长虹集团软件与服务
中心 高级架构师

李伟

演讲主题：《Kubernetes下API网关的微服务实践》

负责长虹各基础服务模块的架构设计与实现，以支撑长虹智能硬件、O2O 电商等业务。

对电商支付系统、大型网站架构均有深入研究和独到见解。

CHANGHONG 长虹

让想象发生

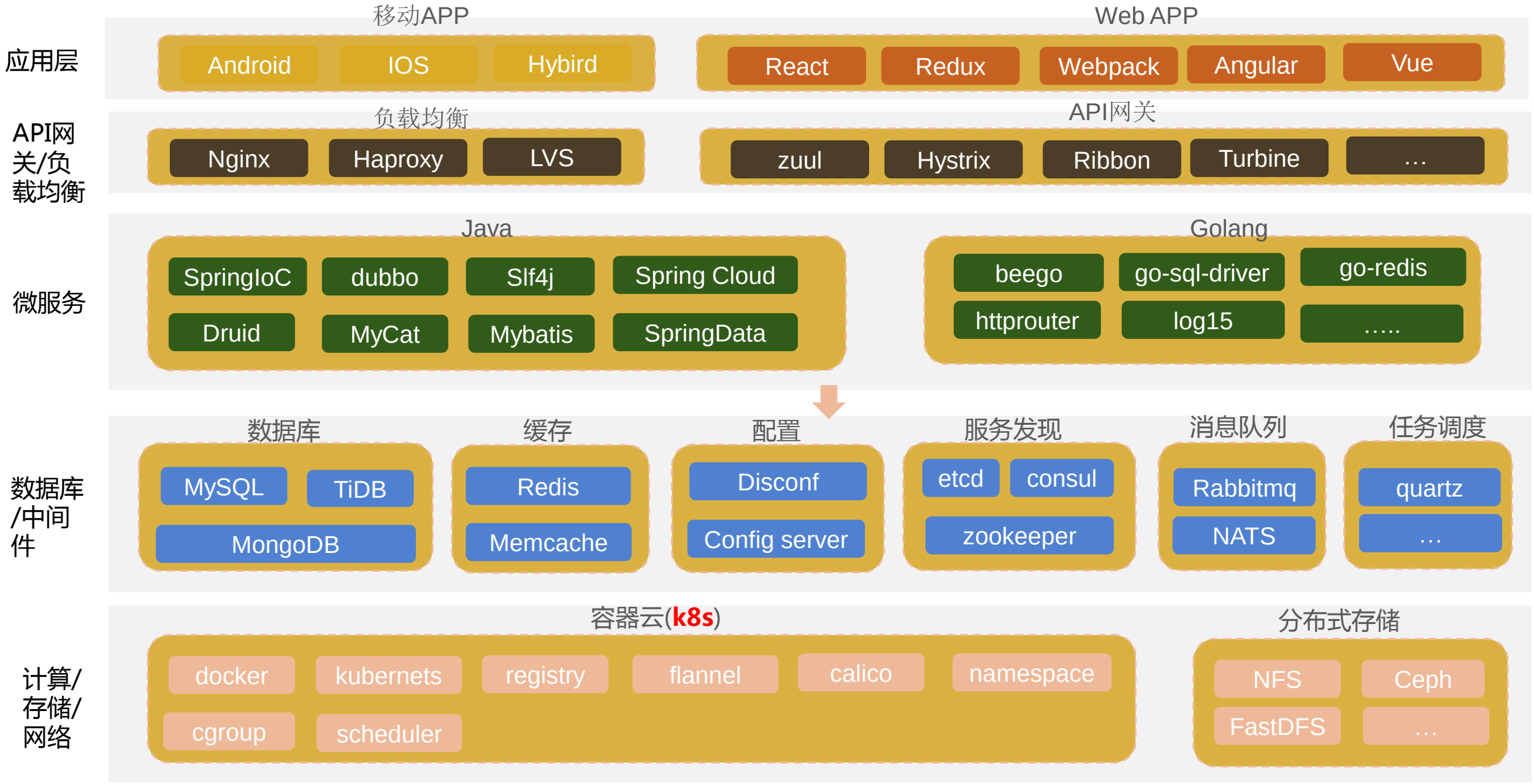
Kubernetes下API网关的微服务实践

软件与服务中心　云服务部　李伟

整体业务架构


应用/客户端
TouchC
云游互联
launcher
超级APP
启客APP
智慧管家
.....
SaaS/能力中心
用户中心
短信中心
订单中心
商品中心
商户中心
报表中心
支付中心
设备中心
消息中心
.....
PaaS
数据库服务
负载均衡
配置文件中心
计划任务调度
搜索服务
日志
缓存服务
消息队列
文件存储
.....
容器云平台（k8s）
调度
容器网络
镜像仓库
服务编排
租户管理
主机管理
主机管理
存储卷
容器管理
服务管理
IaaS/物理资源
主机
存储
网络

技术栈


应用层
移动APP
Android
IOS
Hybird
Web APP
React
Redux
Webpack
Angular
Vue
API网关/负载均衡
负载均衡
Nginx
Haproxy
LVS
API网关
zuul
Hystrix
Ribbon
Turbine
…
微服务
Java
SpringIoC
dubbo
Slf4j
Spring Cloud
Druid
MyCat
Mybatis
SpringData
Golang
beego
go-sql-driver
go-redis
httprouter
log15
…..
数据库/中间件
数据库
MySQL
TiDB
MongoDB
缓存
Redis
Memcache
配置
Disconf
Config server
服务发现
etcd
consul
zookeeper
消息队列
Rabbitmq
NATS
任务调度
quartz
…
计算/存储/网络
容器云(k8s)
docker
kubernets
registry
flannel
calico
namespace
cgroup
scheduler
分布式存储
NFS
Ceph
FastDFS
…

什么是API网关？

API网关跨一个或多个内部API提供单个统一的API入口点。 通常还包括限制访问速率限制和有关安全性等特点。 诸如Tyk.io的API管理层增加了额外的功能，例如分析，计费和生命周期管理。

