

**Broadview**<sup>®</sup>  
www.broadview.com.cn

 LAMP技术大系

本书销售所得  
全部用于公益事业。

# Ubuntu Server 最佳方案

冷罡华 (Hiweed) 编著



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

 LAMP技术大系

# Ubuntu Server 最佳方案

冷罡华 (Hiweed) 编著

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING



## 内 容 简 介

本书是第一本全面介绍 Ubuntu Linux Server 的中文书籍，是作者 10 多年实战经验的结晶；从构思到出版，花费作者近 3 年时间。无论您是初学者还是 Linux 高手，都能从中获益。

在内容上，本书基本上涉猎到了 Linux 服务器的各方面常见应用。“最佳方案”是本书的特色。对于每一种应用，作者都不是泛泛而谈，而是推荐一个“最佳方案”——从硬件服务器的选型到 Linux 入门，从 LAMP 到 Tomcat，从代理服务器到邮件服务器，从 DHCP 到 DNS，从 Samba 到虚拟化，从负载均衡到远程控制，从 RAID 到 LVM 再到系统安全——不管您是在校学生还是在职 Linux 管理员，不管您是小公司还是大企业，都可以直接复制本书内容，在最短的时间内您就可以架设起自己的最佳 Linux 服务器。

拥有本书，您就拥有了一位具有 10 年经验的资深 Linux 管理员和开发者的最佳实战方案，有如专家亲临现场、全程陪护，让您在工作中胸有成竹，胜券在握。

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

Ubuntu Server 最佳方案 / 冷昱华编著. —北京: 电子工业出版社, 2009.6

(LAMP 技术大系)

ISBN 978-7-121-08776-9

I. U… II. 冷… III. Linux 操作系统 IV. TP316.89

中国版本图书馆 CIP 数据核字 (2009) 第 071369 号

策划编辑: 李 冰

责任编辑: 葛 娜

印 刷: 北京智力达印刷有限公司

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: 27 字数: 659 千字

印 次: 2009 年 6 月第 1 次印刷

印 数: 4000 册 定价: 55.00 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 [zlls@phei.com.cn](mailto:zlls@phei.com.cn)，盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

服务热线：(010) 88258888。

# 前 言

“我们的服务器用的是软 RAID，现在硬盘不够了，需要添加新硬盘，请问应该怎么做？”

“我们发现服务器被入侵了，请问应该怎么做？”

“目前 Web 和数据库在同一台服务器上，可是由于我们的企业发展得太快，现在服务器不够用了，计划增加两台服务器，请问您如何设计方案？”

——面试“Linux 系统管理员”时可能会被问到的问题

近年来，Linux（尤其是 Ubuntu）一直保持上升势头，据说目前中国的 Linux 人才缺口已经达到 120 万！在 2008 年开始的全球经济大萧条中，虽然各大公司都在裁员，但是我相信，一个真正优秀的 Linux 系统管理员，是任何公司都不可能轻易解聘的；不知有多少大大小小的公司，正在如饥似渴地寻求 Linux 人才，却常常感叹一才难求！

我在帮助朋友的公司招聘 Linux 系统管理员时，发现一个问题：很多人只是对桌面系统很熟悉，却不熟悉 Linux 服务器；有的人虽然熟悉，却不深入，不精通。

本书正是帮助您迅速提高 Linux 服务器管理技能和经验的绝佳教材。

## 本书的特色

您拨打家电维修电话时，可能会听到下面的语音：

“普通话请按 1，English press 2。”

“个人服务请按 1，企业客户请按 2。”

“小家电请按 1，电冰箱请按 2，空调器请按 3，……”

您也许碰到过下面的问题：

“请选择您最喜欢的颜色，深红色、红色、浅红色、深绿色、绿色、浅绿色、深蓝色、蓝色、浅蓝色……”

您还可能遇到过这种情况：

您上了公交车，发现有很多空座位，这时您会挑来挑去，不知道坐在哪里才好；可是如果上车后只有一个座位，不管这个座位在哪里，您都会毫不犹豫地坐上去……

如今的生活中，到处都充满了“选择”。这么多的“选择”，未必是桩好事，很多人在面对太多选择时，每每会无所适从。

Linux 管理员面对的选择，同样很多。要解决一个问题，可能有多种方案。比如，您要安装 FTP 服务器，那到底是用 ProFTPd 呢，还是 PureFTPd？是用 WU-FTPd 呢，还是

VsFTPD? 这个问题太恼人了。再比如, 为了保证数据安全, 您打算用 RAID。那么是用硬件 RAID 呢, 还是软件 RAID? 是用 RAID0 呢, 还是 RAID1? 是用 RAID5 呢, 还是 RAID10? 这个问题更加恼人。

因此, 本书在编写时, 特别注意实用性、实战性; 针对某方面问题, 给出一个**最佳方案**, 让您拿起本书就可以直接解决问题。“最佳方案”不是一句空洞的口号, 它是一套有 10 年经验的 Linux 资深管理员会采用的策略, 是实实在在、即读即用的实战解决方案。

