

- Ansible基本工具 •
- role和衍生工具Ansible Galaxy •
- 企业级收费软件Ansible Tower •



Ansible快速入门

技术原理与实战

史晶晶 编著

本书提炼了Ansible原理中的精华，
抓住核心，立足于实战，
利用较短的时间使读者掌握其概要，
达到快速上手的目的。



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



Ansible快速入门

技术原理与实战



史晶晶 编著

电子工业出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

本书以新的自动化运维工具 Ansible 为主要内容，侧重于实战，由浅入深地介绍了 Ansible 以及周边产品 Ansible Galaxy 和 Ansible Tower 的用法。本书共计 6 章，前 4 章由浅及深、层层递进地介绍了 Ansible 的使用方法。第 5 章着重介绍了 Ansible 的代码分享机制 role 以及其分享平台 Ansible Galaxy。第 6 章概括性地介绍了企业级软件 Ansible Tower。全书的叙述风格通俗易懂，没有过多地引入复杂的概念，侧重于讲解原理，立足于实战，引领 Ansible 新手轻松入门。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

Ansible 快速入门：技术原理与实战 / 史晶晶编著. —北京：电子工业出版社，2017.6

ISBN 978-7-121-31502-2

I. ①A… II. ①史… III. ①程序开发工具 IV. ①TP311.561

中国版本图书馆 CIP 数据核字（2017）第 105131 号

责任编辑：安 娜

印 刷：三河市兴达印务有限公司

装 订：三河市兴达印务有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：787×980 1/16 印张：11 字数：192 千字

版 次：2017 年 6 月第 1 版

印 次：2017 年 6 月第 1 次印刷

定 价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

前言

内容介绍

Ansible 是对机群进行软件安装、配置和应用部署的自动化工具。自 2012 年 Ansible 出现后，以其使用简单、功能实用等特点得到了广泛关注，成为自动化运维工具中的冉冉新星。仅三年后就被红帽（Red Hat）公司收购，目前受到众多软件公司的关注、推广和使用。自动化部署无论对系统管理员还是对软件开发人员来说，都会减少重复的手工操作，提高部署效率。Ansible 作为学习成本小、学习路径短的一款工具，更是值得了解和使用。

作为一本 Ansible 入门书籍，读者只需对 Linux 有最基本的了解就可以轻松读懂本书。

本书的内容共计 6 章，分为以下三个部分：

第一部分 Ansible 基本工具的讲解（第 1 章～第 4 章）

本书首先介绍了 Ansible 架构，然后讲解了 Ansible 的主要概念，接着又介绍了一些具体使用方法，步步递进、层层深入地介绍了 Ansible 的相关知识。

第 4 章对前面 3 章中的知识细节进行了补充，以便读者能够深入理解 Ansible 的基本使用方法。

第二部分 role 和衍生工具 Ansible Galaxy 的介绍（第 5 章）

role 是 Ansible 最为推荐的重用代码的方式，并为其开发了 Ansible Galaxy 代码分享网站。但因其概念较为复杂，所以对其单独进行讲解。

第三部分 企业级收费软件 Ansible Tower 介绍（第 6 章）

企业级用户面临着更加复杂的应用环境和更高的安全要求，Ansible Tower 就是一款解决企业级用户难题的收费软件。

代码的运行环境

建议读者安装 Linux 虚拟机作为 Ansible 的管理节点来测试本书中的代码。Ansible 目前已被红帽公司收购，对 Red Hat Linux 系统的支持较为完善，建议读者最好选择 Red Hat Linux 7 或 CentOS 7。

排版约定

为了使读者能快速把握到代码的重点，本书中代码的重要部分用加粗字体表示强调。

例如，下面的代码强调变量 “`ansible_os_family`” 的用法：

```
---
- hosts: all
  user: root
  tasks:
    - name: echo system
      shell: echo {{ ansible_os_family }}
    - name install ntp on Debian linux
      apt: name=git state=installed
      when: ansible_os_family == "Debian"
    - name install ntp on redhat linux
      yum: name=git state=present
```

