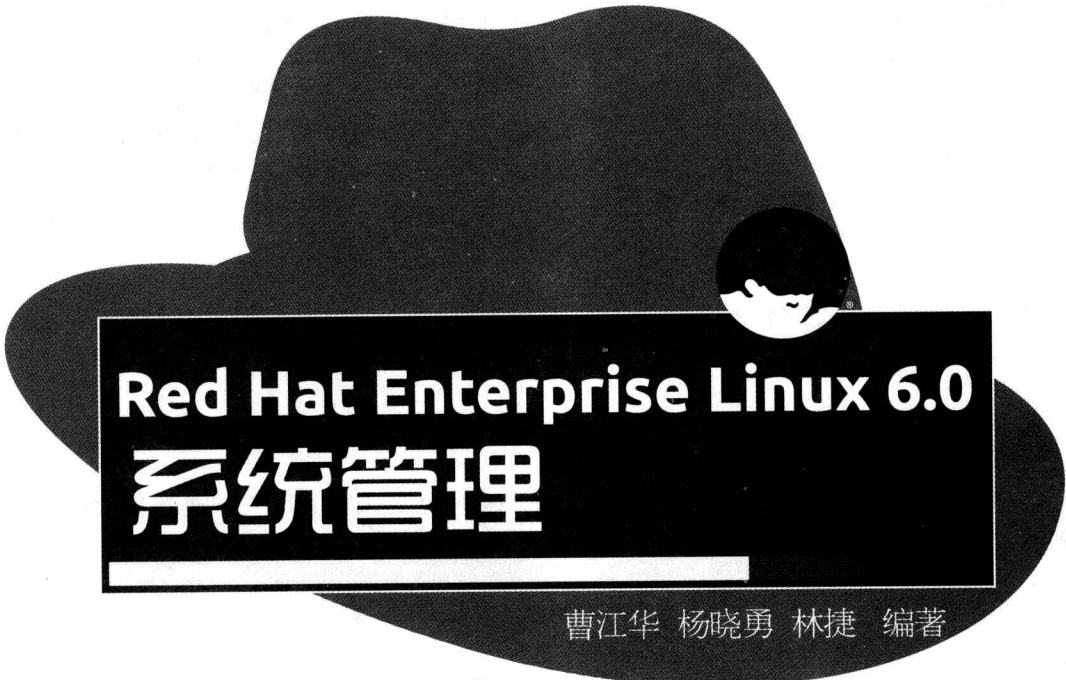




Red Hat Enterprise Linux 6.0 系统管理

曹江华 杨晓勇 林捷 编著





Red Hat Enterprise Linux 6.0 系统管理

曹江华 杨晓勇 林捷 编著

电子工业出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

本书以 RHEL 6.0 为蓝本, 包括 19 章和 1 个附录, 主要介绍了 Linux 操作系统的基本使用和系统管理。主要包括自由软件和开源软件的基础知识、Linux 的基础知识、RHEL 6.0 的安装、软件包管理、用户管理、磁盘管理和 LVM 管理、文件系统管理、TCP/IP 网络配置、系统引导和启动、守护进程管理、系统备份与恢复、虚拟化应用、日志管理、使用 Webmin、Linux iSCSI 和 AoE 存储配置、SELinux 使用、内核审计、打印机管理、防火墙设置和升级、Linux 性能和系统监控、桌面应用等内容。本书内容详尽、结构清晰、通俗易懂, 使用了大量图表对内容进行表述和归纳, 便于读者理解及查阅, 具有很强的实用性和指导性。书中内容适用于 RHEL 6.0, 其中绝大部分内容同时也适用于其他主要发行版本。

本书可以作为高等院校相关专业、Linux 短期培训班的教材, 同时也可供广大 Linux 爱好者自学使用。

未经许可, 不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有, 侵权必究。

图书在版编目(CIP)数据

Red Hat Enterprise Linux 6.0 系统管理/ 曹江华, 杨晓勇, 林捷编著. —北京: 电子工业出版社, 2011.7
ISBN 978-7-121-13746-4

I. ①R... II. ①曹... ②杨... ③林... III. ①Linux 操作系统 IV. ①TP316.89

中国版本图书馆 CIP 数据核字 (2011) 第 102773 号

策划编辑: 李 冰

责任编辑: 李云静

特约编辑: 赵树刚

印 刷: 北京中新伟业印刷有限公司

装 订: 北京中新伟业印刷有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 787×1092 1/16 印张: 32.75 字数: 860 千字

