HZ BOOKS
华章IT

Linux/Unix
技术丛书

Linux运维最佳实践

胥峰 杨俊俊 著

Best Practices in Linux Operations

- 来自盛大游戏拥有10年运维经验的资深专家撰写，盛大游戏、腾讯、金山的多位运营专家联袂推荐
- 技术层面：4大运维方向、21种运维技术、105个最佳实践
- 思想层面：构建运维服务体系，培养运维格局，掌握解决疑难运维问题的思想方法

机械工业出版社
China Machine Press

Linux运维最佳实践

Best Practices in Linux Operations

胥峰 杨俊俊 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Linux 运维最佳实践 / 胥峰，杨俊俊著 . —北京：机械工业出版社，2016.8
（Linux/Unix 技术丛书）

ISBN 978-7-111-54568-2

I. L…　II. ①胥…　②杨…　III. Linux 操作系统　IV. TP316.85

中国版本图书馆 CIP 数据核字（2016）第 193554 号

Linux 运维最佳实践

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：孙海亮　　责任校对：董纪丽
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2016 年 8 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：21.25
书　　号：ISBN 978-7-111-54568-2　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

版权所有 · 侵权必究
封底无防伪标均为盗版
本书法律顾问：北京大成律师事务所　韩光 / 邹晓东

Preface 前　言

为什么要写这本书

《论语·卫灵公》有言："工欲善其事，必先利其器。"

在 Linux 运维领域中，什么是广大系统管理员们的"利器"呢？在我看来，系统管理员的"利器"有 3 个，一个是方法论，一个是经验，最后一个是积极饱满的学习精神。

我们面对的是一个不断变化的世界，业务需求在变，技术架构在变，开源工具与商业系统异构部署，新工具和技术概念层出不穷，唯有一套科学的技术方法论才能应对这些变化。很多时候，我们在面对新的问题时，会束手无措，这恰恰也是方法论缺失导致的结果。从事运维工作 10 余年，我逐渐体会到在运维领域中总结一套问题排除方法论是一件至关重要和有意义的事情。在我的工作中，经常听到有工程师问："网站访问不了了，是什么问题？"此时，我会把我的故障定位方法告诉他，依次实施这些方法，基本都能够有效定位并及时解决问题。我想，若能把这些方法论分享给初入这个行业的人或者在这个领域中工作了多年但仍未打通"任督二脉"的人，将会是一件极有意义的事。

经验是另一个有意思的话题。很多时候，我们对一个问题的判断，是基于以前的思考和处理方法的。有时候经验并不完全正确，但对经验的总结和归纳，却可以给我们提供新的思考方向，因为从经验中获取的知识和技能在未来也是通用的。自 2006 年毕业后，我一直从事与运维相关的工作。在我最开始从事的局域网内网管理工作中，看到了使用 ARP 欺骗竟然可以让一台计算机失去网络连接；看到了 Andrew.S.Tanenbaum 先生所著的《 Computer Networks 》中所讲的每个知识都活了起来。到后来，我加入了一家创业型的公司，全面负责公司的网站和业务运维，从每天上千次网站访问量到日 PV 超过千万，我经历了高性能网站构建、监控、安全和运维自动化等各个方面的实践，使得自己在各个层面都有了丰富的经验积累。再后来，进入盛大游戏，我接触到了大型端游的上线运维、现象级手游的发布运维，使自己又对游戏运维体系有了很多积累和总结。我想把这些经验都积累下来，分享给大家，让大家在考虑架构和运维体系时，既能注意宏观的层面，也能把握技

术细节。通过学习书中每一个技术和体系的最佳实践，所有工程师都能得到提升。通过我的分享，我曾踩过的那些“坑”在大家前进的路上将被填平，并成为大家前进的基础。本书中总结的每一个最佳实践，都将是对系统稳定性和性能的一个优化。

积极饱满的学习精神是系统管理员必备的特质，这也决定了大家的职业之路能走多远。有了方法论和经验，可以让一个人在某个时间段成为某个领域的专家，但是只有不断学习，才能保持在这个领域的优势。就像驾驶一辆汽车在高速上疾驰，也许开始时一路领先，但如果没有持续加油提供动力，还是会被后面的车辆不断超越。在运维工作中，不断学习就是不断给自己的职业能力加油。在面对新概念、新技术时，仅考虑如何使用它是不够的，更多的是思考这些技术的底层原理、实现方法、技术前景预估和判断，这样才能成为不断引领这个领域进步的人。

