

Ubuntu Server 最佳方案

第2版

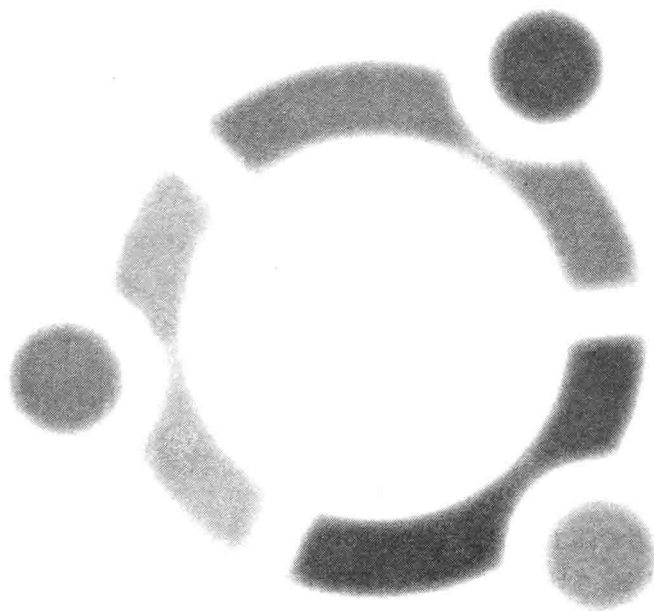
冷罡华 (Hiweed) 编著



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

Ubuntu Server 最佳方案 (第2版)

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

本书是作者 15 年实战经验的结晶, 无论您是初学者还是 Linux 高手, 都能从中获益。2009 年第 1 版出版后, 很快脱销, 一书难求。此次推出的第 2 版, 是基于 Ubuntu 14.04 LTS 的, 给您最新的技术指导。

在内容上, 本书涉猎到了 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 到云计算基础(虚拟化、集群), 再到远程控制, 再到 RAID 和 LVM, 最后到系统安全。不管您是在校学生还是在职 Linux 管理员, 无论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 15 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. —2 版. —北京: 电子工业出版社, 2014.9
ISBN 978-7-121-24115-4

I. ①U… II. ①冷… III. ①Linux 操作系统 IV. ①TP316.89

中国版本图书馆 CIP 数据核字(2014)第 188932 号

策划编辑: 李 冰

责任编辑: 徐津平

印 刷: 涿州市京南印刷厂

装 订: 涿州市京南印刷厂

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: 787×1 092 1/16 印张: 32.25 字数: 778 千字

版 次: 2009 年 6 月第 1 版

2014 年 9 月第 2 版

印 次: 2014 年 9 月第 1 次印刷

定 价: 65.00 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 zlts@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

“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, 早在 2008 年, 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, 但是笔者相信, 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, 正在如饥似渴地募求 Linux 人才, 却常常慨叹一才难求!

笔者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。

本书特色

有的时候, 没有选择权会很令人烦恼。可是, 如果选择太多, 人们往往会无所适从。您拨打家电服务电话时, 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过去……

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, 在太多的选择面前, 大多数人都会很茫然, 反复比较, 仍然举棋不定, 不知所措。

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, 那到底是要用 ProFTPd, 还是用 PureFTPd 呢? 是用 WU-FTPd, 还是用 VsFTPd 呢? 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，还是用软件 RAID 呢？是用 RAID0，还是用 RAID1 呢？是用 RAID5，还是用 RAID10 呢？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 18 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，笔者向读者郑重推荐了 LFS——学习 Linux 的“终南捷径”；笔者以 15 年的经验告诉您，亲爱的读者，要想以最快的速度理解 Linux 操作系统的结构、原理，非 LFS 莫属。当您掌握了 LFS 之后，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，笔者一定会做说明。

本书中的所有方案，包括步骤和配置文件，全部经过笔者本人（Hiweed）亲自实验通过。但是，笔者不敢保证每个人按照同样的步骤都能做成功。就像 Debian GNU/Linux，多年来一直标注说“完全没有担保”，道理是一样的。但是，最起码，这套方法、这套思路是值得参考的。

考虑到很多读者可能没有单独的电脑来做实验，所以本书的大部分章节都是在 VirtualBox 中实现的（虚拟化、集群章节除外）。这是个免费软件，读者可以从网上下载到。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 14.04 LTS 的光盘镜像，在下面的地址可以下载：

