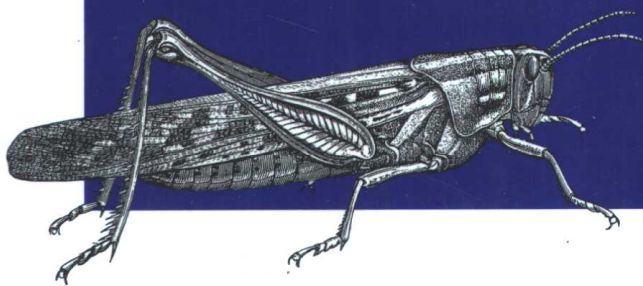


DNS and BIND

第三版
内含 BIND 8



DNS 与 BIND



O'REILLY®
中国电力出版社

Paul Albitz & Cricket Liu 著
雷迎春 陈世林 杨传军 译

DNS 与 BIND

第三版

Paul Albitz & Cricket Liu 著

雷迎春 陈世林 杨传军 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

中国电力出版社

图书在版编目 (CIP) 数据

DNS 与 BIND/ (美) 阿尔比兹 (Albitz, P.)、刘 (Liu, C.) 著; 雷迎春等译. - 北京: 中国电力出版社, 2001. 1

书名原文: DNS and BIND

ISBN 7-5083-0231-1

I .D ... II .①阿 ... ②刘 ... ③雷 ... III .网络服务器 IV .TP393.09

中国版本图书馆 CIP 数据核字 (2000) 第 76726 号

北京市版权局著作权合同登记

图字: 01-1999-3743 号

© 1998 by O'Reilly & Associates, Inc.

Simplified Chinese Edition, jointly published by O'Reilly & Associates, Inc. and China Electric Power Press, 2001. Authorized translation of the English edition, 1998 O'Reilly & Associates, Inc., the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 O'Reilly & Associates, Inc. 出版 1998。

简体中文版由中国电力出版社出版 2001。英文原版的翻译得到 O'Reilly & Associates, Inc. 的授权。此简体中文版的出版和销售得到出版权和销售权的所有者——O'Reilly & Associates, Inc. 的许可。

版权所有, 未得书面许可, 本书的任何部分和全部不得以任何形式重制。

书 名 / DNS 与 BIND

书 号 / ISBN 7-5083-0231-1

责任编辑 / 刘江

技术审校 / 孙国念

封面设计 / Ellie Volckhausen, Hanna Dyer, 张健

出版发行 / 中国电力出版社

地 址 / 北京三里河路 6 号 (邮政编码 100044)

经 销 / 全国新华书店

印 刷 / 北京市地矿印刷厂

开 本 / 787 毫米 × 1092 毫米 16 开本 35.75 印张 580 千字

版 次 / 2001 年 1 月第一版 2001 年 1 月第一次印刷

印 数 / 0001-5000 册

定 价 / 59.00 元 (册)

75083/03

DNS 与 BIND

目录

前言	1
第一章 背景	11
Internet 简史	11
Internet 和 internet	12
域名系统简述	15
BIND 的历史	19
我一定要使用 DNS 吗?	19
第二章 DNS 是如何工作的?	22
域名空间	22
Internet 上的域名空间	28
授权	32
名字服务器和区	33
解析器	38
解析	38
缓存	46

第三章 我该从哪里开始?	49
获得 BIND	49
选择一个域名	53
第四章 建立 BIND	73
我们的域	74
建立 DNS 数据	75
建立一个 BIND 配置文件	88
缩写	91
主机名检查 (BIND 4.9.4 及其后续版本)	96
工具	99
运行一台主名字服务器	100
运行一台辅名字服务器	106
增加更多的域	114
接下来是什么?	114
第五章 DNS 和电子邮件	116
MX 记录	116
邮件交换器到底是什么?	119
MX 算法	121
第六章 配置主机	125
解析器	125
解析器配置示例	137
把损失与不便降到最小	140
与供应商有关的选项	145
第七章 维护 BIND	162
BIND 名字服务器信号	162
更新数据库文件	165

