

O'REILLY®

TURING

图灵程序设计丛书



Docker 开发指南

Using Docker

注重实践、全面实用, 让Web应用的开发、测试和部署更简便快捷

[英] Adrian Mouat 著
黄彦邦 译



中国工信出版集团



人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

Docker开发指南

Using Docker

Developing and Deploying Software with Containers

[英] Adrian Mouat 著

黄彦邦 译



O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo

O'Reilly Media, Inc. 授权人民邮电出版社出版

人民邮电出版社

北 京

图书在版编目 (C I P) 数据

Docker开发指南 / (英) 阿德里安·莫阿特
(Adrian Mouat) 著 ; 黄彦邦译. -- 北京 : 人民邮电出
版社, 2017.4

(图灵程序设计丛书)

ISBN 978-7-115-44957-3

I. ①D… II. ①阿… ②黄… III. ①Linux操作系统
—程序设计 IV. ①TP316.85

中国版本图书馆CIP数据核字(2017)第036596号

内 容 提 要

Docker 容器轻量和可移植的特性尤其适用于动态和分布式的环境, 它的兴起给软件开发流程带来了一场革命。本书对 Docker 进行了全面讲解, 包括开发、生产以至维护的整个软件生命周期, 并对其中可能出现的一些问题进行了探讨, 如软件版本差异、开发环境与生产环境的差异、系统安全问题, 等等。

本书适合软件开发、运维工程师和系统管理员, 尤其是对 DevOps 模式感兴趣的读者。

◆ 著 [英] Adrian Mouat

译 黄彦邦

责任编辑 朱 巍

执行编辑 温 雪

责任印制 彭志环

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号

邮编 100164 电子邮件 315@ptpress.com.cn

网址 <http://www.ptpress.com.cn>

北京昌平百善印刷厂印刷

◆ 开本: 800 × 1000 1/16

印张: 18

字数: 425千字

2017年4月第1版

印数: 1 - 3 500册

2017年4月北京第1次印刷

著作权合同登记号 图字: 01-2017-0541号

定价: 79.00元

读者服务热线: (010)51095186转600 印装质量热线: (010)81055316

反盗版热线: (010)81055315

广告经营许可证: 京东工商广字第 8052 号

站在巨人的肩上
Standing on Shoulders of Giants



iTuring.cn

O'Reilly Media, Inc.介绍

O'Reilly Media 通过图书、杂志、在线服务、调查研究和会议等方式传播创新知识。自 1978 年开始，O'Reilly 一直都是前沿发展的见证者和推动者。超级极客们正在开创着未来，而我们关注真正重要的技术趋势——通过放大那些“细微的信号”来刺激社会对新科技的应用。作为技术社区中活跃的参与者，O'Reilly 的发展充满了对创新的倡导、创造和发扬光大。

O'Reilly 为软件开发人员带来革命性的“动物书”；创建第一个商业网站（GNN）；组织了影响深远的开放源代码峰会，以至于开源软件运动以此命名；创立了 *Make* 杂志，从而成为 DIY 革命的主要先锋；公司一如既往地通过多种形式缔结信息与人的纽带。O'Reilly 的会议和峰会集聚了众多超级极客和高瞻远瞩的商业领袖，共同描绘出开创新产业的革命性思想。作为技术人士获取信息的选择，O'Reilly 现在还将先锋专家的知识传递给普通的计算机用户。无论是通过图书出版、在线服务或者面授课程，每一项 O'Reilly 的产品都反映了公司不可动摇的理念——信息是激发创新的力量。

业界评论

“O'Reilly Radar 博客有口皆碑。”

——*Wired*

“O'Reilly 凭借一系列（真希望当初我也想到了）非凡想法建立了数百万美元的业务。”

——*Business 2.0*

“O'Reilly Conference 是聚集关键思想领袖的绝对典范。”

——*CRN*

“一本 O'Reilly 的书就代表一个有用、有前途、需要学习的主题。”

