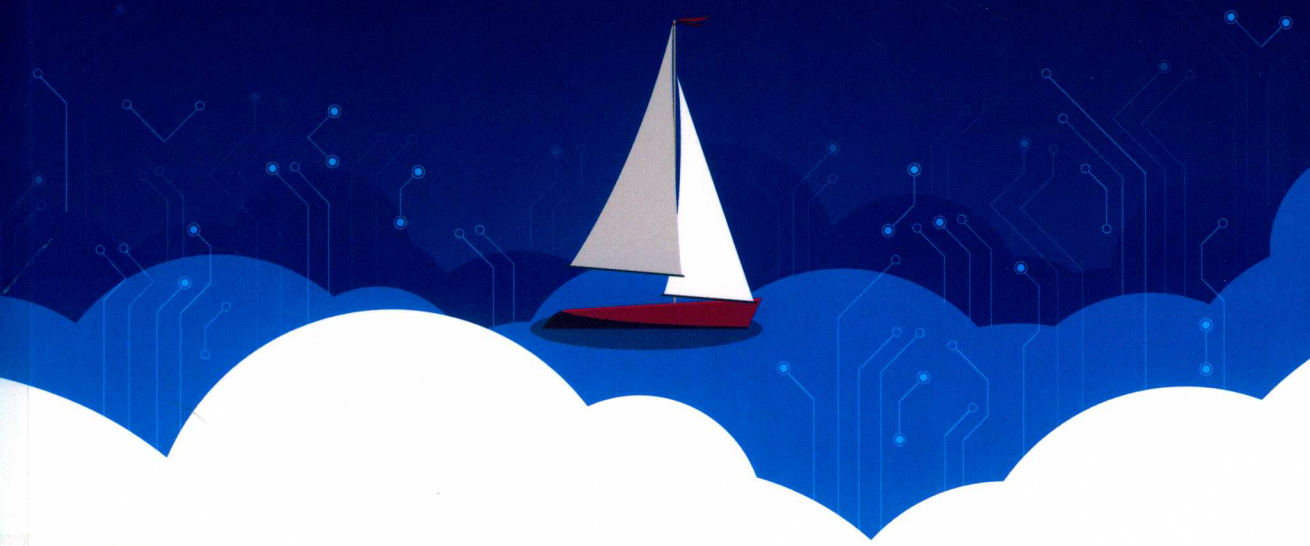
Broadview
www.broadview.com.cn

HUAWEI 华为云原生技术丛书

云原生服务网格 Istio

原理、实践、架构与源码解析

张超盟 章 鑫 徐中虎 徐 飞 编著



中国工信出版集团

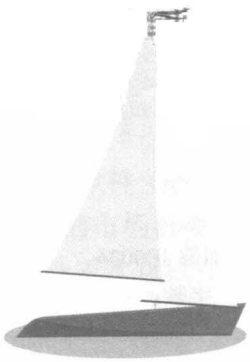
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

华为云原生技术丛书

云原生服务网格 Istio

原理、实践、架构与源码解析

张超盟 章 鑫 徐中虎 徐 飞 编著



電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书分为原理篇、实践篇、架构篇和源码篇，由浅入深地将 Istio 项目庖丁解牛并呈现给读者。原理篇介绍了服务网格技术与 Istio 项目的技术背景、设计理念与功能原理，能够帮助读者了解服务网格这一云原生领域的标志性技术，掌握 Istio 流量治理、策略与遥测和安全功能的使用方法。实践篇从零开始搭建 Istio 运行环境并完成一个真实应用的开发、交付、上线监控与治理的完整过程，能够帮助读者熟悉 Istio 的功能并加深对 Istio 的理解。架构篇剖析了 Istio 项目的三大核心子项目 Pilot、Mixer、Citadel 的详细架构，帮助读者熟悉 Envoy、Galley、Pilot-agent 等相关项目，并挖掘 Istio 代码背后的设计与实现思想。源码篇对 Istio 各个项目的代码结构、文件组织、核心流程、主要数据结构及各主要代码片段等关键内容都进行了详细介绍，读者只需具备一定的 Go 语言基础，便可快速掌握 Istio 各部分的实现原理，并根据自己的兴趣深入了解某一关键机制的完整实现。本书提供源码下载，参见 http://github.com/cloudnativebooks/cloud-native-istio。

