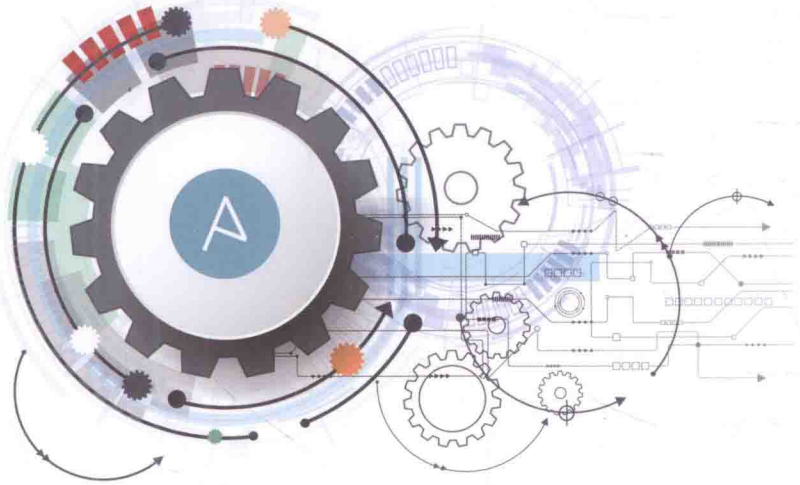
HZ BOOKS
华章IT

本书由资深运维人员联手打造，通过大量实例，详细讲解Ansible自动化运维方式与技巧。

从最基础的架构解析、安装配置，到典型应用场景与案例分析，作者分享了自己在工作中的实战经验，是掌握大规模集群运维管理的必备参考。

實戰



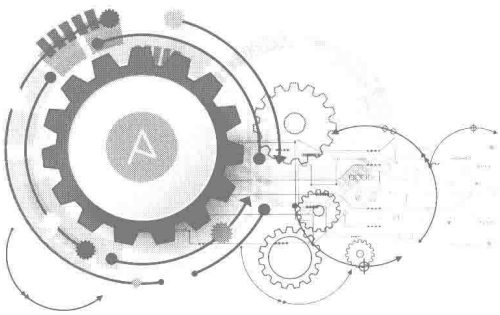
陈金窗 沈灿 刘政委 编著

Ansible for Configuration Management and Automation

Ansible自动化运维
技术与最佳实践

机械工业出版社
China Machine Press

實戰



Ansible for Configuration Management and Automation

Ansible自动化运维
技术与最佳实践

陈金窗 沈灿 刘政委 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Ansible 自动化运维：技术与最佳实践 / 陈金窗，沈灿，刘政委编著 . —北京：机械工业出版社，2016.2
（实战）

ISBN 978-7-111-53115-9

I. A… II. ①陈… ②沈… ③刘… III. 程序开发工具 IV. TP311.52

中国版本图书馆 CIP 数据核字（2016）第 040638 号

本书由资深运维程师联手打造，通过大量实例，详细讲解 Ansible 这个自动化运维工具的基础原理和使用技巧；从基础的架构解析、安装配置，到典型应用案例分析，作者分享了自己在工作中的实战经验，为各类运维操作、运维开发人员提供了翔实的指南。本书主要内容包括：Ansible 架构及安装，Ansible 组件、组件扩展、API，playbook 详解，最佳实践案例分析，用 ansible-vault 保护敏感数据，Ansible 与云计算的结合，部署 Zabbix 组件、Haproxy + LAMP 架构，以及 Ansible 在大数据环境的应用实战等。

Ansible 自动化运维：技术与最佳实践

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：吴 怡 责任校对：殷 虹
印 刷：北京市荣盛彩色印刷有限公司 版 次：2016 年 5 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：20.75
书 号：ISBN 978-7-111-53115-9 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）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

Preface 前　言

随着信息技术的迅速发展，形形色色的互联网应用已经成为我们日常生活不可分割的部分。云计算已经改变 IT 资源部署、配置和管理的方式，服务供应商向着“一切皆服务”交付模式努力。用户享受通过将基础设施扩展并作为服务使用带来的高效、便捷，服务供应商通过云生态环境能够向用户提供更高价值的服务。

这一切背后都有着庞大的 IT 系统做支撑，作为负责保障稳定运行的运维工作所面临的挑战越来越大。传统的人工运维方式已经无法满足业务的发展需求，需要从流程化、标准化、自动化去构建运维体系。随着 DevOps 运动的兴起，运维人员、研发人员、质量控制人员都从更大范围来看待自己的工作，打破运维、研发之间的壁垒，进行相互渗透、融合。DevOps 项目在数量和体量上持续增长，支撑持续集成、持续交付的自动化工具不断涌现。

