

第6章 数据库架构与安全体系

第一部 · 根基篇 · 第二篇 · 技术架构与基础设施

数据是平台的核心资产。对于供销安选这样一个涵盖五十多个功能模块、涉及多个政府部门、服务数百万用户的平台而言，数据库架构的设计不仅决定了系统的性能、可靠性和可扩展性，更关乎数据安全、隐私保护和跨区域互联互通的能力。

本章将系统阐述平台的数据库架构设计，包括Schema划分策略、核心表设计范式、索引优化策略、Redis缓存体系，以及贯穿全生命周期的数据安全架构。同时，本章将从“全国一张网”的战略视角出发，在数据库层面预留跨区域数据交换的标准化接口和数据联邦标识体系，为未来各地平台的互联互通奠定数据基础。这一设计思路与第三章提出的“基础先行”原则一脉相承——在打基础阶段就为未来的扩展留好接口。

6.1 数据库整体架构

6.1.1 一服务一Schema原则

平台采用“一服务一Schema”的数据库架构设计。每个微服务拥有自己独立的数据库Schema，服务之间不共享数据库表。这种设计的核心优势在于：第一，数据隔离。一个服务的数据库变更不会影响其他服务的正常运行。第二，独立扩展。每个服务的数据库可以根据自身的负载特性进行独立的容量规划和性能优化。第三，团队自治。每个开发团队可以独立设计和管理自己服务的数据库结构，不需要与其他团队进行复杂的协调。

平台共计三十一个数据库Schema（第一阶段八个、第二阶段十二个、第三阶段十一个），每个Schema对应一个微服务。Schema的命名规范为`sccmhp\_{模块名}`，如用户中心的Schema名为`sccmhp\_user`，助餐服务的Schema名为`sccmhp\_meal`。

需要说明的是，“一服务一Schema”并不意味着服务之间完全不能进行数据层面的协同。当需要跨服务查询数据时，平台通过服务接口调用而非直接跨库查询来实现。这种设计确保了服务间的松耦合，也为未来某些服务需要独立拆分或迁移提供了便利。

6.1.2 数据库选型与集群架构

平台选择MariaDB 10.11作为关系型数据库。MariaDB是MySQL的完全开源分支，与MySQL完全兼容，同时提供了更好的性能和更多的存储引擎选择。平台采用MariaDB Galera Cluster实现数据库的高可用——三节点多主复制，任意节点都可以处理读写请求，单节点故障不影响整体服务。

Galera Cluster的同步复制机制确保了各节点数据的强一致性，适合对数据一致性要求高的业务场景。在性能方面，三节点集群可以分担读请求压力，写请求通过负载均衡分发到各节点。

各地在部署数据库时，可根据自身条件选择不同的集群方案。条件有限的地方可以从单节点起步，后续再扩展为集群；条件好的地方可以直接部署三节点集群，确保高可用。这种灵活性正是“因地制宜”原则在技术层面的体现。

6.1.3 数据联邦标识体系——为“全国一张网”预留基础

这是本章最重要的一个设计决策。为了实现“星星之火，可以燎原”的战略目标——让各地建设的供销平台能够按照统一标准互联互通，最终形成“全国一张网”——平台在数据库层面预留了一套“数据联邦标识体系”。

具体来说，每个需要跨区域共享或交换的数据表，都包含以下标准字段：

```
-- 数据联邦标识字段（所有需要跨区域协同的表均包含）
data_origin      VARCHAR(12)  NOT NULL  -- 数据来源区域代码（行政区划代码）
data_platform    VARCHAR(50)  NOT NULL  -- 数据来源平台标识（如"SCCMHP-浚县"）
data_federated   TINYINT      DEFAULT 0 -- 是否已纳入联邦数据体系（0-本地 1-已联邦）
data_version     INT          DEFAULT 1 -- 数据版本号（用于冲突检测和增量同步）
data_signature   VARCHAR(128) NULL      -- 数据签名（用于防篡改验证）
```