组织你的文件	175
改变 BIND 8 系统文件的位置	180
BIND 8 日志	181
让一切都运行正常	192
第八章 扩展你的域	214
需要多少名字服务器呢?	214
增加更多的名字服务器	223
注册名字服务器	229
更改生存期	232
预防灾难	236
应付灾难	240
第九章 担当父域	245
何时成为父域	246
该有多少子域呢?	246
给子域起什么名字	247
如何成为父域: 创建子域	249
in-addr.arpa 域的子域	262
做个好父域	267
管理子域的迁移	273
父域的生命期	276
第十章 高级特性和安全性问题	277
地址匹配列表和 ACL	278
DNS NOTIFY (区变动通知)	279
DNS 动态更新	283
系统优化	285
名字服务器地址排序	294
更喜欢使用特定网络上的名字服务器	298

用转发器来构造一个大的缓存	299
一种更受限制的名字服务器	301
非递归名字服务器	302
避免使用伪装的名字服务器	304
确保名字服务器的安全	305
镜像服务器间的负载共享	317
第十一章 nslookup	319
nslookup 是一个好工具吗?	319
交互式与非交互式	321
选项设置	322
避免搜索列表	326
常见的任务	326
不太常见的任务	330
nslookup 的故障诊断与排除	339
网络中的无名英雄	345
第十二章 阅读 BIND 的调试输出	347
调试级别	347
打开调试	350
阅读调试输出	351
解析器搜索算法和负缓存	361
工具	363
第十三章 DNS 和 BIND 排错	364
NIS 确实是你的问题吗?	365
故障诊断与排除工具和技术	366
潜在故障列表	373
版本升级后所带来的问题	393
互操作性和版本问题	394
故障症状	398

第十四章 使用解析器和名字服务器的库例程编程	411
用 nslookup 进行 shell 脚本编程	411
用解析器库例程进行 C 编程	418
使用 Net::DNS 进行 Perl 编程	447
第十五章 其他问题	452
使用 CNAME 纪录	452
通配符	457
MX 记录的限制	459
DNS 和 Internet 防火墙	459
拨号连接	482
网络名和网络号	484
其他资源记录	486
DNS 与 X.500	495
DNS 和 WINS	496
附录一 DNS 消息格式和资源记录	499
附录二 在 Sun 主机上编译和安装 BIND	523
附录三 顶级域	526
附录四 域注册表	535
附录五 in-addr.arpa 注册表	540
附录六 BIND 名字服务器和解析器语句	547

前言

到目前为止，你可能对域名系统（Domain Name System，DNS）所知甚少。但是无论何时使用 Internet，你都会用到 DNS。每次你发送电子邮件或是在网上冲浪，你都必须依赖 DNS。

作为人，我们都宁愿记计算机的名字，而计算机却喜欢用数字（即主机 IP 地址）来称呼彼此。在互联网上，这样的地址是一个 32 位的数字，或者说是介于 0 到大约 40 亿之间的一个数字（注 1）。对于计算机来说这是很容易记住的，因为计算机的内存很适合存储数字，而对于我们人来说，这就不那么好记了。真的不好记吗？现在请翻开一本电话簿，任意将一些区号和电话号码连起来。记住它们，就和记住十个任意的互联网络地址差不多难。

这就是我们需要 DNS 的部分原因。DNS 是用于处理方便我们人类使用的主机名字和由计算机来处理的互联网络地址之间的映射。实际上，DNS 是 Internet 上一个标准机制，用来发布和访问有关主机的各种信息，而不只是地址。而且实际上几乎所有的网间互联软件都在使用 DNS，包括电子邮件、远程终端程序如 *telnet*、文件传输程序如 *ftp*，以及 Web 浏览器，如网景的 Navigator 和微软的 Internet Explorer。

注 1：而对于 IP version 6 而言，它很快就会是 128 位长了，或者说是介于 0 到一个 39 位的十进制数字之间。

DNS 另一个重要特性就是它使得从 Internet 上任何地方都能获得主机的信息。将主机信息按照某种格式存成文件，放在某台计算机上，只能对那台计算机的用户有用。DNS 则提供了一种远程检索信息的方式，你能从网络上任何一个地方查找信息。

还不止这些，DNS 使你能对许多场所和机构中的主机信息进行分布式管理。你不需要将数据提交给某个中心，或定期地检索中心的数据库，只保证名字服务器（name server）上称为区（zone）的部分是最新的就行。你的名字服务器会使网络上其他名字服务器都能访问你区中的数据。

