

本书特色

- 本书在写作思路强调在“授人以渔”的前提下“授人以鱼”。
- 对每个知识点的介绍深入浅出，采用丰富多样的图表并配以具体的步骤实现方式进行详细讲解。
- 书中涉及RHEL 6.0服务器管理诸多方面的内容，绝大部分内容同时也适用于其他发行版本。本书具有很强的实用性、指导性。

Red Hat Enterprise **Linux 6.0** 服务器构建

曹江华 林捷 编著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

Red Hat Enterprise
Linux 6.0

服务器构建

曹江华 林捷 编著

電子工業出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

本书以 RHEL 6.0 和 CentOS 6.0 为蓝本, 以 24 章和 3 个附录的篇幅介绍了 Linux 操作系统在服务器上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、NTP 服务器、DNS 服务器、NFS 服务器、SSH 服务器、MySQL 服务器、Apache 服务器、NIS 服务器、Samba 服务器、DHCP 服务器、FTP 服务器、Linux 系统备份与恢复、Linux 虚拟化应用、PAM、Postfix 电子邮件服务器、Linux iSCSI 和 AoE 存储配置、SELinux 的使用、Squid 代理服务器、防火墙设置和升级、Linux 性能和系统监控、Linux 服务器应急响应流程与步骤、Linux 计算机系统取证、Linux 反删除工具的使用等内容。本书内容详尽、结构清晰、通俗易懂, 使用了大量的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。

本书内容适用于 RHEL 6.0 和 CentOS 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, 也可以供广大 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 服务器构建 / 曹江华, 林捷编著. —北京: 电子工业出版社, 2012.4
ISBN 978-7-121-16182-7

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

中国版本图书馆 CIP 数据核字 (2012) 第 039566 号

策划编辑: 李 冰

责任编辑: 葛 娜

印 刷: 北京天宇星印刷厂

装 订: 三河市皇庄路通装订厂

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: 850×1168 1/16 印张: 34.25 字数: 1055 千字

印 次: 2012 年 4 月第 1 次印刷

印 数: 3500 册 定价: 69.00 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。

前言

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、军事战略以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凸显其不凡之处。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(之一)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 2010 年 RHEL 6.0 出现了。RHEL 6.0 桌面环境/存储和虚拟化方面比 RHEL 5.0 有了不小的变化。例如虚拟化方面,则使用 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了大幅度的提升,可谓绿色 Linux,可以说是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。书中涉及 RHEL 6.0 服务器管理诸多方面的内容,绝大部分内容同时也适用于其他发行版本。书中使用了大量的图表对内容进行表述和归纳,便于读者理解及查阅。本书具有很强的实用性、指导性,脉络清晰,深入浅出。

内容安排

本书分为 24 章 3 个附录,主要内容如下:

章 名	内 容 介 绍
第 1 章 Linux 简介	介绍 Linux 概述,着重介绍 Linux 和 RHEL 的发展历史、特性、主要应用领域
第 2 章 安装 RHEL 6.0 和初始化设置	重点介绍 RHEL 6.0 的安装方法,以及安装后的配置
第 3 章 配置 Linux NTP 服务器	重点介绍 NTP 服务器的工作原理和安装 NTP 服务器的方法
第 4 章 Linux DHCP 服务器安装及配置	重点介绍 DHCP 的工作原理与 3 种 IP 地址分配方式、DHCP 服务器的安装与启动、配置 Windows 和 Linux 的 DHCP 服务、Windows 和 Linux 的 DHCP 客户端配置、DHCP 应用与常见问题的解决方法
第 5 章 Linux DNS 服务器安装及配置	重点介绍 DNS 协议、DNS 服务器的安装和配置、DNS 服务常见故障排除方法
第 6 章 Linux NIS 服务器安装及配置	重点介绍 NIS 协议、NIS 服务器的安装和配置

续表

第 7 章 Linux NFS 服务器安装及配置	重点介绍如何安装配置 NFS 服务，如何使用 NFS 客户端，以及 NFS 服务的安全问题，NFS 服务器常见故障排除
第 8 章 Linux SSH 服务器安装及配置	重点介绍 SSH 服务器的工作原理和如何安装 SSH 服务器，以及 SSH 服务器常见故障排除
第 9 章 Linux Samba 服务器安装及配置	重点介绍配置 Samba 打印共享、测试 Samba 共享打印机配置的正确性、配置 Windows 客户机访问 Samba 共享打印机、图形化配置 Samba 服务器、Samba 相关命令及程序
第 10 章 Linux Squid 代理服务器安装及配置	重点介绍代理服务器的工作原理，以及如何安装 Squid 代理服务器
第 11 章 Linux MySQL 数据库安装及配置	重点介绍 MySQL 数据库简介，以及 MySQL 数据库在 Linux 中的安装和配置
第 12 章 Linux 目录服务	重点介绍 Linux 目录服务器，以及安装和配置 OpenLDAP 服务器及 OpenLDAP 客户端
第 13 章 Linux Apache 服务器安装及配置	重点介绍 Web 应用的起源与发展、WWW 的基本概念、Apache 软件的安装和配置、Web 系统管理员的日常事务，以及 Apache 服务器常见故障排除
第 14 章 Linux 电子邮件服务器 Postfix 安装及配置	重点介绍 E-mail 工作原理、相关协议、如何搭建电子邮件服务器、Postfix 电子邮件服务器的日常管理工作
第 15 章 Linux FTP 服务器安装及配置	重点介绍 FTP 通信协议、Vsftpd 服务器的安装、FTP 服务的配置、访问 FTP 服务、Vsftpd 服务的高级配置
第 16 章 Linux 防火墙设置	重点介绍 Linux 系统的防火墙设置
第 17 章 使用 SELinux	重点介绍 SELinux 的历史和框架，以及 SELinux 的使用方法
第 18 章 PAM 的安装及配置	重点介绍 PAM 工作原理和理解 PAM 配置文件工作，并介绍建立 PAM 应用程序，使用不同的 PAM 模块来增强安全性，以及安全应用 PAM
第 19 章 Linux 网络环境下的 VPN 构建	重点介绍 PPTP VPN 的安装及配置，以及 OpenVPN 服务器和客户端的安装及配置
第 20 章 Linux iSCSI 和 AoE 存储配置	重点介绍 iSCSI 和 AoE 协议以及存储配置
第 21 章 Linux 备份与恢复	重点介绍 Linux 备份恢复基础以及 Linux 备份恢复策略，并介绍 Linux 常用备份恢复工具的使用和 Linux 备份恢复实例
第 22 章 Linux 服务器监控	重点介绍 Linux 服务器监控概念与常用工具、网络服务性能监控、常见性能优化方法、网络服务监控和优化示例
第 23 章 Linux 虚拟化	重点介绍 Linux 服务器的虚拟化技术
第 24 章 Linux 集群配置	重点介绍 Linux 下集群应用技巧和故障排除方法
附录 A Linux 服务器应急响应流程与步骤	重点介绍 Linux 服务器应急响应流程与步骤
附录 B Linux 计算机系统取证	重点介绍 Linux 计算机系统取证知识
附录 C Linux 下反删除和彻底删除工具的使用	重点介绍 Linux 下反删除和彻底删除工具的使用方法