勘误信息

笔者对本书中所有的代码都进行了完整的测试，书中的文字也经过了反复的斟酌。尽管如此，由于时间紧迫且作者水平有限，错误和疏漏难以避免，还需要广大读者的反馈和修订，以使得本书更加完善。因此，如果您发现书中的任何错误，小到错别字，大到代码运行错误，都希望您能及时反馈。您的任何一次勘误，都会令笔者和其他读者受益，再次表示感谢。

勘误地址：

<https://github.com/ansible-book/errata>

或者

<http://getansible.com/reference/errata>

反馈勘误方法：

提问题到 Github 项目上：<https://github.com/ansible-book/errata>

发邮件给笔者：shijingjing02@163.com

致谢

感谢同组（Labs 和 Insights）的同事对本书早期版本的肯定，使我受到鼓舞，有信心编辑成册。感谢我的经理赵东在公司内部推广宣传，感谢周兆林（Jaylin）对早期代码仔细认真的测试，感谢傅炜（网名：Tekkaman Ninja）多次对文字提出大量的修改建议。

这是笔者第一次写书，在写书的过程中耗费了大量的时间和精力，若是没有家人的鼎力支持，这本书根本无法完成。尤其感谢老公为我分担了怀孕和育儿的大量调研工作，使我能够有时间投入本书的写作中。

本书的后期写作和修订正值我怀孕分娩前后，时间上难免拖拉，感谢本书的编辑安娜对我的理解和支持。

轻松注册成为博文视点社区用户（www.broadview.com.cn），扫码直达本书页面。

- **提交勘误：**您对书中内容的修改意见可在 [提交勘误](#) 处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动：**在页面下方 [读者评论](#) 处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：<http://www.broadview.com.cn/31502>



目 录

第 1 章 Ansible 介绍	1
1.1 Ansible 介绍.....	2
1.2 Ansible 解决了什么运维痛点.....	2
1.3 架构.....	2
1.3.1 Ansible 的架构.....	2
1.3.2 Ansible Tower 的架构.....	4
第 2 章 Ansible 入门	6
2.1 安装 Ansible	7
2.1.1 在管理员的电脑上安装	7
2.1.2 被管理的远程主机	7
2.2 Ansible 管理哪些主机.....	8
2.2.1 什么是主机目录	8
2.2.2 主机目录配置文件	8
2.3 Ansible 用命令管理主机.....	9
2.3.1 Ansible 命令的格式.....	9
2.3.2 Ansible 命令的功能.....	9
2.4 Ansible 用脚本管理主机.....	10
2.4.1 执行脚本 Playbook 的方法	11
2.4.2 Playbook 的例子	11
2.4.3 Play 和 Playbook.....	13

2.5	Ansible 模块.....	14
2.5.1	什么是 Ansible 模块.....	14
2.5.2	在命令行里使用模块.....	15
2.5.3	在 Playbook 脚本中使用模块.....	15
2.5.4	Ansible 模块的特点.....	15
2.5.5	常用模块.....	16
第 3 章	Ansible 进阶.....	30
3.1	Ansible 的配置.....	31
3.1.1	可以配置什么.....	31
3.1.2	Ansible 配置文件的优先级.....	31
3.2	主机清单.....	32
3.2.1	远程主机的分组.....	33
3.2.2	设置连接参数.....	34
3.2.3	变量.....	34
3.3	Ansible 的脚本 Playbook.....	36
3.3.1	Playbook 的文件格式 YAML.....	36
3.3.2	执行 Playbook 的命令.....	37
3.3.3	Playbook 的基本语法.....	38
3.3.4	变量.....	45
3.3.5	Playbook 也有逻辑控制语句.....	53
3.3.6	重用 Playbook.....	58
3.3.7	用标签, 实现执行 Playbook 中的部分任务.....	66
3.4	更多的 Ansible 模块.....	69
3.4.1	模块的分类.....	69
3.4.2	Extra 模块的使用方法.....	70
3.4.3	命令行查看模块的用法.....	71
3.5	最佳使用方法.....	71
3.5.1	写 Playbook 的原则.....	71
3.5.2	参考别人的 Playbook.....	72

