腾讯课堂 学习成就梦想 + 动脑学院 DONGNAO COLLEGE

《C/C++Linux服务器架构师课程》

做一家受人尊敬的企业，做一位受人尊敬的老师

动脑学院
DONGNAOEDU

发展历程

IT类目唯一最重量级“卓越贡献奖”连续两年“腾讯认证机构奖”

最早的学习平台

腾讯课堂第一家

中高端IT职业教育

最多学员的平台

腾讯课堂NO.1

最大影响力平台

唯一两次获得

“年度卓越贡献奖”

动脑学院
DONGNAOEDU

安全开放性云平台架构设计

今晚八点·腾讯课堂

主讲老师 **Lee**

动脑合伙人

曾供职于华为和诺基亚通信

担任过两年上市公司产品总监

主要内容

1.什么是openapi

2.open api的设计

3.openresty + lua实战

4. API网关和动态路由

扫码加老师微信

解决学习问题

自我介绍

Lee　李哥

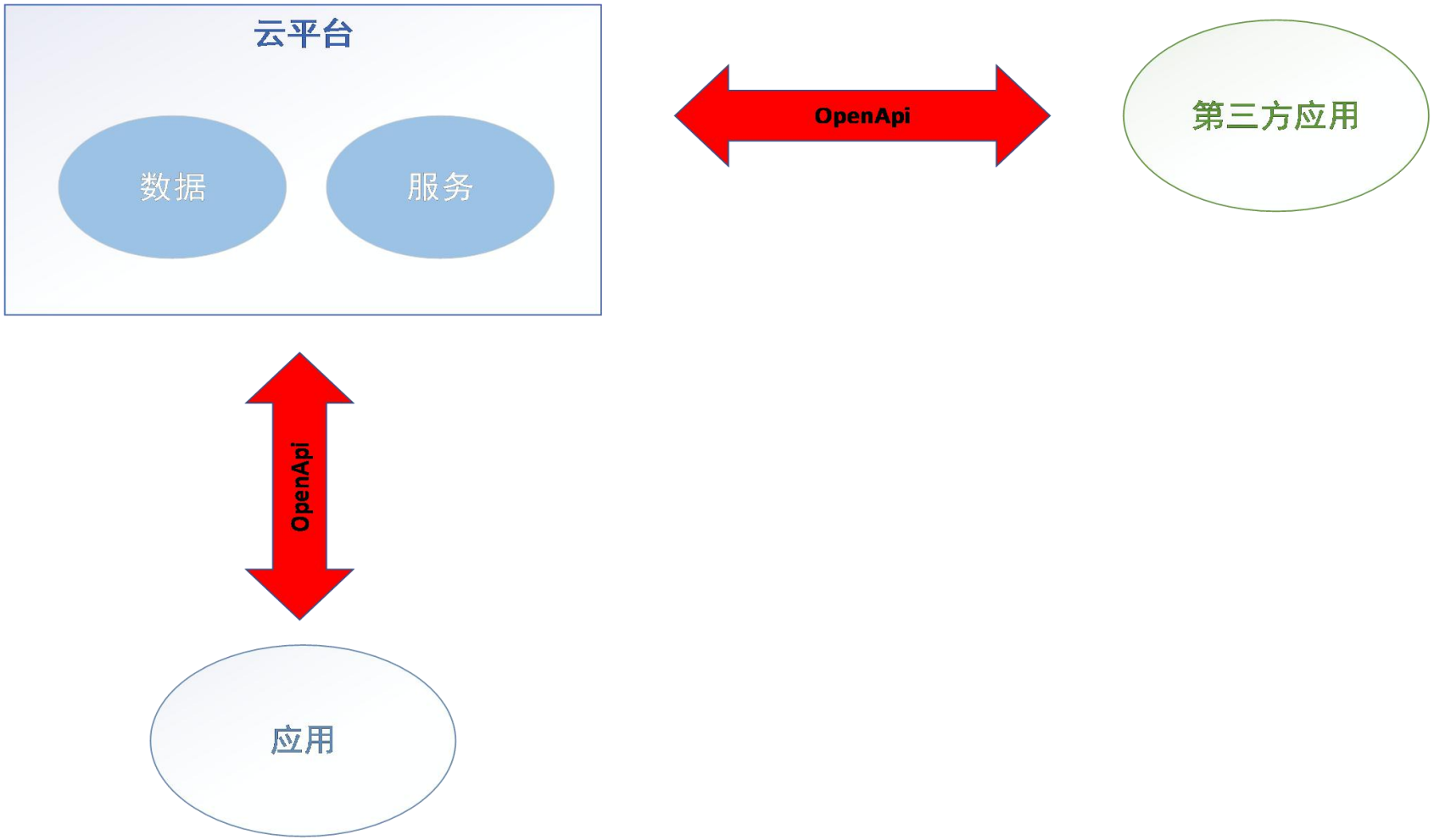
华为技术有限公司	3 years
项目经理	
诺基亚通信系统技术	4 years
技术经理	
comtom	2 years
产品总监	

