

BEIJING 2017

淘宝开放平台网关技术揭密

顾风胜



目录

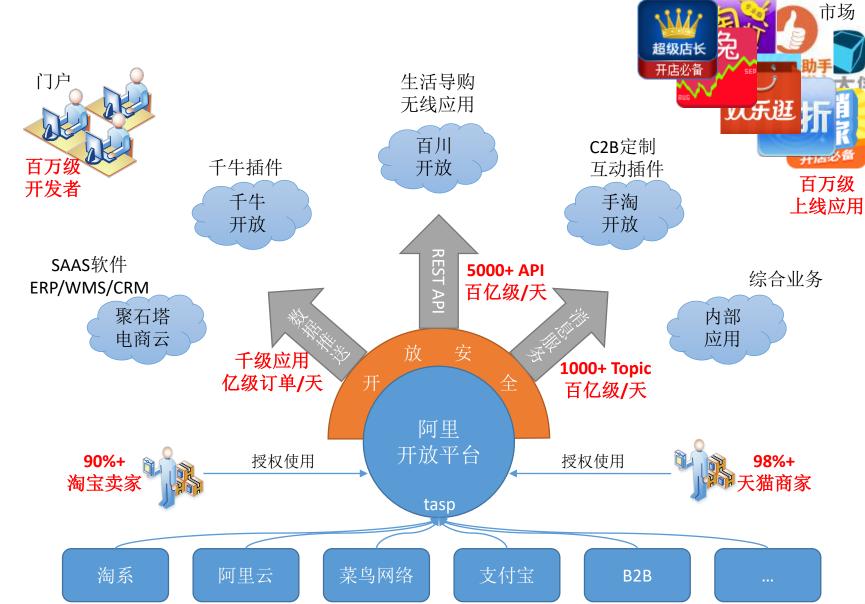
- 01 开放平台概览
- 02 API网关介绍
- 03 API接入自动化
- 04 开放平台工厂
- 05 开放平台安全



