

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



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

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。

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。若您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*

前言

第 1 篇 高性能网站构建

第 1 章 深入理解 DNS 原理与部署

BIND..... 2

最佳实践 1: 禁用权威域名服务器递归

查询..... 2

DNS 的组成部分..... 2

域名服务器的分类..... 3

递归查询与迭代查询的区别..... 5

禁用递归查询的原因与方法..... 6

最佳实践 2: 构建域名解析缓存..... 6

域名解析缓存的必要性..... 6

NSCD 安装配置方法..... 6

域名解析缓存验证..... 7

最佳实践 3: 配置 chroot 加固 BIND..... 8

最佳实践 4: 利用 BIND 实现简单负载

均衡..... 9

最佳实践 5: 详解 BIND 视图技术及

优化..... 10

BIND 视图工作原理..... 10

BIND 视图优化技巧..... 12

最佳实践 6: 关注 BIND 的漏洞信息..... 12

最佳实践 7: 掌握 BIND 监控技巧..... 13

本章小结..... 13

第 2 章 全面解析 CDN 技术与实战..... 14

最佳实践 8: 架构典型 CDN 系统..... 14

最佳实践 9: 理解 HTTP 协议中的缓存

控制: 服务器端缓存控制头部信息..... 16

最佳实践 10: 配置和优化 Squid..... 18

推荐使用大内存服务器..... 18

推荐每个磁盘独立使用..... 18

禁用 atime 更新..... 19

配置 Squid 多实例..... 19

使用 URL 哈希方法对 Squid 多实例

进行调度..... 19

禁用缓存间通信协议..... 19

架构二级缓存..... 19

使用 Squid Manager 获取运行状态..... 20

优化 HTTP Range..... 20

最佳实践 11: 优化缓存防盗链..... 21

Key 的组成..... 21

校验过程..... 21

实施过程..... 22

重定向器..... 22

最佳实践 12: 实践视频点播 CDN..... 23

视频点播 CDN 系统概述	23	LVS-Tun	53
系统模块分类	23	3 种模式对比与推荐	53
用户访问流程	23	最佳实践 22: LVS+Keepalived 实战	
同步源站服务器	24	精讲	53
视频源站服务器	25	LVS+Keepalived 配置过程详解	53
视频转发服务器	26	LVS 重要参数	56
缓存服务器	28	LVS-DR 模式的核心提示与优化	57
最佳实践 13: 设计大规模下载调度		最佳实践 23: 多组 LVS 设定注意事项	58
系统	30	最佳实践 24: 注意网卡参数与 MTU	
本章小结	31	问题	58
第 3 章 负载均衡和高可用技术	32	MTU 的原理	58
最佳实践 14: 数据链路层负载均衡	33	案例解析	59
链路层负载均衡的必要性	33	最佳实践 25: LVS 监控要点	64
Linux Bonding 配置过程	34	性能采集	64
最佳实践 15: 4 层负载均衡	38	可用性监控	64
4 层负载均衡的数据格式	38	最佳实践 26: LVS 排错步骤推荐	64
4 层负载均衡的时序图	39	本章小结	66
最佳实践 16: 7 层负载均衡	40	第 5 章 使用 HAProxy 实现 4 层和	
7 层负载均衡的数据格式	40	7 层代理	67
7 层负载均衡的时序图	40	最佳实践 27: 安装与优化	67
最佳实践 17: 基于 DNS 的负载均衡	41	HAProxy TCP 负载均衡	68
最佳实践 18: 基于重定向的负载均衡	43	HAProxy HTTP 负载均衡	69
下载系统 HTTP 302 重定向	43	HAProxy 的核心配置参数	71
上传系统的重定向方法	44	HAProxy 的会话保持机制	72
最佳实践 19: 基于客户端的负载均衡	45	HAProxy 中 ip_local_port_range 问题	73
哈希方法	45	HAProxy 后端服务器获取客户端 IP	73
数据库读写分离	46	TCP 负载均衡和 HTTP 负载均衡的	
最佳实践 20: 高可用技术推荐	47	对比	74
本章小结	47	最佳实践 28: HAProxy+Keepalived	
第 4 章 配置及调优 LVS	48	实战	75
最佳实践 21: 模式选择	49	最佳实践 29: HAProxy 监控	76
LVS-NAT	49	性能采集	76
LVS-DR	49	可用性监控	76
		最佳实践 30: HAProxy 排错步骤推荐	77

