DTCC 2010-2022

第十三届中国数据库技术大会

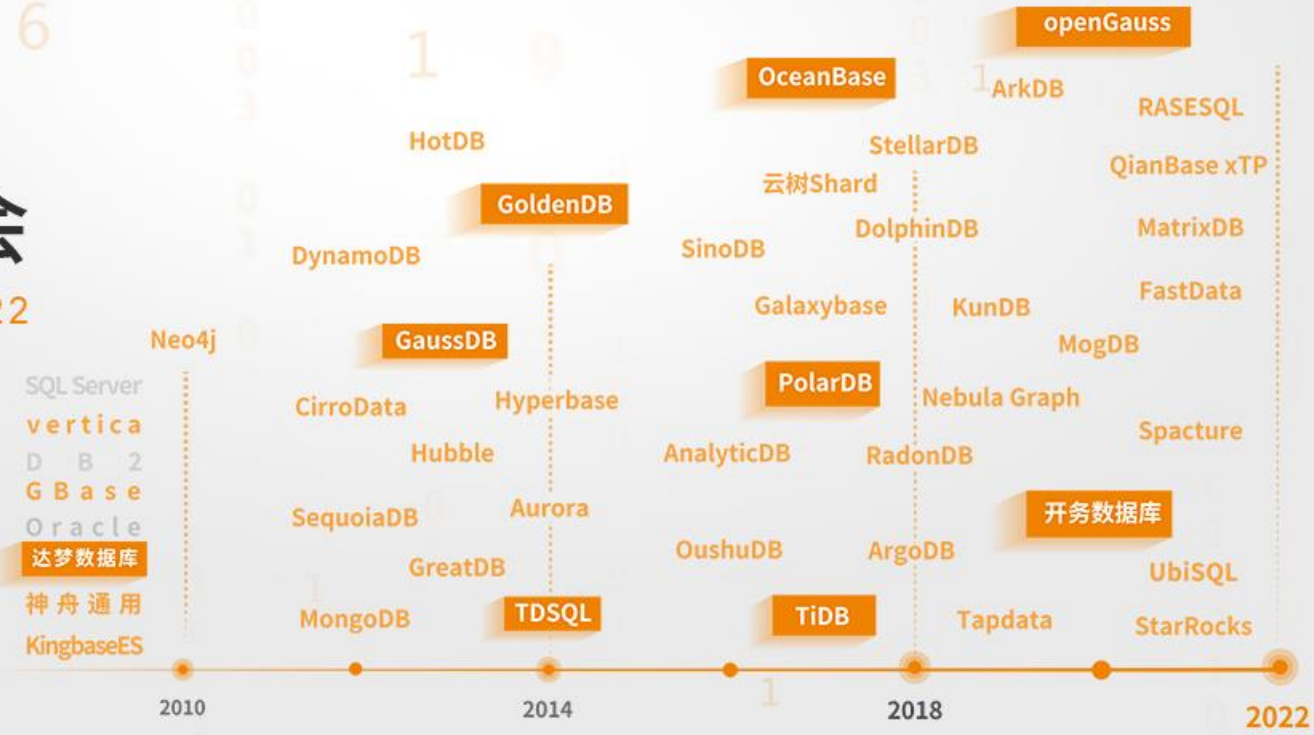
DATABASE TECHNOLOGY CONFERENCE CHINA 2022

数据智能 价值创新

IT168.com ChinaUnix.net ITPUB

线上直播 | 2022/12/14-16

数据来源：数据库产品上市商用时间



加码数据安全，微盟数据安全落地方案

余成真+微盟集团+DBA负责人

大家好，我是余成真，2016年入职微盟，微盟数据库高级技术专家，目前担任技术平台-运维部-数据库团队负责人；有多年的数据库产品管理和技术规划经验，目前负责微盟数据库团队管理及建设、数据库相关的业务保障、数据库技术决策；在微盟工作经历中主导海量实例跨IDC迁移、自建集群到云数据库迁移等迁移工作；组建并带领团队完成数据库产品从0到1，从1到N的跨越；深度参与同城双活/异地多活数据库整体架构及数据同步方案的设计及实施。

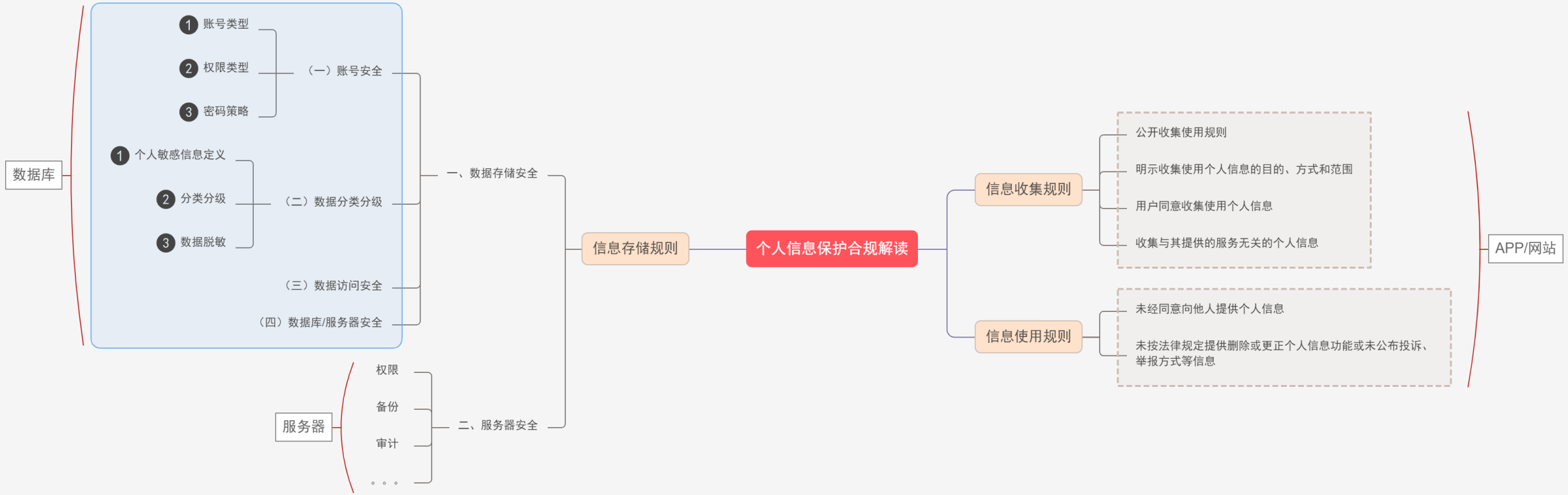
专业技能上：专注于数据库的高性能和高可用技术保障，负责数据库架构设计、数据库运维平台的自动化建设、数据库运维体系规范建设。

