

国家信息产业部全国网络与信息技术培训项目管理中心
广东省Linux公共服务技术支持中心
NTC-Linux系列认证惟一指定教材



Linux系统 管理与开发系列丛书

广东省Linux公共服务技术支持中心
组编

何世晓 主编

张 律 黄锋涛 杜朝辉 黄凤辉 陈 涛 江 冰 编著

Linux

系 统 管 理 师



Linux 系统管理与开发系列丛书

Linux 系统管理师

广东省 Linux 公共服务技术支持中心 组编

何世晓 主编

张 律 黄锋涛 杜朝辉 黄凤辉 陈 涛 江 冰 编著



机械工业出版社

Linux 是当前主流的操作系统之一，不仅在服务器领域占有绝对优势，在桌面领域也发展迅猛。本书着重介绍了 Linux 系统高级配置和 Linux 网络服务器的功能及实用配置。本书理论与实践并重，从操作系统的安装到网络服务的综合配置，采用由浅入深的方式进行讲解，并配有大量的实验，方便用户进行操作，从实践中学会网络服务器的功能及配置方法。

本书为国家信息产业部全国网络与信息技术培训项目管理中心（NTC-MC）和广东省 Linux 公共服务技术支持中心（GDLC）NTC-Linux 认证的指定培训教材。本书适用于参加“Linux 系统管理师”认证的考生以及高校计算机及相关专业的学生、网络工程师、网络管理员、网站维护工程师、系统集成工程师，还可作为广大 Linux 爱好者的参考书。

图书在版编目（CIP）数据

Linux 系统管理师 / 何世晓主编；广东省 Linux 公共服务技术支持中心组编. —北京：机械工业出版社，2009.8

（Linux 系统管理与开发系列丛书）

ISBN 978-7-111-28145-0

I. L … II. ①何…②广… III. Linux 操作系统 IV. TP316.89

中国版本图书馆 CIP 数据核字（2009）第 151227 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：丁 诚

责任编辑：车 忱

责任印制：乔 宇

北京双青印刷厂印刷

2009 年 9 月第 1 版 · 第 1 次印刷

184mm × 260mm · 24.5 印张 · 604 千字

0 001-4 000 册

标准书号：ISBN 978-7-111-28145-0

定价：43.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

销售服务热线电话：（010）68326294 68993821

购书热线电话：（010）88379639 88379641 88379643

编辑热线电话：（010）88379753 88379739

封面无防伪标均为盗版

Linux 系统管理与开发系列丛书编委会

丛书主编:

袁 泉: 广东省 Linux 公共服务技术支持中心 主任

广东省开源软件产业发展促进委员会 会长

广东省职业技能鉴定指导中心 Linux 体系专家组 组长

胡 铮: 国家信息产业部全国网络与信息技术培训项目管理中心 主任

丛书编委:

张 延: 国家信息产业部全国网络与信息技术培训项目管理中心市场部 主任

赵世奎: 国家信息产业部全国网络与信息技术培训项目管理中心市场部 项目主任

韩小莲: 广东省 Linux 公共服务技术支持中心培训部 部长

广东省开源软件产业发展促进会 副秘书长

广东省高校 Linux 推进联盟 秘书长

广东省职业技能鉴定指导中心 Linux 体系专家组 专家

余世清: 广东省 Linux 公共服务技术支持中心技术部 部长

何世晓: 广东省 Linux 公共服务技术支持中心培训部 技术总监

广东省职业技能鉴定指导中心 Linux 体系专家组 专家

黄道金: 广东省 Linux 公共服务技术支持中心培训部 技术副总监

黄锋涛: 广东省 Linux 公共服务技术支持中心培训部 特邀培训顾问

丛 书 序

从 1946 年世界上第一台电子计算机诞生开始,计算机的发展已走过了六十多个春秋,科学技术的日新月异,为我们开启了一个无比辉煌的电子时代。1991 年,芬兰赫尔辛基的大学生 Linus Torvalds 开发了 Linux 操作系统,经过短短的 16 年, Linux 已发展成为当今最流行的操作系统之一。

Linux 具有源代码开放、性能卓越、安全可靠等与生俱来的特点。在信息化建设中,无论从稳定性、安全性以及价格等方面来看, Linux 都具有明显的优势。长期以来,我国一直处在商业操作系统的垄断下,严重阻碍了我国自主软件产业的发展。Linux 的出现,为我们提供了一个自由分享人类科学成果的机会,为我国软件产业的发展提供了一个良好的契机。因而, Linux 在我国信息化建设中将担当起特殊的历史使命,必将使民族软件产业在自主创新的道路上走得更远。