10年（C/C++）开发经验和产品管理经验，研究过多款C/C++优秀开源软件的框架；

主持开发过大型音频广播云平台，

精通需求分析、架构分析和产品管理，精通敏捷开发流程和项目管理。

OpenAPI是什么？

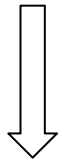


OpenAPI接口长啥样

https://graph.qq.com/user/get_simple_userinfo?**access_token**=1234ABD1234ABD&**oauth_consume**

r_key=12345& **openid**=B08D412EEC4000FFC37CAABBDC1234CC&**format**=json

当然我们可以在http的消息体里携带json数据



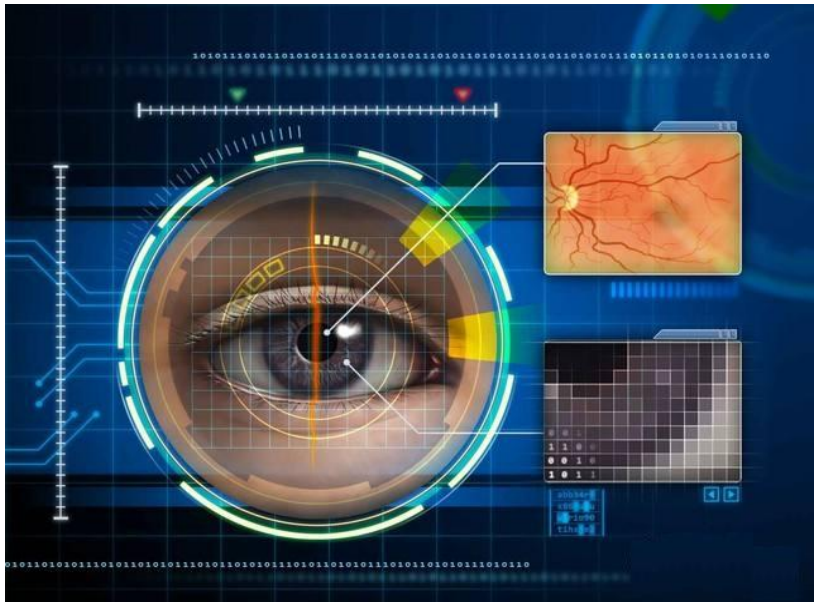
调用成功后返回


```
{
"ret":0,
"msg":"",
"nickname":"Peter",
"figureurl":"http://qzapp.qlogo.cn/qzapp/111111/942FEA70050EEAFBD4DCE2C1FC775E56/30",
"figureurl_1":"http://qzapp.qlogo.cn/qzapp/111111/942FEA70050EEAFBD4DCE2C1FC775E56/50",
"figureurl_2":"http://qzapp.qlogo.cn/qzapp/111111/942FEA70050EEAFBD4DCE2C1FC775E56/100",
"figureurl_qq_1":"http://q.qlogo.cn/qqapp/100312990/DE1931D5330620DBD07FB4A5422917B6/41",
"figureurl_qq_2":"http://q.qlogo.cn/qqapp/100312990/DE1931D5330620DBD07FB4A5422917B6/100",
"is_yellow_vip"：  "1",
"is_yellow_year_vip":"0",
"yellow_vip_level":"6"
}
```

用户账户安全性

12月25日上午10：59，乌云网发布漏洞报告称，大量12306用户数据在网络上疯狂传播。本次泄露事件被泄露的数据达131653 条，包括用户账号、明文密码、身份证和邮箱等多种信息，共约14M数据。这不是12306网站第一次发生用户信息泄露事件了，但是最大的一次。

身份安全性验证



在HTTP协议之上处理授权有很多方法，如HTTP BASIC Auth，OAuth，HMAC Auth等，其核心思想都是验证某个请求是由一个合法的请求者发起。

Basic Auth

这种就是每次在传输的http协议里带上用户名和密码，这种方式就是开发起来很简单，但是缺点也很明显，当然我们也可以进行加密，比如使用Base64加密，但是每次都携带了重要数据，违背了最小暴露原则，隐患也是很巨大的。