本章小结	77	最佳实践 40: NetScaler 监控	104
第 6 章 实践 Nginx 的反向代理和		ns.log 监控	104
负载均衡	78	性能采集	106
最佳实践 31: 安装与优化	79	最佳实践 41: NetScaler 排错步骤	
Nginx 的核心配置参数	81	推荐	106
Nginx 负载均衡算法	81	最佳实践 42: NetScaler Surge Protection	
Nginx Proxy 协议的选择	81	引起的问题案例	107
Nginx 中 ip_local_port_range 问题	86	最佳实践 43: LVS、HAProxy、Nginx、	
Nginx 被代理的后端服务器获取客户		NetScaler 的大对比	108
端 IP	86	最佳实践 44: 中小型网站负载均衡方案	
最佳实践 32: Nginx 监控	86	推荐	109
性能采集	86	本章小结	109
可用性监控	87	第 8 章 配置高性能网站	110
最佳实践 33: Nginx 排错步骤推荐	88	最佳实践 45: 深入理解 HTTP 协议	110
最佳实践 34: Nginx 常见问题的处理		HTTP 协议通信的网络模型	111
方法	88	一次 HTTP 请求的详细分析	112
本章小结	89	最佳实践 46: 配置高性能静态网站	114
第 7 章 部署商业负载均衡设备		缓存配置方法	115
NetScaler	90	压缩配置方法	115
最佳实践 35: NetScaler 的初始化设置	90	防盗链的配置方法	116
NetScaler 中各种用途的 IP 概念	90	图片剪裁的方法	116
NetScaler 初始化的步骤	91	减少 Cookie 携带	117
最佳实践 36: NetScaler 基本负载均衡		实现静态文件的安全下载	117
核心参数配置	94	使用 ngx_http_secure_link_module 模块	
最佳实践 37: NetScaler 内容交换核心		的配置方法	117
参数配置	96	使用 Nginx 中的 X-Accel-Redirect 控制	
NetScaler 被代理的后端服务器获取		头部	118
客户端 IP	98	使用 CDN 加速用户访问	119
最佳实践 38: NetScaler 的 Weblog 配置		最佳实践 47: 配置高性能动态网站	119
与解析	98	PHP-FPM 优化	119
最佳实践 39: NetScaler 高级运维指南	99	Tomcat 优化	120
		最佳实践 48: 配置多维度网站监控	121
		日志监控	122

可用性监控	124	各种 script 功能	150
性能监控	124	最佳实践 59: OpenVPN 的排错步骤	151
本章小结	125	本章小结	154
第 9 章 优化 MySQL 数据库	126	第 11 章 实施 Linux 系统安全策略与	
最佳实践 49: MySQL 配置项优化	126	入侵检测	156
最佳实践 50: 使用主从复制扩展读写		最佳实践 60: 物理层安全措施	156
能力	127	最佳实践 61: 网络层安全措施	157
主从复制监控的方法	128	使用 Linux 的 iptables 限制网络访问	158
主从复制失败的原因分析	128	使用 Windows Server 2003 Enterprise 的	
最佳实践 51: 使用 MHA 构建高可用		ipsecpol 限制网络访问	159
MySQL	131	使用 Windows Server 2008 Enterprise 的	
本章小结	132	netsh advfirewall 限制网络访问	159
		使用 FreeBSD 的 IPFW 限制网络访问	161
		使用 Cisco IOS 的 ACL 限制网络访问	162
		端口扫描的重要性	162
		分布式 DDOS 的防护	163
		最佳实践 62: 应用层安全措施	165
		密码安全策略	165
		SSHD 安全配置	166
		Web 服务器安全	168
		数据库安全策略	171
		BIND 安全配置	171
		最佳实践 63: 入侵检测系统配置	171
		最佳实践 64: Linux 备份与安全	180
		备份与安全的关系	180
		数据备份的注意事项	180
		数据恢复测试	180
		本章小结	180
		第 12 章 实践 Zabbix 自定义模板	
		技术	181
		最佳实践 65: 4 步完成 Zabbix Server	
		搭建	181
第 2 篇 服务器安全和监控			
第 10 章 构建企业级虚拟专用网络	134		
最佳实践 52: 常见的 VPN 构建技术	134		
PPTP VPN 的原理	135		
IPSec VPN 的原理	135		
SSL/TLS VPN 的原理	135		
3 种 VPN 构建技术的对比	136		
最佳实践 53: 深入理解 OpenVPN 的			
特性	136		
最佳实践 54: 使用 OpenVPN 创建 Peer-			
to-Peer 的 VPN	136		
Linux tun 设备精讲	139		
最佳实践 55: 使用 OpenVPN 创建 Remote			
Access 的 VPN	141		
最佳实践 56: 使用 OpenVPN 创建 Site-			
to-Site 的 VPN	148		
最佳实践 57: 回收客户端的证书	149		
最佳实践 58: 使用 OpenVPN 提供的			