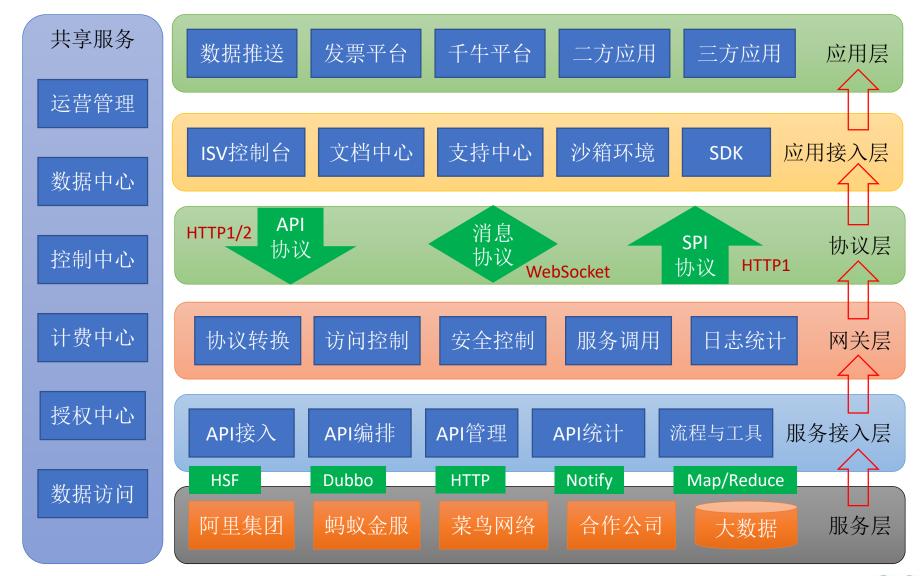
第一部分 开放平台概览

服务

开放平台大图



开放平台技术架构



开放平台产品架构

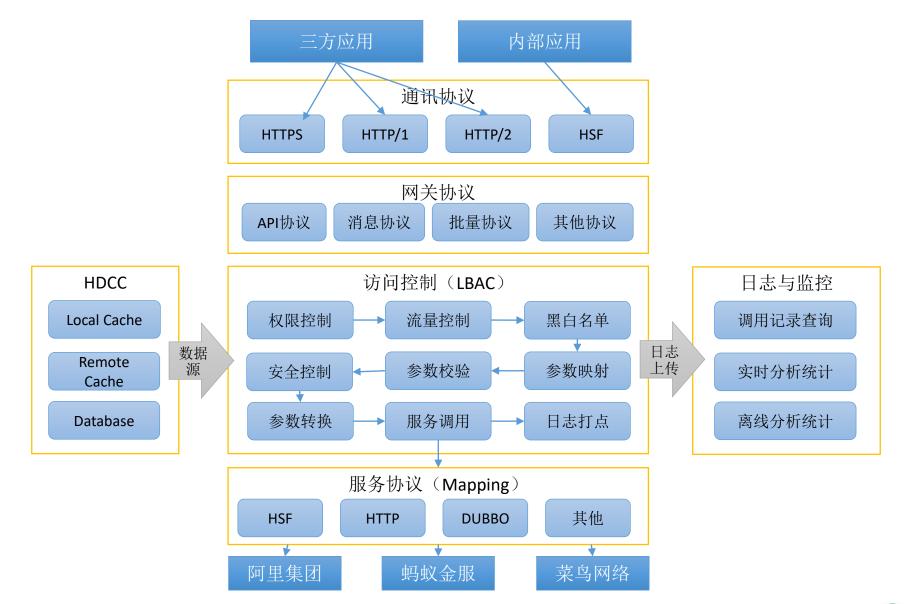


第二部分 API网关介绍

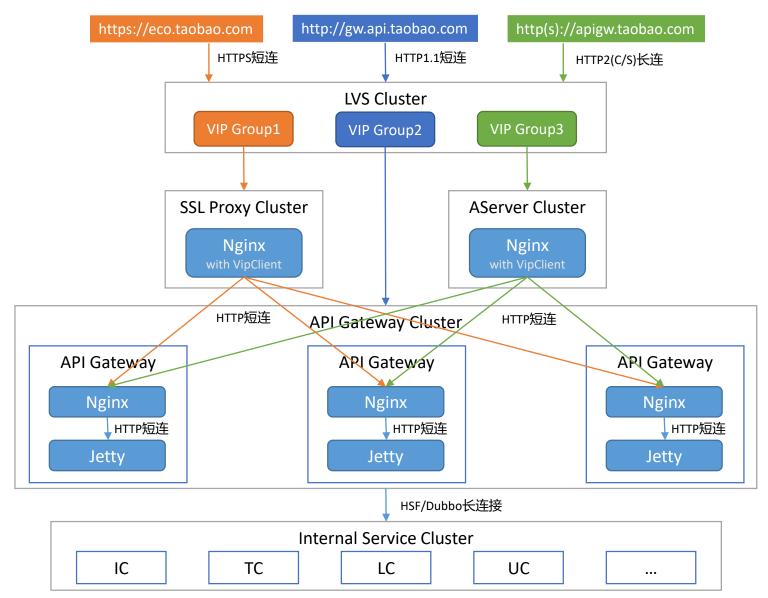