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

请不要在其他版本的 Ubuntu 上使用本书。由于软件版本不同，那样会遇到意想不到的问题，增加学习烦恼。

本书重点内容

本书分为 10 篇，共 26 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 认识 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 分别进行了详细介绍。此外，由于代理服务器也属于 Web 范畴，因此本篇中我们还介绍了最佳代理服务器方案（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 云存储的鼻祖: NFS 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 DNS 和 DHCP 服务器	第 14 章 最佳 DNS 服务器: Bind9 第 15 章 DNS 轮询 第 16 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 6 篇 云计算基础一: 虚拟化	第 17 章 最佳虚拟环境: KVM 第 18 章 最佳容器: LXC	介绍了云计算的基础——最佳虚拟化方案 (KVM、LXC)。其中, KVM 可以让我们虚拟 Linux、Windows 等各种操作系统, 而 LXC 可以在一台物理服务器上虚拟上百台 Linux 服务器
第 7 篇 云计算基础二: 高可用与负载均衡	第 19 章 负载均衡、高可用的 Web 集群 第 20 章 负载均衡、高可用的 MariaDB 数据库集群	介绍了负载均衡、高可用的最佳 Web 集群方案 (具备文件双向同步功能)。最佳 MariaDB (MySQL) 数据库集群方案 (可以多主复制, 可以增量备份)。两个章节中, 我们都采用了 Keepalived+HAProxy 的方案
第 8 篇 远程控制与监控	第 21 章 最佳远程控制方案: SSH 第 22 章 最佳监控方案: Nagios	介绍了最佳远程控制方案 (SSH) 和最佳监控方案 (Nagios)。我们的方案可以隐藏 SSH 服务, 让黑客扫描不到 22 端口。Nagios 监控可以让我们及时了解服务器状况, 免得总是“救火”
第 9 篇 数据安全	第 23 章 最佳 RAID 方案: RAID10 第 24 章 最佳数据安全方案: RAID10+LVM	介绍了最佳 RAID 方案 (RAID10)、最佳数据安全方案 (RAID10+LVM)
第 10 篇 系统安全	第 25 章 Ubuntu 系统安全 第 26 章 入侵检测与系统恢复	介绍了如何使 Ubuntu Server 变得更安全。安全是重中之重, 我们不仅可以自己设置防火墙, 还可以使用 psad 做入侵检测 (自动拦截)。我们还介绍了肉鸡检测的方法, 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, 但是笔者相信, 书中肯定有不妥之处, 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, 请发送 E-mail 到 ubuntu-server@qq.com, 谢谢!

第 2 版变更

在写作第 2 版时, 有些技术已经过时了, 或者有新的技术更值得采用, 所以, 相对第

1 版，变化还是不小的。

- 版式：为了阅读和使用方便，去掉了所有命令前的“\$”提示符；
- 实验平台：由 VMware Server 转到 Oracle VM VirtualBox；
- 数据库：由 MySQL 改为 MariaDB；
- PHP 建站：用 WordPress 换掉 Drupal；
- 邮件系统：添加防僵尸网络的内容，并用 RoundCube 换掉 SquirrelMail；
- 添加云计算基础章节；
- 添加 KVM 虚拟化章节；
- 用 LXC 换掉 OpenVZ；
- Web 集群：增加 unison 双向文件同步；
- 数据库集群：改用 MariaDB Galera，真正的多主复制；并添加增量备份功能；
- SSH 服务器：增加“端口敲门”安全功能；
- Nagios 监控：增加 NRPE 远程监控功能（包括 MariaDB 监控功能）；
- RAID：修复第 1 版的图示错误；
- 系统安全：增加 iptables 防火墙介绍、AppArmor 介绍；
- 入侵检测：用 psad 换掉 snort，实现自动拦截。

致谢

本书第 2 版能够出版，大家要感谢一个人。

他，就是安徽省宣城市敬亭山弘愿寺的住持，阿弥陀佛的使者——净宗法师。如没有净宗法师的劝说，笔者就不会写这个第 2 版。

自从本书第 1 版于 2009 年面世之后，笔者觉得写书实在是太累了，对身体的消耗非常非常大，所以一直不愿投入精力写第 2 版。心想，有那个时间，还不如多念几句“南无阿弥陀佛”呢。