## 本书的使用方法

Linux 高手的成功秘诀是什么? “无他, 唯手熟尔。”话虽如此, 但是方式方法也不可忽略, 否则就可能南辕北辙, 渐行渐远。为此, 我向读者郑重推荐了 LFS——学习 Linux 的“终南捷径”; 我以 10 年经验告诉您, 亲爱的读者, 要想以最快速度理解 Linux 操作系统的结构、原理, 非 LFS 莫属。当您掌握了 LFS 后, 再继续阅读本书的其余部分, 结果会大不一样。

您可以按顺序从头阅读本书, 也可以跳跃阅读。在本书的“方案”部分中, 大多数章节之间没有直接联系; 如果有, 我一定会做说明。

本书中的所有方案, 包括步骤和配置文件, 全部经过作者 Hiweed 本人亲自实验通过。实验环境是 VMware Server, 这是个免费软件, 读者可以从 VMware 的网站上下载到。另外, 我们所安装的服务器的 IP 地址为 192.168.1.10, 这个地址全书通用, 见到这个地址, 您就应该知道它是您的 Ubuntu 实验环境的 IP 地址。

您需要下载 Ubuntu Server 8.04LTS 的光盘镜像, 从下面的地址可以下载:

<http://www.ubuntu.com/getubuntu/download-server>

另外, 为了避免手工输入给您带来的麻烦, 本书的所有要输入的命令、配置信息, 以及屏幕输出信息, 都可以从下面的地址下载到:

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

<http://hiweed.com/files/ubuntu-server.zip>

## 本书的重点内容

本书共分为 9 篇 24 章。

篇	章	内容介绍
第 1 篇 拥抱 Ubuntu Server	第 1 章 敲开 Linux Server 的大门 第 2 章 拥抱 Ubuntu Server	介绍了 Linux 及其选型, 并提供了 Ubuntu 快速入门指南
第 2 篇 LAMP 服务器	第 3 章 用 Apache 做 Web 服务器 第 4 章 LAMP 服务器之 PHP 篇 第 5 章 LAMP 服务器之 Perl 篇 第 6 章 LAMP 服务器之 Python 篇 第 7 章 Apache Tomcat 架设 第 8 章 最佳代理、反向代理服务器: Squid	介绍了最佳 LAMP 服务器, 并对 PHP、Perl、Python、Tomcat 分别进行了详细的介绍。此外, 由于代理服务器也属于 Web 范畴, 因此本篇中还介绍了最佳代理服务器、反向代理服务器方案 (Squid)

续

篇	章	内容介绍
第 3 篇 Mail 服务器	第 9 章 最佳邮件服务器方案 第 10 章 最佳邮件列表: Mailman	介绍了最佳邮件服务器方案 (Postfix), 该方案不仅支持虚拟用户、虚拟域, 还支持 POP3 收信、IMAP 收信、SMTP 认证、TSL 加密、邮件别名和转发、磁盘限额、垃圾邮件过滤, 支持病毒防护、Web 邮件界面, 基本上涵盖了邮件服务器的方方面面。本篇还介绍了最佳邮件列表方案 (Mailman), 让您可以创建自己的邮件列表服务器
第 4 篇 文件服务器	第 11 章 最佳 FTP 服务器方案 第 12 章 最佳 NFS 服务器方案 第 13 章 与 Windows 共舞: Samba	介绍了最佳 FTP 服务器方案 (PureFTPd) 和最佳 NFS 方案, 并介绍了与 Windows 环境沟通的方法 (Samba)
第 5 篇 虚拟化	第 14 章 最佳虚拟化方案: OpenVZ	介绍了最佳虚拟化方案 (OpenVZ), 您可以在一台物理服务器上虚拟几台、十几台甚至上百台 Linux 服务器
第 6 篇 DNS 和 DHCP 服务器	第 15 章 最佳 DNS 服务器: Bind9 第 16 章 DNS 轮询 第 17 章 最佳 DHCP 服务器方案	介绍了最佳 DNS 服务器 (Bind9) 和最佳 DHCP 方案。如果您管理一个内部网络, 这两种服务器不可或缺
第 7 篇 负载均衡和集群	第 18 章 负载均衡、高可用的 Web 集群 第 19 章 负载均衡、高可用的 MySQL 集群	介绍了负载均衡、高可用的最佳 Web 集群方案和最佳 MySQL 数据库集群方案。作为一个 Linux 管理员, 您需要在架构设计之初, 就能预见未来几年内的需求增长, 否则在业务迅速增长、需要添加服务器时, 您将手足无措
第 8 篇 远程控制与监控	第 20 章 最佳远程控制方案: SSH 第 21 章 最佳服务器监控方案: Nagios	介绍了最佳远程控制方案 (SSH) 和最佳监控方案 (Nagios)。远程控制最重要的是安全, 否则黑客很有可能闯进来, 使您失去控制权。监控可以让您及时了解服务器状况, 免得总是“救火”
第 9 篇 数据备份与系统安全	第 22 章 最佳 RAID 方案: RAID10 第 23 章 最佳数据安全方案: RAID10+LVM 第 24 章 Ubuntu Server 系统安全	介绍了最佳 RAID 方案 (RAID10)、最佳数据安全方案 (RAID10+LVM), 并介绍了如何使 Ubuntu Server 变得更安全。安全是重中之重, 您不仅要学会如何设置防火墙, 还要熟知入侵检测和肉鸡检测的方法, 以及如何处理被入侵的服务器

