

**构建OAuth2服务器**

**golang 语言实现**

**讲师：杨波**

**研发总监/资深架构师**

第

1

部分

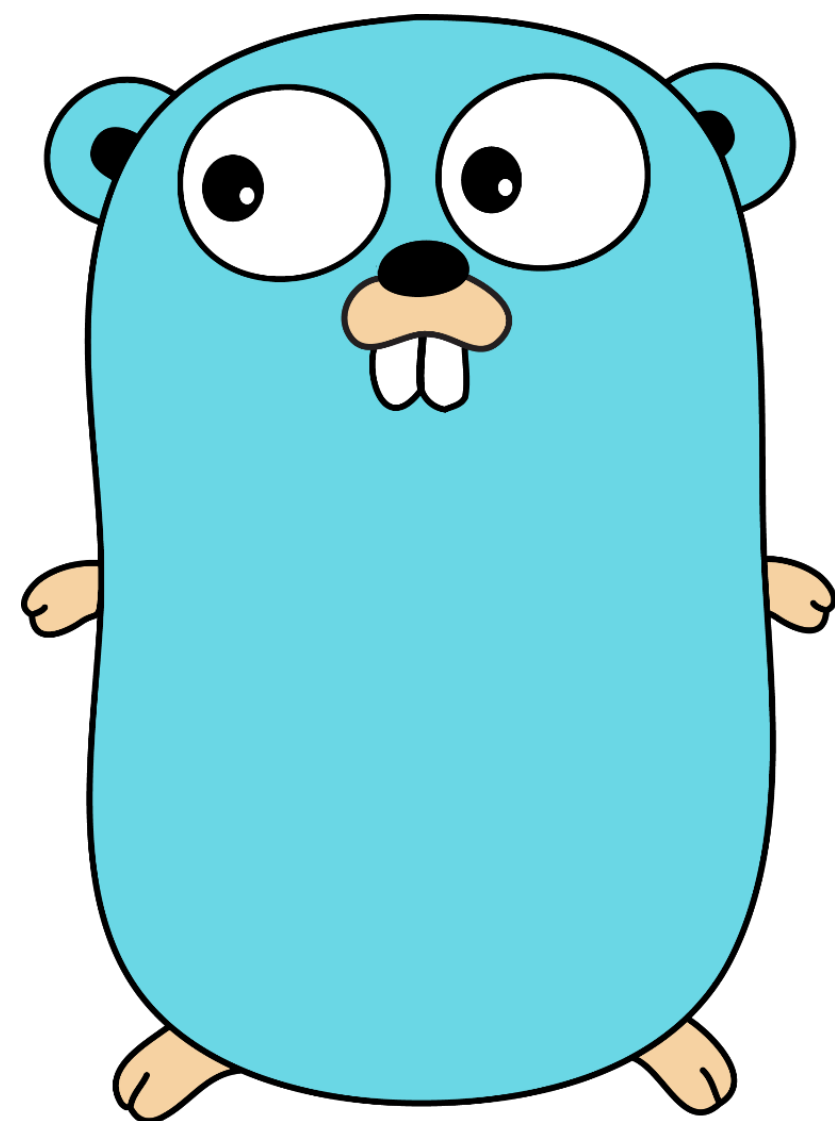
课程概述和背景

# 课程反馈

- 课程反馈OAuth2问题最多
- Spring Cloud OAuth2复杂难理解
- OAuth2的四个流程具体如何实现?
- 课程缺乏项目架构设计和开发实战案例
- 波波老师实践中是如何做架构设计和选型的?
- OAuth2授权认证是微服务架构重要环节



# Why Golang?



- 1 简单入门门槛低，适合课程讲解
- 2 Google开发支持，社区生态好
- 3 云原生基础语言(k8s/docker/etcd/istio)
- 4 微服务多语言(polyglot)开发趋势
- 5 OAuth2实现和具体语言无关

# 课程大纲

- 01 课程概述和背景
- 02 架构和设计
- 03 开发环境搭建(Lab01)
- 04 基础代码(Code Review)
- 05 数据访问模块(Code Review)
- 06 OAuth2服务模块(Code Review)
- 07 Web服务模块(Code Review)
- 08 启动流程(Code Review)
- 09 起步准备实验(Lab02)

10

OAuth2授权码模式实验(Lab03)