基于微服务的架构当中往往包含10到100项甚至更多服务。API网关能够为外部消费方提供一套统一的入口点，且不会受到内部微服务的具体数量与组成的影响。

API网关的使用场景

- 面向Partner OpenAPI
- 面向Mobile App
- 面向Web App
- 面向Partner ExternalAPI

哪些公司在使用API网关？

API网关开源解决方案

Kong

OpenResty
Nginx + Lua

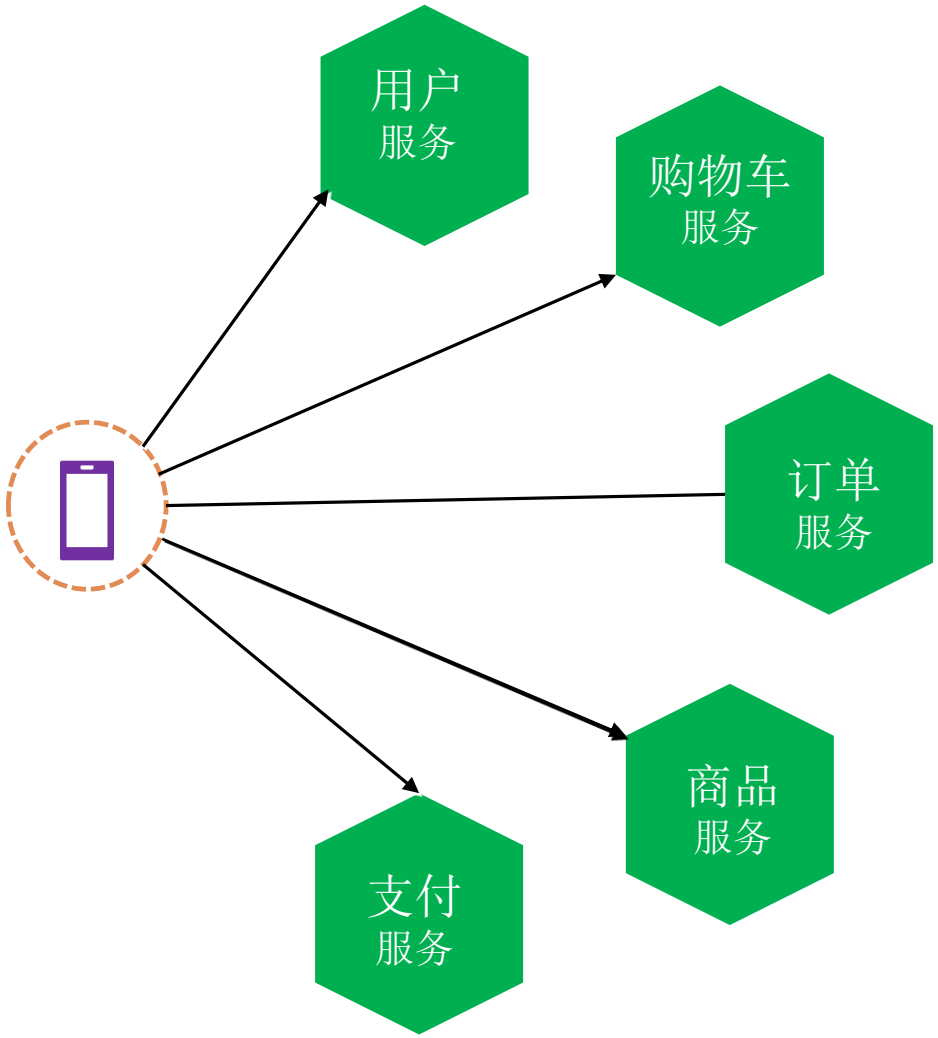
