总体架构与运行环境

文档目的

本章面向开发、测试、部署和运维人员，说明数脉平台各层职责、关键集成、环境要求和安全边界。业务用户无需阅读本章即可完成看板、报表和 AI 问数操作。

图 *10-1* 门户、业务服务、数据底座和外部引擎的分层关系

分层架构

层级	主要组件	职责
用户与门户层	Vue 3、Element Plus、RuoYi-Vue-Plus 风格权限与路由	登录、菜单、工作台、统一交互和受控跳转
应用服务层	Java 21、Spring Boot、MyBatis-Plus	用户权限、业务建模、质量治理、AI 编排、审计和集成票据

层级	主要组件	职责
分析展示层	Superset 6.1.0、JimuReport 2.5.5、GoView 大屏	仪表盘、数据集、SQL、报表和大屏设计
数据治理层	DolphinScheduler、SeaTunnel、Hop、dbt、OpenMetadata	调度、同步、加工、模型构建、元数据和血缘
数据存储层	Doris、MySQL、Redis、对象存储	分析数据、业务配置、缓存与文件资产
模型服务层	企业模型网关 + DeepSeek-V4.1-Flash	自然语言理解、方案生成、受控 SQL 与看板编排

推荐运行环境

项目	要求
Java	21 LTS
Spring Boot	4.1.x
MyBatis-Plus	3.5.17
Node.js	20.19.0 或更高
pnpm	10.0.0 或更高
浏览器	当前版本 Chrome、Edge；启用 JavaScript 和 Cookie
数据库	MySQL 8.x（配置）、Doris（分析）
缓存	Redis 7.x
容器	Docker Engine 与 Docker Compose

关键集成原则

1. 数脉门户是统一身份入口，用户不需要保存 Superset、JimuReport、DolphinScheduler 等子系统的独立口令。
2. 集成跳转使用短时、一次性票据；票据绑定用户、目标页面和有效期，不能在前端日志中回显。
3. 后台服务和数据引擎使用独立服务账号；服务账号凭据通过环境变量或密钥管理注入。
4. 受控 SQL 只允许只读查询，必须限制 Schema、字段、行数和执行时间。
5. 发布链固定为 `DBT → Doris → OpenMetadata → DolphinScheduler → Superset`，每一步都可追溯。
6. AI 不得直接拼接并执行任意 SQL；应先生成结构化方案，再通过白名单编译器和二次确认执行。

开发前必须理解的四条边界

1. 前端不是安全边界。 菜单隐藏只改善体验；接口仍需服务端权限校验。
2. 第三方页面不直接拼接任意 **URL**。 Superset、JimuReport、GoView、DolphinScheduler、Hop 均通过后端页面白名单和一次性票据打开。
3. **AI** 不直接执行任意 **SQL**。服务端会做数据集范围、字段白名单、只读 SQL 和结果行数等校验。
4. 发布使用不可变版本。
   审核通过的模型、发布的大屏和流水线版本不能被原地覆盖，变更应形成新版本并可追溯。

本地开发目录

`ui/`	前端页面与 API 封装
`source/ruoyi-modules/ruoyi-bi/`	BI、建模、ETL、AI 后端模块
`source/script/sql/`	初始化与迁移脚本
`docs/`	设计、验收和部署资料
`infra/`	MySQL、Redis、Doris、Superset 等基础设施

一次典型请求的链路

浏览器 → RuoYi 网关 → JWT 鉴权 → 菜单/按钮权限 → BI 控制器
→ 白名单与参数校验 → 业务服务 → 数据源/第三方平台
→ 脱敏审计日志 → 返回结构化结果

环境配置约定

`APP_BASE_URL`	门户对外地址
`DATABASE_*`	MySQL 配置连接
`REDIS_*`	Redis 连接与认证
`AI_GATEWAY_BASE_URL`	企业模型网关地址
`AI_GATEWAY_API_KEY`	由部署环境注入，禁止入库和入仓
`AI_DEFAULT_MODEL`	默认模型标识
`SUPERSET_*`	Superset 服务与跳转密钥
`DOLPHINSCHEDULER_*`	调度服务与票据配置
`OPENMETADATA_*`	元数据服务配置

> 安全提示：示例只列变量名，不提供真实密钥、数据库口令或内部地址。生产环境应使用 Secret Manager、Kubernetes Secret 或受控环境变量。

部署检查清单

- 前端、后端、数据库、Redis、Superset 和分析数据库健康检查均通过。
- HTTPS 证书、跨域策略、Cookie 属性和反向代理头正确。
- 所有子服务仅暴露必要端口，管理端口不对公网开放。
- 上传目录、备份目录、日志目录具备容量监控和最小权限。
- 时区统一为 `Asia/Shanghai`，数据库、JVM、容器与浏览器时间一致。
- AI Key、JWT、数据库口令不进入 Git、镜像、前端包和帮助文档。
- 发布前执行单元测试、接口测试、页面冒烟、权限回归和敏感信息扫描。

故障排查顺序

1. 用健康检查确认门户和核心接口是否存活。
2. 检查浏览器网络面板，区分 401、403、404、502 和超时。
3. 核对一次性票据是否过期、是否已被消费、目标服务是否健康。
4. 查看后端日志、网关日志和目标引擎容器日志，使用同一时间与请求 ID 关联。
5. 修复后从真实菜单重新进入，不使用手工拼接的临时地址验证。

版本号 #3
由 Admin 创建于 2026-11-06 00:23:36 UTC
由 Admin 更新于 2026-11-15 08:32:46 UTC