因为数据库是分布式的，所以系统还需要能够通过搜索一定的位置来确定要查找的数据在哪里。域名系统使得名字服务器能够很聪明地在数据库之中查找，找到任何区中的数据。

当然，DNS 也有它的问题。例如，为了冗余，系统允许不止一个名字服务器存储一个区的同样的数据。但是这就会导致这些区数据之间的一致性问题。

不过，关于 DNS 最糟糕的问题是，尽管它在 Internet 上广泛使用，但却很少有关于如何管理和维护 DNS 方面的资料。Internet 上大多数管理员使用厂家认为应该提供的资料，再就是从有关这个问题的 Internet 邮件列表和 Usenet 新闻组中搜集到的一些信息。

缺乏资料就意味着，对这种非常重要的互联网络服务——今天 Internet 的关键之一——的理解要么是从一个管理员传授给另一个管理员，就像一个保守严密的家族秘方；要么是从一个个互不相识的程序员和工程师那里重复搜集取得。新的系统管理员重犯着无数人犯过的错误。

我们写这本书的目的就是为了帮助解决这一状况。我们意识到你们当中并非所有人都想成为 DNS 的专家。毕竟，你们中的大多数除了管理一个域（domain）或名字服务器之外还有许多其他事情要做：系统管理、网络工程或软件开发。要一个人只负责 DNS 是完全不可想像的。我们会试着给你足够的信息，让你无论是运行一个小的域还是管理一个跨国的大家伙，无论是负责一个名字服务器还是管理上百个名字服务器，都只做需要做的事。现在你想知道多少，就读多少，如果你想知道更多，可以返回来继续读。

DNS 是个很大的话题 —— 至少大到需要两个作者 —— 但是我们将试着尽可能讲得通俗易懂。头两章是从理论上概述，并且让你了解一些实用的信息，余下来的章节讲的都是核心细节。我们在开始的时候提供了一个路线指南，它根据你的工作或兴趣向你建议适合的阅读路线。

当我们谈到实际的 DNS 软件时，我们主要讲的是 BIND，即 Berkeley Internet Name Domain 软件，它是 DNS 规范的一种最为常见的实现（也是我们所知道的最好的）。我们力图在本书中精心提炼我们在用 BIND 管理和维护域当中的经验 —— 顺便说一句，这个域可能是 Internet 上最大的一个（不是吹牛，我们有这样的把握）。只要有可能，我们会给出在管理中实际用到的程序，为了速度和效率，其中许多都用 Perl 进行了重写。

如果你还是个生手的话，我们希望这本书能帮助你熟悉 DNS 与 BIND，如果你已经熟悉了 DNS，我们希望它能增进你的理解。即使你对 DNS 已经了如指掌，我们还是希望能提供一些有价值的理解和经验。

版本

这本书主要是讲新的 8.1.2 版的 BIND，同时也涉及了早一点的 4.9 版。虽然 8.1.2 是我们撰写这本书时最新的 BIND 版本，但许多供应商的 UNIX 版本中还不包括它，部分是由于 8.1.2 只是最近才刚刚发布，同时许多供应商对于使用这么新的软件还很谨慎。我们也会偶尔提到其他版本的 BIND，特别是 4.8.3 版，因为许多供应商的 UNIX 产品中包括的代码还是基于这个较老版本的 BIND 的。要是特性只适用于 4.8.3、4.9 或者 8.1.2 版，或者在不同版本的使用情况有所不同的话，我们将会指出不同版本的不同使用情况。

我们在例子中大量使用了 *nslookup* 这种名字服务器实用程序。我们所使用的 *nslookup* 的版本是随同 BIND 8.1.2 代码一起提供的。较早版本的 *nslookup* 也提供了 8.1.2 中 *nslookup* 大部分的功能，不过并非全部。在例子中，我们尽量使用对大多数 *nslookup* 都通用的命令；如果无法做到这一点，我们会注明的。

组织

本书或多或少是按照域和域管理员的发展历程来组织的。第一、二章讨论了域名系统理论。第三章到第六章帮助你决定是否建立你自己的域，还讲述了如果你选择建立自己的域，又该如何来做。中间的几章，第七章到第十章讲的是如何维护你的域，如何配置主机以使用你的名字服务器，如何规划你的域扩展，以及如何创建子域。最后几章，第十一章到第十五章，讲述一些排错工具和常见问题，以及使用解析器库例程编程的技术和技巧。

