资深系统架构师鼎力之作

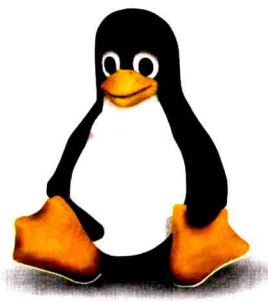
本书以Red Hat Linux发行版为基础，在讲清原理的前提下，通过大量实用的案例，例如企业网站架构、LDAP目录服务配置、Oracle RAC集群与备份、WebLogic集群架设、VMware虚拟化与高可用技术、NetBackup备份服务器架设、MySQL备份技巧、开源信息安全系统OSSIM的详解以及iptables的高级应用等，由浅入深地一一介绍给读者，是一本典型的Linux案例教材。

本书集成了作者近10年Linux平台的系统运维经验，其中大量研究成果可以方便地应用到企业网络管理和运维当中。

本书不但注重提炼与总结，而且详细记录了操作与交互过程，方便学员模仿学习，是一本指导Linux系统工程师“怎么做”和“做什么”的必备参考书。

结合本书内容，配套开通了读者交互网站、微博和QQ讨论群，同时提供书中涉及的开源软件下载地址，方便读者学习和实践。

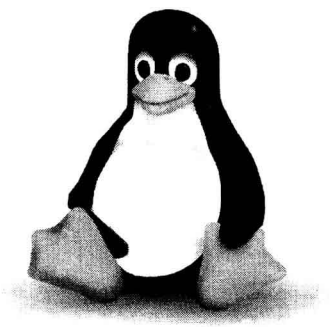
Linux



企业应用案例精解

李晨光 编著

清华大学出版社



Linux
企业应用案例精解

李晨光　编著

清华大学出版社
北京

内 容 简 介

全书共12章，结合几十个经典案例，所讲解的内容无不来源于大中型企业生产一线的实践性总结。其中主要介绍了Web系统集成方法和LAMP安全配置；配置OpenLDAP实现Linux下的应用统一认证；配置Postfix大型邮件系统；Oracle RAC数据库集群的配置与管理；Heartbeat、WebLogic和OSCAR高可用集群的搭建；VSFTP和ProFTP的整合管理；Snort在企业中的部署与管理；配置Xen和VMware的企业虚拟化应用；Linux系统和服务的安全防护策略和经典黑客入侵案例分析；Nagios的安装和高级配置以及OSSIM配置和综合应用分析；iptables防火墙在企业中高级应用；利用Rsync进行数据自动化备份以及NetBackup安装配置与Oracle备份实例等。

本书适合中、高级Linux系统管理员、网络工程师、系统集成工程师使用，也适合作为大专院校计算机专业师生的参考书。

图书在版编目（CIP）数据

Linux企业应用案例精解/李晨光编著. - 北京：清华大学出版社，2012.4
ISBN 978-7-302-27541-1

I. ①L… II. ①李… III. ①Linux操作系统 IV. ①TP316.89

中国版本图书馆CIP数据核字（2011）第268402号

责任编辑：夏非彼
封面设计：王　翔
责任校对：马颖君
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：190mm×260mm　　**印　　张**：29.75　　**字　　数**：762千字
版　　次：2012年4月第1版　　**印　　次**：2012年4月第1次印刷
印　　数：1～4000
定　　价：65.00元

产品编号：044399-01

前　言

随着我国信息化的深入发展，基于 Linux 特有的高可靠性、高稳定性和高安全性等特点，多数企业已将 Linux 操作系统从原来的边缘应用向企业关键业务应用转移。由于 Linux 平台几乎拥有所有企业信息建设需要的软件，能够轻松且廉价地搭建起企业应用服务，因而 Linux 开始替代商业的 UNIX 和 Windows 平台，成为企业建设信息化的重要选择。另外出于建设成本等因素考虑，一些机构也将 UNIX 平台的高端应用向基于 Linux 的服务器平台移植。目前，Linux 操作系统已成为仅次于 Windows 的第二大操作系统。

