开发与运维
数脉平台用户手册 V2.0 · 开发与运维

总体架构与运行环境
API、鉴权与权限模型
AI 生成看板与样式调整
测试、发布与运维

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。

API、鉴权与权限模型

鉴权流程
用户登录后获得平台会话。访问业务 API
时，前端在受控请求层携带会话令牌；后端验证身份、菜单权限、按钮权限和数据范围。打开嵌入式分析工具时，另行申请短时一次性票据，票据只能用于指定目标页面。

浏览器 → 门户登录 → 会话令牌 → 业务 API
浏览器 → 点击分析菜单 → 后端校验权限 → 一次性票据
浏览器 → 目标系统交换票据 → 建立受控会话 → 打开指定页面

API 约定
项目 约定

基础路径 门户后端统一前缀，按模块分组

请求格式 JSON；文件上传使用 multipart/form-data

响应格式 业务码、消息、数据；分页数据包含 rows 与 total

时间格式 ISO 或统一的 yyyy-MM-dd HH:mm:ss

幂等 创建类接口支持请求号或业务唯一键

分页 pageNum、 pageSize；服务端设置最大页大小

错误码 401 未认证、 403 无权限、 404 不存在、 409 状态冲突、 422
校验失败、 429 限流、 502 下游异常

权限模型
平台权限分四层：

1. 菜单权限 ：控制目录和页面是否可见；不能代替接口鉴权。
2. 按钮权限 ：控制新增、修改、删除、审核、导出、运行等操作。
3. 数据权限 ：按全部、本部门、本部门及以下、本人或自定义部门限定数据范围。
4. 服务端资源权限 ：对数据源、项目、数据集、报表和发布目标分别校验归属与角色。

```
用户 → 角色 → 菜单/按钮/数据范围
用户 → 部门 → 数据范围
用户 → 项目成员 → OWNER / EDITOR / REVIEWER / VIEWER
```

典型接口分组

模块	接口前缀	示例
用户与个人中心	`/system/user`	`/system/user/profile`
角色与部门	`/system/role`、`/system/dept`	`/system/role/{roleId}`
在线会话	`/monitor/online`	列表与强制退出
业务建模	`/bi/bm`	项目、字典、质量、审核、发布
数据治理	`/bi/etl`	调度、同步、加工、外部源、元数据
数据探索	`/bi/superset`	状态检查、受控启动
智能报表	`/bi/jimu`	状态检查、受控启动
AI 对话与分析	`/bi/ai`	会话、方案、确认、样式调整

安全要求

- 所有写接口校验 CSRF/重复提交策略和当前用户权限。
- 文件下载和导出再次校验数据范围，不信任前端传入的查询条件。
- SQL 只读、字段白名单、行数上限、超时与取消机制必须由服务端强制执行。
- 跳转子系统的目标地址从服务端白名单生成，禁止开放任意 URL 重定向。
- 日志不得记录密码、Token、Cookie、API Key、完整 SQL 中的敏感常量和个人联系方式。
- 对 AI 输入做长度与内容限制；对 AI 输出做 JSON Schema 校验和操作白名单校验。

最佳实践

1. 前端权限只用于改善体验，最终授权以后端为准。
2. 对重要业务动作使用二次确认、幂等键和审计事件。
3. 对跨服务错误返回稳定的诊断码，不把下游堆栈和内部地址暴露给浏览器。
4. 对敏感字段采用脱敏视图，原始数据访问单独授权并记录。
5. 接口变更保持向后兼容；废弃字段先标记版本，再逐步移除。

AI 生成看板与样式调整

能力边界
AI 对话分析把自然语言问题转换为经校验的分析方案，再由后端创建 Superset 图表并组合到一个看板中。当前产品约束如下：

单次最多生成 5 张图表，统一进入一个看板。
首次请求先生成方案，用户二次确认后才创建资产。
方案 TTL 为 30 分钟，且一次性消费。
用户问题最多 500 字。
SQL 只读，字段来自白名单，结果行数受限。
支持后续用自然语言调整背景色、图表颜色、文字颜色和字号。
默认模型为 DeepSeek-V4.1-Flash，通过企业模型网关访问。