一个人的能力是有限的。虽然每一个章节都经过了仔细推敲、反复试验, 但是书中肯定会有不妥之处, 甚至还会有错误; 就像软件一定会有 Bug 一样。如果您发现问题, 请不吝指教, 直接发邮件给我 (hiweed@gmail.com), 我会认真回复您。

## 《Ubuntu Server 最佳方案》增值服务

图书精彩，但内容毕竟有限，作为《完美应用 Ubuntu》的姊妹篇《Ubuntu Server 最佳方案》，UbuntuChina 互动社区将继续为该书提供专业的线上增值服务。



UbuntuChina 互动 (<http://www.ubuntuchina.com>) 社区是第一个 Ubuntu 中国实验室的社区网站，专注于 Linux 和 Ubuntu 在中国的应用和传播。UbuntuChina 互动社区为《Ubuntu Server 最佳方案》的广大读者提供了如下增值服务：

### (1) 订阅社区精华

通过 RSS 订阅 Ubuntu 中国社区海量线上精华学习资源，文档、视频、资料应有尽有。

### (2) 下载电子期刊

内容丰富的电子期刊《开源实用技术文摘》以及国际著名电子期刊《Full Circle》中文版。

### (3) 与众多 UbuntuChina 社区的朋友在线互动

技术切磋是迅速提高技术水平的捷径，在 UbuntuChina 社区和众多志同道合的朋友以及 Ubuntu 高手一起探讨、切磋 Ubuntu 使用之道。

### (4) 向 UbuntuChina 社区的高手请教

向 UbuntuChina 社区的高手请教主要有两种方式：加入社区 QQ 群（群号 11874375）和 MSN 群（[group26699@msnzone.cn](mailto:group26699@msnzone.cn)）。

## 致 谢

子曰：“孝弟也者，其为仁之本与。”因此，首先我要将本书献给亲爱的父母——父亲大人讳冷家煜，母亲大人讳昌明芳。养儿方知父母恩，我越来越能体会这句话的分量。从降生到养育成人，多少个日日夜夜，父母的爱和恩德，我做儿子的，说上三天三夜，也无法描述其万一。百善孝为先，以后我一定更加孝敬爹妈，养父母之身，养父母之心，养父母之志。

其次，我把本书献给我的哥哥冷照华。没有哥哥，我就上不了大学。为了赚钱供我上学，哥哥真是吃尽了苦头。1991 年，刚满 18 岁的哥哥，就开始了打工生涯；扛大包出苦力，每天赚 5 块钱，吃饭不舍得买菜，吃火烧蘸盐水……每想到此，心中总是翻江倒海，心疼、感恩、惭愧揉在一起，心情难以平静……

我还要将本书献给我的妻子商宁和儿子冷国册。写作之初，妻子还没有怀孕；本书结稿时，儿子已经出生近 7 个月了。这期间，作为丈夫和父亲，我欠他们太多了。为了能让我及时交稿，妻子不仅给了我轻松的环境，使我没有家庭和思想负担，而其总是给我很多赞美和鼓励，在此我深深地感激她。儿子则给我内心带来了前所未有的平静，让我认识了净空法师和《弟子规》，让我找到了人生的方向。所以，对于儿子，我同样心怀感激。

也感谢出版社的策划人李冰和编辑葛娜两位老师，没有她们的帮助，就不会有这本书。

# 目 录

## 第 1 篇 拥抱 Ubuntu Server

第 1 章 敲开 Linux Server 的大门	2
1.1 Linux 到底是什么	2
1.2 为何选 Linux, 不选 Windows	3
1.2.1 Linux 可以定制	4
1.2.2 Linux 比 Windows 稳定	4
1.2.3 Linux 比 Windows 响应快	4
1.2.4 Linux 比 Windows 安全	5
1.2.5 Linux 不用花钱买	6
1.2.6 Linux 更适合远程管理	6
1.3 学习 Linux 的终南捷径	6
1.3.1 兴趣、试验	6
1.3.2 真正的捷径——LFS	7
1.4 选择哪个 Linux 发行版呢	7
1.4.1 先排除 Gentoo	8
1.4.2 再排除 Red Hat、CentOS 和 SUSE	8
1.4.3 Debian 不错	8
1.4.4 推荐使用 Ubuntu	8
1.5 应该买什么样的服务器呢	10
1.5.1 架构设计	10
1.5.2 服务器的选型	10
1.5.3 机房的选择	11
第 2 章 拥抱 Ubuntu Server	12
2.1 Ubuntu 的前世今生	12
2.2 安装 Ubuntu Server	13
2.2.1 安装前的准备	13
2.2.2 安装 Ubuntu Server	13
2.2.3 把语言环境变量改为英文	29