如何打造高可靠的API网关



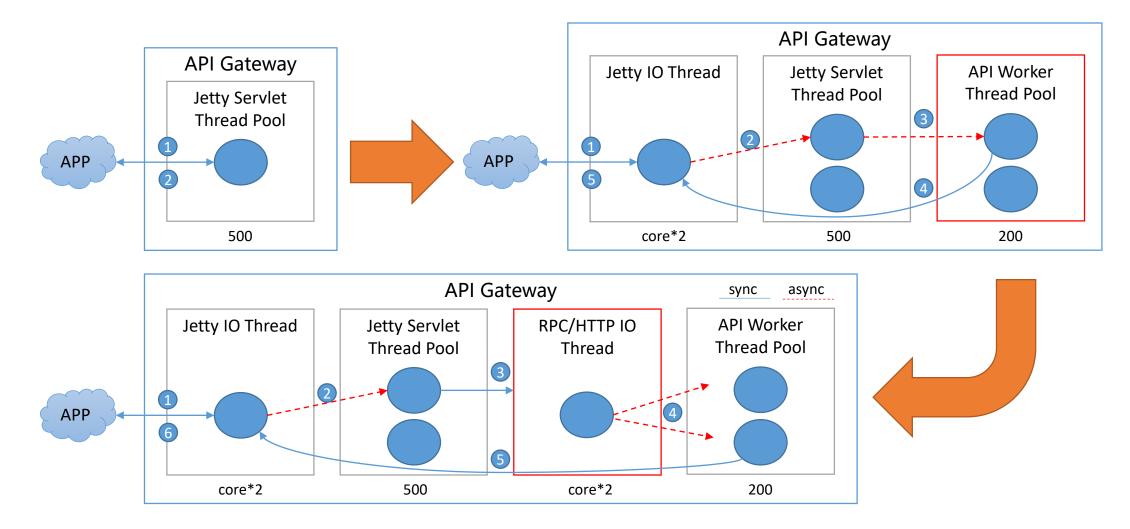
API网关技术架构



API网关部署架构

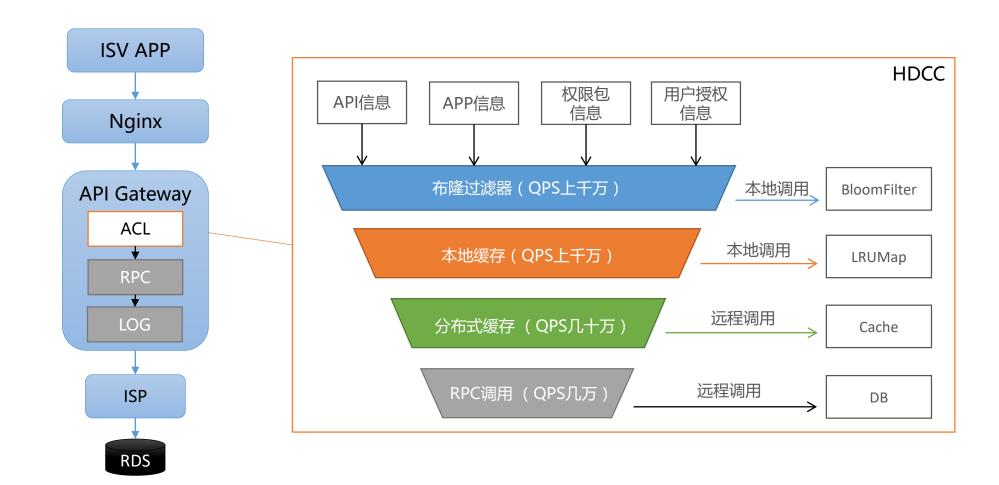


API请求全异步化



释放网络等待引起的线程占用,线程数不再成为网关的瓶颈彻底隔离API请求之间的影响,慢API不会引起网关的不稳定