生成流程

自然语言问题
→ 模型识别业务主题、指标、维度和筛选
→ 方案 JSON 校验
→ 数据集/字段白名单检查
→ 生成只读 SQL
→ 预览影响与图表计划
→ 用户二次确认
→ 创建图表和看板
→ 返回看板链接与操作记录

方案结构示例

{
"title": "华东南亚空调季度经营分析",
"audience": "经营管理层",
"charts": [

```
    {"type": "line", "metric": "销售额", "dimension": "订单月份"},
    {"type": "bar", "metric": "毛利率", "dimension": "产品品类"}
  ],
  "filters": {"region": "华南", "year": 2026},
  "style": {"background": "#071B35", "palette": ["#2A78FF", "#42D3FF"]}
}
```

> 示例仅说明结构，不允许把模型输出直接当作可执行 SQL 或任意配置写入目标系统。

样式调整流程

1. 用户输入“把看板背景改为深蓝，折线图使用青色，标题字号 20”。
2. 模型生成受控样式补丁，只允许颜色、字号、坐标轴和合法图表属性。
3. 服务端校验颜色格式、字号范围和目标图表归属。
4. 返回变更预览；用户确认后应用到指定看板。
5. 保存变更前后的配置快照，记录会话、用户、时间和补丁摘要。

错误与安全

场景	处理
模型超时	返回可重试提示，不重复创建资产
方案过期	提示重新生成方案；一次性 token 不再接受
字段越权	拒绝生成并记录原因，不返回敏感字段元数据
SQL 非只读	编译器拒绝；禁止依赖模型自检
非法颜色 /字号	Schema 校验失败，返回可读错误
重复确认	幂等键阻止重复创建图表

开发检查清单

- 模型网关地址与 API Key 只从环境变量读取。
- 提示词中不包含真实客户明细、密钥或不必要的个人信息。
- 对模型响应使用严格 Schema 校验，禁止“解析失败后直接执行”。
- AI 生成资产必须归属当前用户和项目，支持撤销与审计。

看板创建失败时，清理半成品图表或保持可重试状态。
测试覆盖：空问题、超长问题、越权字段、跨租户、过期方案、重复提交、下游 502、模型限流。

测试、发布与运维

测试分层

层级	重点	典型验证
单元测试	参数校验、权限判断、SQL 编译、样式 Schema	边界值、空值、非法值、幂等
接口测试	鉴权、状态码、事务、审计、错误信息	401/403/404/409/422/502
集成测试	门户票据、Superset 、报表、调度、元数据	免登录跳转、票据过期、服务不可用
端到端测试	用户从菜单进入并完成目标业务	生成多图表看板并调整样式
权限回归	角色、部门、数据集和导出边界	业务用户不能访问管理接口
安全测试	越权、注入、文件上传、敏感信息泄露	白名单、限流、日志脱敏
可用性测试	桌面与移动端、错误提示、加载超时	无横向溢出、可恢复

发布流程

1. 合并前通过静态检查、单元测试和代码评审。
2. 在测试环境执行数据库迁移、配置核对和冒烟测试。
3. 验证所有外部服务健康状态及一次性票据通道。
4. 在变更窗口按依赖顺序发布：数据库 → 后端 → 前端 → 集成配置。
5. 发布后执行登录、菜单、看板、报表、大屏、建模、治理和 AI 核心链路检查。
6. 观察错误率、响应时间和 502 日志；异常时按预案回滚。

运维监控

- 门户后端健康端点与关键接口成功率。
- Superset、JimuReport、GoView、DolphinScheduler、Hop、SeaTunnel、OpenMetadata 容器状态。
- MySQL、Doris、Redis 磁盘、连接、慢查询和内存。
- AI 网关延迟、错误率、限流和模型切换情况。
- 调度失败、质量告警、元数据刷新失败和报表加载失败。

- [illegible]

[illegible]

[illegible]	[illegible]	[illegible]
MySQL	[illegible]	[illegible]
Doris	ODS/DWD/DWS/ADS [illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	Markdown [illegible]	[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- AI [illegible]

[illegible]

502/504[illegible]

401/403[illegible] 401 [illegible] 403 [illegible]

[illegible] **iframe** [illegible] [illegible] `X-Frame-Options/CSP` [illegible]

[illegible] [illegible]

AI [illegible] [illegible] Key [illegible] Key[illegible]