印 次: 2011 年 7 月第 1 次印刷

印 数: 4000 册 定价: 58.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

Linux 应用早已从几年前的盲目推进和前一段的低迷期走出来,更具理性,更重实效的 Linux 应用时代即将到来。在以美国为首的发达国家, Linux 早已涉足政府办公、军事战略及商业运作的方方面面。在我国,随着国民经济与社会信息化的进一步深入, Linux 在电子政务、电子商务等各个信息化建设领域中也突显其不凡之处。Linux 这个免费的开放源代码的操作系统正以狂风暴雨之势席卷着整个世界,它不仅出现在企业服务器和专业怪才们的讨论组中,也开始在家用 PC 上生根了。Red Hat 公司在开源软件界是鼎鼎大名的,该公司发布了最早的 Linux 商业版本 Red Hat Linux。Red Hat 公司在发布 Red Hat Linux 系列版本的同时,还发布了 Red Hat Enterprise Linux,即 Red Hat Linux 企业版,简称为 RHEL。RHEL 系列版本面向企业级客户,主要应用在 Linux 服务器领域。

RHEL 5.0 诞生于 2007 年,是目前应用最为广泛的企业级 Linux 之一,经过 4 年等待,到了 2010 年时 RHEL 6.0 出现了。RHEL 6.0 桌面环境/存储和虚拟化方面较 RHEL 5.0 有了不小的变化。例如虚拟化方面,使用 KVM 替代了 Xen,全面增强了 RHEL 的虚拟化功能;存储方面增强了 iSCSI 和 FC 的支持;在节能方面比前期的版本有大幅度的提升,可谓绿色 Linux,可以说是一个目前最强大的企业级 Linux 发行版之一。

本书特点

本书所讲述的 RHEL 6.0 内容覆盖范围广,适用人群广。在写作思路强调在“授人以渔”的前提下“授人以鱼”,对每个知识点的介绍争取做到深入浅出,从系统、科学的原理和机制介绍出发,并通过丰富多样的图表配以具体的步骤实现和详细的讲解。以方便读者在实际 Linux 的管理和操作中进行对照学习,提高学习效率。涉及 RHEL 6.0 系统管理诸多方面的内容。书中绝大部分内容同时也适用于其他发行版本。本书使用了大量图表对内容进行表述和归纳,便于读者理解及查阅,具有很强的实用性、指导性。

内容安排

本书包括 19 章和 1 个附录，主要内容如下：

章 名	内 容 介 绍
第 1 章 Red Hat Enterprise Linux 6.0 系统简介	本章重点介绍对 Linux 的概述，着重介绍 Linux 和 RHEL 的发展历史、特性、主要应用领域等
第 2 章 Red Hat Enterprise Linux 6.0 系统安装和故障排除	本章重点介绍 RHEL 6.0 的安装方法，以及安装过程的故障排除
第 3 章 Linux 启动过程和系统引导器 GRUB	本章重点介绍 Linux 的启动过程和系统引导器 GRUB 的使用方法
第 4 章 Linux 守护进程、系统服务和 xinetd	本章重点介绍 Linux 守护进程的概念和结构，xinetd 及 Linux 服务管理工具，如何安全选择 Linux 服务
第 5 章 Linux 用户管理	本章重点介绍 Linux 用户和组管理的原理及相关的技巧
第 6 章 Linux 文件系统管理	本章重点介绍 Linux 层次式文件系统，包括文件、文件名、路径名、使用目录、访问权限和 Linux 文件系统管理方法
第 7 章 Linux 磁盘管理及 LVM 管理	本章重点介绍 Linux 硬盘与格式化及分区和 LVM 基本概念，学习 Linux 磁盘管理和分区及 LVM 相关命令和图形化工具
第 8 章 Linux TCP/IP 网络配置管理	本章重点介绍 Linux 网络体系：TCP/IP 网络模型、OSI 七层模型。熟悉 Linux 网络配置文件和 Linux 网络管理命令及使用 NetworkManager 配置网络连接和 Linux 命令行网络监控工具
第 9 章 Linux 软件包管理	本章重点介绍 rpm 和 yum 软件包管理方法及使用图形化工具安装软件包
第 10 章 Linux 性能和系统监控	本章重点介绍主 Linux 服务器监测概念与常用工具、网络服务性能监测、常见性能优化方法、网络服务监测和优化示例
第 11 章 Linux 日志管理	本章重点介绍 Linux 日志管理的基本原理、基本命令和日志管理技巧
第 12 章 Linux 打印系统管理配置	本章首先介绍 Linux 打印系统发展路线图和 RHEL 图形化打印管理器，然后学习配置 CUPS 打印系统，最后学习 Linux 打印管理命令的使用方法
第 13 章 使用 Webmin 管理 Linux	本章重点介绍为 RHEL 6.0 配置 Webmin 管理工具的方法，这对于 Linux 和其他 UNIX 用户非常实用
第 14 章 Linux iSCSI 和 AoE 存储配置	本章重点介绍 Linux 下 iSCSI 和 AoE 的工作原理及存储配置方法
第 15 章 Linux 备份与恢复	本章首先介绍 Linux 备份恢复基础及 Linux 备份恢复策略，然后介绍 Linux 常用备份恢复工具，以及 Linux 备份恢复实例和 rsync 的使用方法
第 16 章 Linux 防火墙设置	本章重点介绍 Linux 系统的防火墙，使用命令行和图形化界面管理防火墙的方法
第 17 章 使用 SELinux	本章重点介绍使用 RHEL 6.0 的 SELinux 机制对系统进行安全增强的技术
第 18 章 Linux 安全审计系统	本章重点介绍 Linux 内核中的安全审计系统配置和使用方法
第 19 章 Linux 虚拟化应用	本章重点介绍 Linux 服务器的虚拟化技术，包括 VirtualBox 和 KVM
附录 A RHEL 6.0 桌面管理	本章使用较少篇幅，简单介绍 Red Hat Enterprise Linux 6.0 桌面管理

