

LIANER FITMOMENTS · ENGINEERING REVIEW

方案评审

网关迁移

11-02 线上故障后的方案：网关这一层要不要，怎么不停服地拿掉 ShenYu。

适用	William · 后端研发 · 运维值班
来源	2026-11-02 生产网关故障复盘
版本	v1.0 · 2026-11-02

练二一下，好状态。

练二健身 · 研发中心　hellolianer.com

CONTENTS

目录

01 结论 03
一句话：不再买网关，逐个服务切走

02 现在的链路 04
网关到底在干什么，今天为什么全挂

03 托管网关管什么 05
阿里云网关的每项能力，我们需不需要

04 要不要专门网关 07
四种做法对比，什么时候才值得上

05 astra 的意见 08
原话要点，以及哪里一致、哪里不同

06 目标架构 09
迁移完成后长什么样

07 迁移步骤 11
五个阶段、时间、谁来做

08 回滚与风险 13
每一步怎么退回，最怕什么

09 验收与待决策 14
做到什么算完成，需要 William 定的事

MUST KNOW

- 双11（11-11）前**只做止血**，不动请求路径
- ZooKeeper 也是服务之间互调的注册中心，下线 ShenYu 时**绝不能一起停**
- 新入口的登录鉴权必须和现在**完全一致且更严**，这是最大风险

01

SCOPE

结论

练二这个规模不需要再买专门的网关，改成服务自己接 HTTP，按服务逐个切走。

- **事故的根子不在 ShenYu 这个牌子**：网关、网关后台、ZooKeeper、nginx 全在一台机上；路由推丢了没人知道；启停全靠手工，所以出现了两个网关进程抢端口。换个产品如果还这样管，照样出事。
- **推荐做法**：阿里云负载均衡 + 两台 nginx + 服务自己接 HTTP + 统一鉴权库。服务之间继续用 Dubbo，前端地址一个字不改。
- **节奏**：本周止血，双11 后按 ground → coach → user → payment 逐个切，约 10 周日历时间、约 5 人周工作量。每一步都能 1 分钟内退回。
- **托管网关以后要用再加**。注意阿里云原 API 网关和 MSE 云原生网关已在 2026-08-23 停止新购，现在只能买「云原生 API 网关」。

> **更正 11-02 上午的两处说法**
>
> 一、服务用的是老版本 Dubbo 2.6.5，不支持「Triple 协议直接对外」，改用服务里已有的 Spring Web 接 HTTP。
>
> 二、生产 ZooKeeper 不只是给网关用的，它也是服务之间互相调用的注册中心，下线 ShenYu 时必须保留，高可用单独立项。

02

— CURRENT

现在的链路

所有前端请求都先经过 ShenYu，由它翻译成服务能听懂的 Dubbo 调用。

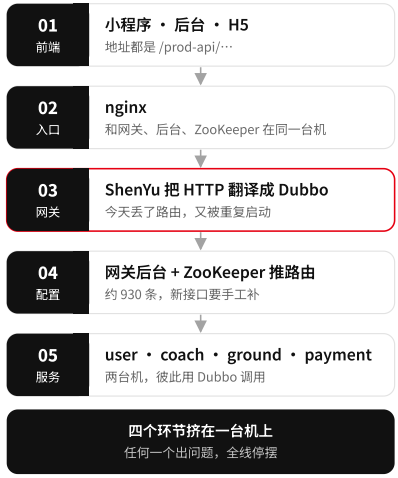


图 2-1 今天的故障：网关丢了路由，后台同步成功却没送到；重启时又起了两个进程

1 网关实际在干的事

按路径分发	把 /user、/coach、/payment、/ground 送到对应服务。nginx 本身就能做
HTTP 转 Dubbo	每个接口一条手工配置，生产不会自动注册，漏配就报 -107 / -102
登录与身份	解析登录 token，把会员、管理员、教练的身份写进请求，服务据此判断是谁

签名、加密	插件开着，但前端代码里没看到签名或加密调用，需在后台只读确认是否在用

> **好消息**
>
> 服务已经能直接对外提供 HTTP：支付和用户的回调地址本来就绕过 ShenYu、由 nginx 直连服务。后台接口的登录校验服务端也已经自己做了一遍。