目前, Linux 已经在我国电子政务、电信、金融、教育等信息化建设领域崭露头角,但其普及的深度和广度还远远不够。因此,如何利用 Linux 进一步推动我国信息化建设已成为一个备受瞩目的课题。如今,社会对 Linux 专业人才的需求不断扩大,在今后的几年内,高水平的 Linux 专业人才无疑将成为 IT 领域乃至整个就业市场中的热点, Linux 人才的培养迫在眉睫。而 Linux 在我国发展至今,还没有一个权威的国家级 Linux 技能认证,显然不利于 Linux 人才的培养与选拔。

正是在这样的背景下,国家信息产业部全国网络与信息技术培训项目管理中心(NTC-MC)与广东省 Linux 公共服务技术支持中心(GDLC)联合开发了“NTC-Linux 系列认证”体系,并推出具有实用性、可读性、权威性的“Linux 系统管理与开发系列丛书”。这是我国在培养 Linux 专业人才方面的一件喜事,也是 GDLC 务实推进我国开源软件发展战略布局中的一个重要举措。

这套丛书共 6 本,它们分别是《Linux 系统管理员》、《Linux 系统管理师》、《Linux 系统高级管理师》、《Linux 系统开发员》、《Linux 系统开发师》、《Linux 系统高级开发师》。该丛书内容全面,自成体系,几乎涵盖了 Linux 系统管理与开发的各个方面。

我们有理由相信,这套丛书将进一步推动开源软件在中国的普及,为促进中国软件产业的发展做出积极的贡献。

广东开源软件产业发展促进委员会会长
广东省 Linux 公共服务技术支持中心主任

袁泉

前 言

Linux 具有安全、可靠、稳定、开源、自由使用的特点。不仅在服务器端占有绝对的优势，在桌面领域发展也很迅猛。Linux 在各大中小型企业、电信、金融、银行、政府、学校应用都非常广泛。近几年 Linux 处于快速发展阶段，应用面越来越广，从服务器端的优势逐渐发展到嵌入式、应用开发、桌面办公等领域。

为什么要写本书

Linux 的飞速发展，导致 Linux 人才的大量缺乏，各跨国企业均出现了 Linux 人才供不应求的局面。而一些想进入 Linux 行业的技术人员因没有统一完整的学习资料而无法很好地学习。另一方面，IT 行业发展至今，还没有出现一个权威的国家级 Linux 技能认证。为了更好地指导 Linux 爱好者和 IT 业内开发人士学习 Linux 技术，同时获得权威的 Linux 系统类技能认证，国家信息产业部全国网络与信息技术培训项目管理中心(简称 NTC-MC)与广东省 Linux 公共服务技术支持中心(简称 GDLC)联合开发了“NTC-Linux 系列认证”体系，将陆续推出一系列实用、可操作、易读、权威的 Linux 系统类教材。

本书的主要内容

本书是 NTC-Linux 系列丛书系统部分的中级教程，也是认证级别为“NTC-Linux 系统管理员”的指定教程。

本书主要内容包括系统引导程序，Linux 交换空间管理，LVM 逻辑卷管理，RAID 磁盘冗余阵列管理，日志分析及备份管理，性能分析工具，Shell 高级编程，内核升级及其配置，Linux 常用网络配置文件，远程管理 Linux 系统，DHCP 服务器，DNS 服务器，Web 服务器的配置与管理，MySQL 服务器的配置与管理，加速 LAMP，FTP 服务器，Sendmail、Postfix 邮件服务的安装与配置，Squid 代理服务，系统安全策略与配置，PAM 概述与工作原理，网络服务安全配置。

本书的特点

1. 循序渐进，由浅入深

为了方便读者学习，本书首先带领读者深入地了解了 Linux 系统模块，再对网络基础进行介绍，最后进入常用网络服务的配置。在进行网络服务器配置时，采用由浅入深的方式进行讲解。最后通过案例的方式进行实验。从而读者可以边学习，边动手，更快地掌握 Linux 网络服务器的各种知识。

2. 实例精讲，内容充实

在编写本书的过程中，作者花费大量的时间在实验配置上，力求在进行实验配置的过程中，做到准确无误，如本书的 bind、dhcp、vsftpd 服务器的配置实验等，以提高实验的完整性和可操作性。