个人能力上：具备危机处理能力、具备多人组织动员能力、具有很强的判断与决策、计划和执行能力。

监管矩阵

监控部门	网信办	公安部	市场监督总局	工信部	中国人民银行
部门名称	CNCERT、各地技术支撑单位	各省市网安、公安、CNNAC（国家移动互联网应用安全管理中心）	CCRC、消协、质监局	各地通管局、赛迪研究院、泰尔实验室、信通院等	银保监会、证监会
适用行业	全行业适用	全行业适用	全行业适用	全行业适用	金融行业适用
监管手段	红头文件、约谈、下架处置	上门检查（以网安法为依据处罚）、通报	公开媒体通报	红头文件、社会通报、下架处置	发标准、做认证、抽查、通报
监管强度	**强**	较弱	较弱	**强**	较强
监管标准	191认定方法2-4个隐私合规问题	公安网安类（2-4个隐私合规问题，2-4个高危漏洞）	191认定方法	164号文2-4个隐私合规问题	191认定方法、164JR/T0171—2020

合规解读


个人信息保护合规解读
信息存储规则
一、数据存储安全
（一）账号安全
1 账号类型
2 权限类型
3 密码策略
（二）数据分类分级
1 个人敏感信息定义
2 分类分级
3 数据脱敏
（三）数据访问安全
（四）数据库/服务器安全
数据库
二、服务器安全
权限
备份
审计
。。。
服务器
信息收集规则
公开收集使用规则
明示收集使用个人信息的目的、方式和范围
用户同意收集使用个人信息
收集与其提供的服务无关的个人信息
信息使用规则
未经同意向他人提供个人信息
未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息
APP/网站

目录

一、数据库账号权限治理

账号归类

按角色

- 研发
- DBA

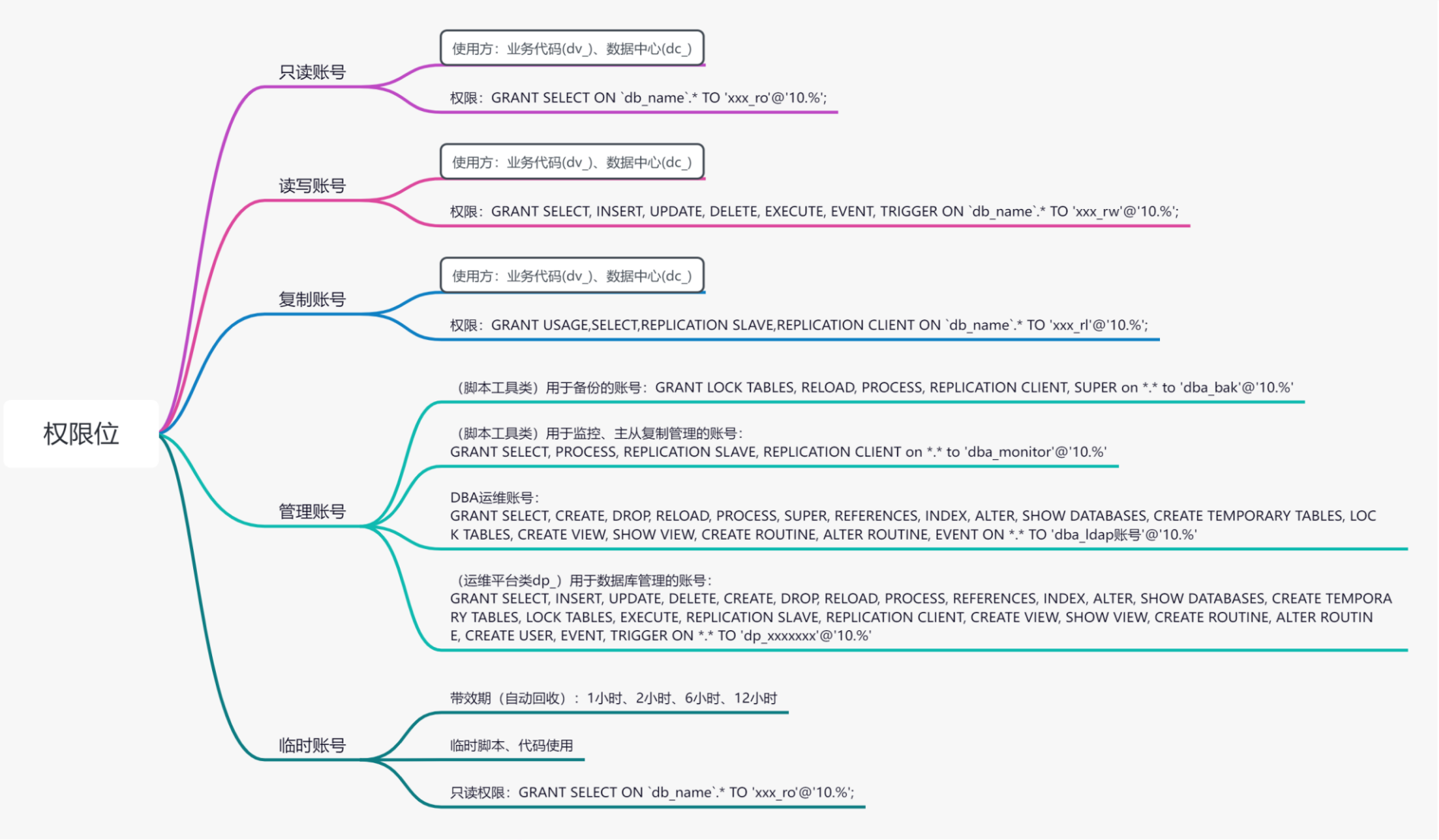
按使用方

- 业务
  - 建立实例与应用关系
  - 账号无DDL权限
- 数据中心
  - 只读权限
  - Binlog复制权限
  - 对业务方实例无DDL权限
- 运维平台
  - DDL/DML权限
  - 部分管理权限
  - 权限低于root
- DBA运维
  - 账号到人
  - 随用随建，用完销毁
  - 无DML权限

按权限

- 只读账号
- 读写账号
- 复制账号
- 管理账号
- 临时账号

账号权限体系


权限位
只读账号
使用方：业务代码(dv_)、数据中心(dc_)
权限：GRANT SELECT ON `db_name`.* TO 'xxx_ro'@'10.%';
读写账号
使用方：业务代码(dv_)、数据中心(dc_)
权限：GRANT SELECT, INSERT, UPDATE, DELETE, EXECUTE, EVENT, TRIGGER ON `db_name`.* TO 'xxx_rw'@'10.%';
复制账号
使用方：业务代码(dv_)、数据中心(dc_)
权限：GRANT USAGE,SELECT,REPLICATION SLAVE,REPLICATION CLIENT ON `db_name`.* TO 'xxx_rl'@'10.%';
管理账号
（脚本工具类）用于备份的账号：GRANT LOCK TABLES, RELOAD, PROCESS, REPLICATION CLIENT, SUPER on *.* to 'dba_bak'@'10.%'
（脚本工具类）用于监控、主从复制管理的账号：
GRANT SELECT, PROCESS, REPLICATION SLAVE, REPLICATION CLIENT on *.* to 'dba_monitor'@'10.%'
DBA运维账号：
GRANT SELECT, CREATE, DROP, RELOAD, PROCESS, SUPER, REFERENCES, INDEX, ALTER, SHOW DATABASES, CREATE TEMPORARY TABLES, LOCK TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT ON *.* TO 'dba_ldap账号'@'10.%'
（运维平台类dp_）用于数据库管理的账号：
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, REPLICATION SLAVE, REPLICATION CLIENT, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, EVENT, TRIGGER ON *.* TO 'dp_xxxxxxx'@'10.%'
临时账号
带效期（自动回收）：1小时、2小时、6小时、12小时
临时脚本、代码使用
只读权限：GRANT SELECT ON `db_name`.* TO 'xxx_ro'@'10.%';