Tyk.io

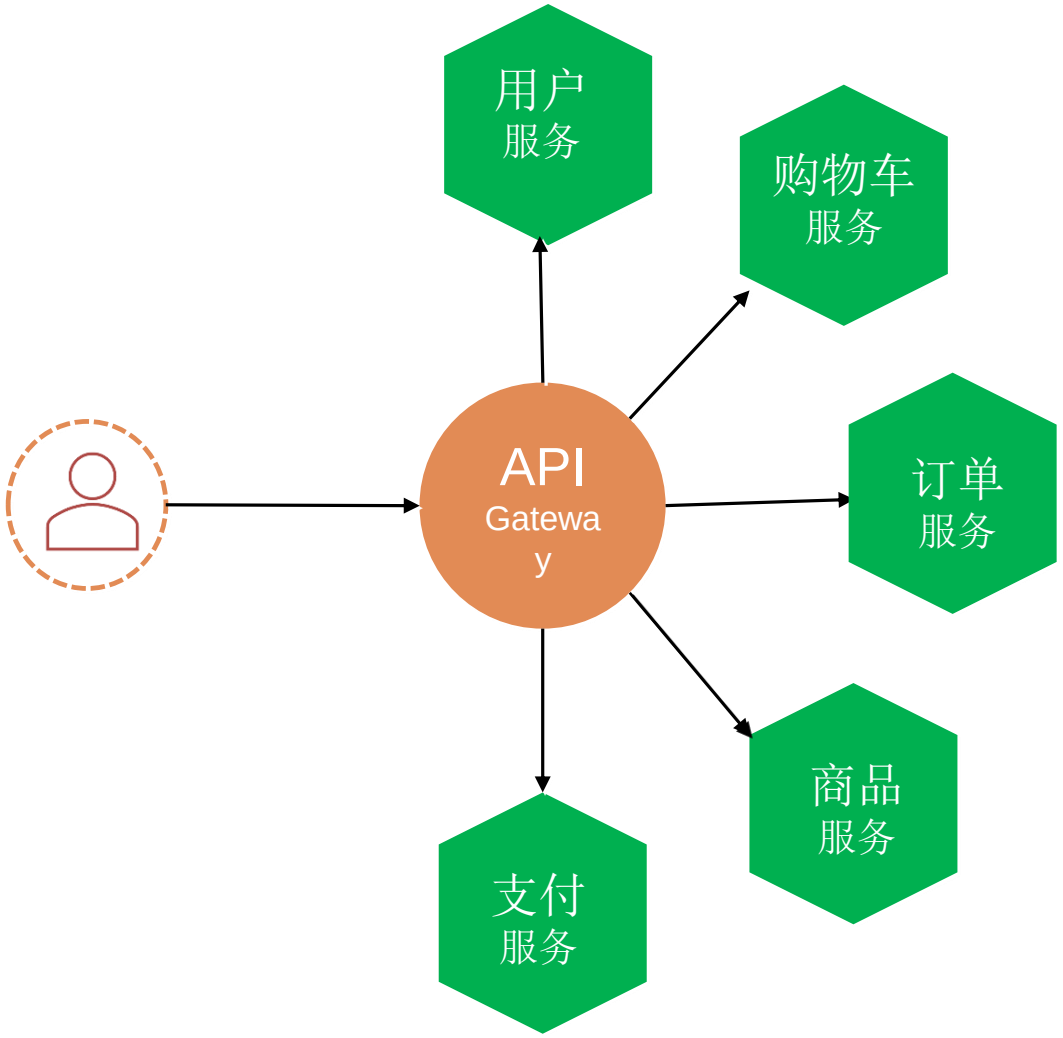
Golang

Zuul

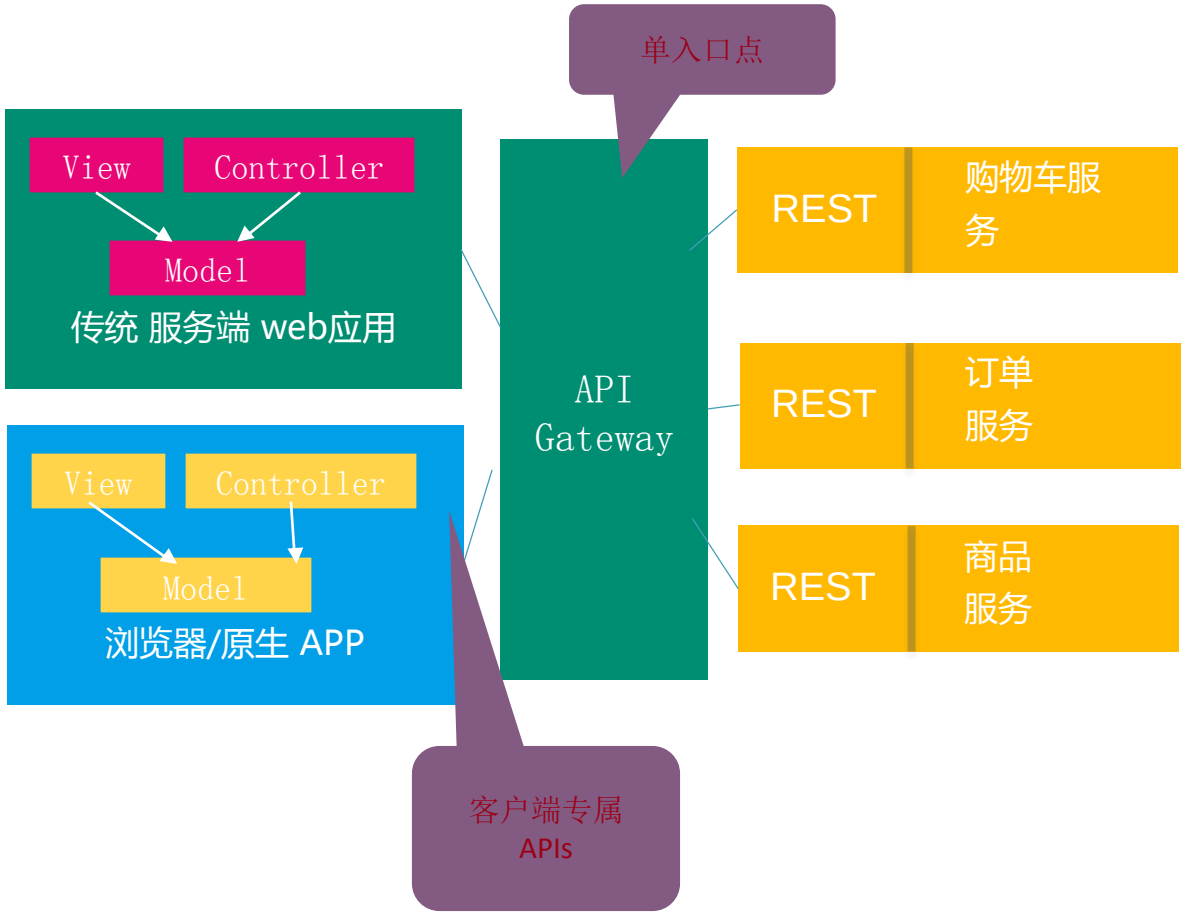
Java
Spring cloud

API网关与微服务


用户
服务
购物车
服务
订单
服务
商品
服务
支付
服务

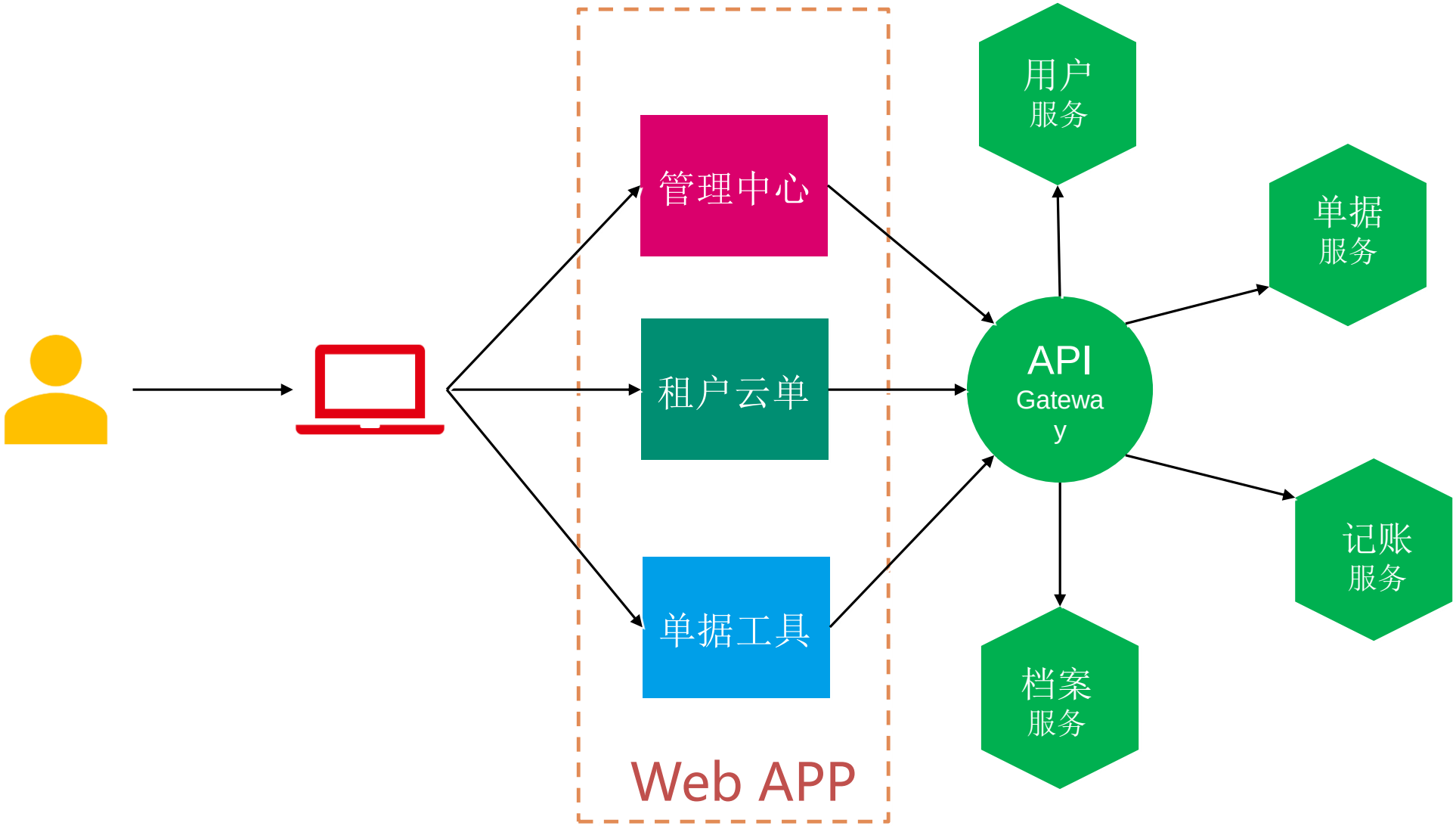

用户
服务
购物车
服务
API
Gatewa