3. 企业案例、分析重现

本书在采用大量实验的过程中，还加入了一些企业案例，如本书的 DNS 配置、网络服务器的配置、文件服务器的配置、企业级代理服务服务器的配置，都采用一些案例重现。

4. 提供完善的售后服务

为了方便读者学习，读者可登录 <http://www.gd-linux.org> 的论坛进行讨论。读者可以将自己遇到的问题发布在该版面，论坛版主将帮助大家一起解决问题。

本书适合的读者

本书为 NTC-MC 和 GDLC 联合认证的指定认证教材，适合于参加“Linux 系统管理师”认证的考生，以及各大高校计算机及相关专业的学生，也可供广大 Linux 技术人员参考使用，还可作为广大 Linux 爱好者的参考书。

本书的创作团队

本书创作团队中有广东省 Linux 公共服务技术支持中心的高级工程师、高级培训讲师，有广东各大高校的高级讲师、政府高级工程师及外企的高级工程师。他们均专职从事开源软件和 Linux 操作系统的开发管理与推广工作。

本书的第 4、5、8、9、18 章由何世晓执笔，第 1、10、11、12、16、21 章由张律执笔，第 14 章由黄锋涛执笔，第 2、3、20 章由杜朝辉执笔，第 13、15、17 章由黄凤辉执笔，第 6、7、19 章由陈涛和江冰执笔。全书由何世晓统稿，韩小莲、何世晓进行审核，何世晓、张律从技术方面对全书进行审稿。

致谢

本书的写作过程中，得到了 GDLC 中心主任袁泉博士的大力支持，同时得到了培训部、技术部全体同仁的大力支持。另外还要感谢各位作者的家人，感谢他们对团队成员的关心、鼓励与支持！

作者
2009 年 3 月

目 录

丛书序

前言

第 1 章 Linux 系统概述	1	3.2 Linux 交换空间管理	25
1.1 Linux 系统发展概况	1	3.2.1 交换空间工作原理	25
1.1.1 Linux 的起源	1	3.2.2 交换分区创建及管理	26
1.1.2 GNU、FSF、开放源码与 Linux 的发展	2	3.2.3 交换文件创建及管理	28
1.2 Linux 的特点	2	3.3 LVM 逻辑卷管理	29
1.3 Linux 的版本	4	3.3.1 LVM 工作原理	29
1.3.1 狭义 Linux	4	3.3.2 LVM 名词与术语	29
1.3.2 广义 Linux	4	3.3.3 LVM 配置实例	31
1.4 Linux 的应用与前景	6	3.4 RAID 磁盘冗余阵列管理	34
1.4.1 桌面应用	6	3.4.1 RAID 种类及其工作原理	35
1.4.2 网络服务器	7	3.4.2 RAID 名词与术语	38
1.4.3 嵌入式系统	7	3.5 RAID 配置实例	40
1.4.4 集群计算机	8	3.5.1 mdadm 工具	40
1.4.5 Linux 的发展前景	8	3.5.2 划分硬盘分区	41
第 2 章 系统引导程序	9	3.5.3 配置 RAID 0	42
2.1 启动引导器	9	3.5.4 配置 RAID 1	44
2.1.1 GRUB 基本配置	9	3.5.5 配置 RAID 5	46
2.1.2 GRUB 多系统引导配置实例	11	第 4 章 日志分析及备份管理	51
2.2 Linux 系统的启动过程及 相关配置文件	12	4.1 日志子系统	51
2.2.1 Linux 计算机系统启动过程	12	4.1.1 日志分析	51
2.2.2 系统启动配置文件	14	4.1.2 日志查看方法	52
2.2.3 服务脚本文件	16	4.1.3 常用日志分析工具	55
2.3 启动过程故障分析及修复	18	4.1.4 日志定制	55
2.3.1 单用户模式	18	4.1.5 日志循环管理	56
2.3.2 修复文件系统	20	4.2 系统备份	57
2.3.3 使用 GRUB 程序修复系统启动	20	4.2.1 备份的重要性	58
2.3.4 系统启动修复实例	22	4.2.2 备份策略	59
第 3 章 高级磁盘管理	24	4.2.3 备份介质的选择	59
3.1 文件系统概述	24	4.3 备份技术及分类	60
3.1.1 磁盘管理基础知识	24	4.3.1 完全备份	60
3.1.2 磁盘分区、格式化及磁盘配额	24	4.3.2 增量备份	60
		4.3.3 差分备份	61
		4.4 备份内容	61