适用对象

本书适用对象为以下几类人群：

- 高等院校相关专业的学生。
- 高、中等职业技术院校相关专业的学生。
- Linux 系统管理员。

感谢

首先感谢在编写过程中领导、朋友和家人的支持及帮助。另外，电子工业出版社的李冰编辑在写书的过程中给予了笔者无私的帮助和鞭策，为了使本书能尽快与读者见面，她也付出了巨大的努力。本书第1章由林捷执笔，第2章由张志军、何清、王鹏执笔，第3章由王波、何勤童、吴少萍执笔，第4~19章由曹江华执笔，附录由杨晓勇执笔，全书由曹江华进行统稿。另外曹元其同志帮助完成了资料收集和文字校对。由于作者水平有限，书中不足及错误之处在所难免，敬请专家和读者给予批评指正。

曹江华

2011年5月

目 录

CONTENTS

第 1 章 Red Hat Enterprise Linux 6.0

系统简介 1

1.1 Linux 简介 1

1.1.1 UNIX 操作系统的诞生 1

1.1.2 GNU 早期简史 2

1.1.3 POSIX 标准历史 3

1.1.4 Linux 概述 3

1.1.5 Linux 和开源软件的 商业化 4

1.1.6 Linux 和开源软件的 商业模式 5

1.2 Linux 内核及其发行版本 6

1.2.1 Linux 发行版本概述 6

1.2.2 Linux 内核的变迁 7

1.2.3 Linux 主要发行版本 8

1.3 Red Hat Enterprise Linux 简介 10

1.3.1 发展轨迹 10

1.3.2 Red Hat Enterprise Linux 6.0 简介 12

第 2 章 Red Hat Enterprise Linux 6.0

系统安装和故障排除 18

2.1 硬件需求与兼容性 18

2.1.1 Linux 硬件驱动现状 18

2.1.2 主要硬件的兼容性 19

2.1.3 收集硬件信息 20

2.1.4 检查系统硬件是否存在大的 缺陷 22

2.1.5 获取 Red Hat Enterprise Linux

6.0 兼容性列表 22

2.2 安装 Red Hat Enterprise

Linux 6.0 23

2.2.1 使用本地光盘介质安装 Red Hat Enterprise Linux 6.0 23

2.2.2 首次启动 Red Hat Enterprise Linux 6.0 的配置 37

2.3 安装的常见故障及其排除 42

2.3.1 开始安装阶段的故障 及其排除 42

2.3.2 初始安装阶段的故障 及其排除 43

2.3.3 安装过程中的问题 43

2.3.4 安装后的问题 44

2.4 Linux 硬件的稳定性检测 46

2.4.1 稳定性检测的作用 46

2.4.2 检测 CPU 46

2.4.3 检测内存 49

2.4.4 使用整体测试工具 PassMark 50

2.5 卸载 Red Hat Enterprise

Linux 6.0 52

第 3 章 Linux 启动过程和系统引导器

GRUB 54

3.1 Linux 启动过程 54

3.1.1 Linux 的启动过程详解 54

3.1.2 Linux 运行级 57

3.1.3	/etc/inittab 文件和 /etc/sysconfig/init 文件	58
3.2	系统引导器 GRUB	62
3.2.1	GRUB 简介	62
3.2.2	GRUB 的启动菜单界面	63
3.2.3	GRUB 的启动菜单项 编辑界面	63
3.2.4	GRUB 命令行界面	64
3.2.5	理解 GRUB 配置文件 grub.conf	65
3.2.6	GRUB 初始引导过程	67
3.2.7	GRUB 命令参考	68
3.2.8	了解 GRUB 常见 错误信息	70
第 4 章	Linux 守护进程、系统服务和 xinetd	75
4.1	守护进程	75
4.1.1	Linux 守护进程的概念	75
4.1.2	Linux 系统提供的服务及其 守护进程列表	75
4.1.3	查看守护进程的方法	79
4.2	xinetd	81
4.2.1	什么是 xinetd	81
4.2.2	xinetd 的特色	81
4.2.3	使用 xinetd 启动守护进程	82
4.2.4	解读/etc/xinetd.conf 和 /etc/xinetd.d/*	83
4.2.5	配置 xinetd	85
4.2.6	xinetd 防止拒绝服务攻击 (Denial of Services) 的 原因	91
4.3	Linux 服务管理工具	92
4.3.1	system-config-services	92
4.3.2	ntsysv	93
4.3.3	chkconfig	93
4.4	TCP Wrappers	94

