APACHE APISIX

基于 APISIX 的自动化运维平台介绍

陈庆

卓盟科技 运维架构师

APACHE APISIX

CONTENT

APACHE APISIX

01 自我介绍

APACHE APISIX

自我介绍

职业

系统架构，全栈开发者，Devopser

履历

卓盟科技（目前）：运维总监兼主架构
同程数科：高级运维经理
爱奇艺：计算云项目经理

联系方式

Mail: chenqing24@163.com
BLog: chenqing24.github.io

APACHE APISIX

02

项目简介

自动化运维平台的特点和核心组件

APACHE APISIX

项目简介

与开发语言无关，可与各种Web Framework集成，前后端分离

HTTP接口管控，全restful级别，由Yapi规范定义

与CMDB对接，数据源规范，可复用

性能高，相当于Nginx的90%，支持多种LB策略

安全性可扩展，支持加载软WAF

提供统一Log

提供统一权限管理

APACHE APISIX

核心组件

服务网关：APISIX

https://github.com/apache/apisix

API管理：YAPI

https://github.com/ymfe/yapi

访问控制框架：Casbin

https://github.com/casbin/casbin

Web框架：mug-skeleton

https://github.com/chenqing24/mug-skeleton 自研

对接第三方平台

CMDB（自研）
OpenLDAP
工作流Activiti（https://github.com/Activiti/Activiti）

APACHE APISIX

03 整体方案

平台架构和常见业务场景

整体方案

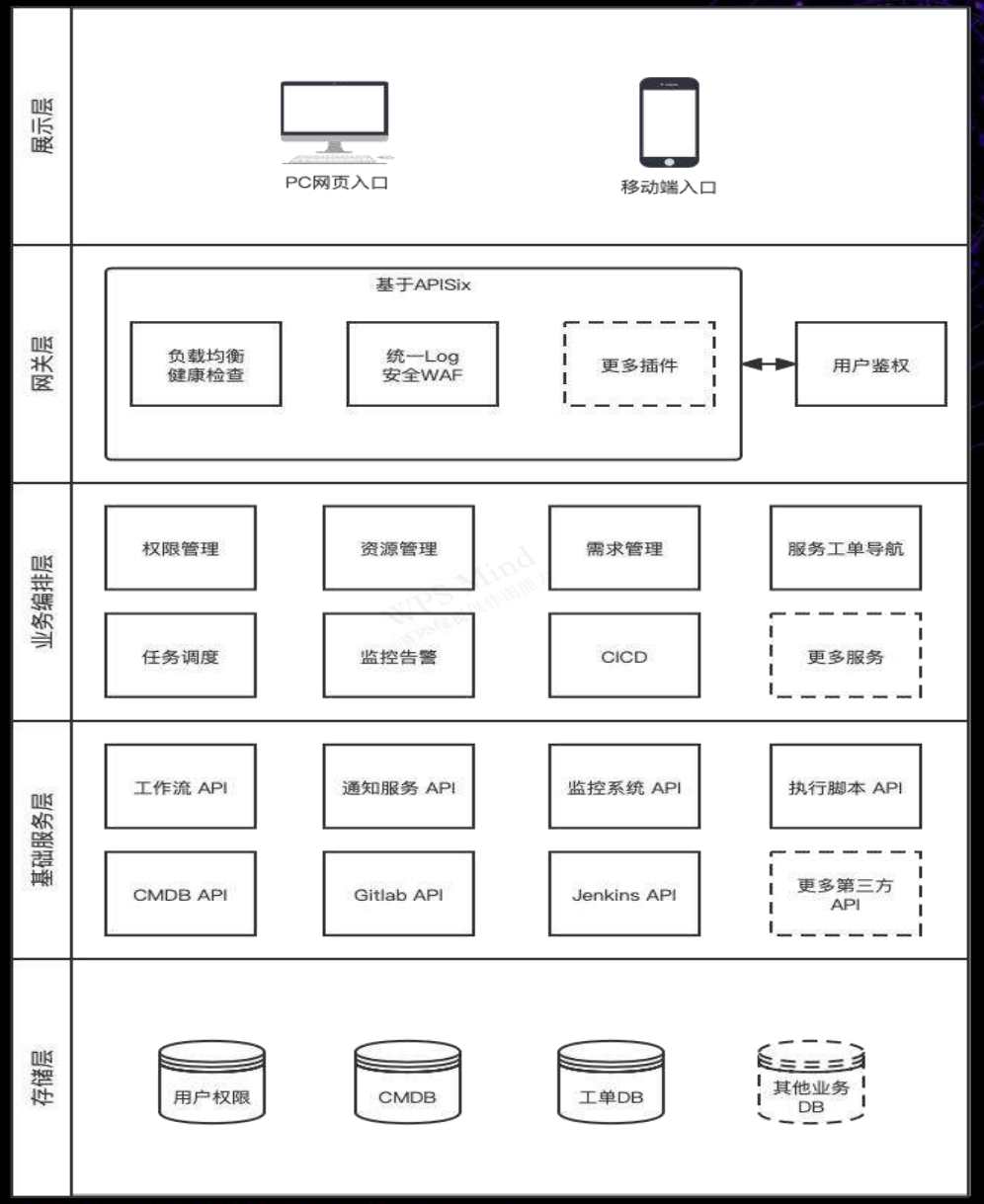
运维平台架构

网关作为服务边界，默认内部可信，外部需要认证

通用模块独立抽出，如权限，让开发者聚焦业务代码

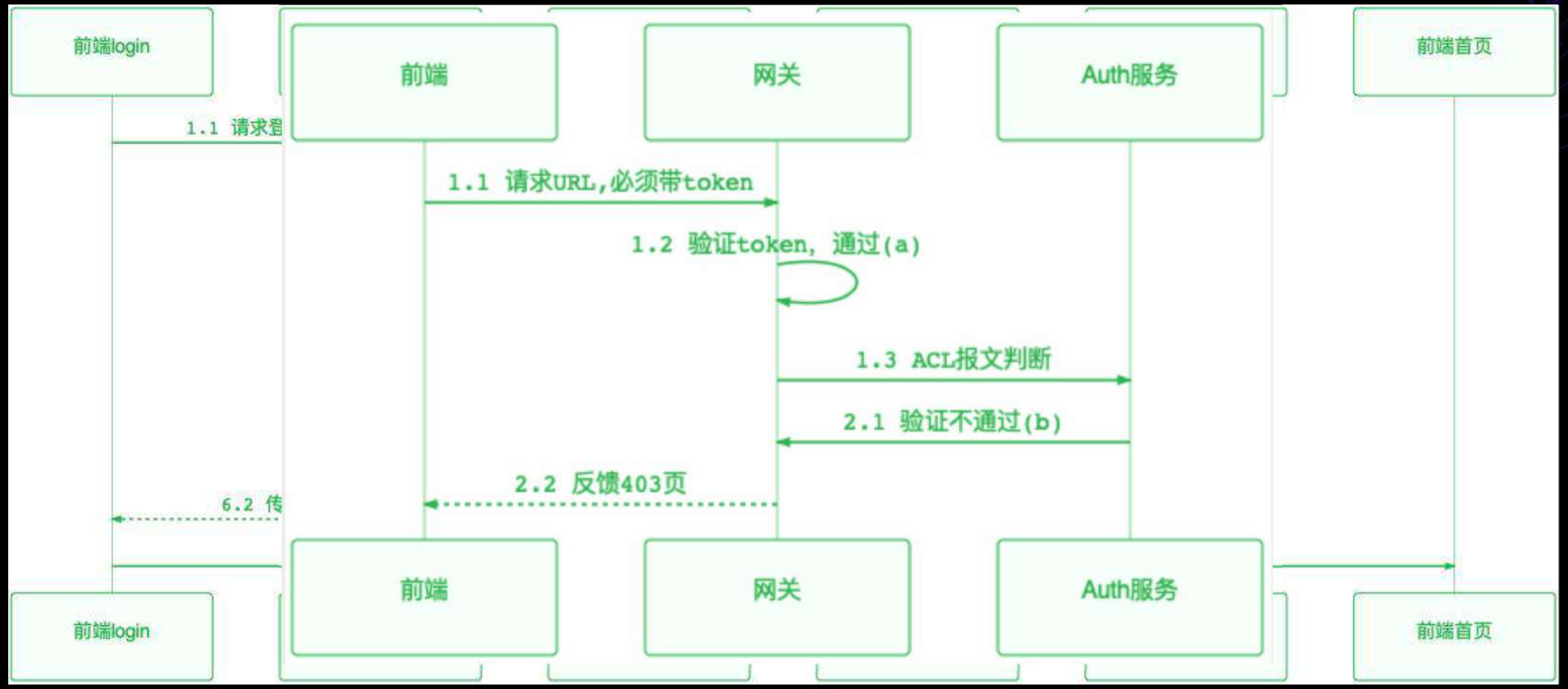
尽可能复用第三方开源组件

业务层服务是对基础服务接口的编排



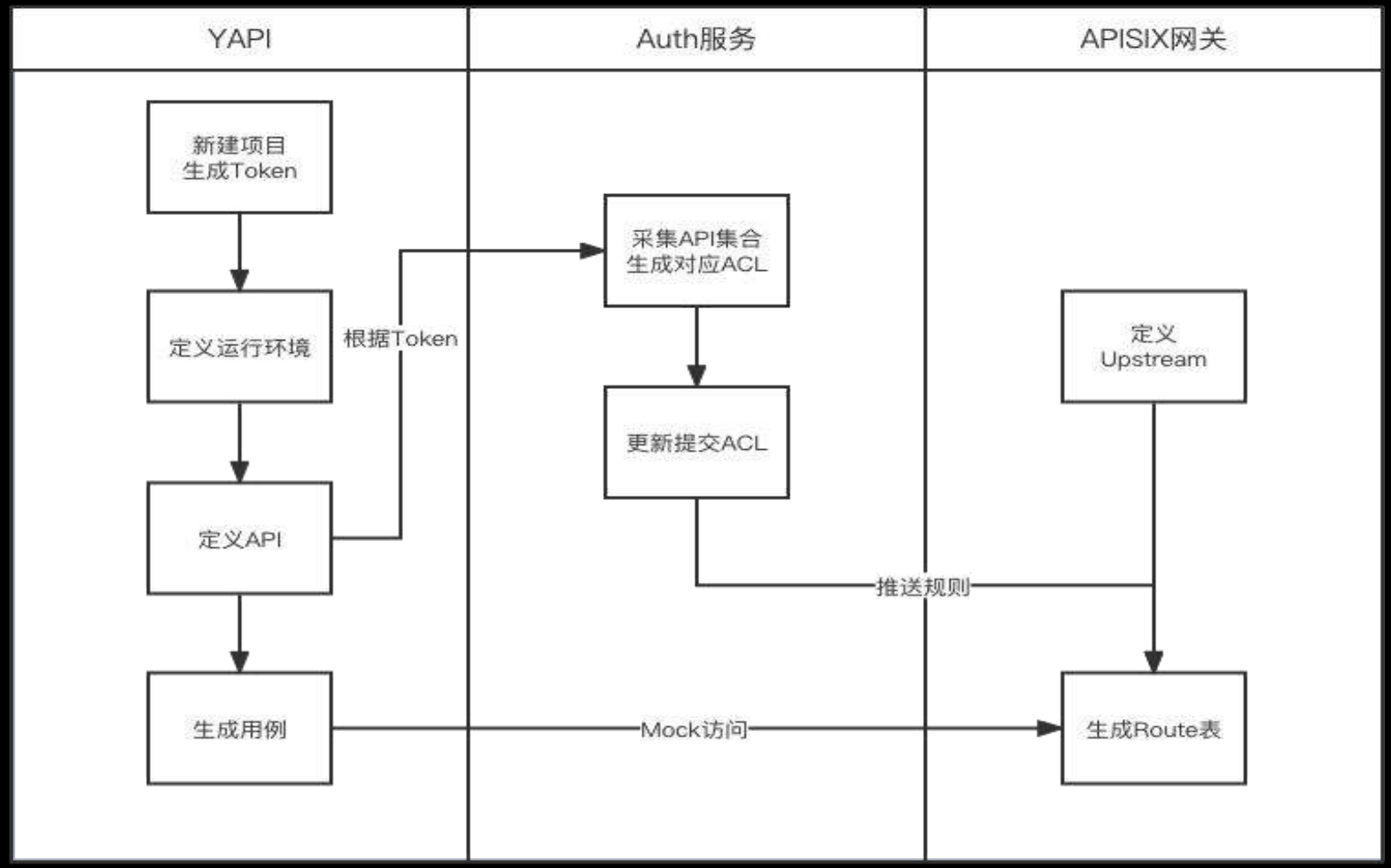
常见业务场景

用户登录/权限验证



常见业务场景

新业务微服务接入



APACHE APISIX

04