读者对象

本书适合以下几类读者阅读：

- 中高级运维工程师；
- Linux 运维爱好者；
- 计算机相关专业的学生。

如何阅读本书

本书分为 4 大部分，具体介绍如下。

第一部分，高性能网站构建。这部分对构建高性能网站所需要的各项技术都做了详尽说明，涵盖域名、CDN、负载均衡、网站部署和数据库的相关知识和最佳技术实践。

第二部分，服务器安全和监控。业务架构起来后，如何保证它的安全性和稳定性，是大家需要关注的焦点。这部分解决两个问题：一个是加固服务器，使其避免轻易成为黑客的“肉鸡”；一个是监控，使故障在发展成为重大事故前就被预警和处理。

第三部分，网络分析技术。这部分给出 Linux 运维领域中的网络分析方法论。通过对这部分的学习，大家将在遇到未知的运维网络服务问题时，能够自信地按方法论实施分析，从而解决问题。

第四部分，运维自动化和游戏运维。随着服务器规模的剧增，使用一台台登录服务器进行管理、运维的方式将成为效率的瓶颈。这部分给出运维自动化实践方案，从开源实现到自主开发，互相补充，互相提升，真正实现适合自己的运维自动化体系。游戏运维，将对端游和手游这两大目前最火的游戏运维主题进行说明。

试读结束：需要全本请在线购买： www.ertongbook.com

勘误和支持

虽然我试图努力保证本书不出现错误，但限于自己的知识和视角，本书难免会出现用词不当、部分场景下技术不适用的问题。在此，我恳请读者不吝指教。您若发现本书存在不足之处，请发送邮件到 xufengnju@163.com 或者加入 QQ 群 434242482（Linux 运维最佳实践）帮助我修正本书。另外，您还可以通过以上两种方式获得技术支持。本书的勘误将列在 http://xufeng.info/errata.html 中。

致谢

感谢盛大游戏高级总监桂总和我的领导老冯的大力支持。

感谢力哥（《深度实践 KVM》作者、西山居运维经理肖力）的引荐，使本书得以从想法落实到出版。

感谢机械工业出版社的杨福川。福川兄出版了一系列 IT 技术领域的畅销书、精品书，本书能够得到福川兄的指正和帮助，是我的荣幸。

感谢我的妻子和可爱的女儿 Cary，你们的理解和支持是我工作的动力，你们的笑容是我幸福的源泉。

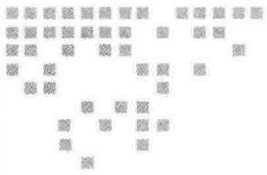
胥　峰

目　录 Contents

试读结束：需要全本请在线购买：www.ertongbook.com

第 1 篇 Part 1

高性能网站构建



Chapter 1 第 1 章

深入理解 DNS 原理与部署 BIND

DNS（Domain Name System，域名系统）是互联网上最核心的带层级的分布式系统，它负责把域名转换到 IP 地址、反查从 IP 到域名的解析以及宣告邮件路由等信息，使得基于域名提供服务成为可能，例如网站访问、邮件服务等。

人们无时无刻不在使用 DNS 提供的服务，但大多数人对它的工作原理知之甚少。在这样的情况下，在出现与 DNS 相关的问题或者故障时，人们会无所适从，无法迅速找到问题根源进而排除故障。本章将对 DNS 的核心概念进行深度探索，从而深入理解 DNS 的工作原理。

BIND（Berkeley Internet Name Domain，伯克利互联网名称域）是 Linux、UNIX 系统上部署最广泛的域名服务器，是域名解析协议的事实标准。可以通过 BIND 构建各种满足不同业务需求的 DNS。本章将讲解使用 BIND 构建 DNS 的最佳实践。

最佳实践 1：禁用权威域名服务器递归查询

我们经常听说 DNS 的“递归查询”和“迭代查询”，那么到底什么是“递归查询”，什么是“迭代查询”呢？

我们并不直接回答这个复杂的问题，而是先从 DNS 相关的重要概念开始学习。只有理解了这些概念，才能真正回答这个问题。

DNS 的组成部分

DNS 的组成概括来讲包括以下两个部分。

- **域名服务器**（Name Server）。提供域名解析服务的软件，一般监听 UDP、TCP 的 53 端口。例如 Linux 系统中常见的 BIND、Windows Server 中集成的 DNS 服务器