4.5	安全选择 Linux 服务	96
第 5 章	Linux 用户管理	97
5.1	Linux 用户管理简介	97
5.1.1	Linux 多用户、任务系统	97
5.1.2	Linux 用户 (User) 和 用户组 (Group) 概念	98
5.1.3	理解 Linux 用户配置文件	99
5.1.4	理解 Linux 用户组 配置文件	101
5.1.5	Linux 用户相关配置文件 ...	103
5.1.6	定制 Linux 系统 环境变量	105
5.2	使用命令行工具管理用户和 用户组	107
5.2.1	useradd: 建立用户	107
5.2.2	userdel: 删除用户	109
5.2.3	usermod: 修改已有 用户信息	109
5.2.4	passwd: 设置密码	110
5.2.5	chage: 密码老化	111
5.2.6	groupadd: 添加组	111
5.2.7	groupdel: 删除组账户	112
5.2.8	groupmod: 修改组	112
5.2.9	vipw: 编辑/etc/passwd 文件	113
5.2.10	vigr: 编辑/etc/group 文件	113
5.2.11	newgrp: 转换组	113
5.2.12	whoami: 显示当前 用户名称	114
5.2.13	who: 显示登录用户	114
5.2.14	id: 显示用户信息	115
5.2.15	su: 切换身份	115
5.2.16	pwck: 检测账户	116
5.2.17	grpck: 检测用户组账号 信息完整性	116

5.3	使用图形化工具：用户和组配置工具	117	7.2	主要 Linux 磁盘管理命令	150
5.3.1	添加新用户	118	7.2.1	fdisk：磁盘分区	150
5.3.2	修改用户属性	118	7.2.2	hdparm：设置磁盘参数	152
5.3.3	添加新组	119	7.2.3	badblock：检查磁盘	153
5.3.4	修改组属性	119	7.2.4	parted：磁盘分区工具	154
5.4	Linux 用户管理实例	119	7.3	Linux 磁盘操作实战	155
5.4.1	Linux 用户管理小技巧	119	7.3.1	为 Linux 添加新硬盘	155
5.4.2	配置 sudo 让 Linux 用户管理更加安全	123	7.3.2	Linux 服务器磁盘配额配置	157
第 6 章	Linux 文件系统管理	129	7.3.3	优化 Linux 系统硬盘	163
6.1	Linux 的文件系统介绍	129	7.4	RAID 配置	165
6.1.1	文件系统定义	129	7.5	LVM 管理	169
6.1.2	Linux 文件系统的体系结构	129	7.5.1	LVM 基础	169
6.1.3	Linux 文件系统结构	130	7.5.2	命令行 LVM 配置实战	172
6.1.4	/proc 文件系统	132	7.5.3	使用 system-config-lvm 管理 LVM	182
6.1.5	Linux 文件系统的组成	133	7.6	使用磁盘使用分析器	186
6.1.6	文件类型	133	7.6.1	磁盘使用分析器简介	186
6.1.7	文件系统的特性	135	7.6.2	磁盘使用分析器快速入门	187
6.1.8	Linux 主流文件格式	135	第 8 章	Linux TCP/IP 网络配置管理	190
6.1.9	查看当前 Linux 支持的文件类型	140	8.1	Linux 网络基础	190
6.2	ext2/ext3 文件系统管理	140	8.1.1	Linux 网络结构的特点	190
6.2.1	创建 ext2/ext3/ext4 文件系统	141	8.1.2	Linux 下端口号分配	192
6.2.2	检查 ext2/ext3/ext4 文件系统	143	8.1.3	Linux 的 TCP/IP 网络配置	194
6.2.3	调整 ext2/ext3/ext4 文件系统的属性	144	8.2	通过 Linux 命令行进行网络操作	195
6.2.4	管理 ext2/ext3/ext4 文件系统的卷标	146	8.2.1	Linux 的 TCP/IP 配置	195
第 7 章	Linux 磁盘管理及 LVM 管理	147	8.2.2	Linux 服务器的静态路由配置	201
7.1	Linux 磁盘简介	147	8.2.3	ADSL 连接配置和故障排除	206
			8.3	使用 NetworkManager 配置网络连接	215
			8.3.1	NetworkManager 简介	215

