

- 本书以Red Hat Linux发行版为基础，在讲清楚原理的前提下，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高级应用等由浅入深地介绍给读者，这种以Linux案例教学模式为主的图书填补了国内Linux教材的空白。
- 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。

Linux



企业应用案例精解

· 李晨光 编著 ·

第2版



本书案例操作教学视频



清华大学出版社

Linux



企业应用案例精解

· 李晨光 编著 ·

第2版

清华大学出版社
北 京

内 容 简 介

全书共 14 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、漏洞测试方法和 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; Linux 内核加固、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 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。

本书封面贴有清华大学出版社防伪标签, 无标签者不得销售。

版权所有, 侵权必究。侵权举报电话: 010-62782989 13701121933

图书在版编目(CIP)数据

Linux 企业应用案例精解/李晨光编著. -2 版. -北京: 清华大学出版社, 2014
ISBN 978-7-302-35226-6

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 (2014) 第 014302 号

责任编辑: 夏非彼

封面设计: 王 翔

责任校对: 闫秀华

责任印制: 杨 艳

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: 北京市密云县京文制本装订厂

经 销: 全国新华书店

开 本: 190mm×260mm 印 张: 34.5 字 数: 883 千字
附光盘 1 张

版 次: 2012 年 3 月第 1 版 2014 年 3 月第 2 版 印 次: 2014 年 3 月第 1 次印刷

印 数: 1~3000

定 价: 89.00 元

产品编号: 056341-01

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 14 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分别进行了深入浅出地讲解。这种写作方式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上机实验，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。本书第 1 版上市仅半年后登上了当当操作系统类图书畅销榜，在当当、京东及豆瓣网广获 IT 同行们肯定，好评率达到 98%。

本版特色

本书在出版当年就获得了不错的销量，从出版社获悉打算再次出版，因此开始对第 1 版做出了改版计划，对第 1 版内容进行优化组合，删减了几个不常用案例（包括第 8 章的 Wine 实战之 Linux 网银、常见问题速查以及制作自己的 LiveCD 的内容）。新增了 140 页的内容，第 1 章新增了构建大型网站方法、基于开源 WAF 的使用方法、Web 漏洞扫描工具的使用、基于 PHP 的 SQL 注入防范措施、SQL 注入漏洞检测方法、Bind View 实现网通电信互访等内容；第 2 章新增了利用 LDAP 实现 Windows 和 Linux 平台统一认证的内容；第 3~5 章修改了一些错别字。

第 6 章增加了 Vsftp 服务器配置技巧的内容；第 7 章增加了分析 snort 规则，以及服务器被入侵后管理员最应做的 5 件事；第 10 章增加了安装远程管理工具 webmin 和 phpmyadmin，为 ossim 增加 gnome，分布式部署（vpn 连接）、Ossim 插件配置管理包括如何创建并启用新插件，收集防火墙日志的方法、手机 CheckPoint 日志的方法，收集 squid 日志的方法，如何解决日志中包含中文的处理方法，如何通过开源软件对 Ossim 进行压力测试内容；第 11 章增加了 Iptables 过滤实例，

包括过滤网站过滤特殊字段等内容,在最后还增加了 13 章内核安全加固案例和第 14 章远程连接的数个经典案例。

实验平台采用 Red Hat Enterprise Linux 和 SUSE Linux Enterprise 操作系统,新增的十几个经典案例,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,目的是为了提提高可操作性。另外,为了便于读者学习作者录制了上百个教学视频,其中包括轻松学习 Linux 之入门篇系列, Lamp, Lnmp, Oracle RAC, KVM, RHCS, JBoss, Ha-Proxy, Hadoop, Weblogic, Openfiler, Postfix, Samba 配置等深受网友们喜爱的内容,读者可从后文中的交互平台下载学习。

主要章节介绍

全书共分 14 章,各章主要内容如下:

第 1 章 Web 系统集成与安全

本章从 LAMP 网站基础架构讲起,包括大型网站架构,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 平台上通过 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,进行了简单明了地讲解。

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，详细介绍了 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地分析，从而打下了虚拟化技术的基础，之后以 SUSE Linux 企业版为基础平台，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、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地描述，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，iptables 过滤实例，包括过滤网站过滤特殊字段等。

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 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。