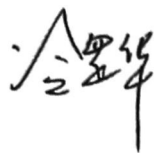
2013 年夏天，笔者在拜会净宗法师时，偶然间提起此事。法师说：

应该要写，因为可以帮到别人。

法师一句话，一锤定音。只要可以帮到别人，就要写。只考虑自己，活着又有什么价值？

所以，请大家和笔者一起，感恩净宗法师，是他直接促成了这本书的写作。

此外，还要感谢电子工业出版社的李冰老师，以及本书编辑、校对、排版、设计、印刷等各个环节的工作人员，没有大家的帮助，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	5
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	7
1.3.1 兴趣、试验	7
1.3.2 真正的捷径——LFS	7
1.4 选择哪个 Linux 发行版	8
1.4.1 关于 Arch 和 Gentoo	9
1.4.2 关于 Red Hat、CentOS 和 Fedora	9
1.4.3 Debian 不错	10
1.4.4 推荐使用 Ubuntu Server	11
1.5 应该买什么样的服务器	12
1.5.1 架构设计	12
1.5.2 服务器的选型	12
1.5.3 机房的选择	13
第 2 章 认识 Ubuntu Server	14
2.1 Ubuntu 的前世今生	14
2.2 安装 Ubuntu Server	15
2.2.1 安装前的准备	15
2.2.2 安装 Ubuntu Server	15

2.2.3 把语言环境变量改为英文	31
2.2.4 安全补丁、版本升级	33
2.2.5 安装 SSH	33
2.2.6 sudo 免密码	33
2.3 Ubuntu 快速入门指南	34
2.3.1 nano 编辑器	34
2.3.2 强大的“资源管理器”： mc	35
2.3.3 快速查找文件	36
2.3.4 软件包管理	36
2.3.5 使用 apt 工具	38
2.3.6 写给 CentOS 用户	47
2.3.7 Ubuntu 网络配置	50
2.3.8 远程管理 Ubuntu Server	54
2.3.9 手工更新系统：apt-get update && apt-get upgrade	55
2.3.10 让系统自动更新	56

第 2 篇 LAMP 服务器

第 3 章 用 Apache 做 Web 服务器	58
3.1 Apache 简介	59
3.2 Apache 的安装、配置	59
3.2.1 Apache 的安装	59
3.2.2 Apache 的配置	60
3.2.3 Apache 虚拟主机	63
3.3 Apache 性能优化	73
3.3.1 选择正确的 MPM 模块	73
3.3.2 优化 Apache 配置	74
3.3.3 使用反向代理	80
3.4 Apache 压力测试 (ab)	80
3.5 Apache 安全	82
3.5.1 安全更新	82

3.5.2	隐藏敏感信息	83	4.7.5	为 WordPress 配置 Apache	112
3.5.3	不要以 root 身份运行 Apache	84	4.7.6	安装 WordPress	113
3.5.4	密码认证	85	第 5 章	LAMP 服务器之 Perl 篇	114
3.5.5	检查文件权限	87	5.1	安装 Perl 模块	114
3.5.6	关闭不用的模块	88	5.2	配置 cgi-bin 目录	114
3.5.7	DDoS 攻击防范	88	5.3	Perl 程序测试	115
3.6	Apache 日志分析	91	5.4	用 Perl 访问 MariaDB 数据库	115
3.6.1	用 Webalizer 分析 Apache 日志	91	5.5	CGI 排错	117
3.6.2	用 AWStats 分析 Apache 日志	93	5.6	实例：用 TWiki 架设 Wiki	118
3.6.3	Apache 日志合并	97	5.6.1	安装 TWiki	118
第 4 章	LAMP 服务器之 PHP 篇	99	5.6.2	配置 TWiki	123
4.1	MariaDB、MySQL 简介	99	第 6 章	LAMP 服务器之 Python 篇	125
4.2	PHP 简介	101	6.1	安装 mod_python	125
4.3	安装 LAMP 相关软件包	102	6.2	配置 Apache	125
4.3.1	LAMP 软件包安装	102	6.2.1	PSP Handler	125
4.3.2	LAMP 软件包卸载	103	6.2.2	Publisher Handler	126
4.4	配置 Apache、MySQL、 PHP	104	6.3	让 Python 支持 MySQL/ MariaDB	127
4.4.1	MariaDB 配置	104	6.3.1	Python 连接 MariaDB 数据库测试	127
4.4.2	PHP 配置	106	6.3.2	Python 的 CGI 程序	128
4.5	Apache、MariaDB、PHP 之间的关联	107	6.3.3	CGI 排错	129
4.6	用 phpMyAdmin 管理 MariaDB 数据库	108	6.4	实例：用 Django 开发 Web 应用程序	130
4.6.1	phpMyAdmin 的安装	108	6.4.1	安装 Django	130
4.6.2	phpMyAdmin 排错	109	6.4.2	创建自己的 Django 项目	130
4.7	实例：用 WordPress 快速架设 Blog 网站	110	6.4.3	运行 Django 开发 服务器	130
4.7.1	WordPress 是什么	110	6.4.4	连接 MariaDB 数据库	131
4.7.2	获取 WordPress	110	6.4.5	后续开发步骤	133
4.7.3	为 WordPress 创建 MariaDB 数据库 和用户	111	6.5	实例：用 MoinMoin 实现 Wiki	133
4.7.4	为 WordPress 配置 PHP	112	6.5.1	安装 MoinMoin	134
			6.5.2	创建 MoinMoin 实例	134