本书书名是《Red Hat Enterprise Linux 6.0 服务器构建》，不过许多章节中也使用了 Red Hat Enterprise Linux 6.0 的克隆版本 CentOS 6.0。所以各个章节中关于发行版的说明部分都是使用 RHEL/CentOS 6.0 表述的，特此说明。

适用对象

- 高等院校相关专业的学生；
- 高、中等职业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、葛娜编辑在我写书的过程中给予了无私的帮助和鞭策，为了使本书能尽快与读者见面，她们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工作。

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
2012年4月

目 录

第 1 章 Linux 简介	1	2.1.1 RHEL 发展轨迹	10
1.1 UNIX 发展史	1	2.1.2 Red Hat Enterprise Linux 6.0 简介	11
1.2 Linux 发展史	1	2.1.3 CentOS 简介	16
1.3 常用的 Linux 发行版介绍	2	2.1.4 安装前准备工作	18
1.3.1 Red Hat	2	2.1.5 检查系统硬件是否存在大的缺陷	19
1.3.2 SUSE	2	2.2 安装 Red Hat Enterprise Linux 6.0	20
1.3.3 Debian	3	2.2.1 使用本地光盘介质安装 Red Hat	
1.3.4 Ubuntu	3	Enterprise Linux 6.0	20
1.3.5 其他的 Linux 系统	4	2.2.2 首次启动 Red Hat Enterprise Linux	
1.4 Linux 内核 (Kernel) 版本简介	4	6.0 的配置	32
1.4.1 进程调度	5	2.3 系统基本配置	36
1.4.2 内存管理	5	2.3.1 设置一个系统管理员账号	36
1.4.3 虚拟文件系统	5	2.3.2 yum 配置	37
1.4.4 网络接口	5	2.4 配置系统服务	38
1.4.5 进程通信	5	2.4.1 system-config-services	39
1.5 Linux 的应用领域及发展前景	5	2.4.2 ntsysv	40
1.5.1 Linux 的应用领域	5	2.4.3 chkconfig	40
1.5.2 Linux 的发展前景	6	第 3 章 配置 Linux NTP 服务器	41
1.6 Linux 的特点	6	3.1 NTP 概述	41
1.6.1 开放性	6	3.1.1 为何需要 NTP 服务器	41
1.6.2 多用户、多任务工作环境	7	3.1.2 网络时间服务的实现方式	41
1.6.3 友好的用户界面	7	3.1.3 NTP 及其选择	42
1.6.4 设备独立性	7	3.1.4 NTP 的网络体系结构和工作原理	42
1.6.5 丰富的网络功能	7	3.1.5 NTP 如何工作	43
1.6.6 丰富的应用程序和开发工具支持	8	3.1.6 NTP 的工作模式	43
1.6.7 良好的可移植性	8	3.1.7 选择 NTP 服务器	44
1.6.8 可靠的安全性	8	3.2 配置 Linux 网络时间服务器	44
1.7 GNU 通用公共许可证和 3 个		3.2.1 配置 Linux 异构网络下的 NTP	
版本简介	8	服务器	44
1.7.1 GPL v1	9	3.2.2 NTP 服务的配置文件	44
1.7.2 GPL v2	9	3.3 NTP 客户端应用	47
1.7.3 GPL v3	9	3.3.1 使用 Linux NTP 客户端	47
第 2 章 安装 RHEL 6.0 和初始化		3.3.2 在 Windows 2003/XP 系统中使用	
设置	10	NTP 校时	48
2.1 Red Hat Enterprise Linux 简介	10		