第 13 章 内核安全加固案例

本章以 Linux 内核安全的为背景，着重介绍用 VXE（虚拟执行环境）技术来保护 Linux 安全，它相当于一个 IPS，通过对进行配置来保护 Linux 系统，接下来从系统缓冲区溢出原理将其逐步分析产生原因和利用 DSM 防范的技巧。

第 14 章 远程连接

从基础的使用 Linux 远程桌面设置讲起，逐步介绍到 XDM 的配置，再介绍常用的 VNC 服务的攻击预防案例分析，接着介绍了加固 SSH 服务器的九种方法，最后讲解 SSH/RDP 等远程访问方式的审计方法。

附录

附录 A：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 B：开源监控软件对比表。

附录 C：本书第一版读者评价。

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，搭建了网站，其中包含了本书中 14 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。

读者交互平台地址 <http://bjlccg.com:8080/>

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

视频教程地址：http://www.tudou.com/home/_117459337

Linux 企业应用 QQ 读者交流群：73120574

适合读者

- 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

致谢

首先感谢我的父母多年来的养育之恩和关心呵护，感谢所有培养教育过我的老师们，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。此外，也要感谢 51CTO 网站、ChinaUnix、IT168、IT 专家网为本书内容的发布所作出的贡献。

编 者
2014 年 1 月

作者简介

李晨光，毕业于中国科学院研究生院，就职于世界 500 强企业信息部门，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、IT 专家网和 ChinaUnix 论坛专家博主；曾获 2011~2013 年度全国 IT 博客 10 强。从事 IDC 机房网络设备运维 10 年，持有 Microsoft、Cisco、CIW 多个 IT 认证；对 Linux/UNIX、Windows Server 操作系统、网络安全防护有深入研究。2012 年受邀担任中国系统架构师大会（SACC）运维开发专场嘉宾主持人；先后在国内《计算机安全》、

《程序员》、《计算机世界》、《网络运维与管理》、《黑客防线》、《办公自动化》等 IT 杂志发表专业论文六十余篇，撰写的技术博文广泛刊登在 51CTO、IT168、ChinaUnix、赛迪网、天极网、比特网、ZDNet 等国内知名 IT 网站。



目 录

第 1 章 Web 系统集成与安全	1
1.1 构建大型网站	1
1.2 LAMP 网站架构方案分析	3
1.2.1 操作系统的选择	3
1.2.2 Web 服务器、缓存和 PHP 加速	4
1.2.3 数据库	5
1.3 LAMP 安装	5
1.3.1 LAMP 安装准备	5
1.3.2 开始安装 LAMP	8
1.3.3 安装 PHP 扩展 Eaccelerator 0.9.6.1 加速软件	11
1.3.4 安装 Suhosin	13
1.4 利用 Nginx 实现 Web 负载均衡	13
1.4.1 安装、配置 Nginx	14
1.4.2 Nginx 实施负载均衡	20
1.4.3 设置 Nginx 的反向代理配置	21
1.4.4 在 Nginx 负载均衡服务器上设置缓存	22
1.5 Apache 安全加固	22
1.5.1 使用配置指令进行访问控制	22
1.5.2 使用 .htaccess 进行访问控制	23
1.5.3 使用认证和授权保护 Apache	25
1.5.4 使用 Apache 中的安全模块	27
1.5.5 使用 SSL 保证 Web 通信安全	28
1.5.6 其他安全措施	30
1.6 利用 Sphinx 提高 LAMP 应用检索性能	33
1.7 Apache 与 Tomcat 集成	36
1.7.1 安装模块	36
1.7.2 Tomcat5 优化	37
1.8 分析 Apache 网站状态	39
1.8.1 AWStats 简介	39