6.5.3	MoinMoin 权限控制	136
6.6	Python Web 应用的性能优化	137
6.6.1	mod-wsgi 介绍	137
6.6.2	mod-wsgi 支持的程序	139
6.6.3	mod-wsgi 的安装	139
6.6.4	测试	139
第 7 章	Apache Tomcat 架设	140
7.1	安装 Tomcat	140
7.1.1	安装 Tomcat 等软件	140
7.1.2	编程测试	141
7.2	配置 Tomcat	141
7.3	Tomcat 和 Apache 的整合: mod_jk	142
7.3.1	mod_jk 的安装	143
7.3.2	mod_jk 的配置	143
7.3.3	安装 Tomcat 示例	144
7.3.4	阅读 Tomcat 文档	145
7.4	Tomcat 安全	145
7.4.1	保护 shutdown 端口	145
7.4.2	修改默认错误页面	145
7.4.3	删除样例文件	146
7.4.4	Manager WebApp 安全	146
第 8 章	最佳代理服务器: Squid	147
8.1	Squid 安装	147
8.2	为 Squid 配置主机名	147
8.3	访问控制列表	148
8.4	正向代理	149
8.4.1	设置端口号	150
8.4.2	禁止某些 IP 地址上网	150
8.4.3	禁止在某时间段上网	150
8.4.4	个别网站的控制	151
8.4.5	用 NCSA 做密码认证	152
8.4.6	透明代理的设置	153
8.5	Squid 排错	157
8.5.1	Squid 运行状态检查	157
8.5.2	Squid 日志文件	157

8.6	用 SquidGuard 过滤网站	157
8.6.1	SquidGuard 能做什么	157
8.6.2	安装 SquidGuard	159
8.6.3	SquidGuard 基本配置	160
8.6.4	SquidGuard 高级配置	165

第 3 篇 Mail 服务器

第 9 章	最佳邮件服务器方案	170
9.1	安装所有相关软件	171
9.1.1	安装服务器软件	172
9.1.2	安装内容过滤软件	173
9.1.3	安装其他软件	173
9.2	为 Postfix 准备数据库	174
9.2.1	创建数据库 maildb	174
9.2.2	为数据库 maildb 创建 数据表	174
9.3	配置 Postfix	177
9.3.1	Postfix 与 MariaDB 的 关联配置	177
9.3.2	让 Postfix 使用 Dovecot 分发邮件	181
9.4	配置 Dovecot	181
9.4.1	配置 Dovecot	181
9.4.2	连接数据库	183
9.4.3	修改配置文件权限	184
9.4.4	重新启动 Dovecot	184
9.5	用 Telnet 进行 SMTP/POP3/ IMAP 测试	184
9.5.1	SMTP 测试	185
9.5.2	测试 POP3	187
9.5.3	测试 IMAP	189
9.6	用 Thunderbird 进行 SMTP/ POP3/IMAP 测试	191
9.6.1	修改 hosts 文件	191
9.6.2	在 Thunderbird 中 创建账号	191