y
订单
服务
商品
服务
支付
服务

API网关简介

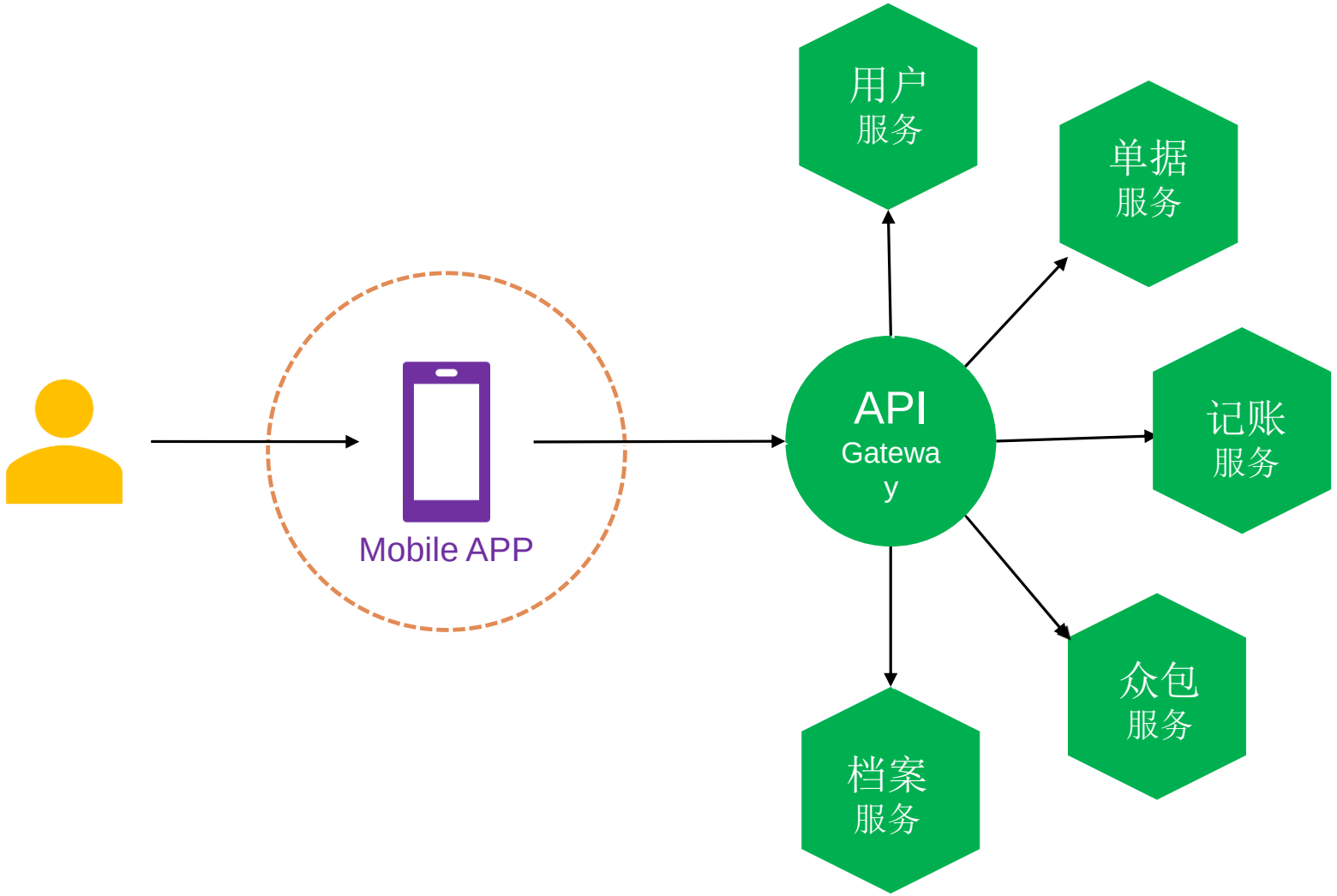


- API网关封装了系统内部架构，为每个客户端提供一个定制的API。它可能还具有其它职责，如身份验证、监控、负载均衡、缓存、“请求整形（request shaping）”与管理、静态响应处理。
- 如身份验证：支持Basic、Key、hmac、Oauth2.0等认证方式。
- 负载均衡：服务发现与负载均衡。
- 监控。
- 数据分析。