Ansible 是 DevOps 项目基础支撑工具之一，是第一款实现读/写跨平台的“ Infrastructure-as-code”工具，从系统管理者到开发者，都可使用 Ansible 自动化部署并维护整个应用的生命周期，实现持续交付。

Ansible 是 Github 上最热门的开源自动化工具之一，当前已经超过 1000 人为 Github 上的 Ansible 做过贡献。2013 年笔者创建的“Ansible 中国用户组”QQ 群（群号：142851673 ）也相当活跃，当前专业会员已超过 1000 人。

本书将带领读者探索 Ansible 自动化运维的神奇之旅，为运维工作节省时间、节约成本，并支持云环境应用部署。

读者对象

本书主要读者对象包括：

- IT 运维人员、系统管理员、企业网管。
- 运营开发人员、应用部署人员。
- 系统架构师。
- 大专院校的计算机专业学生。

主要内容

本书是笔者在多年的学习、研究、实践的基础上，对 Anisble 进行系统的总结和梳理，其中既包括对 Ansible 基础知识的详细讲解，又包括日常运维工作中典型应用场景的实践案例，还介绍 Anisble 业界丰富的进展和发展趋势。本书的实践案例和脚本，可以在实验和生产环境中针对本书描述的场景进行复制和使用。

本书的目标是介绍如何较好地使用 Anisble，从初始的命令行开始，到编写 playbooks，再到管理大型、复杂的环境，最后介绍如何构建自己的模块、编写插件扩展 Ansible 增加新的功能。对于新手来说，本书提供了关于自动化运维的具体操作实战。对有经验的维护人员来说，本书提供了如何把 Ansible 与具体应用相结合，讲解 Ansible 的最佳实践。对于产品专家来说，本书介绍了如何扩展 Ansible 自动化运维工具手段，讨论 Ansible 如何与其他系统的交互才能提供可满足最终用户需求的集成解决方案。

本书主体包括 14 章。各章可以独立阅读，但对于还没有大规模应用经验的新手，建议按照顺序、循序渐进阅读。

本书第 1、2、7、11 ～ 13 章由陈金窗编写，第 3 ～ 6、8 ～ 10、14 章、附录由沈灿编写，最后由刘政委进行校审。由于笔者的水平有限，编写时间仓促，且自动化运维方兴未艾，Ansible 当前仍处于快速发展之中，因此书中内容难免会出现一些错误或不准确的地方，恳请读者评判指正、不吝赐教。

致谢

首先感谢 Ansible 创始人 Michael DeHaan 和他的研发团队独具慧眼、发明创造了

功能强大、轻量级的自动化运维工具。同时感谢提供 Anisble 模块的所有第三方作者，是他们辛勤的劳动和乐于分享，才使得 Ansible 产生巨大威力，在他们身上闪烁着开源精神的绚丽光芒。

感谢机械工业出版社的编辑们一年来始终的支持、积极的鼓励、耐心的帮助，并逐字审阅、校正，才使本书的出版成为可能。

本书有一些内容参考了网络论坛、博客等，由于参考资料众多，有些时间久远无法了解确切出处，在此对热爱分享知识的网友表示深深的谢意。

最后，谨以此书献给我们最亲爱的家人和自己，以及众多热爱开源技术的朋友们！

陈金窗

2016 年 2 月于北京

目　录 *Contents*

第 1 章 Chapter 1

Ansible 架构及特点

IT 行业的工作变得越来越有趣了，我们不再是把软件交付给客户，然后安装在单独的服务器上运行，我们都慢慢地变成了系统工程师。

我们现在部署应用软件的方式是通过服务串联起来，运行在一系列分布式的计算资源上并用各种不同的网络协议进行通信。常见的应用包括 Web 服务、应用服务、基于内存的缓存服务系统、任务队列、消息队列、SQL 数据库、NoSQL 数据存储、负载均衡等。

我们也需要确保采用合适的冗余，当故障发生时软件系统能够很好地处理、适应这些故障。另外有些辅助的服务需要部署、维护，例如日志管理、监控系统、分析系统，需要与第三方服务交互，如通过与 IaaS 接口交互来管理虚拟主机实例。

你可以用手动方式来搭建这些服务：安装服务器操作系统，SSH 登录每一台，安装软件包，编辑配置文件，等等。这种方式耗费大量时间还经常出错，特别是在做了 3 ～ 4 次之后，这枯燥重复的手工劳动是令人非常痛苦的。对于更复杂的任务，比如在你应用环境中搭建一个 OpenStack 云环境，由手工来操作会让人发疯。应有更好的方法。

如果你读到这里，你可能已经有了配置管理的思想，并考虑采用 Ansible 做为你的配置管理工具。无论你是一个开发人员想要把代码部署到生产环境，还是一个系统管理员寻找更好的自动化方法。我觉得 Ansible 对于这些问题都是很好的解决方案。