HMAC Auth

每个客户端第一次发出请求时，将自己的唯一HASH MAC 和请求包发给服务器，以后，服务器就依据这个HMAC来判断客户端的唯一性。

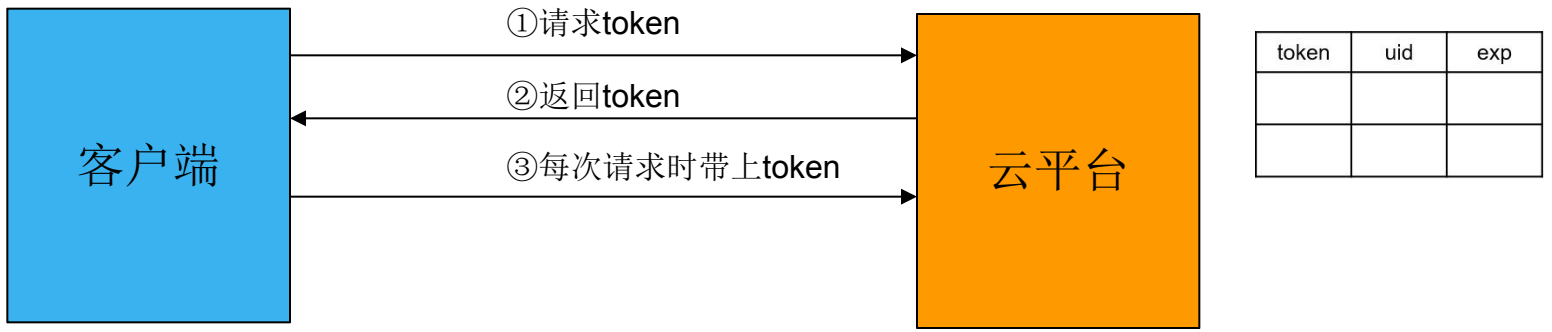
OAuth

OAuth（Open Authorization，开放授权）是为用户资源的授权定义了一个安全、开放及简单的标准，第三方无需知道用户的账号及密码，就可获取到用户的授权信息，并且这是安全的。我们所说的OAuth都是只OAuth2.0。

必须要解释下Oauth

引入token验证身份

- 利用token（授权令牌）机制进行身份验证



- 客户端把加密后的用户名和密码发送给云平台；

  云平台验证用户名和密码，验证通过后，生成一个token，同时保存uid、token、exp保存到redis；

  云平台同时把token传回给客户端；

- 客户端每次访问服务器时都需要带上这个token；

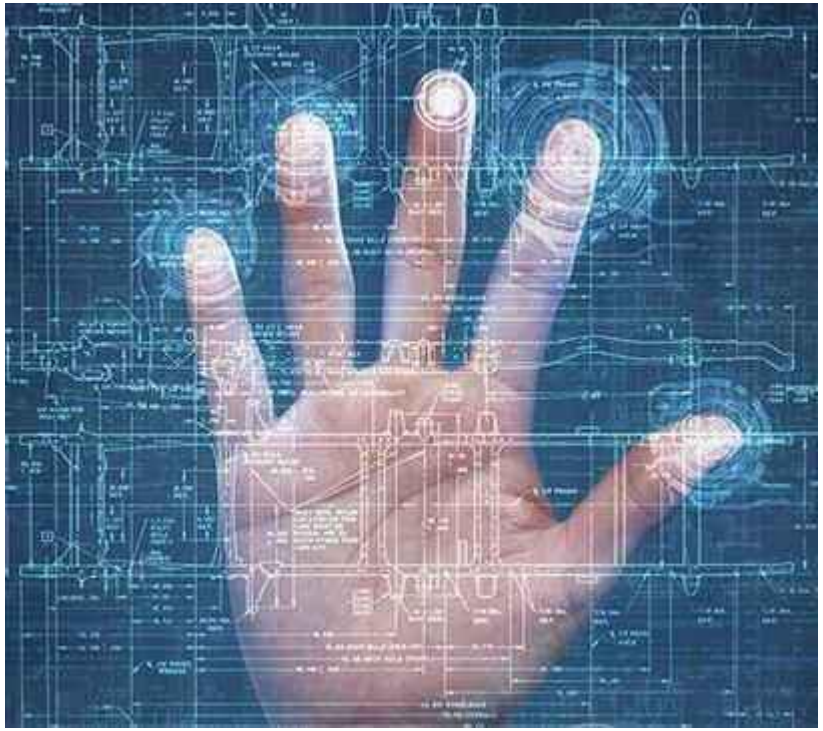
  服务器通过该token验证是哪个用户提交的请求，而不需要在http中携带用户名和密码信息；