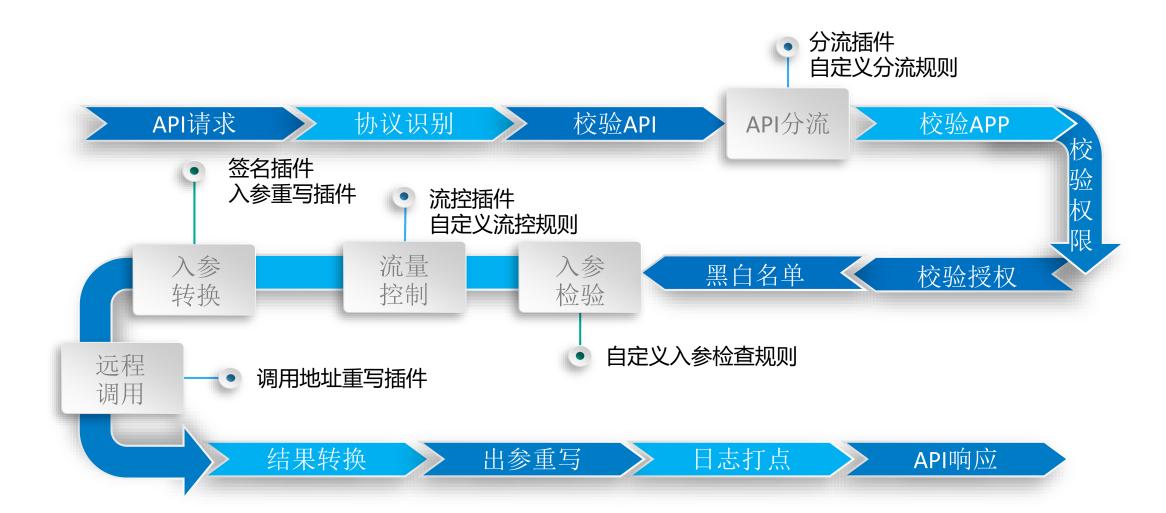
API元数据无阻塞调用



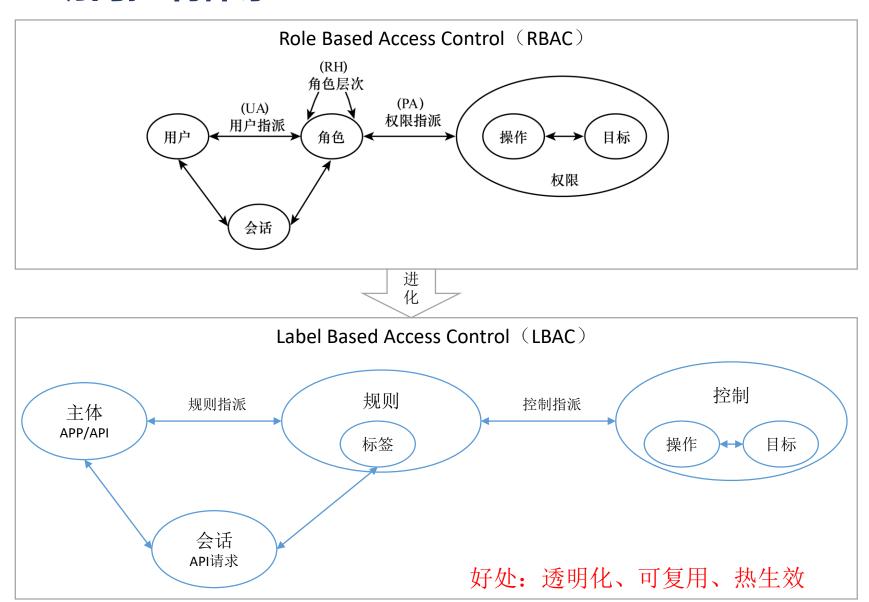
消灭99.9%的IO等待, CPU只用于计算资源 网关耗时降低到1~2毫秒, 较少的DB资源支持高并发