4.5 常用备份工具	62	6.2.6 无条件控制语句 break 和 continue	90
4.5.1 Xtar	62	6.2.7 函数定义	90
4.5.2 KDat	62	6.2.8 命令分组	90
4.5.3 taper	63	6.2.9 信号	90
4.5.4 tar	63	6.3 Shell 函数与函数调用	91
4.5.5 cpio	63	6.3.1 在脚本中使用函数	92
4.5.6 dump 和 restore	64	6.3.2 向函数传递参数	93
4.5.7 dd	65	6.3.3 函数返回值	93
4.5.8 cp	65	6.3.4 函数返回值测试	93
第 5 章 系统及环境管理	67	6.3.5 在 Shell 中使用函数	94
5.1 系统性能指标	67	6.3.6 创建函数文件	94
5.2 影响性能的因素	67	6.3.7 定位文件	94
5.2.1 使用磁盘阵列提速	67	6.3.8 检查载入函数	95
5.2.2 swap 分区优化设置	68	6.4 awk 工具和 sed 工具	95
5.2.3 sysctl 文件设置	69	6.4.1 awk 工具	95
5.3 性能分析工具	70	6.4.2 sed 工具	99
5.3.1 vmstat 工具	70	6.5 Shell 脚本实例	102
5.3.2 top 工具	72	6.5.1 清除/var/log 下的日志文件	102
5.3.3 mpstat 工具	74	6.5.2 一个改良的清除脚本	102
5.3.4 iostat 工具	75	6.5.3 一个增强的和广义的删除 日志文件的脚本	102
5.3.5 sar 测试工具	76	第 7 章 内核升级及其配置	104
5.3.6 ps 工具	78	7.1 内核概述	104
5.3.7 uptime 工具	79	7.2 基于 2.6.x 内核的配置	105
5.3.8 free 命令	79	7.2.1 2.6.x 内核的新特性	105
5.3.9 netstat 工具	80	7.2.2 2.6.x 内核配置项	106
5.3.10 ipcs 工具	80	7.2.3 2.6.x 内核配置实例	107
5.3.11 GlancePlus 工具	81	7.3 内核启动及内核升级 常见故障	113
5.4 性能优化的思路	82	7.3.1 以新内核启动系统	113
第 6 章 Shell 编程	83	7.3.2 内核升级常见故障及解决	113
6.1 Shell 概述	83	7.4 定制内核	114
6.1.1 什么是 Shell	83	7.4.1 定制内核的意义	114
6.1.2 Shell 的作用	83	7.4.2 内核定制实例	114
6.1.3 不同类型的 Shell	86	第 8 章 TCP/IP 协议体系	117
6.2 Shell 流程控制	87	8.1 网络体系概念	117
6.2.1 测试命令	87	8.1.1 计算机网络	117
6.2.2 if 条件语句	88	8.1.2 网络协议	117
6.2.3 case 条件选择	88		
6.2.4 for 循环	89		
6.2.5 while 和 until 循环	89		

8.1.3 网络寻址	118	9.1.7 nslookup 命令	137
8.2 ISO 参考模型	118	9.1.8 wget 命令	138
8.2.1 OSI 参考模型概述	118	9.2 Linux 常用网络配置文件	139
8.2.2 各层的功能	118	9.2.1 /etc/nsswitch.conf	139
8.2.3 工作原理	119	9.2.2 /etc/services	141
8.3 TCP/IP 参考模型	120	9.2.3 /etc/resolv.conf	141
8.3.1 TCP/IP 参考模型概述	120	9.2.4 /etc/sysconfig/network	142
8.3.2 TCP/IP 和 OSI 参考模型的对比	120	9.2.5 /etc/sysconfig/network-scripts/ ifcfg-eth0	142
8.4 IP 地址	121	第 10 章 远程管理 Linux 系统	143
8.4.1 IP 地址概述	121	10.1 Telnet 服务	143
8.4.2 IP 地址的分类	121	10.1.1 安装 Telnet 服务	143
8.4.3 A 类 IP 地址	121	10.1.2 启动 Telnet 服务	143
8.4.4 B 类 IP 地址	122	10.1.3 配置 Telnet 服务	144
8.4.5 C 类 IP 地址	122	10.2 SSH 服务	145
8.4.6 其他类	122	10.2.1 启动 SSH 服务	145
8.5 IP 地址的寻址规则	122	10.2.2 SSH 客户端连接	145
8.5.1 网络寻址规则	122	10.2.3 SSH 服务的常规配置	151
8.5.2 主机寻址规则	123	10.2.4 SSH 密钥认证原理	152
8.6 子网划分、子网计算		10.2.5 SSH 密钥认证配置	153
命令 ipcalc	123	10.3 VNC 服务管理	154
8.6.1 子网划分方法	123	10.3.1 启动 VNC 服务器	154
8.6.2 ipcalc 命令的使用	123	10.3.2 VNC 客户端访问配置	154
8.7 IP 路由、路由设置命令		10.3.3 VNC 后台服务	156
route	125	10.4 Webmin	157
8.7.1 路由的定义	125	10.4.1 Webmin 应用	157
8.7.2 路由的方式	125	10.4.2 安装并配置 JRE	159
8.7.3 静态路由	125	第 11 章 DHCP 服务器	161
8.7.4 动态路由	125	11.1 DHCP 简介	161
8.7.5 route 命令的使用	126	11.2 DHCP 的工作原理	162
第 9 章 Linux 网络命令及配置		11.3 安装 DHCP 服务器	163
文件	128	11.4 DHCP 服务配置	163
9.1 Linux 常用网络命令	128	11.4.1 DHCP 服务主配置文件	163
9.1.1 ifconfig 命令	128	11.4.2 DHCP 服务的客户租约 文件	166
9.1.2 netconfig 命令	130	11.4.3 DHCP 客户端的配置	167
9.1.3 ethtool 命令	132	11.5 DHCP 服务应用	167
9.1.4 mii-tool 命令	133	11.5.1 共享作用域	168
9.1.5 netstat 命令	135	11.5.2 多作用域	168
9.1.6 chkconfig 命令	136		

