HZ BOOKS
华章IT

MANNING

Linux/Unix
技术丛书

Linux IN ACTION

Linux实战

[美] 戴维·克林顿（David Clinton） 著
张凯龙 王路阳 李鹏 等译

通过12个实际项目带你精通Linux系统安全、管理与运维

机械工业出版社
China Machine Press

Linux 实战

LINUX IN ACTION

[美] 戴维·克林顿（David Clinton）著

张凯龙 王路阳 李鹏 等译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Linux 实战 /（美）戴维·克林顿（David Clinton）著；张凯龙等译 . —北京：机械工业出版社，2019.4
（Linux/Unix 技术丛书）
书名原文：Linux in Action

ISBN 978-7-111-62704-3

I. L… II. ①戴… ②张… III. Linux 操作系统 IV. TP316.85

中国版本图书馆 CIP 数据核字（2019）第 086811 号

本书版权登记号：图字 01-2018-5316

Linux 实战

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：赵 静 责任校对：殷 虹
印 刷：中国电影出版社印刷厂 版 次：2019 年 7 月第 1 版第 1 次印刷
开 本：186mm×240mm 1/16 印 张：21.75
书 号：ISBN 978-7-111-62704-3 定 价：109.00 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）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 读者信箱：hzit@hzbook.com

作者简介

戴维·克林顿（David Clinton）是一名系统管理员、教师及作家。他已经为很多重要的技术主题撰写和创建了培训资料，涉及Linux系统、云计算（特别是AWS）以及诸如Docker等容器技术。他是《Learn Amazon Web Services in a Month of Lunches》（Manning，2017）一书的作者。在网站https://www.pluralsight.com/可以找到他的许多视频培训课程。同时，可以在https://bootstrap-it.com找到他编著的其他书籍（关于Linux管理及服务器虚拟化）的链接。

译者简介

张凯龙 博士、博士后（法国），西北工业大学计算机学院副教授，主要研究方向为嵌入式系统、群智能协同系统等。现任西北工业大学——巴黎高科MINES机器人与群智能系统联合实验室主任、CCF嵌入式系统专委会副秘书长、陕西网络创新研究院副院长，曾被评为第二届中国嵌入式系统十大杰出青年。

王路阳 博士，长安大学信息工程学院讲师，主要研究方向为无线传感器网络、车联网路由协议等。曾在美国克莱姆森大学电子与计算机工程学院学习，于2017年获电子工程博士学位。现为陕西省重点科技创新团队“泛在交通信息服务理论与技术团队”成员。

李鹏 航空工业计算所研究员、副所长、硕士生导师，西北工业大学在读博士生，主要研究方向为嵌入式系统、计算机系统结构等。曾获省部级、航空工业集团级科技成果奖二十余项，“中央企业青年创新奖”铜奖、“航空工业首届青年创新奖”金奖，曾被授予“陕西国防科技工业系统十大杰出青年”“中国航空学会青年科技奖”等荣誉称号。

The Translator's Words 译 者 序

Linux 是 IT 领域中尽人皆知的著名开源操作系统，其设计体系完善、运行性能突出，受到全球各地技术企业与技术爱好者的青睐。Linux 继承了 UNIX 的设计思想，在全球的服务器、PC 市场中得到了广泛应用，并形成了 Red Hat 和 Debian 两大版本家族以及 Ubuntu、CentOS、Mint、Kali Linux 等诸多不同版本。同时，鉴于良好的结构设计以及源码级的可定制、可扩展特性，面向物联网和嵌入式装备的 Linux 演化版本也不断涌现，Android、MontaVista、μClinux 等已占据了嵌入式操作系统市场的半壁江山。优秀的设计思想、开放的源码体系、多元的产品形态以及巨大的应用市场使 Linux 在诞生后的近 30 年里受到了政府、企业、高校等各界的持续关注与追捧。