技术细节

自定义Lua插件原理和实例

技术细节

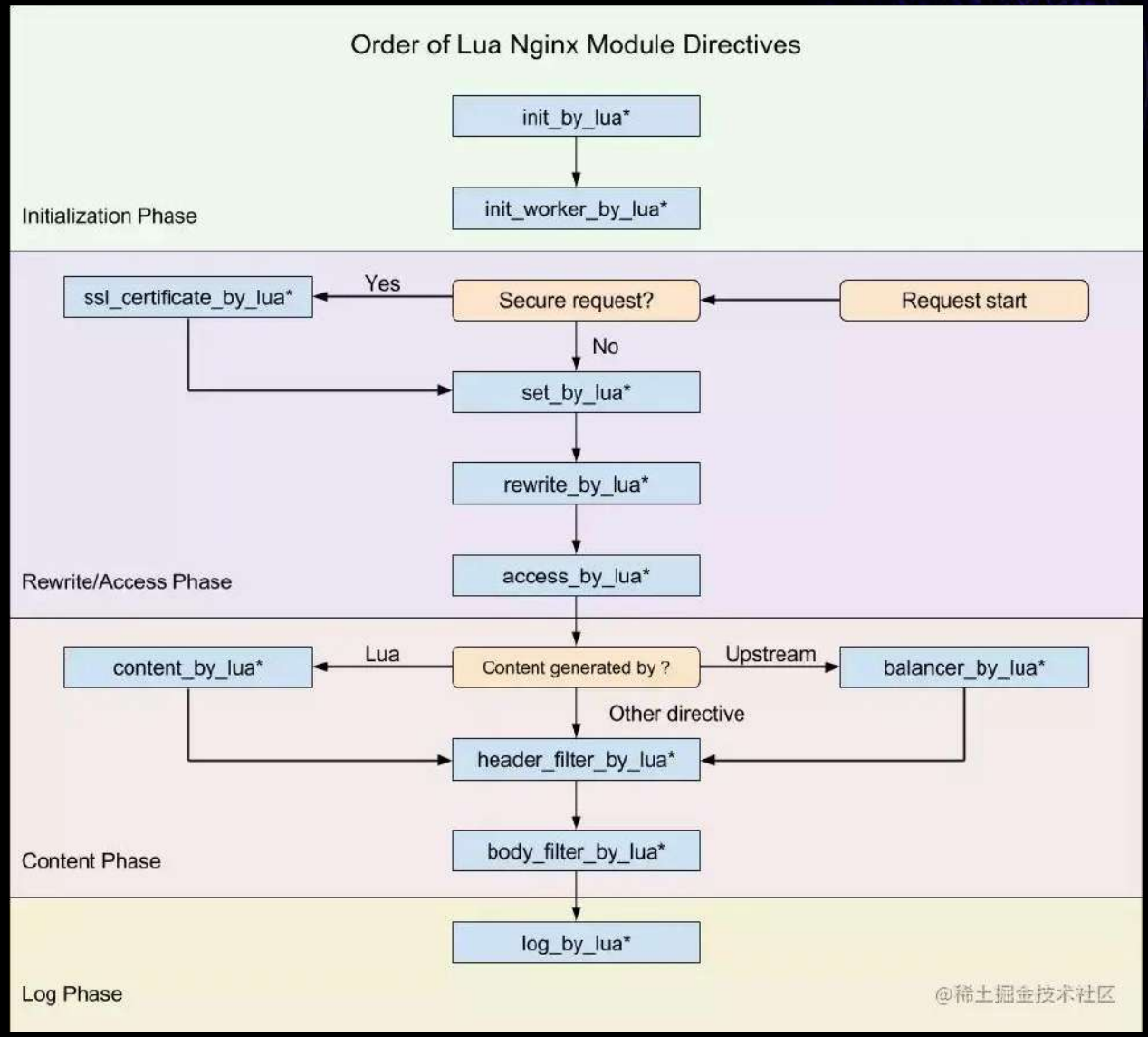
HTTP请求的常见切入点

rewrite_by_lua: 运行于 rewrite 阶段的末尾，常用于转发、重定向、缓存等

access_by_lua: deny指令来自ngx_access 模块，运行于 access 阶段，常用于IP准入、接口权限等情况集中处理

header_filter_by_lua: output-header-filter一般用来设置cookie和headers，可用于灰度发布的流量切换

log_by_lua: 会话完成后本地异步完成日志记录



技术细节

自定义常见实例: acl-plugin.lua

源码: https://github.com/chenqing24/ops-apisix/blob/main/centos/acl-plugin.lua

功能

1. 解析jwt token，获取用户id
2. 在rewrite阶段，向后台ACL验证接口发起请求（用户id，method，uri）
    1. 通过时，log.info
    2. 不通过时，反馈异常状态码：401，500
3. 处理跨域的OPTIONS（当时cors插件还没发布）

部署

1. 复制到/usr/local/apisix/apisix/plugins/acl-plugin.lua
2. apixis的config.yaml的plugins数组中增加acl-plugin.lua

APACHE APISIX

技术细节

acl-plugin.lua配套的auth服务

功能: 服务启动时，从db载入casbin的acl规则表，如果有规则变更，需要通知auth进行reload

核心接口

1. account
    1. login：调ldap认证账号和密码；从cmdb查询用户信息，和过期时间一起生成jwt_token，反馈生成的cookie；注册consumer
    2. acl_check：验证要素（用户id，method，uri），基于Casbin的RESTful模型
2. yapi：
    1. 和YAPI服务接口交互，读取指定项目的api定义，存db
    2. 和权限管理的页面表单交互，生成acl表，转为casbin规则，存db

部署

和 APISIX 实例同宿主机，端口和lua中的定义保持一致

APACHE APISIX

感谢聆听

THANKS