第 4 章 Linux DHCP 服务器安装及配置	50
4.1 DHCP 服务器的工作原理	50
4.1.1 DHCP 简介	50
4.1.2 为什么使用 DHCP	50
4.1.3 DHCP 的工作流程	50
4.1.4 DHCP 的设计目标	51
4.2 安装 DHCP 服务器	52
4.2.1 DHCP 配置文件	52
4.2.2 配置实例	53
4.2.3 启动 DHCP 服务器	54
4.2.4 配置 DHCP 客户端	55
第 5 章 Linux DNS 服务器安装及配置	58
5.1 DNS 简介	58
5.1.1 DNS 服务器的工作原理	58
5.1.2 域名服务的解析原理和过程	60
5.1.3 DNS 分类	61
5.1.4 架设 DNS 服务器的准备工作	61
5.1.5 DNS 常用术语	62
5.2 Linux DNS 服务器简介	62
5.2.1 DNS 配置文件组	62
5.2.2 BIND 9 目录结构	63
5.2.3 DNS 资源记录格式	64
5.3 DNS 服务器和客户端配置	65
5.3.1 安装服务器软件包	65
5.3.2 BIND 主配置文件 named.conf	66
5.3.3 内网区文件设置	68
5.3.4 外网区文件设置	68
5.3.5 内网反向查询文件设置	69
5.3.6 外网反向查询文件设置	69
5.3.7 防火墙和 SELinux 设置	69
5.3.8 重新启动 DNS 服务器	69
5.3.9 配置惟高速缓存域名服务器	70
5.3.10 DNS 客户端配置	70
5.4 DNS 故障排除工具	72
5.4.1 dlint	72
5.4.2 DNS 服务器的工作状态检查	73
第 6 章 Linux NIS 服务器安装及配置	78
6.1 NIS 简介	78
6.1.1 NIS 概述	78
6.1.2 NIS 的体系结构	78
6.1.3 NIS 常用术语和控制 NIS 服务的主要文件	79
6.1.4 NIS 服务的 C/S 模式	80
6.2 Red Hat Enterprise Linux 6.0 之 NIS 服务器配置	80
6.2.1 环境说明	80
6.2.2 配置 NIS 服务器	80
6.2.3 配置 NIS 客户端	82
第 7 章 Linux NFS 服务器安装及配置	84
7.1 NFS 服务器的工作原理	84
7.1.1 NFS 简介	84
7.1.2 为何使用 NFS	84
7.1.3 NFS 协议	84
7.1.4 RPC	86
7.2 安装及配置 NFS 服务器	86
7.2.1 了解 NFS 网络文件的系统结构	87
7.2.2 配置/etc/exports 文件	87
7.2.3 激活 rpcbind 和 nfsd 服务	88
7.2.4 exportfs 命令	88
7.2.5 检验目录/var/lib/nfs/xtab	88
7.2.6 showmount	89
7.2.7 观察激活的端口	89
7.2.8 启动和停止 NFS 服务器	89
7.3 NFS 的防火墙和 SELinux 设置	89
7.3.1 NFS 的防火墙设置	89
7.3.2 NFS 的 SELinux 设置	90
7.4 NFS 客户端配置	90
7.4.1 软件包的安装及配置	90
7.4.2 使用 mount 命令	90
7.4.3 扫描可以使用的 NFS 服务器目录	91
7.4.4 卸载 NFS 网络文件系统	92
7.4.5 应用实例	92
7.4.6 其他挂载 NFS 文件系统的方法	92
7.5 NFS 服务器的故障排除	93
7.5.1 故障排除思路	93
7.5.2 NFS 错误信息	94
7.5.3 使用 nfsstat 命令查看 NFS 服务器状态	94

7.5.4	NFS 典型故障排除步骤	95	9.3.3	创建 Samba 用户账号	130
第 8 章 Linux SSH 服务器安装及配置		97	9.3.4	日志记录和调试	132
8.1	SSH 服务器的工作原理	97	9.3.5	配置 SWAT	134
8.1.1	传统远程登录的安全隐患	97	9.4	Samba 客户端的使用	136
8.1.2	SSH 保护的對象	97	9.4.1	客户端为 Linux 系统	136
8.1.3	SSH 服务器和客户端的工作流程	98	9.4.2	客户端为 Windows 系统	137
8.2	安装及配置 OpenSSH 服务器	99	第 10 章 Linux Squid 代理服务器安装及配置		138
8.2.1	安装与启动 OpenSSH	99	10.1	代理服务器介绍	138
8.2.2	配置文件	99	10.1.1	各种代理服务器的比较	138
8.2.3	配置使用口令验证登录服务器的实例	101	10.1.2	代理服务器运作方式	138
8.3	应用 SSH 客户端	103	10.1.3	代理服务器的种类	139
8.3.1	SSH 客户端工具	103	10.2	Squid 代理服务器	140
8.3.2	生成密钥对	106	10.2.1	Squid 的安装	140
8.3.3	图形界面工具 gFTP	108	10.2.2	Squid 配置文件 squid.conf	141
8.3.4	使用 Windows SSH 客户端登录 OpenSSH 服务器	108	10.2.3	匿名 Squid 服务器设置	144
8.4	配置使用密钥对（证书）方式远程登录服务器实例	113	10.2.4	需要身份验证的 Squid 服务器设置	145
8.5	使用 Xmanager 实现 Linux 远程管理	117	10.2.5	Squid 反向代理服务器的设置	146
8.5.1	简介	117	10.2.6	正向代理服务器的客户端设置	146
8.5.2	配置 Xmanager 服务器端	117	10.3	Squid 安全工具的使用	147
8.5.3	配置 Xmanager 客户端	118	10.3.1	SquidClamav	147
第 9 章 Linux Samba 服务器安装及配置		120	10.3.2	SquidGuard	149
9.1	Samba 简介	120	10.4	Squid 代理服务器的日志	150
9.1.1	什么是 Samba	120	10.4.1	Squid 日志格式	150
9.1.2	SMB 和 CIFS 对比	120	10.4.2	分析 access.log 日志文件	150
9.1.3	SMB 协议	120	10.4.3	使用 Linux 命令	151
9.1.4	为什么使用 Samba	121	10.4.4	使用专业软件分析	151
9.1.5	Samba 软件简介	122	10.4.5	Squid 日志清理	154
9.2	安装及配置 Samba 服务器	123	第 11 章 Linux MySQL 数据库安装及配置		155
9.2.1	安装 Samba 服务器	123	11.1	数据库理论基础	155
9.2.2	防火墙和 SELinux 设置	123	11.1.1	数据存储方式	155
9.2.3	Samba 相关文件	124	11.1.2	数据库泛型	156
9.2.4	Samba 主配置文件 smb.conf	124	11.1.3	数据库在开发中的作用	156
9.3	Samab 配置实例	129	11.1.4	常见的数据库	157
9.3.1	Samab 配置实例 1	129	11.1.5	为什么要使用 MySQL	158
9.3.2	Samab 配置实例 2	130	11.1.6	MySQL 版本和获取	158
			11.2	MySQL 服务器的安装与配置	159
			11.2.1	安装与测试 MySQL 服务器	159