Linux 将在很长一段时间内继续蓬勃发展并广泛应用。用作者的话讲，就是：“Linux 技能具有持久性。由于 Linux 是一个特别成熟和稳定的操作系统，25 年前使用的大多数工具至今仍然在使用，而且，当今使用的大量工具在 25 年后也将有可能继续发挥作用。”因此，我们有必要继续拓展对 Linux 的学习，并且要从不同的维度进行学习。本书即以此为出发点。本书的特点在于，未采用以知识线索来组织内容这一典型方式，而是基于一组实践项目来进行阐述。换句话说，本书将实践项目作为基本教学对象。作者挑选了一组具有代表性的实践项目，在实践步骤中穿插引用相关的 Linux 理论、原理、方法和命令，从而让读者在付诸实践行动的过程中进行有效的学习，掌握方法、汲取知识。想必这就是作者为本书取名为《Linux in Action》的本意了，Action 一词就是要读者付诸行动，要“Learning by doing”。

从本书的目录可知，除了序和第 1 章之外，每一章都有非常具体且相互独立的主题，重点涵盖了 Linux 的运用，特别是突出了网络及安全的特性。下面对本书各章的主要内容进行简要描述。

第 1 章是概述性的内容，帮助读者熟悉或回顾 Linux 的基本知识。

第 2 章阐述 Linux 虚拟化技术以及 Linux 工作环境的基本构建方法，这也是后续章节的基础性技术知识。

第 3 章关注如何用密钥保护远程连接，实现对联网计算机的安全访问。

第 4 章讨论文件归档管理的目的和典型方法。有效保护数据也是安全性的重要方面之一。

第 5 章是前一章的递进，主要关注如何配置并实现自动的异地备份。自动化管理可以大大提高备份的效率和可靠性。

第 6 章关注如何从损坏的 Linux 系统中进行有效的恢复，这种技能对于每一位 Linux 管理员而言都是必需的。

第 7 章展示如何用 Apache、SQL 及 MediaWiki 等软件包搭建一个支持知识管理及自由协作的 MediaWiki 服务器。

第 8 章列举建立一个 Nextcloud 文件共享服务器的步骤，并给出基于云的存储部署方法。

第 9 章将保护 Web 服务器作为实践项目，循序渐进地阐述如何使用访问控制、加密传输、强化认证等方式系统地达成增强安全性的目标。

第 10 章着重讨论如何通过创建 VPN 或 DMZ 来保护网络，这对于全球化部署的大型企业尤为重要。

第 11 章围绕对系统运行进行监视的需求，讨论如何使用、管理和处理系统日志，以及如何使用工具建立入侵检测系统。

第 12 章阐述如何在私有网络上通过网络文件系统进行数据共享，以及如何保证其安全性。

第 13 章聚焦于系统性能的优化，阐述测量和解决 CPU、内存、存储、网络等不同方面性能问题的方案，以及可用的工具。

第 14 章列举与网络连通性相关的各种故障，并给出解决方案及工具的使用方法。

第 15 章以具体的实例说明如何通过对 Linux 内核模块、引导参数、驱动程序等的管理来解决遇到的设备故障。

第 16 章讨论如何使用 DevOps 工具构建和部署一个脚本化的服务器环境，从而实现自动化的资源及安全性管理等。

总结部分对本书的内容进行梳理和重新组织，并为读者给出下一步学习的建议。

附录部分对每章的命令行进行了集中回顾，这些内容也存在于每章的末尾，如此安排是为了便于读者快速查阅。

在翻译本书的过程中，译者们对作者的写作风格达成了共同的认识。内容中，作者采用了大量比喻、隐喻的写作方法并创造了一些新词，而非我们习惯的科技术语及内容表述方式。这使得本书内容看上去非常生动，但实际上也给我们的翻译工作带来了很大挑战。因此，看似熟悉的 Linux 内容，却常常会让译者们绞尽脑汁。例如，第 14 章中有这么一句话，“ It’s roll-up-your-sleeves-and-pull-out-the-drain-snake time”。那么，其中的“ pull-out-the-drain-snake”指什么？结合上下文以及生活常识，我们知道 drain-snake 是管道疏通器（而非“管道蛇”），随后看到 Traceroute 工具才确定它指的是连通性查看工具。类似的问题还有很多，不再一一赘述。所幸，我们这个跨院校的翻译团队中的每位成员都很好学，也

乐于互相帮助。在遇到问题时，我们常常会激烈地争辩和讨论，从而以认真的态度完成了本书的翻译工作。当然，鉴于译者们水平有限，译稿中难免有疏漏、谬误之处，敬请各位读者批评指正（联系邮箱：kl.zhang@nwpu.edu.cn）。