11.6 Linux 网络安装服务器架设 ...	169	与管理	214
11.6.1 工作流程	170	14.1 MySQL 服务概述	214
11.6.2 实现步骤	170	14.2 MySQL 服务的安装与配置 ...	214
第 12 章 DNS 服务器	172	14.2.1 获取 MySQL	215
12.1 DNS 服务概述	172	14.2.2 安装准备工作	215
12.1.1 域名系统	172	14.2.3 开始安装	215
12.1.2 域名解析过程	174	14.3 MySQL 的管理	216
12.1.3 DNS 的服务资源记录	174	14.3.1 启动 MySQL	217
12.1.4 BIND 服务简介	176	14.3.2 停止 MySQL	217
12.1.5 DNS 服务器的安装和启动	176	14.3.3 管理 MySQL 用户	217
12.2 DNS 服务配置	176	14.3.4 常用 MySQL 命令	218
12.2.1 与 DNS 相关的两个文件	176	14.3.5 创建 MySQL 表	219
12.2.2 BIND 服务配置	177	14.3.6 将文本导入数据库	220
12.2.3 DNS 客户端配置	181	14.3.7 导出/导入数据	220
12.2.4 DNS 服务器的其他配置	184	14.3.8 备份和恢复数据	222
12.2.5 DNS 配置常见问题	185	14.3.9 开机自动启动 MySQL	224
12.3 DNS 服务配置实例	185	第 15 章 LAMP 概述	227
第 13 章 Web 服务器的配置与		15.1 LAMP 的概念	227
管理	189	15.2 LAMP 的安装	227
13.1 Web 服务器简介	189	15.2.1 PHP 语言概述	227
13.2 Apache 的安装配置	189	15.2.2 PHP 软件包的安装	228
13.2.1 Apache 的安装	189	15.2.3 PHP 软件的安全配置	230
13.2.2 Apache 的启动与停止	190	15.2.4 Perl 语言概述	232
13.3 Apache 的全局环境配置	191	15.2.5 Python 语言概述	233
13.3.1 全局环境配置	192	15.3 加速 LAMP	235
13.3.2 Apache 的主服务器配置	195	15.3.1 Apache 加速	235
13.3.3 Apache 的高级管理配置	197	15.3.2 PHP 加速	237
13.3.4 Apache 身份认证	200	15.4 LAMP 应用实例	238
13.3.5 虚拟主机的配置	200	15.4.1 软件的简介	238
13.4 Apache 对 JSP 语言的支持	202	15.4.2 安装 MySQL	239
13.4.1 JSP 的特点	202	15.4.3 安装 httpd	240
13.4.2 安装与配置 JSP 的工作		15.4.4 安装 PHP	240
环境	202	15.4.5 安装 Zend Optimizer	241
13.5 日志文件的管理	206	15.4.6 安装 PHPMyAdmin	241
13.5.1 错误日志	206	15.4.7 安装 PHPwind	242
13.5.2 访问日志	207	第 16 章 FTP 服务器	245
13.6 Apache 配置应用实例	208	16.1 FTP 服务器概述	245
13.7 Web 服务器安全——SSL	212	16.1.1 FTP 服务的工作原理	245
第 14 章 MySQL 服务器的配置		16.1.2 流行的 FTP 服务器	246