1.1 Ansible 软件及公司

IT 自动化配置管理最近 20 年获得了迅猛的发展，特别最近几年在移动互联、云计算、大数据、互联网 + 等大规模应用平台的需求推动下，涌现出一批成熟的大规模自动化运维工具。维基百科里列出了二十多个，其中 Puppet、Chef 和 Salt，以及 CFEngine、Vagrant 和 NixOS，大家都可能耳熟能详了。不过后起之秀 Ansible（http://www.ansible.com/）的人气更高，已经是当今最常用的管理基础架构的开源管理工具之一。

从开源仓库 GitHub 上受到使用者、开发者的关注度、加星、贡献、评论（见表 1-1）可以看出，Ansible 的受欢迎程度的数据已经远远超过 Puppet、Chef、CFEngine、SaltStack。

表 1-1 GitHub 上开源自动化工具受关注程度信息表（截至 2015 年 8 月 30 日）

开源自动化配置工具	关注（Watch）	加星（Star）	复制（Fork）	开始时间	评论数	贡献者
ansible/ansible	1 009	12 416	3 697	2012 年 2 月 5 日	15 821	1 146
puppetlabs/puppet	414	3 514	1 468	2005 年 4 月 10 日	20 618	394
saltstack/salt	451	5 573	2 370	2011 年 2 月 20 日	58 452	1 194
Chef/chef	338	3 794	1 554	2008 年 5 月 2 日	13 195	399
CFEngine/core	62	224	136	2007 年 12 月 30 日	12 544	73

Ansible 自从 2012 年 2 月发布以来，一直得到 Ansible 爱好者、用户、开发者的热情参与、持续贡献，如图 1-1 所示。

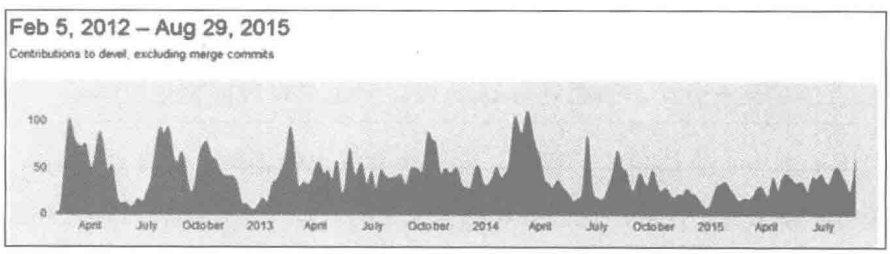


图 1-1 Ansible 受贡献者的支持趋势

Ansible 使用 Python 作为开发语言，巧妙地设计、实现了简单易用、功能强大的自动化管理工具。Ansible 由 Michael DeHaan 发起、开发、创建，他同时也是著名工具软件 Cobbler 与 Func 的开发者。Ansible 的第一个版本发布于 2012 年 2 月，目前下载量已经超过了 100 万。当前在 GitHub 上，它是排名前 10 位的 Python 项目，可以预见

Ansible 的发展不可限量。

Ansible 已经广泛应用于各种规模、各个领域的企业，包括 Rackspace、Twitter、Evernote、NASA、GoPro、Atlassian 等知名企业。

1.1.1　Ansible 应用领域

Ansible 的编排引擎可以出色地完成配置管理、流程控制、资源部署等多方面工作。与其他 IT 自动化产品相比较，Ansible 为你提供一种不需要安装客户端软件、管理简便、功能强大的基础架构配置、维护工具。

Ansible 基于 Python 语言实现，由 Paramiko 和 PyYAML 两个关键模块构建。Ansible 具有独特的设计理念：

- 安装部署过程特别简单，学习曲线很平坦。
- 管理主机便捷，支持多台主机并行管理。
- 避免在被管理主机上安装客户代理，打开额外端口，采用无代理方式，只是利用现有的 SSH 后台进程。
- 用于描述基础架构的语言无论对机器还是对人都是友好的。
- 关注安全，很容易对执行的内容进行审计、评估、重写。
- 能够立即管理远程被管理主机，不需要预先安装任何软件。
- 不仅仅支持 Python，可运行使用任何动态语言开发模块。
- 非 root 账户也可以使用。
- 成为最简单、易用的 IT 自动化系统。

在云计算时代的浪潮中，基础架构必须满足按需自动伸缩、按使用量计费的基本特性，IT 自动化运维软件就是最重要的必备工具之一。下面来看看几个关键的领域中取得的巨大的进展。