如何搭建基于 Linux 服务器的网络应用方案，成为企业网络管理人员需要考虑的一个重要问题。记得我的一位中学数学老师在回答如何学好数学时说过的一句话，“要想学好数学就要多做题，做题时公式不记得就查书，不怕不记得公式，做的题目多了自然就记住了。”在创作本书的时候也是以“理论够用、实践第一”为原则，也就是先做题后讲公式，这样通过几个实验下来，读者的印象也会十分深刻。全书共 12 章，每章都有若干个经典案例，每个案例不仅对事件过程进行了讲解，对一些重点命令和知识点也都进行了深入浅出的讲解。这样写作既不流俗于理论讲解，也不局限于命令的堆积，采用基本概念和实际案例的操作过程相结合，对于关键环节也做出了必要说明，可以照顾到一些 Linux 基础薄弱的读者对案例的学习和消化。本书中所有案例都经本人亲自实验，每个案例讲解力求通俗易懂，语言阐述力求深入浅出，让读者通过读、看、练从而达到具备真正的动手能力。

本书特点

本书采用 Red Hat Enterprise Linux 5 和 SUSE Linux Enterprise 操作系统为主要安装环境，结合几十个经典案例，对企业应用进行分析和重现。在本书的写作过程中，作者花费了大量实践在实验配置上，为了提高可操作性，便于读者学习，作者还专门为每章录制了操作视频，读者可从后文中的交互平台上下载观看。

主要章节介绍

全书共 12 章，各章主要内容如下：

第 1 章　Web 系统集成与安全

本章从 LAMP 网站架构讲起，详细分析了 LAMP 的源码安装过程，在讲解了 LAMP 架设技巧之后，紧接着介绍了利用 Nginx 在服务器上设置缓存，实施负载均衡的经典案例，其中还介绍了 6

点 Apache 安全加固的实用方法。本章也对大型网站常见的数据检索缓慢的情况提出了新的解决方案，即利用 Sphinx Search 提供全文检索。为了使网站服务器能更好地处理 JSP 及 Servlet 程序，本章详细讲解了 Apache 与 Tomcat 集成的步骤；本章的后半部分，从企业网络工程师和骨干运行商等不同角度详细剖析了 DDoS 的检查和预防措施。本章最后详细分析了企业网站遭遇 DDoS 攻击事件的过程，并根据网络连接状况和流量的统计情况，提出了如何检测网站是否遭受 DDoS 攻击的检测方案。

第 2 章 目录服务配置案例

本章讲解了如何在 Linux 平台下通过 LDAP 服务构建统一身份认证的方法，即把传统的网络服务，例如 Web、FTP、SSH、E-mail、Samba 的用户认证都由 LDAP 服务器负责验证，以 Red Hat Linux、SUSE Linux 为例详细讲解了开源软件 OpenLDAP 的安装、账户管理工具的配置过程。

第 3 章 基于 Postfix 的大型邮件系统案例

本章介绍了目前流行的邮件服务器 Postfix 的安装配置与管理过程。从一开始的邮件基本配置讲起，一直深入到 Postfix 反垃圾邮件配置、反病毒配置、安全加密配置及其邮件系统的自动监控配置过程，最后还分析了网易、新浪等分布式大型邮件系统的架构设计。

第 4 章 Oracle RAC 数据库集群在 Linux 系统下搭建案例

本章通过数据系统中心升级的实际案例，配合清晰的安装流程图，详细讲解了从 Oracle 安装准备，环境调整到配置共享存储设备，创建和配置 raw 设备，再讲到 Oracle 安装和配置 Oracle Net，创建与管理维护 RAC 数据库，以及 ASM 的操作注意事项。对于其中不少枯燥的理论术语，进行了简单明了的讲解。

第 5 章 企业集群案例分析

本章通过开源软件 Heartbeat、OSCAR 所这涉及的 HA 高可用集群的搭建过程，通过 Mon 软件实现网络和服务的监控，并讲解了集群搭建完毕的测试技术，在第 4 章 Oracle RAC 设置的基础上，循序渐进地通过实际案例详细讲解了证券交易系统 WebLogic 集群的搭建过程。

第 6 章 FTP 服务器的安全配置案例

本章介绍了高级 FTP 集成应用的综合案例，通过 VSFTPD 和 ProFTPD 用户集中管理，详细解决了 MySQL 和 ProFTP、VSFTP 完美结合的问题，通过两者的融合可以搭建一个高效、稳定且集中管理的 FTP 服务器。通过实际案例讲解了 VSFTP 的安全设置，且对于如何预防暴力破解 FTP 服务器技术做了深入探讨。