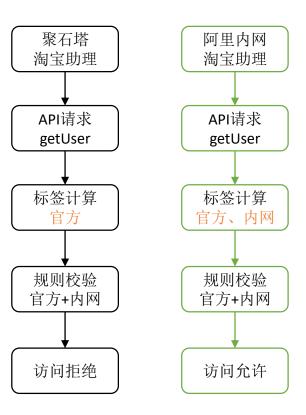
API插件化体系 — 运行时升级网关



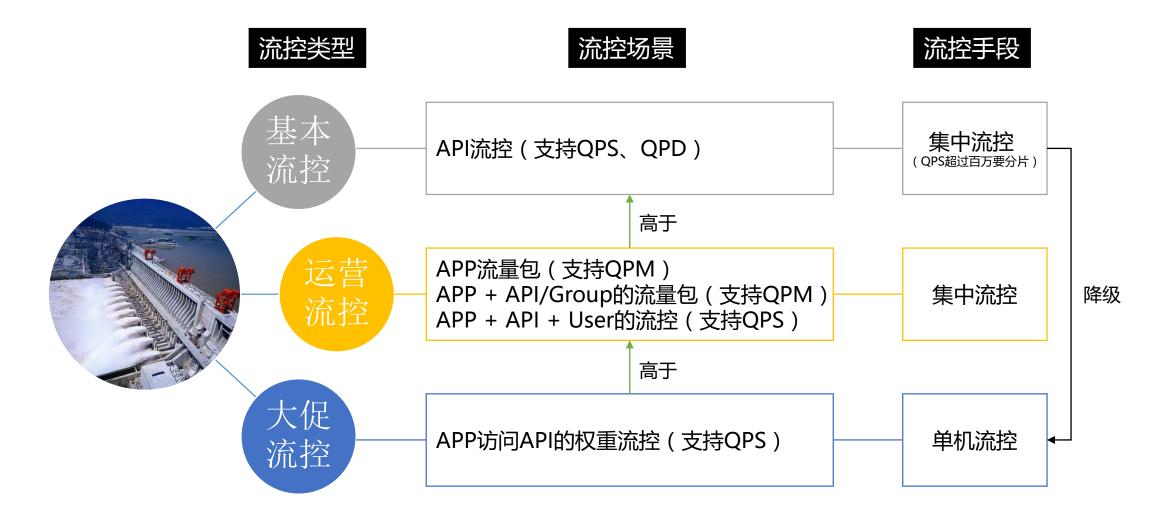
API访问控制体系 — LBAC



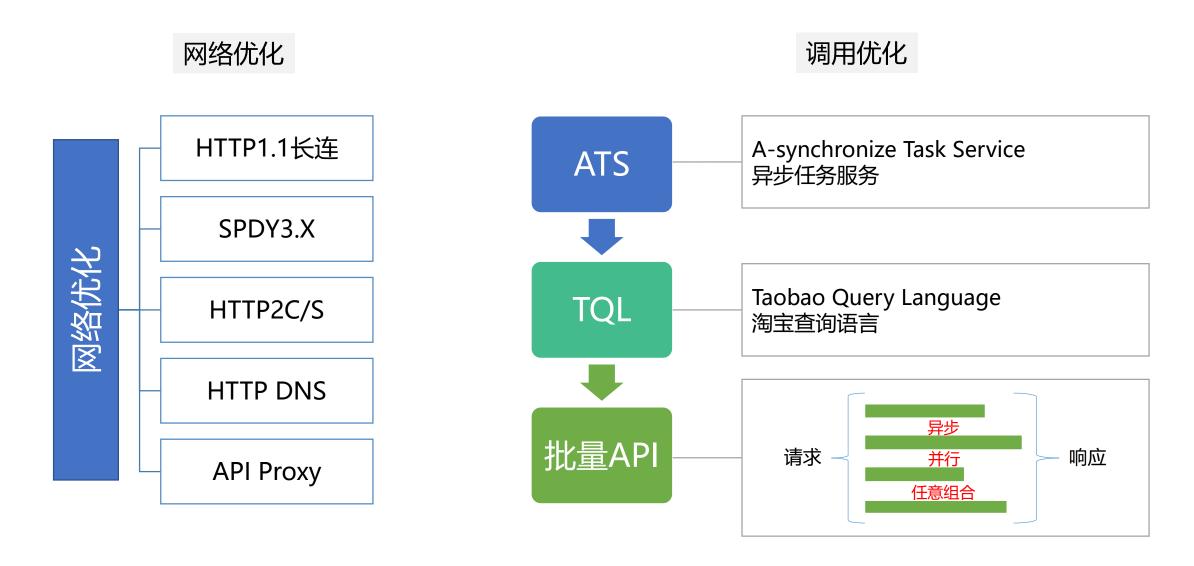
举例: getUser接口只允许 官方应用从内网发起调用



API流量控制

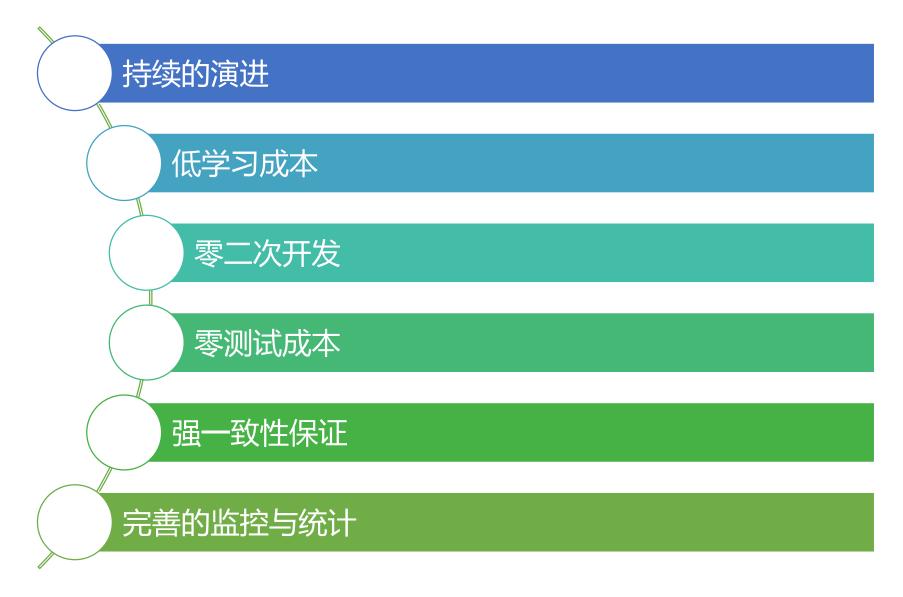


API弱网环境调用优化



第三部分 API接入自动化

如何打造高效的API接入管理平台



API接入自动化演进

纯手工(2009年)

半自助(2011年)

全自助(2015年)

学习

编码



联调



发布

文档



SDK

无从下手,只能找人

依赖业务方Jar包,手写 XML与JSON映射

远程Debug,手写HTTP 代码调用API

无

与应用一起发布

手工写Wiki文档

手工写JAVA SDK

看文档和教程

依赖网关Jar包,手写 Mapping,配置Spring

部署应用,部署API, API测试工具

靠自觉, 旺旺电话催

开放平台小二发布API

自动生成 (对外文档)

自动生成(.NET&JAVA)

流程化接入, 无学习成 本

零依赖,零编码,支持 HSF、Dubbo、HTTP

智能部署,自动化测试

BPM流程、移动审批

自主发布,灰度发布, 一键回滚

自动生成(对内文档, 对外文档,PDF文档)