账密安全使用管理

1.0

明文配置

- 下发明文账密，研发自主配置

2.0

一代加密(AES)

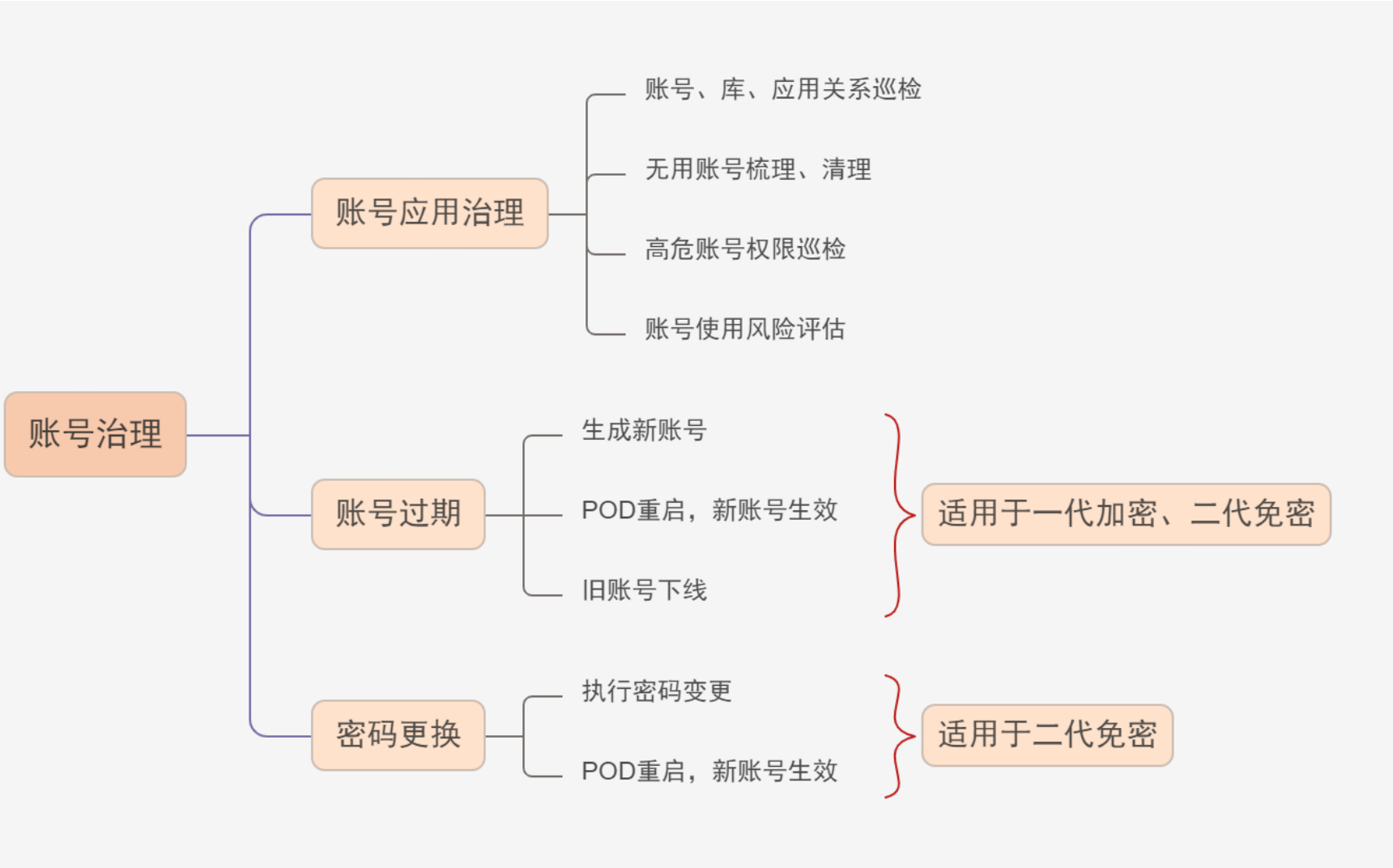
- 根据实例与应用关系，生成AES私钥文件，并保存至特定目录。
- 应用通过Apollo配置数据库连接信息（密文密码）。
- 启动应用时，通过私钥文件解密，应用启动成功。

3.0

二代免密（账密替换）

- 根据实例与应用关系、业务数据库与应用关系，生成应用维度的数据库账号。
- 账号注册至woauth账号中心，woauth对外暴露账密。
- Apollo配置业务数据库占位符
- 应用启动时上报信息至woauth服务，鉴权并推送账密，由应用端agent替换占位符，应用启动成功。

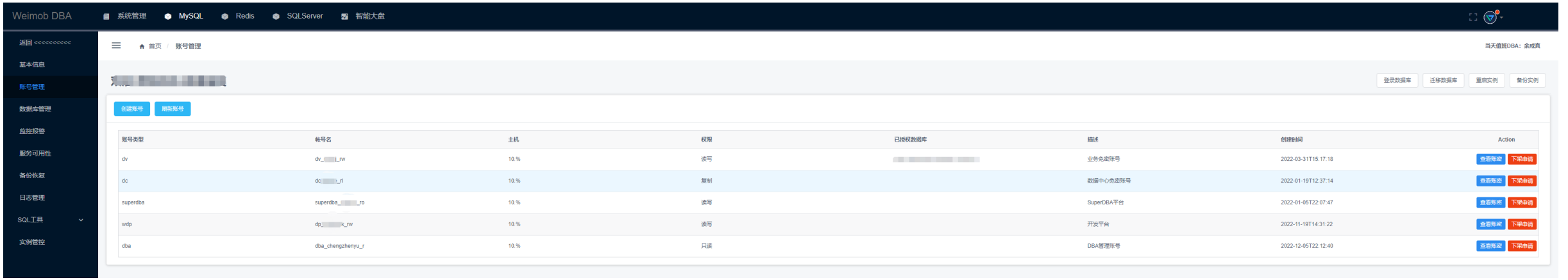
账号治理



符合国家标准
通过安全审计

平台功能支撑


MySQL权限
* 权限类型: ep隐匿账号 数据中心任务隐匿账号
* 实例域名: 请选择
* 数据库权限: 读写权限 只读权限 复制权限
请输入数据库名，按回车键搜索...
数据库名
应用名
该账号未绑定数据库