——*Irish Times*

“Tim 是位特立独行的商人，他不光放眼于最长远、最广阔的视野，并且切实地按照 Yogi Berra 的建议去做了：‘如果你在路上遇到岔路口，走小路（岔路）。’回顾过去，Tim 似乎每一次都选择了小路，而且有几次都是一闪即逝的机会，尽管大路也不错。”

——*Linux Journal*

献给那些不计成败、勇于尝试的人们。

前言

容器是轻量且可移植的仓库，包含应用程序及其依赖的组件。

诚然，这个描述有点枯燥乏味。不过，若使用恰当，容器对开发流程的改进将会是革命性的。容器使新的软件架构和 workflows 成为现实，这股吸引力难以抵挡，仿佛所有大型 IT 公司在一年里都从对 Docker 或容器闻所未闻转为积极研究，甚至已经付诸实践。

Docker 的兴起实在令人惊讶，我印象中没有任何一种技术像它那样，对 IT 产业产生了这么迅速而又深远的影响。我尝试用这本书来帮助你了解容器为什么重要、采用容器技术的好处是什么，以及最重要的是怎样着手使用它。

目标读者

本书试图全面地讲解 Docker，解释使用 Docker 的原因，示范使用方法，以及如何与软件开发流程相结合。本书的内容包括开发、生产以至维护的整个软件生命周期。

本书假设读者只具备 Linux 和软件开发的基础知识，主要的目标读者为软件开发人员、运维工程师以及系统管理员（尤其是考虑往 DevOps 方向发展的管理员），而技术型管理者和技术爱好者也能从中受益。

写作目的

Docker 刚迅速兴起的时候，我就有幸知道它，并开始使用。当有机会写作这本书时，我毫不犹豫地抓住了它。假如拙作可以让部分读者了解这场容器化革命并好好地利用它，这将超越我在多年软件开发生涯里所获得的成就。

我真诚希望你能喜欢这本书，希望它能帮助你在公司或组织里使用 Docker。

本书结构

本书大体由以下几部分组成。

- 第一部分首先讲解什么是容器,以及为什么应该关注它。之后将示范 Docker 的基本操作。最后会用较长篇幅来讲解 Docker 的基本概念和技术,其中包括 Docker 命令的概览。
- 第二部分讲解如何将 Docker 应用于软件开发生命周期。首先讲解如何配置开发环境,然后构建一个简单的 Web 应用,这个 Web 应用的例子将用于整个第二部分。这一部分还会涵盖开发、测试、集成,以及如何部署容器,如何有效地监控和记录生产环境的日志。
- 第三部分的内容更为深入,其中包括在多主机集群环境中,有哪些工具及技巧能使 Docker 容器既安全又可靠地运行。这部分适合已经使用 Docker,并需要了解如何扩展或解决网络和安全问题的读者。

排版约定

本书使用了下述排版约定。

- 楷体
表示新术语。
- 等宽字体 (`constant width`)
表示程序片段,以及正文中出现的变量、函数名、数据库、数据类型、环境变量、语句和关键字等。
- 加粗等宽字体 (**`constant width bold`**)
表示应该由用户输入的命令或其他文本。
- 斜体等宽字体 (*`Constant width italic`*)
表示应该替换成用户提供的值,或者由上下文决定的值。



该图标表示一般性说明。



该图标表示提示、建议或一般注释。



该图标表示警告或警示。

使用代码示例

补充材料(代码示例、练习等)可以从 <https://github.com/using-docker/> 下载。

本书是要帮你完成工作的。一般来说，如果本书提供了示例代码，你可以把它用在你的程序或文档中。除非你使用了很大一部分代码，否则无需联系我们获得许可。比如，用本书的几个代码片段写一个程序就无需获得许可，销售或分发 O'Reilly 图书的示例光盘则需要获得许可；引用本书中的示例代码回答问题无需获得许可，将书中大量的代码放到你的产品文档中则需要获得许可。

我们很希望但并不强制要求你在引用本书内容时加上引用说明。引用说明一般包括书名、作者、出版社和 ISBN。比如：“*Using Docker* by Adrian Mouat (O'Reilly). Copyright 2016 Adrian Mouat, 978-1-491-91576-9.”