1.8.2	安装 AWStats	40
1.8.3	配置 AWStats	40
1.8.4	应用 AWStats 分析日志	41
1.8.5	扩展功能加入 IP 插件	42
1.9	应对分布式拒绝服务 (DDoS) 的攻击	42
1.9.1	DDoS 攻击原理	43
1.9.2	DDoS 的检测方法	45
1.9.3	防范 DDoS 攻击	46
1.9.4	基于角色的防范	49
1.9.5	小结	51
1.10	案例实战：网站遭遇 DDoS 攻击	51
1.10.1	事件发生	51
1.10.2	事件分析	54
1.10.3	针对措施	55
1.10.4	小结	59
1.11	基于开源的 Web 应用防火墙 (FreeWAF)	60
1.11.1	安装 FreeWAF 注意事项	60
1.11.2	FreeWAF 网络部署	62
1.11.3	防篡改设置	63
1.12	Web 漏洞扫描工具	64
1.12.1	Nikto	64
1.12.2	其他 Web 检测工具	66
1.12.3	利用开源软件扫描漏洞	67
1.12.4	Fast-Track	67
1.12.5	商业软件	69
1.12.6	小结	70
1.13	基于 PHP 的 SQL 注入防范	70
1.13.1	服务器端的安全配置	70
1.13.2	PHP 代码的安全配置	71
1.13.3	PHP 代码的安全编写	71
1.13.4	小结	72
1.14	SQL 注入漏洞检测方法	72
1.15	BIND View 实现网通电信互访	76
1.15.1	背景	76
1.15.2	选择 BIND 解决方案	76
1.15.3	BIND View 方案	77
1.15.4	方案实施步骤	79

1.15.5 小结.....	82
第 2 章 目录服务配置案例.....	83
2.1 Linux 下 LDAP 统一认证的实现.....	83
2.1.1 LDAP 概述.....	83
2.1.2 实现思路.....	84
2.1.3 使用 LDAP 做身份认证.....	85
2.1.4 LDAP 版本的选择.....	86
2.1.5 LDAP 软件的选择.....	86
2.1.6 OpenLDAP 的安装和配置.....	86
2.1.7 轻松搞定 LDAP 账号管理.....	89
2.1.8 配置 Apache 支持 LDAP.....	92
2.1.9 利用 Smbldap-tool 工具管理 Samba.....	94
2.1.10 利用 Smbldap-tool 初始化 LDAP.....	97
2.1.11 使用 phpLDAPadmin 管理 LDAP 服务器.....	98
2.1.12 LDAP 的安全管理.....	100
2.2 利用 LDAP 实现 Windows 和 Linux 平台统一认证.....	101
2.2.1 Linux 认证.....	101
2.2.2 Windows 认证.....	104
2.2.3 Linux+Windows 统一认证.....	106
第 3 章 基于 Postfix 的大型邮件系统案例.....	109
3.1 基于 Postfix 的大型邮件系统.....	109
3.1.1 Postfix 与其他 MTA 的对比.....	109
3.1.2 基本邮件服务器的搭建.....	110
3.1.3 Postfix 常见问题.....	114
3.1.4 Postfix 的反垃圾配置.....	116
3.1.5 Postfix 的反病毒配置.....	117
3.1.6 自动监控 Postfix 邮件服务器.....	119
3.2 搭建分布式的邮件系统.....	120
3.2.1 搭建分布式邮件系统的架构设计.....	120
3.2.2 邮件接收服务器的配置与设计.....	121
3.2.3 用户邮件服务器的配置与设计.....	122
3.3 利用 Stunnel 加密保护邮件服务器.....	122
3.3.1 安装编译 Stunnel.....	123
3.3.2 保障 IMAP 安全.....	123
3.3.3 保障 POP3 安全.....	124
3.3.4 保障 SMTP 安全.....	124

第 4 章	Oracle RAC 数据库集群在 Linux 系统下搭建案例	125
4.1	确定 Oracle 系统的规模	126
4.1.1	CPU 规模的调整	126
4.1.2	内存规模的调整	127
4.1.3	I/O 子系统的调整	127
4.1.4	RAID 磁盘子系统	128
4.2	Oracle RAC 设置流程	128
4.2.1	系统安装前的关键配置	129
4.2.2	配置主机解析文件 hosts	132
4.2.3	配置系统内核参数	132
4.2.4	给 Oracle 用户配置 Shell	136
4.2.5	配置系统安全设置	137
4.2.6	添加 Oracle 用户和组	137
4.2.7	设置 Oracle 用户环境变量	138
4.2.8	配置节点间的 SSH 信任	139
4.2.9	配置共享存储系统	140
4.2.10	建立和配置 raw 设备	145
4.2.11	安装 Oracle Clusterware	146
4.2.12	安装 Oracle 数据库	152
4.2.13	配置 Oracle Net	154
4.2.14	创建 RAC 数据库	155
4.2.15	Oracle CRS 的管理与维护	163
4.2.16	测试 Oracle RAC 数据库的集群功能	166
4.2.17	ASM 基本操作	171
第 5 章	企业集群案例分析	175
5.1	基于 Heartbeat 的双机热备系统范例	175
5.1.1	准备工作	175
5.1.2	安装 Heartbeat	176
5.1.3	配置/etc/ha.d/ha.cf	176
5.1.4	配置/etc/ha.d/haresources	177
5.1.5	配置 haresources 文件	178
5.1.6	配置/etc/ha.d/authkeys	179
5.1.7	在备份服务器上安装 Heartbeat	180
5.1.8	设置系统时间	180
5.1.9	启动 Heartbeat	180
5.1.10	在备份服务器上启动 Heartbeat	182
5.1.11	检查主服务器上的日志文件	183