9.6.3	在 Thunderbird 中 收取邮件	192
9.6.4	在 Thunderbird 中 发送邮件	192
9.7	实现 SMTP 认证	194
9.7.1	生成安全证书	194
9.7.2	配置 Postfix	194
9.7.3	用 Telnet 测试 SMTP 认证	195
9.7.4	用 OpenSSL 测试 SMTP 认证	196
9.7.5	用 Thunderbird 测试 SMTP 认证	197
9.8	让用户统一使用 TLS	197
9.9	用 Dovecot 实现 quota (磁盘限额)	197
9.9.1	启用 quota 插件	197
9.9.2	设置 quota 大小	198
9.10	垃圾邮件、病毒过滤	199
9.10.1	配置 SpamAssassin	199
9.10.2	配置 AMaViSd	200
9.10.3	配置 Postfix, 将邮件 交给 AMaViSd 过滤	204
9.10.4	垃圾邮件测试	206
9.10.5	非法附件测试	206
9.11	Postfix 的反垃圾邮件 设置	207
9.11.1	客户端限制	207
9.11.2	helo 指令限制	209
9.11.3	发件人限制	209
9.11.4	收件人限制	210
9.11.5	邮件内容限制	210
9.11.6	防僵尸网络	210
9.12	防止被当成垃圾邮件	212
9.12.1	用 DKIM 做域名标识	212
9.12.2	为 DNS 添加 SPF 记录	215
9.13	Webmail 的实现	216
9.13.1	安装 RoundCube	216

9.13.2	让 Apache 支持 RoundCube	217
9.13.3	配置 RoundCube	217
9.13.4	访问 Webmail	218
9.14	修改系统别名/etc/aliases	218
第 10 章	最佳邮件列表: Mailman	220
10.1	安装 Mailman	220
10.2	配置 Mailman	221
10.2.1	修改 hosts 文件	221
10.2.2	配置 Apache	222
10.2.3	配置 Postfix	223
10.2.4	配置 Mailman	224
10.2.5	创建默认邮件列表	224
10.3	管理 Mailman	225
10.3.1	通过 Web 管理 Mailman	225
10.3.2	通过命令行管理 Mailman	226
10.4	普通用户的 Web 界面	229

第 4 篇 文件服务器

第 11 章	最佳 FTP 服务器方案	232
11.1	要实现的功能	232
11.2	FTP 服务器的选择	233
11.2.1	淘汰标准一: 安全	233
11.2.2	淘汰标准二: 易用性	234
11.3	Pure-FTPd 的安装、配置	234
11.3.1	安装 Pure-FTPd	234
11.3.2	配置 Pure-FTPd	234
11.4	实现 FTP 用户的 Web 管理	237
11.4.1	安装 User manager for PureFTPd	238
11.4.2	配置 User manager for PureFTPd	238
11.4.3	设置 User manager for PureFTPd 管理员	239

11.4.4	Web 管理界面	239
11.5	Pure-FTPd 配置选项介绍	240
11.5.1	逻辑型配置选项	241
11.5.2	数值型配置选项	242
11.5.3	字符串型配置选项	243
11.5.4	IP 地址型配置选项	243
11.5.5	文件型配置选项	243
11.6	实现 TLS 认证	244
11.6.1	证书设置	244
11.6.2	服务器的 TLS 设置	244
11.6.3	FTP 客户端的 TLS 设置	244
11.7	FXP 协议支持	245
11.8	允许匿名访问	246
11.8.1	Pure-FTPd 设置	246
11.8.2	添加系统用户	246
第 12 章	云存储的鼻祖：NFS	247
12.1	安装前须知	248
12.1.1	用户权限	248
12.1.2	组权限	248
12.2	NFS 服务器的安装及配置	248
12.2.1	/etc/hosts 配置	249
12.2.2	安装 NFS 服务器软件	249
12.2.3	RpcBind 安全	249
12.2.4	NIS 服务器配置	250
12.2.5	NFS 服务器配置	252
12.3	NFS 客户端的安装及配置	253
12.3.1	/etc/hosts 配置	253
12.3.2	安装 NFS 客户端	254
12.3.3	配置 NFS 客户端	254
第 13 章	与 Windows 共舞：Samba	256
13.1	Samba 的好处	256
13.1.1	高性能	256
13.1.2	省钱	257

13.2	安装 Samba 并测试	257
13.2.1	安装 Samba	257
13.2.2	在 Windows 客户端上测试	257
13.3	Samba 配置	258
13.3.1	最简单的 Samba 配置	258
13.3.2	Samba 的安全认证	260
13.3.3	共享权限控制	261
13.3.4	文件的写入	261
13.4	基本的家目录共享方案	263
13.4.1	创建私人目录	263
13.4.2	创建新用户	264
13.4.3	配置 Samba	265
13.5	其他共享方案	268
13.5.1	共享光驱	268
13.5.2	小组共享	269

