辑修改, 将 vpopmail 和 lastauth 数据表的创建脚本注释掉。为此可复制 iGENUS.sql 文件的一个拷贝来进行修改。

```
[root@rh9 igenus]# cp ./docs/iGENUS.sql /usr/local/mysql/bin/myiGENUS.sql
[root@rh9 igenus]# cd /usr/local/mysql/bin
[root@rh9 bin]# vi myiGENUS.sql
```

将创建 vpopmail 和 lastauth 数据表的 sql 语句的每一行前面加一个 #, 将其注释掉, 然后存盘退出 vi。下面利用编辑后的 sql 脚本, 通过导入的方式, 在 vpopmail 数据库中创建出所需的另外 8 个数据表。

```
[root@rh9 bin]# ./mysql -u root -psnbj20010814 vpopmail<myiGENUS.sql
```

以上语句是将 myiGENUS.sql 文件中的 sql 语句传递给 mysql 程序执行, 从而创建出所需的数据表。下面删除临时使用的 myiGENUS.sql 脚本文件。

```
[root@rh9 bin]# rm -rf myiGENUS.sql # 删除该文件
```

## 7. 访问 igenus webmail

在浏览器地址栏中输入 <http://mail.pcnetedu.com/igenus> 并回车, 此时就可进入到

igenus 的登录界面,如图 10.9 所示。登录成功后即进入到 igenus webmail 的主界面,如图 10.10 所示。



图 10.9 igenus 登录界面

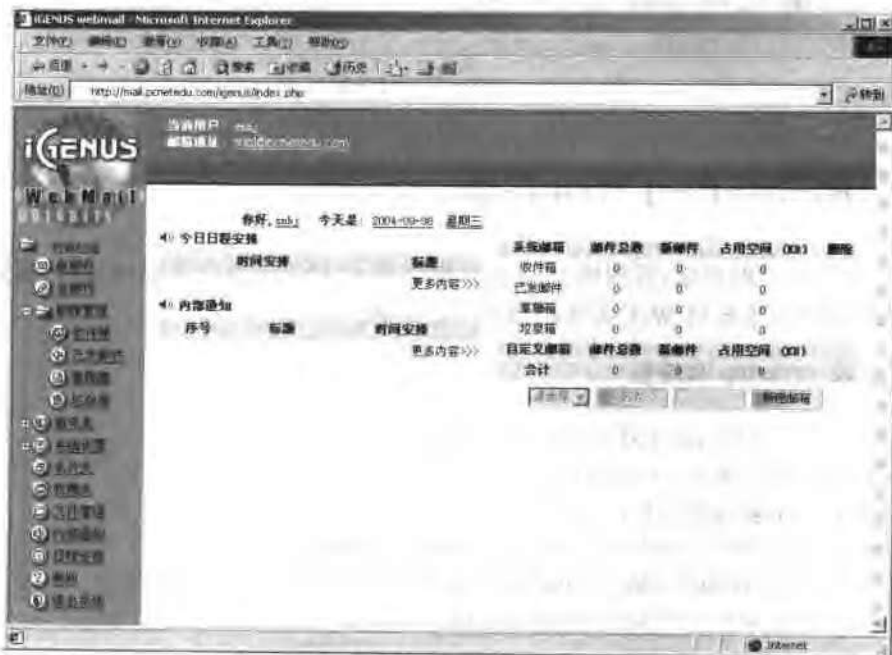


图 10.10 igenus 主界面

单击“发邮件”，此时就可编辑新邮件，其邮件编写界面如图 10.11 所示。igenus 的功能很强大，界面也很美观，推荐使用。



图 10.11 igenus 的邮件编辑界面

## 10.6 邮件账户的 Web 注册

对于邮件账户的创建，可利用 vpopmail 提供的 vadduser 命令来创建，也可通过安装 vqsignup 软件包，来提供 Web 方式的远程用户注册。

### 1. 安装 vqsignup 软件包

```
[root@rh9 qmail]# tar -zxvf vqsignup-0.5.tar.gz
[root@rh9 qmail]# cd vqsignup-0.5
[root@rh9 vqsignup-0.5]# ./configure \
> --enable-qmaildir=/var/qmail --enable-vpopuser=vpopmail \
> --enable-vpopgroup=vchkpw --enable-cgibindir=/usr/local/apache2/cgi-bin \
> --enable-htmldir=/usr/local/apache2/htdocs
```

Current settings

---

vpopmail directory = /home/vpopmail

```
uid = 89
gid = 89
cgi-bin dir = /usr/local/apache2/cgi-bin
```

Be sure to edit html/\* files, vqsignup.conf and vqsignup.html before doing make install-strip  
[root@rh9 vqsignup-0.5]# vi vqsignup.conf

修改配置文件, 设置允许用户注册邮件账户的虚拟域。

```
add_domain defaultdomain.org
add_domain test1.com
add_domain test2.com
add_domain test3.com
add_domain can.do.subdomains.too.test3.com
```

假设默认域为 pcnetedu.com, 另一个域为 pcedu.com, 则将以上配置项修改为:

```
add_domain pcnetedu.com
add_domain pcnet.com
[root@rh9 vqsignup-0.5]# vi vqsignup.html
```

在 vqsignup.html 网页文件中修改并设置可供选择的虚拟域列表。比如, 将文件中的以下内容:

```
<SELECT NAME="domain">
<OPTION VALUE="defaultdomain.org">defaultdomain.org
<OPTION VALUE="test1.com">test1.com
<OPTION VALUE="test2.com">test2.com
<OPTION VALUE="test3.com">test3.com
</SELECT>
```

修改为:

```
<SELECT NAME="domain">
<OPTION VALUE="pcnetedu.com">pcnetedu.com
<OPTION VALUE="pcnet.com">pcnet.com
</SELECT>
[root@rh9 vqsignup-0.5]# make
[root@rh9 vqsignup-0.5]# make install
```

vqsignup 编译安装后, vqsignup.html 安装在 /usr/local/apache2/htdocs 目录中, 它是 vqsignup 的首页文件, 其余文件安装在 /usr/local/apache2/cgi-bin/vqsignup 目录中, 该目录包括 html 子目录、vqsignup.conf 配置文件和 vqsignup.cgi 脚本文件。

## 2. 配置 vqsignup

vqsignup 安装后还需对配置文件和网页文件中的部分代码作相应的修改,才能正常运行。

### (1) 修改 vqsignup.html 首页文件

在编译前对该网页文件进行过修改,设置了允许用户注册邮件账户的邮件域。但在该页面的表单中,用户的注册数据默认是提交给/cgi-bin/vqsignup.cgi 脚本文件处理的,而实际上 vqsignup.cgi 文件的安装位置是/cgi-bin/vqsignup/vqsignup.cgi,因此需要对此进行修改。

将<FORM ACTION="/cgi-bin/vqsignup.cgi" METHOD="POST">更改为:

```
<FORM ACTION="/cgi-bin/vqsignup/vqsignup.cgi" METHOD="POST">
```

### (2) 修改 vqsignup.conf 配置文件

软件包在安装时,相关的网页文件是安装在/cgi-bin/vqsignup/html 目录中的。在配置文件中指定的网页文件路径,是相对于 vqsignup.cgi 脚本文件的,因此,其路径应作相应修改,其修改方法为:

```
[root@rh9 vqsignup-0.5]# cd /usr/local/apache2/cgi-bin/vqsignup
[root@rh9 vqsignup]# vi vqsignup.conf
```

将以下对网页路径的指定:

```
result_error vqsignup/html/error.html
result_failed_user vqsignup/html/failed-user.html
result_failed_pass vqsignup/html/failed-pass.html
result_failed_domain vqsignup/html/failed-domain.html
result_fields vqsignup/html/fields.html
result_domain vqsignup/html/domain.html
result_success vqsignup/html/success.html
```

更改为:

```
result_error html/error.html
result_failed_user html/failed-user.html
result_failed_pass html/failed-pass.html
result_failed_domain html/failed-domain.html
result_fields html/fields.html
result_domain html/domain.html
result_success html/success.html
```

该组配置项用于指定用户注册的每种结果,所显示的网页信息,比如用户注册若成



功,则将显示 html 目录下的 success.html 页面的内容到客户端浏览器。

另外也可直接将 vqsignup.cgi 文件从 cgi-bin/vqsignup 目录,移到 cgi-bin 目录中,这样就可省去(1)、(2)步对 vqsignup.html 和 vqsignup.conf 文件中关于 vqsignup.cgi 文件路径的修改。

### (3) 修改 html 目录下的网页文件,设置允许注册的邮件域

vqsignup 的网页文件安装在/usr/local/apache2/cgi-bin/vqsignup/html 目录中,利用 vi 分别修改 domain.html、failed-domain.html、failed-user.html 和 fields.html 文件,设置允许用户注册的虚拟邮件域。修改方法与对 vqsignup.html 文件的修改相同。

## 3. 运行 vqsignup,测试用户注册

在浏览器地址栏中输入 <http://mail.pcnetedu.com/vqsignup.html> 并回车,此时就可显示出用户注册页面,如图 10.12 所示。

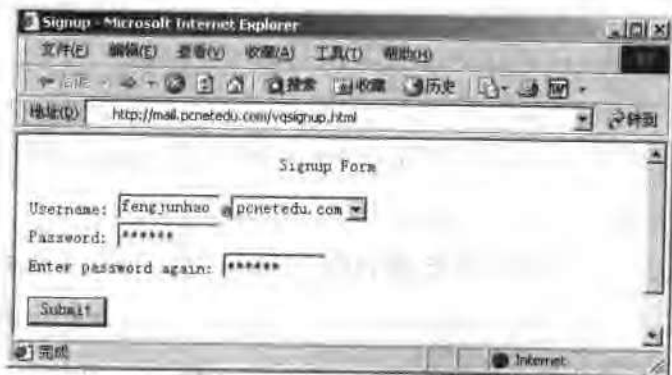


图 10.12 vqsignup 的用户注册界面

该软件包功能较单一,仅实现用户的远程在线注册。对于邮件管理员,可使用 qmailadmin 来对邮件账户进行管理。

用户邮件注册功能,可在 webmail 的登录界面中做一个链接,用户通过单击该链接,就可实现邮件账户的注册申请。另外,若要有条件地开放邮件注册功能,可编辑修改网页,添加相关的控制脚本来实现。

## 10.7 qmail 服务进程的管理

对 qmail 服务进程的管理,可借助 daemontools 守护进程管理工具来实现。daemontools 是一个服务监控程序,可用来监控 qmail-send、qmail-smtpd 和 qmail-pop3d 服务进程,从而实现对 qmail 的所有相关进程的统一管理,更方便地实现对 qmail 服务进

程的启动、重启和停止等操作。

### 1. 安装 daemontools 软件包

```
[root@rh9 qmail]# mkdir /package
[root@rh9 qmail]# chmod 1755 /package
[root@rh9 qmail]# tar -zxvf daemontools-0.76.tar.gz -C /package
[root@rh9 qmail]# cp daemontools-0.76.errno.patch /package
[root@rh9 qmail]# cd /package
[root@rh9 package]# mv admin/daemontools-0.76/ daemontools-0.76
[root@rh9 package]# rmdir admin/
[root@rh9 package]# patch -p0 < daemontools-0.76.errno.patch
[root@rh9 package]# cd daemontools-0.76/
[root@rh9 daemontools-0.76]# ./package/install      #编译安装 daemontools
[root@rh9 daemontools-0.76]# cd ..
[root@rh9 package]# rm daemontools-0.76.errno.patch
```

编译安装后,将会创建/service 目录。要检查 daemontools 软件包是否安装成功,可通过检查 svscan 进程是否在运行来确定,svscan 是后台服务器的管理服务程序。

```
[root@rh9 package]# ps -auxw | grep svscan
```

若有 svscan /service 进程在运行,则说明 daemontools 软件包安装成功。

```
[root@rh9 package]# mkdir /var/run/qmail      #创建 daemontools 进程号文件存放目录
```

daemontools 的可执行文件安装在/usr/local/bin 目录中,可使用 svc 命令来启动 qmail 进程,使用 svtat 监视 qmail 的运行状态。下面利用 daemontools 提供的命令,通过编写控制脚本,来实现 qmail 相关进程的统一启动或停止。

### 2. 创建 qmail 服务的启动脚本

qmail 服务的完整启动脚本和相关文件可到作者主页(<http://www.pcnetedu.com>)下载,脚本包文件名为 qmail-scripts.tar.gz。

(1) 解压 qmail 启动脚本软件包

```
[root@rh9 qmail]# tar -zxvf qmail-scripts.tar.gz
```

(2) 将原/var/qmail/rc 文件更名为 rc\_hak,以作备份

```
[root@rh9 qmail]# mv /var/qmail/rc /var/qmail/rc_bak
```

(3) 建立 supervise 脚本

为 qmail 的服务进程创建 supervise 目录。

```
[root@rh9 qmail] # mkdir -p /var/qmail/supervise/qmail-send/log
[root@rh9 qmail] # mkdir -p /var/qmail/supervise/qmail-smtpd/log
[root@rh9 qmail] # mkdir -p /var/qmail/supervise/qmail-pop3d/log
[root@rh9 qmail] # mkdir -p /var/qmail/supervise/qmail-pop3ds/log
[root@rh9 qmail] # chmod +t /var/qmail/supervise/qmail-send
[root@rh9 qmail] # chmod +t /var/qmail/supervise/qmail-smtpd
[root@rh9 qmail] # chmod +t /var/qmail/supervise/qmail-pop3d/log
[root@rh9 qmail] # chmod +t /var/qmail/supervise/qmail-pop3ds/log
```

复制相关的脚本文件到对应的目录中。

```
[root@rh9 qmail] # cp qmail-scripts/send.run /var/qmail/supervise/qmail-send/run
[root@rh9 qmail] # cp qmail-scripts/send.log.run /var/qmail/supervise/qmail-send/log/run
[root@rh9 qmail] # cp qmail-scripts/smtpd.run /var/qmail/supervise/qmail-smtpd/run
[root@rh9 qmail] # cp qmail-scripts/smtpd.log.run /var/qmail/supervise/qmail-smtpd/log/run
[root@rh9 qmail] # cp qmail-scripts/pop3d.run /var/qmail/supervise/qmail-pop3d/run
[root@rh9 qmail] # cp qmail-scripts/pop3d.log.run /var/qmail/supervise/qmail-pop3d/log/run
[root@rh9 qmail] # cp qmail-scripts/pop3ds.run /var/qmail/supervise/qmail-pop3ds/run
[root@rh9 qmail] # cp qmail-scripts/pop3ds.log.run /var/qmail/supervise/qmail-pop3ds/log/run
```

若邮件服务器的主机名不是“mail.pcnetedu.com”，则应修改/var/qmail/supervise/qmail-pop3d/run 文件，并将其中的“mail.pcnetedu.com”替换为邮件服务器实际的主机名。

设置各 run 脚本为可执行文件。

```
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-send/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-send/log/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-smtpd/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-smtpd/log/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-pop3d/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-pop3d/log/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-pop3ds/run
[root@rh9 qmail] # chmod 755 /var/qmail/supervise/qmail-pop3ds/log/run
```

创建存储 qmail 相关日志的目录。

```
[root@rh9 qmail] # mkdir -p /var/log/qmail/smtpd
[root@rh9 qmail] # mkdir -p /var/log/qmail/pop3d
[root@rh9 qmail] # mkdir -p /var/log/qmail/pop3ds
[root@rh9 qmail] # chown -R qmail /var/log/qmail
```

(4) qmailctl 与 vpopmailctl 启动脚本

qmailctl 脚本用于启动、重启、暂停或停止 qmail-send 和 qmail-smtpd 服务进程。相

当于以前的 rc 和 startsmtp 脚本的启动功能,但以前的脚本只能启动服务,没有停止和重启服务的控制功能。vpopmailctl 脚本用于启动、重启、暂停或停止 qmail-pop3d 和 qmail-pop3ds 服务进程。

将 qmail-scripts 目录中的 qmailctl 和 vpopmailctl 脚本复制到 /var/qmail/bin 目录中。将 rc 复制到 /var/qmail 目录中。

```
[root@rh9 qmail]# cd qmail-scripts
[root@rh9 qmail-scripts]# cp qmailctl vpopmailctl /var/qmail/bin/
```

下面将邮箱格式保存到 defaultdeliver 文件中,供 /var/qmail/rc 文件调用,其调用语句是:

```
qmail-start "cat /var/qmail/control/defaultdelivery"
[root@rh9 qmail-scripts]# echo ./Maildir/ > /var/qmail/control/defaultdelivery
[root@rh9 qmail-scripts]# cp rc /var/qmail/          # 复制新的 rc 文件到 /var/qmail 目录
```

另外也可不进行以上两步操作,而直接将原来 rc 文件中的 qmail-start 语句修改为:

```
qmail-start ./Maildir/
```

即去掉原语句中的 splogger qmail,在此处日志采用 daemontools 提供的 multilog 实用程序来处理,因此就不再需要原来的 syslog 日志记录了。

下面设置最大并行 SMTP 连接数,将该连接数保存在 concurrencyincoming 文件中,主要是便于以后更改该设置值。该文件中的值,将通过以下方式,最终传递给 tcpserver 程序的 -c 参数,并作为 -c 参数的设置值。

```
MAXSMTPD='cat /var/qmail/control/concurrencyincoming'
tcpserver -c "$MAXSMTPD"
[root@rh9 qmail-scripts]# echo 80 > /var/qmail/control/concurrencyincoming
[root@rh9 qmail-scripts]# chmod 644 /var/qmail/control/concurrencyincoming
[root@rh9 qmail-scripts]# chmod 755 /var/qmail/rc
[root@rh9 qmail-scripts]# chmod 755 /var/qmail/bin/qmailctl
[root@rh9 qmail-scripts]# chmod 755 /var/qmail/bin/vpopmailctl
```

下面创建 supervise 目录到 /service 目录的链接,建立该链接后,qmail 的相关进程就会立即被启动,从而利用 daemontools 来启动和管理 qmail-send、qmail-smtpd、qmail-pop3d 和 qmail-pop3ds 等服务进程。svscan 会自动运行 /service 下面的脚本。

```
[root@rh9 qmail-scripts]# cd ..
[root@rh9 qmail]# ln -s /var/qmail/supervise/qmail-send /service
[root@rh9 qmail]# ln -s /var/qmail/supervise/qmail-smtpd /service
```

```
[root@rh9 qmail]# ln -s /var/qmail/supervise/qmail-pop3d /service
[root@rh9 qmail]# ln -s /var/qmail/supervise/qmail-pop3ds /service
```

qmailctl 与 vpopmailctl 脚本的使用方法:

```
[root@rh9 qmail]# ./bin/qmailctl {start|stop|restart|reload|stat|pause}
```

reload 表示重新读取加载 locals 配置文件中的内容。

```
[root@rh9 qmail]# ./bin/vpopmailctl {start|stop|restart|stat|pause}
```

例如,若要停止 qmail 的全部服务进程,则实现操作为:

```
[root@rh9 qmail]# ./bin/qmailctl stop
[root@rh9 qmail]# ./bin/vpopmailctl stop
```

若要再次重新启动 qmail 的全部服务进程,则实现操作为:

```
[root@rh9 qmail]# ./bin/qmailctl start
[root@rh9 qmail]# ./bin/vpopmailctl start
```

最后为使用方便,可给 qmailctl 和 vpopmailctl 在 /usr/bin 目录中创建一个链接。

```
[root@rh9 qmail]# ln -s /var/qmail/bin/qmailctl /usr/bin
[root@rh9 qmail]# ln -s /var/qmail/bin/vpopmailctl /usr/bin
```

### 3. qmail 完整服务的启动

使用 daemontools 管理后,qmail 相关的所有进程在 Linux 系统开机启动时,就会自动被启动。若要暂时停止或暂停或手工启动 qmail 服务,则可利用 qmailctl 和 vpopmailctl 脚本来进行控制了。qmail 服务自动启动后的服务进程如图 10.13 所示。

### 4. daemontools 的日志管理

daemontools 提供了一个用于日志管理的 multilog 实用程序,该程序用于将日志记录到指定目录下的 current 文件中。存储日志的目录通过 multilog 命令行的 t 参数指定。

一个标准的 multilog 日志记录如下所示:

```
@400000004140a33f087a6edc starting delivery 2: msg 150115 to local snbj@pcnetedu.com
```

其中的“@400000004140a33f087a6edc”为 TAI (Temps Atomique International) 时间戳,可利用 daemontools 提供的另一个名为 tai64nlocal 的命令,将其转换为当地易读的时间戳。后面部分是记录的日志消息。

### 5. qmail 的日志分析

对 qmail 日志的分析,可使用 qmailanalog 日志文件分析工具来实现。该分析工具可

```

root@rh9:~# ps -auxw | grep qmail
root      [1895]  0.0  0.0 1344  48 ?        S    08:06   0:00 supervise qmail-send
root      1897  0.0  0.0 1344  48 ?        S    08:06   0:00 supervise qmail-smtpd
root      1899  0.0  0.0 1344  48 ?        S    08:06   0:00 supervise qmail-pop3d
root      1901  0.0  0.0 1344  48 ?        S    08:06   0:00 supervise qmail-pop3ds
qmail    1905  0.0  0.0 1356  60 ?        S    08:06   0:00 multilog t /var/log/qmail
/pop3d
qmail    1907  0.0  0.0 1356  60 ?        S    08:06   0:00 /usr/local/bin/multilog t
/var/log/qmail
qmail    1910  0.0  0.0 1360  64 ?        S    08:06   0:00 multilog t /var/log/qmail
/pop3ds
qmail    1913  0.0  0.0 1356  60 ?        S    08:06   0:00 /usr/local/bin/multilog t
/var/log/qmail/smtpd
qmail    2111  0.0  0.0 1396 100 ?        S    08:23   0:00 [qmail-send]
root      2113  0.0  0.0 1416  80 ?        S    08:23   0:00 /usr/local/bin/tcpserver
-v -H -R -t 1 -l 0 -x /etc/tcp.smtp.cdb -c 80 -u qmaild -g nofiles 0 smtp /var/qmail/bin
/qmail-smtpd /home/vpopmail/bin/vchkpw /bin/true /bin/crond5checkpw /bin/true
root      2116  0.0  0.0 1372  76 ?        S    08:23   0:00 qmail-lspawn ./Maildir/
qmailr    2117  0.0  0.0 1372  80 ?        S    08:23   0:00 [qmail-lspawn]
qmailq    2118  0.0  0.0 1352  60 ?        S    08:23   0:00 [qmail-clean]
root      2236  0.0  0.4 4444 628 pts/0    S    08:27   0:00 grep qmail
root@rh9:~#

```

图 10.13 qmail 正常运行的服务进程

处理 qmail 的日志并生成一系列的报告,其报告可指示出系统正在工作的类型和工作量。比如统计发送和接收的邮件数以及邮件的大小等。其源代码软件包下载地址为:

<http://cr.yip.to/software/qmailanalog-0.70.tar.gz>

## 10.8 qmail 的配置文

qmail 的配置文件也称为控制文件,由许多文件组成,不是集中在一个文件中的。每个进程有自己的控制文件,而且每个进程通常还有多个配置文件,每个配置文件控制相应的功能,所有的配置文件共同决定 qmail 的运行,这些配置文件位于 `/var/qmail/control` 目录中。下面按所属的进程,分别介绍这些配置文件的功能与配置方法。

### 1. 配置文件 me

该配置文件是 qmail 系统的一个十分重要的文件,若该文件不存在, qmail 系统将无法正常运行。配置文件 me 是在 qmail 安装时,使用 `configure-fast` 来创建的。

me 配置文件用来定义本地邮件服务器的主机名。qmail 进程的配置文件,很多都是与 me 有关的,若那些配置文件不存在,系统就会默认从 me 配置文件中读取。

### 2. qmail-smtpd 进程的配置文件

#### (1) badmailfrom

该配置文件用于设置拒绝接收的邮件地址和邮件域,即设置 From 地址黑名单。当

一个邮件地址或邮件域被列入该文件后,从这个地址或这个域下的所有邮件地址发来的邮件,系统就会拒绝接收,从而可以在一定程度上,起到防垃圾邮件的作用。

比如,若要拒绝从 `trueName@263.com` 和 `@163.com` 邮件域发来的邮件,则可在该文件中放入以下内容即可。

```
[root@rh9 root]# vi /var/qmail/control/badmailfrom
trueName@263.com
@163.com
```

编辑好后,存盘退出 `vi`。以后凡是邮件域为 `163.com` 发来的邮件,都将被 `qmail` 服务器拒绝接收。

#### (2) `databytes`

该文件用于定义 `qmail-smtpd` 允许接收的邮件的最大字节数。默认值为 0,表示对要发送的邮件大小没有限制。

若要设置允许发送的邮件的大小最大为 10MB,则设置方法为:

```
[root@rh9 root]# echo 10485760 > /var/qmail/control/databytes
```

以后任何大于 10MB 的邮件都会被拒绝,这样可避免恶意用户利用该邮件服务器发送大量的超大邮件,而使邮件服务器负荷过重,造成系统崩溃。

#### (3) `rcpthosts` 与 `morercpthosts`

该文件用于设置本邮件服务器允许转发邮件的邮件域或主机名,只有这些域的用户或指定主机所发送的邮件,服务器才会对其进行邮件转发。若该文件不存在,则将转发所有用户的邮件。

该配置文件最多可以设置 50 个主机名和域名,若要设置的域或主机数目超出这个值,则应将其他域名主机名保存到扩充配置文件 `morercpthosts` 中,并使用 `qmail-newmrh` 命令程序,生成 `morercpthosts.cdb` 文件,这样 `qmail-smtpd` 才能从这个文件中读取到该设置。

#### (4) `timeoutsmtpd`

用于设置 SMTP 客户端超时的秒数,默认为 1200 秒。

#### (5) `smtpgreeting`

用于设置 SMTP 问候信息。

### 3. `qmail-send` 进程的配置文件

#### (1) `bouncefrom` 与 `bouncehost`

该文件用于设置反弹邮件的发送者用户名,即当用户的邮件投递失败时,系统自动将该信返回给发送者时,所显示的邮件发送者用户名。若不存在该文件,则默认的发送者为

## MAILER-DAEMON。

bouncehost 用于设置反弹邮件发送者的主机名。若不存在,则默认从 me 中读取。

### (2) doublebounceto 与 doublebouncehost

该文件用于设置接收双重反弹邮件的用户,默认为 postmaster。当用户发送一封邮件时,若邮件发送失败,则服务器会自动反弹发送一封邮件给原发信者,若此时该反弹邮件发送也失败了,则会再反弹(此时属于第 2 次反弹)发送一封邮件给 doublebounceto 配置文件所设置的邮件用户,一般是管理员的地址。当该文件不存在时,默认发送给 postmaster。

利用双重邮件反弹技术,可检查发信者的邮件地址的真实性。服务器在正式转发邮件之前,可反弹一封邮件给发信者,若发送失败(此时会有 2 次反弹邮件),则说明该地址是伪造的,则拒绝发送该邮件,从而可在一定程度上防止发送垃圾邮件。

doublebouncehost 用于设置当出现“双重反弹”时,所发送的反弹邮件的主机名和双重反弹的发送者,默认为 me。

### (3) concurrencylocal 与 concurrencyremote

concurrencylocal 用于设置允许同时投递的本地邮件个数,即设置并发的 qmail-local 进程的数目,默认值为 10;concurrencyremote 用于设置允许同时投递的远端邮件(非本地域)的个数,即设置并发的 qmail-remote 进程的数目,默认值为 20,若要设置为 255,则设置方法为:

```
[root@rh9 root]# echo 255 > /var/qmail/control/concurrencyremote
[root@rh9 root]# chmod 644 /var/qmail/control/concurrencyremote
```

### (4) locals

用于设置进行本地邮件投递的邮件域。在 qmail-send 处理邮件投递时,将会使用该文件中的域,与邮件的目标地址进行比较,若相同,则将该邮件交给 qmail-lspawn 进程处理,投递到本地邮件域;若不同,则将邮件交给 qmail-rspawn 进程处理,将其投递给远程的目标邮件服务器。若该文件不存在,则从配置文件 me 中读取,若 me 不存在,qmail-send 将无法正常工作。

### (5) queuelifetime

用于设置邮件在队列内可保留的秒数,默认为 604800 秒,即 7 天。该期限到了后,qmail-send 会进行最后一次的投递尝试,若投递失败,则交给 qmail-clean 进程,从邮件队列中清除。

### (6) virtualdomains

用于设置虚拟邮件域。当创建一个虚拟邮件域时,会自动将该域添加到该文件中。



#### (7) envnoathost

用于设置缺少@符号的邮件地址所使用的默认域名。若该文件不存在,默认使用 me 文件中的域名。

#### (8) percenthack

用于指定可以使用%模式发信的邮件域。即邮件地址中的@使用%替代表示。

### 4. qmail-inject 进程的配置文件

qmail-inject 进程用于处理本地邮件的投递,其配置文件也是针对本地邮件的。

#### (1) defaultdomain

用于设置默认域名。当给本地域的另一用户发送邮件时,若仅指定了用户名,则会自动在该用户名后添加上 defaultdomain 文件中指定的域名,作为该邮件的完整地址,并按该地址进行投递。对于默认域中的用户,在收邮件时,只需输入用户名即可,其他域中的用户在登录时,必须使用“用户名@域名”作为邮件账户。