第 4 章 Ansible Playbook 杂谈	73
4.1 再谈 Ansible 变量	74
4.1.1 变量的作用域	74
4.1.2 变量的优先级	74
4.2 使用 lookup 访问外部文件或数据库中的数据	80
4.2.1 lookup 读取文件	81
4.2.2 lookup 生成随机密码	81
4.2.3 lookup 读取环境变量	82
4.2.4 lookup 读取 Linux 命令的执行结果	83
4.2.5 lookup 读取 template 变量替换后的文件	83
4.2.6 lookup 读取配置文件	84
4.2.7 lookup 读取 CSV 文件的指定单元	86
4.2.8 lookup 读取 DNS 解析的值	87
4.2.9 更多的 lookup 功能	91
4.3 过滤器	91
4.3.1 过滤器使用的位置	91
4.3.2 过滤器对普通变量的操作	92
4.3.3 过滤器对文件路径的操作	96
4.3.4 过滤器对字符串变量的操作	99
4.3.5 过滤器对 JSON 的操作	106
4.3.6 过滤器对数据结构的操作	109
4.3.7 过滤器的链式/连续使用	111
4.4 测试变量或表达式是否符合条件	111
4.4.1 测试字符串	112
4.4.2 比较版本	113
4.4.3 测试 List 的包含关系	113
4.4.4 测试文件路径	114
4.4.5 测试任务的执行结果	115

4.5 认识插件	117
4.5.1 插件类型	118
4.5.2 常用的插件介绍	119
第 5 章 role 和 Ansible Galaxy	123
5.1 role 和 Ansible Galaxy 的简要介绍	124
5.1.1 role	124
5.1.2 Ansible Galaxy	124
5.2 role 的放置位置	124
5.2.1 当前目录的 roles 文件夹下	124
5.2.2 环境变量 ANSIBLE_ROLES_PATH 定义的文件夹	125
5.2.3 Ansible 配置文件中 roles_path 定义的文件夹	125
5.2.4 默认文件夹/etc/ansible/roles	125
5.3 在 Playbook 中如何调用 role	126
5.3.1 调用最简单的 role	126
5.3.2 通过 pre_tasks 和 post_tasks 调整 role 和任务的顺序	127
5.3.3 调用带有参数的 role	129
5.3.4 与 when 一起使用 role	129
5.4 如何写 role	130
5.4.1 role 的完整定义	130
5.4.2 默认变量和普通变量的区别	131
5.4.3 tasks/main.yml 如何使用变量、静态文件和模板	132
5.5 role 的依赖	134
5.6 Ansible Galaxy 网站介绍	136
5.6.1 从 Ansible Galaxy 网站上下载 role	136
5.6.2 分享你的 role	139
5.7 演示 role 的创建和分享	139
5.7.1 改造单个的 Playbook 为 role	141
5.7.2 在 Ansible Galaxy 中分享 role	144

第 6 章	Ansible Tower.....	145
6.1	为什么要用 Ansible Tower.....	146
6.1.1	Ansible 和 Tower 的用户视角架构图.....	146
6.1.2	Ansible Tower 的主要功能.....	147
6.2	如何使用 Ansible Tower.....	149
6.2.1	安装方法	149
6.2.2	使用方法	152
6.2.3	总结	161
6.3	与第三方平台的整合	163
6.3.1	Ansible Tower API	163
6.3.2	Ansible Tower 提供的命令行工具.....	164
附录 A		166

第 1 章

Ansible 介绍

本章重点

- 1.1 Ansible 介绍
- 1.2 Ansible 解决了什么运维痛点
- 1.3 架构

1.1 Ansible 介绍

Ansible 是一个部署一群远程主机的工具。这里“远程主机 (Remote Host)”是指任何可以通过 SSH 登录的主机，所以它既可以是远程虚拟机或物理机，也可以是本地主机。

Ansible 通过 SSH 协议实现管理节点与远程节点之间的通信。理论上来说，只要能通过 SSH 登录到远程主机来完成的操作，都可以通过 Ansible 实现批量自动化操作。

