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。

版本号 #2
由 Admin 创建于 2026-11-06 00:23:37 UTC
由 Admin 更新于 2026-11-06 03:53:34 UTC