Weimob DBA
系统管理
MySQL
Redis
SQLServer
智能大盘
返回 <<<<<<<<<<
基本信息
账号管理
数据库管理
监控报警
服务可用性
备份恢复
日志管理
SQL工具
实例管控
首页 / 账号管理
当天值班DBA：余成真
登录数据库
迁移数据库
重启实例
备份实例
创建账号
刷新账号
账号类型
帐号名
主机
权限
已授权数据库
描述
创建时间
Action
dv
读写
业务免密账号
2022-03-31T15:17:18
查看账密
下架申请
dc
复制
数据中心免密账号
2022-01-19T12:37:14
superdba
读写
SuperDBA平台
2022-01-05T22:07:47
wdp
读写
开发平台
2022-11-19T14:31:22
dba
dba_chengzhenyu_r
只读
DBA管理账号
2022-12-05T22:12:40

二、数据分类分级、数据加密及脱敏

分类分级

哪些数据要分类分级？

分级定义

微盟4级：• 仅在数据归属部门内使用的信息，不允许开放共享的数据 • 法律法规等要求不允许泄露的信息 • 数据未经授权披露、丢失、滥用、篡改或销毁后对国家安全、企业利益或公民权益会造成严重危害

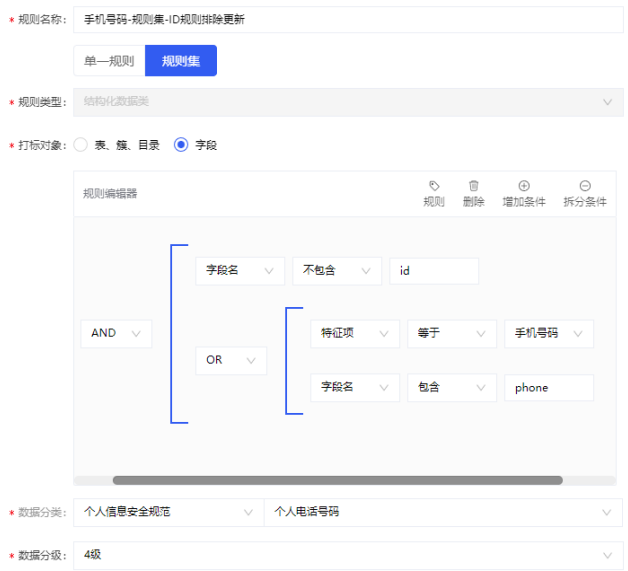
数据扫描

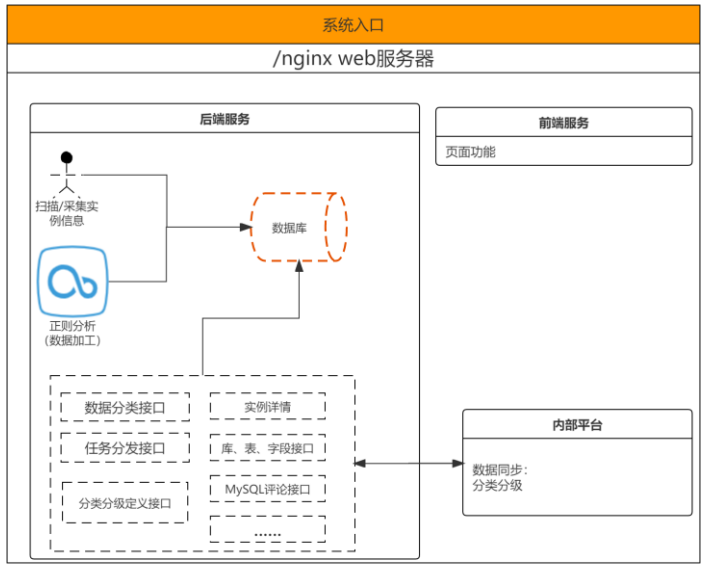
方法：正则

数据扫描

表结构

表数据





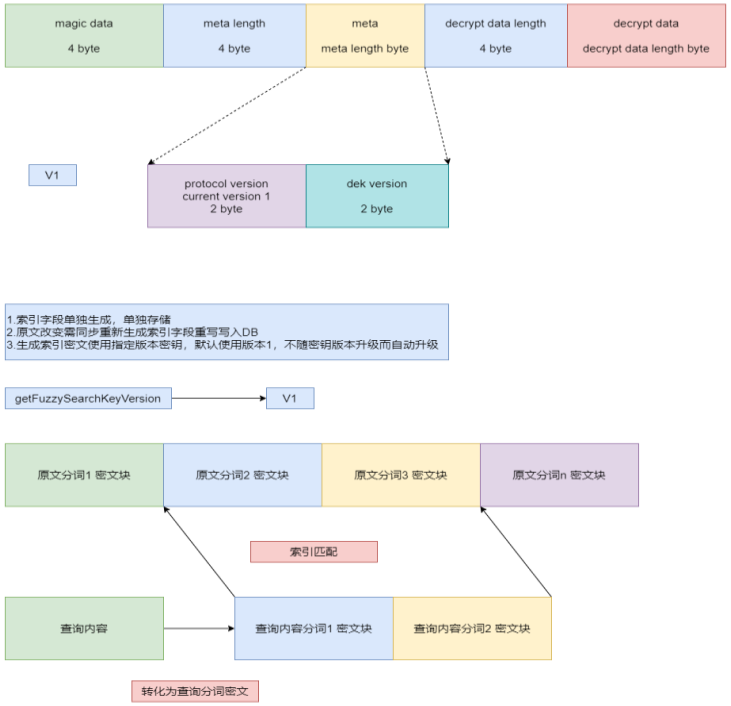
分类分级

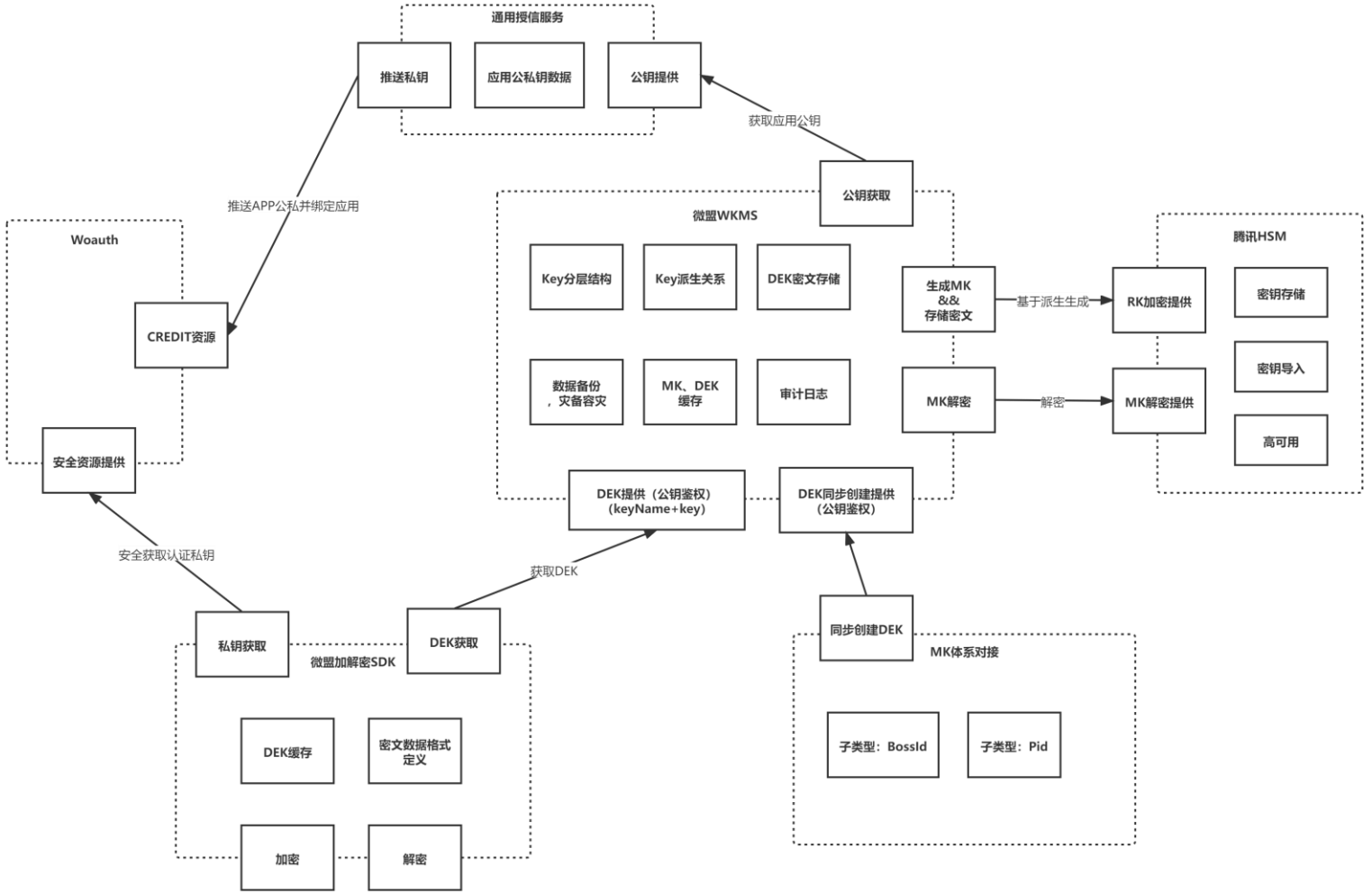