第 5 篇 DNS 和 DHCP 服务器

第 14 章	最佳 DNS 服务器：Bind9	272
14.1	安装 Bind9	272
14.2	Bind9 的几种角色	273
14.3	配置 Bind9	273
14.3.1	Bind9 配置文件介绍	273
14.3.2	DNS 记录类型	273
14.3.3	DNS 缓存服务器的配置	274
14.3.4	主 DNS 服务器的配置	276
14.3.5	从 DNS 服务器的配置	279
14.4	Bind9 安全	282
14.5	Bind9 排错	282
14.5.1	DNS 测试	282
14.5.2	日志文件	284
第 15 章	DNS 轮询	285
15.1	为什么要用 DNS 轮询	285

15.2	DNS 轮询是怎样工作的	285
15.3	DNS 轮询的实现方法	285
15.3.1	多个 CNAMEs 的方法 (Bind4、Bind8) ...	285
15.3.2	多个 A 记录的方法 (Bind9)	286
15.4	DNS 轮询的测试	286
15.5	DNS 轮询的缺陷	287
第 16 章	最佳 DHCP 服务器方案	288
16.1	DHCP 的好处	288
16.2	DHCP 提供信息的方法	289
16.3	安装 DHCP 服务器软件	289
16.4	配置 DHCP 服务器	289
16.4.1	网络环境介绍	289
16.4.2	DHCP 配置	290
16.4.3	测试	291
16.5	DHCP 排错	292

第 6 篇 云计算基础一： 虚拟化

第 17 章	最佳虚拟环境：KVM	294
17.1	KVM 简介	294
17.2	Libvirt 简介	295
17.3	检查 CPU 是否支持虚拟化	295
17.4	安装软件包	296
17.4.1	安装服务端软件包	296
17.4.2	安装用户端软件包	296
17.5	创建虚拟机	296
17.5.1	准备虚拟网卡	296
17.5.2	创建虚拟机	298
17.6	管理虚拟机	299
17.6.1	启动虚拟机	299
17.6.2	重启、关机	300

17.6.3	保存、恢复状态	300
17.6.4	挂起、恢复	300
17.6.5	空间扩容	301
17.6.6	增加 CPU 个数	302
17.6.7	升级内存	304
17.7	克隆虚拟机	305
17.8	虚拟机镜像管理	307
17.9	迁移虚拟机	308
17.9.1	用 NFS 共享存储	308
17.9.2	让目标服务器监听网络	309
17.9.3	迁移虚拟机	310
17.10	删除虚拟机	311
第 18 章	最佳虚拟容器：LXC	312
18.1	LXC 简介	312
18.2	安装 LXC	313
18.3	基本用法	313
18.3.1	特权模式基本用法	313
18.3.2	非特权模式基本用法	319
18.3.3	全局配置文件	321
18.4	克隆 LXC 容器	321
18.4.1	拷贝和快照	321
18.4.2	创建拷贝和快照	322
18.4.3	快照命令	323
18.4.4	临时快照	324
18.5	LXC 的网络	324
18.5.1	使用固定 IP	324
18.5.2	让外界可以访问容器	325
18.6	LXC 的后台	326
18.6.1	后台服务	326
18.6.2	后台存储	327
18.7	容器安全	327
18.7.1	Linux 功能过滤	327
18.7.2	内存限制	328
18.7.3	apparmor	328
18.7.4	SELinux	329
18.7.5	Seccomp	329

