数据安全与权限测试报告

版本：v6.0

创建日期：2025-10-13

适用环境：dts-stack 本地联调

# 1. 测试背景与目标

本报告聚焦数据权限与安全能力验证，确认平台在 ODS→DW→ADS 全链路对密级字段、角色授权及审计追踪的执行情况。

核心目标：确保不同 person\_security\_level 的账号只能访问与其密级相符的数据集，并对越权操作进行拒绝与审计。

# 2. 测试范围

- 数据层次：ODS 原始日志、DW 主题事实、ADS 公共指标。

- 权限模型：RBAC×ABAC（角色能力×作用域×数据密级）。

- 安全功能：前端登录守卫、后端策略判定、数据脱敏、审计落库、错误码反馈。

# 3. 测试数据

使用 worklog/test.sql 构造的演示仓库：

- ODS 表 ods\_user\_logs：含 10 条原始行为日志，密级分布 PUBLIC→TOP-SECRET。

- DW 表 fact\_user\_events：按用户×商品聚合，保留 data\_secret\_level。

- ADS 表 ads\_daily\_product\_summary：按商品汇总，对维度与事实密级取最大值。

数据口径固定为 2023-10-26，以便对不同角色进行比对测试。

# 4. 角色矩阵

- ROLE\_OP\_ADMIN（person\_security\_level=CORE，active\_scope=INST）：治理管理员，可访问全部密级，具备导出权限。

- ROLE\_DEPT\_EDITOR@D001（person\_security\_level=IMPORTANT，active\_scope=DEPT）：部门编辑，仅能访问本部门、密级≤INTERNAL 的数据。

- ROLE\_USER（person\_security\_level=GENERAL，active\_scope=INST）：普通用户，仅能访问 share\_scope=PUBLIC\_INST、密级=PUBLIC 的 ADS 统计。

- 非授权主体：匿名访问、平台未允许角色（如 ROLE\_SYS\_ADMIN）须被前端守卫拦截。

# 5. 测试环境

- 应用版本：dts-platform / dts-admin 0.0.1-SNAPSHOT。

- 前端：React 19 + Vite SPA。

- 服务编排：Docker Compose（Traefik、Keycloak、PostgreSQL、Trino）。

- 关键配置：VITE\_ENABLE\_FE\_GUARD=true；DTS\_COMMON\_AUDIT\_ENABLED=true；数据字典包含 PUBLIC/INTERNAL/SECRET/TOP-SECRET。

# 6. 测试方法

采用脚本注入 + 前端界面 + 后端 API 组合验证：

1) 通过 SQL/HTTP 工具模拟各角色会话，设置 active\_scope/active\_dept 请求头。

2) 执行标准查询（ADS 指标、DW 事实、ODS 明细）与导出动作。

3) 构造越权场景（跨部门、跨密级、匿名访问）验证错误码。

4) 检查审计表 event\_type、operator\_roles、data\_level 等字段是否记录完整。

# 7. 角色视角验证

## 7.1 ROLE\_OP\_ADMIN

- 进入平台后可见全部菜单，active\_scope=INST。

- 执行 `SELECT \* FROM ads\_daily\_product\_summary WHERE product\_id='prod105';`：成功返回 TOP-SECRET 数据。

- 导出 `fact\_user\_events` prod105 记录：成功，AuditEvent 记录 DATA\_EXPORT，details.data\_level=TOP-SECRET。

- 访问 ODS 明细：经授权允许读取原始日志。

## 7.2 ROLE\_DEPT\_EDITOR@D001

- 仅展示与部门相关的菜单。

- 查询 `ads\_daily\_product\_summary` 时仅返回密级≤INTERNAL 的商品，prod105 被过滤。

- 执行 `SELECT \* FROM fact\_user\_events WHERE product\_id='prod104';`：成功返回智能手表数据（密级 INTERNAL）。

- 尝试查询 prod105：返回 403，错误码 dts-sec-0003。

- 导出 prod104 结果：成功，审计标记“脱敏导出”，文件仅含允许字段。

## 7.3 ROLE\_USER

- 登录后仅保留“公共指标”导航。

- 调用 `GET /api/ads/product/top`：仅返回密级 PUBLIC 商品（智能手机X 等），prod105 自动隐藏。

- 尝试访问 SQL 工作台：接口返回 403，错误码 dts-sec-0001。

- 切换 active\_scope=DEPT：接口返回 400 dts-sec-0006（普通用户无部门上下文）。

## 7.4 未授权访问

- 匿名请求 `/api/menu`：被 401 拦截。

- ROLE\_SYS\_ADMIN 登录平台：前端守卫拒绝，提示“您无权登录该系统”。

# 8. 审计与日志核对

- AdminAuditService/AuditTrailService 均记录 DATA\_QUERY、DATA\_EXPORT、DATA\_ACCESS\_DENY 事件。

- 验证 record\_signature 与 chain\_signature 自增，确保链式完整。

- 关联 request\_id：ODS→DW→ADS 同一任务可串联，便于追踪数据来源。

# 9. 权限边界测试结果

- 密级控制：所有角色均遵守 personnel\_level ≥ data\_level，越权场景返回 dts-sec-0003。

- 作用域控制：active\_scope=DEPT 时访问非本部门数据触发 dts-sec-0002。

- 前端守卫：阻止未授权角色进入平台 UI，减少误操作面。

- 导出能力：仅 CORE/IMPORTANT 级别角色成功导出，且文件内容符合脱敏策略。

# 10. 已知风险与改进建议

- PKI 登录仍待落地，证书身份尚未写入 Token claims，需防止绕过密级判定。

- 历史 ODS 表可能缺失 data\_level 字段，建议补齐或设置默认密级。

- SQL 工作台导出缺少明确密级提示，建议增加二次确认。

- 建议引入自动化用例覆盖更多角色组合（如 INST\_VIEWER、临时授权用户）。

# 11. 结论

当前版本在角色区分、密级校验及审计串联方面符合安全策略要求，核心风险集中在 PKI 登录与历史数据补齐，需在后续迭代中解决。



