O'REILLY®

Broadview®
www.broadview.com.cn

混沌工程

Netflix系统稳定性之道

Casey Rosenthal
Lorin Hochstein
[美] Aaron Blohowiak 著
Nora Jones
Ali Basiri

侯杰◎译

Chaos Engineering

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

O'REILLY®

混沌工程

Netflix系统稳定性之道

Casey Rosenthal
Lorin Hochstein
[美] Aaron Blohowiak 著
Nora Jones
Ali Basiri

侯杰◎译

Chaos Engineering

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

内 容 简 介

在一个由很多微服务组成的分布式系统中，我们永远难以全面掌握发生什么事件会导致系统局部不可用，甚至全面崩溃。但我们却可以尽可能地在这些不可用的情况发生之前找出系统中的脆弱点。本书介绍了 Netflix 的工程师团队是如何根据多年实践经验主动发现系统中脆弱点的一整套方法。这套方法现在已经逐渐演变成计算机科学的一门新兴学科，即“混沌工程”。通过一系列可控的实验和执行实验的原则，混沌工程将揭示出分布式系统中随时发生的各类事件是如何逐步导致系统整体不可用的。

本书既适合研发、测试人员用来了解如何构建健壮的系统，也适合软件架构师用来了解设计创建高可用微服务体系的前沿方法，同时更适合在大型互联网或技术组织中专门负责系统稳定性的工程团队阅读。

版权贸易合同登记号　图字：01-2019-4197

图书在版编目（CIP）数据

混沌工程：Netflix 系统稳定性之道 /（美）凯西·罗森塔尔（Casey Rosenthal）等著；侯杰译. —北京：电子工业出版社，2019.8
书名原文：Chaos Engineering
ISBN 978-7-121-36351-1

Ⅰ. ①混… Ⅱ. ①凯… ②侯… Ⅲ. ①分布式计算机系统－系统工程 Ⅳ. ①TP338.8

中国版本图书馆 CIP 数据核字（2019）第 071011 号

责任编辑：刘恩惠
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：787×1092　1/32　印张：3.75　字数：72 千字
版　　次：2019 年 8 月第 1 版
印　　次：2019 年 8 月第 1 次印刷
定　　价：45.00 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。

目录

O'REILLY®

混沌工程

Netflix系统稳定性之道

Casey Rosenthal
Lorin Hochstein
[美] Aaron Blohowiak 著
Nora Jones
Ali Basiri

侯杰◎译

Chaos Engineering

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

内 容 简 介

在一个由很多微服务组成的分布式系统中，我们永远难以全面掌握发生什么事件会导致系统局部不可用，甚至全面崩溃。但我们却可以尽可能地在这些不可用的情况发生之前找出系统中的脆弱点。本书介绍了 Netflix 的工程师团队是如何根据多年实践经验主动发现系统中脆弱点的一整套方法。这套方法现在已经逐渐演变成计算机科学的一门新兴学科，即“混沌工程”。通过一系列可控的实验和执行实验的原则，混沌工程将揭示出分布式系统中随时发生的各类事件是如何逐步导致系统整体不可用的。

本书既适合研发、测试人员用来了解如何构建健壮的系统，也适合软件架构师用来了解设计创建高可用微服务体系的前沿方法，同时更适合在大型互联网或技术组织中专门负责系统稳定性的工程团队阅读。

版权贸易合同登记号　图字：01-2019-4197

图书在版编目（CIP）数据

混沌工程：Netflix 系统稳定性之道 /（美）凯西·罗森塔尔（Casey Rosenthal）等著；侯杰译. —北京：电子工业出版社，2019.8
书名原文：Chaos Engineering
ISBN 978-7-121-36351-1

Ⅰ. ①混… Ⅱ. ①凯… ②侯… Ⅲ. ①分布式计算机系统－系统工程 Ⅳ. ①TP338.8

中国版本图书馆 CIP 数据核字（2019）第 071011 号

责任编辑：刘恩惠
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：787×1092　1/32　印张：3.75　字数：72 千字
版　　次：2019 年 8 月第 1 版
印　　次：2019 年 8 月第 1 次印刷
定　　价：45.00 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。