包括：复制文件、安装包、发起服务，等等。

1.2 Ansible 解决了什么运维痛点

Ansible 解决了如何大批量、自动化地实现系统配置、应用部署、命令和服务操作的问题。其脚本具有灵活、可重入的特性，极大地减少了运维人员的重复劳动，提高了运维效率。

1.3 架构

1.3.1 Ansible 的架构

Ansible 管理节点和远程主机节点间通过 SSH 协议进行通信。所以配置 Ansible 的时候，只需保证从 Ansible 管理节点通过 SSH 协议能够连接到被管理的远程节点即可。注意，SSH 必须配置为公钥认证登录方式，而非密码认证，第 2 章会讲到具体的配置方法。

1. 连接方式 (SSH)

在管理节点安装 Ansible 及所依赖的软件。由于管理节点需通过 SSH 连接被管理的主机来执行命令或者脚本，因此被管理的远程节点需要配置并启用 SSH 服务，此外无须安装其他特殊软件。管理节点只在执行脚本或命令时与远程主机连接，没有特别的同步机制，所以发生断电

等异常时一般不会影响 Ansible。

2. 支持多种类型的主机

Ansible 可以同时管理 Red Hat 系的 Linux、Debian 系的 Linux 以及 Windows 主机。Ansible 的工作原理如图 1.1 所示。