16.2 vsftpd 服务配置	246	18.1.1 代理服务概述	284
16.2.1 启动 vsftpd 服务	246	18.1.2 Squid 代理服务概述	285
16.2.2 vsftpd 服务配置文件	247	18.2 实现 Squid 服务	285
16.2.3 vsftpd 服务用户控制文件	250	18.2.1 安装 Squid	285
16.3 vsftpd 服务器设置实例	251	18.2.2 squid.conf 文件基本配置	287
16.4 vsftpd 客户端访问	252	18.2.3 运行 Squid	287
16.5 vsftpd 虚拟用户	255	18.2.4 客户端配置	288
16.5.1 虚拟用户的创建和实现	256	18.3 Squid 服务配置与应用	289
16.5.2 虚拟用户设置	257	18.3.1 Squid 服务配置选项	289
第 17 章 电子邮件系统	259	18.3.2 访问控制	292
17.1 电子邮件系统概述	259	18.3.3 正向代理应用示例	297
17.1.1 电子邮件系统的组成	259	18.3.4 Web 加速-反向代理	
17.1.2 电子邮件传送协议 SMTP	260	应用示例	299
17.1.3 邮局协议和因特网消息		18.3.5 其他应用	301
存取通信协议	260	18.3.6 配置文件示例	302
17.2 Sendmail 电子邮件服务	261	第 19 章 Linux 系统安全	305
17.2.1 Sendmail 邮件服务的概述	261	19.1 系统安全概述	305
17.2.2 Sendmail 邮件服务器配置		19.1.1 从安全角度看开源软件	305
实例	261	19.1.2 系统安全性和评价	306
17.3 Postfix 邮件服务的安装		19.1.3 安全基础知识	306
与配置	263	19.1.4 系统用户和管理	307
17.3.1 Postfix 的特点	264	19.1.5 数据加密	309
17.3.2 Postfix 的邮件队列与		19.2 系统安全策略与配置	310
配置文件	264	19.2.1 定义安全策略和模型	310
17.3.3 Postfix 常用参数的介绍	265	19.2.2 配置实例	311
17.4 Postfix 的配置实例	267	19.3 PAM 概述与工作原理	312
17.4.1 软件的简介	268	19.3.1 什么是 Linux-PAM	312
17.4.2 安装前准备	269	19.3.2 PAM 的分层体系结构	313
17.4.3 安装 MySQL	270	19.3.3 口令映射	314
17.4.4 安装 httpd 和 PHP 软件包	271	19.4 安全工具	315
17.4.5 安装 courier-authlib	271	19.4.1 nmap 和 nessus 网络安全	
17.4.6 安装 cyrus-sasl	273	扫描工具	316
17.4.7 安装 postfix 2.2.3	274	19.4.2 弱点测试工具	317
17.4.8 安装 courier-imap	277	19.4.3 Sxid 和 Skey	317
17.4.9 安装 postfixadmin	278	19.4.4 日志工具 (logrotate, swatch,	
17.4.10 安装 squirrelmail	280	logcheck)	318
17.4.11 整体测试	281	19.4.5 SSH 和 Tripwire	320
第 18 章 Squid 代理服务	284	19.4.6 反扫描工具 Portsentry	322
18.1 Squid 代理服务概述	284	19.4.7 OpenSSL	323



19.4.8 Linux FreeS/WAN VPN	324	设置	346
第 20 章 Linux 网络服务安全	328	20.2.10 拒绝服务攻击和入侵检测	349
20.1 网络服务安全概述	328	20.2.11 拒绝服务攻击和入侵检测	
20.1.1 网络服务安全含义	328	工具	353
20.1.2 网络服务安全考虑因素	328	第 21 章 Linux 下的防火墙配置	361
20.2 网络服务安全配置	333	21.1 Linux 下的防火墙	361
20.2.1 FTP 安全配置	333	21.1.1 防火墙的基本原理	361
20.2.2 邮件安全配置	335	21.1.2 iptables 工作原理	363
20.2.3 Telnet 和 SSH 安全配置	337	21.2 iptables 防火墙组件	364
20.2.4 Web 服务器安全配置	338	21.2.1 iptables 的元素	364
20.2.5 DHCP 安全配置	341	21.2.2 iptables 工作流程	366
20.2.6 DNS 安全配置	342	21.3 iptables 的安装和实施	369
20.2.7 NFS 文件系统的安全配置	344	21.3.1 iptables 的安装和启动	369
20.2.8 Samba 文件系统的安全配置	344	21.3.2 iptables 的语法	369
20.2.9 tcp-wrapper 及 xinetd 安全		21.3.3 iptables 应用实例	372