分级标签列表
分级名称
权重下限
权重上限
+ 添加
删 除
分级名称
分级权重值
规则数量
分级说明
建议管控策略
操作
非敏感数据 0 0 - - 编辑 | 删除
1级 1 0 • 不会对国家安全、企业利益或公民权益造成不利影响的数据 - 编辑 | 删除
2级 2 0 • 要求采取特殊防范措施，避免未授权的修改或删除，从而保证数据的完整性与机密... - 编辑 | 删除
3级 3 5 • 仅在数据归属部门内使用的信息，不允许开放共享的数据 • 数据未经授权披露、丢... - 编辑 | 删除
4级 4 7 • 仅在数据归属部门内使用的信息，不允许开放共享的数据 • 法律法规等要求不允许... - 编辑 | 删除
共5条
1
15 条/页
数据源分布
类型
资产目录
隶属部门
Mysql 100.00%
资产分类
分类维度： 全部
个人电话号码
个人姓名
住址
电子邮箱
精准定位信息
身份证
IP地址
护照
银行账号
资产分级
4级 73.71%
3级 13.19%
非敏感数据 10.19%
2级 2.91%
1级 0.00%
数据识别概览
分类标签数 101
0.02%
分类覆盖率
数据表
数据字段
文件数
分级标签数 5
0.05%
分级覆盖率
数据表
数据字段
文件数

加密与脱敏

加密与脱敏

姓名	手机号	组织 | 角色
	该信息涉及用户隐私，管理员可在账号权限中设置脱敏规则。 0086-181*******7	微商城 | 超级管理员、…
金*媛	0086-187*******2	微商城 | 超级管理员、…
杨*鹏	0086-158*******5	微商城 | 超级管理员、…