第 7 篇 云计算基础二：
高可用与负载均衡

第 19 章 负载均衡、高可用的
Web 集群..... 332

19.1 介绍..... 332

19.1.1 HAProxy 介绍..... 332

19.1.2 Keepalived 介绍..... 333

19.1.3 HAProxy+Keepalived
的好处..... 333

19.2 架构..... 333

19.2.1 架构详情..... 334

19.2.2 架构图..... 334

19.3 架构的实现..... 335

19.3.1 Web 服务器的安装
及配置..... 335

19.3.2 Keepalived 的安装
及配置..... 336

19.3.3 HAProxy 的安装
及配置..... 340

19.4 测试..... 341

19.4.1 Web 节点故障模拟..... 341

19.4.2 负载均衡节点故障模拟..... 342

19.5 HAProxy 的 Web 统计
页面..... 342

19.6 文件的同步..... 343

19.6.1 安装 unison..... 343

19.6.2 创建密钥..... 344

19.6.3 手工同步..... 345

19.6.4 自动同步..... 347

19.6.5 多台主机的同步..... 348

第 20 章 负载均衡、高可用的
MariaDB 数据库集群..... 351

20.1 MariaDB Galera 集群介绍..... 351

20.1.1 关于 Galera 复制..... 352

20.1.2 MariaDB Galera 集群
的特点..... 353

20.1.3 本例中的服务器.....354

20.2 创建高可用集群.....354

20.2.1 安装 MariaDB Galera
软件包.....354

20.2.2 设置 Galera.....355

20.2.3 启动 Galera 集群.....356

20.2.4 写入测试.....357

20.2.5 故障模拟.....358

20.3 负载均衡.....359

20.3.1 创建 MariaDB 用户.....360

20.3.2 安装数据库客户端.....361

20.3.3 安装配置 Keepalived.....361

20.3.4 安装配置 HAProxy.....362

20.4 数据备份与恢复.....363

20.4.1 安装 xtrabackup.....363

20.4.2 xtrabackup 配置.....364

20.4.3 全备份.....365

20.4.4 增量备份.....365

20.4.5 恢复.....368

20.4.6 自动备份.....369

第 8 篇 远程控制与监控

第 21 章 最佳远程控制方案：SSH.....374

21.1 关于公钥认证.....374

21.1.1 为什么要用公钥认证.....374

21.1.2 公钥认证是怎么
工作的.....375

21.2 SSH 的安装.....375

21.2.1 安装 SSH 服务器和
客户端.....375

21.2.2 测试.....375

21.3 SSH 配置.....376

21.3.1 生成密钥对.....376

21.3.2 将公钥复制到服务器.....376

21.3.3 SSH 登录测试.....377

21.3.4 SSH 服务器配置.....379

21.4	用端口敲门隐藏 SSH 服务	379
21.4.1	端口敲门的工作原理	380
21.4.2	准备防火墙	380
21.4.3	安装 knockd	380
21.4.4	配置 knockd	380
21.4.5	测试敲门服务	381
21.5	SSH 小技巧	382
21.5.1	用 scp 远程复制文件	382
21.5.2	用 sftp 远程传输文件	383
21.5.3	在客户端上指定命令	383
21.5.4	在服务器上限制所执行的命令	384
21.5.5	修改密钥口令	384
21.5.6	将密钥放入内存	385

第 22 章 最佳监控方案: Nagios 386

22.1	Nagios 介绍	386
22.2	安装 Nagios	387
22.3	Nagios 的一般配置	387
22.3.1	Nagios 初始化设置	387
22.3.2	Nagios 监控设置	388
22.4	用 NRPE 进行远程监控	397
22.4.1	设置被监控的主机	397
22.4.2	设置 Nagios 服务器	398
22.5	MariaDB 数据库监控	399
22.5.1	添加主机	399
22.5.2	创建主机组	399
22.5.3	设置对数据库组的监控	400
22.5.4	创建数据库用户	400
22.5.5	重启 Nagios 服务	400
22.6	手机短信提醒	401
22.7	Nagios 排错	401

第 9 篇 数据安全

第 23 章 最佳 RAID 方案:

RAID10	404
--------------	-----

23.1	RAID 方案的选择	404
------	------------------	-----

23.2	RAID10 方案介绍	406
23.3	创建 RAID 物理卷	407
23.3.1	第一块硬盘的分区	407
23.3.2	其他硬盘的分区	410
23.4	软件 RAID 设置	411
23.4.1	创建/boot 分区	411
23.4.2	创建根分区和 swap 分区	413
23.5	分区格式化	414
23.5.1	格式化/boot 分区	414
23.5.2	格式化根分区	415
23.5.3	格式化交换分区	416
23.6	保存分区设置	416
23.7	grub 的问题	417
23.8	RAID10 的日常维护	418

23.8.1	mdadm 的主要工作模式	418
--------	---------------------	-----

23.8.2	mdadm 的选项	418
23.8.3	创建 RAID 阵列	420
23.8.4	查询 RAID 阵列	420
23.8.5	RAID 的监控	421
23.8.6	RAID 的启动/停止	421