2.2.4 安全补丁、版本升级	30
2.3 Ubuntu 快速入门指南	31
2.3.1 nano 编辑器	31
2.3.2 强大的“资源管理器”： mc	32
2.3.3 快速查找文件	32
2.3.4 软件包管理	33
2.3.5 使用 apt 工具	35
2.3.6 给 Red Hat 用户	42
2.3.7 Ubuntu 网络配置	45
2.3.8 远程管理 Ubuntu Server	48
2.3.9 系统更新：apt-get update && apt-get upgrade	49

## 第 2 篇 LAMP 服务器

第 3 章 用 Apache 做 Web 服务器	51
3.1 Apache 简介	51
3.2 Apache 的安装、配置	52
3.2.1 Apache 的安装	52
3.2.2 Apache 的配置	52
3.2.3 Apache 虚拟主机	54
3.3 Apache 性能优化	62
3.3.1 正确选择 MPM	63
3.3.2 优化 Apache 配置	63
3.3.3 使用反向代理	68
3.4 Apache 压力测试 (ab)	68
3.5 Apache 安全	70
3.5.1 安全更新	70
3.5.2 隐藏敏感信息	70
3.5.3 不要以 root 身份运行 Apache	72
3.5.4 密码认证	73



3.5.5	检查文件权限	75	第 5 章	LAMP 服务器之 Perl 篇	95
3.5.6	关闭不用的模块	75	5.1	安装 Perl 模块	95
3.5.7	DDoS 攻击防范	76	5.2	配置 cgi-bin 目录	95
3.6	Apache 日志分析	78	5.3	Perl 程序测试	96
3.6.1	用 Webalizer 分析 Apache 日志	78	5.4	用 Perl 访问 MySQL 数据库	96
3.6.2	用 AWStats 分析 Apache 日志	80	5.5	CGI 排错	98
3.6.3	Apache 日志合并	82	5.6	实例：用 Twiki 假设 Wiki	99
			5.6.1	安装 Twiki	99
			5.6.2	配置 Twiki	99
第 4 章	LAMP 服务器之 PHP 篇	84	第 6 章	LAMP 服务器之 Python 篇	101
4.1	MySQL 简介	84	6.1	安装 mod_python	101
4.2	PHP 简介	85	6.2	配置 Apache	101
4.3	安装 LAMP 相关软件包	85	6.2.1	Publisher Handler	101
4.3.1	LAMP 软件包安装	85	6.2.2	PSP Handler	102
4.3.2	LAMP 软件包删除	86	6.3	让 Python 支持 MySQL	103
4.4	配置 Apache、MySQL、 PHP	86	6.3.1	Python 连接 MySQL 数据库测试	103
4.4.1	MySQL 配置	86	6.3.2	Python 的 CGI 程序	104
4.4.2	PHP 配置	88	6.3.3	CGI 排错	105
4.5	Apache、MySQL、PHP 之间的关联	89	6.4	实例：用 Django 开发 Web 应用程序	105
4.6	用 phpMyAdmin 管理 MySQL 数据库	90	6.4.1	安装 Django	105
4.6.1	phpMyAdmin 的安装	90	6.4.2	创建自己的 Django 项目	105
4.6.2	phpMyAdmin 排错	90	6.4.3	运行 Django 开发服务器	105
4.7	实例：用 Drupal 快速架设 Blog 网站	90	6.4.4	连接 MySQL 数据库	106
4.7.1	Drupal 是什么	90	6.4.5	后续开发步骤	107
4.7.2	获取 Drupal	91	6.5	实例：用 MoinMoin 实现 Wiki	107
4.7.3	为 Drupal 创建 MySQL 数据库和用户	91	6.5.1	安装 MoinMoin	108
4.7.4	为 Drupal 配置 PHP	92	6.5.2	创建 MoinMoin 实例	108
4.7.5	为 Drupal 配置 Apache	92	6.5.3	MoinMoin 权限控制	110
4.7.6	安装 Drupal	92	6.6	Python Web 应用的性能 优化	111
4.7.7	为 Drupal 安装 Blog 模块	93	6.6.1	mod-wsgi 介绍	111
4.7.8	Drupal 的中文界面	94	6.6.2	mod-wsgi 支持的程序	112
			6.6.3	mod-wsgi 的安装	112
			6.6.4	测试	113

## 第7章 Apache Tomcat 架设 ..... 114

- 7.1 安装 Tomcat ..... 114
- 7.2 配置 Tomcat ..... 115
- 7.3 Tomcat 和 Apache 的整合:
  - mod\_jk ..... 115
  - 7.3.1 mod\_jk 的安装 ..... 116
  - 7.3.2 mod\_jk 的配置 ..... 116
- 7.4 Tomcat 安全 ..... 117
  - 7.4.1 保护 shutdown 端口 ..... 117
  - 7.4.2 修改默认错误页面 ..... 118
  - 7.4.3 删除样例文件 ..... 118
  - 7.4.4 Manager WebApp 安全 ..... 118