11

OAuth2简化模式实验(Lab04)

12

OAuth2用户名密码模式实验(Lab05)

13

OAuth2客户端模式实验(Lab06)

14

OAuth2令牌校验实验(Lab07)

15

OAuth2令牌刷新实验(Lab08)

16

项目复盘和扩展环节

17

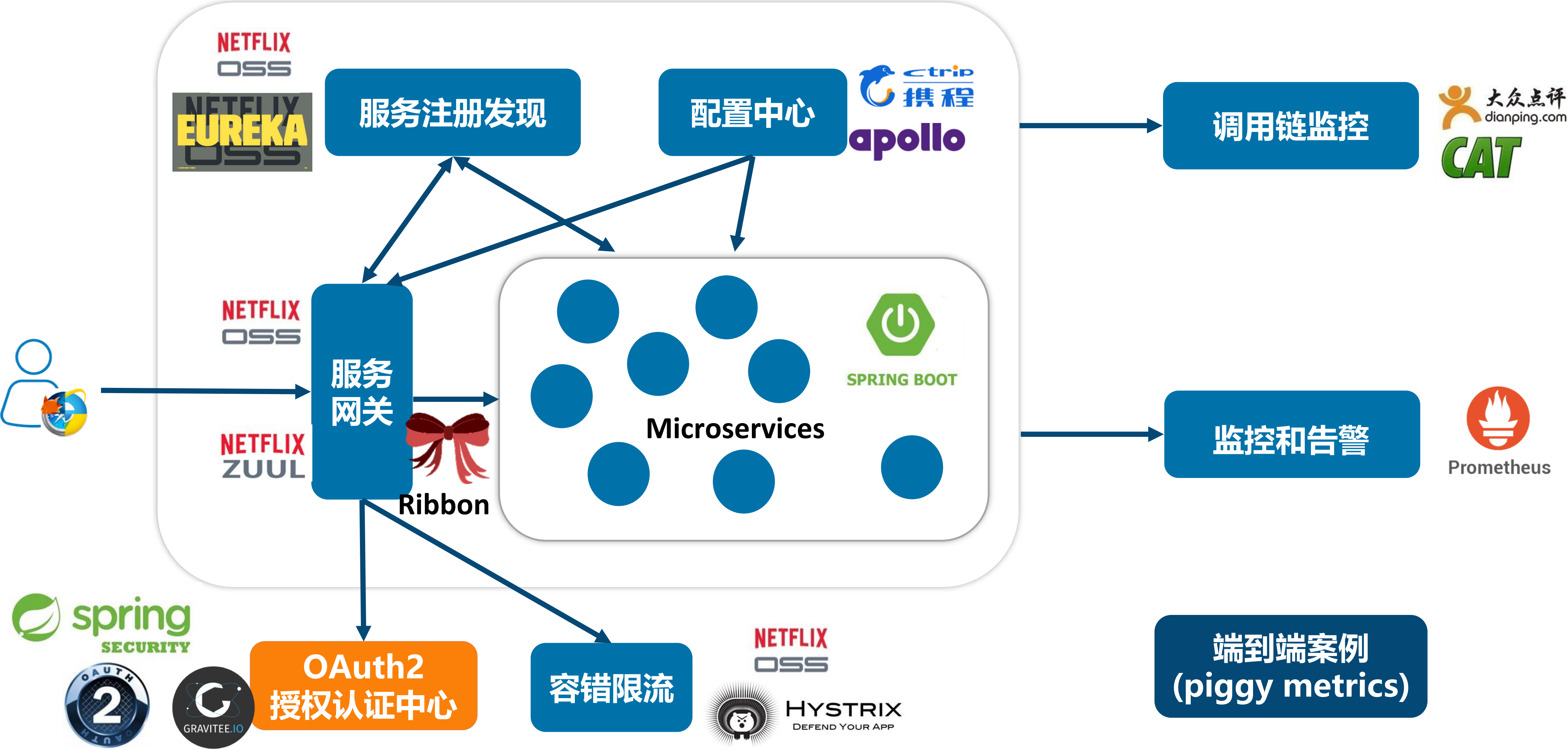