第

1

章

Linux 系统概述

本章主要内容

- Linux 系统发展概况
- Linux 的特点
- Linux 的版本
- Linux 的应用与前景

▶▶ 1.1 Linux 系统发展概况

Linux 从诞生之日起就是一套用户可以免费获得、使用并且自由传播的类 UNIX 操作系统，它由世界各地成千上万的程序员共同设计和实现，是不受任何商品化软件版权制约的、任何人都能自由使用的 UNIX 兼容产品。

▶▶▶ 1.1.1 Linux 的起源

Linux 是一种类 UNIX 操作系统，它在源代码级上兼容绝大部分 UNIX 标准（如 IEEE POSIX、System V、BSD 等），它是一个支持多用户、多进程、多线程、实时性较好的功能强大而且稳定的操作系统。Linux 可以运行在多种硬件平台上（如 x86 PC、Sun SPARC、Digital Alpha、680x0、PowerPC、MIPS 等），它是目前支持硬件平台最多的操作系统。

1990 年，芬兰赫尔辛基大学的学生 Linus Torvalds 用汇编语言编写了一个在 80386 保护模式下处理多任务切换的程序，后来他从 MINIX 系统（由 Tanenbaum 教授设计的微型类 UNIX 操作系统，主要用于操作系统教学）获得启发，编写了一些硬件的设备驱动程序和一个小的文件系统，从而诞生了所谓 0.0.1 版本的 Linux 系统，不过该系统只具有操作系统内核的雏形，而且必须在有 MINIX 的机器上编译后才能运行。

1991 年 10 月 5 日 Linus Torvalds 发布了 0.0.2 版本的 Linux 系统，该版本已经可以运行 Bash（the GNU Bourne Again Shell，一种用户与操作系统内核通信的软件）和 gcc（GUN C 编译器）。

1993 年底 Linux 1.0 版本发布，该版本已经是一个功能完备的操作系统，而且内核写得紧凑高效，可以充分发挥硬件的性能，在 4MB 内存的 80386 PC 上也表现得非常好，从此 Linux 开始走上飞速发展的道路，新版本不断推出，性能也越来越强大。

Linux 系统具有良好的兼容性和可移植性，大约在 1.3 版本以后，它开始向更多硬件平台上移植。自 2.1.x 系列内核开始，Linux 系统开始走高端路线，实践证明 Linux 系统不仅在低



端硬件平台能将硬件的性能充分发挥出来，在高端平台上更能将系统性能发挥得淋漓尽致。

1.1.2 GNU、FSF、开放源码与 Linux 的发展

1984 年，理查德·斯塔尔曼（Richard M. Stallman）首先开创了自由软件体系（GNU），并拟定了体系规则即通用公共许可——GPL（General Public License），GNU 旨在发展一个可自由使用的、类 UNIX 的完整操作系统，即 GNU 系统（GNU 是“GNU is Not UNIX”的首字母缩写）。

GPL 是 GNU 工程所要遵循的规则，按照这一规则，自由软件允许用户自由复制、修改和销售，但是对其源代码的任何修改都必须向所有用户公开，所有人都可以自由地使用自由软件，所有人为自由软件所做出的成果必须和其他人共享。

自由软件基金会（Free Software Foundation, FSF）是 GNU 工程的主要赞助组织，该组织主要致力于消除对计算机程序在复制、分发、修改等方面的限制。

开放源码软件有三个优势：免费分发的源代码、模块化的体系和社区式的开发。由于将程序中的错误公开给数量巨大的用户，社区式的开发过程给开放源码软件以强大的纠错能力；另一方面，任何人都可以复制和发行开放源码软件的代码，这支持了公众利益；开放源码带来了一个更民主的开发方式，在这种方式下，好的思路将被集体共享，而不是作为智力资本被个人独占。

在 GNU 和 Linux 的发展过程中，Linux 系统加入 GNU 是个跨时代的事件，因为当时 GNU 已经有了比较完善的软件体系了，所欠缺的只是一个可作为核心的操作系统内核，而 Linux 加入 GNU 并遵循 GPL 就如同给汽车装配了功能强劲的发动机，同时几乎所有 GNU 库/软件都可移植到 Linux 上，这也完善并提高了 Linux 的实用性。

