数据生命周期测试报告

版本：v2.0

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

本报告总结数据从外部数据源进入平台，经过清洗建模直至 ADS 服务层发布的完整生命周期测试情况。

测试目标：验证数据密级在各层级贯通，确保基于 person\_security\_level 的访问控制符合 RBAC×ABAC 策略。

# 2. 测试范围与对象

数据链路：ODS 原始分层 → DW 主题分层 → ADS 服务分层。

关键系统组件：

- 数据源接入服务（Source Ingestion）：负责采集外部库表并写入 ODS，记录 source\_system、ingest\_time。

- 数据开发服务（DW 层）：依据治理规则清洗转换，并统一补齐 data\_level、owner\_dept、share\_scope。

- 数据服务与分析（ADS 层）：向业务前端提供受控 API/指标，走统一权限与审计流程。

- 身份与权限：Keycloak 携带 dept\_code、person\_security\_level、roles\_scoped，平台后端执行策略判定。

# 3. 测试环境

- 平台版本：dts-platform / dts-admin 0.0.1-SNAPSHOT（Spring Boot 3.4.5）。

- 前端版本：dts-platform-webapp / dts-admin-webapp React 19 + Vite。

- 部署方式：Docker Compose 本地模式，启用 Traefik 代理、Keycloak、PostgreSQL。

- 配置关键点：DTS\_COMMON\_AUDIT\_ENABLED=true，VITE\_ENABLE\_FE\_GUARD=true，数据密级字典 PUBLIC/INTERNAL/SECRET/TOP\_SECRET。

# 4. 角色与权限模型

- ROLE\_OP\_ADMIN（person\_security\_level=CORE）：可访问全部密级与跨部门数据，负责治理与审批。

- ROLE\_USER（person\_security\_level=GENERAL）：仅能访问 share\_scope=PUBLIC\_INST 的 ADS 数据集。

- ROLE\_DEPT\_EDITOR / ROLE\_DEPT\_VIEWER：当 active\_scope=DEPT 时仅能访问 owner\_dept=本部门、data\_level ≤ personnel\_level 的数据。

- 管理端角色（ROLE\_SYS\_ADMIN / ROLE\_AUTH\_ADMIN / ROLE\_SECURITY\_AUDITOR）仅在 dts-admin 内生效，平台前端拒绝登录。

- 统一错误码：dts-sec-0001（RBAC\_DENY）、dts-sec-0002（SCOPE\_MISMATCH）、dts-sec-0003（LEVEL\_TOO\_LOW）用于策略反馈。

# 5. 测试用例与结果

## 5.1 ODS 数据源接入

- 步骤：通过接入向导导入外部库 sales\_ods 的交易与客户表，开启 source\_metadata 记录。

- 断言：ODS 表新增 source\_system、ingest\_time、raw\_payload 列，审计日志产生 DATA\_INGEST\_START/DATA\_INGEST\_FINISH 事件。

- 结果：符合预期；ROLE\_OP\_ADMIN 在 admin 审计中心可检索到事件并包含 operator\_roles、org\_code。

## 5.2 DW 层清洗与密级标注

- 步骤：使用 DW 任务编排构建主题表 dw\_sales\_order，聚合客户信息并计算敏感字段。

- 断言：所有新产出字段写入 data\_level=SECRET，owner\_dept=INST-DATA，share\_scope=SHARE\_INST。

- 结果：Liquibase 元数据与数据探查均显示密级字段存在，未经授权角色访问返回 dts-sec-0003。

## 5.3 ADS 层授权与查询

- 步骤：将 dw\_sales\_order 发布为 ads\_sales\_summary 指标集，配置 ROLE\_USER 仅可读 share\_scope=PUBLIC\_INST 视图。

- 断言：ROLE\_OP\_ADMIN 登录平台后在活动作用域 INST 下可见全部指标；ROLE\_USER 仅能访问脱敏列。

- 结果：前端根据 menuService 返回的可见性加载导航，后台根据 person\_security\_level 执行数据过滤并写入审计。

## 5.4 数据分析与导出

- 步骤：ROLE\_DEPT\_EDITOR 切换 active\_scope=DEPT，执行 SQL 工作台查询 ADS 指标并导出 CSV。

- 断言：跨部门数据触发 dts-sec-0002 拒绝；合法导出生成 AuditEvent event\_type=DATA\_EXPORT，details 包含 target\_table 与 param\_digest。

- 结果：验证通过，导出文件仅包含 owner\_dept=本部门且 data\_level ≤ personnel\_level 的记录。

# 6. 问题与风险

- PKI 登录仍为占位，后端尚未将证书身份映射到 Token，后续需要补齐与 person\_security\_level 的一致性校验。

- 少量历史 ODS 表缺失 data\_level 字段，需在迁移脚本中统一补齐以避免 dts-sec-0009。

- SQL 工作台对自定义导出暂未强制附加密级提示，建议增加操作提醒。

# 7. 后续建议

- 将 ADS 指标发布流程与审批节点绑定，确保 share\_scope 扩大时触发审计与通知。

- 按月核对 Keycloak person\_security\_level 与 dts-admin 用户档案，避免密级漂移。

- 推进审计日志分区与全文索引，实现跨层 trace，支撑数据安全检查。

# 8. 截图清单

- 截图1：数据源接入向导（展示源配置与校验结果）。

- 截图2：DW 任务编排监控页（包含任务 DAG 与执行日志）。

- 截图3：平台前端基于角色的菜单示例（ROLE\_OP\_ADMIN vs ROLE\_USER）。

- 截图4：审计中心查询导出事件明细。

（请在最终稿中插入对应截图或使用占位图片，以便交付物完整。）