## 第8章 最佳代理、反向代理服务器:

- Squid ..... 119
- 8.1 Squid 安装 ..... 119
- 8.2 为 Squid 配置主机名 ..... 119
- 8.3 访问控制列表 ..... 120
- 8.4 正向代理 ..... 121
  - 8.4.1 设置端口号 ..... 121
  - 8.4.2 禁止某些 IP 地址上网 ..... 121
  - 8.4.3 禁止在某时间段上网 ..... 122
  - 8.4.4 个别网站的控制 ..... 122
  - 8.4.5 用 NCSA 做密码认证 ..... 123
  - 8.4.6 透明代理的设置 ..... 123
- 8.5 反向代理 ..... 126
  - 8.5.1 Squid 反向代理单个后台 Web 服务器 ..... 127
  - 8.5.2 Squid 反向代理多个后台 Web 服务器 ..... 127
- 8.6 Squid 排错 ..... 128
  - 8.6.1 Squid 运行状态检查 ..... 128
  - 8.6.2 Squid 日志文件 ..... 128
- 8.7 使用 SquidGuard ..... 128
  - 8.7.1 SquidGuard 能做什么 ..... 129
  - 8.7.2 安装 SquidGuard ..... 131
  - 8.7.3 SquidGuard 基本配置 ..... 131
  - 8.7.4 SquidGuard 高级配置 ..... 135

## 第3篇 Mail 服务器

## 第9章 最佳邮件服务器方案 ..... 141

- 9.1 安装所有相关软件 ..... 142
  - 9.1.1 安装服务器软件 ..... 142
  - 9.1.2 安装内容过滤软件 ..... 143
  - 9.1.3 安装其他软件 ..... 143
- 9.2 为 Postfix 准备数据库 ..... 144
  - 9.2.1 创建数据库 maildb ..... 144
  - 9.2.2 为数据库 maildb 创建数据表 ..... 144
  - 9.2.3 为数据库 maildb 创建视图 ..... 147
- 9.3 配置 Postfix ..... 149
  - 9.3.1 Postfix 与 MySQL 的关联配置 ..... 149
  - 9.3.2 让 Postfix 使用 Dovecot 分发邮件 ..... 155
- 9.4 配置 Dovecot ..... 156
  - 9.4.1 配置 dovecot.conf ..... 156
  - 9.4.2 配置 dovecot-sql.conf ..... 158
  - 9.4.3 修改配置文件权限 ..... 158
  - 9.4.4 重新启动 Dovecot ..... 158
- 9.5 用 Telnet 进行 SMTP/POP3/IMAP 测试 ..... 158
  - 9.5.1 SMTP 测试 ..... 159
  - 9.5.2 测试 POP3 ..... 161
  - 9.5.3 测试 IMAP ..... 162
- 9.6 用 Thunderbird 进行 SMTP/POP3/IMAP 测试 ..... 164
  - 9.6.1 在 Thunderbird 中创建账号 ..... 164
  - 9.6.2 修改 hosts 文件 ..... 165
  - 9.6.3 在 Thunderbird 中用 POP 收取邮件 ..... 166
  - 9.6.4 在 Thunderbird 中用 SMTP 发送邮件 ..... 167

9.6.5	在 Thunderbird 中用 IMAP 收取邮件	167
9.7	实现 SMTP 认证	168
9.7.1	配置 Postfix	169
9.7.2	用 Telnet 测试 SMTP 认证	169
9.7.3	用 Thunderbird 测试 SMTP 认证	170
9.8	强迫用户使用 TLS 加密连接 SMTP	171
9.9	使用自己创建的安全证书	172
9.10	利用 Dovecot 实现 Quota (磁盘限额)	173
9.10.1	启用 quota 插件	173
9.10.2	配置 quota	174
9.11	垃圾邮件、病毒过滤	176
9.11.1	配置 SpamAssassin	176
9.11.2	配置 AMaViSd	176
9.11.3	配置 Postfix, 将邮件交给 AMaViSd 过滤	180
9.11.4	垃圾邮件测试	182
9.11.5	非法附件测试	183
9.11.6	将 Spam 自动转存到“垃圾”文件夹	183
9.12	Webmail 的实现	186
9.12.1	配置 SquirrelMail	186
9.12.2	访问 Webmail	187
9.13	修改系统别名/etc/aliases	188
9.14	Web 管理工具	189
9.14.1	安装 Virtual Mail Manager	189
9.14.2	使用 Virtual Mail Manager	190
<b>第 10 章 最佳邮件列表: Mailman</b> 191		
10.1	安装 Mailman	191
10.2	配置 Mailman	192
10.2.1	修改主机名	192

10.2.2	配置 Apache	192
10.2.3	配置 Postfix	193
10.2.4	创建默认邮件列表	194
10.3	管理 Mailman	195
10.3.1	通过 Web 管理 Mailman	196
10.3.2	通过命令行管理 Mailman	197
10.4	普通用户的 Web 界面	199