如果你觉得自己对示例代码的用法超出了上述许可的范围，欢迎你通过 permissions@oreilly.com 与我们联系。

Safari® Books Online



Safari Books Online (<http://www.safaribooksonline.com>) 是应运而生的数字图书馆。它同时以图书和视频的形式出版世界顶级技术和商务作家的专业作品。技术专家、软件开发人员、Web 设计师、商务人士和创意专家等，在开展调研、解决问题、学习和认证培训时，都将 Safari Books Online 视作获取资料的首选渠道。

对于组织团体、政府机构和个人，Safari Books Online 提供各种产品组合和灵活的定价策略。用户可通过一个功能完备的数据库检索系统访问 O'Reilly Media、Prentice Hall Professional、Addison-Wesley Professional、Microsoft Press、Sams、Que、Peachpit Press、Focal Press、Cisco Press、John Wiley & Sons、Syngress、Morgan Kaufmann、IBM Redbooks、Packt、Adobe Press、FT Press、Apress、Manning、New Riders、McGraw-Hill、Jones & Bartlett、Course Technology 以及其他几十家出版社的上千种图书、培训视频和正式出版之前的书稿。要了解 Safari Books Online 的更多信息，我们网上见。

联系我们

请把对本书的评价和问题发给出版社。

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

北京市西城区西直门南大街 2 号成铭大厦 C 座 807 室 (100035)
奥莱利技术咨询（北京）有限公司

O'Reilly 的每一本书都有专属网页，你可以在那儿找到本书的相关信息，包括勘误表、示例代码以及其他信息。本书的网站地址是：

<http://shop.oreilly.com/product/0636920035671.do>

对于本书的评论和技术性问题，请发送电子邮件到：

bookquestions@oreilly.com

要了解更多 O'Reilly 图书、培训课程、会议和新闻的信息，请访问以下网站：

<http://www.oreilly.com>

我们在 Facebook 的地址如下：<http://facebook.com/oreilly>

请关注我们的 Twitter 动态：<http://twitter.com/oreillymedia>

我们的 YouTube 视频地址如下：<http://www.youtube.com/oreillymedia>

致谢

我很感激在我写作这本书的时候，大家给予我的一切帮助、建议和批评。如果下面遗漏了你的名字，请原谅我的疏忽。即便我没有完全按照你们的建议行事，我还是非常感谢你们为我所做的一切。

我要感谢 Ally Hume、Tom Sugden、Lukasz Guminski、Tilaye Alemu、Sebastien Goasguen、Maxim Belousov、Michael Boelen、Ksenia Burlachenko、Carlos Sanchez、Daniel Bryant、Christoffer Holmstedt、Mike Rathbun、Fabrizio Soppelsa、Yung-Jin Hu、Jouni Miikki 和 Dale Bewley，感谢你们对本书毫无保留的反馈。

针对技术交流和书中一些具体技术的意见，我要感谢 Andrew Kennedy、Peter White、Alex Pollitt、Fintan Ryan、Shaun Crampton、Spike Curtis、Alexis Richardson、Ilya Dmitrichenko、Casey Bisson、Thijs Schnitger、Sheng Liang、Timo Derstappen、Puja Abbassi、Alexander Larsson 和 Kelsey Hightower。同时，还要感谢 Kevin Gaudin 允许我复用 `monsterid.js`。

感谢 O'Reilly 出版社的工作人员所给予的一切帮助，特别是本书编辑 Brian Anderson 和 Meghan Blanchette。在你们的帮助下，本书的出版工作才得以启动。