1. 配置管理

配置管理领域已经涌现出多种工具，配置管理的目标就是确保被管理的主机尽可能快速、按照正确方式达到配置文件中描述的状态，这对管理 IT 环境至关重要。例如，在网站高峰时候需要扩展新的 Web 服务器，这需要一台由配置管理控制的机器能够快速就位，这也就是通常所说的代码化基础架构（Infrastructure as code），因为构建基础架构所有必须的代码都存储在源码控制系统中。这也是逐步引入对代码化基础架

构按照软件开发生命周期（Software Development Lifecycle，SDLC）方式进行管理，这些包括辅助基础架构测试的工具有 Ansible、CFEngine、Chef、Puppet、Salt 等，基础架构测试工具有 Serverspec、Test kitchen 等。

2. 服务即时开通

这个领域的工具主要是在数据中心、虚拟化环境、云计算中快速开通新的主机。几乎所有云计算的服务提供商都有相应的 API 接口，这些自动化工具通过这些 API 接口能够快速地创建主机实例。对于基于 Linux 或最近快速发展的容器（如 Docker、LXC），越来越多的人开始采用自动化工具的方式来保证这些容器的开通。Ansible 在这些场景扮演了重要的角色。

3. 应用部署

这个领域的工具重点关注如何尽可能地零停机部署应用。许多单位已经采用滚动式部署（rolling deployments）或金丝雀部署（canary deployments），Ansible 对这两种方式都支持。流水线式部署也是很常见的，常见的工具包括 ThoughtWorks Go、Atlassian Bamboo、大量插件支持的 Jenkins 条，都是比较优秀的。

4. 流程编排

流程编排主要是进行部署时候如何保证基础架构中的各种组件协调一致。例如，在你对 Web 服务器部署新的软件版本时候，需要确保该 Web 服务器从负载均衡器上移出，这是很常见的场景。这类工具有 Ansible、Mcollective、Salt、Serf、Chef 等。

5. 监控告警

监控告警工具已经发展到能够适应快速处理大规模服务器的环境。以前有成熟的 Nagios、Ganglia、Zenoss、Zabbix，最新发展的有 Graphite、Sensu、Riemann 等，都是相对不错的工具。

6. 日志记录

集中日志数据确保能够正确地收集跨系统和应用的日志，同时能够按照规则进行智能过滤、根本原因分析、告警等。常见的工具有 Logstash-Kibana、SumoLogic、Rsyslog 等。

在上面关键的六个领域中，Ansible 能够非常完美地完成前面四个领域的工作。通

过使用 Ansible，无论是系统管理员、运维团队、基础架构管理员、开发者，或者其他任何需要基础架构自动化者都可以从中受益。本书目的就是介绍如何构建健壮的 IT 基础架构自动化运维系统。

Ansible 软件创始人：Michael DeHaan

2012 年 2 月，曾在 Red Hat 开发 Cobbler 和 Func、又在 Puppet 工作过的 Michael DeHaan 看到了 IT 自动化领域的机会：Linux 管理员不得不用好几类工具来应付不同的工作场景，如配置管理用 Puppet 或 Chef，部署时要用 Fabric 或 Capistrano，还要用 Func 或 mCollective 处理其他任务，总之，太复杂了。同时，多节点部署却没有处理得很好的工具，而在云计算和大规模互联网的基础设施里，这恰恰是最有意思的问题。

一天，DeHaan 在自己的沙发上开始用 Python 开发一个新工具，他的目标是：极为易用，连他自己都很想用；任何人可以在几分钟之内学会并使用。经过短短的 6 个月，第一个版本的工具诞生了，这就是 Ansible。

由于 DeHaan 在运维圈已经很有名气，Ansible 发布后很快流行起来。这期间，Fedora 的 Seth Vidal(yum 作者）采用并在 4 月份发表了 High Scalability，都非常关键。

这之后，DeHaan 还参与了 OpenStack 的开发，但在用 Puppet 自动化管理 OpenStack 的过程中不断撞墙。这时候，Ansible 在 GitHub 上火了起来。很快他决定成立公司——AnsibleWorks。2013 年 8 月公司获得 600 万投资，后来改名为 Ansible 公司。

Ansible 只依赖 SSH，无需在远程机器上安装代理，极为容易上手。Hacker News 上有人称之为 shell scripting++，很到位。

1.1.2　Ansible 软件发布

Ansible 公司负责 Ansible 开源软件的维护、管理，是 Ansible 软件发展的最大贡献者。Ansible 开发团队非常高效，软件发布周期大约是 2 个月发布一个新版本。由于发布周期如此之短，轻微的 bug 通常是在下一个版本中得到修补，而不是对稳定版本发布新补丁。重大的 bug 经评估后，如果确实需要将会发布对稳定版本的补丁，但这种情况很少出现。