## 第 4 篇 文件服务器

<b>第 11 章 最佳 FTP 服务器方案</b> 201		
11.1	要实现的功能	201
11.2	FTP 服务器的选择	202
11.2.1	淘汰标准一: 安全	202
11.2.2	淘汰标准二: 易用性	203
11.3	Pure-FTPd 的安装、配置	203
11.3.1	安装 Pure-FTPd	203
11.3.2	配置 Pure-FTPd	203
11.4	实现 FTP 用户的 Web 管理	206
11.4.1	安装 User manager for PureFTPd	207
11.4.2	配置 User manager for PureFTPd	207
11.4.3	设置 User manager for PureFTPd 管理员	207
11.4.4	Web 管理界面	208
11.5	Pure-FTPd 配置选项介绍	209
11.5.1	逻辑型配置选项	209
11.5.2	数值型配置选项	210
11.5.3	字符串型配置选项	211
11.5.4	IP 地址型配置选项	212
11.5.5	文件型配置选项	212
11.6	实现 TLS 认证	212
11.6.1	证书设置	212
11.6.2	服务器的 TLS 设置	213
11.6.3	FTP 客户端的 TLS 设置	213
11.7	FXP 协议支持	214

11.8	允许匿名访问	214
11.8.1	Pure-FTPd 设置	214
11.8.2	添加系统用户	215
<b>第 12 章</b>	<b>最佳 NFS 服务器方案</b>	<b>216</b>
12.1	安装前须知	217
12.1.1	用户权限	217
12.1.2	组权限	217
12.2	NFS 服务器的安装及配置	217
12.2.1	/etc/hosts 配置	218
12.2.2	安装 NFS 服务器软件	218
12.2.3	Portmap 安全	218
12.2.4	NIS 服务器配置	218
12.2.5	用/etc/exports 配置 共享目录	220
12.3	NFS 客户端的安装及配置	220
12.3.1	/etc/hosts 配置	220
12.3.2	安装 NFS 客户端	221
12.3.3	配置 NFS 客户端	221
<b>第 13 章</b>	<b>与 Windows 共舞:</b>	
	<b>Samba</b>	<b>223</b>
13.1	Samba 的好处	223
13.1.1	高性能	223
13.1.2	省钱	224
13.2	安装 Samba 并测试	224
13.2.1	安装 Samba	224
13.2.2	在 Windows 客户端上 测试	224
13.3	Samba 配置	225
13.3.1	最简单的 Samba 配置	225
13.3.2	Samba 的安全认证	227
13.3.3	共享权限控制	229
13.3.4	文件写入实验	229
13.4	基本的家目录共享方案	231
13.4.1	创建私人目录	232
13.4.2	创建新用户	232
13.4.3	配置 Samba	233

13.5	其他共享方案	236
13.5.1	共享光驱	236
13.5.2	小组共享	237

## 第 5 篇 虚拟化

<b>第 14 章</b>	<b>最佳虚拟化方案:</b>	
	<b>OpenVZ</b>	<b>240</b>
14.1	OpenVZ 简介	240
14.1.1	可扩展性	240
14.1.2	密度	240
14.1.3	管理方便	241
14.2	安装 OpenVZ	241
14.2.1	安装前的准备	241
14.2.2	安装 OpenVZ	242
14.2.3	配置 OpenVZ	242
14.3	虚拟机的基本操作	244
14.3.1	虚拟机的创建	244
14.3.2	虚拟机的启停	245
14.4	vzctl 用法详解	246
14.4.1	vzctl 基本用法	246
14.4.2	创建虚拟机	246
14.4.3	虚拟机的启停等操作	247
14.4.4	设置虚拟机参数	247
14.4.5	其他命令和参数	253
14.5	/etc/vz/vz.conf 详解	253
14.5.1	全局参数	253
14.5.2	磁盘限额参数	253
14.5.3	网卡参数	254
14.5.4	虚拟机默认值	254
14.6	VE 的备份与恢复	254
14.6.1	安装 vldump	255
14.6.2	vldump 的用法	255
14.6.3	备份 VE	256
14.6.4	恢复 VE	256
14.7	OpenVZ 排错	256

## 第 6 篇 DNS 和 DHCP 服务器

第 15 章 最佳 DNS 服务器: Bind9	259
15.1 安装 Bind9	259
15.2 Bind9 的几种角色	260
15.3 配置 Bind9	260
15.3.1 Bind9 配置文件介绍	260
15.3.2 DNS 记录类型	260
15.3.3 DNS 缓存服务器的配置	261
15.3.4 主 DNS 服务器的配置	262
15.3.5 从 DNS 服务器的配置	266
15.4 让 Bind9 运行在 Chroot 环境	268
15.4.1 创建 Chroot 环境	268
15.4.2 Bind9 配置	269
15.4.3 日志路径设置	269
15.4.4 测试	269
15.5 Bind9 排错	269
15.5.1 DNS 测试	269
15.5.2 日志文件	271
第 16 章 DNS 轮询	273
16.1 为什么要用 DNS 轮询	273
16.2 DNS 轮询是怎么工作的	273
16.3 DNS 轮询的实现方法	273
16.3.1 多个 CNAMEs 的方法 (Bind4、Bind8)	273
16.3.2 多个 A 记录的方法 (Bind9)	274
16.4 DNS 轮询的测试	274
16.5 DNS 轮询的缺陷	275
第 17 章 最佳 DHCP 服务器方案	276
17.1 DHCP 的好处	276
17.2 DHCP 提供信息的方法	277
17.3 安装 DHCP 服务器软件	277
17.4 配置 DHCP 服务器	278