还有 Diogo Mónica 和 Mark Coleman，感谢你们在最后关头向我伸出援手。

在此我要特别鸣谢两家公司：Container Solutions 和 CloudSoft。Jamie Dobson 和 Container Solutions 给予我很多发表博客文章和在不同活动中演讲的机会，并向我介绍了几位对本书影响深刻的人。CloudSoft 慷慨地让我在写作本书时使用他们的办公室，并主办了爱丁堡 Docker 聚会，这两件事对我而言非常重要。

感谢我的所有朋友和家人，你们容忍我只顾埋头写作，并因为这本书向你们发牢骚。如果你明白我的意思，你应该知道我说的是谁（不过你们不太可能看到这番话）。

最后，感谢 BBC 6 Music 的电台 DJ 提供了原声配乐，包括 Lauren Laverne、Radcliffe and Maconie（Mark Radcliffe 和 Stuart Maconie）、Shaun Keaveny 和 Iggy Pop。

电子书

扫描如下二维码，即可购买本书电子版。



目录

前言.....	xi
---------	----

第一部分 背景与基础

第 1 章 何谓容器，为何需要它.....	3
1.1 容器与虚拟机的比较.....	4
1.2 Docker 与容器.....	5
1.3 Docker 的历史.....	7
1.4 插件与基础设施.....	8
1.5 64 位 Linux.....	9
第 2 章 安装.....	10
2.1 在 Linux 上安装 Docker.....	10
2.1.1 将 SELinux 置于宽容模式下运行.....	11
2.1.2 不使用 sudo 命令执行 Docker.....	11
2.2 在 Mac OS 及 Windows 上安装 Docker.....	12
2.3 快速确认.....	13
第 3 章 迈出第一步.....	15
3.1 运行第一个镜像.....	15
3.2 基本命令.....	16
3.3 通过 Dockerfile 创建镜像.....	20
3.4 使用寄存服务.....	22

3.5 使用 Redis 官方镜像.....	24
3.6 总结.....	27
第 4 章 Docker 基本概念.....	28
4.1 Docker 系统架构.....	28
4.1.1 底层技术.....	29
4.1.2 周边技术.....	30
4.1.3 Docker 托管.....	31
4.2 镜像是如何生成的.....	32
4.2.1 构建环境的上下文.....	32
4.2.2 镜像层.....	33
4.2.3 缓存.....	35
4.2.4 基础镜像.....	35
4.2.5 Dockerfile 指令.....	37
4.3 使容器与世界相连.....	39
4.4 容器互联.....	40
4.5 利用数据卷和数据容器管理数据.....	41
4.5.1 共享数据.....	43
4.5.2 数据容器.....	44
4.6 Docker 常用命令.....	45
4.6.1 run 命令.....	46
4.6.2 容器管理.....	48
4.6.3 Docker 信息.....	50
4.6.4 容器信息.....	50
4.6.5 镜像管理.....	52
4.6.6 使用寄存服务器.....	54
4.7 总结.....	55

第二部分 Docker 与软件生命周期

第 5 章 在开发中应用 Docker.....	59
5.1 说声“Hello World!”.....	59
5.2 通过 Compose 实现自动化.....	67
5.3 总结.....	69
第 6 章 创建一个简单的 Web 应用.....	71
6.1 创建一个基本网页.....	72

6.2	利用现有镜像	73
6.3	实现缓存功能	78
6.4	微服务	81
6.5	总结	81
第 7 章	镜像分发	82
7.1	镜像及镜像库的命名方式	82
7.2	Docker Hub	83
7.3	自动构建	85
7.4	私有分发	86
7.4.1	运行自己的寄存服务	86
7.4.2	商业寄存服务	92
7.5	缩减镜像大小	92
7.6	镜像出处	94
7.7	总结	94
第 8 章	Docker 持续集成与测试	95
8.1	为 identidock 添加单元测试	95
8.2	创建 Jenkins 容器	100
8.3	推送镜像	106
8.3.1	给镜像正确的标签	106
8.3.2	准生产及生产环境	108
8.3.3	镜像数量激增的问题	108
8.3.4	使用 Docker 部署 Jenkins slaves	109
8.4	备份 Jenkins 数据	109
8.5	持续集成的托管解决方案	109
8.6	测试与微服务	110
8.7	总结	111
第 9 章	部署容器	113
9.1	通过 Docker Machine 配置资源	114
9.2	使用代理	117
9.3	执行选项	122
9.3.1	shell 脚本	122
9.3.2	使用进程管理器（或用 systemd 控制所有进程）	124
9.3.3	使用配置管理工具	127
9.4	主机配置	130
9.4.1	选择操作系统	130