在整个翻译过程中，张凯龙翻译了文前、第 1～4 章、第 15 章和总结部分；王路阳翻译了第 5～7 章；李鹏翻译了第 9～10 章；李刘洋翻译了第 8 章和第 11 章；费超翻译了第 12～13 章；谢尘玉翻译了第 14 章；巩政翻译了第 16 章。张凯龙对全书进行了修改润色，统稿整理。

在此，感谢所有译者的辛勤付出和共同努力！感谢王雨佳、谢策、李孝武等课题组研究生以及所有译者在校稿阶段认真且富有成效的检查和修订，这大大提升了译稿的品质。感谢机械工业出版社华章公司王春华编辑、赵静编辑给予的大力支持！

感谢关心、支持我们的所有亲人和朋友！

张凯龙

2019 年 1 月 7 日于西安

前　言 *Preface*

不论你在 IT 领域或者编程世界中从事什么工作或者已经从事了多久，如果你不学习新东西，就会遇到新问题。这不仅仅是因为平台和范例在持续发生变化，因为新的业务需求需要新的思想，或者因为那些不怀好意的家伙正在不断想出新的办法来攻击你的服务器。原因远远不只这些。停止学习的代价你根本承担不起。关键是要找到一种方法来学习高优先级的技能，而不是守着经验兜圈子。

我的意图和期望在于，通过阅读本书，哪怕是只读了一章，你也能有足够的信心去承担具有挑战性和创造性的工作，也就是那些你之前没有考虑过的事情。如果能一直坚持读到最后，你将学会使用那些支持虚拟化、灾难恢复、基础设施安全、数据备份、Web 服务器、DevOps 以及排除系统故障等关键和流行的技术。

但为什么使用 Linux 呢？因为 Linux 支持大部分的互联网、科学研究以及商业运营——实际上，支持世界上大部分的服务器。那些服务器需要被聪明且接受过良好训练的人员有效地进行配置、启动、保障和管理。聪明是你的天赋，而我能做的是帮助你得到良好的训练。

不确信自己是否拥有足够的 Linux 知识来开始这样一个雄心勃勃的计划吗？第 1 章将很快回答这个问题。之后，请系好你的安全带并准备好面对一段严肃的学习旅程吧。

致谢

撰写一本书时，必须仔细考虑方方面面的情况，否则就不可能度过漫长且时而令人受尽折磨的写作时光并完成写作。就本书来说，如同我写作《Learn Amazon Web Services in a Month of Lunches》时一样，完成这项工作需要 Manning 团队每个环节的工作人员的才华和奉献精神。

再一次说明，Frances Lefkowitz 作为一名策划编辑，为每一章设立了清晰的定位和目标，坚持不懈地让我专注其中并走上正轨。Reka Horvath 和 John Guthrie 耐心地测试了本书中的所有项目并在此过程中给出了有价值的操作建议。文字编辑 Frances Buran 似乎从未遇到过她能认可的副词，至少在我这里如此。但是，目前的书中，字里行间的准确性和优雅

度清楚地说明了她的工作质量。

作为项目主管，Deirdre Hiam 有效地指导我们走完最后一英里[⊖]，并成功地让各个部分同步运转。本书的每一位同行评审人员也都做出了重要贡献。他们可能没有意识到，但是他们所有的宝贵建议都被仔细地分析和权衡，而且，只要可能，就都会被采纳。因此，非常感谢 Angelo Costo、Christopher Phillips、Dario Victor Duran、Flayol Frederic、Foster Haines、George L. Gaines、Gustavo Patino、Javier Collado、Jens Christian B. Madsen、Jonas Medina de los Reyes、Maciej Jurkowski、Mayer Patil、Mohsen Mostafa Jokar 和 Tim Kane。

相较 Linux 管理技能而言，本书的内容更为丰富。要想成为一名成功的管理员，面对自己负责的服务器和系统，应当具备更强的责任感。我非常幸运能在担任 Linux 系统管理员的职业生涯之初，就从一位伟大的导师那里受益良多。Peter Fedorow 对良好运营的细节以及全局大势的关注让他成为一名特别高效的管理员。他把我带进 Linux 虚拟化的世界，甚至没等那些容器冷却下来，它们就把我吸引住了。虽然一切都说完了、做完了，但毋庸置疑，Peter 对我的影响力依然还在。