8.3.2	使用 NetworkManager 配置 有线网络接口	215	10.1.6	监测 Linux 进程运行	253
8.3.3	使用 NetworkManager 连接 Wi-Fi (802.11) 网络	217	10.1.7	监测内存使用情况	254
8.4	掌握 Linux 命令行网络 监控工具	218	10.1.8	监测中央处理器	255
8.4.1	使用 iftop 工具监控网卡的 流量	218	10.1.9	使用 iostat 监测 I/O 性能	257
8.4.2	使用 ngrep 监控 网络接口	219	10.1.10	监测网络性能	258
8.4.3	利用 Bwm-NG 监测带宽	221	10.1.11	sar	261
8.4.4	lsof	222	10.1.12	使用 Ksar	266
8.4.5	使用 IPTraf 监控 Linux 网络	225	10.2	Linux 核心硬件状态监控	272
8.4.6	使用 Tcpdump	227	10.2.1	使用命令行工具检测主板、 CPU	272
第 9 章	Linux 软件包管理	232	10.2.2	使用 lshw 工具	275
9.1	RPM 软件包管理	232	10.2.3	使用 smartmontools 检测 硬盘健康	276
9.1.1	RPM 简介	232	10.3	在 Linux 中监控 硬件温度	278
9.1.2	RPM 的功能	232	10.3.1	命令行下的工作方式	278
9.1.3	RPM 软件包格式	233	10.3.2	图像界面下的工作方式	280
9.1.4	rpm 命令格式	233	第 11 章	Linux 日志管理	283
9.1.5	rpm 命令实例	237	11.1	日志管理简介	283
9.2	YUM 软件包管理	240	11.2	Linux 日志简介	284
9.2.1	YUM 简介	240	11.3	日志管理软件包 psacct	285
9.2.2	YUM 命令	241	11.3.1	psacct 简介	285
9.3	使用图形化工具 安装软件包	246	11.3.2	lastcomm 命令	286
第 10 章	Linux 性能和系统监控	249	11.3.3	sa 命令	287
10.1	服务器性能监控的方法和 步骤	249	11.3.4	ac 命令	289
10.1.1	性能监控方法	249	11.3.5	accton 命令	290
10.1.2	proc 文件系统的特点	250	11.4	其他日志管理实用工具	291
10.1.3	proc 文件系统的功能	250	11.5	Linux 日志管理技巧	293
10.1.4	监测系统负载	250	11.5.1	使用 logrotate 工具	293
10.1.5	使用 phpsysinfo	252	11.5.2	搜索日志文件的策略和 技巧	294
			11.5.3	手动搜索日志文件	295
			11.5.4	使用 logwatch 工具搜索 日志文件	296

11.5.5 其他日志工具	296	12.4.11 lpd: 行打印守护进程	323
11.6 使用图形化工具: 系统日志查看器	296	12.4.12 Linux 打印故障诊断	323
11.6.1 安装	296	第 13 章 使用 Webmin 管理 Linux ..	325
11.6.2 快速使用入门	297	13.1 Webmin 安装配置	325
第 12 章 Linux 打印系统管理配置....	300	13.1.1 Webmin 简介	325
12.1 Linux 打印系统发展路线图	300	13.1.2 下载安装 Webmin	326
12.1.1 PostScript 语言	300	13.2 使用 Webmin	326
12.1.2 BSD LPD 打印系统	302	13.2.1 登录 Webmin	326
12.1.3 LPRng 打印系统	304	13.2.2 Webmin 的自身配置	327
12.1.4 通用 UNIX 打印系统 (CUPS)	304	13.2.3 Webmin 主界面	328
12.1.5 Linux 打印过程	306	13.2.4 理解 Webmin 配置文件	330
12.2 使用 Red Hat Linux 打印配置管理工具	306	13.2.5 Webmin 的安全性	332
12.2.1 下载安装驱动	306	第 14 章 Linux iSCSI 和 AoE 存储配置	333
12.2.2 使用 system-config-printer	307	14.1 企业级存储简介	333
12.3 配置 CUPS 打印系统	311	14.1.1 DAS、NAS、SAN 三种模式	333
12.4 打印机常用命令	313	14.1.2 SAN 的两种模式	335
12.4.1 cupsd: 通用打印程序守护进程	313	14.1.3 iSCSI 技术简介	337
12.4.2 lpadmin: 配置 LP 打印服务	314	14.2 Linux iSCSI 配置	340
12.4.3 lp: 打印文件	316	14.2.1 Linux 安装启动 iSCSI Target	340
12.4.4 lpstat: 显示行式打印机状态信息	317	14.2.2 Linux 安装设置 iSCSI Initiator	341
12.4.5 lpr: 排队打印作业	318	14.2.3 Windows 客户端的使用 iSCSI 磁盘设备	343
12.4.6 lprm: 打印队列删除任务	318	14.3 AoE 存储设置	344
12.4.7 lpc: 控制打印机	319	14.3.1 AoE 简介	344
12.4.8 lpq: 检查假脱机队列	320	14.3.2 Linux 配置 AoE 模块	346
12.4.9 lpinfo: 显示驱动和设备	321	第 15 章 Linux 备份与恢复	351
12.4.10 lpmove: 将作业从一个队列移动到另外一个队列中	322	15.1 Linux 备份基础	351
		15.2 Linux 备份恢复策略	352
		15.2.1 备份前需考虑的因素	352
		15.2.2 选择备份介质	352
		15.2.3 Linux 备份策略	353