17.4.1 网络环境介绍	278
17.4.2 DHCP 配置	278
17.4.3 测试	279
17.5 DHCP 排错	280

## 第 7 篇 负载均衡和集群

第 18 章 负载均衡、高可用的 Web 集群	282
18.1 介绍	282
18.1.1 HAProxy 介绍	282
18.1.2 Keepalived 介绍	282
18.1.3 HAProxy+Keepalived 的 好处	283
18.2 架构	283
18.2.1 架构详情	283
18.2.2 架构图	284
18.3 架构的实现	284
18.3.1 Web 服务器的安装及 配置	284
18.3.2 HAProxy 的安装及配置	285
18.3.3 Keepalived 的安装及 配置	287
18.4 测试	289
18.4.1 Web 节点故障模拟	289
18.4.2 负载均衡节点故障模拟	289
18.5 HAProxy 的 Web 统计页面	290
第 19 章 负载均衡、高可用的 MySQL 集群	291
19.1 MySQL 集群架构介绍	291
19.1.1 架构图	291
19.1.2 本例中的服务器	292
19.2 管理节点 (MGM) 的 安装及配置	292
19.2.1 安装 MySQL	293
19.2.2 配置 ndb_mgmd.cnf	293
19.3 存储节点 (NDB) 的安装 及配置	294

19.3.1	安装 MySQL	294
19.3.2	配置 my.cnf	294
19.4	阶段测试	295
19.4.1	集群连接状态测试	295
19.4.2	测试	296
19.5	实现负载均衡	300
19.5.1	ldirectord+heartbeat 介绍	300
19.5.2	让内核支持 IPVS	301
19.5.3	安装 heartbeat、ldirectord 等软件	302
19.5.4	配置 heartbeat	302
19.5.5	配置 ldirectord	303
19.5.6	NDB 节点配置	304
19.5.7	测试	305
19.6	注意事项	307
19.6.1	数据库引擎问题	307
19.6.2	内存问题	308
19.6.3	安全问题	308

## 第 8 篇 远程控制与监控

### 第 20 章 最佳远程控制方案: SSH 310

20.1	关于公钥认证	310
20.1.1	为什么要用公钥认证	310
20.1.2	公钥认证是怎么工作的	311
20.2	SSH 的安装	311
20.2.1	安装 SSH 服务器和 客户端	311
20.2.2	测试	311
20.3	SSH 配置	312
20.3.1	生成密钥对	312
20.3.2	将公钥复制到服务器	312
20.3.3	SSH 登录测试	312
20.3.4	SSH 服务器配置	314
20.4	SSH 小技巧	315
20.4.1	用 scp 远程复制文件	315
20.4.2	在客户端上指定命令	316
20.4.3	在服务器上限制所 执行的命令	316

20.4.4	修改密钥口令	317
20.4.5	将密钥放入内存	317

### 第 21 章 最佳服务器监控方案:

#### Nagios 318

21.1	Nagios 介绍	318
21.2	安装 Nagios	319
21.3	配置 Nagios	319
21.3.1	Nagios 初始化设置	319
21.3.2	Nagios 监控设置	320
21.4	手机短信提醒	327
21.5	Nagios 排错	328

## 第 9 篇 数据备份与系统安全

### 第 22 章 最佳 RAID 方案: RAID10 330

22.1	RAID 方案的选择	330
22.2	RAID10 的实现	332
22.2.1	手动分区	333
22.2.2	第一块硬盘分区	334
22.2.3	分区复制	338
22.2.4	创建 RAID 阵列	339
22.2.5	在 RAID 上创建分区	340
22.2.6	保存分区	342
22.3	RAID10 的日常维护	343
22.3.1	mdadm 的主要工作模式	343
22.3.2	mdadm 的选项	343
22.3.3	创建 RAID 阵列	345
22.3.4	查询 RAID 阵列	345
22.3.5	RAID 的监控	346
22.3.6	RAID 的启动/停止	346
22.4	故障处理	347
22.4.1	从 RAID 中移除设备	347
22.4.2	添加已有 RAID 物理卷	348
22.4.3	更换全新硬盘	348
22.5	添加备用硬盘	350
22.5.1	插入新硬盘	351