23.9	故障处理	421
------	------------	-----

23.9.1	从 RAID 中移除设备	422
23.9.2	添加已有 RAID 物理卷	422
23.9.3	更换全新硬盘	423

23.10	添加备用硬盘	425
-------	--------------	-----

23.10.1	插入新硬盘	426
23.10.2	新硬盘分区	426
23.10.3	将新分区加入 RAID	426
23.10.4	设置 grub	427
23.10.5	故障模拟	427

23.11	RAID10 的空间扩展	428
-------	--------------------	-----

第 24 章 最佳数据安全方案:

RAID10+LVM	429
------------------	-----

24.1	创建 RAID 物理卷	429
------	-------------------	-----

24.1.1	将第一块硬盘分区	429
--------	----------------	-----

24.1.2	剩余硬盘的分区处理	430
24.2	软件 RAID 设置	430
24.2.1	创建 RAID1 阵列	431
24.2.2	创建 RAID10 阵列	431
24.3	LVM 的创建和配置	432
24.3.1	创建 LVM 物理卷	432
24.3.2	LVM 配置	432
24.4	创建/boot 分区	433
24.5	LVM 的相关命令	434
24.5.1	LVM 物理卷相关命令	434
24.5.2	LVM 卷组相关命令	435
24.5.3	LVM 逻辑卷相关命令	438
24.6	添加新硬盘	440
24.6.1	插入新硬盘	441
24.6.2	配置 RAID	441
24.6.3	在 RAID 上配置 LVM	442
24.6.4	扩容文件系统	443
24.7	更换硬盘	444
24.8	LVM 分区备份	444
24.8.1	创建快照	444
24.8.2	备份快照内容	445
24.8.3	删除快照	445

第 10 篇 系统安全

第 25 章 Ubuntu Server 系统安全 448

25.1	系统安全更新	448
25.1.1	订阅安全列表	448
25.1.2	自动更新	448
25.2	控制台安全	449
25.3	用户、密码管理	449
25.3.1	关于 root 用户	450
25.3.2	关于 sudo	450
25.3.3	关于/etc/sudoers	450
25.3.4	密码策略	452
25.4	ufw 防火墙	453
25.4.1	启用、禁用 ufw	454
25.4.2	基本规则设置	455

25.4.3	常用规则设置	456
25.4.4	高级规则设置	457
25.4.5	IP 伪装	459
25.5	iptables 防火墙	461
25.5.1	iptables 命令	461
25.5.2	基本的 iptables 防火墙	462
25.5.3	保存防火墙规则	464
25.6	AppArmor 配置	464
25.6.1	学习模式和强制模式	465
25.6.2	加载和禁用	466
25.6.3	配置文件	466

第 26 章 入侵检测与系统修复 468

26.1	psad 简介	468
26.2	安装 psad	468
26.3	配置 iptables 规则	469
26.3.1	清空规则表	469
26.3.2	添加规则	469
26.4	配置 psad	471
26.4.1	联系人和主机名	471
26.4.2	危险级别	471
26.4.3	敏感度	471
26.4.4	日志位置	472
26.4.5	要忽略的端口	472
26.4.6	调整报警频率	472
26.4.7	重启 psad 服务	472
26.5	扫描测试	472
26.6	入侵防御	473
26.6.1	定义来源 IP 的危险级别	473
26.6.2	自动拦截	474
26.7	肉鸡检测	475
26.7.1	chkrootkit 的使用	476
26.7.2	rkhunter 的使用	477
26.7.3	unhide 的使用	479
26.8	数据完整性检测	480
26.8.1	安装 Tripwire	481
26.8.2	配置 Tripwire	483

26.8.3	初始化 Tripwire 数据库···	486	26.9.1	保持冷静·····	490
26.8.4	执行完整性检测·····	486	26.9.2	断开网络·····	490
26.8.5	检测报告分析·····	487	26.9.3	找到黑客入侵的方法·····	491
26.8.6	查看 Tripwire 数据库 内容·····	488	26.9.4	黑客文件清理·····	495
26.8.7	使用 Tripwire 的注意 事项·····	489	26.9.5	恢复未受影响的服务·····	495
26.9	被入侵后的系统恢复·····	490	26.9.6	修复问题·····	495
			26.9.7	恢复受影响的服务·····	496
			26.9.8	监控系统·····	496