15.2.4	确定要备份的内容	355	16.4.2	使用 Fwbuilder 快速构架 Linux 防火墙	403
15.2.5	Linux 磁带机备份和 恢复	356	16.5	为 Linux 防火墙添加 7 层 过滤功能	407
15.3	常用备份工具的使用	362	16.5.1	L7-filter 简介	407
15.3.1	用 mirrordir 做硬盘 分区镜像	362	16.5.2	配置 L7-filter 模块	408
15.3.2	使用 partimage 备份恢复 Linux 分区	364	16.6	构建 Linux 下的 NAT 服务器	410
15.3.3	使用 afio 工具备份	365	16.5.1	NAT 基础	410
15.3.4	Linux 备份恢复工具	366	16.6.2	NAT 的优点和不足	418
15.4	使用 rsync	367	第 17 章	使用 SELinux	420
15.4.1	rsync 简介	367	17.1	SELinux 简介	420
15.4.2	rsync 两种部署架构	368	17.1.1	SELinux 起源	420
15.4.3	rsync 命令格式	369	17.1.2	SELinux 构架	421
15.4.4	rsync 使用实例	371	17.1.3	为什么使用 SELinux	425
15.4.5	配置 rsync 服务	373	17.1.4	SELinux 决策进程	426
15.4.6	rsync 服务器应用实例	377	17.1.5	SELinux 相关的文件	427
15.4.7	图形化工具 LuckyBackup	379	17.2	SELinux 使用实战	427
第 16 章	Linux 防火墙设置	381	17.2.1	SELinux 布尔值和 上下文配置	430
16.1	防火墙简介	381	17.3	SELinux 管理命令	434
16.1.1	什么是防火墙	381	17.3.1	setenforce: 设置 SELinux 模式	434
16.1.2	防火墙的功能	381	17.3.2	getenforce: 查看 SELinux 模式	434
16.1.3	防火墙技术分类	382	17.3.3	setsebool: 设置 SELinux 布尔值	434
16.2	Linux 防火墙	384	17.3.4	getsebool: 查看 SELinux 布尔值	435
16.2.1	Linux 防火墙的历史	384	17.3.5	sestatus: SELinux 状态 查看工具	435
16.2.2	Netfilter/iptables 系统 如何工作	385	17.3.6	avcstat: 显示 AVC 统计信息	437
16.2.3	iptables 基础	386	17.3.7	audit2why: 转换 审计消息	437
16.2.4	建立规则和链	392			
16.3	iptables 配置实战	397			
16.4	使用 system-config-firewall 和 Fwbuilder 快速构架 Linux 防火墙	399			
16.4.1	使用 system-config-firewall 快速构架 Linux 防火墙	399			

17.3.8	audit2allow: 生成策略 允许规则	437	18.1.2	了解 audit 配置文件	453
17.3.9	load_policy: 装载策略	439	18.2	启动 auditd 守护进程	460
17.3.10	semanage: 管理 SELinux 策略	439	18.3	分析 auditd 记录	461
17.3.11	semodule: 管理 策略模块	441	18.4	使用 ausearch 命令 搜索记录	463
17.3.12	chcat: 改变语境类别	442	18.5	使用 autrace 审计 跟踪进程	464
17.3.13	restorecon: 恢复文件 安全语境	442	18.6	使用 SELinux 故障诊断工具查看 Linux 安全审计信息	465
17.3.14	chcon: 改变文件 安全语境	443	第 19 章	Linux 虚拟化应用	466
17.3.15	setfiles: 设置文件 安全语境	444	19.1	虚拟化历史	466
17.3.16	seinfo: 提取策略的 规则数量统计信息	445	19.1.1	硬件虚拟化	466
17.3.17	sesearch: 搜索 policy.conf 或二进制策略中特别的 类型	446	19.1.2	处理器虚拟化	466
17.3.18	checkmodule: 编译 策略模块	446	19.1.3	指令集虚拟化	467
17.3.19	sealert: SELinux 信息 诊断客户端工具	447	19.1.4	主流虚拟化硬件 厂商技术	467
17.3.20	selinuxenabled: 查询系统的 SELinux 是否有启用	448	19.1.5	存储虚拟化	469
17.4	SELinux 日志文件的 使用	448	19.1.6	网络虚拟化	469
17.4.1	SELinux 日志文件简介	448	19.2	Linux 虚拟化简介	470
17.4.2	修改 SELinux 上下文解决 SELinux 造成的网络服务 故障实例	448	19.2.1	Linux 虚拟化类型	470
17.5	SELinux 常见问题总结	451	19.2.2	Linux 虚拟化项目	472
第 18 章	Linux 安全审计系统	453	19.2.3	Linux 服务器虚拟化的 重要性	472
18.1	安装软件包并且配置审计 守护进程	453	19.3	VirtualBox 虚拟化技术	473
18.1.1	安装软件包	453	19.3.1	VirtualBox 简介	473
			19.3.2	Linux 下安装、卸载 VirtualBox	475
			19.3.3	启动 VirtualBox	475
			19.3.4	建立一个虚拟机	476
			19.3.5	虚拟机配置	477
			19.3.6	使用 VirtualBox 在 Linux 下 安装运行 Windows XP SP3 的 技巧	479
			19.3.7	增强功能工具其他功能	482
			19.4	KVM 虚拟机配置	483