03

— GATEWAY

托管网关管什么

托管网关卖的是「入口不用自己运维」和「统一治理」，下面逐项看我们需不需要。

多机热备	**需要**。不买网关的办法：负载均衡 + 两台 nginx
路由	**需要但简单**。nginx 4 条转发规则就够
统一登录校验	**需要**。服务里本来就要校验一遍，入口再做是锦上添花
限流防刷	大促有用。nginx 能做简单限流；业务防刷本来就要写在服务里
防攻击 WAF	有用。WAF 是单独的产品，可直接挂在负载均衡或域名上，不依赖网关
HTTP 转 Dubbo	**不推荐**。还是每个接口手工配一遍，等于把今天的痛点搬上云

灰度切流	迁移期有用。nginx 按比例分流就能做
开放平台	给第三方发密钥、按量收费。我们现在没有这种需求
日志监控	有用。nginx 日志接入阿里云日志服务即可

费用参考：MSE 云原生网关每个节点（2 核 4G）约 422 元/月，至少 2 个节点；云原生 API 网关以购买页为准。钱不是主要成本，主要成本是多一个要学、要配、出事要查的产品。

04

— OPTIONS

要不要专门网关

坦白说：现在不需要。4 个服务、一个团队、没有开放平台，nginx 加统一鉴权库就够了。

四种做法

A 继续用 ShenYu，只加固
改动最小，手工配路由的痛点还在
只做止血

B 不要专门网关
nginx + 服务自己接 HTTP + 统一鉴权
推荐

C 托管网关 + 服务 HTTP
免运维、功能全，多一个产品和月费
以后再说

D 托管网关做 HTTP 转 Dubbo
930 个接口要在云上再手工配一遍
不推荐

练二现在的规模，B 就够用

图 4-1 B 方案以后随时能在 nginx 前加托管网关，不用推倒重来

1 什么时候才值得上托管网关

- 要给**第三方开放接口**，需要发密钥、限配额。
- **多个团队**各自对外发布接口，需要一个统一入口管起来。
- 灰度、限流规则变得**很频繁**，nginx 改不过来。
- 合规要求**集中审计**所有入口流量。

05

— REVIEW

astra 的意见

11-02 17:10 把现场情况和代码事实交给 astra，以下是它的原话要点，未改动。

> astra
> 同意去 ShenYu，不赞成把采购网关作为前置条件。这次暴露的是单机故障域、配置同步不可观测和手工运维失控。换产品不能自动解决这些问题。

> astra
> 这个规模可以不设专门网关。建议 SLB→双实例 nginx→服务 HTTP 适配层，共享鉴权库，内部暂留 Dubbo。出现多团队、多消费者配额、频繁灰度或明显入口运维负担，再买托管网关。

> astra
> 最大风险是 REST 绕过服务端鉴权。HTTP 入口必须验签、校验有效期和角色，覆盖外传的身份字段，并执行门店、资源权限检查。不能只平移 JWT 解析。

> astra
> 本周先止血：单实例启停、健康检查和回滚；备份配置与规则，核查签名和加密插件；增加真实业务探针与同步异常告警。下线 ShenYu 绝不能顺手停 ZooKeeper。

要不要网关　一致：先不采购

ZooKeeper	**一致**：保留，高可用单独做；据此更正了上午的说法
鉴权	**一致**；补充：入口一律先去掉客户端自带的身份字段，再按登录 token 写回
工期	**一致**：4～6 周只算试点；按双11 冻结排成约 10 周日历时间
网关选型	**补充更正**：astra 区分了传统 API 网关和 MSE 网关，这两款都已停止新购
HTTP 入口做法	**补充**：自动扫描现有接口注解生成同名 HTTP 入口，不用逐个手写

06

— TARGET

目标架构

前端不改，入口变成负载均衡加两台 nginx，服务自己接 HTTP。

统一鉴权库	规则照搬现在网关的做法；更严：先清掉客户端自带的身份字段，后台接口没有有效登录一律拒绝，返回码和现在一样
HTTP 入口	启动时自动扫描现有接口，生成路径一模一样的 HTTP 入口。新接口发布即生效，告别 -107 / -102
nginx	按路径分发；迁移期按比例分流；配置放 Git、走 Jenkins 发布