当 defaultdomain 文件不存在时,可以从配置文件 me 中读取。若环境变量 QMAILDEFAULTDOMAIN 已被设置,则 defaultdomain 配置文件将被忽略。

#### (2) defaulthost

该文件用于定义默认主机名,当邮件系统收到没有指定目标主机名的邮件时,将采用该设置。若环境变量 QMAILDEFAULTHOST 已被设置,则 defaulthost 配置文件将被忽略。

#### (3) idhost

用于定义在 Message-ID 中使用的主机名。若不存在,则默认从 me 中读取。

### 5. qmail-remote 进程配置文件

#### (1) helohost

用于设置在 SMTP HELLO 命令中使用的主机名,即 qmail-remote 进程在与其他远程邮件服务器建立连接时所使用的本机名。若文件不存在,则从 me 配置文件中读取。

#### (2) smtproutes

该配置文件用于设置静态的 SMTP 路由信息,其格式为:

```
HOST:TARGET_HOST
```

HOST 可以是主机名或域名,若缺省则代表任意的主机或邮件域。该路由信息是将所有目标是 HOST 的邮件转发给 TARGET\_HOST 邮件服务器。

#### (3) timeoutconnect

用于设置 SMTP 连接超时的秒数,默认为 60 秒。

#### (4) timeoutremote

用于设置 qmail-remote 进程等待远端服务器响应的最大时间,默认为 1200 秒。若到

时没有响应,则将断开与对方的连接,并将失败记录到日志文件中。

## 10.9 qmail 防病毒与反垃圾邮件

目前带毒邮件和泛滥的垃圾邮件,已成为邮件用户最为头痛的事,据公安部 2004 年 9 月份公布的全国信息网络安全调查结果,中国计算机用户病毒感染率 87.9%,垃圾邮件是祸首,因大规模垃圾邮件传播病毒造成的安全事件占 36%,因此,邮件服务器具备防病毒和反垃圾邮件的功能,就显得尤为重要。

### 1. qmail 防病毒与反垃圾邮件简介

#### (1) qmail 防病毒简介

目前邮件服务器反病毒扫描的实现原理一般是使用防病毒的 SMTP 网关,替代原来的 SMTP 服务,然后将经病毒扫描检查后的信件,再转交给原来的 SMTP 服务进程实现发信。H+BEDV 公司提供有反病毒的邮件服务器网关产品。

qmail 邮件服务器通常使用 qmail-scanner 和一种基于 UNIX 的杀毒软件和垃圾邮件检测软件相结合,来实现防病毒和反垃圾邮件。

qmail-scanner 是专门针对 qmail 邮件服务器而设计的一个扫描器,它使用 qmail-scanner-queue.pl 替代接管 qmail 的 qmail-queue 服务进程,从而实现对进入发送队列的邮件进行病毒和垃圾邮件的扫描检查,经杀毒和垃圾邮件过滤处理后的正常邮件,再转交给 qmail 原来的 qmail-queue 服务进程处理。从中可见,这种实现方式,实际上是在 qmail 原工作流程的 qmail-queue 之前,增加了一道防病毒和反垃圾邮件的网关。

qmail-scanner 软件包目前的最新版是 1.23,可从 <http://qmail-scanner.sourceforge.net> 网站下载。qmail-scanner 还需要结合使用一种支持 qmail-scanner 的 UNIX 杀毒软件,其支持的杀毒软件和反垃圾邮件软件有:

- Trend's InterScan VirusWall Virus scanner
- Sophos's "sweep" virus scanner
- H+BEDV's antivir scanner
- Kaspersky's AVPLinux scanner
- MacAfee's (NAI's) virus scanner
- Command's virus scanner
- F-Secure Anti-Virus scanner
- F-Prot Anti-Virus scanner
- InocuLAN Anti-Virus scanner
- BitDefender Linux Edition
- Central Command's Vexira antivirus scanner

- Clam Antivirus - an Open Source antivirus scanner
- Sophie; Daemon front-end to Sophos Sweep
- Trophie; Daemon front-end to Trend iscan
- Spam Assassin Daemon

## (2) qmail 反垃圾邮件简介

目前对抗垃圾邮件主要采用邮件过滤技术(Mail Filter),其实现方式主要有两种:一种是根据设置的规则或实时黑名单,直接拒收或拒绝发送垃圾邮件;另一种是先将邮件接收下来,然后再实施过滤。二者相比较,前一种方案具有更高的效率,对邮件直接拒收/拒发,减轻了服务器的负荷,但是容易“殃及无辜”,使部分正常的邮件丢失。后一种方案虽然效率上差一些,但可减少出错机率,对邮件的过滤通常由专门的过滤软件来实现,一般是通过设置规则,对邮件头进行检查来过滤邮件。

Spam Assassin Daemon 就是一款较为出色的垃圾邮件过滤软件,可与 qmail-scanner 结合使用,实现对垃圾邮件的检查和过滤,是 qmail 反垃圾邮件的较好选择。

Spam Assassin 引入了以可能性为尺度的新型计分方法来分类处理邮件,而不是简单地接收或拒收邮件,从而有效降低正常邮件的丢失率。其工作原理是:对一封信件应用各项规则之后,生成一个综合分值来表示其为垃圾邮件的可能性。如果分值为负,表示这封信件是正常的;若分值为正,则表示信件有问题;如果超过了默认的或预设定的分值,过滤器就会标识该邮件为垃圾邮件,然后交由用户做出最终抉择。

Spam Assassin 预设了上百条规则,包括对邮件头的处理、对邮件内容的处理及对邮件结构的处理等,每条规则都对应一个分值(可正、可负),每封信件的分值就是所匹配规则的分值之和。另外,Spam Assassin 还可自动“学习”垃圾邮件的特点,来提高垃圾邮件的识别能力。

## 2. qmail-scanner 的使用要求

要安装使用 qmail-scanner, qmail 服务器必须满足以下几个条件:

① 对于 qmail 1.03 必须打 qmailqueue-patch 补丁。该补丁使 qmail-queue 允许病毒扫描和反垃圾邮件软件扫描队列,并允许使用 QMAILQUEUE 环境变量来指定所使用的 qmail 队列进程程序,以便用以替代默认的 qmail-queue 队列进程。

在前面安装 qmail 时所打的补丁集中已包含了 qmailqueue 补丁,此处不再需要安装。

② 安装 Maildrop 1.3.8 及以上版本。

③ 必须安装 Perl 解释器。qmail-scanner-queue.pl 是一个 Perl 脚本,因此必须安装 Perl。一般 Linux 在安装时就已安装了 perl 5.8.0-88,可利用“rpm -q perl”命令查看是否安装。若未安装,可在第 1 张安装光盘找到 perl-5.8.0-88.i386.rpm 来安装。

④ Perl 的 Time::HiRes 模块。模块文件名为 HiRes.pm。

⑤ Perl 的 DB\_File 和 Sys::Syslog 模块。Sys::Syslog 模块在安装 Perl 时一般会预

安装,模块文件名为 Syslog.pm。DB\_File 模块不会预安装,该模块的文件名为 DB\_File.pm。

⑥ perl-suidperl 模块。

⑦ TNEF 软件包。该软件包支持将封装成 TNEF 的邮件附件提取出来加以分析。TNEF 是微软系统的邮件附件(application/ms-tnef)类型。

### 3. 准备相关软件包

① 从 <http://qmail-scanner.sourceforge.net> 网站下载 qmail-scanner-1.23.tgz 软件包。补丁下载地址为:

<http://xoomer.virgilio.it/j.torihio/qmail-scanner/download/q-s-1.23st-20040819.patch.gz>

② clamav 反病毒软件官方网站为 <http://www.clamav.net>, 0.75 版本的下载地址为:

<http://optusnet.dl.sourceforge.net/sourceforge/clamav/clamav-0.75.1.tar.gz>

③ H+BEDV 反病毒软件的官方网站为:

<http://www.hbedv.com/en>

<http://www.antivir.de/en>

<http://www.hbedv.com/files/antivir/release/av\xsrv.tgz>

<http://www.hbedv.com/private/>

<ftp://mail.redhut.net/linux/hbedv.key>

④ Maildrop 邮件过滤软件包下载地址为:

<http://www.courier-mta.org/download.php> # maildrop 或 <http://download.sourceforge.net/courier/maildrop-1.7.0.tar.bz2>

⑤ TNEF 软件包下载地址为 <http://sourceforge.net/projects/tnef/>, 最新的 1.2.3.1 下载地址为:

<http://optusnet.dl.sourceforge.net/sourceforge/tnef/tnef-1.2.3.1.tar.gz>

⑥ perl 的 DB\_File、Time::HiRes 和 perl-suidperl 模块在 Red Hat Linux 的第 2 张安装光盘中有相应的 rpm 安装包,其文件名分别为:

perl-DB\_File-1.804-88.i386.rpm

perl-Time-HiRes-1.38-3.i386.rpm

perl-suidperl-5.8.0-88.i386.rpm

⑦ Spam Assassin 的官方网站为 <http://spamassassin.apache.org>。软件包下载地址为:

<http://spamassassin.apache.org/downloads.html>

<http://old.spamassassin.org/released/Mail-SpamAssassin-2.64.tar.gz>

<http://spamassassin.apache.org/released/Mail-SpamAssassin-3.0.0-rc4.tar.gz>

#### 4. 安装 maildrop 软件包

maildrop 用于实现邮件过滤器,更详细的内容可参阅 <http://www.courier-mta.org/maildrop/>。

```
[root@rh9 root]# cd /usr/local/src/qmail
[root@rh9 qmail]# tar -jxvf maildrop-1.7.0.tar.bz2
[root@rh9 qmail]# cd maildrop-1.7.0
[root@rh9 maildrop-1.7.0]# ./configure --enable-maildrop-uid=vpopmail \
>--enable-maildrop-gid=vchkpw --enable-userdb --enable-syslog=1
[root@rh9 maildrop-1.7.0]# make
[root@rh9 maildrop-1.7.0]# make install-strip
[root@rh9 maildrop-1.7.0]# make install-man
```

编译安装后,其可执行文件(maildrop、maildirmake、mailbot)位于/usr/local/bin 目录中。

#### 5. 安装 TNEF 软件包

```
[root@rh9 qmail]# tar -zxvf tnef-1.2.3.1.tar.gz
[root@rh9 qmail]# cd tnef-1.2.3.1
[root@rh9 tnef-1.2.3.1]# ./configure
[root@rh9 tnef-1.2.3.1]# make
[root@rh9 tnef-1.2.3.1]# make install
```

编译安装后,可执行文件 tnef 位于/usr/local/bin 目录中。

#### 6. 安装 Perl 的 DB\_File 和 Time::HiRes 模块

```
[root@rh9 qmail]# rpm -ivh perl-DB_File-1.804-88.i386.rpm
[root@rh9 qmail]# rpm -ivh perl-Time-HiRes-1.38-3.i386.rpm
[root@rh9 qmail]# rpm -ivh perl-suidperl-5.8.0-88.i386.rpm    # 安装 perl-suidperl
```

另外,也可在线安装 DB\_File 和 Time::HiRes 模块,其安装方法为:

```
[root@rh9 qmail]# perl -MCPAN -c shell
cpan>install Time::HiRes                # 安装 Time::HiRes 模块
cpan>install DB_File                     # 安装 DB_File 模块
cpan>quit
```

## 7. 安装与配置反病毒软件

clamav 是一个开放源代码的免费杀毒软件。Clam Anti-Virus 反病毒软件默认使用 clamav 的用户身份运行,所属的组也为 clamav,其创建方法为:

```
[root@rh9 gmail]# groupadd clamav
[root@rh9 gmail]# useradd -g clamav -s /bin/false -c "Clam Antivirus" clamav
```

### (1) 安装 clamav 反病毒软件

```
[root@rh9 gmail]# tar -zxvf clamav-0.75.1.tar.gz
[root@rh9 gmail]# cd clamav-0.75.1
[root@rh9 clamav-0.75.1]# ./configure
[root@rh9 clamav-0.75.1]# make
[root@rh9 clamav-0.75.1]# make check
[root@rh9 clamav-0.75.1]# make install
```

下面清除源代码目录中因编译产生的二进制文件和 object 文件。

```
[root@rh9 clamav-0.75.1]# make clean
```

编译安装后,clamav-config、clamdscan、clamscan 和 freshclam 等可执行文件安装在 /usr/local/bin 目录中,clamav 的守护进程文件安装在 /usr/local/sbin 目录中。病毒库安装在 /usr/local/share/clamav 目录中,库文件安装在 /usr/local/lib 目录中。

另外在编译配置时,也可利用“--prefix”配置参数指定安装位置,让这些文件安装在统一的目录下面,比如 /usr/local/clamav。

### (2) 测试病毒检查

```
[root@rh9 clamav-0.75.1]# cd /usr/local/bin
[root@rh9 bin]# clamscan -h | less
```

# 获得命令用法帮助

下面利用 clamscan 命令,以命令行方式对当前目录进行病毒检查,并将检查结果保存到 scanreport.txt 文件中,以检查该杀毒软件运行是否正常。

```
[root@rh9 bin]# clamscan -r -l scanreport.txt
```

其中参数 -l 用于指定报告文件,-r 表示递归检查当前目录下的所有文件。下面查看生成的报告文件,然后删除所产生的 scanreport.txt 文件。

```
[root@rh9 bin]# cat scanreport.txt
[root@rh9 bin]# rm -rf scanreport.txt
```

若要对 /home 目录进行病毒检查,则执行命令: /usr/local/bin/clamscan -r /home

### (3) clamav 的配置文件

在配置编译 clamav 软件包时,没有使用“--prefix”指定安装位置,默认安装在/usr/local 目录下,所以可执行文件安装在/usr/local/bin 目录中,其配置文件因此安装在/usr/local/etc 目录中。

```
[root@rh9 bin]# cd ../etc
[root@rh9 etc]# ls
clamav.conf  freshclam.conf
```

clamav.conf 是 clamd 守护进程的配置文件,freshclam.conf 是病毒库自动升级程序 freshclam 的配置文件。clamav.conf 和 freshclam.conf 是一个配置样例,绝大部分的配置项均是用#注释掉了的,用户应根据自己的实际情况和要求进行配置,否则 clamd 守护进程将无法启动。

下面利用 vi 对 clamav.conf 配置文件进行修改,去掉配置项前面的#,让配置项生效。

```
[root@rh9 etc]# vi clamav.conf
# 注意将以下的 Example 在前面加“#”将其注释掉,系统由此判断是否对配置文件作过修改
# Example
LogFile /var/log/clamd.log          # 启用日志。原记录在/tmp/clamd.log 文件中
LogFileMaxSize 8M                   # 指定日志文件的最大大小,原为 2MB。0 则不受限制
LogTime                             # 对每条日志都记录时间
LogVerbose                          # 使用详细的日志
PidFile /var/run/clamd.pid           # 指定 clamd 进程号保存文件
TemporaryDirectory /var/tmp         # 设置临时目录
# 下面设置病毒库的安装目录,配置文件默认为/var/lib/clamav
DatabaseDirectory /usr/local/share/clamav
# 注意: 以下两项不要启用。clamav 只能使用 Local TCP
# LocalSocket /tmp/clamd             # 设置 clamd 守护进程通信用的 socket 文件
# FixStaleSocket                     # 非正常关机后删除 socket
TCPSocket 3310                       # clamd 守护进程的 TCP 端口
# TCPAddr 127.0.0.1                  # 设置监听地址,默认监听本机的全部地址
MaxConnctionQueueLength 30
StreamSaveToDisk                     # 输入的数据流在病毒扫描前先存到磁盘
StreamMaxLength 10M                  # 允许的最大数据流,超过的将关闭该连接
MaxThreads 10                        # 允许的最大线程数
ReadTimeour 300                      # 等待客户端数据的超时时间,单位为秒,默认为 120 秒
MaxDirectoryRecursion 15             # 允许目录扫描的深度
FollowDirectorySymlinks              # 允许目录链接
```

```

FollowFileSymlinks           # 允许文件链接
# 下面设置每隔多个秒钟从 internet 检查一次病毒库结构的完整性和真实性。默认为 1 小时,即
3600 秒
SelfCheck 36000
# 以下设置当发现病毒时,利用 send_sms 程序发送消息,%v 代表病毒的名称
# VirusEvent /usr/local/bin/send_sms 123456789 "VIRUS ALERT: %v"
User clamav                  # 指定以 clamav 用户身份运行 clamd 进程
ScanOLE2                     # 设置允许扫描 word 文档
ScanMail                     # 设置允许扫描邮件
ScanArchive                  # 设置允许扫描文档
ScanRAR                      # 设置允许扫描 RAR 压缩文档
# 以下设置将保护系统不受文件炸弹的攻击,而产生拒绝服务
ArchiveMaxFileSize 10M       # 允许扫描的文档的最大字节数,超过的将不扫描
# 下面设置对压缩文档的扫描的深度。主要针对压缩文档中又有压缩文档的情况
ArchiveMaxRecursion 5
ArchiveMaxFiles 1000         # 一个文档中允许扫描的最大文件数
ArchiveMaxCompressionRatio 200 # 将潜在的文件炸弹标记为病毒
# 用较慢的解压算法解压文档,以防止使用过多内存。仅对 bzip2 解压程序有效
ArchiveLimitMemoryUsage
# ArchiveBlockEncrypted      # 标记加密的 .zip 或 .rar 文档为病毒
ClamukoIncludePath /home     # 设置病毒检查的目录。其下的子目录也将全部扫描检查
# ClamukoExcludePath /home/guru # 用于设置要排除病毒检查的目录。包括下面的子目录
ClamukoMaxFileSize 1M        # 设置允许被扫描的文件最大字节数
ClamukoScanArchive           # 启用文档支持

```

设置好后,存盘退出 vi。下面编辑修改 freshclam.conf 配置文件。

对 freshclam.conf 配置文件的修改,对于共有的配置项,如对病毒库位置的设置,要注意与 clamav.conf 中的设置保持一致。

```

[root@rh9 etc]# vi freshclam.conf
DatabaseDirectory /usr/local/share/clamav      # 指定病毒库的安装位置
UpdateLogFile /var/log/freshclam.log           # 设置病毒升级日志文件
LogVerbose
DatabaseOwner clamav                          # 设置病毒库的拥有者
DatabaseMirror database.clamav.net             # 病毒库升级的站点,不要更改
MaxAttempts=3                                  # 病毒升级失败时重试的次数
Checks 12                                       # 病毒库升级检查的时间间隔,单位小时
# 下面是对代理服务器进行设置。若是直接上网,则不用设置
# HTTPProxyServer myproxy.com
# HTTPProxyPort 1234

```



```
# HTTPProxyUsername myusername
# HTTPProxyPassword mypass
#
# NotifyClamd [/optional/config/file/path]      # Send the RELOAD command to clamd
# OnUpdateExecute command                       # 病毒库升级后运行指定的命令
# OnErrorExecute command                       # 升级失败后运行指定的命令
```

下面创建所需的日志文件：

```
[root@rh9 etc]# touch /var/log/clamd.log /var/log/freshclam.log
[root@rh9 etc]# chmod 644 /var/log/clamd.log
[root@rh9 etc]# chmod 644 /var/log/freshclam.log
[root@rh9 etc]# chown clamav:clamav /var/log/clamd.log /var/log/freshclam.log
```

#### (4) 启动 clamd 守护进程

配置文件设置好后,接下来就可以启动 clamd 守护进程了。该守护进程可实时监控和杀除 Linux 系统的病毒。若仅是为了防邮件病毒,也可不启动该守护进程,在设置好 qmail-scanner 扫描器后,扫描器会自动调用该杀毒软件来对邮件进行病毒检测和杀除带毒邮件。

```
[root@rh9 etc]# /usr/local/sbin/clamd          #启动 clamd 守护进程
[root@rh9 etc]# ps -auxw | grep clamd          #查看该进程
```

#### (5) clamav 病毒库的升级

反病毒软件应定期更新病毒库,以便能检查和杀除一些新出现的病毒。clamav 病毒库的更新有两种方式,一种是从官方网站下载病毒升级库文件,然后使用 clamscan 命令来装载病毒库,其命令用法为:

```
/usr/local/bin/clamscan -d file/dir
```

-d 参数用于指定病毒库升级文件或目录,若为目录,则从该目录下的所有升级文件中,加载病毒库。clamav 的病毒升级库文件扩展名为.cvd,安装后有 daily.cvd 和 main.cvd 两个病毒库文件。

另一种升级方式是使用 freshclam 命令实现从官方网站自动升级病毒库,在设置好 freshclam.conf 配置文件后,即可实现病毒库的按时自动升级。另外,也可通过手工执行该命令,来主动升级病毒库,其操作命令为:

```
[root@rh9 etc]# /usr/local/bin/freshclam
ClamAV update process started at Wed Sep 15 12:58:31 2004
Reading CVD header (main.cvd): OK
Downloading main.cvd [ * ]
```

```
main.cvd updated (version: 26, sigs: 22925, f-level: 2, builder: tomek)
Reading CVD header (daily.cvd): OK
Downloading daily.cvd [ * ]
daily.cvd updated (version: 491, sigs: 1239, f-level: 2, builder: ccordes)
Database updated (24164 signatures) from database.clamav.net (211.234.111.17).
```

## 8. 安装反垃圾邮件软件

SpamAssassin 目前的正式版为 2.64, 该软件包需要 Perl 的 Mail::SpamAssassin 模块支持, 在安装 SpamAssassin 之前, 可利用以下命令, 利用在线方式安装该模块。

```
[root@rh9 ~]# perl -MCPAN -e shell
CPAN>o conf prerequisites_policy ask
CPAN>install Mail::SpamAssassin          # 在线安装指定的模块
CPAN>quit                                # 退出 CPAN 命令行
```

在安装 SpamAssassin 软件包前还必须设置环境变量 LANG 的值为 en\_US, 否则在运行 perl Makefile.PL 时将会报错。另外, 也可直接修改 /etc/sysconfig/i18n 文件, 将其中的 LANG="en\_US.UTF-8" 改为 LANG="en\_US"。

```
[root@rh9 ~]# tar -zxvf Mail-SpamAssassin-2.64.tar.gz
[root@rh9 ~]# cd Mail-SpamAssassin-2.64
[root@rh9 Mail-SpamAssassin-2.64]# LANG=en_US perl Makefile.PL
[root@rh9 Mail-SpamAssassin-2.64]# make
[root@rh9 Mail-SpamAssassin-2.64]# make install
[root@rh9 Mail-SpamAssassin-2.64]# make test          # 测试安装结果
```

若最后报告 "All tests successful.", 则安装成功。

该软件包默认安装在 /usr 目录下, 可执行文件 spam、spamd、spass 安装在 /usr/bin 目录中。SpamAssassin 还预设了很多默认规则, 安装在 /usr/share/spamassassin 目录中, 一般情况下, 用户不需要修改这些预设的规则。若要添加规则, 可通过用户自定义规则文件 /etc/mail/spamassassin/local.cf 来实现。规则的定义方法可参看白名单列表文件 60\_whitelist.cf。白名单是与黑名单相对而言的, 是指确信不会发送垃圾邮件的邮件地址或邮件域。

spamd 是 SpamAssassin 的后台守护进程程序, 在源代码目录 Mail-SpamAssassin-2.64 下面有一个名为 spamd 的子目录, 在该目录中有一个名为 redhat-rc-script.sh 的启动脚本, 将其复制到 /etc/rc.d/init.d/ 目录中, 即可实现在开机时的自动启动, 其操作命令为:

```
[root@rh9 Mail-SpamAssassin-2.64]# cd spamd
```

```
[root@rh9 spamd]# cp ./redhat-rc-script.sh /etc/rc.d/init.d/spamassassin
```

另外也可利用以下命令来实现该守护进程的启动、重启、停止和状态查询。

启动 spamd 守护进程,实现命令: service spamassassin start。

重新启动 spamd 守护进程,实现命令: service spamassassin restart。

停止 spamd 守护进程,实现命令: service spamassassin stop。

查询 spamd 守护进程的启动状态,实现命令: service spamassassin status。

下面创建/etc/default/spamassassin 配置文件:

```
[root@rh9 spamd]# vi /etc/default/spamassassin
ENABLED=1
OPTIONS="-v -m 50 --auto-whitelist"
```

编辑修改/etc/mail/spamassassin/local.cf 配置文件:

# 设置判定为垃圾邮件的综合分值,默认为 5.0。

```
required_hits 6.0
```

```
rewrite_subject 1
```

# 在邮件头中包含 spam 报告

```
report_header 1
```

# 在报告中减少过多的解释

```
use_terse_report 1
```

```
defang_mime 1
```

```
dns_available yes
```

```
dec_add_header 1
```

```
use_dec 1
```

required\_hits 配置项用于指定判定为垃圾邮件的邮件综合分值。如果出现将正常邮件误标为垃圾邮件,可以将判定为垃圾邮件的分值由默认的 5.0 适当调高一些,比如调整到 6.0。

安装和配置好该邮件过滤器后,接下来将其整合到 qmail-scanner 扫描器中,就可实现利用该过滤器来对邮件进行反垃圾检查了。以后在收到的邮件头中,如果出现与 spam 检查相关的内容,则就说明 SpamAssassin 已经开始发挥作用。

在 qmail-scanner 中指定 SpamAssassin 扫描器时,可指定为 fast\_spamassassin 或 verbose\_spamassassin 工作模式。fast\_spamassassin 仅对 250KB 以下的邮件进行检查,超过的将不作检查,verbose\_spamassassin 则对邮件都要进行检查。

## 9. 安装 qmail-scanner

qmail-scanner 进程默认使用 qscand 用户身份运行,该用户默认所属的用户组也为 qscand,该用户的主目录(home directory)为/home/qscand,其创建方法为:

```
[root@rh9 qmail]# groupadd qscand
[root@rh9 qmail]# useradd -g qscand -s /bin/false qscand
```

下面安装 qmail-scanner:

```
[root@rh9 qmail]# tar -zxvf qmail-scanner-1.23.tgz
[root@rh9 qmail]# gunzip q-s-1.23st-20040819.patch.gz
[root@rh9 qmail]# cd qmail-scanner-1.23
[root@rh9 qmail-scanner-1.23]# patch -p1 < ../q-s-1.23st-20040819.patch
[root@rh9 qmail-scanner-1.23]# ./configure --help | less    # 获得安装配置帮助
[root@rh9 qmail-scanner-1.23]# ./configure --qs-user qscand --qs-group qscand \
> --spooldir /var/spool/qmailscan --qmaildir /var/qmail --bindir /var/qmail/bin \
> --qmail-queue-binary /var/qmail/bin/qmail-queue --admin-fromname "Mail admin" \
> --scanners "clamscan, verbose_spamassassin" --scanners-per-domain yes \
> --admin postmaster --domain pcnnetedu.com --lang en_GB \
> --notify sender,admin,recips --silent-viruses auto --archive yes --unzip yes \
> --redundant yes --add-dscr-hdrs yes --log-crypto 0 \
> --sa-subject " * * * * * SPAM * * * * *" --sa-delete 5 --install
```

以上语句将自动检测当前系统所安装的软件,并创建安装目录树。其安装过程为:

Building Qmail-Scanner 1.23st...

This script will search your system for the virus scanners it knows about, and will ensure that all external programs qmail-scanner-queue.pl uses are explicitly pathed for performance reasons.

It will then generate qmail-scanner-queue.pl — it is up to you to install it correctly.

Continue? ([Y]/N) 回答 Y

Searching .....

Found tnrf on your system! That means we'll be able to decode stupid M\$ attachments:-)

---

The following binaries and scanners were found on your system:

---

mimeunpacker=/usr/local/bin/reformime

unzip=/usr/bin/unzip

tnrf=/usr/local/bin/tnrf

Content/Virus Scanners installed on your System

clamscan=/usr/local/bin/clamscan

verbose\_spamassassin=/usr/bin/spamc

```

Qmail-Scanner details.
log-details= syslog
fix-mime= 2
ignore-eol-check= 0
debug= 0
notify= sender, admin, recipis
redundant-scanning= yes
block-password-protected= 0
archiving everything into /var/spool/qmailscan/archives/
virus-admin= postmaster@pcnnetedu. com
local-domains= 'pcnnetedu. com'
silent-viruses= 'klez', 'bugbear', 'hybris', 'yaha', 'braid', 'nimda', 'tanatos', 'sobig', 'winevar',
'palyh', 'fizzer', 'gibe', 'cailont', 'lovelorn', 'swen', 'dumaru', 'sober', 'hawawi', 'hawaii', 'holar-i',
'mimail', 'poffer', 'bagle', 'worm. galil', 'mydoom', 'worm. sco', 'tanx', 'novarg', '@mm', 'cissy',
'cissi', 'qizy', 'bugler', 'dloade', 'netsky', 'spam'
scanners= "clamscan_scanner", "verbosc_spamassassin"

-----
st: configuration options for 1.23st
-----

admin-fromname= 'Mail admin'
minidebug= 1
scanners-per-domain= 1
dscr-hdrs-text= 'X-Qmail-Scanner'

sa-delta    = 0
sa-alt      = 0
sa-debug    = 0      (only valid if sa-alt is enabled)
sa-report   = 0      (only valid if sa-alt and sa-debug are enabled)

Spamassasin Required_Hits= 6.0
sa-quarantine= 0      (no mail will be quarantined)
sa-delete    = 5      (messages over 11 hits will be deleted)
sa-reject     = 0
-----

```

If that looks correct, I will now generate qmail-scanner-queue.pl  
for your system...