参考资料

# 杨波的微服务基础架构体系2018





# 架构和技术栈





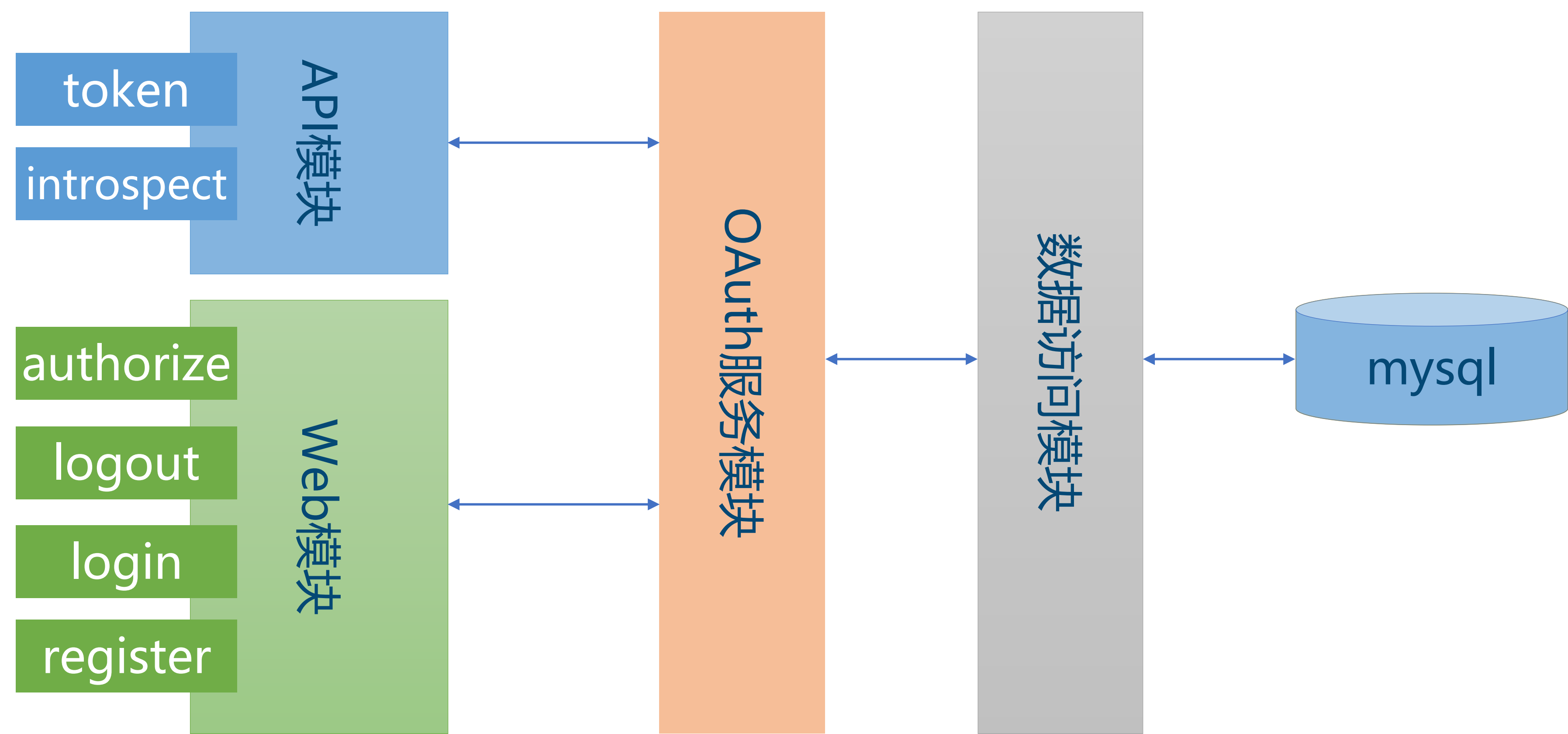
第

2

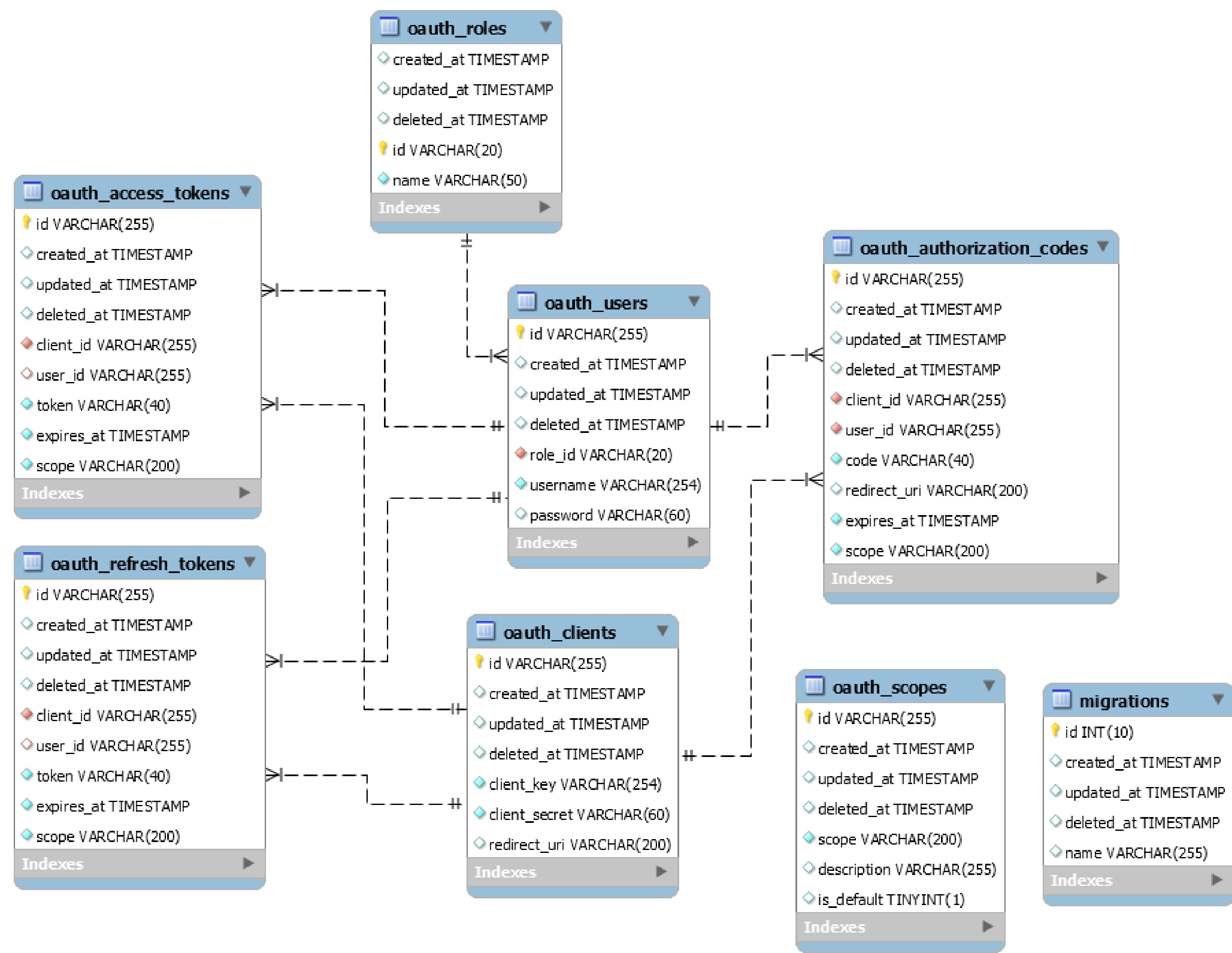
部分

# 架构和设计

# 总体架构



# 数据模型



# 接口模型

接口名	模块	HTTP方法	用途
tokens	API	POST	获取令牌
introspect	API	POST	校验和获取令牌信息
register	Web	GET/POST	用户注册
login	Web	GET/POST	用户登录
logout	Web	GET	用户登出
authorize	Web	GET/POST	授权获取授权码或令牌