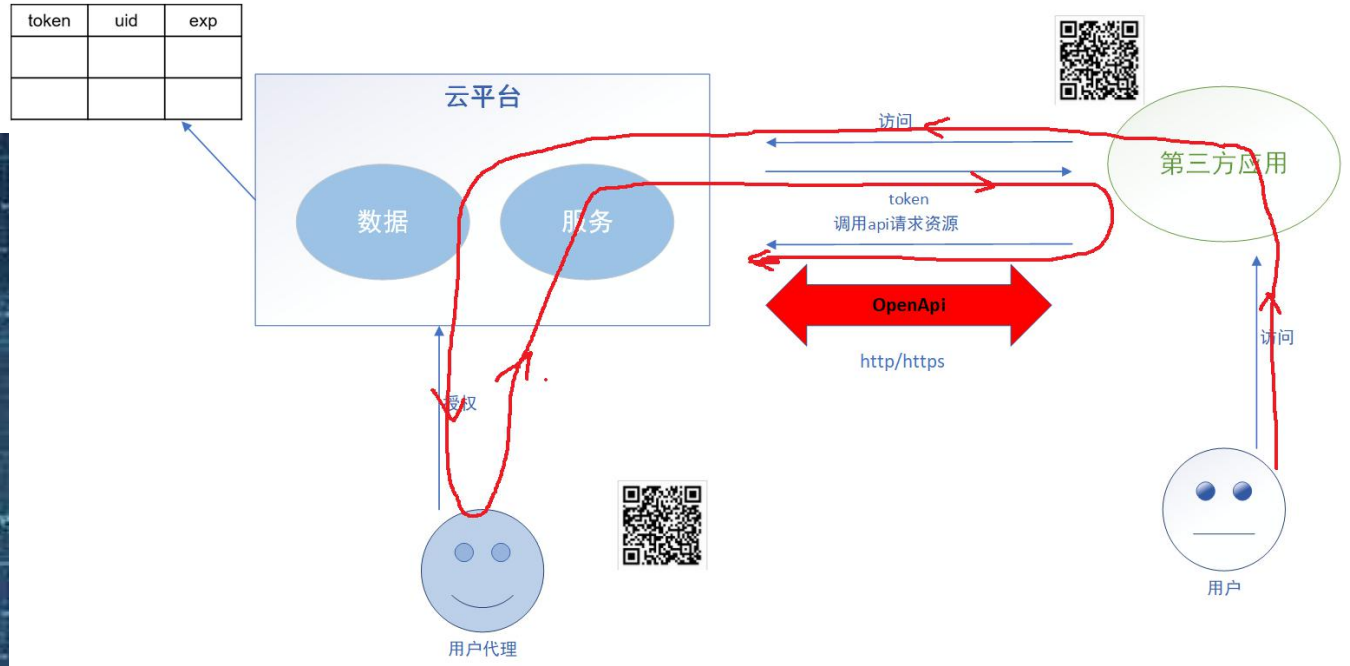
单点登录怎么做的？

oppo

huawei

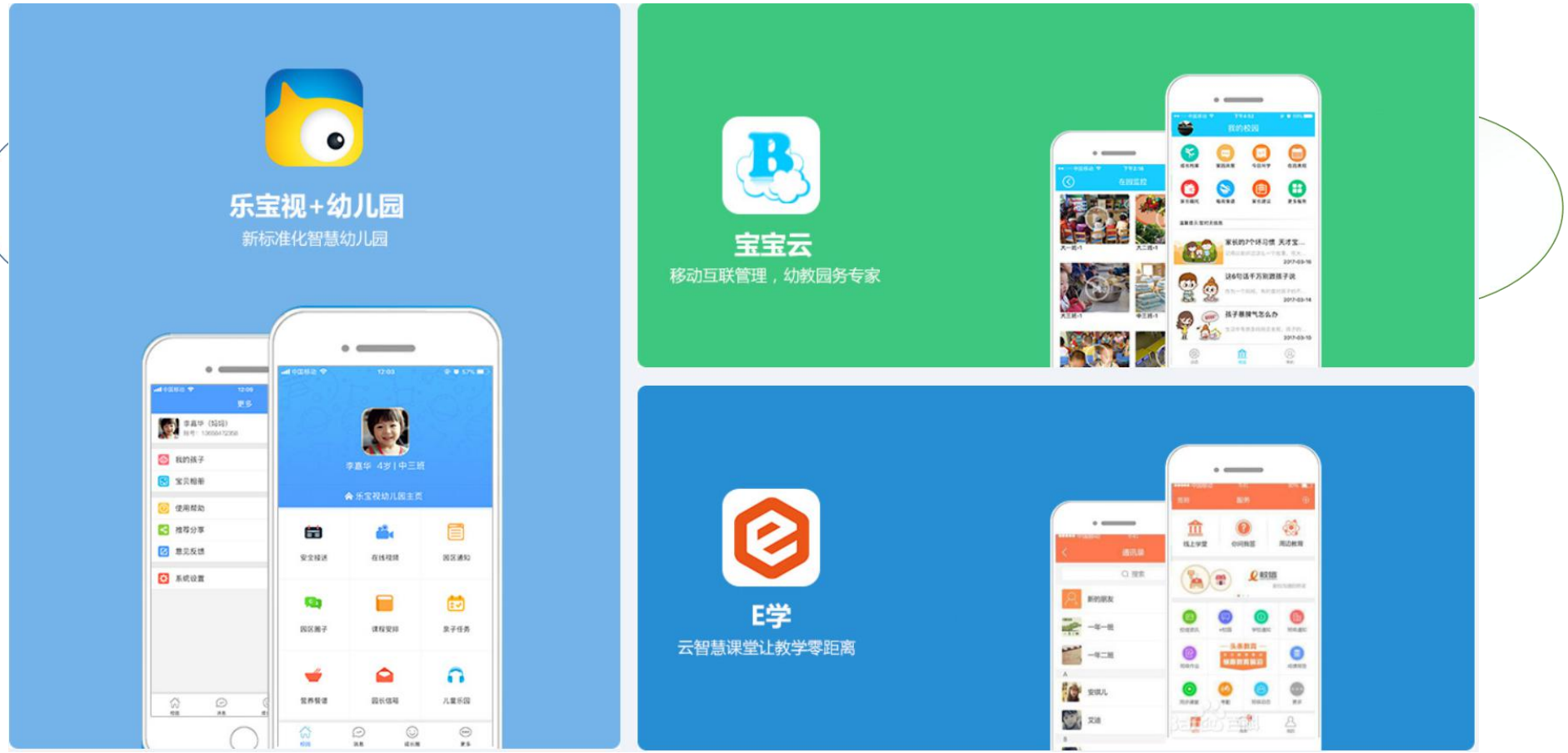
第三方应用如何验证身份





1. 客户端要求用户给予授权
2. 用户同意给予授权
3. 根据上一步获得的授权，向认证服务器请求令牌（token）
4. 认证服务器对授权进行认证，确认无误后发放令牌
5. 客户端使用令牌向资源服务器请求资源
6. 资源服务器使用令牌向认证服务器确认令牌的正确性，确认无误后提供资源