Continue? ([Y]/N) 回答 Y

Testing suid nature of /usr/bin/perl...

Looks OK...

Hit RETURN to create initial directory structure under /var/spool/qmailscan,  
and install qmail-scanner-queue.pl under /var/qmail/bin; perlscanner: generate new DB file from /  
var/spool/qmailscan/quarantine-attachments.txt  
perlscanner: total of 9 entries.

Finished installation of initial directory structure for Qmail-Scanner under /var/spool/qmailscan and  
qmail-scanner-queue.pl under /var/qmail/bin.

Finished. Please read README(.html) and then go over the script

(/var/qmail/bin/qmail-scanner-queue.pl) to check paths/etc.

"/var/qmail/bin/qmail-scanner-queue.pl -r" should return some well-known virus  
definitions to show that the internal perlscanner component is working.

If you're upgrading, remember that your previous quarantine-attachments.txt file  
has not been changed, maybe it's a good idea to have a look at the file  
coming with this distribution.

That's it!

You have enabled 'scanners-per-domain' remember to edit the file

"/var/spool/qmailscan/scanners\_per\_domain.txt" and build the database with the command  
/var/qmail/bin/qmail-scanner-queue.pl -p, other-wise qmail-scanner will fall  
to the '@scanners\_installed' installed.

\* \* \* \* \* FINAL TEST \* \* \* \* \*

Please log into an unprivileged account and run /var/qmail/bin/qmail-scanner-queue.pl -g

If you see the error "Can't do setuid", or "Permission denied", then refer to the FAQ.

(e.g. "setuidgid qmaild /var/qmail/bin/qmail-scanner-queue.pl -g")

That's it! To report success.

编译安装后,将创建初始目录/var/spool/qmailscan,qmailscan.的日志文件、临时文件和其他一些文件一般均存放在该目录中。最后将 qmail-scanner-queue.pl 安装在/var/qmail/bin 目录中。

```
[root@rh9 qmail-scanner-1.23]# cd /var/qmail/bin
```

```
[root@rh9 bin]# ./qmail-scanner-queue.pl -g
```

```
perlscanner: generate new DB file from /var/spool/qmailscan/quarantine-attachments.txt
```

```
perlscanner: total of 9 entries.
```

在输出的信息中,只要没有看到“Can't do setuid”或“Permission denied”等错误信息,则说明安装成功。执行以下命令,还应该查看到一些已知的病毒信息。

```
[root@rh9 bin]# ./qmail-scanner-queue.pl -r
```

下面发送一封正常邮件、两封带毒邮件和一封垃圾邮件到 postmaster@pcnetedu.com 邮箱,以测试防病毒和反垃圾邮件。

```
[root@rh9 qmail-scanner-1, 23]# ./contrib/test_installation.sh -doit
QMAILQUEUE was not set, defaulting to /var/qmail/bin/qmail-scanner-queue.pl for this test...
Sending standard test message — no viruses...
done!
Sending eicar test virus—should be caught by perlscanner module...
done!
Sending eicar test virus with altered filename—should only be caught by commercial anti-virus
modules (if you have any)...
Sending bad spam message for anti-spam testing—In case you are using SpamAssassin...
Done!
Finished test. Now go and check Email for postmaster@pcnetedu.com
```

查看 /var/spool/qmailscan/qmail-queue.log 文件, 可以看到发现“Love Letter Virus/Trojan”和“Happy99 Trojan”病毒和垃圾邮件的相关日志记录, 比如:

```
Sat, 18 Sep 2004 09:46:09 CST; 31169; SA: yup, this smells like SPAM -hits = 14.2 -deleting
message...
```

另外, 也可选用 H+BEDV 公司的商业反病毒软件, 在官方网站可申请一个试用注册键文件(hbedv.key), 然后将其复制到安装目录中即可使用。在 qmail-scanner 安装配置时, 其病毒扫描引擎的名称应使用 antivir, 即要表达为“--scanners antivir, verbose\_spamassassin”。

#### 10. 设置使用 qmail-scanner-queue.pl

为了通知 qmail-smtpd 进程使用 qmail-scanner-queue.pl, 替代 qmail 原来的 qmail-queue 进程, 需要设置 QMAILQUEUE 环境变量, 并将该环境变量的值指定为 qmail-scanner-queue.pl。

若使用 daemontools 来管理 qmail 服务的启动, 则修改 /var/qmail/supervise/qmail-smtpd/run 文件, 在该文件中添加以下对 QMAILQUEUE 环境变量的定义。

```
QMAILQUEUE=/var/qmail/bin/qmail-scanner-queue.pl
export QMAILQUEUE
```

由于此时还需要额外运行 Perl 解释器、病毒和反垃圾邮件扫描软件, 因此需要更多的内存空间来运行进程, 为此需要修改 softlimit 语句, 设置允许使用的内存空间大小为 5~15MB 左右。

修改后的 /var/qmail/supervise/qmail-smtpd/run 文件的内容为:

```
[root@rh9 root]# vi /var/qmail/supervise/qmail-smtpd/run
#! /bin/sh
QMAILDUID=qmaild
NOFILESGID=nofiles
MAXSMTPD='cat /var/qmail/control/concurrencyincoming'
QMAILQUEUE=/var/qmail/bin/qmail-scanner-queue.pl
export QMAILQUEUE
exec /usr/local/bin/softlimit -m 15000000 \
    /usr/local/bin/tcpserver -v -H -R -t 1 -l 0 \
    -x /home/vpopmail/etc/tcp.smtp.cdb -c "$MAXSMTPD" \
    -u "$QMAILDUID" -g "$NOFILESGID" 0 smtp \
    /var/qmail/bin/qmail-smtpd \
    /home/vpopmail/bin/vchkpw /bin/true /bin/cmd5checkpw /bin/truc 2>&1
```

另外也可通过中继控制文件 tcp.smtp 来设置 QMAILQUEUE 环境变量,修改 tcp.smtp 文件后,注意重新生成 tcp.smtp.cdb 文件。

```
127. 0. 0. 1; allow, RELAYCLIENT="", QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
61. 186. 170. 130; allow, RELAYCLIENT="", QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
;allow, QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
```

### 11. qmail 的其他反垃圾邮件措施

也可通过以下几种途径来防范垃圾邮件。

#### (1) 封发件者的 IP 或网段

对于垃圾邮件发送者 IP 固定或基本位于某一网段范围时,可利用中继控制文件,限制这些主机与邮件服务器的 SMTP 连接。

比如,若要禁止 220.172.42 网段的主机连接本邮件服务器,则可在 tcp.smtp 中添加以下语句:

```
220.172.42. :deny
```

#### (2) 封邮件账户或邮件域

对于有真实邮件地址的垃圾邮件发送者,可利用 qmail 的配置文件 badmailfrom,来拒收这些账户所发送来的邮件。

#### (3) 使用实时黑名单拒绝垃圾邮件

为了使用实时黑名单技术来拒收垃圾邮件,ucspi-tcp 0.88 软件包提供了一个名为



rbldsmtpd 的后台服务程序,该程序可利用反垃圾邮件联盟提供的实时黑名单(Realtime Blackhole List,RBL),来拒收从这些地址发送来的邮件。利用 rbldsmtpd 程序的-r 参数可指定提供黑名单数据库的网址。

中国反垃圾邮件联盟提供了两个实时黑名单数据库(CBL+ 和 CBL-)。CBL- 是去掉了国内大型邮件服务运营商(如 163、sina 等)的邮件服务器地址的实时黑名单数据库,使用该黑名单数据库,可以接收来自这些运营商邮件服务器发送来的邮件;若使用 CBL+ 则不能收到这些邮件服务器转发来的邮件。CBL+ 实时黑名单数据库提供网址为 cblplus.anti-spam.org.cn,CBL- 的网址为 cbless.anti-spam.org.cn,这两个数据库均只收集整理了国内的垃圾邮件发送源地址,对于国外的垃圾邮件发送源,可用-r 参数同时指定使用国外的实时黑名单数据库,如 relays.mail-abuse.org、relays.ordb.org 和 rbl.maps.vix.com。

如果某个邮件服务器地址被加入了黑名单,又需要临时接收从该邮件服务器发来的邮件,可将该邮件服务器地址加入到白名单(/usr/share/spamassassin/60\_whitelist.cf)中来解决。

CBL+ 和 CBL- 都是公开服务,无须申请即可自行在服务器上配置使用。实时黑名单反垃圾邮件技术,可与前面介绍的邮件过滤技术同时结合使用。

启用实时黑名单反垃圾邮件的方法是:

在 SMTP 启动脚本的“0 smtp”和“/var/qmail/bin/qmail-smtpd”之间,加上/usr/local/bin/rbldsmtpd,并用-r 参数指定实时黑名单数据库的提供网址,可同时指定多个黑名单数据库。

添加实时黑名单反垃圾邮件功能后的 SMTP 启动脚本为:

```
#! /bin/sh
QMAILDUID=qmaild
NOFILESGID=nofiles
MAXSMTPD='cat /var/qmail/control/concurrencyincoming'
QMAILQUEUE=/var/qmail/bin/qmail-scanner-queue.pl
export QMAILQUEUE
exec /usr/local/bin/softlimit -m 15000000 \
    /usr/local/bin/tcpserver -v -H -R -t 1 -l 0 -x /home/vpopmail/etc/tcp.smtp.cdb \
    -c "$MAXSMTPD" -u "$QMAILDUID" -g "$NOFILESGID" 0 smtp \
    /usr/local/bin/rbldsmtpd -r cbless.anti-spam.org.cn -r relays.ordb.org \
```

```
/var/qmail/bin/qmail-smtpd \
```

```
/home/vpopmail/bin/vchkpw /bin/true /bin/cmd5checkpw /bin/true 2>&.1
```

有关 rblsmtpd 的最新信息,可参阅 <http://cr.yp.to/ucspi-tcp/rblsmtpd.html>。

#### (4) 设置 qmail-default 文件

默认情况下,qmail 会认为所有邮箱都是合法的,当有其他邮件发到 qmail 邮件服务器时,qmail 都会接收,而不管该邮箱在服务器中是否真的存在。这一点就有可能被利用,导致收到的垃圾邮件过多,增加服务器的负荷,为此,可对 qmail-default 文件进行以下设置:

```
[root@rh9 root]# vi /var/qmail/alias/.qmail-default
/home/vpopmail/bin/vdelivermail '' bounce-no-mailbox
```

这样当邮件发送到本服务的一个并不存在的邮箱时,邮件服务器就会自动弹回邮件,并告知“no this mailbox”。

## 习题

1. qmail 采用模块化设计,不同的功能由不同的进程来实现。用于接收本地域邮件用户投递的邮件的进程是( ),用于接收远端主机投递到本邮件服务器的进程是( )。

- |                 |                |
|-----------------|----------------|
| A. qmail-smtpd  | B. qmail-queue |
| C. qmail-inject | D. qmail-send  |

2. 用于最终实现将邮件投递给远端用户的进程是( ),用于最终实现将邮件投递到本地邮件用户的邮箱中的进程是( )。

- |                 |                 |
|-----------------|-----------------|
| A. qmail-remote | B. qmail-local  |
| C. qmail-rspawn | D. qmail-lspawn |

3. 以下软件包中,用于为 qmail 邮件系统提供虚拟邮件域功能支持和管理的是( )。

- |                          |                                 |
|--------------------------|---------------------------------|
| A. ucspi-tcp-0.88.tar.gz | B. qmail-smtpd-auth-0.31.tar.gz |
| C. vpopmail-5.4.6.tar.gz | D. daemontools-0.76.tar.gz      |

4. 以下软件包中,用于为 qmail 提供连接管理的是( )。

- |                            |                            |
|----------------------------|----------------------------|
| A. ucspi-tcp-0.88.tar.gz   | B. vpopmail-5.4.6.tar.gz   |
| C. qmailadmin-1.2.2.tar.gz | D. daemontools-0.76.tar.gz |

## 实训 10 安装与配置 qmail 服务器

[实训目的] 熟悉和掌握 qmail 服务器的配置步骤与配置方法。

[实训环境] 在虚拟 PC 机的 Linux 操作系统中进行实作。

[实训内容]

1. 下载 qmail 邮件服务器安装所需的相关软件包,并事先注册申请一个正式的域名,并要求服务商配置好该域名的 MX 记录。
2. 卸载当前系统默认安装的 sendmail 和 postfix 邮件服务器。
3. 创建 qmail 和 vpopmail 所需的用户和用户组。
4. 按本书所讲的步骤与方法,逐步编译、安装和配置各相关软件包。

# 第 11 章

## 配置防火墙与代理服务器

Linux 相对于 Windows 2000/2003 Server 操作系统而言,占用的系统资源较少,运行速度和效率较高,稳定性和安全性也更好,很适合用作软件式防火墙和代理服务器。本章将介绍用 Linux 作防火墙和代理服务器的配置方法。

### 11.1 配置 Linux 防火墙

防火墙是一种非常重要的网络安全工具,利用防火墙可保护企业内网免受外网的攻击,作为网络管理员,掌握防火墙的安装与配置十分重要。本节将重点介绍用于 Linux 防火墙配置的 IP 包过滤和网络地址转换,以及防火墙的配置示例。

#### 11.1.1 防火墙简介

##### 1. 什么是防火墙

防火墙一词来源于建筑业,利用防火墙可以防止火灾从建筑物的一侧蔓延到另一侧,从而起到隔离的作用。在网络领域,防火墙也起到类似的作用,利用防火墙可将两个网络隔离开来,让网间的通信在防火墙规则的控制下,进行有条件地通信、过滤和阻隔对网络有危害的访问和连接,从而对网络起到保护作用。通常情况下,防火墙主要用于校园网或企业内网与 Internet 网之间,以保护内网避免受到来自 Internet 网的攻击。

从中可见,防火墙是一套能够在两个网络间,对网路进行隔离并实现有条件通信的软硬件设备组合,其基本功能是分析出入防火墙的数据包,根据 IP 包头结合防火墙的规则,来决定是否接受或允许数据包通过。被防火墙隔离开来的网络,彼此间通过封包转发来相互通信。

防火墙作为一种保护网络安全的设施,必须部署在受保护网络的边界处,只有这样防火墙才能控制所有出入网络的数据通信,达到将入侵者拒之门外的目的。

## 2. 防火墙的分类

防火墙通常分为硬件防火墙和软件防火墙两种,二者都需要硬件和软件的支持,其区别在于:硬件防火墙使用专用硬件和专用的安全操作系统,而软件防火墙一般使用普通的计算机硬件设备和普通的操作系统(如 Windows 2000 或 Linux)。

硬件防火墙通常配备有三块网卡,提供有外网接口、内网接口和 DMZ 接口。为了配置管理方便和安全的需要,内网需要向外提供服务的服务器群通常放在一个单独的网段中,这个网段便是非军事化区,简称 DMZ 区。外网口用于连接 Internet 网,内网口用于连接代理服务器或内部网络,DMZ 接口则专门用于连接提供服务的服务器群(如 Web 服务器、FTP 服务器、邮件服务器等)。由于服务器有多台,通常应在核心交换机中划分出一个 VLAN,专门用于连接各服务器和 DMZ。防火墙在网络拓扑结构中的位置如图 11.1 所示。

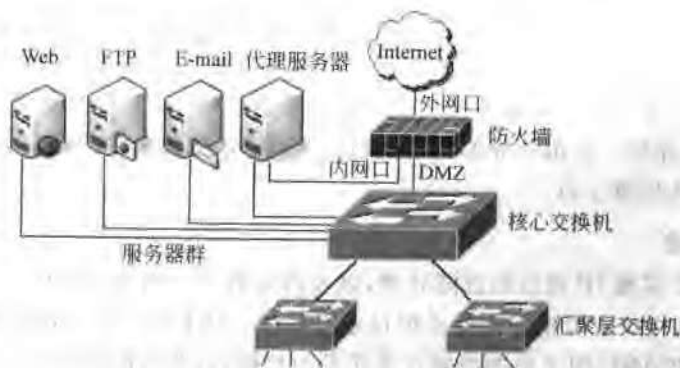


图 11.1 防火墙在网络中的位置

安装 Linux 系统的计算机,通过安装三块网卡,利用内核的包过滤功能,也可实现硬件防火墙相同的功能,并可具备 NAT 和地址伪装等功能。

防火墙按运作方式可分为封包过滤式(packet filter)、应用层网关式(application-level gateway)和电路层网关式(circuit-level gateway),其中被广泛使用的主要是封包过滤式防火墙,本节也主要以该类防火墙为例进行介绍。

封包过滤式防火墙工作在 IP 层,其工作方式是:检查出入防火墙的每一个 IP 数据封包,若 IP 包头所含的数据内容符合预设定的过滤规则,则进行预定的处理,若都不符合过滤规则,则按默认策略进行处理,其处理方式主要有允许通过(ACCEPT)、丢弃(DROP)或拒绝(REJECT)。为了能检查分析 IP 数据封包,防火墙具备分析封包来源 IP 和目的 IP 地址、来源端口和目的端口、封包类型、封包流向、封包进入防火墙的网卡接口以及 TCP 连接状态等能力。

## 11.1.2 IP 包过滤与网络地址转换

### 1. netfilter 简介

netfilter 是 Linux 核心中的一个通用框架,该框架定义了包过滤子系统功能的实现,提供了 filter、nat 和 mangle 3 个表(tables),默认使用的是 filter 表,每个表包含有若干条内建的链(chains),用户也可在表中创建自定义的链。在每条链中,可定义一条或多条过滤规则(rule),即链是规则的一个列表。每条规则应指定所要检查的包的特征以及如何处理与之相匹配的包,这被称作 target(目标),目标值可以是用户自定义的一个链名,以便跳转到同一个表内的用户自定义链进行规则检查,也可以是 ACCEPT、DROP、REJECT 或 RETURN 等值。

每条规则的定义方式一般是“如果封包符合这样的条件,就这样处理该数据包”。当一个 IP 数据包到达一条链时,系统就会从第一条规则开始检查,看是否符合该规则所定义的条件,若满足,则按该规则所定义的方法处理该数据包,若不满足则继续检查下一条规则,如果该数据包不符合该链中的任何一条规则,系统就会按该链预先定义的策略(policy)来处理该数据包。链的策略定义一般是默认 ACCEPT 或 DROP。

规则比较遵循第一匹配优先原则,在表达规则时应注意先后顺序。若未指定源或目的地址,则默认为任意主机。

### 2. IP 包过滤

filter 表用于实现 IP 封包的过滤处理,该表内建有 3 个名为 INPUT、FORWARD 和 OUTPUT 的链,用户也可根据需要添加自定义的链。INPUT 用于处理目标地址是本机的数据包、FORWARD 用于处理要通过或转发的数据包,即目标地址不是本机的数据包、OUTPUT 用于处理本地进程生成的要外发的数据包。filter 表中封包的处理流程如图 11.2 所示。

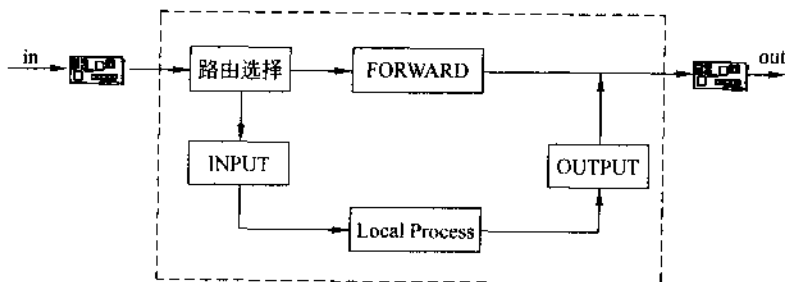


图 11.2 filter 表中封包的处理流程

当一个 IP 数据包从以太网卡进入防火墙时,内核首先根据路由表决定数据包的目标,若数据包的目的地址是本机,则将数据包送往 INPUT 链进行规则检查;若数据包的

目的地址不是本机,则检查内核是否允许转发,若允许,则将数据包送往 FORWARD 链进行规则检查,若不允许转发,则丢弃该数据包;若是防火墙主机本地进程产生并准备发出的包,则数据包送往 OUTPUT 链进行规则检查。

只有内核打开 IP 包转发功能后,一个封包才能被送到转发链(FORWARD)进行规则检查,若没有打开转发功能,则与防火墙相连的两边网络是完全隔离的。打开 Linux 内核包转发功能,可使用以下命令来实现。

```
[root@rh9 root]# echo "1" > /proc/sys/net/ipv4/ip_forward
```

另外也可通过执行/sbin/sysctl -w net.ipv4.ip\_forward="1"命令来开启内核的包转发功能。

以上两条命令均只能在本次打开内核的包转发功能,重启系统后又恢复为 0 值,处于不允许包转发状态。若要系统启动后自动打开包转发功能,可编辑修改/etc/sysctl.conf 配置文件,将其中的 net.ipv4.ip\_forward=0 语句更改为 net.ipv4.ip\_forward=1 来打开内核的包转发功能。对于 Red Hat Linux,还可在/etc/sysconfig/network 配置文件中,通过以下配置项来开启内核的包转发功能。

```
FORWARD_IPV4=true
```

### 3. 网络地址转换

#### (1) NAT 简介

网络地址转换(network address translation)通常也简称为 NAT。随着 Internet 的飞速发展,IP 地址短缺已成为一个非常严重的问题,私有地址可以在不同的企业网内重复使用,这在很大程度上缓解了 IP 地址短缺的矛盾。由于含有私有地址的 IP 报文在 Internet 网中传输时,会被 Internet 中的路由器丢弃,不能被路由,因此,使用私有地址的主机不能访问 Internet。但如果使用私有地址的主机在与 Internet 通信之前,把 IP 报文中的私有地址转换成公有地址,这时使用私有地址的主机也就能与 Internet 通信了。NAT 就是用来将 IP 报文头中的目的或源私有地址修改成公有地址的一种设备,利用 NAT 可实现私有地址与公网地址的相互转换。

#### (2) NAT 的工作原理

NAT 的工作原理如图 11.3 所示。当客户机(192.168.1.2)访问 Web Sever(212.87.194.56)时,客户端会随机选择一个大于 1024 的端口来与服务器的 80 端口建立连接,假设客户端选择使用的是 1029 端口,则从客户端发出的数据包源 socket(IP 地址加 TCP/UDP 端口)为 192.168.1.2:1029,目的 socket 为 212.87.194.56:80,当数据包从 eth0 进入 NAT 设备后,NAT 对数据包的源 socket 进行修改,将源 IP 地址替换为 eth1 网卡的 IP 地址,源端口一般保持不变,若该端口已被使用,则替换使用另一个端口,并将

该替换的对应关系保存在 NAT 表中。经过 NAT 替换修改后的数据包,其源 socket 变为 61.186.160.120:1029,目的 socket 保持不变,此时的数据包具有了公网 IP 地址,就可与 Internet 网中的 Web Server 通信了。

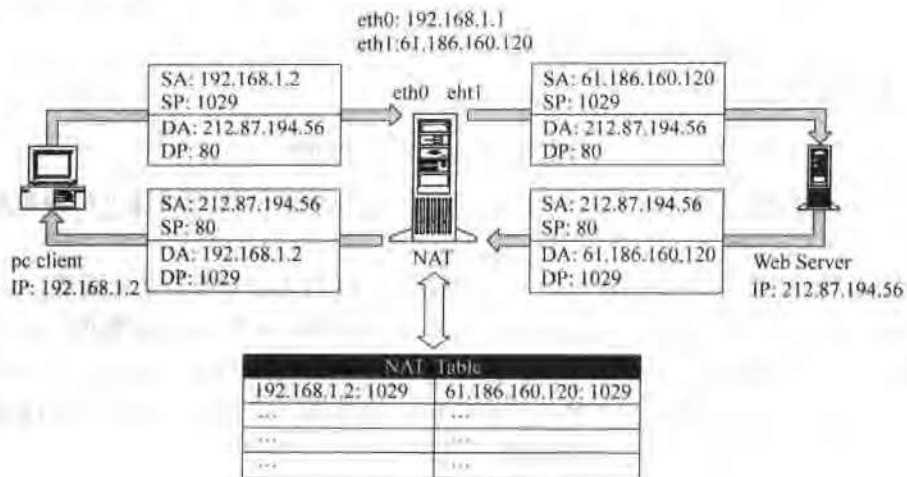


图 11.3 NAT 的工作原理

Web Server 的响应数据包源 socket 为 212.87.194.56:80,目的 socket 为 61.186.160.120:1029,NAT 收到该响应包后,利用 NAT 表中保存的转换对应关系,将响应包的源 socket 替换修改为 192.168.1.2:1029,源 socket 保持不变,这样 Web 服务器的响应包就能顺利进入内网,送达到 192.168.1.2 客户机了。

在这一通信过程中,NAT 设备是透明的,就好像不存在,客户端像是在直接访问 Web 服务器一样。利用 NAT,可实现透明代理企业内网用户访问 Internet,这也是透明代理实现的关键。

### (3) NAT 表

在 Linux 中,网络地址和地址端口的转换均通过 NAT 表来实现,filter 表仅对封包进行过滤处理,不对封包的源或目的地址或端口进行修改。对源地址或源端口进行替换修改,称为 SNAT(source NAT),对目的地址或端口进行替换修改,称为 DNAT(destination NAT)。

NAT 表内建有 3 个名为 PREROUTING、POSTROUTING 和 OUTPUT 的链。

封包从网卡进入之后,在尚未交给路由判断之前的处理在 PREROUTING 链中进行,即刚刚进入网络层的数据包在此链中进行检查处理。在该链中,可以实现对需要转发的数据包的目的 IP 地址和端口进行替换修改(DNAT),从而实现端口或主机的重定向。squid 缓存代理服务器默认的代理端口为 3128,若要将企业内网用户对 80 端口的请求,



重定向到代理服务器的 3128 端口,则可使用该链来实现。内建的端口重定向 REDIRECT 实际上就是 DNAT 的一个特例。

POSTROUTING 是在路由判断之后,所有马上就要通过网卡出去的封包,在此链中进行检查处理,可在此链中进行 SNAT 的设定,实现对封包的源 IP 地址或端口进行替换修改。Linux 内建的 IP 伪装(MASQUERADE)实际上就是 SNAT 的一个特例,它是将封包的源地址直接替换修改为封包出去的网卡的 IP 地址。图 11.3 所介绍的 NAT 工作原理,实际上就是 IP 伪装的工作原理,在 Linux 中,实现该 IP 伪装,可通过以下语句来实现:

```
[root@rh9 root]# /sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

其中,参数 `-t` 用于指定所操作的表, `-A POSTROUTING` 表示在 POSTROUTING 链中增加一条规则, `-o` 用于指定封包流出的网络设备,封包进入的网络设备用 `-i` 参数指定, `-j` 用于指定对封包的处理动作。以上语句的含义就是将从 eth1 网卡流出的封包,进行 IP 伪装。

对于本地进程产生并准备发出的封包由 OUTPUT 链进行检查处理,可在此链进行 DNAT 操作。NAT 表中封包的处理流程如图 11.4 所示。

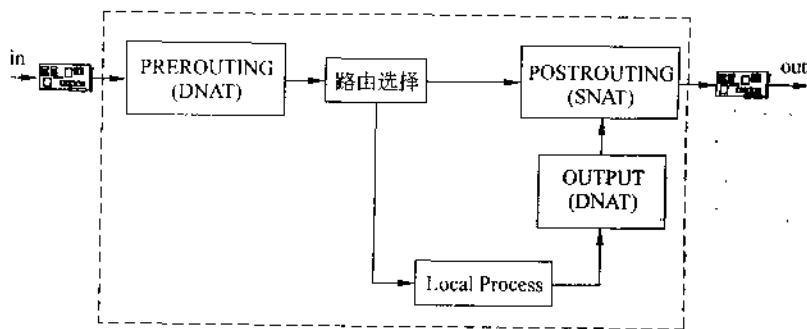


图 11.4 NAT 表中封包的处理流程

只有新连接的第一个数据包才会遍历 NAT 表,而随后的数据包将根据第一个数据包的结果进行同样的转换处理。

mangle 表用于对数据包进行处理,内建有 PREROUTING 和 OUTPUT 链。对 mangle 表的使用较少,此处就不再作介绍。

### 11.1.3 使内核支持防火墙

#### 1. 内核模块的加载

netfilter 要求 Linux 的内核版本不得低于 2.3.5, Red Hat Linux 9 的内核版本为 2.4.20-8,因此其内核是支持防火墙的。在编译内核时,应将 Networking support、

Network packet filtering (replace ipchains)和一些相关的支持模块编译进内核或编译成动态模块,需要时再使用 modprobe 命令加载相关的支持模块。编译配置时需要选择的模块如下所示,\* 代表编译进内核,M 代表编译成动态模块。