最后，如果没有我的妻子愉快的参与和帮助，我的任何专业（或私人）项目都不会顺利完成。我们充分分担着这项艰苦的工作，但成功主要归功于她。

关于本书

你正在期望学习管理 Linux 计算机吗？这是一个很好的选择。虽然 Linux 常常驻留于消费者的桌面计算机上，但它同时也是服务器领域的绝对主宰，特别是虚拟服务器和云服务器。鉴于现在大多数严格的服务器管理都是远程实施的，通过某个这样或那样的 GUI 进行工作只会增加无谓的开销。如果你打算管理当前引人关注的服务器和网络体系架构，你将不得不围绕 Linux 的命令行展开学习。

一个好消息是，核心 Linux 命令集可以实现跨地域和跨公司的运行，你可以仅关注计算机与业务相交的那些地方。一个更好的消息是，相对而言，Linux 技能具有持久性。因为它是一个特别成熟和稳定的操作系统，25 年前使用的大多数工具至今仍然在使用，而且，当今使用的大量工具在 25 年后也将可能继续发挥作用。换句话说，学习 Linux 将是一生的投资。

但是你非常繁忙，工作堆积如山。好吧，我不能保证掌握 Linux 与学会系鞋带一样简单。但是我可以帮助你像激光一样进行聚焦，从而将那些不需要的东西都扔到公路上去，让它们窒息在你开车驶过后留下的尾气中（当然，得假设你驾驶的不是一辆特斯拉，因为特斯拉是纯电动汽车）。

我将如何实现这一点呢？本书不采用技术培训的讲授方式。也就是说，虽然其他的书籍、课程及在线资源都围绕常规主题来组织内容（好了，孩子们，拿出你们的尺和笔，今天我们将学习 Linux 文件系统），但我却将基于现实生活中的一组项目来进行讲授。

⊖ 1 英里＝1609.344 米。——编辑注

例如，我本可以基于 Linux 文件系统构建完整的一章（或两章）。但本书并未按照这种方式处理，相反，你将学习如何构建企业文件服务器、系统恢复盘以及用来复制关键数据归档文件的脚本等。在这个过程中，你将会顺带学习文件系统的知识，这是本书提供的免费红利。

请不要认为我会覆盖 Linux 管理的所有工具。那是不可能的，毫不夸张地说，这样的工具有成千上万个。但也不用担心。本书将涵盖 Linux 管理员职业生涯早期所需掌握的核心技能，并且只有当实际的关键项目需要某些技能时，才会做有针对性的介绍。读完本书后，你能学到的将比基于传统资源所能学到的更多。你将学会如何掌控十几个主要的管理项目，而且能够轻松地处理更多的项目。

现在你有所了解了吗？我想是的。

读者对象

本书的目的是让你获得一系列可靠的 Linux 管理技能。也许你是一位开发者，更希望直接在驻留应用程序的服务器环境工作。或者，也许你已经准备好在服务器管理或 DevOps 领域开展工作。不论怎样，你就是我们中的一员。

你应该拥有什么基础知识呢？你至少应该能轻松地使用文件、网络及现代操作系统资源来进行工作。系统管理、网络管理与编程语言方面的经验肯定没有坏处，但不是必需的。最为重要的是，你应该不畏惧探索新的环境，并有试用新工具的热情。另一件事情是，期望你知道如何进行简单、直接的 Linux 操作系统的安装。

内容组织

这里简要给出本书的组织方式。除了第 1 章之外，本书的每一章都包括一个或两个实际项目。鉴于第 1 章的内容主要用来填补你的 Linux 知识体系中可能存在的基础知识空白，因此其组织形式与其他章节有所不同。不需要这些基础知识吗？我敢肯定你在第 2 章就能找到很多有趣的新玩具。

伴随本书中的这些项目，我还将介绍你需要掌握的技能和工具。另外，每章中的项目通常都是基于之前章节所学习的技能来构建的。为了清楚地表述我的意思，这里给出一个非常完整的列表，其中分章列出了你将在本书中碰到的技能范畴及工具。

章　节	技能范畴	工　具
第 1 章	Shell、分区及文件系统	Bash、man
第 2 章	虚拟化、文件系统	VirtualBox、LXC、apt、yum/dnf
第 3 章	安全性、远程连接	ssh、scp、systemctl、ps、grep
第 4 章	分区、文件系统及文本流	tar、dd、redirects、rsync、locate、split、chmod、chown