组件等。

- **解析器**（Resolver）。访问域名服务器的客户端，它负责解析从域名服务器获取的响应，向调用它的应用返回 IP 地址或者别名等信息，例如 Linux 系统中的 gethostbyname() 函数、Windows 系统中的 nslookup 等。

域名服务器的分类

域名服务器根据用途不同，可以进行如下分类。

1. 权威域名服务器（Authoritative Name Server）

负责授权域下的域名解析服务，由上级权威域名服务器使用 NS 记录进行授权。

有以下 3 级权威域名服务器。

（1）根域名服务器（Root Name Server）

最上层权威域名服务器，负责对 .com、.cn、.org 等顶级域名的向下授权。目前有 13 组这样的服务器，详见表 1-1。

表 1-1　根域名服务器分布情况表

主 机 名	IP 地址	管 理 方
a.root-servers.net	198.41.0.4	VeriSign, Inc.
b.root-servers.net	192.228.79	University of Southern California (ISI)
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53	US Army (Research Lab)
i.root-servers.net	192.36.148.17	Netnod
j.root-servers.net	192.58.128.30	VeriSign, Inc.
k.root-servers.net	193.0.14.129	RIPE NCC
l.root-servers.net	199.7.83.42	ICANN
m.root-servers.net	202.12.27.33	WIDE Project

对于表 1-1 中的服务器，这里指出是 13 组，而不是 13 台，是因为其中的大部分服务器采用了 anycast 技术，将其分布到不同地区，也就是说，虽然看起来只有 13 个 IP，但实际的服务器数量远远超过了 13 台。Anycast 是在大型 DNS 系统中广泛使用的多点部署、分布式方案，对于提高可用性、提高性能、抵抗 DDOS 有重要作用。有兴趣的读者可以参考 Wikipedia 上 anycast 技术的详细介绍：https://en.wikipedia.org/wiki/Anycast。

（2）顶级域名服务器（Top Level Name Server）

顶级域名服务器有以下2类。

- 通用顶级域名（Generic Top Level Domains，GTLD）服务器。例如服务于.com、.org、.info等授权的域名服务器。
- 国家代码顶级域名（Country Code Top Level Domains，CCTLD）服务器。例如服务于.uk、.cn、.jp等授权的域名服务器。

完整的顶级域名服务器列表，可以从http://www.iana.org/domains/root/db这个链接获取。例如负责.cn授权的国家代码顶级域名服务器，详见表1-2。

表1-2 负责解析.cn的顶级域名服务器列表

主 机 名	IP地址
ns.cernet.net	202.112.0.44
a.dns.cn	203.119.25.1
c.dns.cn	203.119.27.1
b.dns.cn	203.119.26.1
d.dns.cn	203.119.28.1
e.dns.cn	203.119.29.1

（3）二级域名服务器（Second Level Name Server）

这类域名服务器，服务于具体域名解析，例如负责解析sdo.com域的域名服务器ns.uugame.com等。

以上3类权威域名服务器的授权结构可以参考图1-1。

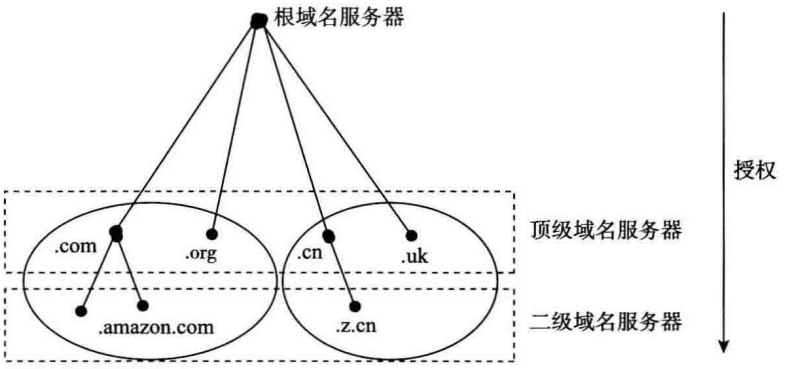


图1-1 权威域名服务器的授权结构图

2. 缓存域名服务器（Caching Name Server）

这类域名服务器，负责接收解析器发过来的DNS请求，通过依次查询根域名服务器→顶级域名服务器→二级域名服务器来获得DNS的解析条目，然后把响应结果发送给解析

试读结束：需要全本请在线购买： www.ertongbook.com