如何保障数据的隔离性



如何防止黑客修改http消息的数据

如何保证API调用的唯一性和重放攻击

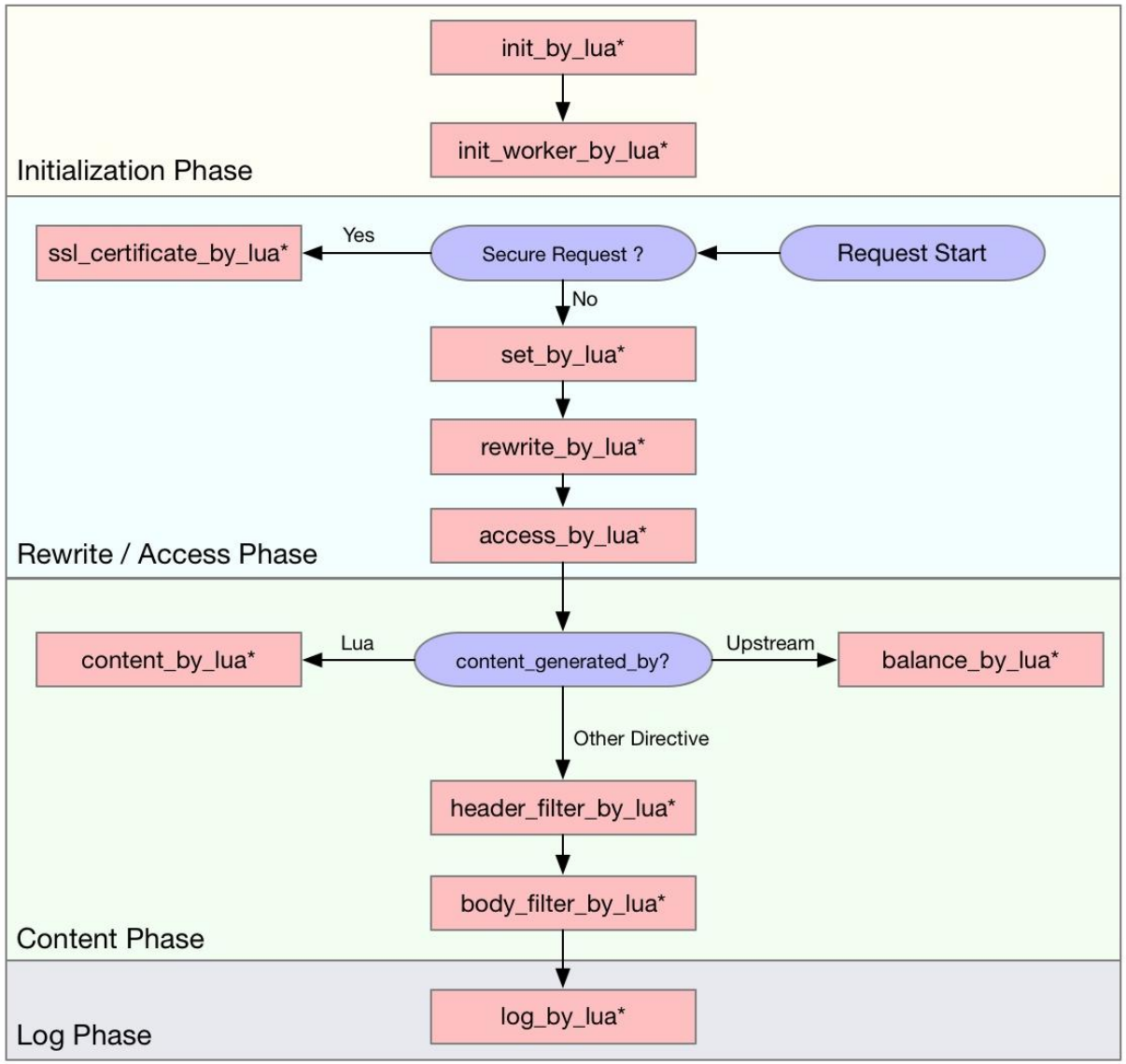
如何设计API接口的安全性

1. 把所有参数按照字母升序排列；
2. 表明第三方调用者身份的appkey；
3. 调用接口时，获取调用时的系统时间信息，并填写在http请求里；
4. 向服务器请求一个公钥（secret），依据该公钥对对http参数、appkey、token、timestamp进行加密，生成签名（sign），且把该sign值填写在http请求里，如下：

http://api.XXX.com/getproduct?id=value1&appkey=XXX&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9&timestamp=12445323134&sign=78093C377FDE63280F990CA9D8FAF0C2ED6ACAEA

5. 服务器处理该请求时，首先校验第三方调用者身份；
6. 然后验证用户合法性；
7. 验证调用次数限制；
8. 通过appkey找到公钥，用该公钥对http请求加密，生成签名，与http请求里的签名进行比对，一直则请求合法。