11.2.2	管理 MySQL 服务器	160	13.2.1	安装	207
11.2.3	MySQL 服务器的用户管理	164	13.2.2	启动 Apache 服务器并且测试	207
11.2.4	MySQL 服务器日志管理	165	13.2.3	目前运行的 Apache 服务器的 相关信息	209
11.2.5	使用 phpMyAdmin 管理 MySQL	167	13.3	Apache 服务器的一般配置	216
11.3	MySQL 服务器数据备份、恢复	170	13.3.1	基本配置指令	216
11.3.1	使用 MySQL 相关命令进行简单 的本地备份	170	13.3.2	配置用户的个人 Web 空间	216
11.3.2	使用网络备份	172	13.4	Apache 服务器的访问控制、认证 和授权	217
11.3.3	实时恢复 MySQL 数据方法	173	13.4.1	Apache 服务器的访问控制	217
11.3.4	使用 phpMyBackupPro 备份 恢复 MySQL 数据库	175	13.4.2	Apache 服务器的认证和授权	217
11.4	MySQL 的安全配置	178	13.5	在 Apache 服务器上配置虚拟主机	219
11.4.1	操作系统安全	178	13.5.1	虚拟主机简介	219
11.4.2	MySQL 用户安全配置	179	13.5.2	虚拟主机的类型	220
11.4.3	MySQL 加固配置	180	13.5.3	基于名称的虚拟主机配置	220
11.4.4	MySQL 的安全例行审计	181	13.6	为 Apache 服务器配置 WebDAV	222
11.4.5	了解 MySQL 安全信息	182	13.6.1	WebDAV 简介	222
11.5	MySQL 的 SQL 注入简介	183	13.6.2	WebDAV 技术的提出	222
11.5.1	SQL 注入简介	183	13.6.3	从 HTTP 到 WebDAV	222
11.5.2	MySQL 中的 SQL 注入	183	13.6.4	WebDAV 工作流程	223
13.6.5	WebDAV 工作方式	224	13.6.6	支持 WebDAV 的服务器工具	224
13.6.7	在 Apache 2.x 系列服务器中设置 WebDAV	224	13.6.8	通过 WebDAV 客户端软件访问 Apache 服务器	225
13.7	多种开发环境语言在 Linux 下的 整合	228	13.7.1	在 Apache 服务器上运行 CGI	228
13.7.2	在 Apache 服务器上运行 PHP	229	13.7.3	在 Apache 上运行 Ruby	231
13.8	Apache 服务器的进阶配置	233	13.8.1	Apache 服务器的实时监控	233
13.8.2	Apache 服务器的日志分析	234	13.8.3	使用 Visitors 分析 Apache 日志	236
13.9	Apache 服务器的安全设置	237	13.10	Apache 服务器的故障排除	239
13.10.1	检查配置文件的错误	239	13.10.2	使用错误日志	240
13.10.3	检查 Apache 服务器模块问题	242	13.10.4	解决 Apache 服务器故障	243
13.11	Apache 服务器网络资源的相关 文档	244			

第 14 章 Linux 电子邮件服务器

Postfix 安装及配置.....245

- 14.1 电子邮件系统的组成和相关协议.....245
 - 14.1.1 操作系统.....245
 - 14.1.2 邮件传输代理 (MTA).....245
 - 14.1.3 邮件分发代理 (MDA).....247
 - 14.1.4 邮件用户代理 (MUA).....248
 - 14.1.5 电子邮件服务器协议及其相关命令.....248
- 14.2 电子邮件服务器的工作原理.....253
 - 14.2.1 电子邮件的发送接收流程.....253
 - 14.2.2 电子邮件的历史.....254
 - 14.2.3 电子邮件地址的组成.....254
 - 14.2.4 电子邮件系统和 DNS 的联系.....255
- 14.3 安装及配置 Postfix.....255
 - 14.3.1 Postfix 的安装.....255
 - 14.3.2 Postfix 的配置文件介绍.....256
 - 14.3.3 Postfix 配置实例.....260
 - 14.3.4 Dovecot 的安装与设置.....261
- 14.4 安全配置.....262
 - 14.4.1 安装病毒过滤系统.....262
 - 14.4.2 日志分析.....264
 - 14.4.3 防火墙和 SELinux 设置.....268

第 15 章 Linux FTP 服务器安装及配置.....269

- 15.1 FTP 的工作原理.....269
 - 15.1.1 FTP 简介.....269
 - 15.1.2 FTP 的功能.....269
 - 15.1.3 FTP 服务器登录方式的分类.....269
 - 15.1.4 FTP 的工作原理.....270
 - 15.1.5 FTP 的典型消息和子命令.....271
 - 15.1.6 Linux 服务器的主要 FTP 软件.....273
- 15.2 配置 Vsftpd 服务器.....275
 - 15.2.1 快速构建 Vsftpd 服务器.....275
 - 15.2.2 Vsftpd 配置文件.....275
 - 15.2.3 Vsftpd 的配置文件.....275
- 15.3 使用客户端工具.....283
 - 15.3.1 命令行.....283
 - 15.3.2 图形界面.....284
 - 15.3.3 使用 Windows FTP 客户端.....288
- 15.4 Vsftpd 服务器故障排除.....289