第

3

部分

## 开发环境搭建(Lab01)

# 第 4 部分

## 基础代码(Code Review)



第

5

部分

# 数据访问模块(Code Review)

第

6

部分

# OAuth2服务模块(Code Review)

第

7

部分

# Web服务模块(Code Review)

第

8

部分

## 启动流程(Code Review)

第

9

部分

## 起步准备实验 (Lab02)

# 第10部分

## OAuth2授权码模式实验 (Lab03)

<https://tools.ietf.org/html/rfc6749#section-4.1>



# 第11部分

## OAuth2简化模式实验 (Lab04)

<https://tools.ietf.org/html/rfc6749#section-4.2>

# 第12部分

## OAuth2用户名密码模式实验 (Lab05)

<https://tools.ietf.org/html/rfc6749#section-4.3>

# 第13部分

## OAuth2客户端模式实验 (Lab06)

<https://tools.ietf.org/html/rfc6749#section-4.4>

# 第14部分

## OAuth2令牌校验实验 (Lab07)

<https://tools.ietf.org/html/rfc7662>

# 第15部分

## OAuth2令牌刷新实验 (Lab08)

<https://tools.ietf.org/html/rfc6749#section-6>

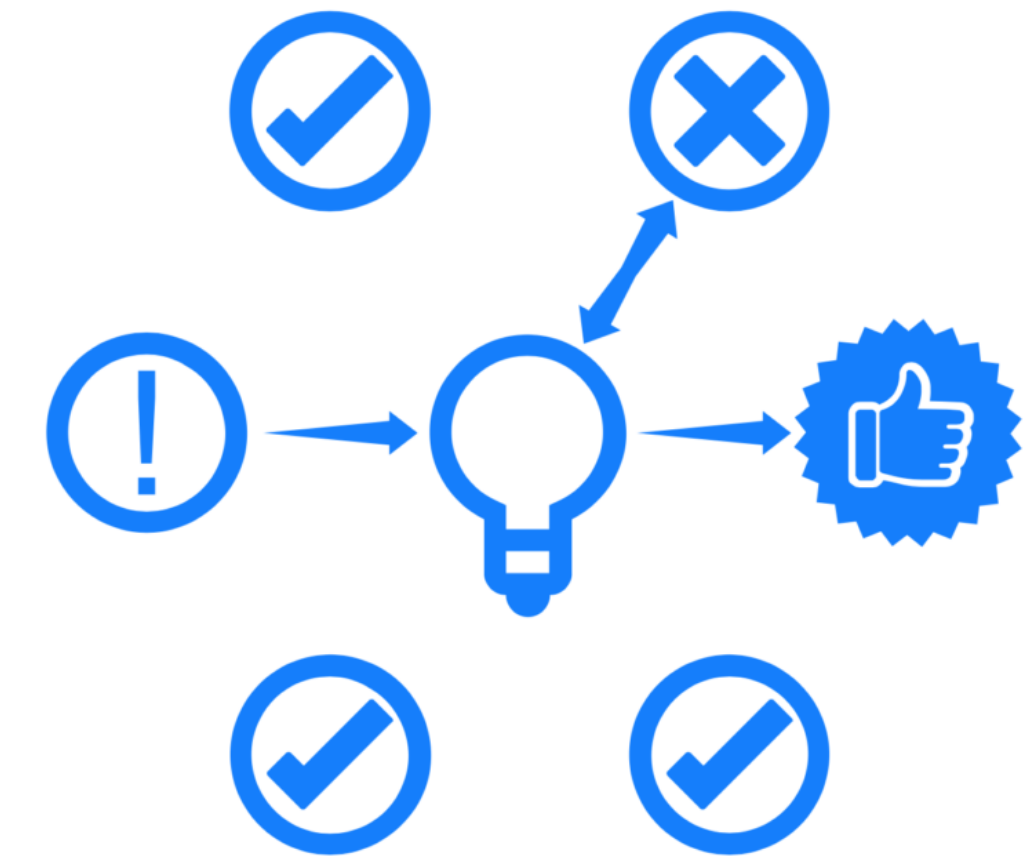
# 第16部分

## 项目复盘和扩展环节



# 项目复盘

- **深入一种语言编程**
  - Programming into a language, not in a language
  - 《代码大全》
- **架构设计要素**
  - 总体架构
  - 数据模型(领域模型)
  - 接口模型
- **多语言编程(polyglot)**
- **利用开源**
  - <https://github.com/RichardKnop/go-oauth2-server>
  - 快速熟悉技术领域
  - 定制改造



# 生产扩展

- 支持token revoke端点
- 支持jwt令牌
- Client管理
- 对接企业内部用户数据
- 监控(prometheus?)
- 高可用高性能
- 集中式缓存
- 其它语言实现(java?)