无论是对于刚入门 Istio 的读者，还是对于已经在产品中使用 Istio 的读者，本书都极具参考价值。

图书在版编目（CIP）数据

云原生服务网格 Istio：原理、实践、架构与源码解析 / 张超盟等编著. —北京：电子工业出版社，2019.7
（华为云原生技术丛书）
ISBN 978-7-121-36653-6

Ⅰ. ①云… Ⅱ. ①张… Ⅲ. ①互联网络－网络服务器 Ⅳ. ①TP368.5

中国版本图书馆 CIP 数据核字（2019）第 100573 号

责任编辑：张国霞
印　　刷：三河市君旺印务有限公司
装　　订：三河市君旺印务有限公司
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：39.25　　字数：810 千字
版　　次：2019 年 7 月第 1 版
印　　次：2019 年 7 月第 1 次印刷
印　　数：5000 册　　定价：139.00 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。

推荐序

服务网格技术 Istio 是云原生（Cloud Native）时代的产物，是云原生应用的新型架构模式，而云原生又是云计算产业发展的新制高点。云计算是近 10 年左右流行的概念，但实际上，云已经走了很长一段路。

云的概念可以追溯到 20 世纪 60 年代。约翰·麦卡锡教授在 1961 年麻省理工学院的百年庆典上说："计算机也许有一天会被组织成一种公用事业，就像电话系统是一种公用事业一样。每个订阅者只需为实际使用的容量付费，就可以访问到具有非常庞大的系统的计算资源……"。第一个具有云特征的服务出现在 20 世纪 90 年代，当时，电信公司从以前主要提供点对点的专用数据电路服务，转到提供服务质量相当但成本较低的虚拟专用网络（VPN）服务。VPN 服务能够通过切换流量和平衡服务器的使用，更有效地使用整体的网络带宽。电信公司开始使用云符号来表示提供商和用户之间的责任界面。在自 20 世纪 60 年代以来流行的分时模式的基础上，服务提供商开始开发新的技术和算法，优化计算资源和网络带宽的分布，用户可以按需获取高端计算能力。

2006 年，亚马逊首次推出弹性计算云（EC2）服务，云计算的新时代开始了。两年后，第一个用于部署私有云和公有云的开源软件 OpenNebula 问世；谷歌则推出了应用引擎的测试版；Gartner 公司也首次提到了云的市场机会。2010 年，Rackspace 和 NASA 联手创建了 OpenStack 开源云计算平台，企业首次可以在标准硬件上构建消费者可以使用的云。甲骨文、IBM、微软等众多公司也相继发布云产品，云市场开始进入快速增长期。

云计算使企业摆脱了复杂而昂贵的 IT 基础设施建设和维护，因此，当时的云计算使用以资源（虚拟机、网络和存储）为主，也就是基础设施即服务（IaaS）。企业主要关心怎样将现有的 IT 基础架构迁移到云上，但在关键应用上对云还是敬而远之。随着云的成熟，包括 Netflix 和 Airbnb 在内的众多雄心勃勃的互联网初创公司开始把云计算变成了新商业模式，直接在云上构建企业的关键应用和业务；与此同时，在技术上，人们开始将