15.4.1 日志文件.....289

15.4.2 Vsftpd 常见故障排除.....290

第 16 章 Linux 防火墙设置.....292

- 16.1 防火墙简介.....292
 - 16.1.1 什么是防火墙.....292
 - 16.1.2 防火墙的功能.....292
 - 16.1.3 防火墙技术分类.....292
- 16.2 Linux 防火墙.....294
 - 16.2.1 Linux 防火墙的历史.....294
 - 16.2.2 Netfilter/iptables 系统如何工作.....295
 - 16.2.3 iptables 基础.....296
 - 16.2.4 建立规则和链.....301
- 16.3 iptables 配置实战.....305
- 16.4 使用 system-config-firewall 和 Fwbuilder 快速构架 Linux 防火墙.....306
 - 16.4.1 使用 system-config-firewall 快速构架 Linux 防火墙.....306
 - 16.4.2 使用 Fwbuilder 快速构建 Linux 防火墙.....309
- 16.5 为 Linux 防火墙添加 7 层过滤功能.....313
 - 16.5.1 L7-filter 简介.....313
 - 16.5.2 配置 L7-filter 模块.....313
- 16.6 构建 Linux 下的 NAT 服务器.....315
 - 16.6.1 NAT 基础.....315
 - 16.6.2 NAT 的优点和不足.....320

第 17 章 使用 SELinux.....322

- 17.1 SELinux 简介.....322
 - 17.1.1 SELinux 起源.....322
 - 17.1.2 SELinux 架构.....323
 - 17.1.3 为什么使用 SELinux.....326
 - 17.1.4 SELinux 决策进程.....327
 - 17.1.5 SELinux 相关文件.....327
- 17.2 SELinux 使用实战.....328
 - 17.2.1 SELinux 布尔值和上下文配置.....329
- 17.3 SELinux 管理命令.....333
 - 17.3.1 setenforce: 设置 SELinux 模式.....333
 - 17.3.2 getenforce: 查看 SELinux 模式.....333
 - 17.3.3 setsebool: 设置 SELinux 布尔值.....333
 - 17.3.4 getsebool: 查看 SELinux 布尔值.....334

17.3.5	sestatus: SELinux 状态查看工具	334
17.3.6	avcstat: 显示 AVC 统计信息	335
17.3.7	audit2allow: 生成策略允许规则	335
17.3.8	semanage: 管理 SELinux 策略	336
17.3.9	semodule: 管理策略模块	337
17.3.10	chcat: 改变语境类别	338
17.3.11	restorecon: 恢复文件安全语境	339
17.3.12	chcon: 改变文件安全语境	339
17.3.13	setfiles: 设置文件安全语境	340
17.3.14	seinfo: 提取策略的规则数量 统计信息	340
17.3.15	sesearch: 搜索 policy.conf 或 二进制策略中特别的类型	341
17.3.16	sealert: SELinux 信息诊断客户 端工具	342
17.4	SELinux 日志文件的使用	342
17.5	SELinux 和网络服务设置	343
17.5.1	Apache 与 SELinux	343
17.5.2	Samba 和 SELinux	344
17.5.3	Vsftp 和 SELinux	345
17.5.4	NFS 和 SELinux	346
17.5.5	MySQL 和 SELinux	346
17.5.6	DNS 和 SELinux	347
第 18 章 PAM 的安装及配置		348
18.1	PAM 工作原理	348
18.1.1	什么是 PAM	348
18.1.2	为什么使用 PAM	348
18.1.3	PAM 体系结构	349
18.1.4	PAM 工作流程	349
18.2	PAM 配置文件	350
18.2.1	Module-Type (模块类型)	350
18.2.2	Control-Flag (控制字)	351
18.2.3	Module-Path (模块路径)	351
18.2.4	Module-Args (模块参数)	351
18.3	PAM 应用实例	351
18.3.1	限制 su 命令	351
18.3.2	设置指纹应用	351
18.3.3	使用 PAM 控制 Samba 用户的 共享登录	353
18.3.4	使用 PAM 控制 FTP 用户的登录	353

第 19 章 Linux 网络环境下的 VPN 构建		355
19.1	VPN 概述	355
19.1.1	VPN 定义	355
19.1.2	VPN 功能	355
19.1.3	VPN 分类	356
19.1.4	Linux 下的主要 VPN 技术	357
19.2	PPTP VPN 安装及配置	360
19.2.1	PPTP 及 Poptop 简介	360
19.2.2	PPP 简介	361
19.2.3	在 Linux 下安装及配置 PPTP 服务器	362
19.3	OpenVPN 安装及配置	365
19.3.1	OpenVPN 简介	365
19.3.2	OpenVPN 服务器安装及配置	366
19.3.3	OpenVPN 客户端安装及配置	369
第 20 章 Linux iSCSI 和 AoE 存储配置		371
20.1	企业级存储简介	371
20.1.1	DAS、NAS、SAN 三种模式	371
20.1.2	SAN 的两种部署方案	372
20.1.3	iSCSI 技术简介	374
20.2	Linux iSCSI 配置	376
20.2.1	Linux 下安装启动 iSCSI Target	376
20.2.2	Linux 下安装设置 iSCSI Initiator	377
20.2.3	Windows 客户端使用 iSCSI 磁盘 设备	378
20.3	使用 openfiler 搭建 iSCSI 网络 存储	380
20.3.1	openfiler 简介	380
20.3.2	安装 openfiler	380
20.3.3	openfiler 配置	382
20.4	AoE 存储设置	385
20.4.1	AoE 简介	385
20.4.2	Linux 下配置 AoE 模块	387
第 21 章 Linux 备份与恢复		390
21.1	Linux 备份基础	390
21.2	Linux 备份恢复策略	390
21.2.1	备份前需考虑的因素	390
21.2.2	选择备份介质	391