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。无论是通过书籍出版、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

序

要设计良好的系统需要考虑很多因素，比如可靠性、安全性、可扩展性、可定制化、可伸缩性、可维护性、用户体验等。为了更高效地支撑业务发展，越来越多的企业选择基于云服务或云原生理念来构建平台。采用新思路和新技术必然会带来系统架构和组织结构的变革，引入风险因素。如何通过实验证明生产环境下的分布式系统在面对失控条件的时候依然具备较强的“可观测性”和故障恢复能力呢？这就是混沌工程要解决的问题。

为了提升研发效率、支撑未来业务发展，2008 年淘宝完成了服务化拆分和改造。伴随着应用数量的激增，多起因为不合理依赖导致的可用性故障发生了。作为保障高可用的技术团队，2011 年我们开始尝试使用故障注入的方法来验证和治理系统

的依赖问题，并在故障模拟实现、自动化验证、环境隔离、流量制造等方面进行了多次方案升级，沉淀了一套自动化的依赖治理方案。2016 年，为了更真实地验证系统的容错设计和组织响应问题的能力，我们开始尝试在生产环境中进行故障场景演练。通过几年的发展，线上故障演练已经覆盖了大部分核心业务，提前发现了很多系统、工具、流程方面的问题。

也许很多人听说过 Netflix 的 Chaos Monkey，但是大多数人对于混沌工程的概念还是比较模糊的。随着 2017 年本书的英文版面世，这种状况得到了改观。书中凝聚了第一批混沌工程师的智慧和经验，从建立稳定状态的假设、用多样的现实世界事件做验证、在生产环境中进行实验、自动化实验以持续运行、最小化爆炸半径五个角度对混沌工程进行抽象和概括，详细地阐述了混沌工程的演进和实践原则。书中的每条原则都既传递了一种思想，也代表着一套工具产品的设计思路。结合阿里巴巴在依赖治理、故障演练方面的实践积累，更能体会到每条原则的精妙。

近两年，混沌工程发展得很快，2017 年被收录到 ThoughtWorks 的技术雷达中，2018 年成为 CNCF（Cloud Native Computing Foundation）的一个技术领域，越来越多的企业开始计划引入混沌工程。作为混沌工程的早期实践者和推动者，有三点经验与大家分享：

第一，引入混沌工程，需要建立进行面向失败设计（可以使系统暴露出已有问题的设计）和拥抱失败的技术文化。

在思想上要认识到混沌工程的核心是通过引入一些风险变量去暴露已有问题，而不是创造问题。在恰当的时间和可控的爆炸半径下进行实验，有助于问题的发现和处理，降低潜在故障带来的影响。

传统的基础设施对稳定性和健壮性有非常高的要求，虽然降低变更频率可以减少故障，但这不是解决问题的根本方法。随着各项服务被迁移到云上，基础设施的管理被转移给云厂商负责，上层业务更需要做好面向失败设计才可以应对可能存在的极端情况。

第二，实施混沌工程，需要定义一个清晰可衡量的目标。

混沌工程的业务价值并不适合用过程指标（比如模拟了多少种实验场景、发起多少次实验等）来衡量，需要配合其他稳定性手段一起来衡量。比如，前期可以选择对历史故障进行复现，确保故障改进的有效性；中期可以选择监控发现率，验证故障发现能力和监控的完备程度；随着实施混沌工程的经验越来越丰富，后期可以考虑引入一些复杂的 MTTR（Mean Time To Restoration）度量指标，比如故障的“发现-定位-恢复”时长这种综合性指标。

第三，推广混沌工程，要在控制风险的前提下不断提升效率。

越贴近生产环境的实验，结果越真实，同时风险也越大。大家可以先从一些简单的场景开始尝试，逐渐增加对系统和组织的信心。实验准备比实验执行更重要，混沌工程不是故障注入测试，要明确定义系统稳定状态和终止条件。

混沌工程是一种实践思想，本身不绑定任何技术或工具。不过在进行规模化推广和实施时，从真实性、开发成本、运维效率的角度考虑，还是建议复用一些成熟的开源组件或商业工具。