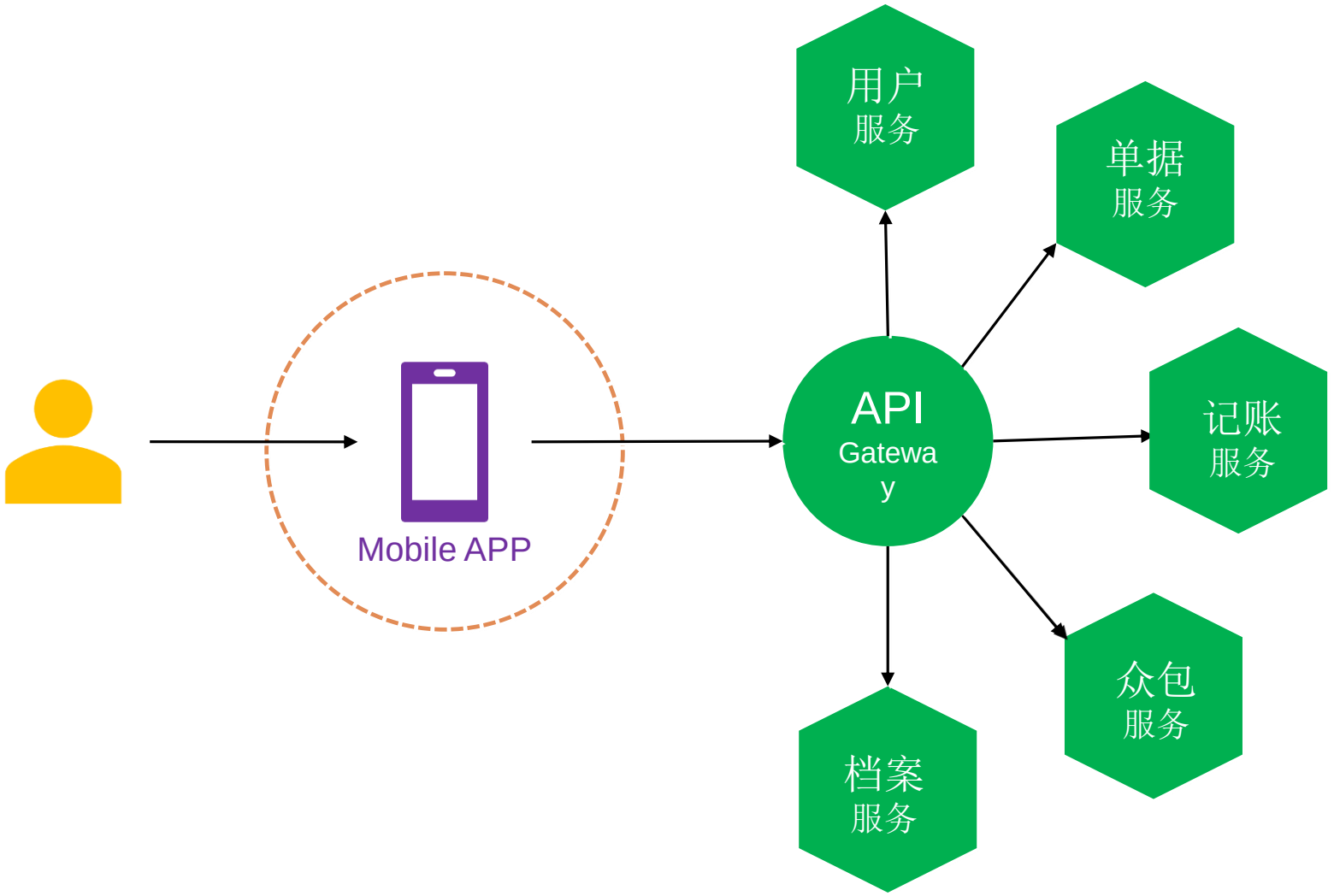
公司某金融业务API网关职能

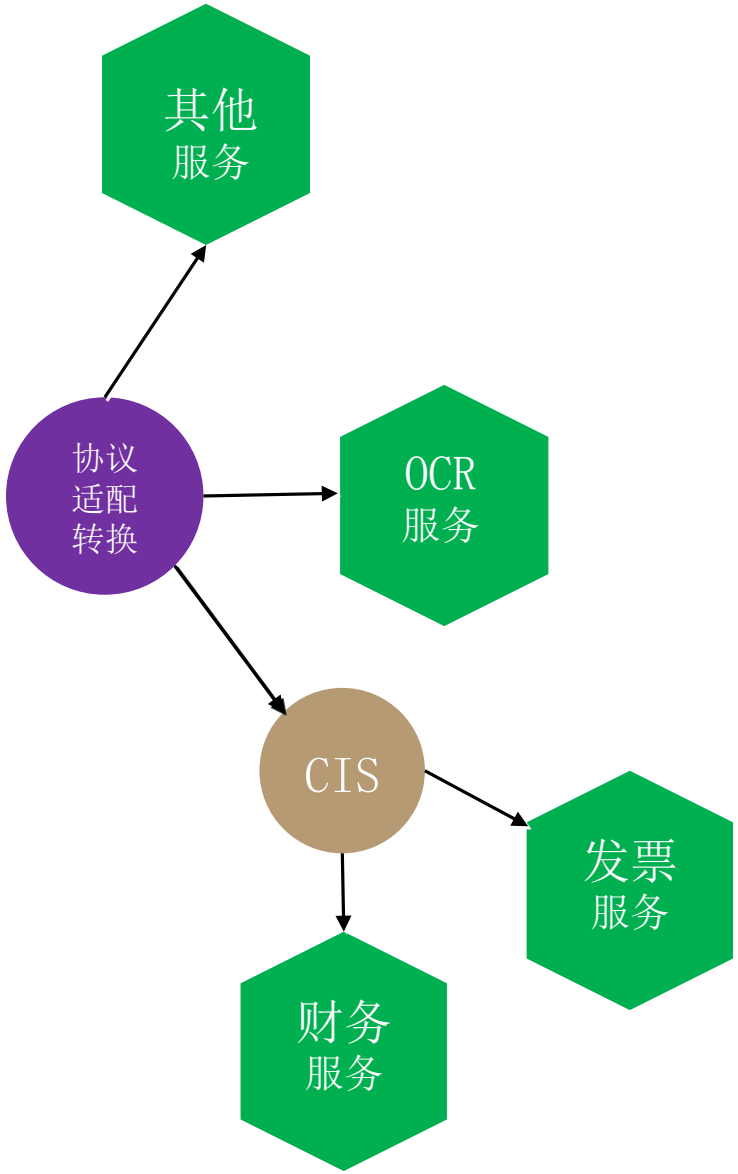


公司某金融业务API网关职能



公司某金融业务API网关职能





API网关的优缺点

优点

- 统一入口便于统一分析
- 后端服务更容易重构
- 通过编排可简化客户端
- 统一鉴权加强安全简化后端服务实现

缺点

- 增加开发、部署、维护工作量
- API网关可能因为设计不当或者缺陷成为瓶颈（开发、运行期）

API网关技术选型

- 基于Netflix Zuul
- 服务发现 Consul
- 负载均衡robbin
- 断路器hystrix
- 前置流量控制nginx + Lua + consul 服务自动发现

API网关核心功能

API GW本身

- NIO接入，异步接出
- 流控与屏蔽
- 秘钥交换
- 客户端认证与报文加解密
- 业务路由框架
- 报文转换