5.1.12	停止并启动 Heartbeat	183
5.1.13	监视资源	184
5.1.14	小结	184
5.2	企业服务器搭建双机集群配置	185
5.2.1	Heartbeat、Mon、Rsync 简介	185
5.2.2	安装环境	185
5.2.3	安装 Heartbeat	187
5.2.4	测试 HA 系统	190
5.2.5	Mon 服务监控	191
5.2.6	数据同步	193
5.2.7	集群测试技术	194
5.3	利用 HA-OSCAR 创建高可用 Linux 集群	197
5.3.1	支持的发行版和系统要求	197
5.3.2	HA-OSCAR 的体系结构	198
5.3.3	HA-OSCAR 的向导安装步骤详解	200
5.3.4	监控和配置 Webmin	203
5.3.5	小结	208
5.4	WebLogic 集群高可用案例	209
5.4.1	RHEL 5.4 操作系统的安装	210
5.4.2	Java 环境的配置安装	211
5.4.3	设置环境变量	211
5.4.4	WebLogic 11 安装部署	212
5.4.5	启动 WebLogic 的 AdminServer 服务	217
5.4.6	部署 Web 应用	221
5.4.7	启动 Web 应用	222
5.4.8	WebLogic 优化	224
第 6 章	FTP 服务器的安全配置案例	225
6.1	VSFTP 服务的基本配置	225
6.2	Linux 下 VSFTPD 和 ProFTPD 用户集中管理	230
6.2.1	建立程序安装目录	231
6.2.2	安装 MySQL	231
6.2.3	安装 ProFTPD	232
6.2.4	MySQL 与 ProFTPD 组合	234
6.2.5	VSFTPD 与 MySQL 的组合	237
6.2.6	开机自动启动 VSFTPD	239
6.3	在 VSFTPD 中实现对 IP 的安全管理案例	239

6.3.1	项目背景.....	240
6.3.2	准备工作.....	240
6.3.3	用于封禁和解封的 Shell 脚本.....	241
6.3.4	部署实施.....	242
6.3.5	小结.....	243
6.4	暴力破解 FTP 服务器的技术探讨与防范.....	243
6.4.1	网络本身的负载能力与高速网络.....	243
6.4.2	CPU 运算、处理能力低下的解决方法.....	245
6.4.3	安全策略的突破.....	246
6.4.4	应对措施——第三方软件 Fail2ban 加固方法.....	250
第 7 章	部署 IDS 案例分析.....	254
7.1	在 Linux 下部署 IDS 案例.....	254
7.1.1	安装 Snort.....	254
7.1.2	维护 Snort.....	258
7.1.3	编写 Snort 规则.....	262
7.1.4	分析 Snort 规则.....	265
7.2	Linux 下 PortSentry 的配置.....	270
7.2.1	入侵检测工具简介.....	270
7.2.2	PortSentry 的安装配置.....	271
7.2.3	启动检测模式.....	273
7.2.4	测试.....	274
7.3	利用 IP 碎片绕过 Snort.....	274
7.3.1	事件发生.....	274
7.3.2	故障处理.....	277
7.3.3	数据包解码.....	278
7.3.4	针对 IP 碎片攻击的预防措施.....	284
7.3.5	评估 NIDS 的两个工具.....	285
7.3.6	服务器被入侵后应该做的 5 件事.....	285
7.3.7	小结.....	286
第 8 章	虚拟化技术应用案例.....	287
8.1	Linux 下 Wine 虚拟机.....	287
8.1.1	Wine 的体系结构.....	287
8.1.2	Wine 运行的技术背景.....	288
8.1.3	Wine 启动分析.....	289
8.1.4	Win32 启动分析.....	290
8.1.5	Winelib 启动分析.....	290
8.1.6	Win16 与 DOS 程序启动分析.....	290