openresty

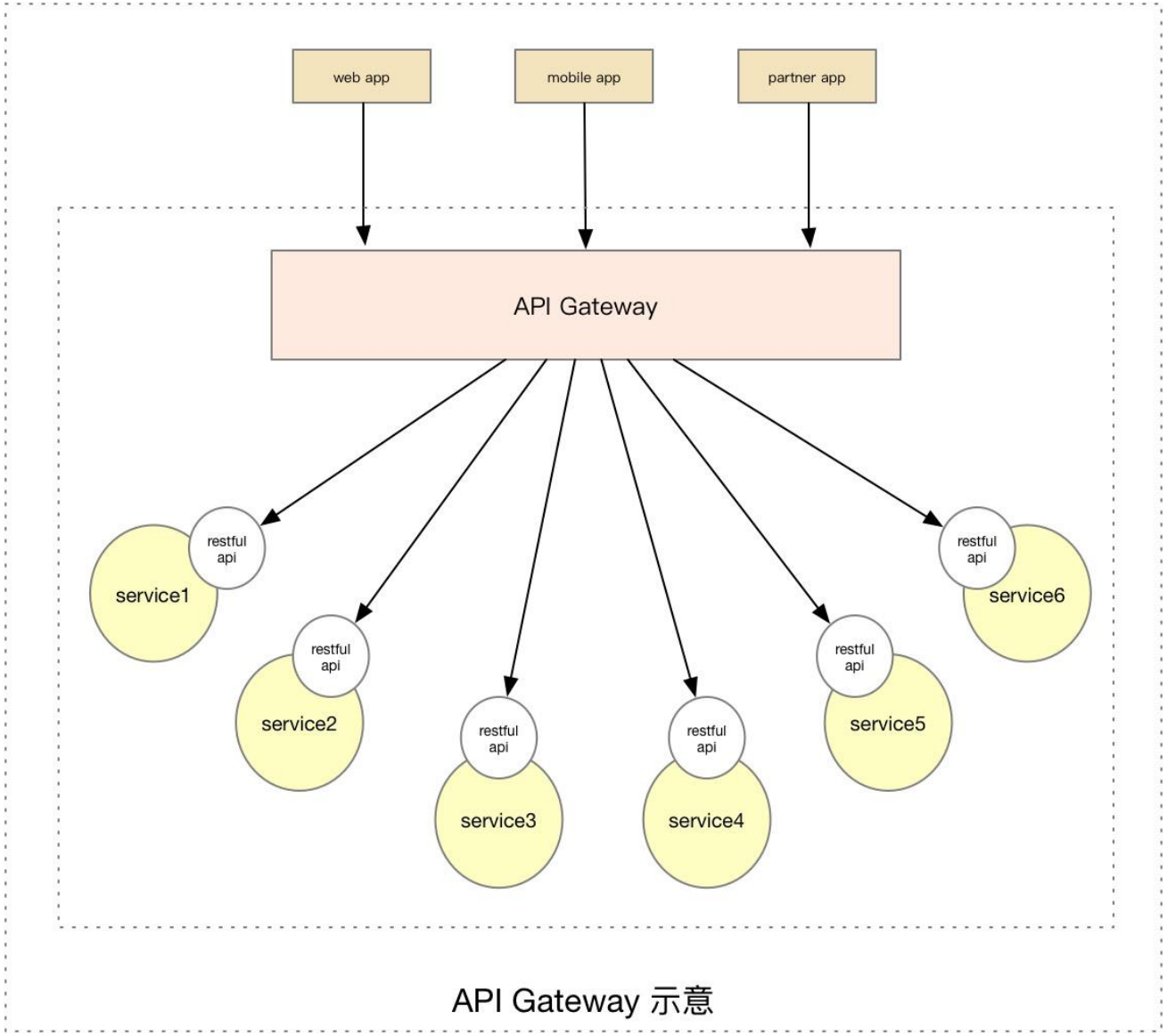


Order of Lua Nginx Module Directive

openresty官网：https://openresty.org/cn/

openresty源码：https://github.com/openresty

什么是APIGateway



API Gateway 示意

如何动态路由？

如何更新upstream呢？

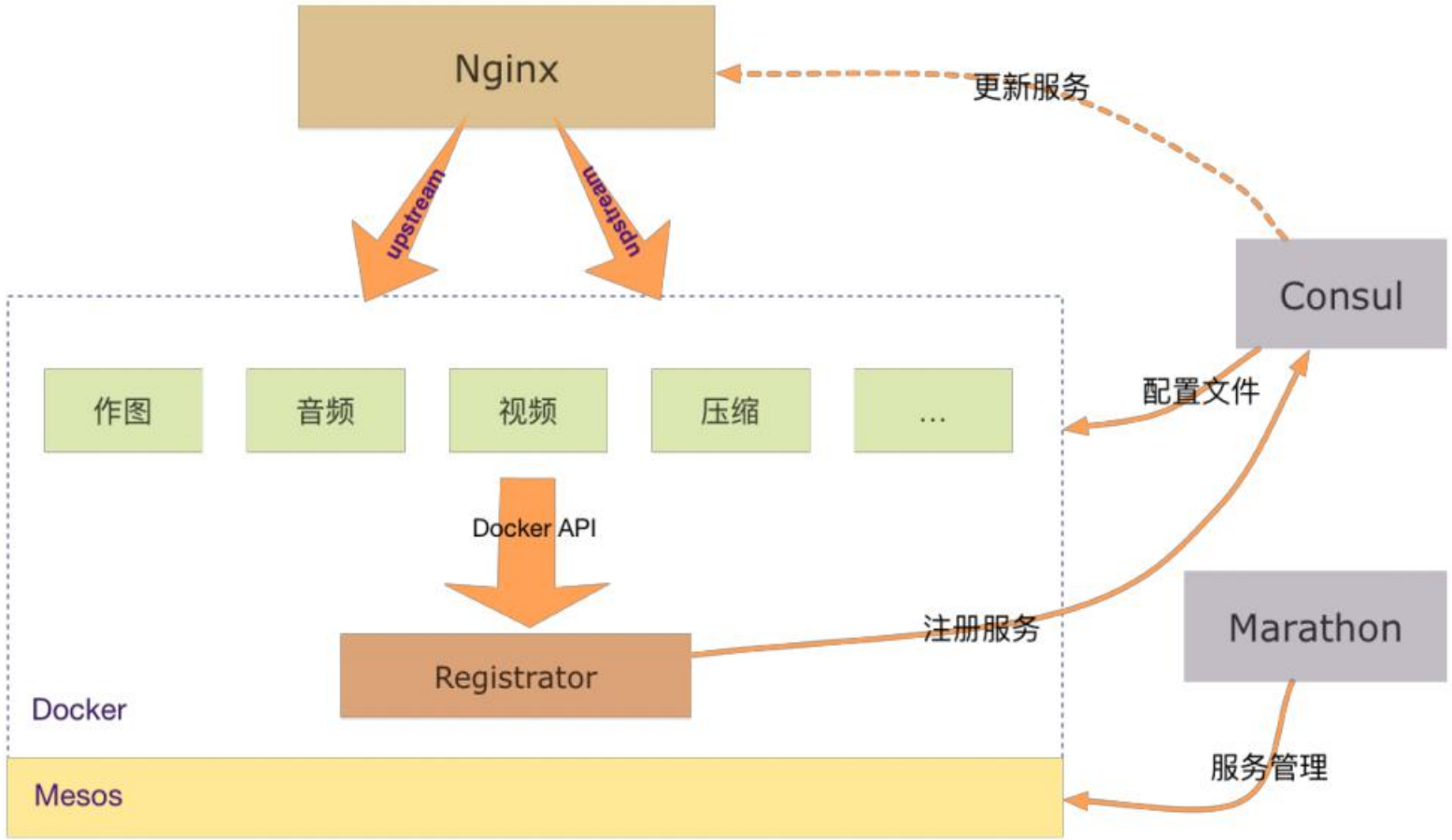
```
http {
    upstream test {
        # fake server otherwise ngx_http_upstream will report error when startup
        server 127.0.0.1:11111;
    }
    upstream bar {
        server 127.0.0.1:8090 weight=1 fail_timeout=10 max_fails=3;
    }

     server {
        listen 8080;
        location = /proxy_test {
            proxy_pass http://test;
        }
        location = /bar {
            proxy_pass http://bar;
        }
        location = /upstream_show {
            upstream_show;
        }
    }
}
```