- HTTP DNS/ Direct IP

API GW 客户端 SDK / Library

- 基本通信
- 秘钥交换与Cache
- 身份认证与报文加解密

配套的在线自助服务平台

- 代码生成
- 文档生成
- 沙盒调测

Stargate总体业务架构

业务 APP | 业务 WEB | 业务 SERVICE | 合作伙伴系统

API 网关

统一用户门户（API 使用者）

- 项目/应用
- API 调试
- 申请服务授权
- 联系人管理
- 查看 API 文档

平台运营控制台（平台运营者 、 API 提供者）

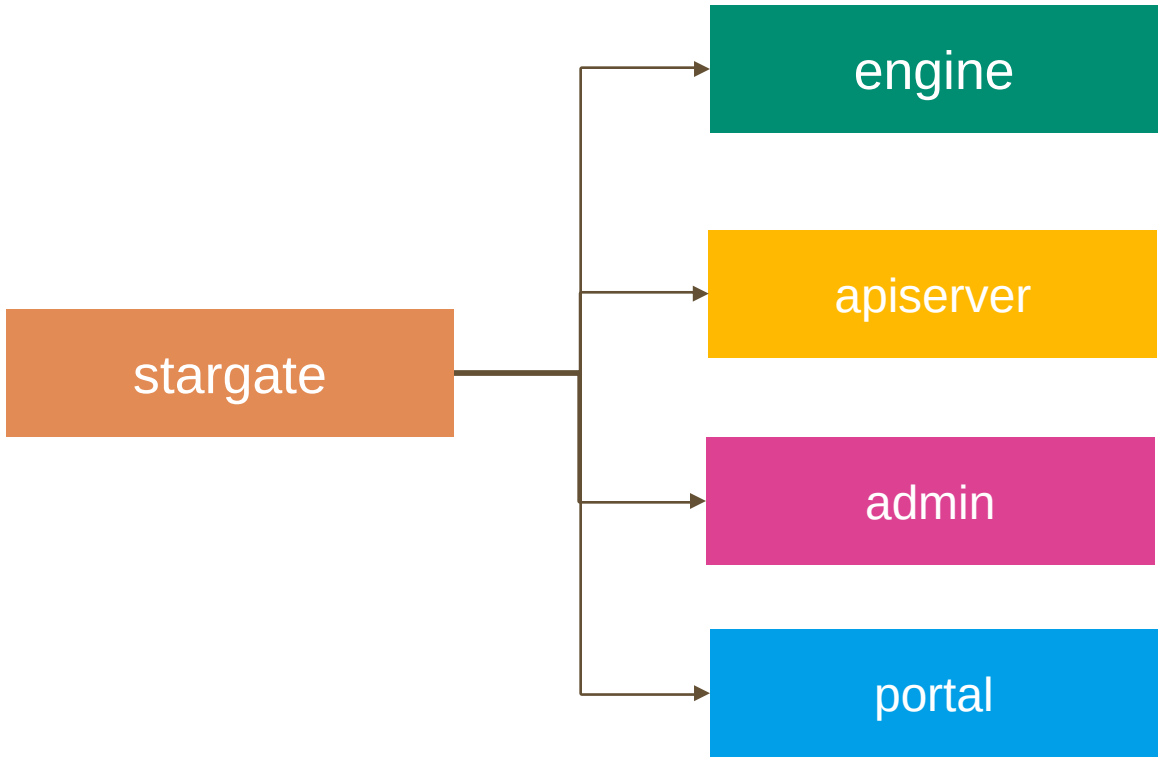
- 能力 API 路径映射
- API 调试
- 服务接入
- 服务授权管理
- 监控（请求、响应、流量）
- 流量控制策略
- …
- 系统管理
- 能力服务管理
- 用户管理
- 项目/应用管理
- 联系人管理
- 服务文档管理
- 公告管理
- 操作日志/缓存
- …