如今，各种使用 Linux 作为内核的 GNU 操作系统正在被广泛地使用，虽然这些系统通常被称为 Linux，但因为它们实际上是由 Linux 内核及各种 GNU 软件组合而成的，所以更准确的称呼应该是 GNU/Linux 系统。

1.2 Linux 的特点

Linux 操作系统支持在其他 UNIX 操作系统中能找到的大部分功能，还包括 UNIX 系统某些版本中没有的功能。

Linux 具有以下主要特点。

（1）开放性。开放性是指系统遵循世界标准规范，特别是遵循开放系统互连（OSI）国际标准，凡遵循国际标准所开发的硬件和软件都能彼此兼容，可方便地实现互连。

（2）多用户。多用户是指系统资源可以被不同用户拥有，即每个用户对自己的资源（如文件、设备等）有特定的权限而互不影响，Linux 和 UNIX 都具有多用户的特性。

（3）多任务。多任务是现代计算机的最主要的一个特点，它是指计算机同时执行多个程序，而且各个程序的运行互相独立。Linux 系统调度每一个进程平等地访问 CPU，由于 CPU 的处理速度非常快，其结果是启动的应用程序看起来好像在并行运行。

（4）良好的用户界面。Linux 向用户提供了两种界面：用户界面和系统调用。

Linux 的传统用户界面是基于文本的命令行界面，即 Shell，Shell 有很强的程序设计能力，

会出现库代码在内存中有多个副本而浪费存储空间的情况。Linux 支持动态链接方式，当运行时才进行库链接，如果所需要的库已被其他进程装入内存则不必再装入，否则才从硬盘中将库调入，这样能保证内存中的库程序代码是唯一的。

(10) 支持多种文件系统。目前 Linux 支持的文件系统有 Ext2、Ext3、XIAFS、ISOFS、HPFS、MSDOS、UMSDOS、PROC、NFS、SYSV、MINIX、SMB、UFS、NCP、VFAT、NTFS、AFFS、JFS、XFS、ReiserFS 等近百种，这有赖于 Linux 采用的虚拟文件系统（VFS）机制。

▶▶ 1.3 Linux 的版本

实际上 Linux 有狭义和广义两层含义，狭义的 Linux 是指 Linux 的内核（Kernel），内核可以完成如进程管理、内存管理、设备驱动等操作系统的基本功能，但是不包含应用程序，广义的 Linux 是指以 Linux 内核为基础，包含 GNU 应用程序和相关的系统设置与管理工具的完整操作系统。

▶▶▶ 1.3.1 狭义 Linux

到目前为止，Linux 的内核仍然由 Linus Torvalds 领导下的开发小组负责开发。开发小组根据 Linux 内核的开发批次和状态为内核设置了内核版本号。

Linux 的内核版本号由 3 个数字组成，一般表示为 X.Y.Z 形式。

- X：表示主版本号，一般在一段时间内比较稳定。
- Y：表示次版本号，如果是偶数，代表这个内核版本是正式版本，可以公开发行，如果是奇数，则代表这个内核版本是测试版本，还不太稳定，仅供测试。
- Z：表示修改号，这个数字越大，表明修改的次数越多，版本也越完善。

Linux 的正式版本与测试版本是相互关联的。正式版本只针对上个版本的严重缺陷进行修改。而测试版本在正式版本的基础上继续增加新的功能，当测试版本被证明稳定后，就成为正式版本。正式版本和测试版本不断循环，不断完善内核的功能。

例如，版本号为 2.6.15 的内核的主版本号为 2，次版本号是 6，因为次版本号是偶数，所以这是一个稳定版本，最后一个数字 15 表示这个版本是自 2.6 版本的内核发行以来经过 15 次修改以后发行的一个版本，而版本号为 2.5.12 的内核明显是一个测试版本的内核，因为它的次版本号是奇数。

在编写本书的时候，Linux 内核的最新版本是 2.6.28.7，要获得关于 Linux 内核最全面的信息，可以访问 Linux 内核的工程网站 <http://www.kernel.org>。

▶▶▶ 1.3.2 广义 Linux

随着时代发展，为了更好地促进 GNU 事业，GNU 也对原有的 GPL 做了一些变通，如在遵循公共版权许可证和在继承自由软件精神的前提下，不再排斥对自由软件的商业行为（如把自由软件打包以光盘形式出售），不排斥商家对自由软件的进一步开发，不排斥在 Linux 上开发商业软件。

在以上的原则规定下，不同厂商、组织甚至个人将 Linux 内核与其他 GNU 开源软件组合，并开发相关的管理工具，从而形成不同的 Linux 发行版本，即广义的 Linux。