自动生成,Maven自动 上传,主流语言支持

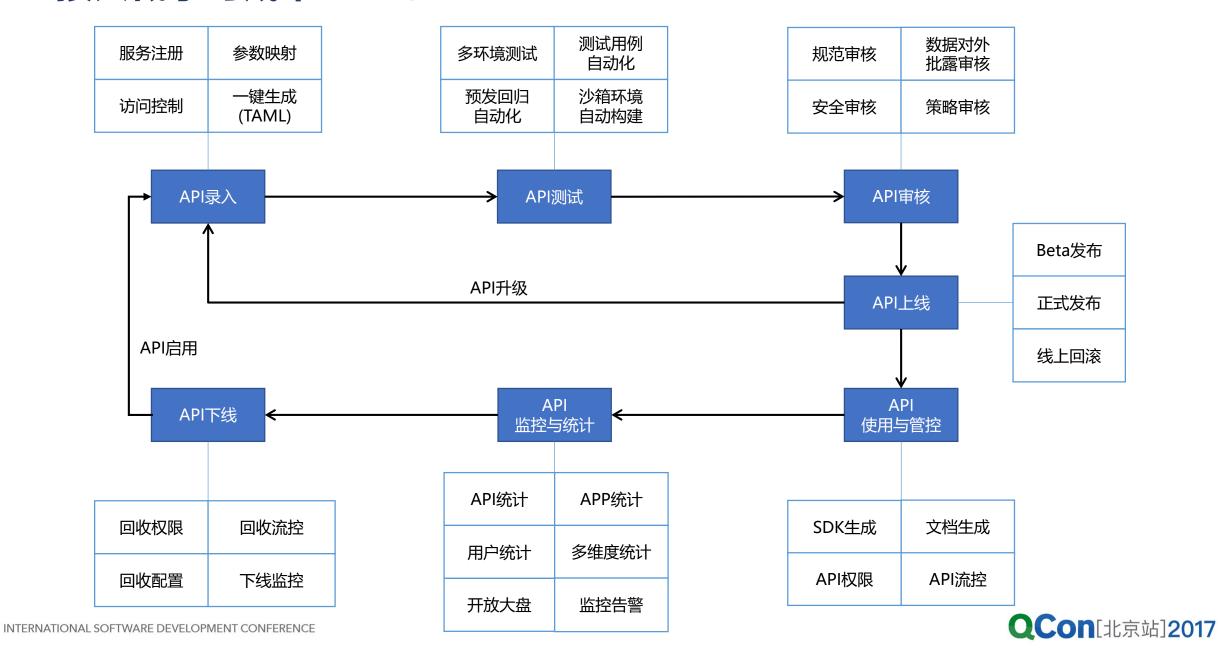
一个月

一周

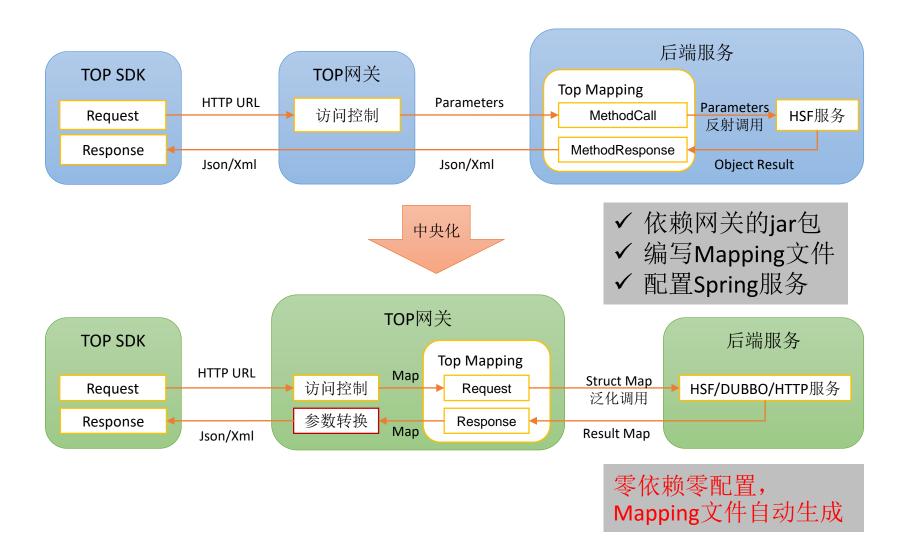
一天



API接入低学习成本 — 流程化与自助化



API接入的零二次开发 — 映射中央化



API变更零测试成本 — 回归测试自动化 线上请求 ISP提交API测试 API请求流程 线上 预发 Mock返 API 环境 环境 入参 回值 API正式网关 回归测试工具 API 消息监听器 请求拦截器 配置规则 入参映射 线上参数 线上结果 命中规则 **RPC** 入参 公网消 息队列 消息处理器 ISP线上服务 **RPC** 读执行器 写执行器 服务 线上参数 反推RPC出参 重试请求 API预发网关 RPC 出参 ↓ 出参映射 ISP预发服务 ISP预发Mock API 出参 Ν 结果比较器 测试报告 INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