21.2.3	Linux 备份策略	392	22.3.9	配置 IMAP 插件	445
21.2.4	确定要备份的内容	393	22.4	使用 Zabbix	445
21.2.5	Linux 磁带机备份和恢复	394	22.4.1	Zabbix 简介	445
21.3	常用备份工具的使用	399	22.4.2	安装及配置 Zabbix	447
21.3.1	使用 mirrordir 做硬盘分区镜像	399	22.4.3	配置前台 Web 界面	448
21.3.2	使用 partimage 备份恢复 Linux 分区	400	22.4.4	设置报警	450
21.3.3	使用 afio 工具备份和恢复	401	第 23 章 Linux 虚拟化	453	
21.3.4	Linux 备份恢复工具	402	23.1	虚拟化历史	453
21.4	使用网络备份工具 Bacula	403	23.1.1	硬件虚拟化	453
21.4.1	Bacula 简介	403	23.1.2	处理器虚拟化	453
21.4.2	Bacula 安装及配置	406	23.1.3	指令集虚拟化	453
21.4.3	执行备份和恢复	410	23.1.4	主流虚拟化技术	454
21.4.4	使用图形化工具 bacula-console-bat	413	23.1.5	存储虚拟化	455
第 22 章 Linux 服务器监控	415		23.1.6	网络虚拟化	456
22.1	服务器性能监控	415	23.2	Linux 虚拟化简介	456
22.1.1	性能监控方法	415	23.2.1	Linux 虚拟化类型	456
22.1.2	lproc 文件系统的特点	415	23.2.2	Linux 虚拟化项目	457
22.1.3	lproc 文件系统的功能	416	23.2.3	Linux 服务器虚拟化的重要性	458
22.1.4	监控系统负载	416	23.3	VirtualBox 虚拟化技术	459
22.1.5	使用 phpsysinfo	417	23.3.1	VirtualBox 简介	459
22.1.6	监控 Linux 进程运行	418	23.3.2	Linux 下安装、卸载 VirtualBox	460
22.1.7	监控内存使用情况	419	23.3.3	启动 VirtualBox	460
22.1.8	监控中央处理器	420	23.3.4	建立一个虚拟机	461
22.1.9	使用 iostat 监控 I/O 性能	421	23.3.5	虚拟机配置	462
22.1.10	监控网络性能	422	23.3.6	使用 VirtualBox 在 Linux 下安装运行 Windows XP SP3 的技巧	464
22.1.11	sar	424	23.3.7	增强功能工具的其他功能	466
22.1.12	使用 kSar	428	23.4	KVM 虚拟机配置	467
22.2	Linux 核心硬件状态监控	433	23.4.1	KVM 虚拟机简介	467
22.2.1	使用命令行工具检测主板、CPU	433	23.4.2	安装及配置 KVM 相关软件	468
22.2.2	使用 smartmontools 检测硬盘健康状况	436	23.4.3	使用 virt-manager 建立一个 KVM 虚拟机	469
22.3	使用 Nagios	437	23.4.4	RHEL 6 KVM 虚拟机新功能	471
22.3.1	Nagios 简介	437	23.4.5	使用命令行执行高级管理任务	475
22.3.2	安装 Nagios	438	23.5	KVM 虚拟机存储管理	477
22.3.3	添加监测目标	439	23.5.1	KVM 虚拟机存储模式解析	477
22.3.4	在监测主机上安装 nrpe 代理	440	23.5.2	创建基于分区的存储池	478
22.3.5	设置报警	441	23.5.3	创建基于目录的存储池	479
22.3.6	安装其他插件	442	23.5.4	创建基于 LVM 的存储池	480
22.3.7	配置 SMTP 插件	443	23.5.5	使用命令行方式管理存储池	481
22.3.8	配置 POP 插件	444	23.6	KVM SPICE 配置	483

23.6.1	SPICE 简介	483	24.2.1	LVS 诞生背景	495
23.6.2	安装及配置 SPICE 服务器	483	24.2.2	IPVS 负载调度算法	496
23.6.3	使用 SPICE 客户机	485	24.2.3	LVS 系统介绍	496
23.7	KVM 虚拟机安全	486	24.3	组建基本的 LVS 系统	499
23.7.1	SELinux 设置	486	24.3.1	ipvsadm 的安装和使用	499
23.7.2	防火墙设置	487	24.3.2	调度服务器设置流程	500
23.8	远程管理虚拟机	487	24.3.3	应用服务器设置流程	501
第 24 章	Linux 集群配置	488	24.3.4	测试 LVS 系统	501
24.1	Linux 集群技术简介	488	24.3.5	使用 Piranha 配置调度服务器	502
24.1.1	集群计算 IEEE 工作组	488	24.4	使用 Corosync 和 Pacemaker	507
24.1.2	集群系统	488	24.4.1	安装及配置 Corosync 和 Pacemaker	507
24.1.3	集群的作用	489	24.4.2	配置虚拟 IP 地址	508
24.1.4	Linux 集群的作用	489	24.4.3	监测 http 服务	509
24.1.5	Linux 集群体系结构	490	附录 A	Linux 服务器应急响应流程 与步骤	511
24.1.6	Linux 集群分类	491	附录 B	Linux 计算机系统取证	518
24.1.7	Linux 集群发展趋势	491	附录 C	Linux 下反删除和彻底删除工 具的使用	527
24.1.8	创建一个 Linux 集群	492			
24.1.9	成功配置 Linux 集群的建议	494			
24.2	LVS 安装及配置	495			