22.5.2	新硬盘分区	351	24.3	用户、密码管理	372
22.5.3	将新分区加入 RAID	351	24.3.1	关于 root 用户	372
22.5.4	设置 grub	352	24.3.2	关于 sudo	373
22.5.5	故障模拟	352	24.3.3	关于/etc/sudoers	373
22.6	RAID10 的空间扩展	352	24.3.4	密码策略	375
<b>第 23 章</b>	<b>最佳数据安全方案:</b>		24.4	ufw 防火墙	376
	RAID10+LVM	354	24.4.1	启用、禁用 ufw	376
23.1	创建 RAID 物理卷	354	24.4.2	基本规则设置	377
23.1.1	将第一块硬盘分区	354	24.4.3	常用规则设置	378
23.1.2	剩余硬盘的分区处理	355	24.4.4	高级规则设置	380
23.2	创建 RAID 阵列	355	24.4.5	IP 伪装	382
23.2.1	创建 RAID1 阵列	355	24.5	入侵检测	384
23.2.2	创建 RAID10 阵列	356	24.5.1	安装 LAMP	384
23.3	LVM 的创建和配置	356	24.5.2	安装、配置 Snort	384
23.3.1	创建 LVM 物理卷	356	24.5.3	安装、配置 BASE	387
23.3.2	LVM 配置	356	24.6	肉鸡检测	392
23.4	创建/boot 分区	358	24.6.1	chkrootkit 的使用	393
23.5	LVM 的相关命令	359	24.6.2	rkhunter 的使用	394
23.5.1	LVM 物理卷相关命令	359	24.6.3	unhide 的使用	396
23.5.2	LVM 卷组相关命令	360	24.7	数据完整性检测	397
23.5.3	LVM 逻辑卷相关命令	363	24.7.1	安装 Tripwire	398
23.6	添加新硬盘	365	24.7.2	配置 Tripwire	400
23.6.1	插入新硬盘	365	24.7.3	初始化 Tripwire 数据库	403
23.6.2	配置 RAID	365	24.7.4	执行完整性检测	403
23.6.3	在 RAID 上配置 LVM	367	24.7.5	检测报告分析	403
23.6.4	扩容文件系统	368	24.7.6	查看 Tripwire 数据库 内容	405
23.7	更换硬盘	368	24.7.7	使用 Tripwire 的注意 事项	406
23.8	LVM 分区备份	368	24.8	被入侵后的系统恢复	406
23.8.1	创建快照	369	24.8.1	保持冷静	407
23.8.2	备份快照内容	369	24.8.2	断开网络	407
23.8.3	删除快照	370	24.8.3	找到黑客入侵的方法	407
<b>第 24 章</b>	<b>Ubuntu Server 系统安全</b>	371	24.8.4	黑客文件清理	412
24.1	系统安全更新	371	24.8.5	恢复未受影响的服务	412
24.1.1	订阅安全列表	371	24.8.6	修复问题	412
24.1.2	自动更新	371	24.8.7	恢复受影响的服务	412
24.2	控制台安全	372	24.8.8	监控系统	412

PART

# 1

## 第 1 篇 拥抱 Ubuntu Server

本篇我们将对 Linux 进行介绍，然后介绍 Ubuntu Server。

也许你已经对 Linux 和 Ubuntu 很熟悉了，对它们的“介绍”不屑一顾；但是 Hiweed（本书作者）还是建议你仔细阅读一下。

希望你能找到别的书里找不到的内容。





# 第 1 章

## 敲开 Linux Server 的大门

这个年头再一五一十、如数家珍地介绍 Linux，好像有点瞧不起人——你可能会说：Hiweed 啊，不用再介绍了，我早就知道 Linux 了，你当我是火星来的啊？——且慢，客官，先听我讲个故事，再听我慢慢道来。

### 1.1 Linux 到底是什么

我当然相信，现在的 IT 系统管理员没有几个没听说过 Linux，就好像现在没有几个搞 IT 的人不知道比尔·盖茨一样；而且很多人已经在自己的电脑上（或者在虚拟机里）安装、使用过 Linux；更有些人干脆干掉了电脑上的 Windows 操作系统，每天只使用 Linux 完成各项任务，成为了 Linux 的忠实用户和宣传者。不过，我能断定，这些人当中，敢说自己有信心去做一个中小企业的 Linux 管理员的，为数不多。

2007 年 6 月，我的一个朋友从美国 Google 总部离职回国，创建了一家电子商务公司。因为一时请不到好的 Linux 系统管理员，朋友把我叫到上海，帮他做一些前期的系统架构相关的事情。这个事情做完后，朋友让我帮他招聘两名 Linux 系统管理员。结果我花了大半年的时间，只找到了一位。我到网上搜索简历，去招聘网站发布信息，通过电话和分布在祖国大江南北的应聘者沟通；有的只聊了一两分钟就无法继续了，有的聊了长达 1 小时并最终约到公司面谈，但可惜的是，最终也无法通过面试。

在这里，Hiweed 想说的是，Linux 不是你想象的那样。

你必须重新认识 Linux，才能找到自己的学习目标，只有这样，你才能成长。

狭义地说，Linux 根本算不上操作系统，它只是一个内核（Kernel）而已。广义地说，Linux 其实是一个包含了各种应用程序和服务的有机体。当然这个广义的说法，把众多的 GNU 软件以及各种各样的第三方软件和服务，全都用 Linux 这个字眼来代替了。

我们平常所说的 Linux，既不是狭义的，也不是广义的；一般只是指 Linux 桌面，或者 Linux 服务器。

但是，要想成为企业级的 Linux 系统管理员，你必须对这个“广义”的 Linux 有机体非常熟悉，对各种桌面和服务程序了如指掌，能够针对不同企业（政府、学校、银行等）的需求制定合理的 Linux 系统架构。

仅能够熟练安装各种 Linux 发行版的桌面和服务系统，不足以让你成为一个合格的