三、数据库平台安全管控

安全目标

平台安全管控**目标**：最小权限分配原则

授权范围

资源只给对应的租户（业务团队）使用。

隔离策略

租户（业务团队）间信息相互隔离

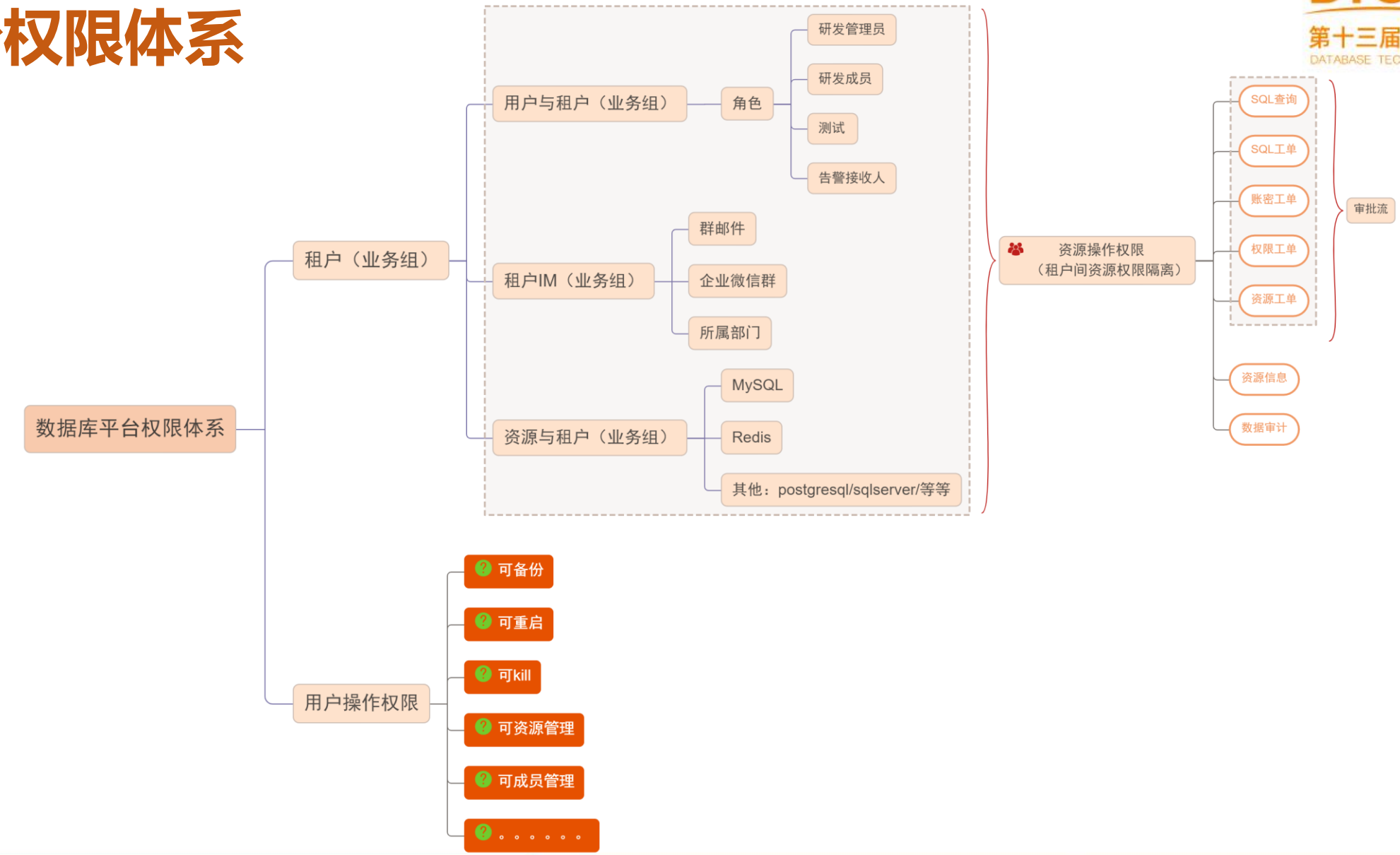
信息互通

业务团队（租户）内所有信息共享：工单、资源监控、告警/慢日志推送等等。

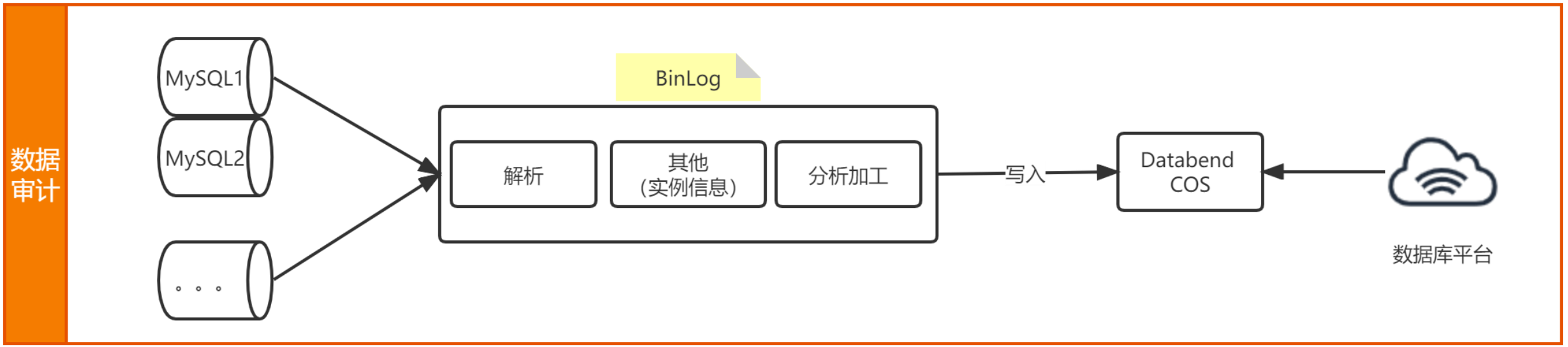
可审计

数据库DML审计日志。
平台操作审计日志：
人在什么时间看了什么数据
实例被什么人在什么时间查看

平台权限体系



数据审计



数据审计

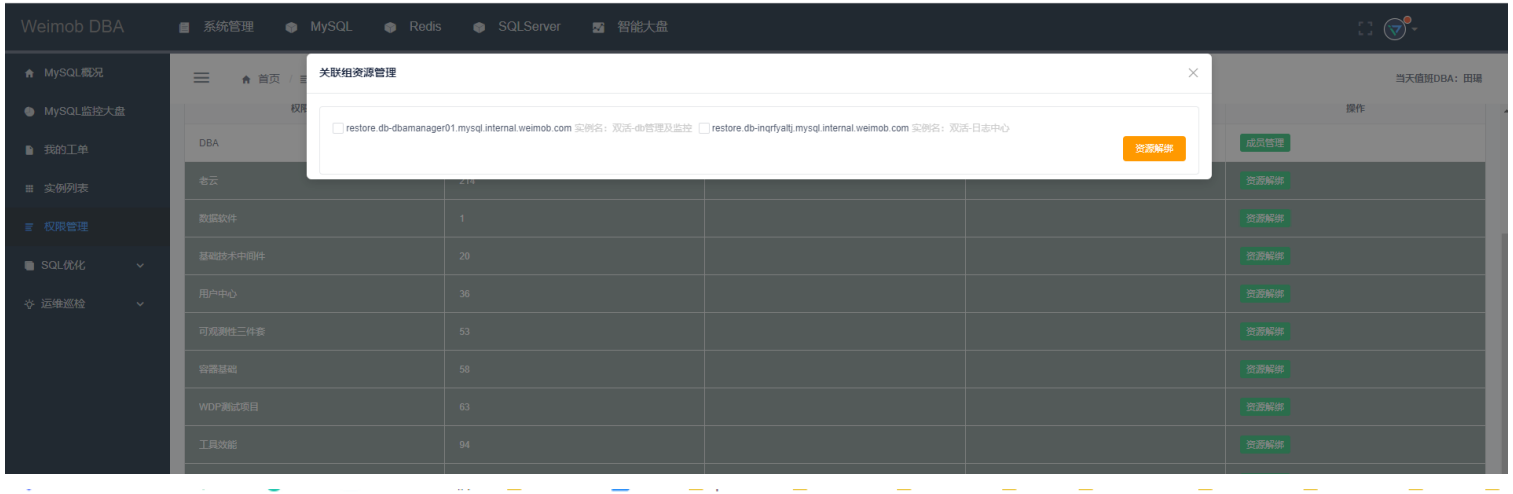
- 高危命令治理/审计：delete、drop
- 业务操作数据的变更审计
- 数据快照能力
- 在线事务、长事务分析
- 数据操作地图：频繁被修改的表