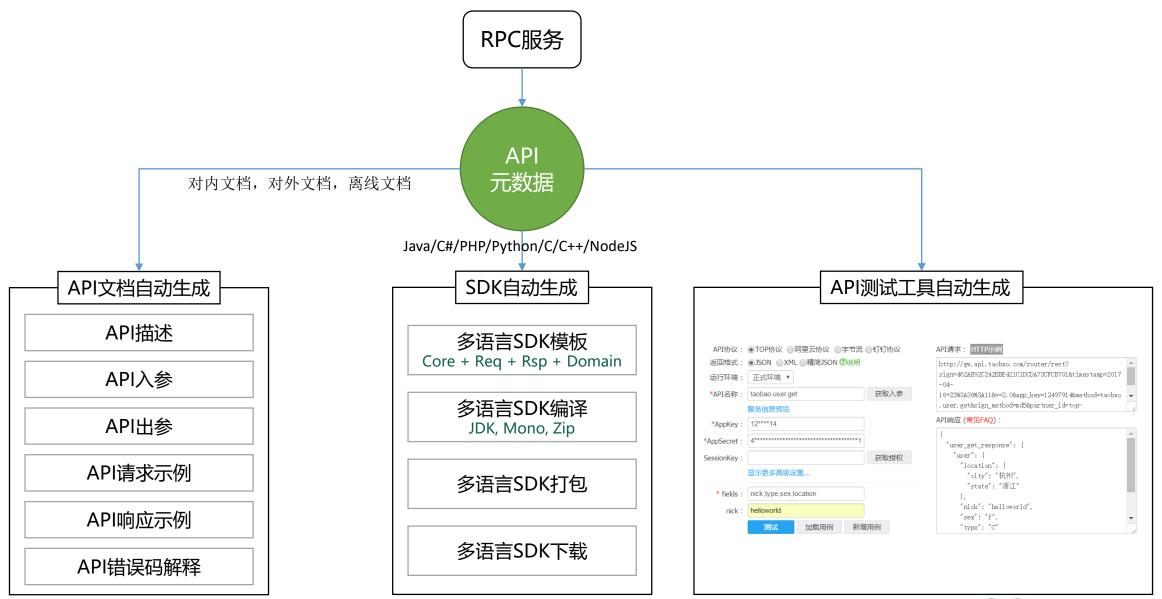
关键点:

- 线上请求复制到预发
- 自动生成测试用例
- API请求重放(读API)
- API结果Mock(写API)
- · API测试结果比较

优势:

- 测试用例全面
- 快速发现问题
- 零测试成本
- 变更稳定性保障

API元数据强一致性保证 — 自动化生成文档、SDK、工具



API接入自动化演示 — 三分钟接入一个API

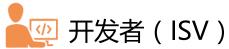
和阿里开放平台 ?帮助~ 关键字 Q **★** 开放 □运营 ◎风胜 ~ ■ 数据 多运维 API / 我的变更 ~ API 我的变更 ▼ ・ 变更范围: 我负责的 ▼ ・ 变更状态: 进行中 ▼ ・ 所属项目: 搜索 API类型: 我的项目 所属项目 变更原因 API名称 负责人 进度 操作 所有API 萧玄 承仙 风胜 日常测试中-未审核 支付宝收藏夹消息 TOP专用日常 预览API 修改变更 关闭变更 taobao_mercury_Add > 工具 似年 > 权限 萧玄 承仙 风胜 taobao cart UnDelete 日常测试中-未审核 TOP专用日常 taobao_cart_UnDelete 预览API 修改变更 关闭变更 似年 > 流程 萧玄 承仙 风胜 支付宝消息接入 日常测试中-未审核 TOP专用日常 预览API 修改变更 关闭变更 taobao cart Delete > 文档 似年 萧玄 承仙 风胜 支付宝消息接入 TOP专用日常 日常测试中-未审核 预览API 修改变更 关闭变更 taobao_cart_Update 似年 萧玄 承仙 风胜 支付宝消息接入 TOP专用日常 日常测试中-未审核 预览API 修改变更 关闭变更 taobao_cart_Add 似年 萧玄 承仙 风胜 TOP专用日常 taobao.item.rules.vip.check API 3.0 TOP专用日常 录入中 预览API 修改变更 关闭变更 似年 萧玄 吴迪 风胜 萧玄测试日常 录入中 taobao.sunshao.test.samservice API 2.0 萧玄测试日常 预览API 修改变更 关闭变更 溪行 萧玄 吴迪 风胜 录入中 萧玄测试日常 萧玄测试日常 预览API 修改变更 关闭变更 taobao.xiaoxuanmock.getresult API 2.0 溪行 萧玄 吴迪 风胜 萧玄测试日常 录入中 萧玄测试日常 预览API 修改变更 关闭变更 taobao.xiaoxuanmockone.test API 2.0 溪行

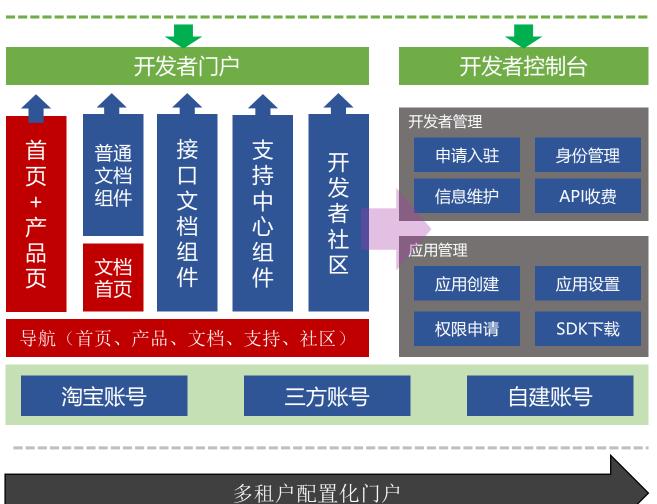


《上一页 1 下一页》 共1页 到

9四部分 开放平台工厂

开放平台工厂 — 多租户与配置化门户(前端)