Linux 容器与基于微服务架构的应用结合起来，实现云应用真正意义上的可扩展、高可靠和自动恢复等能力，于是云原生计算诞生了。

云原生的崛起源于企业应用的快速发展和弹性可扩展的需求。在云原生时代最具代表性和历史性的技术是 Kubernetes 容器应用编排与管理系统，它提供了大规模和高效管理云应用所需的自动化和可观测性。Kubernetes 的成功源于应用容器的兴起，Docker 第一次真正使得容器成为大众所喜欢和使用的工具。通过对应用的容器化，开发人员可以更轻松地管理应用程序的语言运行环境及部署的一致性和可伸缩性，这引发了应用生态系统的巨变，极大地减小了测试系统与生产系统之间的差异。在容器之上，Kubernetes 提供了跨多个容器和多主机服务及应用体系结构的部署和管理。我们很高兴地看到，Kubernetes 正在成为现代软件构建和运维的核心，成为全球云技术的关键。Kubernetes 的成功也代表了开源软件运动所能提供的前所未有的全球开放与合作，是一次具有真正世界影响力的商业转型。华为云 PaaS 容器团队很早就开始参与这一开源运动，是云原生计算基金会 CNCF 的初创会员与董事，在 Kubernetes 社区的贡献位于全球前列，也是云原生技术的主要贡献者之一。

云原生容器技术和微服务应用的出现，推动了人们对服务网格的需求。那么，什么是服务网格？简而言之，服务网格是服务（包括微服务）之间通信的控制器。随着越来越多的容器应用的开发和部署，一个企业可能会有成百上千或数万计的容器在运行，怎样管理这些容器或服务之间的通信，包括服务间的负载均衡、流量管理、路由、运行状况监视、安全策略及服务间身份验证，就成为云原生技术的巨大挑战。以 Istio 为代表的服务网格应运而生。在架构上，Istio 属于云原生技术的基础设施层，通过在容器旁提供一系列网络代理，来实现服务间的通信控制。其中的每个网络代理就是一个网关，管理容器或容器集群中每个服务间的请求或交互。每个网络代理还拦截服务请求，并将服务请求分发到服务网格上，因此，众多服务构成的无数连接“编织”成网，也就有了“网格”这个概念。服务网格的中央控制器，在 Kubernetes 容器平台的帮助下，通过服务策略来控制和调整网络代理的功能，包括收集服务的性能指标。

服务网格作为一种云原生应用的体系结构模式，应对了微服务架构在网络和管理上的挑战，也推动了技术堆栈分层架构的发展。从分布式负载平衡、防火墙到服务的可见性，服务网格通过在每个架构层提供通信层来避免服务碎片化，以安全隔离的方式解决了跨集群的工作负载问题，并超越了 Kubernetes 容器集群，扩展到运行在裸机上的服务。因此，虽然服务网格是从容器和微服务开始的，但它的架构优势也可以适用于非容器应用或服务。

从初始的云理念到云计算再到云原生的发展过程中，我们看到服务网格是云原生技术

发展的必然产物。作为云原生架构和技术栈的关键部分，服务网格技术 Istio 也逐渐成为云原生应用平台的另一块基石，这不仅仅是因为 Istio 为服务间提供了安全、高可靠和高性能的通信机制，其本身的设计也代表一种由开发人员驱动的、基于策略和服务优先的云原生架构设计理念。本书作者及写作团队具有丰富的 Istio 实战经验，在本书中由浅入深地剖析了 Istio 的原理、架构、实践及源码。通过阅读本书，读者不但能够对 Istio 有全面的了解，还可以学到云原生服务网格的设计思路和理念，对任何一名软件设计架构师或工程师来说都有很大的帮助，这是一本非常有价值的云原生时代分布式系统书籍。

廖振钦
华为云 PaaS 产品部总经理

前言

这是一本介绍“云原生”与“服务网格”技术的书籍。你或许对这两个词语感到陌生，或者耳熟却不明其意，其实，这两个术语分别与“云计算”与“微服务”的概念有着非常紧密的联系。

依据 CNCF 基金会（Cloud-Native Computing Foundation）的定义，云原生是对在现代的动态环境下（比如云计算的三大场景：公有云、私有云及混合云）可用来构建并运行可扩展应用的技术的总称；服务网格则是云原生技术的典型代表之一，其他技术还包括容器、微服务、不可变基础设施、声明式 API 等。

从技术发展的角度来看，我们可以把云原生理解为云计算所关注的重心从“资源”逐渐转向“应用”的必然结果。以“资源”为中心的上一代云计算技术关注物理设备如何虚拟化、池化、多租化，典型代表是计算、网络、存储三大基础设施的云化，以及相关硬件、操作系统、管控面等技术；而以“应用”为中心的云原生技术则关注应用如何更好地适应云环境，相对于传统应用通过迁移改造“上云”而言，云原生希望通过一系列的技术支撑，使用户能够在云环境下快速开发和交付云原生应用。