最佳实践 66: Zabbix 利器 Zabbix	184
最佳实践 67: Zabbix Agent 自动注册	185
最佳实践 68: 基于自动发现的 KVM 虚拟机性能监控	188
本章小结	195

第 13 章 服务器硬件监控 196

最佳实践 69: 服务器硬盘监控	196
最佳实践 70: SSD 定制监控	198
SSD 优势与内部结构	198
SSD 选型	198
SSD 应用场景及定制监控	199
最佳实践 71: 服务器带外监控: 带外 邮件警告	202
本章小结	205

第 3 篇 网络分析技术

第 14 章 使用 tcpdump 与 Wireshark

解决疑难问题 208

最佳实践 72: 理解 tcpdump 的工作 原理	209
tcpdump 的实现机制	209
tcpdump 与 iptables 的关系	210
tcpdump 数据包长度超过网卡 MTU 的 问题	210
tcpdump 的简要安装步骤	210
最佳实践 73: 学习 tcpdump 的 5 个参数 和过滤器	211
学习 tcpdump 的 5 个参数	211
学习 tcpdump 的过滤器	211
最佳实践 74: 在 Android 系统上抓包的 最佳方法	212

最佳实践 75: 使用 RawCap 抓取回环 端口的数据	214
最佳实践 76: 熟悉 Wireshark 的最佳 配置项	215
Wireshark 安装过程的注意事项	215
Wireshark 的关键配置项	216
使用追踪数据流功能	218
最佳实践 77: 使用 Wireshark 分析问题 的案例	219
案例一 定位时间戳问题	219
解决方法	220
案例二 定位非正常发包问题	220
抓包方法	221
分析方法	222
解决方法	223
最佳实践 78: 使用 libpcap 进行自动化 分析	223
本章小结	224

第 15 章 分析与解决运营商劫持

问题 225

最佳实践 79: 深度分析运营商劫持的 技术手段	225
中小运营商的网络现状	225
基于下载文件的缓存劫持	226
基于页面的 iframe 广告嵌入劫持	229
基于伪造 DNS 响应的劫持	230
网卡混杂模式与 raw socket 技术	230
最佳实践 80: 在关键文件系统部署 HTTPS 的实战	233
HTTPS 证书的获取方法	233
Nginx 支持 HTTPS 的按照方式	235
Nginx 配置文件示例	235
本章小结	235

第 16 章 深度实践 iptables237	第 18 章 利用 Perl 编程实施高效运维267
最佳实践 81: 禁用连接追踪.....237	最佳实践 87: 多进程编程技巧.....268
排查连接追踪导致的故障.....237	最佳实践 88: 调整 Socket 编程的超时时间.....270
分析连接追踪的原理.....239	为什么设置 Socket 超时.....270
禁用连接追踪的方法.....240	设置 Socket 超时的方法.....271
确认禁用连接追踪的效果.....243	最佳实践 89: 批量管理带外配置.....271
最佳实践 82: 慎重禁用 ICMP 协议.....243	带内管理与带外管理.....271
禁用 ICMP 协议导致的故障案例一则.....243	HP iLO 的批量管理方法.....272
MTU 发现的原理.....245	Dell iDRAC 的批量管理方法.....273
解决问题的方法.....247	最佳实践 90: 推广邮件的推送优化.....274
最佳实践 83: 网络地址转换在实践中的案例.....247	推送优化的思路与代码分析.....274
源地址 NAT.....247	推广邮件的效果分析.....275
目的地址 NAT.....248	最佳实践 91: 使用 PerlTidy 美化代码.....276
最佳实践 84: 深入理解 iptables 各种表和链.....248	本章小结.....278
本章小结.....250	
	第 19 章 精通 Ansible 实现运维自动化279
第 4 篇 运维自动化和游戏运维	最佳实践 92: 理解 Ansible.....280
	Ansible 安装及原理.....280
第 17 章 使用 Kickstart 完成批量系统安装252	Ansible 原理与架构.....281
最佳实践 85: Kickstart 精要.....252	Ansible 配置项说明.....283
PXE 启动过程及原理.....252	Inventory 定义格式.....284
Kickstart 创建及结构组成.....253	最佳实践 93: 学习 Ansible Playbook 使用要点.....285
pre-installation 与 post-installation 应用实践.....256	Playbook 基本语法和格式.....285
最佳实践 86: 系统配置参数优化.....258	使用 Include、Roles 组织 Playbook.....287
Web 服务器中的参数优化.....259	Ansible 多样的变量定义与使用法则.....290
DB 服务器中的参数优化.....261	最佳实践 94: Ansible 模块介绍及开发.....293
NUMA.....263	Ansible 常用模块介绍.....293
KVM 宿主机中的参数优化.....265	如何开发 Ansible 模块.....294
本章小结.....266	最佳实践 95: 理解 Ansible 插件.....296