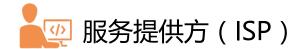


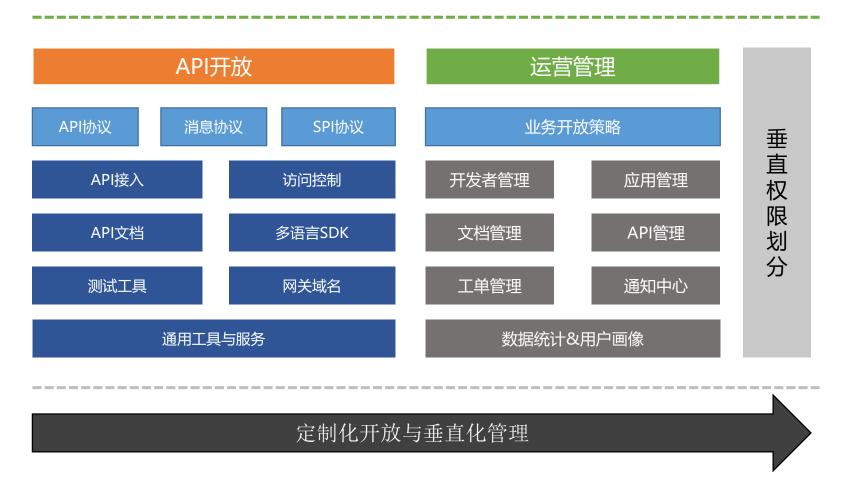






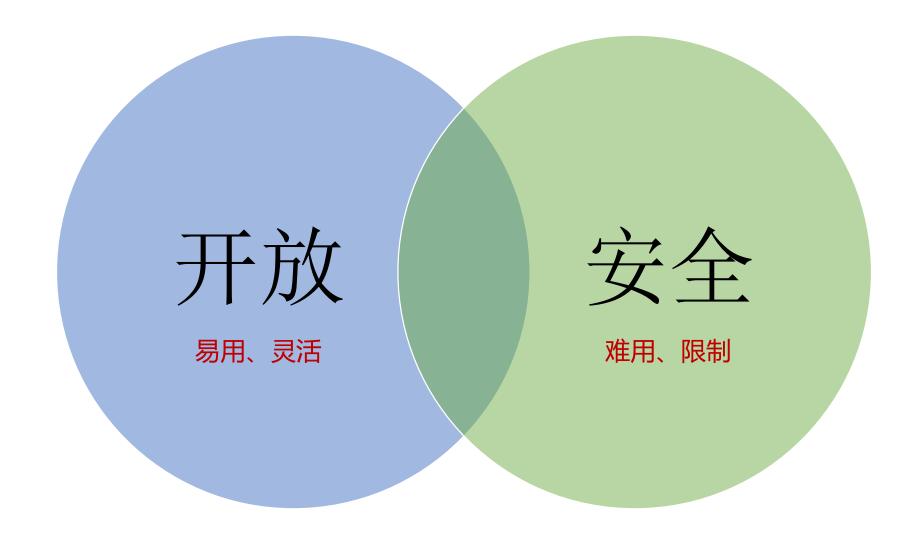
开放平台工厂 — 定制化开放与垂直化管理(后端)





第五部分 开放平台安全

开放与安全



安全控制手段

网关安全

用户身份认证(OAuth2)

API协议安全(SSL、防篡改、防重放)

API权限控制(APP级,用户级)

多维度流控(APP+API+User)

黑白名单控制(应用级、用户级)

日志打点与分析(API级、字段级)

数据安全

对外数据披露审批流程

数据分级(API级,字段级)

数据脱敏(模糊化)

数据混淆 (Open Security ID)

数据加密(API响应, RDS数据)

安全保镖(行为监控,异常报警)

应用安全

ISV入驻规范、安全技术要求

APP创建申请、API权限包申请

应用安全配置(IP绑定、用户绑定)

应用安全扫描(黑盒扫描、白盒扫描)

安全托管环境(聚石塔、干牛、TAE)

人机识别防刷(无线安全保镖)

《尽在双十一》





联系作者:winwindg

Thanks!





诚邀志同道合的朋友加入淘宝开放平台:fengsheng@alibaba-inc.com