这套标识体系的意义在于：第一，明确数据归属。每一条数据都能追溯到它的来源区域和来源平台，确保数据主权清晰。第二，支持联邦查询。当需要进行跨区域数据汇总时，可以通过`data\_origin`字段筛选特定区域的数据，通过`data\_platform`字段区分不同平台来源。第三，防篡改可验证。通过`data\_signature`签名字段，可以验证数据在联邦传输过程中是否被篡改。第四，增量同步支持。通过`data\_version`版本号，可以实现联邦节点之间的增量数据同步。

这套数据联邦标识体系，正是本书所倡导的“标准化互联互通”理念在数据库层面的具体实现。各地在按照本书建设平台时，只要在数据库设计中遵循这套标识体系，未来当条件成熟时，就可以无缝接入全国供销数据联邦网络。

6.2 核心表设计规范

6.2.1 通用字段规范

平台所有业务表都遵循统一的字段规范，包含以下通用字段：

字段名	类型	说明
id	BIGINT AUTO_INCREMENT	主键ID，全局唯一自增
is_deleted	TINYINT DEFAULT 0	逻辑删除标记（0-正常 1-已删除）
create_time	DATETIME DEFAULT NOW()	创建时间
update_time	DATETIME ON UPDATE NOW()	更新时间
region_code	VARCHAR(12)	所属区域代码（行级数据隔离）

其中，`region\_code` 字段是平台实现六级行政区域行级数据隔离的核心字段。所有涉及多层级数据管理的业务表都包含此字段，数据查询时根据用户的数据权限范围自动注入过滤条件。

此外，涉及需要跨区域协同的表，还包含上一节所述的数据联邦标识字段。各地在实施时，可根据实际需要决定是否启用联邦标识——本地使用的表可以不包含这些字段，但未来可能参与跨区域协同的表建议在初期就预留好。

6.2.2 命名规范

表命名遵循` t\_{模块缩写}\_{表名}` 格式，如用户主表命名为` t\_user\_info`，助餐核销记录表命名为` t\_meal\_consume`。关联表命名格式为` t\_{模块}\_{表A}\_{表B}\_rel`，日志表命名格式为` t\_{模块}\_log\_{业务}`，聚合表命名格式为` t\_{模块}\_aggregation\_{维度}`。

字段命名采用全小写下划线分隔，如` resident\_id`、` consume\_time`。索引命名格式为` idx\_{字段}`用于普通索引、` uk\_{字段}`用于唯一索引。这种统一的命名规范使得数据库结构清晰可读，便于新加入的开发人员快速上手。

6.2.3 字符集与存储引擎

所有表统一使用 utf8mb4 字符集和 utf8mb4_unicode_ci 排序规则。utf8mb4 是 MySQL/MariaDB 中真正的 UTF-8 实现，支持 emoji 等四字节字符。所有表统一使用 InnoDB 存储引擎，支持事务、行级锁和外键约束。

6.3 索引策略与性能优化

6.3.1 索引设计原则

索引设计是数据库性能优化的核心。平台的索引设计遵循以下原则：

第一，主键索引。所有表使用BIGINT自增主键，InnoDB以主键为聚簇索引组织数据存储。

第二，唯一索引。业务上需要唯一性的字段（如订单编号、合同编号、用户手机号等）建立唯一索引，确保数据完整性。

第三，联合索引。高频的组合查询条件建立联合索引。平台中最常见的查询模式是“区域+时间”的组合查询（如查询某区域某时间段的助餐记录），因此`(region\_code, create\_time)`是最常见的联合索引模式。

第四，覆盖索引。对于高频的查询，尽量设计覆盖索引，避免回表查询。例如，查询用户列表时常用的`(user\_id, real\_name, phone, status)`联合索引可以覆盖大部分列表查询需求。

第五，前缀索引。对于长字符串字段（如地址、备注等），使用前缀索引减少索引大小。

6.3.2 分区策略

对于数据量增长迅速的大表（如消息记录表、操作日志表、积分变动记录表等），采用按月分区策略。分区键选择`create\_time`字段，每个月的数据存储在一个独立的分区中。分区的好处在于：查询时可以只扫描相关分区，大幅减少扫描数据量；历史数据归档时可以直接操作整个分区，效率更高。