第 7 章 部署 IDS 案例分析

本章通过源码包讲解如何在企业内部网中部署 Snort，面对千兆企业环境下如何解决 IDS 所带来的瓶颈问题，其中涉及了交换机的端口镜像 SPAN 和多网卡的绑定等重点问题，并讲解了如何通过网络数据流量来创建新的 Snort 规则。同时也通过 Snort Center 的安装讲解如何管理 Snort，当然 Snort 应用也不会是一帆风顺的，笔者通过一个亲身经历的案例，根据案情描述和取证信息详细

讲解了互联网黑客利用 IP 碎片绕过 Snort 攻击企业服务器的案例。

第 8 章 虚拟化技术应用案例

本章首先对 Linux 系统中运行 Windows 程序的一种实现——Wine 内核运行的机理和实例进行了详细的分析，从而打下了虚拟化技术的基础，之后以 SUSE Linux 企业版 10.0 为基础平台，详细讲解了 Xen 虚拟化技术的应用特点和使用方法，其中还对 Xen 控制虚拟主机的常用命令、故障处理技巧进行了详细叙述。在本章的最后，还和大家一起分享了 VMware HA 构建高可用集群案例的实施心得。

第 9 章 Linux 性能优化

本章针对导致系统性能瓶颈的几个方面：CPU、内存、磁盘 I/O、网络子系统进行分析，介绍了常用的检测工具：top、vmstat、iostat、netstat 等，最后重点从几个方面详细介绍了 Oracle 数据库性能优化的问题，以及 LAMP 网站优化问题。

第 10 章 主机监控应用案例

本章首先讲解运用 Linux 下的开源软件 Nagios 结合 NRPE 插件，实现各种网络服务监控配置及利用飞信实现 Nagios 短信报警功能。其次详细讲解了 Ntop 监控和分析网络流量，并介绍了扩展的几个高级应用例如与 Google Map 整合实现标注监控 IP 位置的功能、对 PDA 手持设备的支持、NetFlow 功能的实现分别做了详细讲解，最后通过调整内核来提升 Ntop 的性能。第 5 章已讲解过 Mon 对集群的监控，这里将介绍又一开源的集群监控工具 Ganglia，实现对整个集群节点的全面监控，并对数据进行综合分析和对处理结果进行相应决策。接下来本章详细介绍了用 cheops-ng 来管理网络设备；最后重点介绍了一个信息安全监控软件 OSSIM，它将前面介绍过的 Nagios、Ntop、Cheops、Nessus、Snort、Nmap 这些工具监控的功能集成在一起提供综合的安全保护平台，使用户得到一站式的服务。文中详细分析了 OSSIM 提供的功能和流程，然后对其安装部署、系统配置和主要功能的使用都做了详细的描述，并提供了与 Cacti、Zabbix 监控软件的系统集成。

第 11 章 iptables 防火墙应用案例

本章深入系统内核详细讲解了调整 netfilter 内核模块以限制 P2P 连接、限制 BT 下载、预防 Syn Flood 攻击的方法，并通过来自生产一线的实用脚本分析了基于 iptables 的 Web 认证的实现过程。

第 12 章 数据备份与恢复

本章从备份的基础讲起，首先提供了运用 SSH、Rsync 实现数据自动备份的案例，然后又向读者介绍了运用日志进行 MySQL 数据库实时恢复的案例，最后花费大量篇幅重点讲解了 NetBackup 安装、配置及管理和进行 Oracle 数据库备份和恢复的案例，每个案例都采用概念和实例相结合的方式，通俗易懂。

附 录

附录 A：用一问一答的形式列举了常见系统和网络管理中出现的各种问题并提供了简单扼要

的回答，方便工作查阅。

附录 B：本书中介绍的所有案例都是通过源码包安装部署的，但是 Linux 下源码包部署时不可回避的就是软件包的依赖问题，作者在这里提供了解决方法。

附录 C：用 10 个步骤讲述了制作 Linux LiveCD 的全过程，这对于理解整个 Linux 系统起到十分重要的作用。

关于读者交互平台

读者交互平台是作者专门为此书的读者交流方便，在 Linux 系统下利用 LAMP 搭建的 Web2.0 网站，其中包含了本书中 12 章的实验内容，即操作视频教程，还包括了本书的基础章节的内容及系统管理与维护的基础视频，这些内容是对本书案例的有利补充。

