

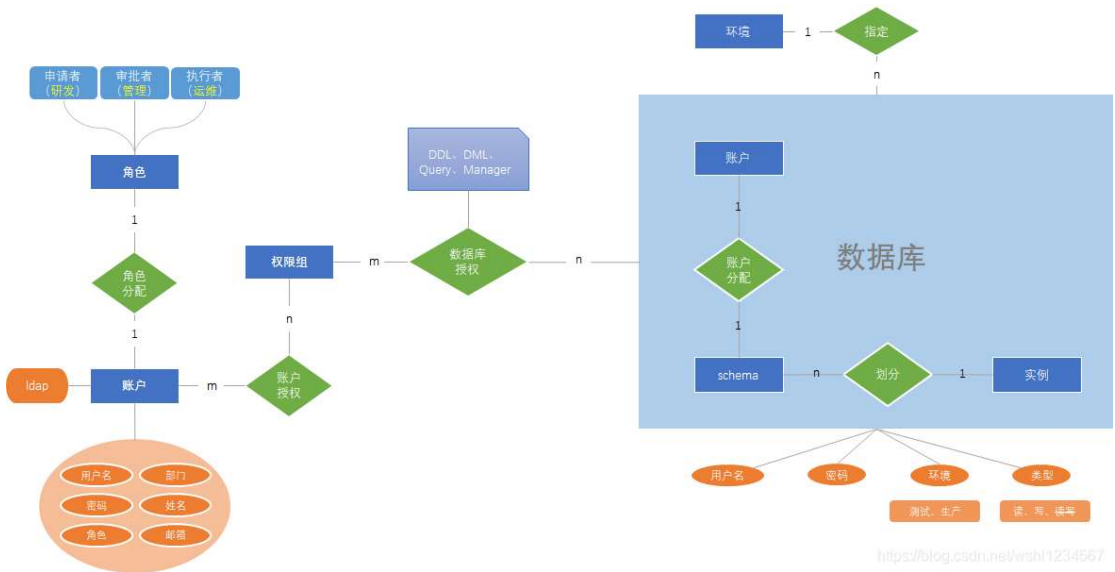
山东万维 SQL 运维审计系统设计方案

1. 项目背景

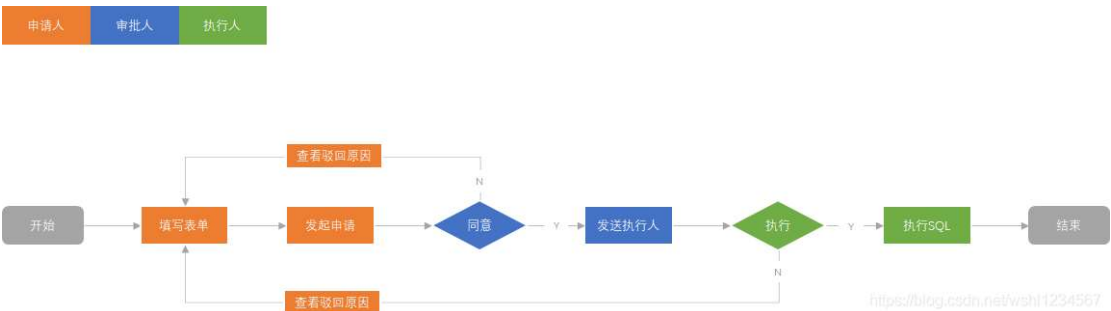
为了满足山东万维网络工程有限公司服务运营管理系统升级迭代中对频繁使用的 SQL 语言设计的是否满足合规性，SQL 语句语法检测，查询结果是否脱敏的需求，需要开发一个 SQL 审核需求的 web 端可视化 SQL 审核平台，实现常规的 sql 审核功能，实现数据查询等一系列便捷的功能，以提高运营管理系统开发工作效率，保证 SQL 语句语法的合规性。

2. 设计原型

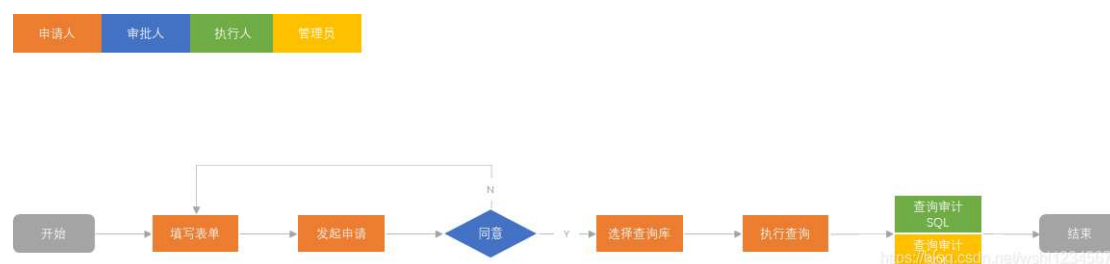
系统 RR 图：



DDL/DML审核流程（多级审核）：



查询审核:



3. 模块设计方案

一、用户模块

1、dashboard

dashboard 主要展示各项数据包括用户数/数据源数/工单数/查询数以及其他图表, 个人信息栏内用户可以修改密码/邮箱/真实姓名, 同时可以查看该用户权限以及申请权限。

2、我的工单

展示用户提交的工单信息, 对于执行失败/驳回的工单点击详细信息后可以重新修改 sql 并提交, 对于执行成功的工单可以查看回滚语句并且快速提交 SQL

3、工单-DDL

具有以下功能:

- 1) DDL 相关 SQL 提交审核
- 2) 查看表结构/索引
- 3) SQL 语法高亮/自动补全

如果想获取表结构详细信息, 必须选填表名并完整填写工单信息。所有的 SQL 只有在检测后错误等级为 0 时提交按钮才会激活, 如下拉列表框内没有相关数据源显示请联系管理员是否赋予相应数据源权限。

4、工单--DML

具备以下功能:

- 1) DML 相关 SQL 提交审核
- 2) SQL 语法高亮/自动补全

所有的 SQL 只有在检测后错误等级为 0 时提交按钮才会激活,如下拉列表框内没有相关数据源显示请联系管理员是否赋予相应数据源权限。

5、查询

具备以下功能:

- 1) 查询/导出数据
- 2) SQL 语法高亮/自动补全
- 3) 快速 DML 语句提交

如果开启查询审核,提交该查询申请后需对应审核人同意后方可查询,超级管理员在设置页面开启数据导出功能后,查询申请页面才会显示数据导出按钮(默认为.csv 格式),获取表结构功能必须点击相应表名此为前置条件,快速提交功能仅支持 DML 语句,如下拉列表框内没有相关数据源显示请联系管理员是否赋予相应数据源权限。

二、审核模块

1、工单审核

功能: DDL/DML 管理员审核并执行

实时刷新开关默认打开,如需删除记录请先关闭该开关。如定时工单的时间小于当前时间,执行该工单将会立即执行,目前仅支持延时工单中止,其他工单执行后无法中止!

2、查询审核

功能: 用户查询审核

点击全部中止按钮将会中止所有用户的查询权限 如没有在设置页面开启查询审核开关,则默认用户查询申请提交后自动获得查询权限。 用户查询时限在设置页面进行设置

3、权限审核

功能: 用户权限审核

权限由用户在首页个人信息处自主申请,管理员可在该审核页面决定是否给予用户申请的权限,由于用户可能存在胡乱申请权限的问题,所以管理员在查看用户权限申请工单的同时可对工单申请的权限进行修改,确定具体的权限给予。

三、记录

1、工单审计

主要是审计工单的执行情况，记录工单的执行时间、申请人、执行人等信息。

2、查询审计

针对数据库查询记录做审计

四、管理员模块

1、用户

功能：创建/修改/删除用户

当多级审核关闭后系统并不会自动将角色为执行人的用户重置角色，需要自行重置相应用户角色

2、数据库

功能：添加/编辑/删除 数据源

所有添加的数据源应在添加之前点击测试连接按钮进行连接性测试，保证连接性。

数据源分为查询数据源/非查询数据源。查询数据源仅会出现在细粒度权限的查询数据源范围内。非查询数据源同理。（对于查询与执行数据源应拆分为二，保障线上执行数据源不会因为查询慢 sql 影响业务），此类别添加后无法通过编辑进行修改，需要慎重添加。

3、用户权限

功能：用户权限修改/清空

批量赋权仅支持角色为使用人的用户。由于批量赋权为覆盖更新，仅适合在用户权限为空时使用。

4、设置

功能：

1) 设置消息推送相关信息 包括钉钉机器人/email

2) 设置 LDAP 相关信息

3) 进阶设置—全局配置信息，全局配置开关

在配置填写无误后点击测试按钮进行相关测试，使用消息推送前必须先打开对应消息推送开关，否则 Yearning 不会进行推送

5、审核规则

功能:设置 SQL 检测规则

保存后即时生效

1. 数值型规则 0 值都为不受限制。
2. 开启检查时间字段默认值, 所有时间类型字段都必须设置默认值且默认值必须为 CURRENT_TIMESTAMP
3. osc 相关规则请参考相关工具参数说明。
4. 受制于各种条件影响, 影响行数判断并不一定准确, 走主键及索引的语句会提交准确性, 仅作为部分参考, 如预测结果偏移量较大。可考虑语句性能是否存在可优化空间或提高影响行数上限
5. OSCMinTableSize 当表体积大于该值时如果启动 osc 则走 osc 执行。
6. 排序/字符集/建表必须拥有字段设置 请使用逗号分隔多个值