19.4.1	KVM 虚拟机简介	483	19.4.4	RHEL 6 KVM 虚拟机 新功能	488
19.4.2	安装配置 KVM 相关软件	485	19.4.5	使用命令行执行高级 管理任务	493
19.4.3	使用 virt-manager 建立一个 KVM 虚拟机	485	附录 A	RHEL 6.0 桌面管理	498

01

Red Hat Enterprise Linux 6.0 系统管理

Red Hat Enterprise Linux 6.0 系统简介

1.1 Linux 简介

Linux 操作系统是 UNIX 操作系统的一种克隆系统，它诞生于 1991 年的 10 月 5 日（这是第 1 次正式向外公布的时间）。以后借助于 Internet，并经过全世界各地计算机爱好者的共同努力，它已成为今天世界上使用最多的一种 UNIX 类操作系统，并且使用人数还在迅猛增长之中。Linux 操作系统的诞生、发展和成长过程始终依赖着几个重要支柱，即 UNIX 操作系统、Minix 操作系统、GNU 计划和 POSIX 标准。

1.1.1 UNIX 操作系统的诞生

UNIX 是一个多用户、多任务的操作系统，最初由 AT&T 贝尔实验室的 Ken Thompson 于 1969 年开发成功。UNIX 当初设计的目标是允许大量程序员同时访问计算机，共享其资源。它非常简单，但是功能强大、通用，并且可移植，可以运行在从微机到超级小型计算机，以及大型机上。

UNIX 系统的核心是内核，即一个系统引导时加载的程序。内核用于与硬件设备打交道，调度任务，并且管理内存和辅存。正是由于 UNIX 系统这种精练特性，所以众多小而简单的工具和实用程序被开发出来。因为这些工具（命令）能够很容易地组合起来执行多种大型的任务，所以 UNIX 迅速流行起来。其中最重要的工具之一就是 shell，即一个让用户能够与操作系统沟通的程序，本书将剖析当今主流 shell 的特性。最初 UNIX 被科学研究机构和大学采用，其费用微不足道，后来慢慢扩展到计算机公司、政府机构和制造业领域。1973 年，美国国防部高级研究计划署（Defense Advanced Research Projects Agency, DARPA）启动一项计划，研究使用 UNIX 将跨越多个网络的计算机透明地连接在一起的方式。这个计划和从该研究中形成的网络系统，导致了 Internet 的诞生。

在 20 世纪 70 年代后期，许多在大学期间接触并体验过 UNIX 的学生投身工业界并要求工业界向 UNIX 转换，声称它是最适合复杂编程环境的操作系统。很快大量或大或小的厂家开始

开发自己的 UNIX 版本，在自己的计算机体系结构上对其进行优化，以期占领市场。最著名的两个 UNIX 版本是 AT&T 的 System V 和 BSD UNIX，后者源于 AT&T 版本，由加州大学伯克利分校于 20 世纪 80 年代早期开发成功。

面对如此众多版本的 UNIX（有一个图表列出了 80 多个 UNIX 版本，访问 <http://www.ugu.com/sui/ugu/show?ugu.flavors>），如果不花费时间和精力考虑兼容问题，则在一个系统上能够正常运行的应用程序和工具可能无法在另一个系统上工作。由于缺乏统一的标准，许多厂家放弃了 UNIX 转而使用比较古老的非 UNIX 专用系统，如 VMS，它们被证明是更加一致和可靠的。在 1993 年初，AT&T 将其 UNIX 系统实验室出售给了 Novell。1995 年，Novell 将其 UNIX 商标权和规范（后来变成了单一 UNIX 规范）转让给 The Open Group，将 UNIX 系统源代码卖给了 SCO。当今有很多公司都在出售基于 UNIX 的系统，包括 Sun Microsystems 的 Solaris、HP-UX 和来自 Hewlett-Packard 的 Tru64 UNIX，以及来自 IBM 的 AIX。除此之外，还有许多免费的 UNIX 和与 UNIX 兼容的工具，如 Linux、FreeBSD 和 NetBSD。Linux 操作系统是 UNIX 操作系统的一个克隆版本，现在几乎每个主要的计算机厂商都有其自有版本的 UNIX。

1.1.2 GNU 早期简史

1971 年，作为开放源码的先驱，Richard Stallman 加入了麻省理工学院的一个专门研究免费软件的组织。作为 Emacs 文本编辑程序的开发者，他后来建立了 GNU 项目，从而最终导致了免费的 Linux 操作系统的诞生。

1983 年，为了反对软件所有权私有化的趋势，Stallman 建立了 GNU 计划来推进免费软件模型，并为此开发了一个免费的操作系统、应用程序，以及开发工具。更重要的是，GNU 计划建立了 General Public License (GPL)，即 Copyleft，它成为许多开放源码软件所采用的模型。

1985 年 3 月，Richard Stallman 在 Dr.Dobb's 杂志上发表了《GNU 宣言》，在宣言中他陈述了自由软件运动的起因。

1986 年，Larry Wall 建立了 Perl (Practical Extraction and Report Language)，这是一种编写 CGI 程序广泛采用的通用编程语言，CGI 为 Web 带来了更多动态内容。