8.1.7	Wine 安装.....	291
8.2	基于 SUSE Linux Server 上的 Xen 虚拟化应用.....	292
8.2.1	Xen 和 KVM 虚拟化的对比.....	292
8.2.2	Xen 的特点.....	292
8.2.3	Xen 架构和 Xen 虚拟化技术简介.....	293
8.2.4	安装使用 SUSE Xen 软件.....	294
8.2.5	引导 Xen 系统.....	297
8.2.6	安装 Xen 客户机——Domain-U.....	300
8.2.7	故障查询.....	304
8.3	VMware HA 在企业中的应用.....	305
8.3.1	项目基本情况.....	305
8.3.2	VMware 资源动态分配的实现.....	306
8.3.3	VMware 高可用性的实现.....	306
8.3.4	高可用性集群的实现.....	306
第 9 章	Linux 性能优化.....	309
9.1	Linux 性能评估.....	309
9.2	网络性能优化.....	318
9.2.1	网络性能.....	318
9.2.2	TCP 连接优化.....	320
9.3	Oracle 应用优化案例.....	321
9.3.1	Oracle 数据库性能优化.....	321
9.3.2	Oracle 数据库系统性能调优的方法.....	321
9.3.3	性能调优工具.....	323
9.3.4	系统调整.....	323
9.4	动态 PHP 网站优化案例.....	324
9.4.1	初期性能问题及处理.....	324
9.4.2	逐步解决问题.....	324
9.4.3	网站结构优化.....	324
第 10 章	主机监控应用案例.....	325
10.1	基于 Linux 系统的 Nagios 网络管理.....	325
10.1.1	Nagios 系统及特点.....	326
10.1.2	在 Linux 上运行 Nagios 系统.....	327
10.1.3	运用 Nagios 实现对网络上服务器的监控.....	328
10.1.4	对 Nagios 系统的评价和建议.....	330
10.2	运用 NRPE 扩展 Nagios 功能.....	331
10.2.1	监控原理.....	331
10.2.2	配置 Nagios 客户端.....	331

10.2.3	配置 Nagios 服务器端	333
10.3	利用飞信实现 Nagios 短信报警功能	335
10.3.1	飞信简介	335
10.3.2	安装与配置飞信	335
10.3.3	整合飞信到 Nagios 中	337
10.4	运用 Ntop 监控网络流量	338
10.4.1	几种流量采集技术的比较	340
10.4.2	Ntop 系统的部署及性能	341
10.4.3	Ntop 安装配置	342
10.4.4	应用 Ntop	344
10.4.5	优化 Ntop	356
10.5	基于 Linux 的集群监控系统	360
10.5.1	安装准备	361
10.5.2	集群节点管理器部署 Ganglia	361
10.6	使用 cheops-ng 加强管理 Linux 网络	368
10.6.1	cheops-ng 的工作原理	368
10.6.2	cheops-ng 的下载和安装	368
10.6.3	cheops-ng 的配置	369
10.6.4	cheops-ng 的运行	373
10.7	打造开源安全信息管理平台	375
10.7.1	Ossim 背景介绍	375
10.7.2	安装 Ossim	378
10.7.3	安装远程管理工具	380
10.7.4	安装 X-Window	381
10.7.5	配置解析	383
10.7.6	分布式部署 (VPN 连接) 举例	384
10.7.7	Ossim 的系统配置	386
10.7.8	Ossim 的后台管理及配置	397
10.8	Ossim 插件配置管理	402
10.8.1	原始日志格式对比	402
10.8.2	插件配置工作步骤	403
10.8.3	插件导入方法	404
10.8.4	收集 Cisco 防火墙日志	408
10.8.5	收集 CheckPoint 设备日志	411
10.8.6	将 Squid 的日志收集到 Ossim 系统	413
10.8.7	对日志中含有中文字符的处理方式	413
10.8.8	Linux 系统下网络服务日志方法总结	414
10.9	Ossim 压力测试	415