- 认证鉴权
- 访问控制
- 传输加密
- 流量控制
- 数据统计
- …
- 服务状态监控
- 平台管理 API

能力中心

- 通行证
- 设备中心
- 商品中心
- 订单中心
- 短信中心
- 售后提单
- 更多能力
- …

Stargate组件



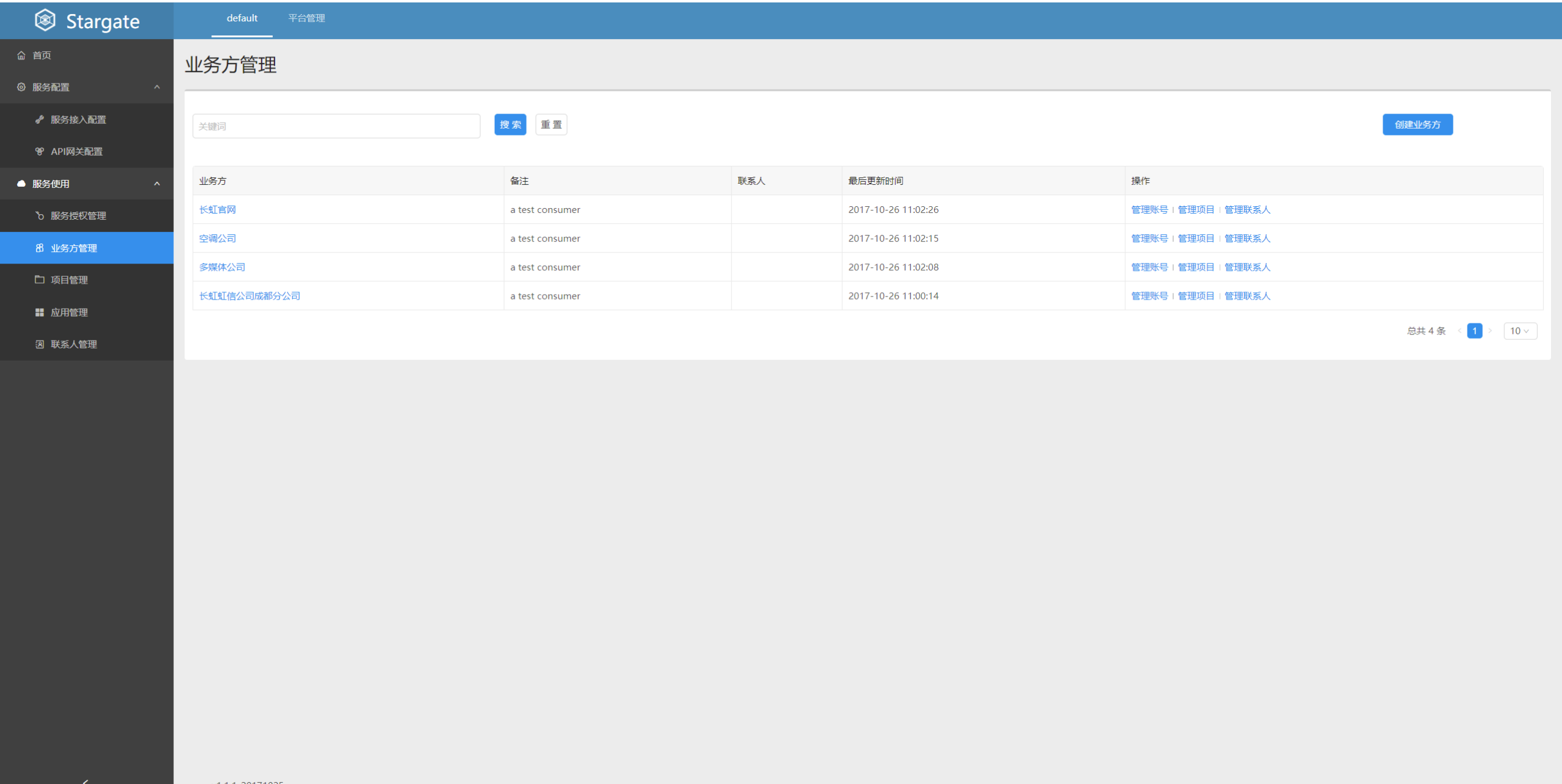
认证鉴权、路由、负载均衡、请求整形、接口编排

消费者、项目、应用等管理API

面向配置、运营人员的管理dashboard

面向消费者的API store 门户　接入文档 SDK下载 服务申请 项目、应用管理 在线接口调试

API网关运营管理后台

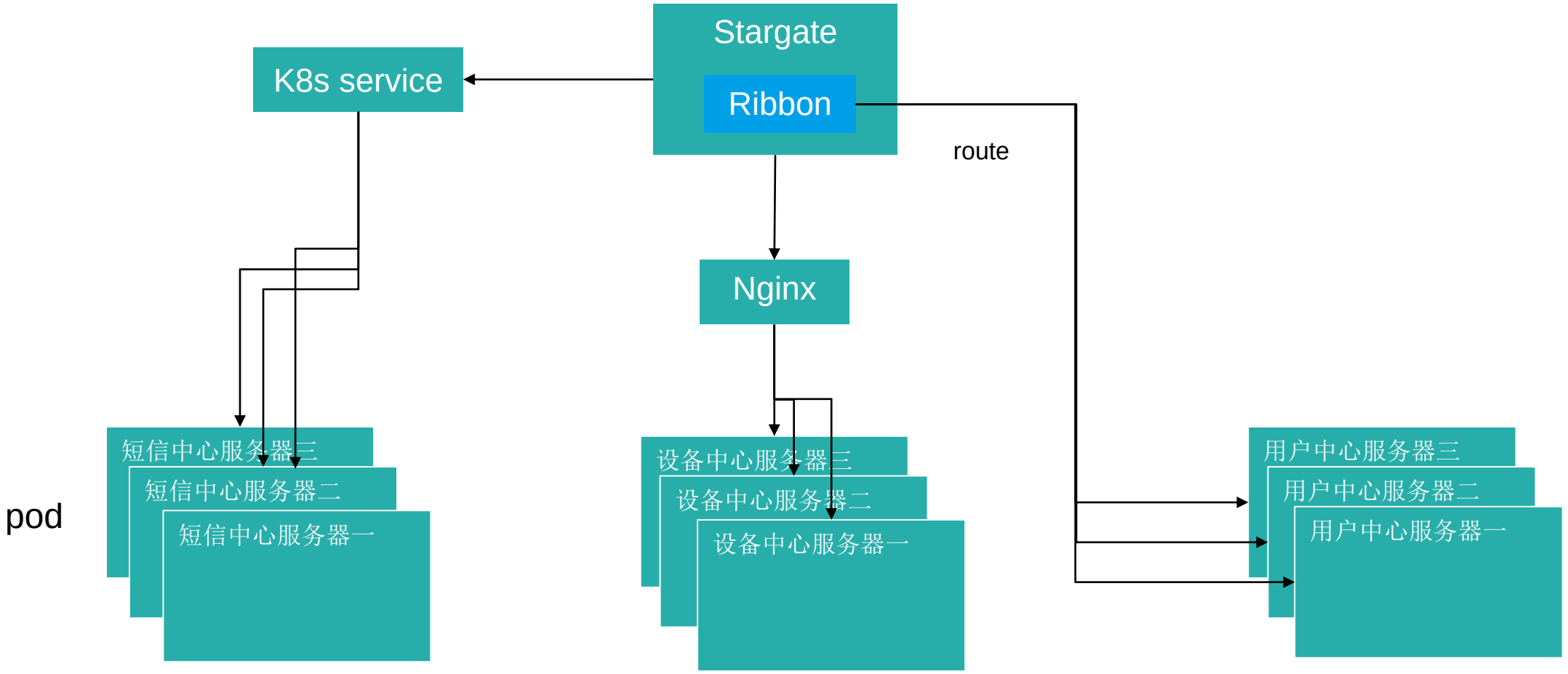


API负载均衡

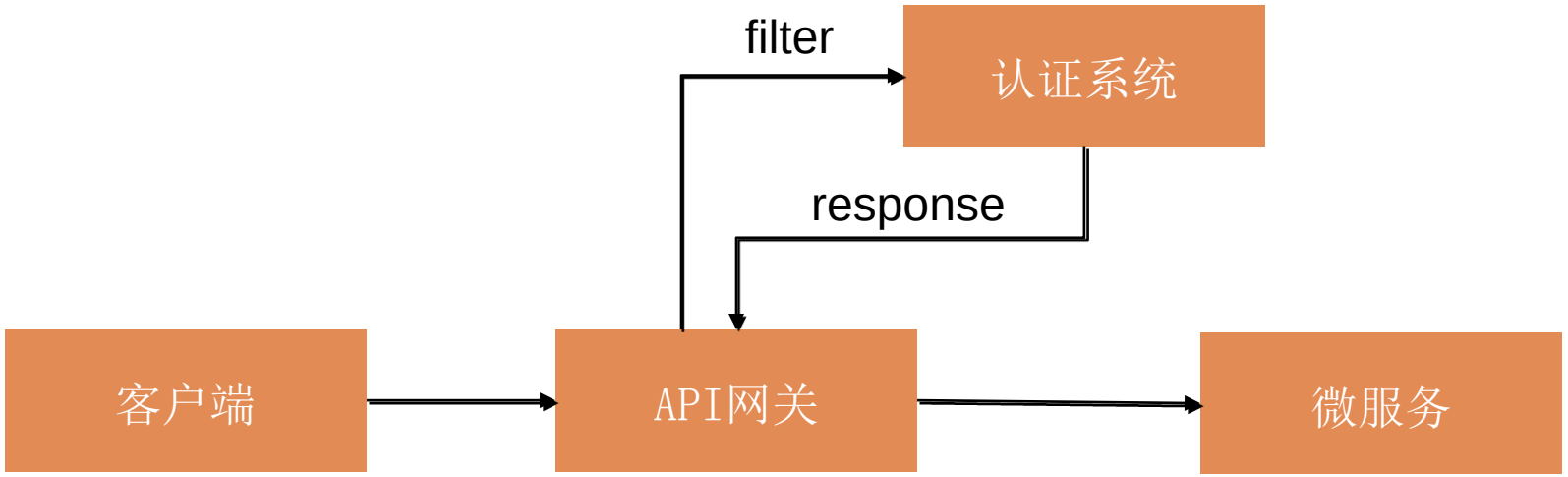
服务发现针对后端服务种类不同

- Kubernets service
- Nginx 代理过后的服务
- 提供微服务ip list 网关轮询

API负载均衡


Stargate
Ribbon
K8s service
route
Nginx
pod
短信中心服务器三
短信中心服务器二
短信中心服务器一
设备中心服务器三
设备中心服务器二
设备中心服务器一
用户中心服务器三
用户中心服务器二
用户中心服务器一

API OAuth2认证授权



API hmac认证示例

对请求body进行验签

```
$ curl -i -X POST http://api.changhong.com/books \
    -H "Host: api.changhong.com" \
    -H "Date: Thu, 22 Jun 2017 21:12:36 GMT" \