第 1 章

Linux 简介

1.1 UNIX 发展史

谈到 Linux 的发展史，就不得不谈一谈 UNIX 的发展过程。1965 年，由 AT&T 贝尔实验室、通用电气、麻省理工学院三大机构共同组建了一个 MAC 课题组，一起联合开发一个称为 Multics 的新操作系统。Multics 系统的目标是要向大的用户团体提供对计算机的同时访问，支持强大的计算数据存储，以及允许用户在需要的时候共享数据。

Multics 项目中止后，Ken.Thompson 和 Dennis.Ritchie 利用在 Multics 项目中所学的内容，一起着手开发 DEC PDP-7 上的操作环境。1973 年，Thompson 和 Ritchie 在 Purdue 大学召开的操作系统原理研讨会上，发表了第一篇关于 UNIX 的论文，会后得到大量爱好者的支持，并得到他们开发的 UNIX 源代码。

不久后，AT&T 公司受到美国反托拉斯法的诉讼，与美国联邦政府签署了一份协议，这份协议不允许 AT&T 公司生产与电话和电报服务无关的设备，也不允许从事除“公用通信服务”以外的任何商业活动。这样，AT&T 公司就陷入了不能经营计算机产品的尴尬局面。为了满足大家的需要，AT&T 公司在签署简单协议的前提下，将 UNIX 系统无偿地提供给大学，以供教学和研究。

在美国高校，UNIX 经过 10 年的开发研究。因各高校开发理念的不同，后来产生了很多个 UNIX 操作系统分支。其中，BSD UNIX 分支是一个非常重要的分支，其技术含量已达到商业操作系统的标准，并于 1982 年由 Bill Joy 成立了 SUN 公司（已被 Oracle 公司收购）；基于 BSD 开发，也就是现在的 Solaris 系统。另外还有 System V 分支，一直在贝尔实验室开发，引进了许多新特性、新设施，最具代表性的就是进程间通信机制。比如 IBM 公司基于 UNIX 系统开发 AIX，运行在 RS6000 小型机上；HP 公司开发 HP-UX，运行在 HP 的计算机上。

因 UNIX 商业化运作，高校无力购买商业版的 UNIX 系统。后来，芬兰的 Tanenbaum 教授为了教学开发了一个 mini 的 UNIX 系统，简称 Minix 系统。Minix 系统主要用于教学，让学生更形象、更清楚地了解操作系统的原理，20 世纪 90 年代它在中国高校流行。但后来因对应的软件非常少而使用较难，在 90 年代末期，它逐渐被淘汰。

1.2 Linux 发展史

Tanenbaum 教授开发了 Minix 系统后，引发了学生 Linus Torvalds 的兴趣。Minix 是个教学工具，而不是一个强大的操作系统。后来，Linus Torvalds（“Linux 之父”）在此操作系统基础上，开发出一个基于 386 系统的自由 Linux 系统，并将其发布到新闻组上，称这是一个开源、自由、免费使用的操作系统，后得到全球广大爱好者的大力支持，在此基础上添加了很多代码。1994 年 3 月 14 日，Linux 1.0 发布，Linux 转向 GPL 版权协议。同年，第一个商业化的 Slackware Linux 系统发布。后来各种不同的 Linux 操作系统相继问世。1999 年，Linux 的简体中文版发布，RedFlag Linux 就是一个代表。2004

年，Linux 操作系统得到大力发展。后在广东省政府的大力支持下，成立了广东省 Linux 公共服务技术支持中心，在广东及泛珠三角地区大力推广 Linux 系统。因 Internet 的快速发展，互联网服务器得到前所未有的重视。而 Linux 以其安全、稳定、高性能的优势，占据了大量的服务器市场，并得到了企业用户和政府用户的一致好评。近几年，Linux 操作系统在桌面系统上也得到了快速发展，其中 Ubuntu 就是典型代表，得到了全球广大用户的大力好评。在欧洲的许多国家，都以 Linux 操作系统作为政府的电子商务系统。

1.3 常用的 Linux 发行版介绍

Linux 最早由 Linus Torvalds 在 1991 年开始编写。在早期，Richard Stallman 创建了 Free Software Foundation (FSF) 组织以及 GNU 项目，不断地编写、创建 GNU 程序，并遵从 GPL 许可方式。后来有更多的程序员和开发者不断地加入 GNU 组织，造就了今天人们所看到的 Linux 操作系统，也称 GNU/Linux 系统。不同的操作系统厂商发布不同的 Linux 版本，其中最著名的是 Red Hat 公司的 Red Hat 系列以及社区组织的 Debian 系列等。下面就简单介绍一下目前比较流行的 Linux 发行版本。

1.3.1 Red Hat

Red Hat Linux 系统是全球最受欢迎的服务器版操作系统，其服务器的功能非常强，性能也非常好，对系统和内核做了很好的调优。大多数企业都在使用 Red Hat Linux 系统。Red Hat 最早由 Bob Young 和 Marc Ewing 在 1995 年创建。而公司在近几年才开始真正步入盈利时代，这归功于收费的 Red Hat Enterprise Linux (RHEL, Red Hat 企业版)。目前，Red Hat 系统大体分以下 3 个系列：

第一个系列是由 Red Hat 公司提供收费技术支持和更新的 Red Hat Enterprise Linux。现在最新版本为 Red Hat Enterprise Linux 6.0。企业用户使用比较多的是 Red Hat Enterprise Linux 6.0 和 5.0。

第二个系列是由社区开发的免费的 Fedora Core (简称 FC)。最新版本为 Fedora Core 16，发布于 2011 年 11 月，而 FC 的定位是桌面用户。FC 提供了最新的软件包，同时，它的版本更新周期也非常短，仅 6 个月左右。一般不建议服务器使用 FC 系列。