图 6-1 迁移完成后的链路：红框是这次要新写的统一鉴权和 HTTP 入口

07

— PLAN

迁移步骤

五个阶段，双11 冻结期不动；负责人按角色写，具体人选待定。



图 7-1 日期为建议开始日；payment 预计切到 01-08

1 阶段 0 止血（运维值班 + 后端负责人）

- **只能起一个网关**：启停做成 Jenkins 任务或系统服务，启动前检查进程数，不是 0 就拒绝。
- **告警发企微群**：每分钟用真实只读接口探测 4 个服务；网关进程数、ZooKeeper 健康、同步异常都要报。
- **备份与核查**：只读导出全部路由配置进 Git（不含密钥）；确认签名、加密、websocket 插件是否在用。
- **查根因、写手册**：保留今天的日志，查清网关为什么丢路由；启停步骤写成一页纸。

- **审计身份安全**：确认所有小程序接口都无法在未登录状态下冒用他人身份。这条不等迁移，本周先查。

2 阶段 1 鉴权库 + HTTP 入口（后端负责人 + 测试）

先只发到测试2。每个服务挑 20～30 个高频接口，经旧网关和新入口各请求一遍，返回必须一致；覆盖「未登录」「登录过期」「正常」三种情况。前端各端在测试2 跑一遍主流程。

3 阶段 2～3 逐个服务切流（后端负责人 + 运维值班）



图 7-2 每个服务都走这四档；旧路由在 100% 后保留 1 周才停用

1 ground	68 条路由，前端调用最少，用户主要是店长和总部
2 coach	66 条，重点测教练登录和教练身份
3 user	207 条，重点测小程序登录、开门、人脸
4 payment	587 条，最后切；测下单、退款、回调不重复；不做写请求双跑；财务确认对账

4 阶段 4 下线（运维值班，William 确认）

旧网关连续 2 周零请求后停网关和网关后台，程序和配置备份保留 3 个月；补上第二台 nginx 和负载均衡。ZooKeeper 保留，2027 年一季度单独做高可用。

08

— RISKS

回滚与风险

每一步都能退回；最怕的是身份校验出漏洞和支付重复。

1 怎么回滚

阶段 0	新的启停方式不好用，就照手册手工启停，分钟级
阶段 1	只在测试2，生产不受影响
阶段 2～3	nginx 对应服务改回旧网关并重载，1 分钟内
阶段 4	用保留的程序和配置重新启动旧网关并同步，约 30 分钟

2 主要风险

01 新入口的身份校验不能有一点出入

身份算错就可能越权看到或改到别人的数据。统一库一处实现，对照测试覆盖未登录、过期、冒用三种情况。

02 payment 最后切，避开月初关账

下单、退款、回调出错会直接影响钱。只按比例分流，不做写请求双跑，回调地址不变。

03 下线时 ZooKeeper 必须保留

它停了，服务之间的调用会全部中断，影响比今天更大。

其他风险：返回格式或错误码不一致导致前端不跳登录页（靠对照测试 + 小比例切流发现）；个别接口参数转换不同（按现有路由配置逐条核对）；签名、加密插件实际在用（阶段 0 先确认）。

09

— DECISIONS

验收与待决策

截至 2026-11-02 均未开始；下面是验收标准和需要 William 拍板的事。

1 验收标准

- 网关只能有 1 个进程；测试环境断开 ZooKeeper，5 分钟内企微群收到告警。
- 高频接口新旧返回一致（含未登录、过期）；新增接口不需要任何后台配置。
- 每个服务切满 1 周，错误率不高于切换前、无登录类客诉；payment 当月对账无差异。

- 旧网关 2 周零请求后才停机；关掉任意一台 nginx，线上不受影响。

2 需要 William 拍板

方向	同意 B 方案：不买专门网关，本周止血、双11 后切流
人选	后端负责人（约 5 人周）和有生产机权限的运维值班
费用	是否加一台 nginx 和阿里云负载均衡（少量费用）
插队	身份安全审计如发现问题，是否立即插队修复

LIANER® 练二健身

练二一下，好状态。

让更多人身心健康

ShenYu 网关解耦与迁移方案 · v1.0 · 2026-11-02

依据：lianer-back 等仓库只读核对、生产 nginx 配置、阿里云帮助中心（11-02 查询）、astra 意见

不含截图；路由数为 11-02 网关后台计数

练二健身 · hellolianer.com