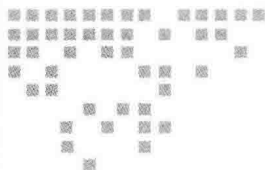
最佳实践 96: Ansible 自动化运维实例: Ansible 自动安装配置 zabbix 客户端... 298 本章小结..... 299	最佳实践 103: 运维体系框架建设..... 315 本章小结..... 316
第 20 章 掌握端游运维的技术要点300	第 21 章 精通手游运维的架构体系 ...317
最佳实践 97: 了解大型端游的技术 架构..... 301 服务器架构设计..... 301 服务器角色说明及通信原理..... 303	最佳实践 104: 推荐的手游架构..... 318 手游和端游运维的异同点..... 318 使用 HTTP 协议的优点..... 318 推荐的网络架构..... 319
最佳实践 98: 理解游戏运维体系发展 历程..... 304	最佳实践 105: 手游容量规划..... 320 机房选择..... 320 网络带宽容量规划..... 321 Web 服务器承载能力规划..... 321 Memcached 承载能力规划..... 322 数据库承载能力规划..... 324 官网论坛访问能力规划..... 325 人数曲线接入..... 325
最佳实践 99: 自动化管理技术..... 305 平台架构与设计原则..... 305 平台功能划分..... 307	本章小结..... 325
最佳实践 100: 自动化监控技术..... 311	
最佳实践 101: 运维安全体系..... 312	
最佳实践 102: 运维服务管理体系..... 314	



第 1 篇 *Part 1*

高性能网站构建

- 第 1 章 深入理解 DNS 原理与部署 BIND
 - 第 2 章 全面解析 CDN 技术与实战
 - 第 3 章 负载均衡和高可用技术
 - 第 4 章 配置及调优 LVS
 - 第 5 章 使用 HAProxy 实现 4 层和 7 层代理
 - 第 6 章 实践 Nginx 的反向代理和负载均衡
 - 第 7 章 部署商业负载均衡设备 NetScaler
 - 第 8 章 配置高性能网站
 - 第 9 章 优化 MySQL 数据库
-



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



注意 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。

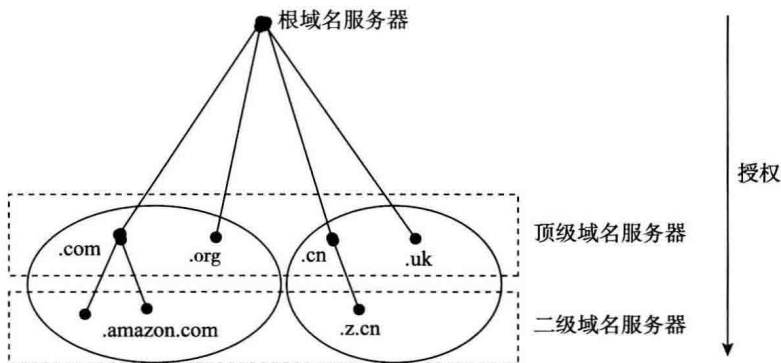


图 1-1 权威域名服务器的授权结构图

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