下面是每一章更详细一些的介绍：

- 第一章“背景”，提供了一些历史资料，讨论了导致DNS发展的问题，然后又概述了DNS理论。
- 第二章“DNS是如何工作的？”，更详细地回顾了DNS理论，包括DNS名字空间、域和名字服务器。我们还介绍了一些很重要的概念，像名字解析（name resolution）和缓存（caching）。
- 第三章“我该从哪里开始？”，谈到了如果你还没有DNS软件的话，该如何获取BIND，以及一旦你得到了又该怎么办：如何确定你的域名是什么，以及如何同域的授权组织联系。
- 第四章“建立BIND”，详细介绍了如何建立你的头两个BIND名字服务器，包括创建你的名字服务器数据库、启动你的名字服务器和检查它们的操作。
- 第五章“DNS和电子邮件”，讲的是DNS的MX记录，它允许管理员指定别的主机来处理发往给定目的主机的邮件。这一章涉及了对各种网络和主机的邮件路由策略，包括有安全防火墙的网络和没有直接连到Internet的主机。
- 第六章“配置主机”，解释了如何配置一个BIND解析器（resolver）。我们还将注明许多常见UNIX厂商的解析器实现的特性，同时还会谈到Windows 95和NT的解析器。
- 第七章“维护BIND”，讲述了为保证一个域的平稳运行管理员所需要做的定期维护的工作，如检查名字服务器是否正常，以及它的授权情况。

- 第八章“扩展你的域”，涉及的是如何规划扩大和发展你的域，包括如何扩大和如何为移动和出错做准备。
- 第九章“担当父域”，探索了成为父域的乐趣。我们解释了何时成为一个父域（创建子域），如何命名你的子域，如何创建它们，以及如何监视它们。
- 第十章“高级特性和安全性问题”，讲述了一些较少用到的名字服务器配置选项，它们能帮助你优化你的名字服务器的操作，使你的名字服务器更安全，还能使你的管理更轻松。
- 第十一章“nslookup”，详细介绍了最常用的调试 DNS 的工具，包括挖掘远程名字服务器给出的模糊信息技术。
- 第十二章“理解 BIND 调试的输出”，这些输出开始时就像是罗赛塔石碑上的文字（译注 1）那样神秘。这一章将会有助于你理解那些 BIND 显示的神秘信息的意义，从而使你能更好地了解你的名字服务器。
- 第十三章“DNS 和 BIND 疑难排错”，涉及了许多常见的 DNS 和 BIND 问题及其解决方法，而且还讲述了一些不太常见、较难诊断的情况。
- 第十四章“用解析器和名字服务器库例程编程”，演示了如何在一个 C 程序中使用 BIND 的解析器例程，来查询名字服务器并从中检索数据。我们还包括了一个有用的程序（希望如此！），它可以用来检查你的名字服务器正常与否以及授权情况。
- 第十五章“其他问题”，将所有松散的头绪连在一起。我们讲到了 DNS 通配符、通过防火墙连接到 Internet 网络的特殊配置、通过拨号断断续续地连接到 Internet 的主机和网络、网络名字编码，还有新的试验性的记录类型。
- 附录一“DNS 消息格式和资源记录”，包括一个字节一个字节地分解了 DNS 查询和响应中使用的格式，另外还有当前定义的资源记录类型的综合列表。
- 附录二“在 Sun 主机上编译和安装 BIND”，包含了关于如何在 Solaris 2.X 上编译和安装 8.1.2 版 BIND 的一步一步的指令。

译注 1：罗赛塔碑是 1798 - 1799 年拿破仑远征埃及期间，法军发现的埃及古碑。由于碑文同时刻有古埃及象形文字、通俗体文字和希腊文，它成为法国古文字学家商博良破译古埃及象形文字的关键线索。

- 附录三“顶级域”，列出了目前 Internet 域名空间中的顶级域名。
- 附录四“域注册表”，是目前申请建立一个由 InterNIC 运行的子域的表格。
- 附录五“in-addr.arpa 注册表”，是 American Registry for Internet Numbers 目前申请建立一个 *in-addr.arpa* 域的子域的表格。
- 附录六“BIND 名字服务器和解析器语句”，总结了用来配置名字服务器和解析器的每一个参数的语法和语义。

读者

本书主要是为管理一个域和一个或多个名字服务器的系统管理员而写的，但是它也适合于网络工程师、邮件管理员以及其他一些人。不过，不同的读者对各个章节的兴趣大小并不一样，你不一定要读完所有的十五章才找到与你工作相关的信息。我们希望下面的阅读指南能帮助你找到自己的阅读路线。