作为云原生技术栈的一部分，服务网格则指由云原生应用的服务化组件构成的一种网格。换句话说，我们可以将服务网格理解为一种应用网络，即为在应用内部或应用之间由服务访问、调用、负载均衡等服务连接关系构成的一种网络。你可能会注意到，这里并没有使用“微服务”这个术语。微服务更多地从设计、开发的视角来描述应用的一种架构或开发模式，而服务网格事实上更为关注运行时视角，因此，采用“服务”这个用于描述应用内外部调用关系的术语更为合适。服务网格与微服务在云原生技术栈中是相辅相成的两部分，前者更关注应用的交付与运行时，后者更关注应用的设计与开发。

本书的主角 Istio，作为服务网格技术的事实标准，是一个比较年轻的开源项目。它在 2017 年 5 月由 Google 与 IBM 联合发布之后，经过一年多的快速发展，于 2018 年 7 月发

布了 1.0 版本，并于 2019 年 3 月发布 1.1 这个大更新版本，该版本算是第一个生产可用的 GA 版本（虽然官方宣称 1.0 版本“Production-Ready”，但从实践评估来看，1.1 作为 GA 版本更合适一些）。

Istio 体现了云原生领域核心项目 Kubernetes 的创建者 Google 对服务网格技术的思考，还包含了云计算先行者 IBM 对服务网格最早的实践经验，因此一经发布就得到云原生领域的广泛响应，它是继 Kubernetes 之后云原生领域非常火爆的项目之一。截至 2019 年年初，国内外已经有超过百家公司的公开实践案例。

本书作者所在的华为公司作为云原生领域的早期实践者与社区领导者之一，在 Istio 项目发展初期就参与了 Istio 社区，积极实践 Istio 并推动 Istio 项目的发展。目前，华为公司内部的多个产品线已经使用了 Istio，部分实践已经进入生产环境，Istio 的商业化产品也已经包含在华为公有云、私有云、混合云解决方案中，并面向华为云客户群进行推广。华为作为 Istio 社区的当前领导者之一，会继续致力于 Istio 项目及服务网格技术的推广与演进。

本书写作目的

本书作为华为云原生技术丛书的一员，面向云计算领域的从业者及感兴趣的技术人员，普及与推广 Istio 服务网格技术。本书作者来自华为云应用服务网格产品研发团队及华为云原生开源社区团队。本书结合作者在华为云及 Istio 社区的设计与开发实践，以及与服务网格强相关的 Kubernetes 容器、微服务和云原生领域的丰富经验，对服务网格技术、Istio 开源项目的原理、实践，架构和源码进行了深入剖析，由浅入深地讲解 Istio 的功能、用法、设计与实现，帮助读者全面、立体地了解云原生服务网格 Istio 的每个技术细节。对于刚入门的读者，本书提供了从零开始的 Istio 上手实战指导；对于已经在产品中使用 Istio 的读者，本书也提供了丰富的案例与经验总结。

本书结构

本书分为原理篇、实践篇、架构篇和源码篇，总计 24 章，由浅入深地将 Istio 项目庖丁解牛并呈现给读者。

对于有不同需求的读者，我们建议这样使用本书。

◎ 对云原生技术感兴趣的读者，可阅读并理解原理篇。本篇介绍了服务网格技术与 Istio 项目的技术背景、设计理念与功能原理，能够帮助读者了解服务网格这一云原生领域的标志性技术，掌握 Istio 流量治理、策略与遥测和安全功能的使用方法。

◎ Istio 一线实践者或动手能力较强的技术人员，通过实践篇可以从零开始搭建 Istio 运行环境并完成一个真实应用的开发、交付、上线监控与治理的完整过程，能够熟悉 Istio 的功能并加深对 Istio 原理的理解。