平台权限体系--功能实现

用户细粒度操作权限

- 具体到实例的操作权限
- 不同的实例不同操作权限

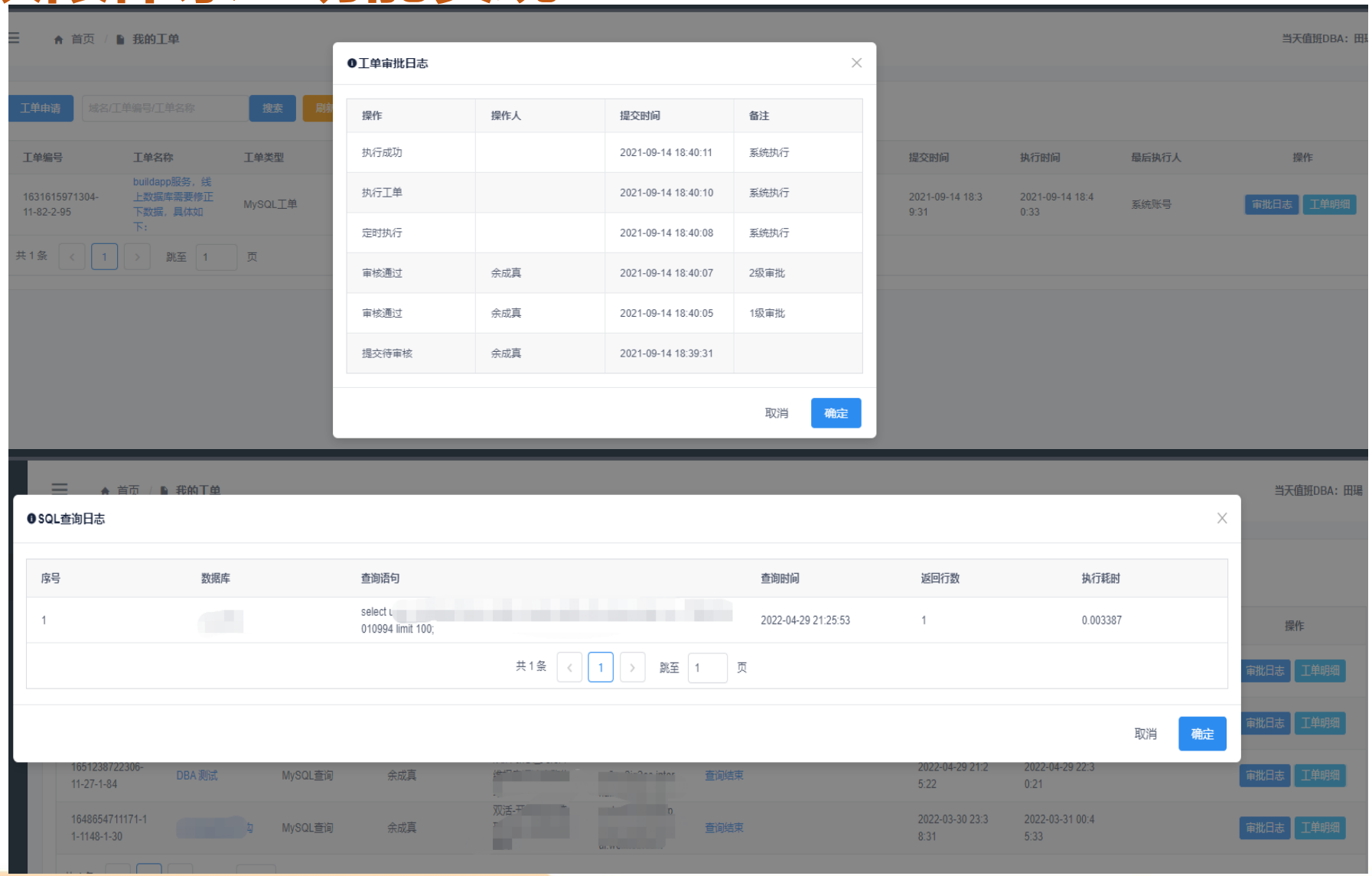
平台权限体系--功能实现



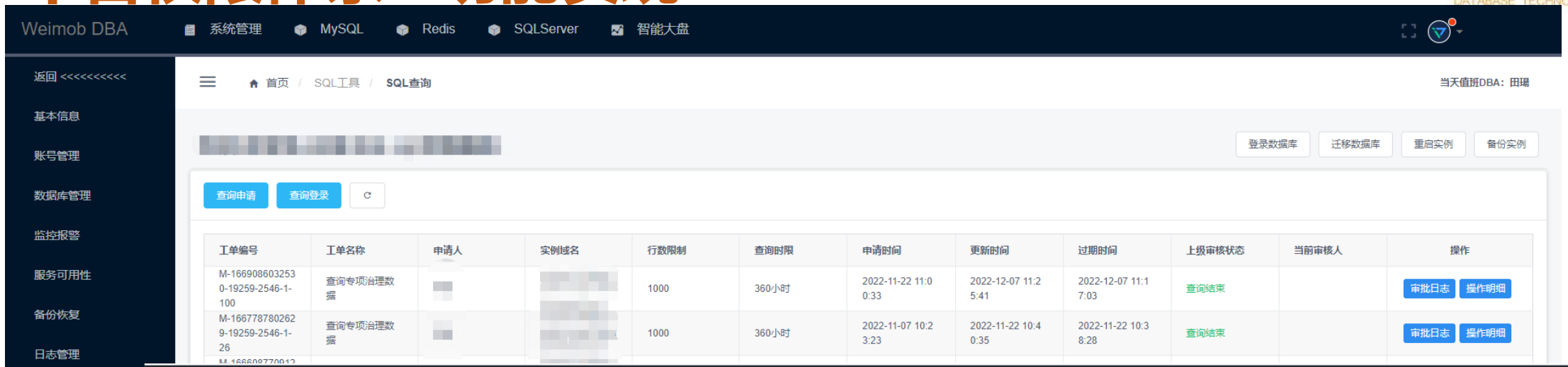
租户（业务组）对资源的管理：控制租户能操作的资源

租户（业务组）下，成员操作记录共享、信息共享、互相审计

平台权限体系--功能实现


首页 / 我的工单
当天值班DBA：田瑞
工单申请
域名/工单编号/工单名称
搜索
工单编号
工单名称
工单类型
提交时间
执行时间
最后执行人
操作
1631615971304-11-82-2-95
buildapp服务，线上数据库需要修正下数据，具体如下：
MySQL工单
2021-09-14 18:39:31
2021-09-14 18:40:33
系统账号
审批日志
工单明细
共 1 条
跳至 1 页
工单审批日志
操作
操作人
提交时间
备注
执行成功
2021-09-14 18:40:11
系统执行
执行工单
2021-09-14 18:40:10
定时执行
2021-09-14 18:40:08
审核通过
余成真
2021-09-14 18:40:07
2级审批
2021-09-14 18:40:05
1级审批
提交待审核
2021-09-14 18:39:31
取消
确定
SQL查询日志
序号
数据库
查询语句
查询时间
返回行数
执行耗时
1
select
010994 limit 100;
2022-04-29 21:25:53
1
0.003387
共 1 条
跳至 1 页
1651238722306-11-27-1-84
DBA 测试
MySQL查询
余成真
查询结束
2022-04-29 21:25:22
2022-04-29 22:30:21
1648654711171-11-1148-1-30
2022-03-30 23:38:31
2022-03-31 00:45:33

平台权限体系--功能实现


Weimob DBA
系统管理
MySQL
Redis
SQLServer
智能大盘
返回 <<<<<<<<<<
基本信息
账号管理
数据库管理
监控报警
服务可用性
备份恢复
日志管理
SQL工具
SQL查询
SQL工单
SQL优化
实例管控
首页 / SQL工具 / SQL查询
当天值班DBA：田瑞
登录数据库
迁移数据库
重启实例
备份实例
查询申请
查询登录
工单编号
工单名称
申请人
实例域名
行数限制
查询时限
申请时间
更新时间
过期时间
上级审核状态
当前审核人
操作
M-166908603253 0-19259-2546-1-100
查询专项治理数据
1000
360小时
2022-11-22 11:0 0:33
2022-12-07 11:2 5:41
2022-12-07 11:1 7:03
查询结束
审批日志
操作明细
M-166778780262 9-19259-2546-1-26
查询专项治理数据
1000
360小时
2022-11-07 10:2 3:23
2022-11-22 10:4 0:35
2022-11-22 10:3 8:28
查询结束
审批日志
操作明细