（续）

章　节	技能范畴	工　具
第 5 章	脚本、系统进程管理与安全性	脚本、cron、anacron、systemd 定时器
第 6 章	分区、文件系统及设备管理	parted、GRUB、mount、chroot
第 7 章	数据库、网络、包管理	PHP、MySQL(MariaDB)、Apache Web 服务器、包依赖性
第 8 章	包管理、网络及安全性	snapd、文件系统、加密
第 9 章	网络、安全性、系统监控	Apache、iptables、/etc/group、SELinux、apt、yum/dnf、chmod、chown、Let's Encrypt
第 10 章	网络与安全性	firewalls、ssh、Apache、OpenVPN、sysctl、easy-rsa
第 11 章	系统监控、文本流及安全性	grep、sed、journalctl、rsyslogd、/var/log/、Tripwire
第 12 章	网络、分区及文件系统	nfs、smb、ln、/etc/fstab
第 13 章	系统监控、系统进程管理与网络	top、free、nice、nmon、tc、iftop、df、kill、killall、uptime
第 14 章	网络	ip、dhclient、dmesg、ping、nmap、traceroute、netstat、netcat (nc)
第 15 章	设备管理	lshw、lspci、lsusb、, modprobe、CUPS
第 16 章	脚本、虚拟化	Ansible、YAML、apt

关于代码

本书中，代码清单和普通文本行中包括大量的源代码示例。在这两种情况下，源代码都被设置为代码体，以区别于常规的文本内容。

很多情况下，我调整了原有源代码的格式，增加了换行符并重置了缩进符以适应可用的页面空间。在极少数情况下这种方法还不够用，代码中还会包括续行符标记（➥）。另外，当在文字中描述一段源代码时，通常会从清单中移除该段代码的注释。很多清单中都有代码注释，以突出一些重要的概念。

Linux 发行版本

当前在有效维护的 Linux 发行版本有很多。对于所有 Linux 发行版本而言，大多数的基础都是相同的，但总有一些版本是能够在“这里”运行而不能够在“那里”运行的。出于实践性的目的，我将主要聚焦于两个版本：Ubuntu 和 CentOS。为什么是这两个版本呢？因为这两个版本代表了不同的版本系列。Ubuntu 与 Debian、Mint、Kali Linux 及其他版本是同源的，而 CentOS 则与红帽（Red Hat）企业 Linux 和 Fedora 同源。

这并不是说我不重视 Arch Linux、SUSE 以及 Gentoo 等其他发行版本，或者说你在本书中学到的东西对在其他版本的环境中开展工作没有帮助。但是，对 Ubuntu 和 CentOS 的完全覆盖意味着抓住了 Linux 馅饼中最大的那一块，我仅使用这两个版本就可以达到这个目标。

本书的论坛

欢迎访问 Manning 出版公司运营的网络论坛，在该论坛中你可以对本书进行评论、提出技术问题并获得来自作者和其他用户的帮助等。你可以通过链接 https://forums.manning.com/forums/linux-in-action 访问该论坛。你也可以通过链接 https://forums.manning.com/forums/about 了解 Manning 论坛及其管理规则。

Manning 对广大读者的承诺是，在读者之间以及读者与作者之间提供一个进行有意义对话的平台。这并非对作者具体参与度的任何承诺，他们对论坛的贡献是自愿的（而且是免费的）。我们建议大家向作者咨询一些有挑战性的问题，以免他丧失了兴趣！只要本书还在发行，你就可以在出版商的网站上访问该论坛以及之前讨论的内容。

其他在线资源

遇到问题了吗？网络搜索是你最好的朋友，因为它可以快速地将你与现有的 Linux 指南、排除故障的专业知识关联到一起。但是，你不该忘记 StackExchange 系列网站，特别是 serverfault.com。如果某个系统配置出现了错误或者网络已经丢失，那么其他人已经遇到过相同问题的概率会很高，可能有人已经在 ServerFault 上问过这个问题并得到了答案。找不到任何答案吗？那么请自己留言提问。LinuxQuestions.org 和 ubuntuforums.org 也会很有帮助。

同时，喜欢视频培训的用户将在 Pluralsight.com 上找到范围非常广泛的 Linux 课程，其中包括了十多门我自己的课程。

Contents 目　录