◎ 关注 Istio 架构设计或者正在评估是否将 Istio 引入当前技术栈的技术人员，架构篇能够帮你剖析 Istio 项目的三大核心子项目 Pilot、Mixer、Citadel 的详细架构，熟悉 Envoy、Galley、Pilot-agent 等相关项目，并深入挖掘 Istio 代码背后的设计与实现思想。

◎ 对 Istio 源码感兴趣且希望更深入地了解 Istio 实现细节的读者，可以通过源码篇进入 Istio 源码世界。源码篇对 Istio 各个项目的代码结构、文件组织、核心流程、主要数据结构及各主要代码片段等关键内容都进行了详细介绍。读者只需具备一定的 Go 语言基础，便可快速掌握 Istio 各部分的实现原理，并根据自己的兴趣深入了解某一关键机制的完整实现，以期成为 Istio 高手，甚至作为贡献者参与到 Istio 项目开发中来。

本书篇章组织概述如下。

◎ 原理篇：介绍 Istio 概念、核心功能、原理和使用方式，为后续的实践提供理论基础。其中，第 1～2 章分别介绍 Istio 的背景知识、基本工作机制、主要组件及概念模型等；第 2～7 章分别介绍 Istio 的五大块功能集，即非侵入的流量治理、可扩展的策略和遥测、可插拔的服务安全、透明的 Sidecar 机制及多集群服务治理。

◎ 实践篇：通过实际操作介绍如何通过一个典型应用进行 Istio 实践。其中，第 8 章讲解环境准备，完成 Kubernetes 与 Istio 平台的基础设施准备工作；第 9～13 章分别介绍如何实际操作一个天气预报应用在 Istio 平台上实现流量监控、灰度发布、流量治理、服务安全、多集群管理等功能。

◎ 架构篇：从架构角度剖析 Istio 多个主要组件的设计原理、关键内部流程及数据结构等内容，为高级用户提供架构与设计层面的参考。其中，第 14～19 章分别介绍了 Pilot、Mixer、Citadel、Envoy、Pilot-agent 与 Galley 等 6 个 Istio 核心组件。

◎ 源码篇：本篇包括第 20～24 章，分别介绍 Istio 整体的代码组织情况，以及 Pilot、Mixer、Citadel、Envoy 与 Galley 的代码结构与关键代码片段。

源代码与官方参考

Istio 是一个开源项目，本书也开源了实践篇示例应用的源代码，读者可通过如下链接获取本书源码及相关内容。

◎ Istio 项目官网：https://istio.io/。
◎ Istio 源代码：https://github.com/istio。
◎ 本书示例应用源代码：https://github.com/cloudnativebooks/cloud-native-istio。

勘误和支持

若您在阅读本书的过程中有任何问题或者建议，则可以通过本书源码仓库提交 Issue 或者 PR，也可以关注华为云原生官方微信公众号并加入微信群与我们交流。我们十分感谢并重视您的反馈，会对您提出的问题、建议进行梳理与反馈，并在本书后续版本中及时做出勘误与更新。

致谢

在本书的写作及成书过程中，本书作者团队得到了公司内外许多领导、同事及朋友的指导、鼓励和帮助。感谢华为云郑叶来、张宇昕、廖振钦、方璞等业务主管对华为云原生技术丛书及本书写作的大力支持；感谢华为云容器团队王泽锋、罗荣敏、毛杰、张琦等对本书的审阅与建议；感谢华为云应用服务网格团队陈冬冬、巩培尧、王少东、李汉辰、秦玉函、张云等为本书编写示例程序及分享实践经验；感谢电子工业出版社博文视点张国霞编辑一丝不苟地制订出版计划及组织工作；感谢华为云邢紫月对本书的出版建议与指导；最后，也感谢 CNCF 基金会及 Istio、Kubernetes 社区众多开源爱好者辛勤、无私的工作，使得我们在这个技术爆发的时代能够充分领略到技术的魅力并能够亲身参与到这份有激情、有挑战的事业中来。谢谢大家！

刘赫伟 博士
华为云原生技术丛书 总编
华为云容器服务域 技术总监

张超盟
华为云应用服务网格 首席架构师

目录

原 理 篇

实 践 篇