1987 年，开发者 Andrew Tanenbaum 发布了 Minix，在发布时带有完整的源代码。

1989 年 1 月，GPL 版本 1 由斯道曼撰写，用于 GNU 计划，它以 GNU Emacs、GDB 和 GCC 的许可证的早期版本为蓝本。这些许可证都包含有一些 GPL 的版权思想，但仅只针对特定程序。斯道曼的目标就是创造出一种四海之内皆可使用的许可证，这样就能为许多源代码共享计划带来福音。

到 1990 年时，因为一些共享库而出现了对比 GPL 更宽松的许可证的需求。所以当 GPL 版本 2 在 1991 年 6 月发布时，另一许可证——库通用许可证 (Library General Public License, LGPL) 也随之发布，并记为“版本 2”以示对 GPL 的补充。版本号在 LGPL 版本 2.1 发布时不再相同，而 LGPL 也被重命名为“GNU 宽通用公共许可证 (Lesser General Public License)”以体现 GNU 哲学观。

1991 年 8 月 25 日，Linus 在 Usenet 新闻组上公开了关于 Linux 的构想。为了超越 Minix，发布了一个新的 UNIX 变种——Linux。3 年后，Linux 正式接受 GPL。

1.1.3 POSIX 标准历史

POSIX (Portable Operating System Interface of UNIX) 是由 IEEE 和 ISO/IEC 开发的一组标准。该标准是基于现有的 UNIX 实践和经验, 描述了操作系统的调用服务接口, 用于保证编制的应用程序可以在源代码一级上在多种操作系统上移植运行。它是在 1980 年早期一个 UNIX 用户组 (Usr/Group) 的工作的基础上取得的。该 UNIX 用户组原来试图将 AT&T 的系统 V 和 Berkeley CSRG 的 BSD 系统的调用接口之间的区别重新调和集成, 从而于 1984 年产生了 /usr/group 标准。1985 年, IEEE 操作系统技术委员会标准小组委员会 (TCOS-SS) 开始在 ANSI 的支持下责成 IEEE 标准委员会制定有关程序源代码可移植性操作系统服务接口正式标准。到了 1986 年 4 月, IEEE 就制定出了试用标准。第 1 个正式标准是在 1988 年 9 月份批准的 (IEEE 1003.1-1988), 即以后经常提到的 POSIX.1 标准。1989 年 POSIX 的工作被转移至 ISO/IEC 社团, 并由 15 工作组继续将其制定成 ISO 标准。到 1990 年, POSIX.1 与已经通过的 C 语言标准联合, 正式批准为 IEEE 1003.1-1990 (也是 ANSI 标准) 和 ISO/IEC 9945-1:1990 标准。

在 20 世纪 90 年代初, POSIX 标准的制定正处在最后投票敲定时, 此时 Linux 刚刚起步。这个 UNIX 标准为 Linux 提供了极为重要的信息, 使得 Linux 能够在标准的指导下进行开发, 并与绝大多数 UNIX 系统兼容。在最初的 Linux 内核代码中 (0.01 版及 0.11 版) 就已经为 Linux 与 POSIX 标准的兼容做好了准备工作。

1.1.4 Linux 概述

通过上述说明, 我们可以对上述 Linux 的几个支柱归纳如下。

(1) UNIX 操作系统: 1969 年诞生在 Bell 实验室, Linux 是其一一种克隆系统。

(2) Minix 操作系统: 也是 UNIX 的一种克隆系统, 1987 年由著名计算机教授 Andrew S. Tanenbaum 开发完成。由于 Minix 系统的出现并且提供源代码 (只能免费用于大学内), 所以在全世界的大学中刮起了学习 UNIX 系统旋风, Linux 开始就是参照 Minix 系统于 1991 年开始开发。

(3) GNU 计划: 开发 Linux 操作系统, 以及 Linux 上所用大多数软件基本上都出自 GNU 计划, Linux 只是操作系统的一个内核。没有 GNU 软件环境 (比如说 bash shell), 则 Linux 将寸步难行。

(4) POSIX 标准: 在推动 Linux 操作系统以后朝着正规路上发展起着重要的作用, 是 Linux 前进的灯塔。

Linux 是由 Linus Benedict Torvalds 等众多软件高手共同开发的, 是一种能运行于多种平台 (如 PC 及其兼容机、Alpha 工作站及 SUN Sparc 工作站)、源代码公开、免费、功能强大、遵守 POSIX 标准, 并且与 UNIX 兼容的操作系统。

Linux 运行的硬件平台起初是 Intel 386、486、Pentium 及 Pentium Pro 等, 现在还包括 Alpha、PowerPC 和 Sparc 等。Linux 不但支持 32 位, 还支持 64 位, 如 Alpha。它既支持单 CPU, 也支持多 CPU。

Linux 内核和许多系统软件, 以及应用软件的源代码是公开的, 也是免费的。Linux 系统软