Weimob DBA
系统管理
MySQL
Redis
SQLServer
智能大盘
MySQL概况
MySQL监控大盘
我的工单
实例列表
权限管理
SQL优化
运维巡检
首页 / 我的工单
工单申请
域名/工单编号/工单名称
工单编号
工单名称
M-166986900763 7-19162-27-1-31
查询工单
M-166986431517 5-18740-27-1-94
值班支持
刷数据解决，已完成售后单储值卡退款金额与储
M-166979021626
执行时间
最后执行人
2022-12-01 13:4 0:54 至 2022-12-16 13:40:54
2022-12-01 11:4 1:27 至 2022-12-16 11:41:27
2022-11-30 14:3
2022-11-30 14:4
工单申请
资源审计：资源全生命周期管理
实例申请
查询申请
SQL工单申请
加入项目组
数据库权限
实例下架申请

四、数据库安全运维

安全运维--变更规范

类型										MySQL	Redis
新建实例	低	低	低	低	低	低	低	低	低	低	低
下架实例	中	中	中	中	中	中	中	中	中	中	中
资源扩容	低	低	低	低	低	低	低	低	低	低	低
资源缩容	N/A	低	低	低	低	低	低	低	低	低	低
资源扩容(数据搬迁)	中	中	中	中	中	中	高	中	中	中	中
资源缩容(数据搬迁)	中	中	中	中	中	中	高	中	中	中	中
集群升级主节点规格	低	N/A	N/A	N/A	中	中	中	中	中	N/A	N/A
集群降低主节点规格	低	N/A	N/A	N/A	中	中	中	中	中	N/A	N/A
热更新配置(高)	高	高	高	高	N/A	N/A	N/A	N/A	N/A	高	高
热更新配置(中)	中	中	中	中	N/A	N/A	N/A	N/A	N/A	中	中
热更新配置(低)	低	低	低	低	N/A	N/A	N/A	N/A	N/A	低	低
静态更新配置 (中)	中	中	中	中	中	中	中	中	中	中	中
静态更新配置(高)											
升级版本											
重启集群											
重启节点											
任务管理											
数据同步											
主从切换											
授权修改											

运维生产变更流程

操作风险等级	是否常规发布窗口	审批流程定义			
		发起点	一道审批	二道审批	三道审批
高	是	应用管理员（运维）	项目管理员		
中	是	应用管理员（运维）	项目管理员		
低	是	应用管理员（运维）	项目管理员		
高	否	应用管理员（运维）	项目管理员		
中	否	应用管理员（运维）	项目管理员		
低	否	应用管理员（运维）	项目管理员		
高	封版操作	项目管理员			
中	封版操作	应用管理员（运维）	项目管理员		
低	封版操作	应用管理员（运维）	项目管理员		

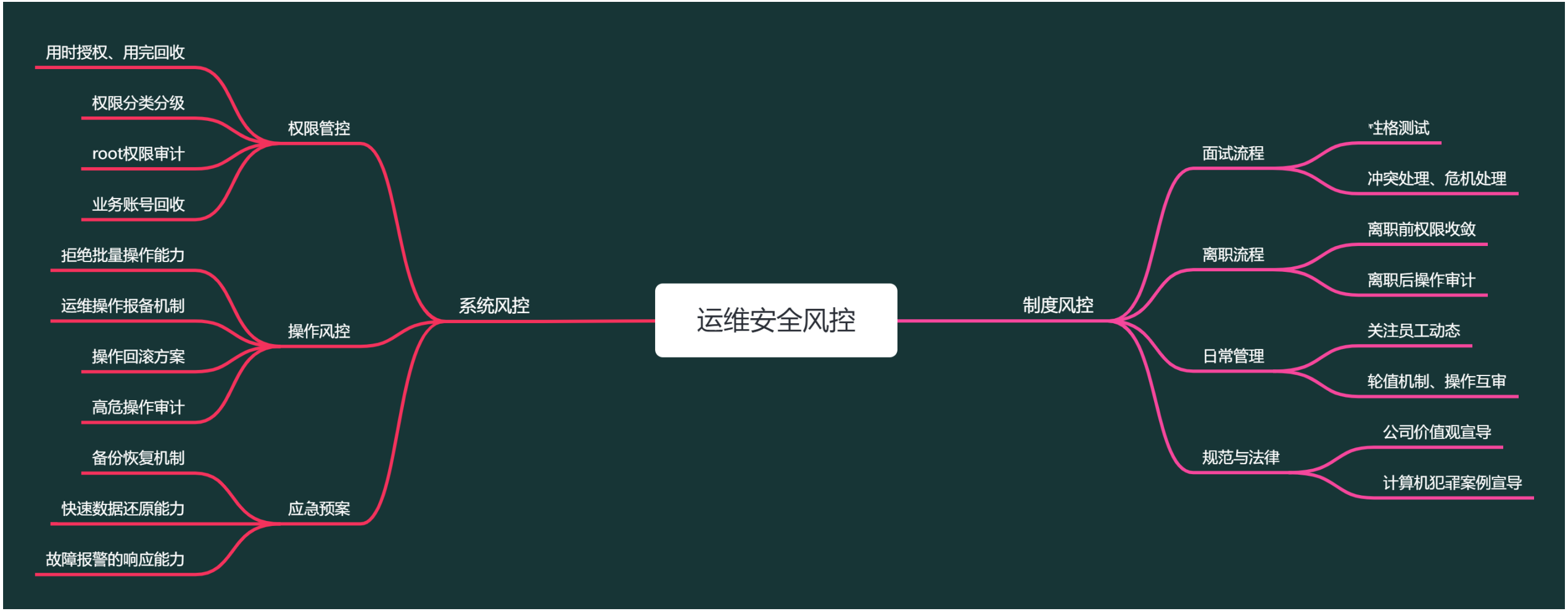
备注：低风险：8:00 ~ 8:00 (全天24小时)　　中风险：　　高风险：

紧急审批：线上出现故障，优先先恢复，事后审计；

安全运维--规范流程


规范流程
操作SOP
实例申请、扩缩容、下架流程
SQL上线
SQL查询
实例拆分、迁移、归档
安全组、重启、账号权限、运维变更
应急预案
CPU异常
活跃线程异常
存储容量异常
DTS同步异常
数据修复
报告总结
告警总结
慢SQL问题总结
需求总结
工作建议
权限收敛
研发权限收敛
DBA权限收敛

安全运维风控


运维安全风控
系统风控
权限管控
用时授权、用完回收
权限分类分级
root权限审计
业务账号回收
操作风控
拒绝批量操作能力
运维操作报备机制
操作回滚方案
高危操作审计
应急预案
备份恢复机制
快速数据还原能力
故障报警的响应能力
制度风控
面试流程
性格测试
冲突处理、危机处理
离职流程
离职前权限收敛
离职后操作审计
日常管理
关注员工动态
轮值机制、操作互审
规范与法律
公司价值观宣导
计算机犯罪案例宣导


openGauss
OceanBase
ArkDB
RASESQL
HotDB
StellarDB
QianBase xTP
云树Shard
GoldenDB
DolphinDB
MatrixDB
DynamoDB
SinoDB
FastData
Galaxybase
KunDB
SQL Server
vertica
D B 2
GBase
Oracle
达梦数据库
Spacture
开务数据库
UbiSQL
神舟通用
TDSQL
TiDB
Tapdata
StarRocks
KingbaseES
2010
2014
2018

THANKS