读者交互平台登录地址 http://bjlcg.com:8080/

作者博客地址：http://chenguang.blog.51cto.com

作者微博地址：http://weibo.com/cgweb

QQ 读者交流群：Linux 企业应用 73120574

适合读者

- 中、高级 Linux 系统管理员
- 网络工程师
- 系统集成工程师
- 大专院校计算机专业师生

阅读本书最好具备 Linux 系统的相关知识，以及 Shell 的基础知识。

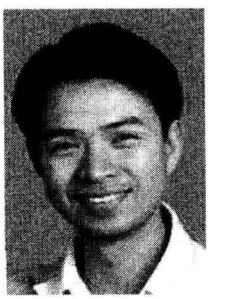
致谢

首先感谢我的父母多年来的养育之恩和关心呵护。还要感谢我的妻子，是她精心的照顾，我才能全身心的投入到创作当中，没有她的支持和鼓励，我无法持之以恒完成本书。最后我要由衷地感谢清华大学出版社的夏毓彦编辑，为了本书能尽快和读者见面，他花费了大量时间和精力与我沟通，并为本书的质量把关起到了重要作用。也要感谢 51CTO 网站、ChinaUnix 为本书内容的发布所作出的贡献。

编　者

2012 年 1 月

作者简介



李晨光，毕业于中国科学院研究生院，就职于中国中铁，资深网络架构师、IBM 精英讲师、Linux 系统安全专家，现任中国计算机学会（CCF）高级会员、会员代表；51CTO 和 IT 专家网特邀专家；获 2010 年度全国 IT 博客 50 强、2011 年度全国 IT 博客 10 强。从事 IDC 机房服务器、网络设备管理 10 年，持有 Microsoft、Cisco、CIW 多个 IT 认证；对 Linux/UNIX、Windows Server 操作系统、系统监控、网络安全防护有着深入研究。先后在国内《计算机安全》、《程序员》、《计算机世界》、《网管员世界》、《黑客防线》、《办公自动化》等 IT 杂志发表专业论文五十余篇，技术博文广泛刊登在 51CTO、IT168、ChinaUnix、赛迪网、天极网、比特网、ZDNet、人民网等国内知名 IT 网站。

目　录

第 1 章　Web 系统集成与安全

1.1　LAMP 网站架构方案分析

LAMP（Linux-Apache-MySQL-PHP）网站架构是目前国际流行的 Web 框架，该框架包括：Linux 操作系统，Apache 网络服务器，MySQL 数据库，Perl、PHP 语言，所有组成产品均是开源软件，是国际上成熟的架构框架，很多流行的商业应用都是采用这个架构，与 Java/J2EE 架构相比，LAMP 具有 Web 资源丰富、轻量、快速开发等特点，与微软的.NET 架构相比，LAMP 具有通用、跨平台、高性能、低价格的优势，因此 LAMP 无论是性能、质量还是价格都是企业搭建网站的首选平台，LAMP 网站优化架构如图 1.1 所示。

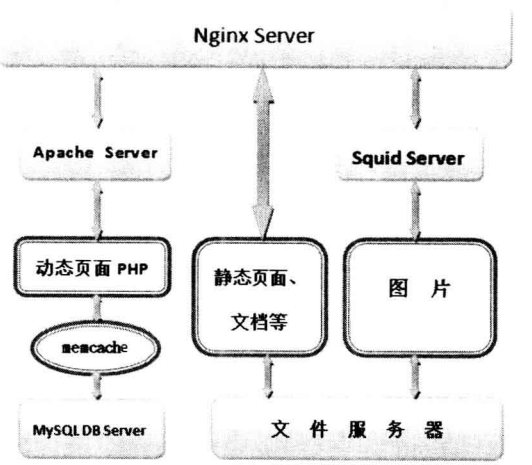


图 1.1　LAMP 网站优化架构

对于大流量、大并发量的网站系统架构来说，除了硬件上使用高性能的服务器、负载均衡、CDN 等之外，在软件架构上需要重点关注下面几个环节：使用高性能的操作系统（OS）、高性能的网页服务器（Web Server）、高性能的数据库（Database）、高效率的编程语言等。下面将从这几点对其进行讨论。

1.1.1　操作系统的选择

Linux 操作系统有很多不同的发行版本，如 Red Hat Enterprise Linux、SUSE Linux Enterprice、Debian、Ubuntu、CentOS 等，每一个发行版本都有自己的特色，比如 RHEL 的稳