6.3.3 慢查询监控

平台对所有数据库操作进行慢查询监控。超过一秒的查询记录到慢查询日志中，定期分析慢查询日志，对高频慢查询进行索引优化或SQL改写。在开发阶段，所有SQL必须经过EXPLAIN分析，确保使用了正确的索引。

6.4 Redis缓存体系

6.4.1 缓存架构

平台采用Redis 7 Cluster作为缓存层。Redis Cluster支持自动分片和故障转移，能够满足平台对高可用和高性能的需求。缓存主要用于以下几个场景：

第一，热点数据缓存。用户信息、区域树结构、商品信息等高频读取的数据缓存在Redis中，减少数据库压力。第二，会话管理。JWT令牌和用户会话信息存储在Redis中，支持分布式环境下的会话共享。第三，在线状态管理。乡音即时通讯的用户在线状态通过Redis的键过期机制实现——用户心跳每三十秒更新一次，超时自动标记为离线。第四，分布式锁。使用Redis的SETNX命令实现分布式环境下的资源锁定。第五，实时计数。今日助餐人数、今日检测人次等实时统计指标通过Redis的计数器实现，定时同步到数据库。

6.4.2 缓存策略

不同数据类型采用不同的缓存策略：用户信息缓存三十分钟，修改时主动删除缓存；区域树缓存为永久有效，启动时加载，变更时刷新；当日运营数据缓存五分钟，定时任务刷新；历史聚合数据缓存一小时，每日预计算后更新；商品信息缓存十分钟，修改时主动删除；在线状态心跳三十秒续期一次。

缓存的更新策略遵循“Cache Aside”模式——读操作先查缓存，缓存命中直接返回，未命中则查数据库并回写缓存；写操作先更新数据库，再删除缓存（而非更新缓存），由下一次读操作触发缓存的重新加载。

6.5 数据安全架构

6.5.1 数据分级分类管理

平台将数据按照敏感程度分为高、中、低三个级别。高级别数据包括个人信息（姓名、身份证号、手机号、人脸特征）、健康数据（血压、血糖、心电、检验报告）、家族数据（族谱、家训、家族成员关系）和合同数据（电子合同、数字签名、CA证书）。中级别数据包括交易数据（订单、补贴、支付记录）和时间币数据（账户余额、交易记录）。低级别数据包括位置数据（站点地址、配送轨迹、服务人员位置）。

不同级别的数据采用不同的安全措施。高级别数据必须加密存储（AES-256-GCM），传输必须加密（TLS 1.3），访问必须经过严格的权限控制并全量记录审计日志。中级别数据采用传输加密和访问控制。低级别数据采用基本的访问控制。

6.5.2 加密存储方案

对于需要加密存储的敏感字段，平台采用应用层加密方案。加密算法使用AES-256-GCM，密钥由密钥管理服务统一管理，定期轮换。应用层加密的优势在于：即使数据库被非法访问，没有密钥也无法解密数据；加密和解密在应用层完成，对数据库透明；不同字段可以使用不同的加密密钥，实现更精细的安全控制。

对于需要模糊查询的加密字段（如手机号），平台采用“哈希+加密”双存储方案：哈希值用于精确匹配查询，加密值用于解密后展示。身份证号等不需要模糊查询的字段，直接加密存储。

6.5.3 审计日志

所有对敏感数据的访问操作都全量记录审计日志。审计日志包含：操作用户、操作时间、操作类型（查询/修改/删除）、操作对象、请求来源IP、操作结果。审计日志存储在独立的数

数据库Schema中，与业务数据隔离，确保审计日志的完整性和不可篡改性。

平台还设置了异常行为检测规则——高频访问敏感数据、非工作时间大量查询、异地登录后访问敏感数据等行为自动触发告警。

6.6 跨区域数据交换标准——为全国互联预留接口

这是本章从“全国一张网”战略出发最重要的前瞻性设计。虽然平台在初期以县域为单位独立建设和运营，但从长远来看，各县级平台之间的数据互通和业务协同是必然趋势。为此，平台在数据库层面预留了跨区域数据交换的标准接口和数据格式规范。