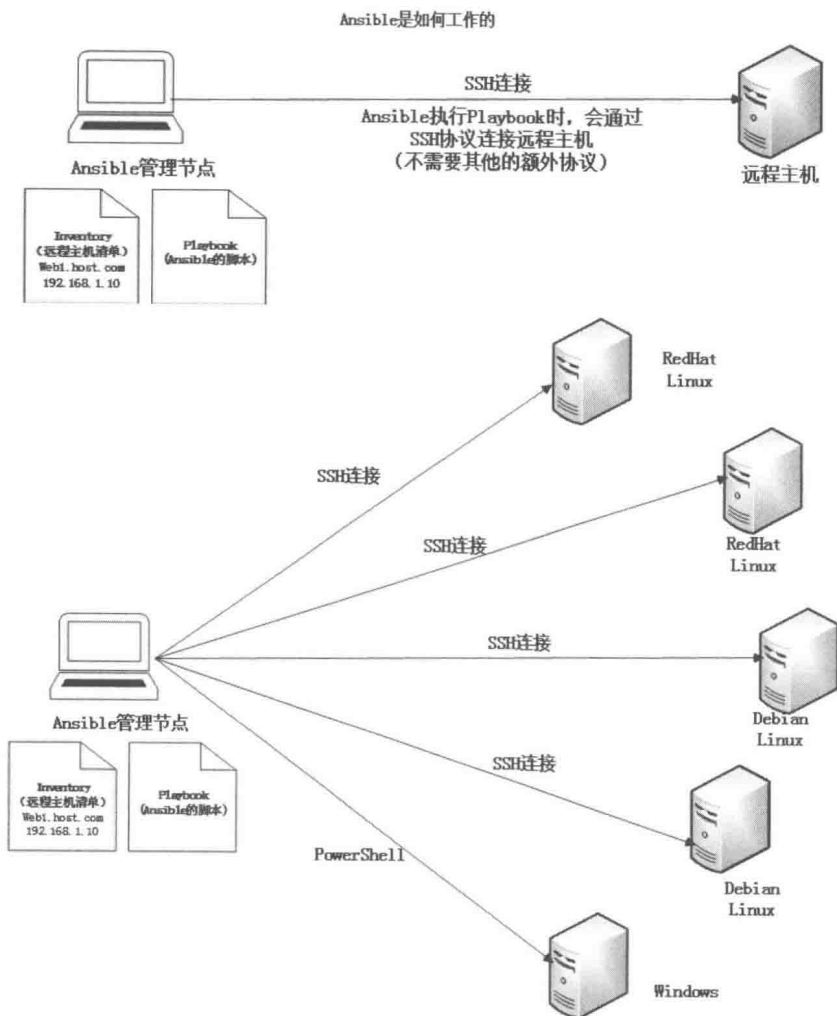


图 1.1 Ansible 工作原理

1.3.2 Ansible Tower 的架构

1. Ansible Tower 的由来

Ansible Tower 是一款针对企业用户的收费软件。

在 1.3.1 节的 Ansible 架构和第 2 章 Ansible 的安装中会讲到，每一台被 Ansible 远程管理的主机，都需要配置采用公钥认证的 SSH 连接。密钥的配置和维护对于管理几台虚拟机和远程主机的个人用户不会有什么问题，但对于拥有大量主机和管理人员的企业用户来说，则可能有以下困扰。

- ◎ 维护工作量大：每增加一台主机，都需要手工配置一下 SSH 连接，企业级的 PC 主机成百上千，每个管理员都需要在自己的电脑上配置所有的 SSH 连接，无疑工作量巨大。
- ◎ 安全隐患大：在安全方面如果管理员能够拿到 SSH 私钥，或者复制给别人，那么对于生产环境来说，无疑是最大的安全隐患。
- ◎ 协同性弱：每个管理员都可能有自己的脚本库，有的脚本可能是为了解决同一个问题，但管理员之间没有一个通用的协作共享脚本的机制。
- ◎ 可视性差：基本一般通过 Shell 终端运行，对于大量主机批量配置的情况，其执行状态的表现能力有限，不利于后期对于结果的统计和分析。

Ansible Tower 是一款针对企业用户的收费软件，功能强大，很好地解决了以上困扰。

2. Ansible Tower 能做什么

Ansible Tower 则是针对企业用户环境、中心化的 Ansible 管理节点，它向管理员提供网页接口，来运行 Ansible 脚本 Playbook。

- ◎ 管理员在 Ansible Tower 上使用和分享主机的 SSH 私钥，但是不能查看和复制私钥文件。
- ◎ Ansible 网站上的所有管理员都可以共享 Playbook 脚本，减少重复工作。
- ◎ 此外，Ansible Tower 还可以收集和展现所有主机的 Playbook 的执行状况，以便于统计和分析主机的状态。

Ansible Tower 架构图如图 1.2 所示。

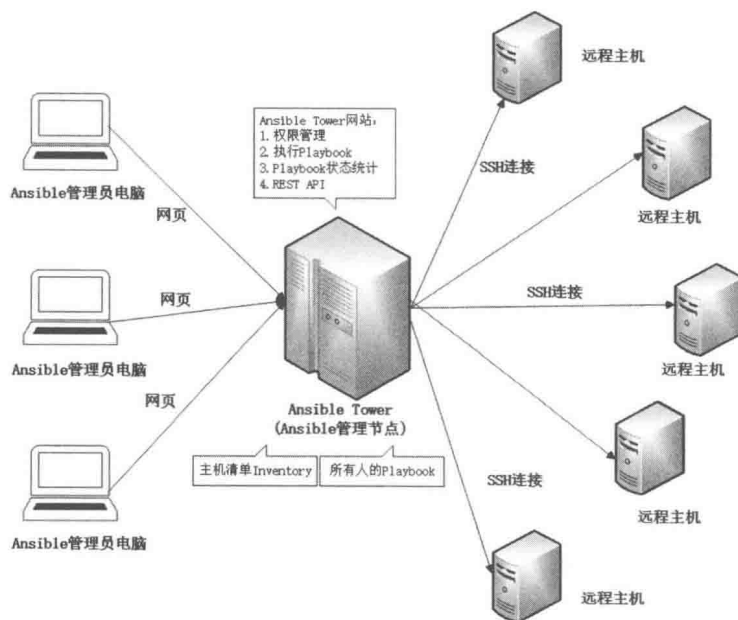


图 1.2 Ansible Tower 架构图

第 2 章

Ansible 入门

本章重点

- 2.1 安装 Ansible
- 2.2 Ansible 管理哪些主机
- 2.3 Ansible 用命令管理主机
- 2.4 Ansible 用脚本管理主机
- 2.5 Ansible 模块