```
[ * ] Kernel/User netlink socket
[ ] Routing messages
< * > Netlink device emulation
[ * ] Network packet filtering (replaces ipchains)
:
```

在“IP: Netfilter Configuration --->”配置项中选择以下选项:

```
<M> Connection tracking (required for masq/NAT)
<M> FTP protocol support
<M> IP tables support (required for filtering/masq/NAT)
<M> limit match support
<M> MAC address match support
<M> Netfilter MARK match support
<M> Multiple port match support
<M> TOS match support
<M> Connection state match support
<M> Packet filtering
<M> REJECT target support
<M> Full NAT
<M> MASQUERADE target support
<M> REDIRECT target support
<M> Packet mangling
<M> TOS target support
<M> MARK target support
<M> LOG target support
< > ipchains (2.2-style) support
< > ipfwadm (2.0-style) support
```

编译后,与 netfilter 相关的动态模块存放在/lib/modules/2.4.20-8/kernel/net/ipv4/netfilter 目录中,Linux 的内核模块扩展名通常为.o。

使用 Red Hat Linux 9 安装光盘直接安装的系统,不需要重新编译内核,系统已支持包过滤,并编译好了相关的内核支持模块。

为了使用 IP 包过滤和 NAT,必须用 modprobe 命令载入相关的内核模块(已编译入内核的除外),在载入指定模块时,也会一并载入与之相关的模块。iptables\_filter 模块在运行时会自动载入,其他模块则应根据需要手工载入,各模块的功能与加载方法如

表 11.1 所示。

表 11.1 Linux 的内核支持模块

模块加载方法	模块功能
/sbin/modprobe ip_tables	netfilter 核心模块
/sbin/modprobe ip_conntrack	该模块支持连接状态跟踪
/sbin/modprobe iptable_filter	filter 表支持模块
/sbin/modprobe iptable_nat	nat 表支持模块
/sbin/modprobe iptable_mangle	mangle 表支持模块
/sbin/modprobe ip_conntrack_ftp	ftp 连接状态跟踪
/sbin/modprobe ip_nat_ftp	ftp nat 模块,用于支持 ftp 的 non-PASV 传输模式
/sbin/modprobe ipt_LOG	日志记录支持模块
/sbin/modprobe ipt_limit	该模块支持限制每秒/每分钟/每小时允许通过的数据包的数量
/sbin/modprobe ipt_MASQUERADE	IP 伪装支持模块
/sbin/modprobe ipt_mark	该模块支持在 mangle 表中对包进行标记
/sbin/modprobe ipt_owner	filter using owner as part of the match
/sbin/modprobe ipt_multiport	支持用-m multiport 来表达多个不连续的端口或一个端口范围
/sbin/modprobe ipt_REJECT	该模块使系统支持 REJECT 动作,即在丢弃包后,将回应一个 ICMP 响应
/sbin/modprobe ipt_state	该模块支持对 TCP 标志位的匹配检查
/sbin/modprobe ipt_unelean	该模块支持捕获含有无效 TCP/IP 标记的数据包
/sbin/modprobe ipt_tcpmss	This target affects the TCP MSS
/sbin/modprobe ip_conntrack_irc	irc 连接状态跟踪

要查看已加载的内核模块,可使用 lsmod 命令。若要卸载某个已加载的内核模块,则使用 rmmod 命令。

## 2. 包过滤管理工具

Linux 具有很强的网络服务功能,从 1.1 版本的内核开始,Linux 就已经具备包过滤功能,2.0 版本的内核使用 ipfwadm 来操作包过滤规则,2.2 版本的内核使用 ipchains 来控制包过滤规则,在 2.4 版本的和最新的 2.6 版本的内核中,则使用了一种全新的包过滤管理工具——iptables,其功能更为强大,使用上也更为方便和简单。

利用 iptables 命令可以创建、删除或插入链(chains),并可在链中创建、删除或插入过

滤规则。iptables 仅是一个包过滤管理工具,对过滤规则的执行则是通过 Linux 的 Network packet filtering 内核(netfilter)和相关的支持模块来实现的。

Red Hat Linux 9 在安装时,也安装了对旧版 ipchains 的支持,但 iptables 不能与 ipchains 同时使用,要检查当前内核是否已加载了 ipchains,可使用以下命令来检查。

```
[root@rh9 root]# lsmod | grep ipchains
```

若已加载,可使用命令 `rmmod ipchains` 来卸载该模块。

### 3. 安装 iptables 软件包

为了使用 iptables 包过滤管理工具, Linux 必须安装 iptables 软件包,可使用以下命令检查是否已安装。

```
[root@rh9 root]# rpm -q iptables
iptables-1.2.7a-2
```

若输出以上版本号,则说明当前 Linux 系统已安装 iptables 软件包。Red Hat Linux 9 在安装时,一般会安装该软件包。iptables 命令安装在 `/sbin` 目录中。若未安装,可在 Red Hat Linux 9 的第 1 张安装光盘找到 RPM 安装包 `iptables-1.2.7a-2.i386.rpm`,也可从以下地址下载源代码软件包来安装。

```
http://www.iptables.org/files/iptables-1.2.8.tar.bz2
ftp://ftp.netfilter.org/pub/iptables/iptables-1.2.8.tar.bz2
```

源代码软件包安装方法:

```
[root@rh9 root]# tar -jxvf iptables-1.2.8.tar.bz2
[root@rh9 root]# cd iptables-1.2.8
[root@rh9 iptables-1.2.8]# make PREFIX=/usr
[root@rh9 iptables-1.2.8]# make PREFIX=/usr install
```

### 4. 启动或停止 iptables 服务

启动 iptables 服务,实现命令: `service iptables start`

重启 iptables 服务,实现命令: `service iptables restart`

停止 iptables 服务,实现命令: `service iptables stop`

## 11.1.4 iptables 命令用法

iptables 用于创建、维护和检查 Linux 内核的 IP 包过滤规则,利用该命令可创建、删除或更名链,在链中创建或删除规则,设置链的策略等,功能很强大,用法也比较多,其命令基本格式为:

```
iptables [-t table] command [match] [-j target/jump]
```

其中,参数 `-t` 用于指定规则表,若未指定,则默认为 `filter` 表,`-j` 用于指定对符合过滤规则的包所进行的处理,对包的处理动作,称为 `target`,`jump` 代表一个用户自定义的链名,用于跳转到该链进行规则检查。对于包的过滤,常用的处理动作主要有 `ACCEPT`、`DROP` 或 `REJECT`。使用“`iptables --help`”命令可获得用法帮助,该命令的具体用法有:

```
iptables [-t] chain rule-specification [options]
iptables [-t] chain rulenum rule-specification [options]
iptables -D chain rulenum [options]
iptables -I [-FZ] [chain] [options]
iptables -I [NX] chain
iptables -E old-chain-name new-chain-name
iptables -P chain target [options]
```

## 1. 对链的操作

### (1) 查看链

命令参数: `-L` 或 `--list`

`iptables` 的命令参数通常有两种表达法,一般使用简写表达法。

命令功能: 列出指定表的全部链及其规则。

命令用法: `iptables -L [chain]`

例如,若要列出 `filter` 表的全部规则链,则操作命令为:

```
[root@rh9 root]# iptables -L
```

若要列出 `nat` 表的全部规则链,则操作命令为:

```
[root@rh9 root]# iptables -t nat -L
```

若要列出 `INPUT` 链的所有规则,则实现命令为: `iptables -L INPUT`。

### (2) 创建与删除链

创建新链使用 `-N` 或 `--new-chain` 命令参数,删除链使用 `-X` 或 `--delete-chain` 命令参数。

命令用法: `iptables -I [NX] chain`

例如,若要创建一个名为 `block` 的链,则创建命令为:

```
[root@rh9 root]# iptables -N block
```

```
[root@rh9 root]# iptables -L
```

# 查看新建的链

若要删除刚才新建的 `block` 链,则实现命令为:

```
[root@rh9 root]# iptables -X icmp_packets
```

```
[root@rh9 root]# iptables -L
```

# 查看删除结果

### (3) 更改链的名称

命令参数: -E 或 --rename-chain

命令用法: iptables -E old-chain-name new-chain-name

链更名后,其序号和规则均不受影响。

## 2. 对规则的操作

### (1) 删除规则链中的所有规则

命令参数: -F 或 --flush

命令用法: iptables -F [chain]

命令功能: 删除指定链中的全部规则,若未指定链,则删除表中所有链中的规则。

若要清除 filter 表中 INPUT 链中的全部规则,则实现命令为:

```
[root@rh9 root]# iptables -F INPUT
```

若要删除 filter 表中的全部规则,则实现命令为: iptables -F。

若要删除 nat 表中的全部规则,则实现命令为: iptables -t nat -F。

### (2) 归零封包计数器

封包计数器是用来计算同一封包出现的次数。

命令参数: -Z 或 --zero

命令用法: iptables -Z [chain]

若要将 filter 表中的所有封包计数器归零,则实现命令为: iptables -Z。

若要将 nat 表中的所有封包计数器归零,则实现命令为: iptables -t nat -Z。

### (3) 设置链的默认策略

命令参数: -P 或 -policy

命令用法: iptables -P chain target

命令功能: 定义链的默认策略。即设置所有过滤规则都不满足的封包的默认处理方式。

例如,若要将 INPUT、FORWARD 和 OUTPUT 链的默认策略设置为 ACCEPT,则实现命令为:

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

### (4) 新增规则

命令参数: -A 或 --append

命令功能: 新增规则到指定的链中。新增的规则添加到该链的最后。

例如,若要在 INPUT 链中添加一条规则,禁止所有主机 ping 本机,则实现命令为:

```
[root@rh9 root]# iptables -F                # 清除 filter 表中的原有规则
[root@rh9 root]# iptables -A INPUT -s 0/0 -p icmp --icmp-type echo-request -j DROP
```

其中,-s 用于指定包的来源地址,-p 用于指定协议名称,--icmp-type 用于指定 icmp 包的类型,echo-request 代表 ping 包。

```
[root@rh9 root]# iptables -L INPUT                # 查看 INPUT 链中的规则
Chain INPUT (policy ACCEPT)
target      proto      opt      source      destination
DROP        icmp      --        anywhere    anywhere    icmp echo-request
[root@rh9 root]# ping 192.168.168.154                # 此时将发现无法 ping 通了
```

若用户是通过 ADSL 拨号上网,若仅禁止从外网 ping 本机,则实现的规则为:

```
iptables -A INPUT -p icmp --icmp-type echo-request -i ppp0 -j DROP
```

若要禁止 220.174.156.22 主机访问本机,则实现的规则为:

```
iptables -A INPUT -s 220.174.156.22 -j DROP
```

#### (5) 替换规则

命令参数: -R 或 --replace

命令功能: 用指定的规则,替换原有的规则。

命令用法: iptables -R chain rulenum rule-specification

例如,若要将 INPUT 链中的第 1 号规则替换为“-p icmp --icmp-type echo-request -i ppp0 -j DROP”,则实现命令为:

```
[root@rh9 root]# iptables -R INPUT 1 -p icmp --icmp-type echo-request -i ppp0 -j DROP
[root@rh9 root]# iptables -L INPUT                # 查看规则替换结果
# 此时就可以 ping 通本机了,但在外网不能 ping 通本机(防火墙)
[root@rh9 root]# ping 192.168.168.154
```

#### (6) 删除规则

命令参数: -D 或 --delete

参数后面跟要删除的规则或该规则的编号。规则编号从 1 开始。

例如,若要删除刚才添加的规则,则实现命令为:

```
[root@rh9 root]# iptables -D INPUT -p icmp --icmp-type echo-request -i ppp0 -j DROP
或 [root@rh9 root]# iptables -D INPUT 1
```

### (7) 插入规则

命令参数: `-I` 或 `--insert`

命令用法: `iptables -I chain rulenum rule-specification`

命令功能: 在指定规则的前面插入一条规则, 原规则将自动后移。若未指定规则号, 则默认为 1, 即插入在所有规则的前面。

例如, 若要在 INPUT 链的 1 号规则之前插入一条规则 “`-m state --state NEW, INVALID -i ppp0 -j DROP`”, 则实现命令为:

```
[root@rh9 root]# iptables -I INPUT 1 -m state --state NEW,INVALID -i ppp0 -j DROP
[root@rh9 root]# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt          source          destination
DROP       all  --  anywhere       anywhere        state INVALID,NEW
DROP       icmp --  anywhere       anywhere        icmp echo-request
```

该条规则的功能是禁止外网主动连接防火墙, 并丢掉无法识别和未知连接的封包。

## 3. iptables 的 options 选项

### (1) `-p` 或 `--[!]protocol`

用于在规则中设置要检查的包的协议名称。可指定的协议可以是 `tcp`、`udp` 或 `icmp` 中的一个或者全部。也可使用非运算符 “`!`” 来表示除某协议外的其他全部协议, 比如 “`-p !tcp`”。关键字 `all` 或数字 `0` 代表全部协议, 比如 “`-p all`”。若未指定协议, 则默认为全部协议。

例如, 若要禁止对 `tcp` 445 端口的连接和转发, 则实现的命令为:

```
iptables -A INPUT -p tcp --dport 445 -j DROP
iptables -A FORWARD -p tcp --dport 445 -j DROP
```

当协议为 `icmp` 时, 还可使用 “`--icmp-type`” 进一步指定 `icmp` 的类型。对于 `ping` 包, 其 `icmp` 的类型为 `echo-request`, 其他可用的 `icmp` 类型, 可使用 “`iptables -p icmp -h | less`” 命令来查看。

### (2) `-s` 或 `--src` 或 `--source address[/mask]`

该参数用于在规则中设置要比较的封包的源地址。任意来源可表达为 `-s 0/0`; 对于某网段, 可使用 “网络号/子网掩码中为 1 的位数” 方式来表达。比如, 若要表达来源地址为 192.168.168.0 的 C 类网段的主机, 则表示方法为 `-s 192.168.168.0/24`。

### (3) `-d` 或 `--dst` 或 `--destination address[/mask]`

该参数用于设置要比较的封包的目标地址, 即比较封包要到达的目标地址。设置方法与 `-s` 相同。



(1) `-i` 或 `--in-interface`

该参数用于设置比较封包是从哪一个网络接口卡进入的。比如,若要判断封包是否从 `eth0` 网卡进入,则设置方法为 `i eth0`,若要表达除 `eth0` 以外的其他以太网卡,则表达方法为 `-i !eth0`。

如果接口名后面加上“+”,则所有以此接口名开头的接口都会被匹配,比如: `-i eth+`。如果该选项被忽略,则会假设为“+”,将匹配任意接口。

(5) `-o` 或 `--out-interface`

该参数用于设置要比较封包即将从哪个网络接口卡送出。设置方法与 `-i` 相同。

(6) `--sport` 或 `--source-port`

该参数用于设置要比较封包的来源端口号。可以设置为某一个端口,也可设置为一个端口范围,范围的下限与上限间用“:”进行分隔。比如,若要表达 21~80 端口范围,则表达方法为 `--sport 21:80`,另外端口表达也可使用“!”运算符。

对于不连续的多个端口,可使用以下方法来表达,最多可以指定 15 个端口,只能和 `-p tcp` 或者 `-p udp` 连着使用。

`-m multiport --sport 端口 1,端口 2,端口 3,...`

IP 地址用于告诉与哪一台主机进行连接,端口号则用于进一步指定与该主机上的哪一个服务程序建立连接。一般服务程序均是通过某个或某几个端口来提供服务,并在这些端口上进行侦听(listening),以等待客户端的连接请求。

(7) `--dport` 或 `--destination-port`

用于设置要比较的封包的目标端口,设置方法与 `--sport` 相同。

例如,若要禁止对目标端口为 135、137、138、139 和 445 端口的连接转发,实现命令为:

```
[root@rh9 root]# iptables -A FORWARD -p tcp -m multiport --dport 135,137,138,139,445 -j DROP
```

```
[root@rh9 root]# iptables -L FORWARD -n
```

# 参数 `-n` 表示地址和端口采用数字形式输出

(8) `-m multiport --port`

用于设置比较来源端口号和目的端口号均相同的封包,若一个封包的来源端口为 80,而目标端口是 8080,则该封包将不符合该过滤规则。

(9) `--tcp-flags`

该参数用于设置要比较的封包的 `tcp` 标志位, `--tcp-flags` 后面的参数分为两部分:第一部分是要检查的 `tcp` 标志,是一个用逗号分隔的列表;第二部分用于指定其标志位被设置的 `tcp` 标志,两部分间用空格分隔。

`tcp` 的标志位有 `SYN`(同步)、`ACK`(应答)、`FIN`(结束)、`RST`(重设)、`URG`(紧急)、

PSH(强迫推送), ALL 代表所有的标志位。比较标志时,也可使用“!”运算符。

要充分理解 tcp 标志位在防火墙设置中的应用,必须掌握 TCP 建立连接的三次握手过程。TCP 是一个基于连接的协议,要在客户端和服务器之间传送 TCP 数据,必须先建立一个 TCP 连接,建立 TCP 连接的标准过程分三步,通常也称为三次握手(three-way handshake):

① 每个 TCP 连接,都必须由一端(通常是客户端)发起连接请求,其 TCP 封包的 SYN 标志位将被设置,这是整个连接过程中的第一个封包,此时客户端的连线状态为 SYN\_SENT。

② 若另一端(通常是服务器)接受这个请求,则会向请求端回送一个封包,此时的封包除 SYN 标志外,ACK 标志位也将被设置,并同时在本机上建立资源,以待连接之需。此时服务器端的连接状态为 SYN\_RECV。

③ 请求端获得第一个回应封包后,必须再回应对方一个 ACK 确认封包,此时的封包只有 ACK 标志位被设置,服务器收到该确认封包后,TCP 连接就建立成功了。此时的连线状态为 ESTABLISHED。

在 TCP 建立连接的这三步中,只要某一步中的封包无法成功接收到,则 TCP 连接都无法成功建立。

对于请求联机的 TCP 封包,其 SYN 标志位是被设置了的,而其他的 FIN 和 ACK 标志位没有被设置。若允许企业内网的这类封包通过,则实现规则为:

```
iptables -A FORWARD -p tcp -s 192.168.0.0/16 --tcp-flags SYN,FIN,ACK SYN -j ACCEPT
```

(10) --syn

该参数与--tcp-flags SYN、FIN、ACK SYN 等效。匹配那些设置了 SYN 位,而清除了 ACK 和 FIN 位的 TCP 封包。

(11) -m state --state state

该参数用于设置要比较的联机状态,state 代表一个逗号分隔的匹配连接状态列表。常用的联机状态有 ESTABLISHED、NEW、RELATED 和 INVALID 四种,其含义为:

ESTABLISHED 表示该封包属于某个已经建立的双向传送的连接。

NEW 表示属于某个新连接的封包。

RELATED 表示该封包属于某个已经建立联机的基础上所建立的新连接。比如,建立 FTP 连接时,首先要建立命令连接通道,在进行数据传输时,又要建立数据传输通道。

INVALID 表示该封包的 Session ID 无法识别,属未知连接的封包,这类封包通常应丢掉。

例如,若允许转发从 eth1 进来的,状态为 ESTABLISHED 或 RELATED 的封包,则实现命令为:

```
iptables -A FORWARD -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

(12) `-m limit -limit avg --limit-burst number`

该参数用于设置某段时间内允许通过的平均封包数和触发该限制的突发包的数量。单位可以是 /second(每秒)、/minute(每分钟)和 /day(每天)。

例如,若要设置平均每秒允许通过 1 个 ping 包,触发此限制的突发包的数量为 10 个,则设置命令为:

```
iptables -A FORWARD -p icmp -m limit --limit 1/s --limit-burst 10 -j ACCEPT
```

若要对 IP 碎片的流量进行限制,允许每秒通过 100 个 ip 碎片,触发该限制的突发包数量为 120 个,则设置命令为:

```
iptables -A FORWARD -f -m limit --limit 100/s --limit-burst 100 -j ACCEPT
```

其中,参数 `-f` 代表 ip 碎片,也可表达为 `--fragment`。

(13) `-m iplimit --iplimit-above number --iplimit-mask netmask`

用于设置每个 IP 允许的并发连接数(number)。

例如,若要限制一个 C 段的 IP 地址,连往本机的 squid 服务的并发连接数不得超过 8 个,超过的被拒绝,则设置命令为:

```
iptables -I INPUT -p tcp --syn --dport 3128 -m iplimit --iplimit-above 8 -iplimit-mask 24 -j REJECT
```

(14) `-m mac --mac-source`

该参数用于设置要比较的封包的来源网络接口的硬件地址。例如,若封包来自物理地址为 00:0C:29:03:F3:75 的网络接口,就丢掉该包,则设置方法为:

```
iptables -A FORWARD -m mac --mac-source 00:0C:29:03:F3:75 -j DROP
```

一个 ip 包在经过路由器的转发后,其源 mac 地址将变成路由器的 mac 地址。

#### 4. 规则的处理动作

对规则的处理动作通过 `-j` 参数指定,常用的处理动作有: ACCEPT、REJECT、DROP、REDIRECT、MASQUERADE、DNAT、SNAT、LOG、RETURN 和 MARK。

##### (1) ACCEPT

允许封包通过或接收该封包。

##### (2) REJECT

拦截该封包,并回传一个封包通知对方,可以回传的封包类型有: `icmp-net-unreachable`、`icmp-host-unreachable`、`icmp-port-unreachable`、`icmp-net-prohibited`、`icmp-host-prohibited`、`echo-reply` 和 `tcp-reset`。`tcp-reset` 将回应一个 TCP RST 封包,要求对方

关闭该连接,回传的封包类型使用--reject-with 指定。

例如,若要禁止对 445 端口的连接,并回传一个 tcp-reset 封包,要求对方关闭该连接,则实现命令为:

```
iptables -A FORWARD -p tcp --dport 445 -j REJECT --reject-with tcp-reset
```

### (3) DROP

直接丢弃封包。

### (4) REDIRECT

将封包重新定向到另一个端口,从而实现网络地址端口的转换。

squid 缓存代理服务器默认的代理端口为 3128,若要将企业内网用户对 80 端口的请求,重定向到代理服务器的 3128 端口,则实现命令为:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-ports 3128
```

### (5) MASQUERADE

用于改写封包的来源 IP 为封包流出的外网卡的 IP 地址,以实现 IP 的伪装。利用 IP 伪装,可实现透明代理企业内网用户访问 Internet。假设外网卡为 eth1,则实现命令为:

```
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/16 -j MASQUERADE
```

若用户是通过 ADSL 拨号上网,则外网卡应改为 ppp0,此时的 IP 伪装实现方法为:

```
iptables -t nat -A POSTROUTING -o ppp0 -s 192.168.0.0/16 -j MASQUERADE
```

IP 伪装自动将源地址替换为封包流出的外网卡的地址,不需要显式地指定源 ip 地址,非常适合于拨号上网或合法 IP 地址不固定的情况。

### (6) SNAT 与 DNAT

利用 NAT 可以实现公有地址与私有地址以及端口间的转换。SNAT 用于改写封包的来源 IP 和端口为某指定的 IP 和端口。

假设代理或防火墙外网卡(eth1)的 IP 地址为 61.186.160.150,若要将从外网卡出去的封包的源地址更改为该网卡的地址,端口范围为 1024~65535,则实现的命令为:

```
iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.0.0/16 -j SNAT --to-source 61.186.160.150:1024-65535
```

DNAT 用于改写封包的目的地 IP 地址和端口。利用 DNAT 可实现主机和端口的重定向功能。内建的 REDIRECT 是 DNAT 的一个特例。系统先进行 DNAT,然后才进行路由和过滤等操作。

例如,若要将从防火墙内网卡 eth0 进来的目标端口为 80 的封包,重定向到 IP 地址

为 61.186.160.150 的代理服务器的 3128 端口,则实现命令为:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp -s 192.168.0.0/16 --dport 80 -j DNAT --to-destination 61.186.160.150:3128
```

#### (7) LOG

用于将符合指定规则的封包的相关信息记录在日志文件中。进行完此处理动作后,将继续比较其他规则。

可结合使用 `--log-prefix` 在每条日志记录之前添加一个前缀,用以标识该类日志,前缀字符最多允许 30 个字符。

使用 `--log-level` 可指定记录信息的级别,级别有 `debug`、`info`、`notice`、`warning`、`err`、`crit`、`alert`、`emerg`,分别对应 7 到 0 的数字。例如:

```
iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN,RST -m limit --limit 5/minute -j LOG --log-level 6 --log-prefix "SYN/RST"
```

#### (8) RETURN

结束对当前链中规则的比较,返回主规则链。

#### (9) 自定义链

对规则的处理动作也可以是一个自定义链的名称,该链应事先建立好,并在链中设置好相应的规则。如果在自定义链中找不到匹配的规则,则将自动返回原链的下一行规则继续检查。内建链与自定义链间的调用关系如图 11.5 所示。

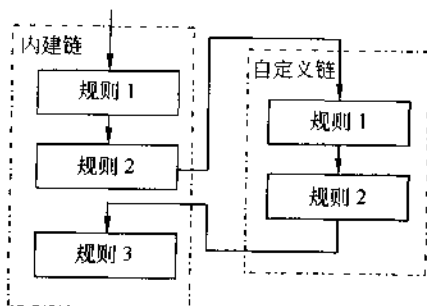


图 11.5 内建链调用自定义链

#### (10) MARK

将封包打上某个标志,以供后续的过滤规则判断处理。进行完此处理动作后,将继续比较其他的规则。只适用于 `mangle` 表,对标志的设置使用 `--set-mark mark`,例如:

```
iptables -t mangle -A PREROUTING -p tcp --dport 22 -j MARK --set-mark 2
```

### 11.1.5 防火墙配置实例

**[例 11.1]** 现有某企业通过光纤直连方式接入 Internet, 有一固定的 IP 地址 61.186.160.202, 假设企业域名为 www.abc.com, 在 Internet 网中, www.abc.com 和 mail.abc.com 域名均指向 61.186.160.202 地址, 网络拓扑结构如图 11.6 所示。

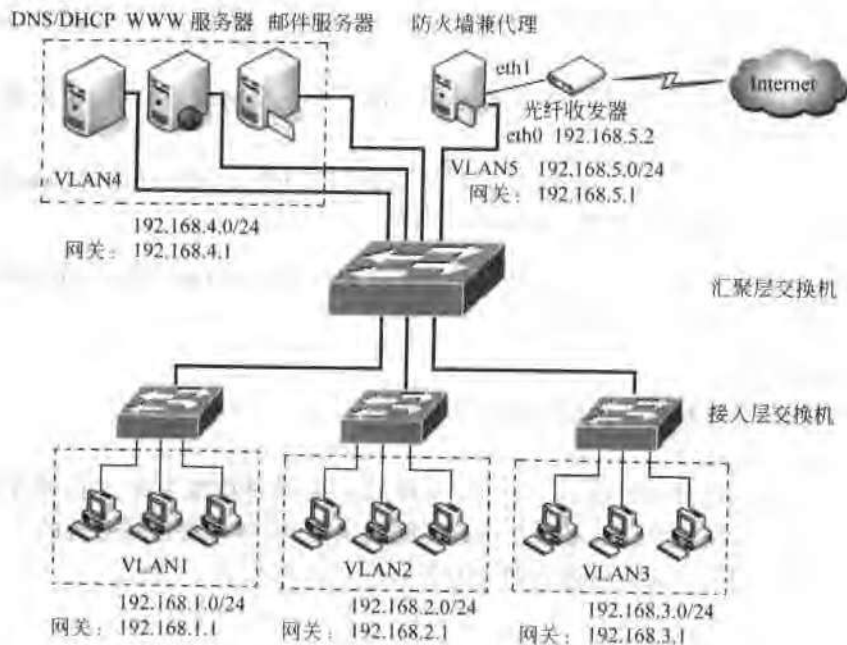


图 11.6 某企业的网络拓扑结构

内网中的 192.168.4.100 地址固定分配给 WWW 服务器, 192.168.4.101 固定分配给邮件服务器, 并对内和对外提供 WWW 和邮件服务, 192.168.4.254 固定分配给 DNS 和 DHCP 服务器, 该台服务器同时提供 DNS 和 DHCP 服务, 该台 DNS 服务器负责将企业域名 www.abc.com 解析为内网地址 192.168.4.100, 将 mail.abc.com 解析为内网地址 192.168.4.101, 对于其他域名的解析, 该域名服务器转发给 Internet 网中的域名服务器进行解析。

企业内网用户使用自动获得 IP 地址和 DNS 服务器方式上网, 获得的 DNS 服务器为内网的 192.168.4.254。现要求编写防火墙脚本, 实现对内网的保护并代理内网访问 Internet。用户可在内网或 Internet 网中, 使用 www.abc.com 域名访问企业的 WWW 服务器, 使用 mail.abc.com 访问企业的邮件服务器。

**分析:** 当用户在企业内网访问企业自己的 WWW 服务器时, 域名服务器将其解析为内网地址, 从而实现通过内网直接访问该 WWW 服务器; 当用户在 Internet 网中访问企

业的 WWW 服务器时,域名由 Internet 网中的 DNS 来负责解析,域名被解析为公网地址 61.186.160.202,该地址也即防火墙的外网卡地址,此时可通过 DNAT,将对 61.186.160.202 主机 80 端口的访问,重定向到内网中的 192.168.4.100 主机,即 WWW 服务器,从而实现从外网访问内网中的主机。对于邮件服务器也类似,可将 192.168.4.100 主机 25 和 110 端口的访问,重定向到内网中的邮件服务器(192.168.4.101)即可。