第三个系列是 Red Hat 克隆版 CentOS，内容与 Red Hat Enterprise Linux 操作系统一样，只是将 Red Hat Enterprise Linux 操作系统的 logo 和 rpm 进行了重新编译，形成了一个免费的 Linux 系统，基本上与 Red Hat Enterprise Linux 操作系统同步发行。国外的很多企业都使用这个版本。现在最新版本为 CentOS 6.0。

优点：拥有庞大的用户群及众多的技术资料社区。

缺点：免费版的 FC，生命周期太短，对多媒体的支持不是很好。

软件包管理系统：up2date(rpm)、yum(rpm)。

是否免费下载：是。

官方网站：<http://www.redhat.com/>，<http://www.centos.org/>，<http://fedoraproject.org/>。

1.3.2 SUSE

SUSE 是德国最著名的 Linux 发行版，在整个 Linux 行业中具有较高的名誉。从市场份额来看，SUSE 操作系统占据服务器市场第二的位置。最新发布的 11.2 版本得到广大爱好者的青睐，在企业中的使用量也非常大；对 3D 的支持非常好，但对内存的要求比较高。SUSE 自主开发的软件包管理系统 YaST 也大受好评。SUSE 发布版本显得比较混乱，比如 9.0 版本是收费的，由于各种压力方面的原因，10.0 版本又免费发布。这使得一部分企业用户感到困惑，从而转向使用其他的 Linux 发行版本。但是，瑕不掩瑜，SUSE 仍然是一个非常专业、优秀的 Linux 发行版本。openSUSE 项目是 Novell 公司资助的社区计划，在方方面面促进 Linux 的普及应用，并提供免费、易于访问的 openSUSE 这个完整的 Linux

发行版本。openSUSE 项目有三个主要目标：让 openSUSE 成为任何人都能最容易获得且最广泛使用的 Linux 发行版本；利用开源软件的联合来使 openSUSE 成为世界上可用性最强的 Linux 发行版本，以及新手和资深 Linux 用户的桌面环境；显著地简化并开放其开发及打包过程，以使 openSUSE 成为 Linux 开发人员及软件提供商选择的平台。

优点：专业、易用的 YaST 软件包管理系统。

缺点：FTP 发布通常要比零售版晚 1~3 个月。

软件包管理系统：YaST(rpm)、第三方 APT(rpm)软件库。

是否免费下载：取决于版本。

官方网站：<http://www.suse.com/>，<http://www.opensuse.org/>。

1.3.3 Debian

Debian GNU/Linux 是 Linux 爱好者最中意的 Linux 操作系统，Debian 计划是一个以创建一个自由操作系统为共同目标的个人团体所组建的协会。Debian 最早由 Ian Murdock 夫妇于 1993 年创建，可以算是迄今为止最遵循 GNU 规范的 Linux 系统。Debian 系统分为 3 个版本分支，包括 stable、testing 和 unstable。

- unstable 为最新的测试版本，其中包括最新的软件包，但是也有相对较多的 bug，适合桌面用户使用。
- testing 版本都经过 unstable 中的测试，相对较为稳定，另外还支持不少新技术（比如 SMP 等）。
- stable 版本一般只用于服务器，上面的软件包大部分都比较过时，但是稳定性和安全性非常高。

Debian 提供了 25000 多套软件，都是已经编译好的软件，并按一种优秀的格式打包，可以供用户在机器上方便地安装。这一切都可以免费获得。为何有如此多的用户痴迷于 Debian 呢？主要是因为 Debian 系统软件包更新非常方便，可采用 apt-get 和 dpkg 命令实现。其中 dpkg 是 Debian 系列特有的软件包管理工具，被誉为所有 Linux 软件包管理工具（比如 rpm）中最强大！配合 apt-get，在 Debian 上安装、升级、删除和管理软件变得异常容易。

优点：遵循 GNU 规范，完全免费，优秀的网络和社区资源。

缺点：安装相对较难，stable 版本的软件极度过时。

软件包管理系统：APT(DEB)。

是否免费下载：是。

官方网站：<http://www.debian.org/>。

1.3.4 Ubuntu

现在最流行的 Linux 桌面系统莫过于 Ubuntu 了，Ubuntu 基于 Debian 的 unstable 版本演变而来，应该说 Ubuntu 是一个拥有 Debian 所有优点的桌面操作系统。Ubuntu 是一个相对较新的发行版本，同时，它的出现也改变了许多潜在用户对 Linux 的看法。从前人们认为 Linux 难以安装、难以使用，但是 Ubuntu 出现后，这些都成了历史。Ubuntu 默认采用的 Unity 桌面系统也将 Ubuntu 的界面装饰得简易而不失华丽。即使你是一个 KDE 的拥护者，Ubuntu 也同样适合你。Ubuntu 的安装非常人性化，只要按照提示一步步地进行即可，和 Windows 一样简便。Ubuntu 被誉为对硬件支持最好且最全面的 Linux 发行版之一，支持的软件也是最新的版本。例如最新开发的 Ubuntu 11.04，已经安装好了新版的 OpenOffice 办公自动化软件；同时 Ubuntu 系统可以轻松实现网上快速更新。为了安全管理，在默认情况下 Ubuntu 系统不允许 root 通过图形界面登录，若要安装某个软件，则可以采用 sudo 命令进行。

最让人开心的事情是新版的 Ubuntu 系统内置有桌面动画，当然用户也可以自己安装 beryl 软件包；能够更好地支持 3D 桌面，能让你的桌面变得更酷！

优点：人气颇高的论坛提供优秀的资源和技术支持，拥有固定的版本更新周期和技术支持，可从