第一次建立自己域的系统管理员要了解 DNS 的理论，应该读第一、二章；要了解开始和选择一个好域名，应该读第三章；要学习第一次如何建立域，应该读第四章和第五章。第六章解释了如何配置主机来使用新的名字服务器。接下来他们就该读第七章了，这一章介绍了如何通过建立其他的名字服务器和添加附加数据，使他们的域“有血有肉”。然后是第十一、十二和十三章，讲述了排错工具和技术。

有经验的管理人员读读第六章，能够学习如何在不同的主机上配置 DNS 解析器，读第七章能学习维护域方面的知识。第八章包含有如何为域的扩大和发展做准备，这对于大域的管理人员更有价值。第九章解释了成为父域——创建子域——这对考虑要进行大的移动的管理员来说是很应该看一看的。第十章涉及了新的 BIND 8.1.2 名字服务器的安全特性，其中许多对有经验的管理人员来说是很有用的。第十一到十三章描述了排错的工具和技术，即使是对高级管理人员来说也是值得一读的。

没有完全连接到 Internet 的网络的系统管理员应该读一读第五章，学习一下如何在这类网络上配置邮件，还应该读一读第十五章，学习一下如何建立一个独立的 DNS 基础设施。

程序员应该读一下第一、二章，了解一下 DNS，然后是第十四章，其中详细介绍了如何使用 BIND 解析器库例程编程。

不直接负责域的网络管理员还是应该读一下第一、二章，了解一下 DNS 理论，然后是第十一章，学习如何使用 nslookup，及第十三章，学习排错技巧。

邮件管理员应该读第一、二章，了解一下 DNS 理论，还有第五章，学习 DNS 和电子邮件是如何共存的。第十一章描述了 *nslookup*，这将有助于邮件管理员从域名空间中挖掘出邮件路由信息。

感兴趣的读者可以读一读第一、二章，学习 DNS 理论，除此之外，想读什么就读什么吧！

注意，我们假设你很熟悉基本的 UNIX 系统管理以及 TCP/IP 网络工作原理，并能够使用简单的 Shell 脚本和 Perl 来编程。除此之外，我们不要求您有任何其他专业的知识。当我们提到一个新的术语或概念的时候，我们会尽力定义或解释的。只要可能，我们将与 UNIX（以及现实世界）相比较，来帮助你理解。

获取示例程序

本书中的示例程序可以通过 *ftp* 从下面的网址获得：

```
ftp://ftp.uu.net/published/oreilly/nutshell/dnsbind/dns.tar.Z
```

```
ftp://ftp.ora.com/published/oreilly/nutshell/dnsbind/dns.tar.Z
```

无论你从何处下载，都要输入以下命令来解开压缩文件：

```
% zcat dns.tar.Z | tar xf -
```

系统 V 中则要求输入下面的 tar 命令：

```
% zcat dns.tar.Z | tar xof -
```

如果你的系统上没有 *zcat*，可以分别使用 *uncompress* 和 *tar* 命令。

如果你不能直接通过 Internet 得到这些例子，但可以收发邮件，你可以用 *ftpmail* 来获取它们。要想知道如何使用 *ftpmail*，发送电子邮件到 *ftpmail@online.oreilly.com*，不用写主题，只用在正文中写一个单词“help”。

本书中所使用的约定

我们用下面所示的字体和格式惯例来表示 UNIX 命令、工具和系统调用：

- 脚本或配置文件的摘录以固定宽度的字体来显示：

```
if test -x /etc/named -a -f /etc/named.conf
then
    /etc/named
fi
```

- 简单的交互式会话的例子，命令行输入和相应的输出，是以固定宽度的字体来显示的，其中需要用户输入的用黑体显示：

```
% cat /etc/named.pid
78
```

- 如果命令必须由超级用户输入，那么我们在前面使用 # 符号：

```
# /etc/named
```
- 当命令行正好作为用户输入出现时，如果在段落中就用斜体表示。例如：运行 *ls* 来列出一个目录中的文件。
- 当域名在段落中出现时也用斜体表示。
- 在一段文字中出现的 UNIX 命令（只是随便提到，而不是作为命令行的一部分时）和 UNIX 联机手册，也用斜体表示。例如：想找到关于 *named* 的更多信息，用户可以求助于 *named* (1m) 的联机手册。
- 文件名用斜体印刷；例如：BIND 名字服务器的配置文件通常是 */etc/named.conf*。