减少问题的最好方法就是让问题经常性地发生，通过不断重复失败过程并找出解决方案，来持续提升系统的容错能力和弹性。混沌工程作为一门新兴学科，还处于一个定义和被定义的过程。如果你对混沌工程感兴趣，愿意去了解和实践混沌工程，非常推荐你从阅读本书开始行动。

周洋（花名：中亭）
阿里巴巴高可用架构团队高级技术专家
开源项目 ChaosBlade 发起人
2019.4

译者序

软件服务于人类的历史，历经了从单机软件在本地运行，到复杂系统通过网络提供服务的发展历程。软件的功能和质量每向前发展一步，都伴随着更多新的组成部分的加入。为了更好地服务于更多用户，进行规模更大、更复杂的运算，软件系统的能力需要不断进化升级，小型软件开始一步一步演化发展为大型分布式复杂系统。在软件系统变强的同时，越来越多的组成部分被加入系统，复杂性也在随之逐步增加。

每个软件从业者从写下第一行代码开始，就一刻不停地在和软件中的错误做斗争。开发和维护（修复缺陷、确保资源充足等保障软件运行的活动）是一对伴随软件运行而产生的双生子。热爱从零到一开发软件是开发者的天性，看着自己编写的软件完美运行，为其他人提供服务，一直是驱动开发者前进的

动力。为了更快更好地开发软件，我们不断改进开发方法和软件架构，但是开发者在使用新的方法和更复杂的架构时，往往会低估潜在的风险。

近年来，随着系统架构逐渐向微服务架构演化，开发效率以及系统扩展性大幅提高。但同时，系统的复杂性也随之逐渐增长到了一个拐点，传统的测试方法已经不能全面理解和覆盖系统所有可能的行为，测试的有效性被大打折扣。我们通过各种测试、SRE、DevOps、金丝雀发布、蓝绿部署、预案、故障演练等方法，希望能够防患于未然。但服务规模不断增长，服务之间的依赖性所带来的不确定性也呈指数级增长。在这样的服务调用网中，任何一环出现的正常或异常的变化，都有可能对其他服务造成类似蝴蝶效应一般的影响。

软件系统自身复杂度的激增、开发者在引入复杂性的同时对风险的低估和忽视，是系统可用性面临的两大挑战。

为了应对这两大挑战，Netflix 选择了一条不同寻常的路。从混乱猴子开始，Netflix 为应对不确定性的领域带来了一种全新的思维方式——主动出击。这种主动出击的思维方式衍生出的一套实践方法，被称为混沌工程（Chaos Engineering），它旨在从根本上改变开发者应对软件缺陷和故障的思维方式。在此之前，我们期望通过一系列的测试验证手段，尽最大的可能确

保在线上运行的系统没有缺陷和故障。而混沌工程的理念认为这既不现实，也不符合系统自然发展的规律。混沌工程提倡我们首先要正面接受系统一定会存在缺陷，并且一定会时不时地发生故障的事实；然后，要求我们通过一系列实验找出可能发生问题的风险点，进而在不断加固系统的同时，促使开发者在开发软件时必须选择将防御性内建在系统中。

混沌工程的理论，建构于塔勒布在《反脆弱》一书中所阐述的思想之上，即系统如何在不确定性中获益。在接受“系统越复杂，越脆弱”的事实之后，让系统在每一次失败中获益，然后不断进化，这是混沌工程的核心思想。在实践中，混沌工程提倡用一系列实验来真实地验证系统在各类故障场景下的表现，通过频繁地进行大量实验，既使得系统本身的反脆弱性持续增强，也让开发者对系统越来越有信心。这个信心同时也是系统高速迭代，占尽市场先机的一个前提因素。

各个行业都涌现出了很多基于混沌工程应对上述两大挑战的实践案例。译者所从事的汽车金融行业是一个长链条，重流程，涉及获客、风控、审批、资金流转、贷后管理等多个环节的复杂业务体系。任何差错都有可能造成故障及问题数据的蔓延，轻则导致各种程度的业务不可用，重则可能会造成重大资损（资产损失）。传统的各类方法已经无法保障这样一个大