# 第17部分

## 参考资源和后续课程预览

# Golang语言参考

- **Go by Example中文版**
  - <https://gobyexample.xgwang.me/>
- **Golang Cheat Sheet**
  - <https://github.com/a8m/go-lang-cheat-sheet>



# 其它OAuth2开源产品

- **Redhat Keycloak (Java, 3k stars)**



- <http://www.keycloak.org>

- **Apereo Cas (Java 3k stars)**



- <https://github.com/apereo/cas>

- **IdentityServer (C#, 3.6k stars)**



- <https://identityserver.io>

- **Ory Hydra (Golang, 5.1k stars)**



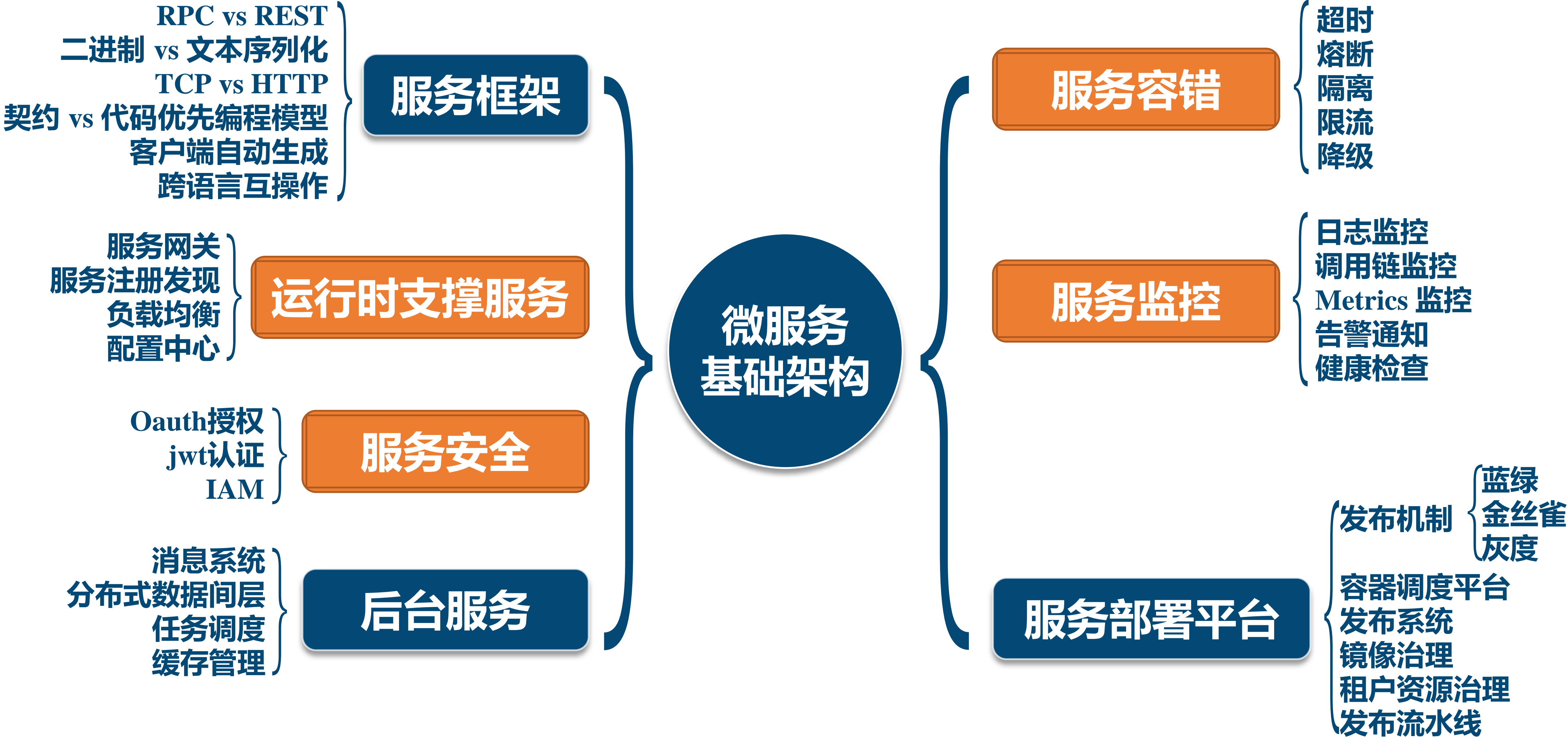
- <https://github.com/ory/hydra>

- **ThePHPLeague OAuth2 2.0 Server (PHP, 4.3k stars)**



- <https://github.com/thephpleague/oauth2-server>

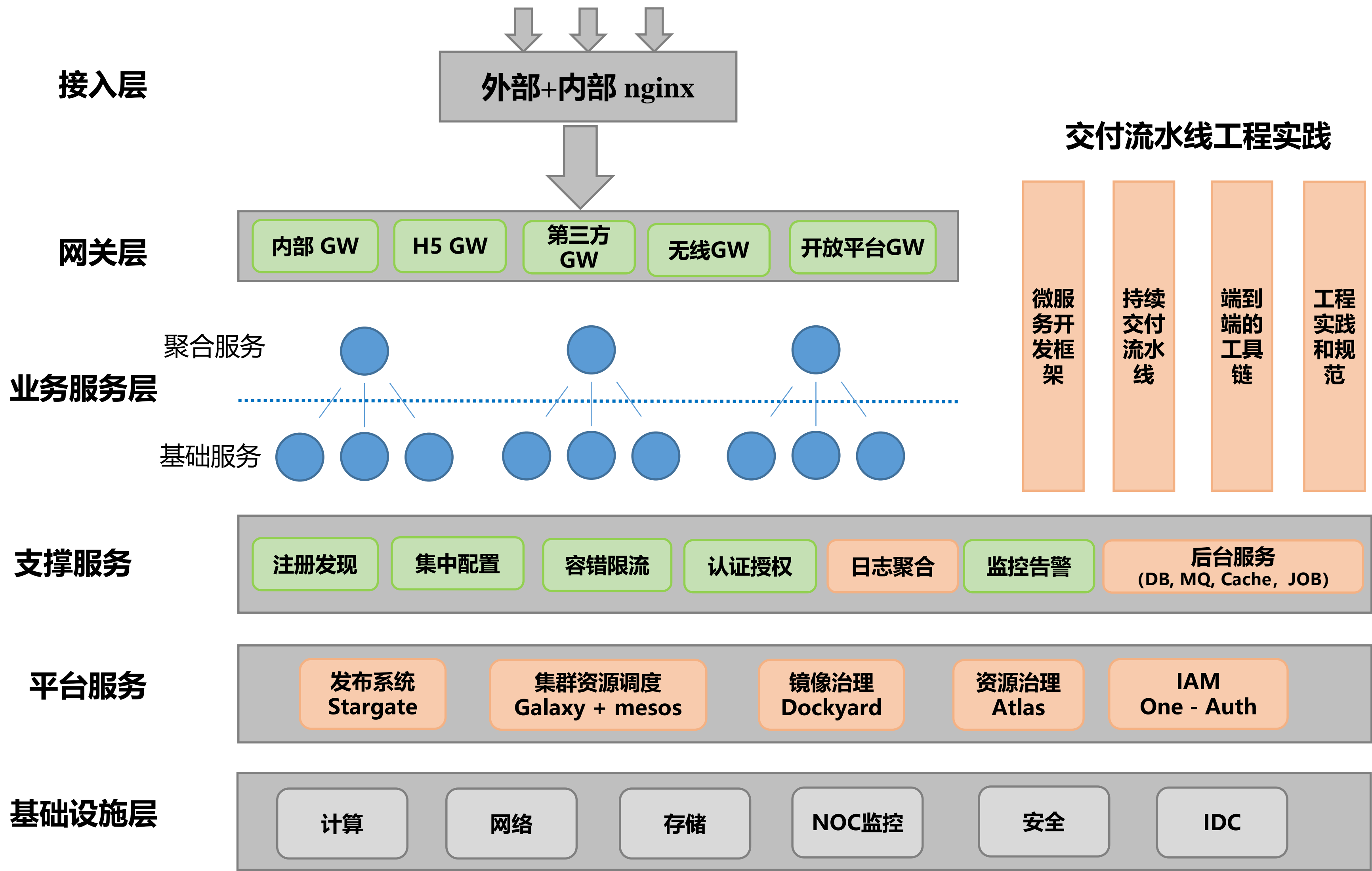
# 后续课程预览~2018课程模块





# 后续课程预览~技术体系

微服务架构总体技术体系



# 架构和技术栈回顾