    -H "Digest: SHA-256=SBH7QEtqnYUpEcIhDbmStNd1MxtHg2+feBfWc1105MA=" \
    -H 'Authorization: hmac accesskey="alice123", algorithm="hmac-sha256", headers="date request-line digest", signature="gaweQbATuaGmLrUr3HE0Dzl
    -d "A small body"
HTTP/1.1 200 OK
...
```

上面请求使用SHA-256算法计算body摘要并添加Digest头信息，格式如下：

```
body="A small body"
digest=SHA-256(body)
base64_digest=base64(digest)
Digest: SHA-256=<base64_digest>
```

时钟偏移

支持时钟偏移检查，以防止重放攻击（replay attacks),配置允许过去/将来的偏移量（一般为>300s)，任何具有较高或者较低的时间值的请求将被拒绝。

支持开关开启/关闭 该功能（绑定服务）

说明：服务器与客户端应与NTP服务器同步，并且使用X-Date或者Date标头发送有效时间（GMT格式）

API网关防重放攻击

X-Stargate-Timestamp

X-Stargate-Nonce

- 时间误差15min
- 随机数保存时间15min内

Stargate数据库、缓存选型

短期:MySQL

- 易于操作
- 结合Redis缓存保证性能
- Caffeine 内存缓存

长期：Cassandra

- 海量数据存储
- 易于管理、水平扩展
- 安全

Thank you.