9.4.2	选择存储驱动程序	130
9.5	专门的托管方案	132
9.5.1	Triton	132
9.5.2	谷歌容器引擎	134
9.5.3	亚马逊 EC2 容器服务	135
9.5.4	Giant Swarm	136
9.6	持久性数据和生产环境容器	138
9.7	分享秘密信息	139
9.7.1	在镜像中保存秘密信息	139
9.7.2	通过环境变量传递密钥	139
9.7.3	通过数据卷传递密钥	140
9.7.4	使用键值存储	140
9.8	网络连接	141
9.9	生产环境的寄存服务	141
9.10	持续部署 / 交付	141
9.11	总结	142
第 10 章	日志记录和监控	143
10.1	日志记录	144
10.1.1	Docker 默认的日志记录	144
10.1.2	日志汇总	145
10.1.3	使用 ELK 进行日志记录	146
10.1.4	通过 syslog 实现日志管理	155
10.1.5	从文件抓取日志	160
10.2	监控和警报	161
10.2.1	使用 Docker 工具进行监测	161
10.2.2	cAdvisor	162
10.2.3	集群解决方案	163
10.3	商用的监听及日志记录解决方案	166
10.4	总结	166

第三部分 工具和技术

第 11 章	联网和服务发现	169
11.1	大使容器	170
11.2	服务发现	173
11.2.1	etcd	173

11.2.2	SkyDNS	177
11.2.3	Consul	181
11.2.4	服务注册	185
11.2.5	其他解决方案	186
11.3	联网选项	187
11.3.1	网桥模式	187
11.3.2	主机模式	188
11.3.3	容器模式	188
11.3.4	未联网模式	188
11.4	全新的 Docker 联网功能	188
11.5	网络解决方案	190
11.5.1	Overlay	191
11.5.2	Weave	193
11.5.3	Flannel	196
11.5.4	Calico 项目	201
11.6	总结	205
第 12 章 编排、集群和管理		207
12.1	集群和编排工具	208
12.1.1	Swarm	208
12.1.2	fleet	214
12.1.3	Kubernetes	219
12.1.4	Mesos 和 Marathon	226
12.2	容器管理平台	235
12.2.1	Rancher	236
12.2.2	Clocker	237
12.2.3	Tutum	238
12.3	总结	239
第 13 章 容器安全与限制容器		241
13.1	需要考虑的事项	242
13.2	纵深防御	244
13.3	如何保护 identidock	245
13.4	以主机隔离容器	246
13.5	进行更新	246
13.6	镜像出处	249
13.6.1	Docker 摘要	250
13.6.2	Docker 的内容信任机制	250

13.6.3	可复制及可信任的 Dockerfile	254
13.7	安全建议	256
13.7.1	设置用户	256
13.7.2	限制容器联网	257
13.7.3	删除 setuid 和 setgid 的二进制文件	258
13.7.4	限制内存使用	259
13.7.5	限制 CPU 使用	260
13.7.6	限制重新启动	261
13.7.7	限制文件系统	261
13.7.8	限制内核能力	262
13.7.9	应用资源限制	263
13.8	运行加固内核	264
13.9	Linux 安全模块	265
13.9.1	SELinux	265
13.9.2	AppArmor	268
13.10	审核	268
13.11	事件响应	269
13.12	未来特性	269
13.13	总结	270
	作者简介	271
	关于封面	271