内网用户要访问 Internet,可通过网络地址转换(IP 伪装)来实现。防火墙与代理服务关系很密切,通常使用一台 Linux 服务器来同时实现防火墙和代理的双重功能。对于中小企业,这是个不错的选择。对于大中型企业,防火墙通常使用硬件式防火墙。

配置步骤:

① 以最小化方式安装 Linux 服务器,然后配置网络接口卡。eth0 网络接口卡用作连接企业内网,IP 地址为 192.168.5.2,不要设默认网关;eth1 用于连接外部 Internet 网,IP 地址设置为 61.186.160.202,默认网关设置为服务商提供的网关。设置好后,应保证在 Linux 服务器上能正常访问 Internet。

② 编写防火墙脚本。

```
[root@rh9 root]# vi /etc/rc.d/init.d/firewall
# ! /bin/sh
echo "Starting firewall iptables rules..."
# 开启 IP 包转发功能
echo 1 > /proc/sys/net/ipv4/ip_forward
# 开启动态 IP 支持
echo 1 > /proc/sys/net/ipv4/ip_dynaddr
# 关闭 Explicit Congestion Notification
echo 0 > /proc/sys/net/ipv4/tcp_ccn
# 开启 syn 泛洪攻击保护(SYN Cook Flood)
# syn 攻击利用 TCP 协议缺陷,发送大量伪造的 TCP 连接请求,使被攻击方资源耗尽,导致拒绝
# 服务
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
# Ignore any broadcast icmp echo requests
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
# 装载内核支持模块
/sbin/modprobe ip_tables
/sbin/modprobe iptable_nat
/sbin/modprobe iptable_filter
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ipt_MASQUERADE
```

```

/sbin/modprobe ipt_state
/sbin/modprobe ipt_multiport
# 清除链的规则
/sbin/iptables -F
/sbin/iptables -t nat -F
# 清除封包计数器
/sbin/iptables -Z
/sbin/iptables -t nat -Z
# 设置默认策略为 DROP,然后再开放允许的,这是比较安全的做法
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT DROP
# 允许本地连接
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
# 允许 ping 代理
/sbin/iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s --limit-burst 10 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
# 允许代理服务器 ping 其他主机
/sbin/iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
# 允许代理服务器主机进行 DNS 查询
/sbin/iptables -A OUTPUT -dport 53 -j ACCEPT
/sbin/iptables -A INPUT --sport 53 -j ACCEPT
# 下面开始处理转发规则
# 对由内向外发起的连接,先进行必要的过滤,防止局域网内病毒的泛洪连接
# 禁止对 135,137,138,139 和 445 端口的连接请求
/sbin/iptables -A FORWARD -p tcp -m multiport --dport 135,137,138,139,445 -j DROP
# 允许转发由内向外的其他访问连接
/sbin/iptables -A FORWARD -i eth0 -j ACCEPT
# 允许转发对已经建立的连接的回应,允许建立在已建立连接基础上的新连接,如 ftp-data
/sbin/iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
# 接收 ip 碎片,允许每秒通过 100 个 ip 碎片,触发该限制为每秒突发 120 个,以防止 ip 碎片攻击
/sbin/iptables -A FORWARD -f -m limit --limit 100/s --limit-burst 120 -j ACCEPT
# 下面进行 NAT 转换,实现从外网访问内网中的服务器。注意连接是双向的,有来有往
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 80 -j DNAT --to-destination 192.168.4.100:80
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 80 -j SNAT --to-

```



```

source 61.186.160.202;80
# web 服务器通常还提供有 FTP 服务,下面对 FTP 服务进行 NAT 转换
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 21 -j DNAT
--to-destination 192.168.4.100;21
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 21 -j SNAT
--to-source 61.186.160.202;21
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 20 -j DNAT
--to-destination 192.168.4.100;20
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 20 -j SNAT
--to-source 61.186.160.202;20
# 对 https 服务(443 端口)进行 NAT 转换。TOMCAT 默认使用 8080 端口
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 443 -j DNAT
--to-destination 192.168.4.100;443
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 443 -j SNAT
--to-source 61.186.160.202;443
# 下面对邮件服务器进行 NAT 转换。SMTP 使用 25 号端口,POP3 使用 110 号端口,IMAP 使用
143 号端口
# 对于使用 SSL 加密的邮件系统,其 SMTPS 使用 465 号端口,POP3S 使用 995 号端口,IMAPS 使
用 993 号端口
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 25 -j DNAT
--to-destination 192.168.4.100;25
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 25 -j SNAT
--to-source 61.186.160.202;25
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 110 -j DNAT
--to-destination 192.168.4.100;110
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 110 -j SNAT
--to-source 61.186.160.202;110
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth1 -d 61.186.160.202 --dport 143 -j DNAT
--to-destination 192.168.4.100;143
/sbin/iptables -t nat -A POSTROUTING -p tcp -o eth1 -s 192.168.4.100 --sport 143 -j SNAT
--to-source 61.186.160.202;143
# 若需对服务器开放 telnet(23 号端口)或 ssh(22 号端口)登录,则对相应端口进行转换即可
# 利用 IP 伪装方式代理内网访问 Internet
/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

```

保存文件,退出 vi。

③ 将防火墙脚本设置为可执行文件。

```
[root@rh9 root]# chmod 755 /etc/rc.d/init.d/firewall
```

① 在防火墙上为 192.168.0.0/16 网络增加一条路由,将网关设置为防火墙主机所

在 VLAN 的网关。

```
[root@rh9 root]# route add -net 192.168.0.0 netmask 255.255.0.0 dev eth0 gw 192.168.5.1
```

⑤ 在汇聚层交换机上设置默认路由,指向防火墙主机。

⑥ 运行防火墙脚本,启动防火墙和代理服务。

⑦ 保证交换机 VLAN 划分和配置正确,DNS 和 DHCP 服务器配置和工作正常。在局域网中,检查各主机能否正确获得 IP 地址、DNS 服务器地址和默认网关。各客户机的网关应是所在 VLAN 的网关地址。如果 IP 地址和 DNS 获取正常,此时应可以正常访问 Internet 网了。

防火墙规则运行正常后,也可使用 iptables-save 命令,将正在运行的防火墙规则保存到指定的文件中,以后需要启用防火墙规则时,可用 iptables-restore 命令来从文件中恢复规则。其实现命令为:

```
[root@rh9 root]# /sbin/iptables-save > /etc/sysconfig/iptables      # 保存防火墙规则
[root@rh9 root]# /sbin/iptables-restore < /etc/sysconfig/iptables    # 恢复防火墙规则
```

## 11.2 安装与配置透明代理服务器

### 11.2.1 代理服务器简介

#### 1. 什么是代理服务器

包含私有网络地址的数据包会被 Internet 网的路由器丢弃,无法被路由,因此使用私有地址的主机不能与 Internet 网中的主机通信,为了解决企业内网中大量没有公网地址的用户能访问 Internet,从而就诞生了代理服务器。

所谓代理服务器就是代表内部私有网中的客户,去连接请求 Internet 网中的资源,并将响应的数据返回给客户机的服务器。在这一通信过程中,客户机向 Internet 服务器发起的请求,将被重定向到代理服务器,代理服务器分析用户的请求,先查看自己缓存中是否有所请求的数据,若有,则从缓存中直接取出数据,传送给客户端;若没有,就代替客户端向 Internet 服务器发出请求,服务器响应后,代理服务器将响应的数据再传送给客户端,同时在自己的缓存中保留一份该数据的备份,以后再有客户端请求相同的数据时,代理服务器就可以直接将数据传送给客户端,而不再需要向 Internet 服务器发起请求,从而加快了响应速度,这是缓存型代理服务器的工作原理。

从中可见,代理服务器位于内网与外网之间,是内网访问外网的一个网关,若没有单独的防火墙进行安全保护,为了保护内网和代理服务器自身的安全,代理服务器通常兼有防火墙的功能。

## 2. 什么是透明代理服务器

透明代理中的透明是指客户端感觉不到代理的存在,不需要在浏览器中设置代理服务器,只需要设置默认网关和 DNS 服务器,即可访问 Internet,就好像代理不存在,是在直接访问 Internet 网一样。

对于没有划分 VLAN 的小型网络,此时用户的网关应设置为代理服务器的内网卡地址。对于划分有多个 VLAN 的三层式交换网络,各用户的网关应设置为所在 VLAN 的网关,然后在核心交换机上,设置一条默认路由指向代理服务器。

在 Linux 中,实现透明代理有两种方式:一是直接利用网络地址转换(IP 伪装)来实现内网对 Internet 的透明访问,该方式的优点是可以代理访问任何服务,缺点是没有代理缓存功能;二是将 squid 缓存代理服务器与网络地址转换结合使用,利用 squid 代理最常用的 http 和 ftp,对于其他 squid 无法代理的访问则通过网络地址转换来实现,这是一种较好的代理解决方案。

### 11.2.2 利用网络地址转换实现透明代理

利用网络地址转换(IP 地址伪装),可实现透明代理企业内网中的用户访问 Internet。对于一般中小企业或中小学校,由于局域网内用户数不是很多,通常选择较经济的 ADSL 拨号或网通的拨号宽带,并代理局域网内的用户上网;对于大、中型企业,一般使用光纤直连方式接入互联网,这种方式可以提供高速的接入带宽。不管使用哪种方式,透明代理服务器的配置方法基本相同,惟一不同的就是外网卡的设备名称不同,对于 ADSL 拨号上网,外网卡的设备名应使用 ppp0,对于光纤直连或网通的宽带拨号或 DDN 上网方式,外网是直接以太网卡相连的,因此设备名应使用 eth0 或 eth1。

至于用哪一块网卡连接内网,哪一块网卡连接外网,没有统一的规则,本书统一采用 eth0 连接内网,eth1 连接外部网络。对于代理服务器,连接内部网络的网卡不要设置默认网关,使用内部私有网络地址,连接外部网络的外网卡使用公网地址,并设置好默认网关。

要实现透明代理,若不考虑安全,最关键的是 IP 伪装这条配置命令。

对于 ADSL 拨号,IP 伪装实现命令:

```
/sbin/iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

对于使用以太网卡与 Internet 相连的上网方式,IP 伪装实现命令为:

```
/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

代理与防火墙联系比较紧密,对于小型的网络,代理通常兼具有防火墙的功能,对于大中型网络,防火墙通常采用单独的硬件式防火墙来担当,没有条件的也可使用 Linux 来配置一台软防火墙。

[例 11.2] 某企业采用 ADSL 宽带拨号上网,并代理局域网内的主机上网访问 Internet。网络拓扑结构如图 11.7 所示。代理服务器的 eth0 用于连接内部网络,地址为 192.168.1.1,eth1 与 ADSL modem 相连用于连接 Internet,拨号成功后,将会生成 ppp0 网络接口。现要求配置该台代理服务器,实现代理内网的主机上网,并具备防火墙功能。

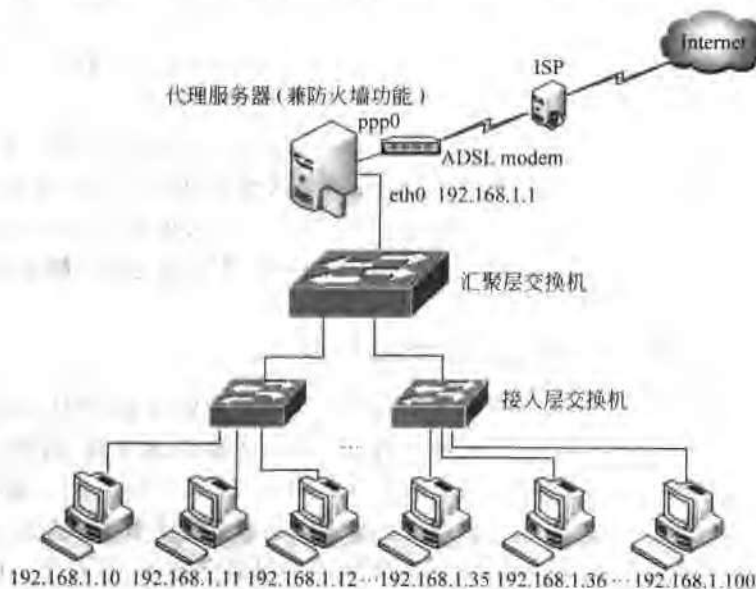


图 11.7 局域网透明代理上网

配置步骤:

① 配置代理服务器的网卡。

在代理服务器上安装并配置好两块以太网卡,注意选择 Linux 能直接识别的、性能较好的网卡。并配置用于连接内网的 eth0 网卡的 IP 地址为 192.168.1.1,不要设置默认网关。相关的配置文件设置为:

```
[root@rh9 root]# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=rh9
FORWARD_IPV4=true
[root@rh9 root]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.1.1
NETMASK=255.255.255.0
```

```
ONBOOT yes
```

② 安装配置 ADSL 拨号,并保证在代理服务器上,通过拨号能正常访问 Internet。

ADSL 拨号上网的安装与配置方法参阅 6.2.2 节的介绍。

③ 编写代理防火墙脚本,实现安全的透明代理。

在 /etc/rc.d/init.d 目录下创建一个名为 adsl\_proxy\_firewall 的脚本,实现透明代理企业内网用户上网。

```
[root@rh9 root]# vi /etc/rc.d/init.d/adsl_proxy_firewall
#!/bin/sh
echo "Starting adsl proxy iptables rules..."
# 开启 IP 包转发功能
echo 1 > /proc/sys/net/ipv4/ip_forward
# 开启动态 IP 支持
echo 1 > /proc/sys/net/ipv4/ip_dynaddr
# 关闭 Explicit Congestion Notification
echo 0 > /proc/sys/net/ipv4/tcpecn
# 开启 SYN 泛洪攻击保护(SYN Cook Flood)
# SYN 攻击利用 TCP 协议缺陷,发送大量伪造的 TCP 连接请求,使被攻击方资源耗尽,导致拒绝
# 服务
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
# Ignore any broadcast icmp echo requests
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
# 装载内核支持模块
/sbin/modprobe ip_tables
/sbin/modprobe iptable_nat
/sbin/modprobe iptable_filter
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ipt_MASQUERADE
/sbin/modprobe ipt_state
/sbin/modprobe ipt_multiport
# /sbin/modprobe ipt_LOG
# /sbin/modprobe ipt_REJECT
# 清除链的规则
/sbin/iptables -F
/sbin/iptables -t nat -F
# 清除封包计数器
/sbin/iptables -Z
```

```

/sbin/iptables -t nat -Z
# 设置默认策略
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT ACCEPT
# 允许本地连接
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
# 对由内向外发起的连接,先进行必要的过滤,防止局域网内病毒的泛洪连接
# 禁止对 135、137、138、139 和 445 端口的连接请求
/sbin/iptables -A FORWARD -p tcp -m multiport --dport 135,137,138,139,445 -j DROP
# 允许对已经建立的连接的回应,允许建立在已建立连接基础上的新连接,如 ftp-data
/sbin/iptables -A FORWARD -i ppp0 -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A FORWARD -m state --state NEW -i ! ppp0 -j ACCEPT
# 进行 IP 伪装,这是实现透明代理上网的关键
/sbin/iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

```

保存代理脚本,退出 vi 编辑器。

④ 设置代理脚本为可执行文件。

```
[root@rh9 root]# chmod 755 /etc/rc.d/init.d/adsl_proxy_firewall
```

⑤ 测试代理服务器。

在代理服务器中利用 ADSL 拨号接入 Internet,然后在局域网中将客户机的网关设置为代理服务器的地址(192.168.1.1),DNS 设置为当地的 DNS 服务器,然后利用客户机访问网页、收发邮件、利用 FTP 上传下载文件,若都能正常访问,则代理成功。

本代理服务器脚本与网络拓扑结构无关,对于划分有多个 VLAN 的三层交换式网络也适用。此时需要在核心交换机上设置默认路由指向代理服务器,在三层交换式网络中,代理服务器通常在一个 VLAN 中,为了保证代理服务器能与其他 VLAN 中的主机通信,应在代理服务器上设置一条指向本 VLAN 网关的路由,假设代理服务器所在 VLAN 的网关为 192.168.252.1,则路由添加语句为:

```
route add -net 192.168.0.0 netmask 255.255.0.0 dev eth0 gw 192.168.252.1
```

可将该语句放在/etc/rc.d/rc.local 文件中,以便系统启动时能自动运行。

⑥ 设置开机自启动代理脚本。

为了实现在 Linux 服务器开机时,能自动运行代理脚本,以提供代理服务,可将代理的启动脚本加入到/etc/rc.d/rc.local 文件中,添加方法:

利用 vi 修改/etc/rc.d/rc.local 文件,在文件的最后添加: /etc/rc.d/init.d/adsl\_

proxy\_firewal。

若用户采用的是光纤直连或网通的宽带拨号或 DDN 上网方式,该脚本仍然适用,只需将配置语句/sbin/iptables -A FORWARD -m state --state NEW -i ! ppp+ -j ACCEPT 替换为:

```
/sbin/iptables -A FORWARD -m state --state NEW -i eth0 -j ACCEPT
```

将/sbin/iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE 替换为:

```
/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

另外还应注意设置外网接口卡的 IP 地址和默认网关。

利用该方法所实现的透明代理,不具备网页缓存功能。若要实现具备缓存功能的透明代理,则应安装 squid 缓存代理服务器,并结合使用端口重定向和网络地址转换来实现。

### 11.2.3 安装与配置 squid 缓存透明代理

squid 是一个高性能的具有网页缓存功能的代理服务器,支持 HTTP 和 FTP 协议的代理,squid 在缓存数据的同时,也缓存 DNS 查询结果,并支持 SSL 和访问控制,是 Linux 系统常用的一种代理服务器软件。对于 squid 无法代理的服务,可通过网络地址转换来实现,从而使透明代理服务器同时具有网页缓存的功能,从而加快对网页的访问速度。

假设某企业采用光纤和以太网接口连入 Internet 网,其网络拓扑结构如图 11.8 所示,外部网络接口卡的地址假设为 61.186.160.25,本节以此为例,介绍具有网页缓存功能的透明代理服务器的实现方法。对于采用 ADSL 拨号上网或其他网络拓扑结构,本代理服务器仍然适用,注意更改相应的外网卡设备名和 IP 地址。

#### 1. 检查是否安装 squid 软件包

```
[root@rh9 root]# rpm -q squid
package squid is not installed.
```

#### 2. 安装 squid 源代码软件包

squid 源代码软件包可从官方网站 <http://www.squid-cache.org> 下载。目前最新的稳定版下载地址为: <http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE6.tar.gz>。

```
[root@rh9 root]# cd /usr/local/src
[root@rh9 src]# wget http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE6.tar.gz
[root@rh9 src]# tar -zxvf squid-2.5.STABLE6.tar.gz
```

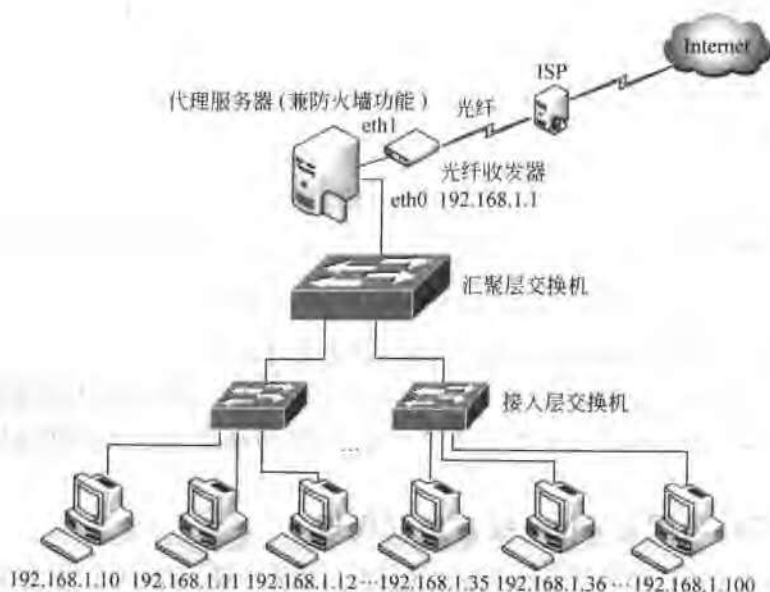


图 11.8 局域网光纤共享上网

```
[root@rh9 src]# cd squid-2.5.STABLE6
[root@rh9 squid-2.5.STABLE6]# ./configure --prefix=/usr/local/squid --enable-ssl \
> --enable-linux-netfilter
[root@rh9 squid-2.5.STABLE6]# make all
[root@rh9 squid-2.5.STABLE6]# make install
```

编译安装后,RunAccel、RunCache 和 squidclient 可执行文件位于/usr/local/squid/bin 目录中,squid 守护进程程序位于/usr/local/squid/sbin/目录中,squid.conf 是 squid 的配置文件,位于/usr/local/squid/etc 目录中。基于 Web 的 cache Manager 位于/usr/local/squid/libexec 目录中,可将 cachemgr.cgi 复制到 Web 站点的 cgi-bin 目录,实现用 Web 页面来管理缓存(cache)。

### 3. 修改配置文件,以支持透明代理

squid 功能十分强大,并支持访问控制(ACL)。squid 配置文件将各项配置都罗列了出来,并做了非常详细的配置说明,但各项配置都是注释了的,应编辑配置文件,开启并修改相应的配置项。

为了使 squid 支持透明代理,以下四项设置是关键,必须开启。

```
httpd_accel_host virtual #透明代理必须设置的项
httpd_accel_port 80 #squid 将请求重定向(中继)到的端口
```



```
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

http\_port 配置语句用于设置代理服务器监听客户 http 请求的地址和端口,默认使用的是 3128 端口。为了使代理服务器只监听内网口地址,该配置语句可修改如下:

```
http_port 192.168.1.1:3128
```

以后利用端口重定向功能,向客户端发出的所有对 80 端口的请求,都重定向到代理服务器监听的 3128 端口即可,其实现语句为:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-ports 3128
```

代理服务器的 squid 守护进程要以 root 用户身份来启动,为了安全起见,启动成功后,可切换到一个指定的用户身份来运行,通常采用 nobody 用户,这可利用配置文件中的以下配置命令来实现:

```
cache_effective_user nobody
cache_effective_group nobody
```

squid 的配置项相当多,根据各配置项的功能,划分为 13 段,通常情况下,除了个别配置项需要修改外,大多数配置项只需去掉前面的注释符,直接启用,使用其默认配置即可。

下面编辑修改配置文件,以便 squid 守护进程能正常启动。

```
[root@rh9 XXX]# vi /usr/local/squid/etc/squid.conf
# NETWORK OPTIONS(有关网络的选项)
http_port 192.168.1.1:3128           # squid 监听 http 客户请求的端口,默认为 3128
# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY                 # 定义不缓存查询
# OPTIONS WHICH AFFECT THE CACHE SIZE(定义 cache 大小的有关选项)
# 下面设置 squid 可使用内存的大小,默认为 8MB,可根据服务器内存情况,适当调大
cache_mem 200MB
cache_swap_low 90
cache_swap_high 95
maximum_object_size 4096KB
minimum_object_size 1KB
maximum_object_size_in_memory 8KB
ipcache_size 1024
ipcache_low 90
ipcache_high 95
```

```

fqdn_cache_size 1024
# LOGFILE PATHNAMES AND CACHE DIRECTORIES(定义日志文件路径及 cache 目录)
# cache_dir 用于指定 squid 用来存储对象的交换空间的大小及其目录结构。可以用多个 cache_
dir 命令来定义多个这样的交换空间,并且这些交换空间可分布不同的磁盘分区
# 下面设置交换空间的顶级目录为 /usr/local/squid/var/cache,允许使用 3000MB 空间,允许在该
目录下建立 16 个一级目录和 256 个二级目录
cache_dir ufs /usr/local/squid/var/cache 3000 16 256
# 下面指定日志文件,若不需要记录,可设置为 none,如: cache_access_log none
cache_access_log /usr/local/squid/var/logs/access.log      # 设置客户请求的记录日志文件
cache_log /usr/local/squid/var/logs/cache.log              # squid 一般信息日志文件
cache_store_log /usr/local/squid/var/logs/store.log        # 指定记录对象存储的日志文件
mime_table /usr/local/squid/etc/mime.conf
pid_filename /usr/local/squid/var/logs/squid.pid           # 指定保存 squid 进程号的文件
# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS(外部支持程序选项)
ftp_user Squid@
ftp_list_width 32
ftp_passive on
ftp_sanitycheck on
ftp_telnet_protocol on
unlinkd_program /usr/local/squid/libexec/unlinkd
# OPTIONS FOR TURNING THE CACHE(调整 cache 的选项)
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320
quick_abort_min 16KB
quick_abort_max 16KB
quick_abort_pct 95
negative_ttl 5 minutes
positive_dns_ttl 6 hours
negative_dns_ttl 1 minute
range_offset_limit 0KB
# TIMEOUTS(超时)
forward_timeout 4 minutes
connect_timeout 1 minute
peer_connect_timeout 30 seconds
read_timeout 15 minutes
request_timeout 5 minutes      # 建立连接后, squid 花多长时间等待客户发出 http 请求
persistent_request_timeout 1 minute
client_lifetime 60 minutes     # 设置连接可以保持多长时间,默认为 1 day

```

```

half_closed_clients off           # 默认为 on, 此处设置为 off, 不允许半连接
pronn_timeout 120 seconds         # squid 与其他服务器建立连接后, 闲置多长时间后被关闭
ident_timeout 10 seconds          # 等待用户认证请求的时间
shutdown_lifetime 30 seconds
# ACCESS CONTROLS(访问控制)
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80             # http
acl Safe_ports port 21             # ftp
acl Safe_ports port 443 563        # https, suews
acl Safe_ports port 70             # gopher
acl Safe_ports port 210            # wais
acl Safe_ports port 1025-65535     # unregistered ports
acl Safe_ports port 280            # http-mgmt
acl Safe_ports port 188            # gss-http
acl Safe_ports port 591            # filemaker
acl Safe_ports port 777            # multiling http
acl CONNECT method CONNECT
# Recommended minimum configuration;
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to unknown ports
http_access deny ! Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
http_access deny to_localhost
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
# acl our_networks src 192.168.1.0/24 192.168.2.0/24
acl our_networks src 192.168.0.0/16           # 定义网络对象
http_access allow our_networks                # 允许该网络访问代理服务器
# And finally deny all other access to this proxy
http_access deny all                          # 设置访问策略为拒绝
# Allow replies to client requests. Recommended minimum configuration:
#
# Insert your own rules here.

```

```

#
# and finally allow by default
http_reply_access allow all
icp_access deny all
# ADMINISTRATIVE PARAMETERS(管理参数)
cache_mgr webmaster           # 设置管理员邮件地址
cache_effective_user nobody   # 设置 squid 守护进程启动后以 nobody 用户身份运行
cache_effective_group nobody
visible_hostname rh9          # 定义在返回给用户的出错信息中的主机名
# OPTIONS FOR THE CACHE REGISTRATION SERVICE(cache 注册服务选项)
# HTTPD-ACCELERATOR OPTIONS(HTTPD 加速选项)
# 以下前四项是设置 squid 为透明代理的关键
httpd_accel_host virtual      # 透明代理必须设置的项
httpd_accel_port 80           # squid 将请求重定向(中继)到的端口
httpd_accel_with_proxy on     # 透明代理必须设置的项
httpd_accel_uses_host_header on
httpd_accel_single_host on
# MISCELLANEOUS(杂项)
logfile_rotate 10
# DELAY POOL PARAMETERS(延时池参数)
# Note: This option is only available if Squid is rebuilt with the
#      --enable-delay-pools option

```

修改完毕后保存配置文件。

#### 4. 创建 cache 目录,并设置属主

```
[root@rh9 squid]# mkdir /usr/local/squid/var/cache
```

squid 进程以 root 用户身份启动后,将切换到配置文件指定的 nobody 用户身份运行。为了使 nobody 用户能对 cache 目录和 /usr/local/squid/var/logs 日志存放目录有读、写操作权限,为此需设置 logs 目录和 cache 目录的属主为 nobody 用户,其设置命令为:

```

[root@rh9 squid]# chown nobody.nobody /usr/local/squid/var/cache
[root@rh9 squid]# chown nobody.nobody /usr/local/squid/var/logs

```

squid 的日志文件保存在 /usr/local/squid/var/logs 目录中。

#### 5. 创建 cache 交换目录

在启动 squid 进程之前,应使用“squid -z”命令对 cache 目录进行初始化,以在 cache

目录中创建出 16 个一级目录(00~0F)和 256 个二级目录(00~FF)。

```
[root@rh9 squid]# /usr/local/squid/sbin/squid -z
2004/09/20 16:00:23| Creating Swap Directories
```

## 6. 启动 squid 进程

```
[root@rh9 squid]# /usr/local/squid/bin/RunCache &
[root@rh9 squid]# ps ax                                # 查看进程
```

在进程列表中,应该可以看到以下 3 个进程:

```
20388    tty1      S    0:00 /bin/sh . RunCache
20391    tty1      S    0:01 [squid]
20394    ?          S    0:00 (unlinkd)
```

```
[root@rh9 squid]# netstat -ln                                # 查看相应端口是否在监听
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:3128	0.0.0.0:*	LISTEN
udp	0	0	0.0.0.0:3130	0.0.0.0:*	

squid 默认监听客户代理请求的 TCP 端口是 3128,相关的 UDP 端口为 3130。只要 3128 端口处理 LISTEN 状态,则说明 squid 进程启动成功,代理服务器可以接受代理请求了。

也可通过查看 /usr/local/squid/var/logs/cache.log 日志和 /usr/local/squid/var/squid.out 文件,来了解代理服务器的启动和运行情况。若在启动过程中有什么错误,可通过查看 cache.log 日志来了解出错原因。

## 7. 设置防火墙规则

squid 进程启动后,监听客户端 http 请求的端口是 3128,而客户发起的 http 请求的端口是 80,因此,需要利用端口重定向将所有对 80 端口的请求,重定向到 3128 端口。如不考虑安全,对于 squid 代理服务器,只需运行以下两条规则即可。

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-ports 3128
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

下面在 /etc/rc.d/init.d/ 目录中编写代理的防火墙脚本 squid\_proxy\_firewall。

```
[root@rh9 root]# vi /etc/rc.d/init.d/squid_proxy_firewall
#!/bin/sh
echo "Starting squid proxy iptables rules..."
# 开启 IP 包转发功能
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```

# 开启动态 IP 支持
echo 1 > /proc/sys/net/ipv4/ip_dynaddr
# 关闭 Explicit Congestion Notification
echo 0 > /proc/sys/net/ipv4/tcp_ecn
# 开启 syn 泛洪攻击保护 (SYN Cook Flood)
# syn 攻击利用 TCP 协议缺陷, 发送大量伪造的 TCP 连接请求, 使被攻击方资源耗尽, 导致拒绝
# 服务
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
# Ignore any broadcast icmp echo requests
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
# 装载内核支持模块
/sbin/modprobe ip_tables
/sbin/modprobe iptable_nat
/sbin/modprobe iptable_filter
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ipt_MASQUERADE
/sbin/modprobe ipt_state
/sbin/modprobe ipt_multiport
# 清除链的规则
/sbin/iptables -F
/sbin/iptables -t nat -F
# 清除封包计数器
/sbin/iptables -Z
/sbin/iptables -t nat -Z
# 设置默认策略
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT DROP
# 允许本地连接
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
# 禁止对 135、137、138、139 和 445 端口的连接请求
/sbin/iptables -A FORWARD -p tcp -m multiport --dport 135,137,138,139,445 -j DROP
# 允许 squid 进程向外发起对 80 端口的代理请求
/sbin/iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
# 允许接收 squid 进程对外请求的回应包
/sbin/iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
# 允许 DNS 查询
/sbin/iptables -A OUTPUT -p udp --dport 53 -j ACCEPT

```

```

/sbin/iptables -A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
# 允许 ping 代理
/sbin/iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s --limit-burst 10
-j ACCEPT
/sbin/iptables -A OUTPUT -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
# 允许转发对已经建立的连接的回应, 允许建立在已建立连接基础上的新连接, 如 ftp-data
/sbin/iptables -A FORWARD -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
# 允许转发由内向外的新连接
/sbin/iptables -A FORWARD -p tcp -i eth0 --syn -j ACCEPT
# /sbin/iptables -A FORWARD -m state --state NEW -i eth0 -j ACCEPT
# 将对 80 端口的请求重定向到代理监听的 3128 端口
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-ports 3128
# 对于非 80 端口的请求, 利用 IP 伪装方式代理访问 Internet
/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

```

保存文件, 然后设置为可执行文件。

## 8. 设置代理脚本为可执行文件

```
[root@rh9 root]# chmod 755 /etc/rc.d/init.d/squid_proxy_firewall
```

## 9. 启动 squid 代理服务

```

[root@rh9 root]# /usr/local/squid/bin/RunCache &      # 启动 squid 代理守护进程
[root@rh9 root]# /etc/rc.d/init.d/squid_proxy_firewall # 启动防火墙规则

```

此时代理服务器就可正常工作了。

### 11.2.4 squid 的配置命令

要使 squid 代理服务器工作在最优状态, 就必须了解和掌握 squid 配置命令的功能与用法, 以配置出适合自己的最佳配置文件。本节将介绍一些常用配置选项的功能与用法。

#### 1. 有关网络的选项

##### (1) http\_port

用法: http\_port port 或 http\_port IP 地址:port

功能: 指定 squid 代理进程监听客户端 http 请求的端口号, 默认使用 3128, 用户也可自行指定, 另外还可同时指定所监听的 IP 地址。

比如: 若代理服务器内网卡地址为 192.168.1.1, 则配置命令通常为:

```
http_port 192.168.1.1:3128
```

### (2) https\_port

用于指定监听客户端 https 请求的端口号。必须使用“--enable-ssl”配置参数编译 squid 才能支持该功能。

### (3) icp\_port

用法: icp\_port port

功能: 用于指定 squid 与其他相邻缓存服务器之间发送和接收 ICP 查询时所监听的端口号, 默认使用 3130。

### (4) htcp\_port

用法: htcp\_port port

功能: 指定 squid 同其他相邻缓存服务器之间发送和接收 HTCP 查询时所监听的端口, 默认使用 4827。该功能要求使用“--enable-htcp”配置参数编译 squid 才能支持。

### (5) udp\_incoming\_address 与 udp\_outgoing\_address

udp\_incoming\_address 为 ICP 套接字指定接收来自其他 squid 代理服务器的包的 IP 地址, 默认配置为 udp\_incoming\_address 0.0.0.0。

udp\_outgoing\_address 为 ICP 套接字指定向其他 squid 代理服务器发送包的 IP 地址, 默认为 udp\_outgoing\_address 255.255.255.255。

绑定的地址可使用 IP 指定, 也可以用完整的域名来指定。

## 2. OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM

### (1) cache\_peer

用法: cache\_peer hostname type http\_port icp\_port options

功能: 用于指定网络中的其他缓存服务器, 默认值为 none。

参数说明:

hostname 为要指定的其他缓存服务器的 IP 地址或主机名。

type 代表该缓存服务器同当前 squid 服务器之间的关系类型。其类型可以是 parent、sibling(对等或同级)或 multicast。

http\_port 代表该缓存服务器监听客户端 http 请求的端口, 默认为 3128。

icp\_port 为该缓存服务器 ICP 查询所使用的端口, 默认为 3130。

options 用于指定一个功能选项, 对于代理, 通常使用的是 proxy-only。

例如, 若要指定一个与当前 squid 代理服务器同级的另一个缓存代理服务器, 其 IP 地址为 61.186.160.240, 则配置命令为 cache\_peer 61.186.160.240 sibling 3128 3130 [proxy-only]。

### (2) cache\_peer\_domain

用法: cache\_peer\_domain cache-host domain

功能: 用于限制查询相邻的缓存服务器的域, 默认为 none。



### (3) icp\_query\_timeout

用于设置一个 ICP 查询超时的时间,单位为 msec(毫秒),若要设置超时时间为 2 秒,则设置命令为 icp\_query\_timeout 2000。

### (4) dead\_peer\_timeout

用于设置等待多长时间(单位为秒),若一个对等的缓存服务器没有响应,则宣布其死亡,默认值为 10 秒。

### (5) no\_cache

用法: no\_cache deny | allow aclname

功能: 用于设置指定的对象不被记录到缓存中去。

推荐的配置:

```
acl QUERY urlpath_regex cgi-bin \?  
no_cache deny QUERY
```

## 3. 定义 cache 大小的有关选项

### (1) cache\_mem

用于指定 squid 可以使用的内存大小,这部分内存被用来存储以下对象:

In-Transit objects(传入的对象)

Hot Objects(热对象,即用户常访问的对象)

Negative-Cached objects(消极存储的对象)

系统默认使用 8MB,可根据代理服务器所配置内存的大小,适当调高允许使用的内存值。该配置项只是定义了 squid 所使用的内存的一个方面, squid 还会在其他方面使用内存。

假如代理服务器拥有 1GB 的内存,需要将 cache-mem 设置为 300MB,则配置命令为:

```
cache_mem 300MB
```

### (2) cache\_swap\_low 与 cache\_swap\_high

squid 使用大量的交换空间来缓存对象,使用一段时间后,交换空间就会被用完,因此必须定期清除过期的对象,以释放交换空间。

cache\_swap\_low 和 cache\_swap\_high 使用百分比来设置,默认值分别为 90% 和 95%。即当使用的交换空间达到总交换空间的 95% 时,就开始释放过期对象,一直到使用的交换空间降至 cache\_swap\_low 规定的 90% 为止。

### (3) maximum\_object\_size

用于设置大于该配置项指定的值的对象,将不会被保存到硬盘缓存中。默认为

4MB,其配置命令为 `maximum_object_size 4096KB`。

(4) `minimum_object_size`

用于设置小于该配置项指定的值的对象,将不会被保存到硬盘缓存中。默认为 1KB,其配置命令为 `minimum_object_size 1KB`。

(5) `maximum_object_size_in_memory`

用于设置大于该配置项指定的值的对象,将不会被保存到内存缓存中。默认为 8KB。其配置命令为 `maximum_object_size_in_memory 8KB`。

#### 4. 日志与缓存目录

(1) `cache_dir`

命令用法: `cache_dir type Directory-Name Mbytes Level1 Level2`

命令功能: 指定 squid 用来存储对象的交换空间的大小及其目录结构。可以使用多个 `cache_dir` 命令来定义多个这样的交换空间,并且这些交换空间可分布在不同的磁盘分区。

参数说明:

`type` 用于指定缓存交换空间的文件系统类型,默认使用 `ufs`。

`Directory-Name` 用于指定交换空间顶级目录的路径。

`Mbytes` 指定交换空间的大小,单位为 MB,默认为 100MB。

`Level1` 用于指定在交换空间的顶级目录下允许创建多少个一级子目录,`Level2` 用于指定在每一个一级子目录下,允许创建多少个二级子目录。

若要设置交换空间顶层目录为 `/usr/local/squid/var/cache`,允许使用的磁盘交换空间大小为 3000MB,允许 16 个一级子目录,256 个二级子目录,则配置命令为:

```
cache_dir ufs /usr/local/squid/var/cache 3000 16 256
```

如果要使用一个磁盘或一个磁盘分区来作为交换空间,可将该分区或磁盘挂载到交换空间的顶级目录下即可。

(2) `cache_access_log`

用于设置记录客户请求(HTTP 请求或来自邻居缓存服务器的 ICP 请求)的日志文件的路径及日志文件名。默认配置为 `cache_access_log /usr/local/squid/var/logs/access.log`。

若不记录该类日志,则配置语句为 `cache_access_log none`。

(3) `cache_log`

用于设置 squid 产生的一般信息的日志文件名及路径。默认配置为:

```
cache_log /usr/local/squid/var/logs/cache.log
```

通过该日志文件,可了解代理服务器的启动和运行情况。

#### (4) cache\_store\_log

用于设置记录对象存储情况的日志文件名及路径。在该日志文件中,记录有哪些对象被写到交换空间,哪些对象被从交换空间清除等信息。默认配置为:

```
cache_store_log /usr/local/squid/var/logs/store.log
```

#### (5) mime\_table

用于指定存储 squid 支持的 MIME 类型的文件。mime.conf 文件保存在 /usr/local/squid/etc/ 目录中,其配置应设置为 mime\_table /usr/local/squid/etc/mime.conf。

#### (6) pid\_filename

用于指定保存 squid 进程号的文件名及路径。默认配置为:

```
pid_filename /usr/local/squid/var/logs/squid.pid
```

#### (7) debug\_options

用于设置日志记录的范围和详细程序。默认配置为 debug\_options ALL,1。

ALL 表示对每一方面都做记录,1 代表日志记录的详细程度为最低,最高为 9,此时将产生很大的日志文件。

#### (8) log\_fqdn

命令用法: log\_fqdn on | off

用于控制在 access.log 日志文件中,对用户地址的记录方式。若设置为 on,则记录用户的完整域名,此时将增加代理服务器的负荷,为了获得完整域名,代理服务器将进行 DNS 反向查询。若设置为 off,则只记录客户端的 IP 地址。默认配置为 log\_fqdn off。

### 5. 外部支持程序选项

#### (1) ftp\_user

设置匿名登录 FTP 服务器时,所提供的电子邮件地址。默认配置为 ftp\_user Squid@。

#### (2) ftp\_list\_width

设置 ftp 列表时的显示宽度。若设置太小,将无法浏览到长文件名。默认配置为:

```
ftp_list_width 32
```

#### (3) ftp\_passive

命令用法: ftp\_passive on | off

设置是否允许 squid 采用被动方式连接 FTP 服务器,设置为 on,则允许;设置为 off,则不允许。默认配置为 ftp\_passive on。

#### (4) cache\_dns\_program

该配置项用于设置 DNS 查询程序的完整路径。该配置项仅在采用了“--disable-internal-dns”配置参数编译 squid 时才有效。默认配置为：

```
cache_dns_program /usr/local/squid/libexec/dnsserver
```

#### (5) dns\_children

该配置项也仅在使用“--disable-internal-dns”配置参数编译 squid 时才有效。用于设置允许的 DNS 查询程序的进程数。默认为 5 个,建议设置为 10~32。squid 主进程需要等待域名查询的结果才能进行后续的操作,减少了允许的 DNS 查询进程,会影响 DNS 查询速度,从而进一步影响到 squid 的效率。

#### (6) dns\_timeout

用于设置 DNS 查询超时的时间,默认为 2 分钟,其配置为 dns\_timeout 2 minutes。

#### (7) dns\_nameservers

命令用法: dns\_nameservers DNS1 DNS2 ...

设置用于域名解析的 DNS 服务器的地址。启用该配置项后, squid 将不再从/etc/resolv.conf 配置文件中获得 DNS 服务器列表。若未启用该配置,则从/etc/resolv.conf 配置文件中获得 DNS 服务器的地址。

#### (8) unlinkd\_program

用于指定文件删除进程(unlinkd)的路径。unlinkd 文件位于/usr/local/squid/libexec/目录中,因此相应的配置应为 unlinkd\_program /usr/local/squid/libexec/unlinkd。

#### (9) pinger\_program

该配置项仅在使用“--enable-icmp”配置参数编译 squid 时才有效。用于指定 pinger 进程的完整路径,该进程被 squid 利用来测量与其他邻居的路由距离。相应的配置命令为:

```
pinger_program /usr/local/squid/libexec/pinger
```

### 6. cache 调整配置选项

#### (1) request\_header\_max\_size

用于指定一个 HTTP 请求数据报中,包头的最大长度。默认为 10KB,其配置命令为:

```
request_header_max_size 10KB
```

#### (2) request\_body\_max\_size

用于指定 HTTP 请求数据报中,数据段的最大长度。默认设置为 0KB,表示不受限制,其配置命令为 request\_body\_max\_size 0KB。

### (3) refresh\_pattern

该配置项用于设置清除缓存中过期对象的方法。配置文件推荐的设置为：

```
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%       1140
refresh_pattern .              0         20%      4320
```

### (4) quick\_abort\_min、quick\_abort\_max 与 quick\_abort\_pct

该组配置用于控制 squid 是否继续传输被用户中断的请求。

当用户中断请求时, squid 将检测 quick\_abort\_min 的值。如果剩余部分小于配置项 quick\_abort\_min 指定的值, 则 squid 将继续完成剩余部分的传输, 并将其保存在缓存中; 如果剩余部分大于 quick\_abort\_max 指定的值, 则 squid 将终止剩余部分的传输; 如果已完成配置项 quick\_abort\_pct 指定的百分比, 则 squid 将继续完成剩余部分的传输。默认配置为:

```
quick_abort_min 16KB
quick_abort_max 16KB
quick_abort_pct 95
```

### (5) negative\_ttl

命令用法: negative\_ttl time-units

用于设置消极存储对象的生存时间。消极存储对象是指“连接被拒绝”及“404 Not Found”等错误信息。默认设置为 5 分钟, 配置命令为 negative\_ttl 5 minutes。

### (6) positive\_dns\_ttl

命令用法: positive\_dns\_ttl time-units

设置缓存成功的 DNS 查询结果的生存时间, 默认为 6 小时, 其配置命令为:

```
positive_dns_ttl 6 hours
```

### (7) negative\_dns\_ttl

设置缓存失败的 DNS 查询结果的生存时间, 默认为 1 分钟, 其配置命令为:

```
negative_dns_ttl 1 minute
```

建议设置值不应低于 10 秒。

## 7. 超时设置

### (1) connect\_timeout

用于设置 squid 等待连接完成的超时值, 默认为 1 分钟, 其配置命令为:

```
connect_timeout 1 minute
```

## (2) peer\_connect\_timeout

用于设置连接其他缓存服务器的超时值,默认为 30 秒,其配置命令为:

```
peer_connect_timeout 30 seconds
```

## (3) read\_timeout

如果客户在指定的时间内,未从 squid 服务器读取任何数据,则 squid 将终止该客户的请求,默认为 15 分钟,其配置命令为 read\_timeout 15 minutes。

## (4) request\_timeout

设置 squid 与客户端建立连接后,squid 等待客户发出 HTTP 请求的超时时间,默认为 5 分钟,其配置命令为 request\_timeout 5 minutes。

## (5) persistent\_request\_timeout

在前一个连接请求完成后,在同一个连接上等待下一个新的 HTTP 请求的超时时间。默认设置为 1 分钟,其配置命令为 persistent\_request\_timeout 1 minute。

## (6) client\_lifetime

该配置项用于设置客户在与 squid 建立连接后,可以将该连接保持多长时间。默认值为 1 天。由于建立连接会消耗一定的系统资源,当连接数较多时又得不到及时释放时,将会消耗大量的系统资源,因此应适当调小该设置值。若要设置为 2 小时,则配置命令为:

```
client_lifetime 2 hours
```

或 client\_lifetime 120 minutes

## (7) half\_closed\_clients

命令用法: half\_closed\_clients on ; off

该配置项用于设置是否允许 TCP 半连接。默认为 on 允许,强烈建议更改为 off,不允许半连接,此时系统会立即断开可能的半连接,相应的配置命令为 half\_closed\_clients off。

在 TCP 连接的三次握手过程中,如果一个客户端在向服务器发送 SYN 报文后突然死机或掉线,则服务器在发出 SYN+ACK 应答报文后,将无法收到客户端的 ACK 应答报文,第三次握手将无法完成,此时的状态通常也称为半连接。根据 TCP 协议的规定,此时服务器将会重试(再次发送 SYN+ACK 给客户端)并等待一段时间,这个等待的时间就是 SYN 超时时间(Timeout),一般为 30 秒~2 分钟,如果重试几次均无法收到客户端的 ACK 应答报文,服务器就会丢弃这个未完成的 TCP 连接。

少量的半连接不会对服务器造成影响,但如果一个恶意的攻击者成千上万的大量模拟半连接,服务器端就会消耗大量的资源,并常常可能导致 TCP/IP 堆栈溢出而导致系统崩溃,或使服务器因忙于处理攻击者伪造的大量 TCP 连接请求,而无法响应客户端的正

常请求,从而出现拒绝服务现象,这就是通常所说的 SYN 洪水攻击,其破坏性极强,应予以防范。

#### (8) pconn\_timeout

用于设置 squid 在与其他服务器和代理建立连接后,该连接闲置多长时间后被关闭,默认为 120 秒,其配置命令为 pconn\_timeout 120 seconds。

#### (9) ident\_timeout

设置 squid 等待用户认证请求的超时时间,默认为 10 秒,其配置命令为:

```
ident_timeout 10 seconds
```

#### (10) shutdown\_lifetime

当收到 SIGTERM 或者 SIGHUP 信号后, squid 将进入一种 shutdown pending 的模式,等待所有活动的套接字关闭。在过了 shutdown\_lifetime 所指定的时间后,所有仍活动的用户都将收到一个超时信息。默认为 30 秒,其配置命令为:

```
shutdown_lifetime 30 seconds
```

## 8. 访问控制列表

### (1) acl

命令功能: 定义访问控制列表。

命令用法: acl aclname acltype string1 ...

参数说明: acltype 用于指定 acl 的类型,可使用的类型较多,常用的主要是 src、dst、port、proto、time 和 method 等。

① src 用于指定源地址,其表达方法有以下两种:

指定一个 IP 地址: acl aclname src ip-address/netmask

指定一个 IP 地址范围: acl aclname src addr1-addr2/netmask

② dst 用于指定客户请求的服务器的 IP 地址,即目的地址,指定方法为:

```
acl aclname dst ip-address/netmask
```

③ port 用于指定所访问的端口,其指定方法为:

指定某一个端口: acl aclname port port\_no

指定不连续的多个端口: acl aclname port port\_no1 port\_no2 ...

指定连续的多个端口: acl aclname port port\_begin-port\_end

④ proto 用于指定所访问的协议,多个协议间用空格分隔,其指定方法为:

```
acl aclname proto HTTP FTP ...
```

⑤ time 用于指定访问的时间,定义语法为:

```
acl aclname time [day-abbrevs] [hh:mm1-hh2:mm2]
```

day-abbrevs 参数项可使用的值有：

```
S - Sunday
M - Monday
T - Tuesday
W - Wednesday
H - Thursday
F - Friday
S - Saturday
```

[hh1:mm1-hh2:mm2]用于指定访问的时间段, hh1:mm1 必须小于 hh2:mm2。

若要定义一个名为 acltime 的访问控制列表,其时间段为星期一的上午 9 点至下午 5 点,则定义方法为:

```
acl acltime time M 9:00-17:00
```

⑥ method 用于设置用户请求的方法。设置方法为:

```
acl aclname method GET POST ...
```

配置文件中推荐的最小访问控制列表定义如下:

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70         # gopher
acl Safe_ports port 210        # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
acl CONNECT method CONNECT
```

## (2) http\_access

用于根据访问控制列表允许或禁止某一类用户访问代理服务器。其用法为:



```
http_access deny ! allow aclname
```

deny 表示拒绝 aclname 指定的用户访问代理, allow 表示允许 aclname 指定的用户访问代理。比如, 若要允许所有用户访问代理服务器, 则实现命令为 http\_access allow all。

通常可先设置允许访问的用户, 最后再通过执行 http\_access deny all 来禁止其他用户对代理的访问。

若要允许 192.168.0.0/16 网络中的用户访问代理服务器, 则实现的访问控制命令为:

```
acl our_networks src 192.168.0.0/16
http_access allow our_networks
http_access deny all
```

## 9. 管理参数

### (1) cache\_mgr

设置管理员的邮件地址, 默认为 webmaster, 相应的配置命令为:

```
cache_mgr webmaster
```

### (2) cache\_effective\_user 与 cache\_effective\_group

该组配置命令用于设置 squid 启动后, 以何用户身份运行。通常设置为 nobody 用户, 其配置命令为:

```
cache_effective_user nobody
cache_effective_group nobody
```

### (3) visible\_hostname

用于定义在返回给用户的出错信息中所显示的主机名。配置命令为:

```
visible_hostname rh9
```

## 10. HTTPD 加速选项

### (1) httpd\_accel\_host 与 httpd\_accel\_port

httpd\_accel\_host 用于定义 squid 加速模式, 对于透明代理, 应设置为 virtual, 即虚拟主机加速模式。httpd\_accel\_port 用于定义要加速的请求端口, 通常应设置为 80 端口。对于 squid 透明代理, 这两项应配置为:

```
httpd_accel_host virtual
httpd_accel_port 80
```

## (2) httpd\_accel\_with\_proxy

对于 squid 透明代理,必须设置为 on,在该模式下,squid 既是 Web 请求的加速器,又是缓存代理服务器。其配置为 httpd\_accel\_with\_proxy on。

## (3) httpd\_accel\_uses\_host\_header

在透明代理模式下,为了使代理服务器的缓存功能正常工作,必须将该配置设置为 on,其配置为 httpd\_accel\_uses\_host\_header on。

## 11.3 端口扫描与数据包捕获

### 11.3.1 端口与端口扫描工具

#### 1. 端口

端口分为 TCP 端口和 UDP 端口,每类端口中,允许使用的端口总数是 64K,即 0~65535,TCP 端口通常用于建立连接,UDP 端口通常用于数据传输。端口号在 1024 以下的一般为系统所保留,分配给各服务程序使用。客户端程序连接服务程序时,一般从 1024 及以上端口中随机选择一个未用的端口,来与服务程序的特定端口建立连接,并实现通信。

服务程序为了监听客户端的请求,通常会使用某个特定的 TCP 端口来监听客户的请求,同时还可能使用一个或多个 UDP 端口来传输数据。常用服务程序所监听的 TCP 端口和所使用的 UDP 端口如表 11.2 所示。

表 11.2 常用服务程序的 TCP 和 UDP 端口

服务程序	TCP 端口	UDP 端口	说 明
	135		用于启动与远程计算机的 RPC 连接。与 Linux/UNIX 的 111 端口功能相似
	137	137	netbios-ns。用于计算机的名称或 IP 查询服务。NetBIOS 服务一般是通过 137 和 138 端口实现的
	138	138	netbios-dgm。提供 NetBIOS 环境下的计算机名浏览功能
	139	139	netbios-ssn。实现通过网上邻居访问局域网中的共享文件或共享打印机以及 Samba 服务
	445		microsoft-ds。与 139 端口功能相同。139 端口是基于 SMB 协议(服务器协议族)对外提供共享服务;445 是基于 CIFS 协议(common internet file system),即通用因特网文件系统协议来提供共享服务的

续表

服务程序	TCP 端口	UDP 端口	说 明
FTP	21,20		21 用于建立命令通道连接,20 用于建立数据通道连接
SSH	22		用于建立安全的远程登录连接
Telnet	23		用于建立远程登录连接
DNS	53	53	提供域名解析服务
DHCP Server	67	67	DHCP/Bootstrap Protocol Server
DHCP Client	68	68	DHCP/Bootstrap Protocol Client
tftp	69	69	Trivial File Transfer
http	80		提供 WWW 服务
https	443		提供安全的 HTTP 连接
Tomcat	8080		提供 WWW 服务,是 JSP 的 Web Server,默认使用 8080
SMTP	25		提供 SMTP 服务
POP3	110		提供 POP3 服务
IMAP	143		提供 Internet 消息访问服务,可实现有选择性地从邮件服务器接收邮件,目前使用的是 IMAP4
SMTPS	465		提供安全的 SMTP 服务,传输的邮件数据会加密传输
POP3S	995		提供安全的 POP3 服务
IMAPS	993		提供安全的 IMAP 服务
mysql	3306		提供 MySQL 数据库服务
PostgreSQL	5432		提供 PostgreSQL 数据库服务
SQL Server	1433	1433	Microsoft SQL Server
	1434	1434	Microsoft SQL Monitor
squid	3128		squid 代理默认使用 3128 端口
远 程 桌 面 连接	3389		Windows 2000、Windows XP 的远程桌面连接程序默认使用
MSN	1863		服务器域名:gateway.messenger.hotmail.com
QQ	80 或 443		服务器:tcpconn.tencent.com 或 tcpconn2.tencent.com
BT 下载	6881~6890		

## 2. 端口扫描工具

任何服务程序都会绑定在某一端口上提供服务,为了检查计算机当前有哪些端口正处于监听服务状态,可使用端口扫描工具来实现,这样可及时发现一些不正常的服务程序,如常见的“木马”类程序。

Linux 下常用的端口扫描工具是 nmap(network mapper),其最新的 RPM 安装包或源代码包可从 <http://www.insecure.org/nmap/> 网站下载安装,目前最新的版本是 3.7。

### (1) 安装 nmap

在 Red Hat Linux 9 的第 2 张安装光盘中,提供有 3.0 版的 RPM 安装包。

```
[root@rh9 root]# rpm -ivh nmap-3.00-4.i386.rpm
```

安装后,可执行程序 nmap 位于 /usr/bin 目录中。

### (2) nmap 命令

命令用法: nmap [scantype] [option] <host or net>

命令功能: 扫描和嗅探指定的主机或指定网络中的主机所开放的端口和所提供的服务。

参数说明:

scantype 用于指定扫描的类型,常用的类型有以下几种:

-sT 扫描 TCP 端口,此为默认扫描方式。

-sS 进行 TCP 隐蔽性扫描,以防止被目标主机检测到。此方式需要用户拥有 root 权限才能运行。若目标主机安装了过滤和日志软件来检测 SYN 标志,此时-sS 的隐蔽作用就会失效,此时可采用更隐蔽的-sF(FIN)、-sX(Xmas)或-sN(Null)方式来扫描。

-sU 扫描 UDP 端口。

-sP 进行 ping 扫描,以发现任何可到达的主机。

常用的 option 功能选项有以下几种:

-O 推测目标主机的操作系统类型。

-oN file 将扫描结果保存到指定的 file 文件中。

-p 指定要扫描的端口范围。例如: -p 21-80,1080,3128,8080。

-F 只扫描 /usr/share/nmap/nmap-services 文件中列出的端口。

-v 显示更详细的扫描内容。若连用两次,即“-v -v”,将显示更为详细的内容。

要扫描的主机或网络的表达方法:

多个主机之间以及主机与网络之间用空格进行分隔,网络可采用“网络地址/子网掩码中为 1 的个数”方式进行表达,如 192.168.0.0/16。同一网段的多台主机可采用“202.186.100.10-60”方式表达。多个网络可采用‘192.88-90.\*.\*’方式表达,例如:

```
nmap -v -sS -O 192.168.0.0/16 202.186.100.10-60 '192.88-90.*.*'
```

### (3) nmap 用法示例

若要扫描检查当前计算机所开放的端口和提供的服务,则扫描命令为:

```
[root@rh9 root]# nmap -O localhost
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on rh9 (127.0.0.1):
(The 1590 ports scanned but not shown below are in state: closed)
Port      States      Service
22/tcp    open       ssh
25/tcp    open       smtp
80/tcp    open       http
110/tcp   open       pop3
111/tcp   open       sunrpc
631/tcp   open       ipp
873       open       rsync
1024      open       kdm
1025      open       NFS-or-IIS
3306      open       mysql
8080      open       http-proxy

Remote operating system guess: Linux Kernel 2.4.0-2.5.20
Uptime 0.046 days (since Sat Oct 9 20:20:44 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
```

## 11.3.2 tcpdump 数据包捕获命令

tcpdump 可用于捕获指定或全部网络接口卡进出的所有封包,以便于对数据包进行分析。其命令用法为:

```
tcpdump [-adeflnNOPqRStuvxX] [-c count] [-C file_size] [-F file] [-i interface] [-r file]
        [-s snaplen] [-T type] [-w file] [expression]
```

### 1. 功能选项

- a 将网络地址和广播地址转变成名字。
- d 将匹配数据包的内容以易理解的汇编格式输出。
- dd 将匹配数据包的内容以 C 语言程序段的格式输出。
- ddd 将匹配数据包的内容以十进制形式输出。
- e 在输出行打印出数据链路层的头部信息。
- f 将外部的 Internet 地址以数字形式打印输出。
- l 使标准输出变为缓冲行形式。
- n 不把网络地址转换成名字。

-t 在输出的每一行不打印时间戳。  
-v 输出较详细的信息。  
-vv 输出详细的报文信息。  
-c 指定要接收的数据包的数量。接收到的数量达到后, tcpdump 就会停止接收。  
-F 从指定的文件中读取表达式, 忽略其他的表达式。  
-i 指定要监听的网络接口。  
-r 从指定的文件中读取数据包。这些包是通过 -w 选项保存得到的。  
-w 直接将数据包写入指定的文件中, 不分析和打印输出。  
-T 将监听到的包直接解释为指定类型的报文, 常用的类型有 rpc(远程过程调用)和 snmp(简单网络管理协议)。

## 2. 表达式

tcpdump 使用正则表达式来作为过滤报文的条件, 并可使用指定数据包类型、传输方向和协议的关键字, 来构造表达包过滤条件。若条件满足, 则捕获该报文。若未指定条件, 则捕获所有进出的数据包。

tcpdump 捕获的是运行 tcpdump 命令的主机上进出的数据包, 通常在代理服务器上运行该命令, 以捕获局域网内各主机通信的数据包。

### (1) 包类型关键字

包类型关键字有 host、net 和 port。host 用于表达一台主机, net 用于表达一个网络地址, port 用于指定端口号。若表达式缺省该类型的关键字, 则默认为 host。

例如, 若要捕获源和目的地址为 192.168.168.155 的所有数据包, 则实现命令为:

```
tcpdump host 192.168.168.155
```

若要捕获所有源和目的端口为 80 的所有数据包, 则实现命令为:

```
tcpdump tcp port 80
```

### (2) 确定传输方向的关键字

确定传输方向的关键字主要有: src、dst、dst or src、dst and src。若缺省该关键字, 系统默认为 dst or src。src 192.168.168.155 代表源地址为 192.168.168.155 的数据包。

例如, 若要捕获所有源地址为 192.168.168.155 的所有数据包, 则实现命令为:

```
tcpdump src 192.168.168.155
```

若要捕获所有目的地址为 192.168.168.154 的所有数据包, 则实现命令为:

```
tcpdump dst 192.168.168.154
```

若要捕获所有目的网络为 61.186.170.0 的所有数据包, 则实现命令为:

```
tcpdump dst net 61.186.170.0
```

### (3) 协议关键字

协议关键字用于指定要捕获的数据包所使用的协议。可使用的协议关键字有 fddi、ip、arp、rarp、tcp、udp 和 icmp。若未指定协议,则将监听所有协议的数据包。

fddi 是分布式光纤数据接口网络上所使用的网络协议,是 ether 的别名。

除了以上三种关键字外,还可使用 and 或 &&、or 或 ||、not 或 ! 三种逻辑运算符来构造表达式。

例如,若要捕获源地址为 192.168.168.155,目的端口为 80 的所有数据包,则实现命令为:

```
tcpdump src 192.168.168.155 and tcp dst port 80 -i eth0
```

以上命令实际上就是捕获 192.168.168.155 主机对外 80 端口访问所有的数据包。

若要捕获 192.168.4.120 主机和 192.168.168.97 或 192.168.168.120 主机通信的所有数据包,则实现命令为:

```
tcpdump host 192.168.4.120 and \ (192.168.168.97 or 192.168.168.120\)
```

在正规表达式中,括号需要使用转义字符\来表达。

### 3. tcpdump 的输出信息

假设要捕获源或目的为 192.168.168.155 主机的所有数据包,则执行命令:

```
[root@rh9 root]# tcpdump host 192.168.168.155 -i eth0
```

然后在 192.168.168.155 主机中打开浏览器,访问 192.168.168.154 (www.myweb1.com) 站点,此时的输出信息如下所示:

```
tcpdump: listening on eth0
11:31:45.355172 192.168.168.155.1122 > www.myweb1.com. http: S 889138576:889138576
(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
11:31:45.355343 www.myweb1.com. http > 192.168.168.155.1122: S 1318149386:1318149386
(0) ack 889138577 win 5840 <mss 1460,nop,nop,sackOK> (DF)
11:31:45.355635 192.168.168.155.1122 > www.myweb1.com. http: . ack 1 win 65535 (DF)
11:31:45.359200 192.168.168.155.1122 > www.myweb1.com. http: P 1:200(199) ack 1 win
65535 (DF)
11:31:45.359299 www.myweb1.com. http > 192.168.168.155.1122: . ack 200 win 6432 (DF)
11:31:45.369060 www.myweb1.com. http > 192.168.168.155.1122: . 1:1461(1460) ack 200
win 6432 (DF)
11:31:45.369379 www.myweb1.com. http > 192.168.168.155.1122: . 1461:2921(1460) ack
```

```

200 win 6432 (DF)
11:31:45.369622 192.168.168.155.1122 > www.myweb1.com.http: . ack 2921 win 65535
(DF)
11:31:45.369781 www.myweb1.com.http > 192.168.168.155.1122: . 2921:4381(1460) ack
200 win 6432 (DF)
11:31:45.370197 www.myweb1.com.http > 192.168.168.155.1122: . 4381:5841(1460) ack
200 win 6432 (DF)
11:31:45.370389 www.myweb1.com.http > 192.168.168.155.1122: . 5841:7301(1460) ack
200 win 6432 (DF)
11:31:45.370153 192.168.168.155.1122 > www.myweb1.com.http: . ack 4381 win 65535
(DF)
11:31:45.370672 www.myweb1.com.http > 192.168.168.155.1122: P 7301:8501(1200) ack
200 win 6432 (DF)
.....
11:32:00.425584 192.168.168.155.1123 > www.myweb1.com.http: . ack 4871 win 65046
(DF)
11:32:05.413506 192.168.168.155.1123 > www.myweb1.com.http: R 889204127:889204127
(0) win 0 (DF)

68 packets received by filter
10 packets dropped by kernel

```

由于是 http 访问,因此输出的全部是 TCP 包,TCP 包的输出格式一般是:

```
time id src > dst: flags data-seqno ack win urgent options
```

其中,time 代表该包接收到或发出的时间,比如第一行(第一个包)的 11:31:45。

id 是包的序列号,如第一个包的 355172。

src>dst 代表由 src 源主机发起的对 dst 目标主机的连接,IP 地址或域名后面是所使用的端口号,比如 192.168.168.155.1122 > www.myweb1.com.http,代表 192.168.168.155 主机使用 1122 端口,发起对 www.myweb1.com 主机的 http 端口即 80 端口的连接请求。

flags 位置代表的是 TCP 包中被设置的 tcp 标志位,比如第一行中的 S,它代表的是 SYN 标志,说明是请求建立 tcp 连接的第一个包。F 代表 FIN,P 代表 PUSH,R 代表 RST,若没有标志被设置,则该位置显示为“.”。

data-seqno 是数据包中的数据顺序号。如:889138576;889138576(0)。

ack 表示是对序列号为 xxxx 的包的响应。如第二行中的 ack 889138577。

win 代表接收缓存的窗口大小,如第三行中的 win 65535。

urgent 表明数据包中是否有紧急指针,如第二行中的 < mss 1460, nop, nop,



sackOK>。

options 是功能选项,如(DF)。

## 习题

- 下面对防火墙的描述中,不正确的是( )。
  - 防火墙是一种网络安全设备,通常安装在两个网络的边界,以保护一个网络不受到来自另一个网络的攻击
  - 硬件式防火墙通常提供有 DMZ 接口,该接口用于连接服务器
  - 防火墙的内网卡地址应设置为内部网络的地址,并设置好默认网关
  - 防火墙的外网卡地址通常应设置为一个公网地址,并设置好默认网关
- 若要开启 IP 包转发功能,以下命令中,不正确的是( )。
  - 在/etc/sysconfig/network 配置文件中,设置 FORWARD\_IPV4=true
  - 执行命令: echo "1" > /proc/sys/net/ipv4/ip\_forward
  - 执行命令: sysctl -w net.ipv4.ip\_forward="1"
  - 修改/etc/sysctl.conf 配置文件,设置 ip\_forward=1
- 要查看当前所安装的内核模块,可使用命令( )。
  - modprobe
  - lsmod
  - rmmod
  - insmod
- 若要清除 filter 表中所有自定义的链,以下命令中正确的是( )。
  - iptables -F -t filter
  - iptables -Z
  - iptables -X
  - iptables -Z -t filter
- 若要将从 eth1 网卡出去的包进行 IP 伪装,以下命令中正确的是( )。
  - /sbin/iptables -t nat -A POSTROUTING -i eth1 -j MASQUERADE
  - /sbin/iptables -t nat -A PREROUTING -o eth1 -j MASQUERADE
  - /sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
  - /sbin/iptables -A POSTROUTING -o eth1 -j MASQUERADE
- 以下对代理的描述中,不正确的是( )。
  - 利用 iptables 的 IP 伪装可以实现透明代理
  - squid 代理具备网页缓存功能,可加快网页的访问速度,但不能实现透明代理
  - 利用 squid 与 IP 伪装相结合,可实现具有网页缓存功能的透明代理
  - Linux 的代理服务器通常也可具备防火墙的功能,但这会影响代理的性能,因此防火墙与代理服务器最好分开
- 在 iptables 命令中,若要使用-m multiport 选项进行多端口表达,则应事先加载( )内核支持模块。

- |                   |                  |
|-------------------|------------------|
| A. ipt_MASQUERADE | B. ipt_multiport |
| C. iptable_filter | D. ip_multiport  |

## 实训 11 配置防火墙与透明代理

**〔实训目的〕** 掌握 Linux 防火墙和透明代理服务器的配置方法。

**〔实训环境〕** 一台安装有 2 块网卡的 PC 机,并事先安装好 Linux 操作系统。一个固定的公网 IP 地址。

**〔实训内容〕**

1. 按照例 11.1 所示,配置并测试防火墙。
2. 按照例 11.2 所示,配置并测试透明代理服务器。
3. 按照 11.2.3 节所讲的步骤与方法,利用 squid 配置带缓存的透明代理服务器。

## Linux 的远程登录管理

为了实现远程登录和访问 Linux 系统,为此系统提供了 telnet 和 SSH 服务。SSH 功能与 telnet 相似,但采用了加密方式传输数据,可以实现安全的远程访问和连接,是 telnet 的安全替代产品,也是 Red Hat Linux 9 默认使用的方式。

本章将介绍 telnet 和 SSH 服务的安装方法,以及如何利用 telnet 和 SSH 来远程登录和访问 Linux 服务器。

### 12.1 使用 telnet 远程登录

telnet 采用明文方式传输网络数据(包括用户账户和密码),安全性较差,目前已逐渐被 SSH 所取代,因此在 Red Hat Linux 9 中,系统默认安装使用 SSH 服务,而未安装 telnet 服务,但安装有 telnet 客户端程序。若要使用 telnet 服务来登录 Linux 服务器,则应在 Linux 服务器中安装 telnet 服务。

#### 1. 查询 telnet 服务器和客户端程序

```
[root@rh9 root]# rpm -q telnet                # 查询是否安装 telnet 客户端程序
telnet-0.17-25
[root@rh9 root]# rpm -q telnet-server          # 查询是否安装 telnet 服务器程序
package telnet-server is not installed
```

#### 2. 安装 telnet 服务器

在 Red Hat Linux 9 的第 3 张安装光盘的“RedHat/RPMS”目录中,提供了 telnet 的服务器安装包,其文件名为 telnet-server-0.17-25.i386.rpm。

```
[root@rh9 root]# mount /mnt/cdrom
[root@rh9 root]# rpm -ivh /mnt/cdrom/RedHat/RPMS/telnet-server-0.17-25.i386.rpm
[root@rh9 root]# umount /mnt/cdrom
```

```
[root@rh9 root]# rpm -q telnet-server  
telnet-server-0.17-25
```

### 3. 启动 telnet 服务器

telnet 服务器由 xinetd 服务管理器管理,默认情况下并不会启动。若要启动 telnet 服务器,则实现命令为:

```
[root@rh9 root]# chkconfig telnet on          # 设置在启动系统时,启动 telnet 服务  
[root@rh9 root]# service xinetd restart      # 重启 xinetd 服务,以使 telnet 服务立即启动
```

telnet 服务器启动成功后,才能在远程使用 telnet 命令来登录访问 Linux 服务器。

### 4. 远程登录 Linux 服务器

Linux 和 Windows 系统均提供有 telnet 的客户端程序 telnet,利用该程序,即可实现远程登录 Linux 服务器。

在 Windows 系统和 Linux 系统登录的方法相同,下面以 Windows 系统登录为例,假设 Linux 服务器的 IP 地址为 192.168.168.154,则登录命令为:

```
C:\>telnet 192.168.168.154  
Red Hat Linux release 9 (Skrake)  
Kernel 2.4.20-8 on an i686  
login: root                                # 输入用户账户  
Password:                                # 输入用户密码  
[root@rh9 root]#
```

只要出现了 Linux 的命令行提示符,则说明登录成功,此时就可远程访问和管理 Linux 服务器了。

## 12.2 使用 SSH 远程登录

### 1. SSH 简介

SSH 是 Secure Shell 的缩写,OpenSSH 是免费的 SSH 协议版本,是一种可信赖的安全连接工具。telnet、rlogin 和 ftp 在进行网络连接时,对数据流没有加密,利用 sniffer 等工具通过对数据包的分析,很容易获得用户的账户和密码,安全性很差。OpenSSH 加密网络通信中的所有数据,从而可以有效防止信息被窃取,提高了网络连接和访问的安全性。

OpenSSH 需要 OpenSSL-0.97 或以上版本的支持,OpenSSL 提供与加密相关的管理工具和库文件,并可向其他软件包提供加密支持。

OpenSSH 提供有很多安全的实用程序,利用 SSH 可替代 rlogin 和 telnet 程序,利用 sftp 可替代 ftp,利用 scp 可替代 rcp 程序。sshd 是 SSH 服务的守护进程程序。OpenSSH 目前的最新版本是 3.6.1,支持 SSH1 和 SSH2 协议。OpenSSH 和 OpenSSL 的下载地址为:

```
ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.6.1p1.tar.gz
```

```
ftp://ftp.openssl.org/source/openssl-0.9.7b.tar.gz
```

openssh 源代码软件包提供了 SSH 客户端和服务端程序(sshd)。

## 2. 安装 OpenSSH

Red Hat Linux 9 在安装时默认会安装 OpenSSH 和 OpenSSL,可以使用以下命令检查当前系统是否已安装。

```
[root@rh9 root]# rpm -qa |grep ssh
openssh-3.5p1-6
openssh-server-3.5p1-6
openssh-clients-3.5p1-6
```

若输出了以上三项,则说明系统已安装 OpenSSH,可直接使用。其中 openssh-3.5p1-6 是 OpenSSH 的核心软件包,不管是安装 OpenSSH 的服务器,还是安装 OpenSSH 的客户端,都需要安装该软件包。openssh-server-3.5p1-6 是 OpenSSH 的服务端程序,openssh-clients-3.5p1-6 是客户端程序。

若当前系统没有安装,可在 Red Hat Linux 9 的第 1 张安装光盘中,找到这三个软件包,然后使用以下命令进行安装。

```
[root@rh9 root]# mount /mnt/cdrom/
[root@rh9 root]# rpm -ivh /mnt/cdrom/RedHat/RPMS/openssh-3.5p1-6.i386.rpm
[root@rh9 root]# rpm -ivh /mnt/cdrom/RedHat/RPMS/openssh-server-3.5p1-6.i386.rpm
[root@rh9 root]# rpm -ivh /mnt/cdrom/RedHat/RPMS/openssh-clients-3.5p1-6.i386.rpm
```

对于提供远程访问的服务器,必须安装 openssh 服务器软件,对于 Linux 客户端,即用来远程登录访问 Linux 服务器的客户机,必须安装 openssh 的客户端软件包。

```
[root@rh9 root]# rpm -q openssl                                # 查询是否已安装 openssl
openssl-0.97a-2
```

## 3. 配置 OpenSSH 服务器

OpenSSH 服务器软件包提供了服务器进程程序(/usr/sbin/sshd)、配置文件、启动脚本和帮助文档。可使用以下命令查看该软件包所安装的文件以及安装到的位置。

```
[root@rh9 root]# rpm -ql openssh-server
```

```

/etc/pam.d/ssh
/etc/rc.d/init.d/ssh
/etc/ssh
/etc/ssh/ssh_config
/usr/libexec/openssh/sftp-server
/usr/sbin/ssh
/usr/share/man/man5/ssh_config.5.gz
/usr/share/man/man8/sftp-server.8.gz
/usr/share/man/man8/ssh.8.gz
/var/empty/ssh
# sshd 进程启动脚本
# ssh 服务的配置文件
# sftp 服务进程
# sshd 守护进程程序

```

OpenSSH 服务器的配置文件是 `/etc/ssh/ssh_config`，使用其默认配置即可正常工作，通常不需要修改。

#### 4. 启动与停止 OpenSSH 服务器

`/etc/rc.d/init.d/ssh` 是 OpenSSH 服务器的启动脚本，可使用该脚本或用 `service` 命令来启动 `sshd` 服务进程。

启动 OpenSSH 服务器，实现命令为：`service sshd start` 或 `/etc/rc.d/init.d/ssh start`。

查看服务器的启动状态，实现命令为：`service sshd status` 或 `/etc/rc.d/init.d/ssh status`。

停止 OpenSSH 服务器，实现命令为：`service sshd stop` 或 `/etc/rc.d/init.d/ssh stop`。

重启 OpenSSH 服务器，实现命令为：`service sshd restart` 或 `/etc/rc.d/init.d/ssh restart`。

Red Hat Linux 9 默认安装 OpenSSH 后，会在 2、3、4、5 运行级别，自动启动 OpenSSH 服务器。

#### 5. 使用 SSH 远程登录访问服务器

对于 Linux 客户端，若要登录访问 Linux 服务器，则应安装 `openssh-clients` 和 `openssh` 软件包，该软件包提供了用于安全登录连接的实用程序。可通过以下命令查看该软件包所提供的实用程序及安装位置。

```

[root@rh9 root]# rpm -ql openssh-clients
/etc/ssh/ssh_config
/usr/bin/scp
/usr/bin/sftp
/usr/bin/slogin
/usr/bin/ssh
# 客户端配置文件
# 安全的远程文件复制程序
# 使用 SSH1 和 SSH2 协议，安全的类 FTP 程序
# 安全的远程登录程序
# 用于登录 openssh 服务器的客户端程序

```

```

/usr/bin/ssh-add           # 为 ssh-agent 添加密钥的工具
/usr/bin/ssh-agent         # 一个保存私有密钥的授权代理
:

```

客户端配置文件通常也不需要修改,使用默认配置即可正常工作。远程登录安装有 OpenSSH 的服务器使用 ssh 命令,该命令是 rlogin、rsh 和 telnet 命令的安全替代程序,允许在登录远程主机并在该主机上执行命令。ssh 命令的用法为:

```
ssh 用户名@主机 IP 地址
```

ssh 命令由于是安全的连接访问,因此允许使用 root 用户进行远程登录和访问,其登录方法为:

```

[root@rh9 root]# ssh root@192.168.168.154
The authenticity of host '192.168.168.154(192.168.168.154)' can't be established.
RSA key fingerprint is e6:c8:93:86:0a:4e:33:5b;77:30:1b:91:e9:03:6d:48.
Are you sure you want to continue connecting (yes/no)? yes

```

第一次登录需要确认密钥,回答 yes 才能继续登录。

```

Warning: Permanently added '192.168.168.154' (RSA) to the list of known hosts.
root@192.168.168.154's password:           # 此时输入用户密码
Last login: Tue Sep 21 21:10:04 2004 from rh9
[root@rh9 root]#

```

出现 Linux 的命令行提示符后,则登录成功,此时客户机就相当于服务器的一个终端,在该命令行上进行的操作,实际上是在操作远端的 Linux 服务器。操作方法与操作本地机一样。

## 6. 对远程主机的操作

利用 ssh 登录到远程主机后,可以使用 scp 或 sftp 命令进行文件的复制以及上传或下载等操作。

### (1) 使用 scp 命令复制文件

由于 scp 命令使用 ssh 协议进行数据传输,因此操作更安全。该命令用于将一台主机上的文件复制到另一台主机。其命令用法为:

```
scp 源文件 目录文件
```

其中源文件的表达格式为:当前登录的用户名@主机地址:要复制的文件全路径名

比如,若要将远程主机上的 /usr/local/src/rp-pppoe-3.5.tar.gz 文件复制到客户端的 /root 目录,则实现命令为:

```
[root@rh9 root]# scp root@192.168.168.154:/usr/local/src/rp-pppoe-3.5.tar.gz /root
```

```

root@192.168.168.154's password:
rp pppoc-3.5.tar.gz 100% | * * * * *
* * * * * 184KB 00:00
[root@rh9 root]# exit                                # 关闭与远程主机的连接
Connection to 192.168.168.154 closed.

```

## (2) 使用 sftp 命令上传或下载文件

sftp 的功能与 ftp 类似,是一种安全的上传/下载程序,可用于登录连接安装有 OpenSSH 并启动了 sftp server 服务的服务器,并实现对服务器数据的上传和下载。

sftp 的服务器程序是 sftp-server,它作为 OpenSSH 服务器的一个子进程运行。在 sshd\_config 配置文件中,通过以下配置语句来启动 sftp 服务子进程。

```
Subsystem          sftp          /usr/libexec/openssh/sftp-server
```

利用 sftp 连接远程服务器的命令用法为: sftp 用户名@服务器 IP 地址

例如,若要利用 root 账户登录连接 192.168.168.154 服务器,则实现命令为:

```

[root@rh9 root]# sftp root@192.168.168.154
Connecting to 192.168.168.154...
root@192.168.168.11's password:          # 输入 root 账户的密码
sftp>                                     # 登录成功,出现 sftp 的命令提示符

```

出现 sftp> 命令行后,则表示登录成功。在该命令行中,通过执行 sftp 提供的相关命令,即可实现数据的上传与下载操作。sftp 提供的命令与 ftp 命令很类似,可键入 ? 来获得命令帮助。

```

sftp>?
Available commands:
cd path                改变远程主机的当前目录
lcd path               改变本地主机的当前目录
chgrp grp path         设置指定文件所属的用户组
chmod mode path        设置指定文件的权限
chown own path         设置指定文件的属主
help                   显示本帮助信息
get remote-path [local-path] 下载文件
put local-path [remote-path] 上传文件
lls [ls-options [path]]    显示本地目录文件列表
ln oldpath newpath        对远程主机上的文件创建符号链接
symlink oldpath newpath   对远程主机上的文件创建符号链接
lnkdir path             在本地主机创建目录
mkdir path              在远程主机创建目录

```



lpwd	显示本地主机的当前目录
pwd	显示远程主机的当前目录
ls [path]	显示远程主机的目录文件列表
lumask umask	设置本地主机的 umask
cxit	退出 sftp
quit	退出 sftp
rename oldpath newpath	对远程主机上的文件进行更名操作
rmdir path	删除远程主机上的指定目录
rm path	删除远程主机上的指定文件
version	显示 sftp 的版本信息
!command	在本地主机执行命令,command 代表要执行的命令
!	退回到本地命令行状态
?	显示本帮助信息
sftp>exit	# 关闭 sftp 连接

## 12.3 Windows 平台使用 SSH 客户端登录

Linux 平台提供了 OpenSSH 客户端软件来实现远程登录,在 Windows 平台,可使用 PuTTY 软件来作为 SSH 的客户端。该软件很小,无需安装可直接运行,在下载页面,可下载整个软件包,也可下载单个实用程序,putty.exe 是 PuTTY 的主程序,使用该程序来实现 SSH 登录。pscp.exe 用于实现 scp 命令的功能,psftp.exe 用于实现 sftp 命令的功能。该软件包的下载地址为: <http://www.chiark.greenend.org.uk/~sgtatham/putty/>。

双击运行 putty.exe,其界面如图 12.1 所示。

SSH 服务默认使用 TCP 22 号端口,telnet 默认是 TCP 23 号端口。选择协议类型为 SSH,在 Host Name (or IP address)输入框中输入要登录的 Linux 服务器的 IP 地址,然后单击 Open 按钮,即可开始以安全方式登录连接 Linux 服务器。此时将弹出一个安全警告对话框,单击“是”按钮,然后系统将打开一个终端的窗口,供输入用户账户和密码,登录成功后的终端窗口如图 12.2 所示。

登录成功后,就可在 Windows 平台远程访问和操作 Linux 服务器了,若要关闭连接,可执行 exit 命令。

若要限制非 root 用户的远程登录,可用 touch 命令创建/etc/nologin 文件,这样所有的非 root 用户都不能远程登录服务器。若不允许任何用户登录 Linux 服务器,可通过停止 telnet 和 ssh 服务来实现。若要设置允许远程登录 Linux 的主机,可通过设置防火墙规则来实现。telnet 使用的是 TCP 23 号端口,SSH 使用的是 TCP 22 号端口。

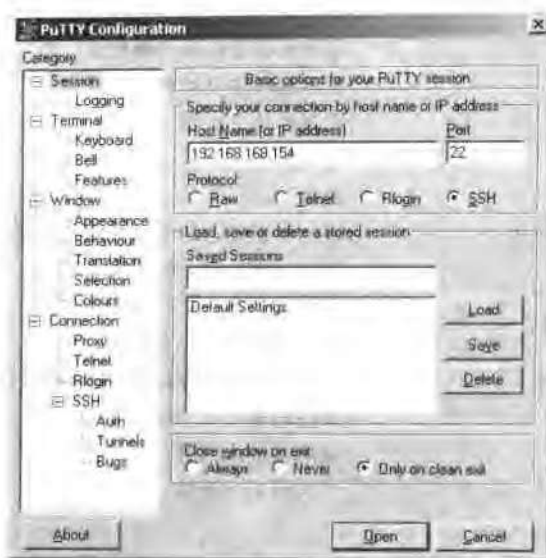


图 12.1 PuTTY SSH 客户端主界面



图 12.2 Windows 平台远程登录 Linux 服务器

## 习题

- 在以下远程登录方式中,允许使用 root 账户登录的是( )。  
A. telnet      B. ssh      C. ssl      D. rlogin
- 若要更改 SSH 服务器所使用的端口,应在( )配置文件中设置或修改。  
A. /etc/ssh/ssh\_config      B. /etc/ssh/sshd\_config  
C. /etc/ssh/host\_key      D. /etc/ssh.conf
- 在 Windows 平台要安全登录 Linux 服务器,登录所用的客户端软件应使用( )。  
A. telnet      B. ssh      C. 超级终端      D. 'putty'
- SSH 服务器默认使用的端口号是( ),telnet 服务器默认使用的端口号是( )。  
A. 21      B. 22      C. 23      D. 20

5. 以下描述中,不正确的是( )。
- A. 通过修改 SSH 服务器的配置文件,SSH 服务器也可使用其他端口来提供远程登录服务
  - B. 利用 sftp 可实现安全的上传或下载文件
  - C. telnet 远程登录时,其用户名和密码采用加密方式传输,一般数据采用明文传输
  - D. Linux 必须安装和启动了 telnet 服务器或 SSH 服务器后,客户端才能远程登录该服务器

## 实训 12 远程登录

**[实训目的]** 掌握利用 telnet 和 SSH 远程登录 Linux 服务器的方法。

**[实训环境]** 在虚拟 PC 机的 Linux 操作系统中进行实际操作。

**[实训内容]**

1. 检查当前 Linux 系统是否安装有 telnet 服务器和客户端软件包,若未安装,则安装该软件包。
2. 在宿主操作系统上运行 putty 软件,协议类型选择 telnet,然后在 HostName 输入框中输入 Linux 服务器主机的 IP 地址,然后单击 Open 按钮,开始 telnet 登录。  
**注意:** telnet 只能使用普通用户身份进行远程登录。
3. 进入 Windows 的 MS-DOS 方式,然后使用 telnet 命令登录 Linux 服务器。
4. 检查当前 Linux 系统是否安装 SSH 服务,若未安装,则安装该服务器。
5. 在 Windows 平台启动 putty 软件,协议类型选择 ssh,在 HostName 输入框中输入 Linux 服务器的 IP 地址,然后单击 Open 按钮,开始 ssh 远程登录。输入 Linux 的 root 账户和密码,检查能否正常登录。
6. 使用 sftp 命令登录 FTP 服务器,并练习 sftp 所提供的子命令的功能及用法。

# 第 13 章

## Linux 内核的升级

### 13.1 Linux 2.6 内核新特性

Linux 2.6 内核的诞生,对于 Linux 的发展和应用又进入了一个新的里程碑。新内核可以大大增强高端商用服务器的性能,支持更多新的设备和特性。Red Hat Linux Fedora Core 2 就采用了 Linux 2.6 内核。Linux 2.6 内核的主要新特性如下:

- 功能更为强大,支持更多的设备和处理器类型。对于服务器,支持最多 255 个 CPU 和 64GB 的内存。
- 改进和部分重写了功能模块(modules),增强了系统的可靠性。修改了部分 I/O 子系统,保证了系统在各种负荷情况下,I/O 系统都有很好的响应速度。
- 采用抢占式内核,使交互操作的响应速度大大提高。
- 全面支持各种 USB 设备,并正式支持 USB 2.0 标准。
- 加强了对无线设备的支持。
- 全面改进了文件系统,重写了 NTFS 文件系统的支持,改进了 HPFS。
- 更新了 IDE/ATA、SCSI 等存储总线,解决和改善了一些以前存在的问题。2.6 版内核可以直接通过 IDE 驱动程序来支持 IDE CD/RW 设备,而不必像以前需要使用 SCSI 模拟驱动程序来操作。
- 在网络方面新增了对 IPSec 安全协议的支持,改进了对 IPv6 的支持。
- 支持更多种类和型号的多媒体设备,增加了一种全新的 ALSA(advanced Linux sound architecture)声音系统,该系统能很好地支持全杜比录音及回放、无缝混音、支持声音合成设备以及 USB 声卡。其设计目的就是要用它来取代缺陷较多的 OSS(open sound system)音频系统。

## 13.2 升级到 Linux 2.6 内核

目前 Linux 的最新内核版本为 2.6.8.1, 本节以此内核版本为例, 介绍 Linux 内核的升级方法。

### 1. 获得内核源代码

要升级内核, 首先就必须下载取得新内核的源代码包, 可从内核的官方网站 <http://www.kernel.org> 下载。2.6.8.1 内核的下载地址为:

```
http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.8.1.tar.bz2
```

```
[root@rh9 root]# mkdir /src
```

```
[root@rh9 root]# wget http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.8.1.tar.bz2
```

### 2. 解压内核源代码

```
[root@rh9 root]# cd /src
```

```
[root@rh9 src]# tar -jxvf linux-2.6.8.1.tar.bz2
```

### 3. 升级相关的软件包

在升级内核之前, 应升级一些相关的软件包, 在源代码目录的 Documentation/Changes 文件中, 指出了升级内核时, 相关软件包必须满足的最低版本号, 以及检查版本号的相关命令和最新软件包的下载地址。相关的软件包及所要求的版本号和当前版本的检测方法如表 13.1 所示。

表 13.1 升级到 2.6.8.1 内核相关软件包的版本要求

软件包名称	要求的版本号	检测版本号的命令	当前版本号
GNU C	2.95.3	gcc --version	3.2.2
GNU make	3.79.1	make --version	3.79.1
binutils	2.12	ld -v	2.13
util linux	2.10	fdformat --version	2.11
module-init-tools	0.9.10	depmod -V	2.4.22
e2fsprogs	1.29	tune2fs	1.32
jfsutils	1.1.3	fsck.jfs -V	1.0.17
reiserfsprogs	3.6.3	reiserfsck -V 2>&1 grep reiserfsprogs	3.6.4
xfsprogs	2.6.0	xfs_db -V	

续表

软件包名称	要求的版本号	检测版本号的命令	当前版本号
pcmcia-cs	3.1.21	cardmgr -V	3.1.31
quota-tools	3.09	quota -V	3.06
PPP	2.4.0	pppd --version	2.4.1
isdnt4k-utils	3.1pre1	isdntctrl 2>>&1 grep version	3.1pre4
nfs-utils	1.0.5	showmount --version	1.0.1
procps	3.2.0	ps --version	2.0.11
oprofile	0.53	oprofiled --version	

内核对 module-init-tools 软件包的版本号与 Red Hat Linux 对该软件包的版本号计算标准不相同,因此存在很大差异,该软件包是内核模块加载工具,对内核的升级至关重要,在内核升级前,建议升级到最新版本。对于当前系统没有涉及的软件包即没有使用到的功能,可不用升级。通过以上版本比较,需要事先升级的软件包及下载地址如下:

```
module-init-tools  ftp://ftp.kernel.org/pub/linux/kernel/people/rusty/modules/
jfsutils           http://oss.software.ibm.com/jfs
quota-tools        http://sourceforge.net/projects/linuxquota/
nfs-utils          http://sourceforge.net/project/showfiles.php?group_id=14
xfsprogs           ftp://oss.sgi.com/projects/xfs/download
oprofile           http://oprofile.sf.net/download/
```

将这些软件包下载并存放在/src/other 目录中。

#### (1) 升级安装 module-init-tools 软件包

```
[root@rh9 src]# cd other
[root@rh9 other]# tar -zxvf module-init-tools-3.1-pre5.tar.gz
[root@rh9 other]# cd module-init-tools-3.1-pre5
[root@rh9 module-init-tools-3.1-pre5]# ./configure --prefix=/
```

对于第一次安装,需要运行 make moveold 命令,将旧版的 insmod、modprobe、rmmod 和 lsmod 命令分别更名为 insmod.old、modprobe.old、rmmod.old 和 lsmod.old。

```
[root@rh9 module-init-tools-3.1-pre5]# make moveold
[root@rh9 module-init-tools-3.1-pre5]# make
[root@rh9 module-init-tools-3.1-pre5]# make install
```

对于第一次安装,还需要运行以下命令,将原来的/etc/modules.conf 配置文件转换

成/etc/modprobe.conf。

```
[root@rh9 module-init-tools-3.1-pre5]# ./generate-modprobe.conf /etc/modprobe.conf
```

最后检查升级后的软件包的版本号。

```
[root@rh9 module-init-tools-3.1-pre5]# depmod -V
module-init-tools 3.1-pre5
```

## (2) 升级 jfsutils 软件包

```
[root@rh9 module-init-tools-3.1-pre5]# cd ..
[root@rh9 other]# tar -zxvf jfsutils-1.1.7.tar.gz
[root@rh9 other]# cd jfsutils-1.1.7
[root@rh9 jfsutils-1.1.7]# ./configure
* * * * *
checking uuid/uuid.h usability... no
checking uuid/uuid.h presence... no
configure: error: 'You need the uuid library'
* * * * *
[root@rh9 jfsutils-1.1.7]# make
[root@rh9 jfsutils-1.1.7]# make check
[root@rh9 jfsutils-1.1.7]# make install
[root@rh9 jfsutils-1.1.7]# make clean
```

## (3) 升级 quota-tools 软件包

```
[root@rh9 jfsutils-1.1.7]# cd ..
[root@rh9 other]# tar -zxvf quota-3.12.tar.gz
[root@rh9 other]# cd quota-tools
[root@rh9 quota-tools]# ./configure
[root@rh9 quota-tools]# make
[root@rh9 quota-tools]# make install
```

下面查询安装后的版本号。

```
[root@rh9 quota-tools]# quota -V
Quota utilities version 3.12.
Compiled with RPC
Bugs to mivw@planets.elm.net,jack@suse.cz
```

## (4) 升级 nfs-utils 软件包

```
[root@rh9 quota-tools]# cd ..
```

```
[root@rh9 other]# tar zxvf nfs-utils-1.0.6.tar.gz
[root@rh9 other]# cd nfs-utils-1.0.6
[root@rh9 nfs-utils-1.0.6]# ./configure
[root@rh9 nfs-utils-1.0.6]# make
[root@rh9 nfs-utils-1.0.6]# make install
[root@rh9 nfs-utils-1.0.6]# showmount -v          # 查询新的版本号
showmount for nfs-utils 1.0.6
```

#### (5) 升级oprofile软件包

```
[root@rh9 nfs-utils-1.0.6]# cd ..
[root@rh9 other]# tar -zxvf oprofile-0.8.1.tar.gz
```

### 4. 配置Linux内核

升级完相关的软件包后,就可开始配置Linux内核,配置完后就可开始编译和安装Linux的内核。

配置Linux内核,可使用源代码包提供的基于文本或图形界面的配置向导来实现。新内核提供了两个基于图形界面的配置工具。

make menuconfig 是一个基于文本界面的内核配置向导;make xconfig 则是一个使用QT库的基于图形界面的内核配置向导,使用前必须先安装QT库,一般发行光盘中都包含了该软件包;make gconfig 是一个使用GTK库作为界面的内核配置工具,其界面更符合Windows界面的使用习惯。使用前应先安装GTK库。

对内核进行配置时,大部分的选项一般都可使用默认值,只有小部分需要根据用户不同的需要,进行设置和调整。

在进行配置时,可按Y键将该功能编译进内核,按M键则将该功能编译成内核模块,需要时再动态装入内核,以减小内核的大小,按N键则不选择该功能。

在编译升级内核之前,建议先执行/sbin/lspci命令,查看了解当前系统的PCI和SCSI设备的类型和型号,以便在配置新内核时能正确选择相应的设备型号。

```
[root@rh9 src]# /sbin/lspci
[root@rh9 src]# cd linux 2.6.8.1
```

若要清除以前编译留下的文件,可执行make mrproper命令。对于首次编译不需要。

```
[root@rh9 linux-2.6.8.1]# make mrproper
CLEAN scripts/package
[root@rh9 linux-2.6.8.1]# make menuconfig          # 基于文本的配置向导
```

执行make menuconfig命令后,将启动内核的基于文本界面的配置向导,如图13.1所示。



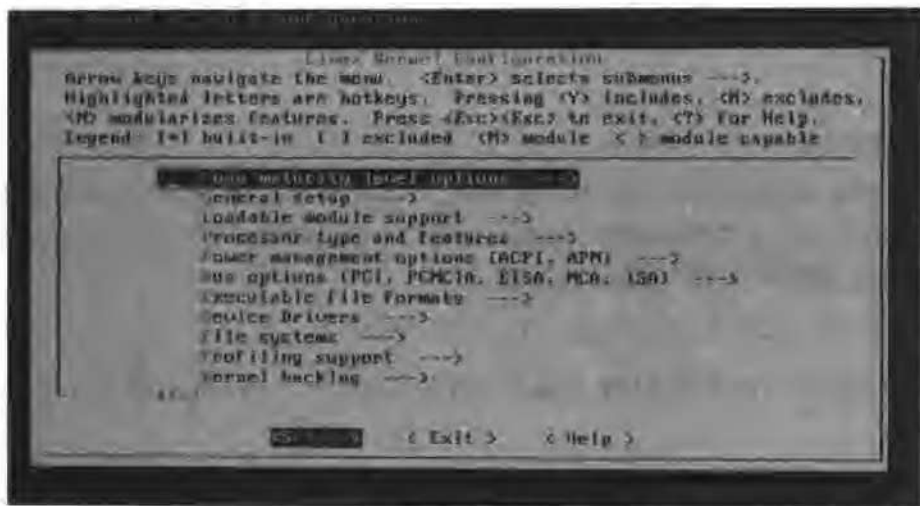


图 13.1 Linux 基于文本界面的内核配置向导

在该界面的顶部介绍配置工作的操作方法,即:使用光标键在各选项间移动,使用回车键 Enter 进入下一层子菜单,每个选项上的高亮字母为快捷键,在括号中按 Y 键表示将这个项目编译进内核中,按 M 键则编译为模块,按 N 键表示不选择,按 Esc 键返回到上层菜单。

下面分别对各配置选项进行介绍和说明。

#### (1) Code maturity level options (代码成熟度选项) —>

将光标移动到该项,然后按回车,此时将进入其子菜单选项,如下所示:

- [\*] Prompt for development and/or incomplete code/drivers
- [\*] Select only drivers expected to compile cleanly (NEW)

这两个选项默认都是选择的,用户一般不需要更改,第 2 个选项选中后,表示仅提供经过严格测试的驱动程序,对于可能存在问题的驱动程序将不被包含进来。

#### (2) General setup —>

按 Esc 键返回到上级菜单,然后按向下光标键,将光亮条移动到 General setup 选项,按回车键,即可进入该选项的下级子菜单。其选项及功能如下:

- [\*] Support for paging of anonymous memory

使内核支持虚拟内存,默认选择。

- [\*] System V IPC

为进程提供通信机制,使系统中各进程间有交换信息与保持同步的能力。默认选择,一般不要更改。

- ☐ POSIX Message Queues (NEW)
- ☒ BSD Process Accounting

默认选择,将会让内核为用户层的进程建立一个账目(进程通过一个特殊的系统调用来通知内核),当程序退出时,内核会将进程的相关信息记录到账目文件中,主要包括进程的创建时间、创建者、内存占用情况等信息。

- ☒ BSD Process Accounting version 3 file format (NEW)

默认未选中,若选择则设置进程账目文件的格式为版 3 格式。可以按 Y 键选择该选项。

- ☒ Sysctl support

默认选择,这将提供一个接口,以便可以动态更改一些核心参数与变量,而不需要重新启动系统。

- ☐ Auditing support (NEW)
- (14) Kernel log buffer size (16=>64KB,17=>128KB) (NEW)
- ☒ Support for host-pluggable devices
- ☐ Kernel .config support

默认未选择。若选择,则将内核的配置信息与相关的说明文档编译进内核,以便以后可使用一些工具来提取并重新构建内核,通常不用选择。

- ☐ Configure standard kernel features (for small systems) (NEW) --->

最后一个选项为小型系统配置标准的内核特性,后面带有“--->”,表示还有下级子菜单,光亮条移动该配置项后,按回车,将显示以下子配置项:

- Configure standard kernel features (for small systems)
- Load all symbols for debugging/kksymoops
- ☐ Include all symbols in kallsyms (NEW)
- ☐ Do an extra kallsyms pass (NEW)

(3) Loadable module support (可加载模块选项) --->

- ☒ Enable loadable module support

默认选择,让内核支持加载动态模块。模块可在系统内核运行时根据需要动态加载(使用 modprobe 命令加载),为内核增加一些特性或对某种硬件提供支持。利用模块,可

将不常用的一些驱动程序或特性编译成一些模块,以减小内核的大小。

对于一些功能或特性,是直接编译进内核中,还是编译成模块的一个原则是:对于不常使用的,特别是在系统启动时不需要的驱动程序,可编译为模块;对于在系统启动时就需要使用的,应编译进内核中,比如文件系统、系统总线的支持、USB 驱动、声卡等。

☐ Module unloading (NEW)

该配置项用于设置是否允许卸载不再使用的模块,默认未选择。若选择,则允许卸载不再使用的模块。可根据需要进行选择设置,若选中该配置项,此时还将显示一个新的配置项,用于设置是否允许强行卸载模块。

☐ Forced module unloading (NEW)

以上配置项仅在选中“Module unloading”配置项后,才会出现。

☐ Module versioning support (EXPERIMENTAL)

默认选择,允许使用其他版本的内核编译的模块。

☐ Automatic kernel module loading

默认选择。允许内核在需要某个模块时,能自动调用 modprobe 命令加载该模块。强烈建议选择,不要更改。

(4) Processor type and features(处理器类型和特性)--->

Subarchitecture Type (PC-compatible) --->

在该配置项上按回车,将显示其下级子配置项:

(X) PC-compatible

( ) AMD Elan

( ) Voyager (NCR)

( ) NUMAQ (IBM/Sequent)

( ) SGI 320/540 (Visual Workstation)

默认为 PC 兼容机。目前所使用的 PC 机都是遵循 IBM 兼容结构(PC/AT)的,因此不需要更改。

Processor family (Pentium-Pro) --->

在该配置项上按回车,将显示可供选择的 CPU 类型,默认为 Pentium-Pro,目前的计算机一般是 P4 系列,通常应选择“Pentium-4/Celeron(P4-based)/Pentium-4 M/Xeon”类型。将光亮条移动到“Pentium-4/Celeron(P4-based)/Pentium-4 M/Xeon”类型上,然后按回车键选中。

☐ Generic x86 support (NEW)

该选项提供对 x86 系列 CPU 最大的兼容能力,以支持一些很少见的基于 x86 体系的 CPU。对于能在“Processor family”列表中找到相应型号的 CPU,通常不再需要设置该配置项,选择启动该项功能,会降低一些系统性能。

☐ HPET Timer Support (NEW)

HPET 是高精度事件定时器的缩写,是 Intel 公司制定的用以代替传统 8254(PIT)中断定时器与 RTC 的定时器。默认未选择,对于较新的计算机,通常可以选择启用,启用后,将出现以下新的配置项:

☐ Provide RTC interrupt (NEW)

通常可选择提供 RTC 中断定时器。

☐ Symmetric multi-processing support

默认未选择。若使用的是多处理器的计算机,则应选择启用多处理器支持,若是单 CPU 系统,则不用选择。启动多处理支持后,将进一步显示以下配置项:

(8) Maximum number of CPUs (2-255) (NEW)

该配置项用于设置 Linux 最多支持多少个 CPU,默认为 8 个,可根据需要设置,设置方法是在该配置项上按回车,然后在弹出的输入框中输入支持的 CPU 个数。

☐ SMT (Hyperthreading) scheduler support (NEW)

该配置项用于设置超线程调度支持,通常可选择。

☐ Preemptible Kernel (NEW)

该配置项用于设置是否支持抢先式内核,通常可以选择启用。

☒ Machine Check Exception

默认选择。启用后,当系统出现问题时(比如 CPU 过热),内核将会在屏幕上打印输出相关的提示信息,该功能需要硬件支持。可使用“grep mce /proc/cpuinfo”命令查询 CPU 是否支持该功能,若在/proc/cpuinfo 文件中有 mce 标志,则说明支持,此时就可启用该功能。

< > Check for non-fatal errors on AMD Athlon/Duron /Intel Pentium

该配置项仅在选择“Machine Check Exception”后才有效,默认未选择。对于 AMD Athlon/Duron / Intel Pentium 4 类型的 CPU,可以选择。启用该项功能后,系统将会检

查机器可能存在的问题,若有非致命错误出现,将会自动修复并记录,从而可帮助查找程序出现问题的原因。

< M> Toshiba Laptop support

默认编译为模块。该功能针对 Toshiba 笔记本,启用后可以访问 Toshiha 的系统管理模式,实现直接修改 BIOS。

<M> Dell laptop support

功能与上相同,只针对 Dell 的笔记本。

<M> /dev/cpu/microcode—Intel IA32 CPU microcode support

该配置项允许更新 Intel IA32 系列处理器的微代码。

<M> /dev/cpu/\* /msr—Model-specific register support

该配置项用于支持使用寄存器改变 CPU 原有物理结构的用途。

<M> /dev/cpu/\* /cpuid—CPU information support

该配置项用于支持 CPU 信息查询。

Firmware Drivers -->

在该配置项上按回车,将显示以下子配置项:

< M> BIOS Enhanced Disk Drive calls determine boot disk (EXPERIMENTAL)

该配置项用于打开实模式下 BIOS 中的增强磁盘设备服务,以决定从哪个磁盘上启动。

High Memory Support (4GB) -->

在该配置项上按回车,将显示以下子配置项,用于设置支持的内存大小,默认为 4GB。

( ) off

(X) 4GB

( ) 64GB

对于内存超过 4GB 的,在编译内核时就应注意启用 64GB 内存支持,以便能使用超过 4GB 的内存空间。

[ ] Math emulation

若 CPU 没有数字协处理器,则可选择该配置项让内核来模拟,以提升浮点计算能力。不过目前的计算机一般都有数字协处理器,因此通常不需要选择。

[ \* ] MTRR (Memory Type Range Register) support

在较新的 Intel CPU 中,有一个内存类型范围寄存器,可用来控制处理器访问的内存范围。默认选择启用。

(5) Power management options (ACPI, APM)(高级电源管理) -->

[ \* ] Power Management support

默认选择,使 Linux 支持高级电源管理(如软件关机、系统休眠等)。

[ ] Software Suspend (EXPERIMENTAL)

默认未选择,若选择该功能,则允许 Linux 挂起计算机,以后可使用 swsusp 或者 shutdown -z 命令来挂起计算机。

启用挂起计算机功能后,系统会将当前内存中的内容,作成镜像保存到交换分区中,重新启动时内核就会将上次工作时的内核从镜像文件中恢复到内存。

[ ] Suspend-to-Disk Support

该配置与上面功能基本相同,只是可以通过子选项指定保存内存镜像的交换分区。通常不需要选择。

ACPI (Advanced Configuration and Power Interface) Support -->

在该配置项上按回车,将显示其下级配置菜单:

[ ] ACPI Support

该配置项用于设置是否启用 ACPI 电源管理。默认未选择,当选择启用后,将进一步显示以下配置项,为了实现用 ACPI 来管理计算机电源,还应在系统中安装启动 acpid 守护进程。

[ \* ] Sleep States (EXPERIMENTAL) (NEW)

该配置项允许计算机进入低电能消耗的睡眠状态。

<M> AC Adapter (NEW)

该配置项主要针对笔记本电脑,使 Linux 支持诊断当前使用的是交流适配器供电,还是使用的是电池。

<M> Battery (NEW)

使内核支持通过 `/proc/acpi/battery` 来向用户提供电池的电量状态信息。对于笔记本电脑,可按 Y 键,将其编译进内核。

☐ `<M>` Button (NEW)

该配置项使内核支持基于电源按钮的事件,如 power 和 sleep 等,当按下电源按钮时,事件将发生,一个守护进程程序将读取 `/proc/acpi/event`,并执行用户在这些事件上定义的动作。

☐ `< * >` Fan (NEW)

使内核支持对系统风扇进行控制,比如打开、关闭、读取当前风扇的运行状态等。默认为编译成模块,可按 Y 键,将其编译进内核。

☐ `< * >` Processor (NEW)

使内核支持 CPU 的 IDIE 状态处理能力,即让处理器在空闲时节省电能。按 Y 键,将其编译进内核。

☐ `< * >` Thermal Zone (NEW)

该配置使内核支持当系统温度过高时,ACPI 可以控制系统并及时调整其工作状态,以保护 CPU。按 Y 键,将其编译进内核。

☐ `<M>` ASUS/Medion Laptop Extras (NEW)

该配置项针对 ASUS 笔记本电脑准备的,以提供对这些系统的额外按钮的支持。用户可以通过这些按钮打开或者关闭 LCD 的背光、调整亮度、定制 LED 的闪烁指示等功能。用户也可通过 `/proc/acpi/asus` 来改变这些设置。

☐ `<M>` Toshiba LapTop Extras (NEW)

该配置项用于对 Toshiba 笔记本提供特别的支持。

☐ `[ ]` Debug Statements (NEW)

默认未选择,若启用,当 ACPI 出错时将会打印输出详细信息。

PM (Advanced Power Management) BIOS Support --->

在该配置项按回车,可进入对高级电源管理的设置,通常不需要修改这些配置。

CPU Frequency scaling --->

在该配置项上按回车,可进入对 CPU 频率缩放的详细设置,若对这方面不是很熟悉,建议不要轻易修改。

## (6) Bus options (PCI, PCMCIA, EISA, MCA, ISA) --&gt;

在该配置项上按回车,可进入对总线支持的设置。目前的计算机一般不再使用 ISA 总线, EISA 总线,若要减小内核大小,也可不提供对这些总线的支持。一般情况下,使用系统默认配置即可,不需要作更多的设置修改。

## (7) Executable file formats --&gt;

使用默认配置即可,一般不需要修改。

## (8) Device Drivers --&gt;

该配置项用于设置系统支持的硬件设备,配置项相当多,可根据自己的需要进行设置或删除,若直接编译进内核,则按 Y 键,若编译为模块,则按 M 键。关于网络功能的配置项如下所示:

Device Drivers -->

Networking support -->

[ \* ] Networking support

Networking options -->

< \* > Packet socket

[ \* ] Packet socket: mmaped IO

< \* > Netlink device emulation

< \* > Unix domain sockets

...

[ \* ] Network packet filtering (replace ipchains) -->

--Network packet filtering (replace ipchains)

[ ] Network packet filtering debugging

[ \* ] Bridged IP/ARP packets filtering

IP: Netfilter Configuration -->

< M > Connection tracking (required for masq/NAT)

< M > FTP protocol support

< M > IR protocol support

< > TFTP protocol support

< > Amanda backup protocol support

< M > Userspace queueing via NETLINK

< M > IP tables support (required for filtering/masq/NAT)

< M > limit match support

< M > IP range match support

< M > MAC address match support

< M > Packet type match support

< M > Netfilter MARK match support

< M > Multiple port match support



```
<M> TOS match support
< > recent match support
<M> ECN match support
<M> DSCP match support
<M> AH/ESP match support
<M> LENGTH match support
<M> TTL match support
<M> tcpmss match support
<M> helper match support
<M> Connection state match support
<M> Connection tracking match support
<M> Owner match support
< > Physdev match support
<M> Packet filtering
<M> REJECT target support
<M> Full NAT
<M> MASQUERADE target support
<M> REDIRECT target support
< > NETMAP target support
< > SAME target support
[ ] NAT of local connections (READ HELP)
<M> Basic SNMP-ALG support (EXPERIMENTAL)
<M> Packet mangling
<M> TOS target support
<M> ECN target support
<M> DSCP target support
<M> MARK target support
< > CLASSIFY target support
<M> LOG target support
<M> ULOG target support
<M> TCPMSS target support
<M> ARP tables support
<M> ARP packet filtering
< > ARP payload mangling
< > ipchains (2.2-style) support
< > ipfwadm (2.0-style) support
< > raw table support (required for NOTRACK/TRACE)
< > address type match support
< > realm match support
```

将所有配置项设置修改完毕后,按 Esc 键,会弹出“do you wish to save your new kernel configuration?”的对话框,此时回答 Yes,保存配置。或者直接选择“Save Configuration to an Alternate file”菜单项,保存对内核的配置。

### 5. 编译、安装内核与模块

对内核配置好后,接下来就可以编译安装内核和模块了。

编译压缩形式的内核使用 make zImage 或 make bzImage。若要内核支持较多的外设和功能,直接编译入内核的功能比较多时,内核可能会变得很大,此时应使用 make bzImage 命令来编译生成大内核。

```
[root@rh9 linux-2.6.8.1]# make bzImage # 编译压缩形式的内核
```

编译后的压缩内核位于/src/linux-2.6.8.1/arch/i386/boot/目录下,文件名为 bzImage。

```
[root@rh9 linux-2.6.8.1]# make # 编译内核,需要约 1~2 小时
[root@rh9 linux-2.6.8.1]# make modules # 编译选择的模块
```

内核模块的标准存放位置是/lib/modules/a.b.c 目录中,其中 a.b.c 是内核的版本号,安装新内核之前,需要手工创建存放新内核模块的目录。

```
[root@rh9 linux-2.6.8.1]# mkdir /lib/modules/2.6.8.1
[root@rh9 linux-2.6.8.1]# make modules_install # 将编译后的模块安装到默认位置
[root@rh9 linux-2.6.8.1]# make install # 安装内核
```

最后利用 reboot 命令重新启动 Linux 系统,并查看内核版本是否显示为 2.6.8.1,若是,则升级成功。通过升级内核,可在不重新安装和配置服务器的情况下,获得新内核带来的强大功能,同时还可修补一些已发现的漏洞。

Red Hat Linux 的安全补丁可访问 <http://www.redhat.com/apps/support/updates.html> 网站获得。

## 参 考 文 献

- [1] 金洁瑜,丁娟. Red Hat Linux 9 系统管理,北京:机械工业出版社,2004
- [2] Red Hat Linux 9 x86 安装指南,Red Hat, Inc. ,2003
- [3] Red Hat Linux 9 入门指南,Red Hat,Inc. ,2003
- [4] Red Hat Linux 9 定制指南,Red Hat,Inc. ,2003
- [5] The Official Red Hat Linux Reference Guide,Red Hat. Inc. ,2003