6.6.1 跨区域数据交换的元数据标准

为了实现不同区域平台之间的数据互通，首先需要统一数据的“语义”——即不同平台对同一概念使用相同的编码和格式。平台定义了以下核心元数据标准：

第一，统一区域编码。采用国家标准的行政区划代码（六位数字），确保全国范围内的区域标识唯一且可识别。第二，统一业务编码。关键业务实体（如用户、订单、服务项目等）采用“区域代码+业务类型+序号”的编码规则，确保全局唯一。第三，统一数据字典。核心枚举值（如性别、服务类型、订单状态等）采用统一的编码表，不同平台之间通过编码映射实现语义对齐。第四，统一时间格式。所有时间字段采用UTC时间戳或ISO 8601标准格式，避免时区差异导致的数据不一致。

6.6.2 联邦数据交换协议

平台定义了三种层次的跨区域数据交换模式：

第一层：脱敏汇总数据上报。各县级平台定期向上级平台（市、省、国家）上报脱敏的汇总统计数据。例如，每月上报本县助餐服务的总人次、总补贴金额、覆盖率等指标，而不是上报每个老人的详细用餐记录。这种模式保护了原始数据的安全，同时满足了上级部门的统计需求。

第二层：有条件的数据共享。当需要进行跨区域的业务协同时（如跨县农产品流通、跨区域就业信息共享），相关区域平台在获得授权后，通过标准接口进行有条件的数据共享。共享的数据仅包含协同所需的最小必要字段，不共享完整的原始数据。

第三层：联邦查询。当需要汇总多个区域的数据进行分析时（如省级或国家级的数据驾驶舱），通过联邦查询机制，向各区域平台发送查询请求，各平台在本地完成数据计算后返回脱敏的查询结果，由发起方进行汇总展示。原始数据始终保留在各区域平台本地，不出域。

这三种层次的设计遵循了“数据主权归属本地、数据价值全国共享”的联邦数据原则——每个区域平台对自己的数据拥有完整的主权，但可以通过标准化的协议与其他平台进行安全、可控、最小必要的数据交换。

6.6.3 实现路径：从本地到全国

跨区域数据交换的实现不是一蹴而就的，而是随着平台的发展逐步推进的。在第一阶段，各区域平台独立建设和运营，优先满足本地的业务需求，但在数据库设计中预留联邦标识字段和标准接口。在第二阶段和第三阶段，当多个县级平台建成并稳定运行后，开始在市域或省域范围内进行互联互通试点，验证和完善联邦数据交换协议。在第四阶段，逐步推广到全国范围，形成完整的供销数据联邦网络。

这种循序渐进、从本地到全国的实现路径，正是第三章“基础先行、生态完善、运营深化”原则在数据互联互通领域的具体应用。

6.7 总结

数据库架构是平台的“地基”。一个好的数据库设计，不仅要满足当前业务的需求，还要为未来的扩展和互联互通预留空间。本章提出的“一服务一Schema”架构、统一字段规范、索引优化策略和Redis缓存体系，为平台的高性能和高可用提供了保障。完善的数据安全架构——从分级分类、加密存储到审计日志——确保了平台数据的安全合规。

更重要的是，本章从“全国一张网”的战略高度出发，在数据库层面预留了数据联邦标识体系和跨区域数据交换标准。这套标准化的设计，使得各地按照本书建设的平台，在未来条件成熟时能够无缝接入全国供销数据联邦网络。每一颗扎根乡土的火种，通过标准化的通道连接起来，就能形成燎原之势。这正是本书的深层愿景——不仅是一本指导单个平台建设的手册，更是一套推动全国供销系统数字化互联的方法论。

本章核心观点

数据库架构采用“一服务一Schema”原则，MariaDB Galera Cluster保障高可用，Redis Cluster提供高性能缓存。所有表遵循统一的字段规范和命名规范。数据安全覆盖分级分类管理、AES-256-GCM加密存储和全量审计日志。从“全国一张网”战略出发，在数据库层面预留数据联邦标识体系（data_origin、data_platform、data_signature），定义跨区域数据交换的元数据标准和三级联邦交换协议（脱敏上报、条件共享、联邦查询），为各地平台的互联互通奠定标准化基础。