如何动态更新**upstream**呢？

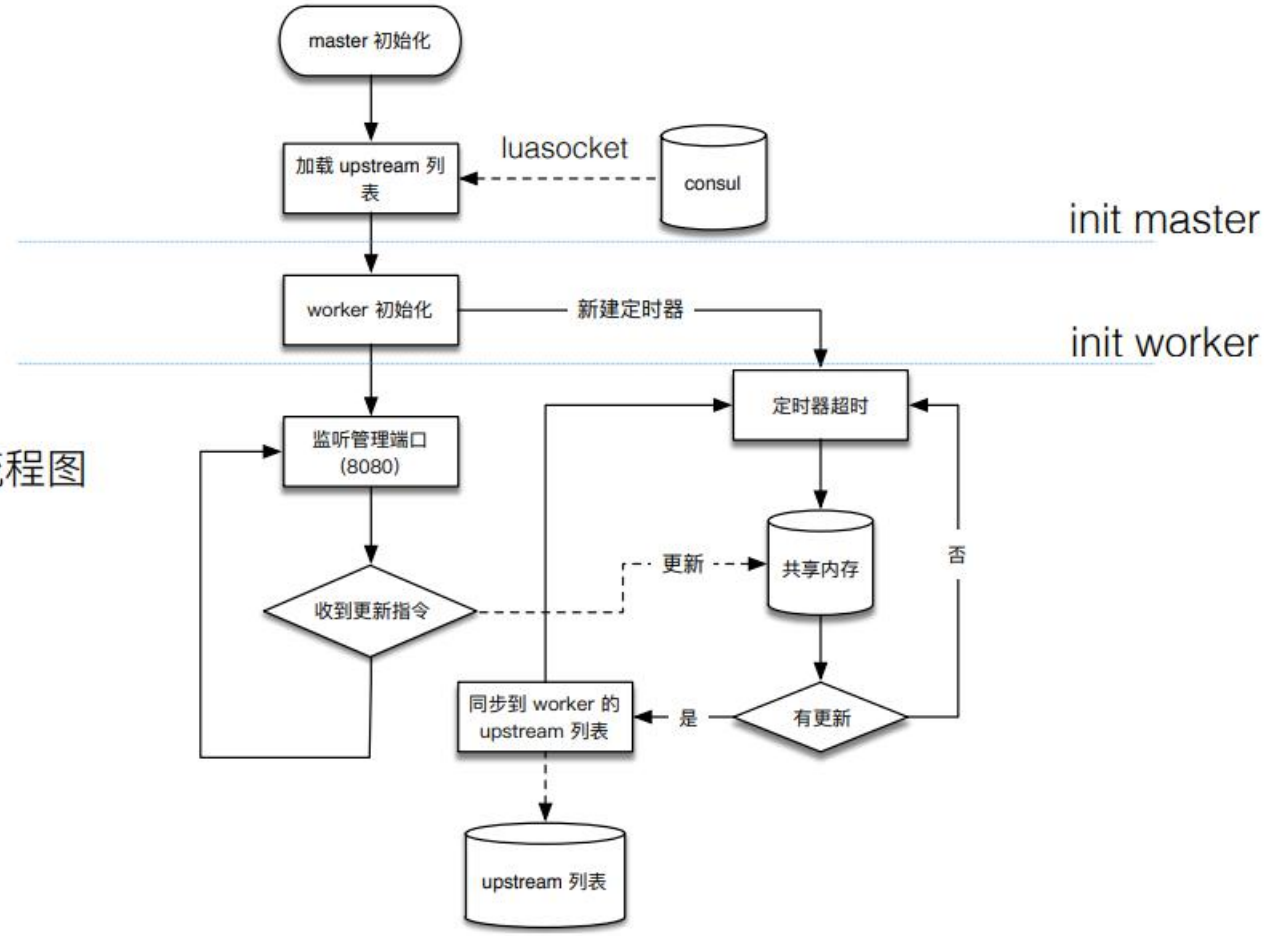
所有的服务注册到一个注册中心

Nginx + Consul + Registrator



更新upstream

动态upstream流程图



https://github.com/upyun/lua-resty-checkups