中科京云伟道可信数据空间

VISOM WeiDAO Trust Data Space

技术白皮书

Technology Whitepaper

版本：v3.3　　发布日期：2026 年 6 月

北京中科京云控股有限公司

版权声明

版权所有 © 北京中科京云控股有限公司 2026-2028。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

中科京云、伟道均为中科京云公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受中科京云公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，中科京云公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

公司信息

北京中科京云控股有限公司

地址：北京市海淀区北四环西路 9 号 1806-1808

网址：https://www.wiseom.com

客户服务邮箱：support@wiseom.com

前言

概述

本文档详细描述了中科京云伟道可信数据空间（VISOM WeiDAO Trusted Data Space，简称 VISOM WeiDAO TDS）的系统架构、核心技术、安全体系与应用实践，让用户对 VISOM WeiDAO TDS 有一个深入细致的了解。

VISOM WeiDAO TDS 是中科京云自主研发的企业级可信数据空间平台，以"合约化授权、隐私计算、链上存证、全链路审计"为核心技术特征，构建"数据可用不可见、可控不可改、全程可追溯"的数据流通环境，为政府、金融、医疗、工业等行业提供安全、高效、可信的数据要素流通基础设施。

读者对象

本文档主要适用于以下人员：

- 各地数据局/政数局、数据/数投集团等
- 企业 CIO/CTO 及技术决策者
- 数据安全与合规管理人员
- 系统架构师与开发工程师
- 数据要素市场从业者
- 科研机构与行业分析师

修改记录

文档版本	发布日期	修改说明
v3.3	2026-06-08	缓存架构优化版本，新增 Redis/Redisson 缓存体系、7 个缓存命名空间、缓存策略与序列化防护机制
v3.2	2026-04-15	安全增强版本，完善纵深防御安全模型、数据全生命周期安全、合规审计体系
v3.0	2026-01-20	首个正式发布版本，包含 11 个微服务架构、智能合约、链上存证、TEE 隐私计算等核心能力

版权所有©北京中科京云控股有限公司 2026-2028

目 录

 版权所有©北京中科京云控股有限公司 2026-2028

 版权所有©北京中科京云控股有限公司 2026-2028

 版权所有©北京中科京云控股有限公司 2026-2028

 版权所有©北京中科京云控股有限公司 2026-2028

一、行业背景与发展趋势

1.1 数据要素市场化改革

随着数字经济的深入发展，数据已成为国家基础性战略资源和关键生产要素。2022 年 12 月，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（简称"数据二十条"），首次从国家层面系统部署数据基础制度建设，明确了数据产权、流通交易、收益分配、安全治理四大制度框架，标志着我国数据要素市场化改革进入全面推进的新阶段。

数据二十条提出建立"数据资源持有权、数据加工使用权、数据产品经营权"三权分置的数据产权制度框架，为数据要素市场化配置奠定了制度基础。随后，《数字中国建设整体布局规划》《关于加强数据要素市场化配置改革的指导意见》等政策文件相继出台，数据要素市场建设从顶层设计逐步走向落地实施。

在政策推动下，全国已设立近 50 家数据交易机构，数据交易场所体系初步形成。然而，数据要素市场仍处于发展初期，面临确权难、定价难、互信难、监管难等诸多挑战，亟需技术创新与制度创新协同推进。

1.2 数据安全与合规要求

数据安全是数据要素流通的前提和底线。近年来，《网络安全法》《数据安全法》《个人信息保护法》等法律法规相继颁布实施，构建了我国数据安全与个人信息保护的法律框架。《数据安全法》确立了数据分类分级保护、数据安全审查、数据出口管制等重要制度，《个人信息保护法》则对个人信息处理活动进行了全面规范。

与此同时，行业监管也在不断强化。金融、医疗、交通等重点领域的数据安全监管要求日益严格，数据跨境流动、数据共享、数据出境等活动均需履行严格的安全评估程序。企业在数据流通与共享过程中，面临着日益严峻的合规压力。

传统的数据共享模式已难以满足安全合规要求。一方面，数据一旦交付即失去控制，存在滥用、泄露的风险；另一方面，审计依赖事后日志，缺乏事中不可篡改的存证，难以满足监管审计要求。如何在合规框架内实现数据价值的安全释放，成为企业数字化转型的核心痛点。

1.3 可信数据空间的兴起

可信数据空间（Trusted Data Space，TDS）作为一种新型数据流通基础设施，正在全球范围内兴起。欧盟在《欧洲数据战略》中明确提出建设"共同欧洲数据空间"（Common European Data Spaces），旨在打破数据孤岛，在保障数据安全与隐私的前提下促进数据共享与再利用。

 版权所有©北京中科京云控股有限公司 2026-2028

在我国，可信数据空间也被视为数据要素市场化配置的关键技术路径。可信数据空间通过构建"数据可用不可见、可控可计量、全程可追溯"的数据流通环境，实现数据所有权与使用权的分离，既保障数据提供方的数据主权，又满足数据消费方的使用需求，是平衡数据利用与安全保护的有效技术方案。

可信数据空间的核心技术特征包括：

- **合约化授权**：数据访问由显式合约授权，无合约即无权访问
- **隐私计算**：数据不移动、计算移动，通过 TEE、联邦学习等技术实现"数据可用不可见"
- **链上存证**：关键操作上链存证，提供不可抵赖的审计轨迹
- **全链路审计**：每一步操作都有记录，实现数据流通全程可追溯

1.4 行业痛点与核心挑战

尽管数据要素市场前景广阔，但企业间数据协作仍面临诸多现实挑战：

第一，数据权属模糊。数据一旦交付，接收方即可无限复制，提供方失去对数据的控制权。传统的 API 接口、数据拷贝等共享方式，无法有效界定数据使用边界，也难以防止数据二次流转。

第二，信任成本高昂。企业间数据共享往往依赖点对点谈判，信任建立周期长、成本高。缺乏中立的第三方信任基础设施，导致数据流通效率低下，大量数据价值被闲置。

第三，合规风险突出。数据共享涉及多方主体，合规责任边界不清。一旦发生数据泄露或滥用，难以追溯责任主体，企业面临巨大的法律与声誉风险。

第四，技术标准不统一。不同企业、不同行业的数据格式、接口标准、安全要求差异较大，互联互通成本高，难以形成规模化的数据流通网络。

VISOM WeiDAO TDS 正是为系统性解决上述问题而设计的企业级可信数据空间平台，致力于为数据要素流通提供安全、高效、可信的技术基础设施。

版权所有©北京中科京云控股有限公司 2026-2028

二、产品概述与设计哲学

2.1 产品定位

VISOM WeiDAO TDS（VISOM WeiDAO Trusted Data Space）是中科京云自主研发的企业级可信数据空间平台，旨在为政府、金融、医疗、工业等行业提供安全、高效、可信的数据要素流通基础设施。

平台以"合约化授权、隐私计算、链上存证、全链路审计"为核心技术特征，构建"数据可用不可见、可控不可改、全程可追溯"的数据流通环境，实现数据所有权与使用权的有效分离，帮助企业在保障数据安全与隐私的前提下，充分释放数据要素价值。

VISOM WeiDAO TDS 定位为企业级数据空间操作系统，向下兼容各类数据源与存储系统，向上支撑数据共享、数据交易、联合建模、数据服务等多种业务场景，为数据要素市场化配置提供技术底座。

2.2 核心价值

VISOM WeiDAO TDS 为数据流通参与各方创造多重价值：

参与方	核心价值	具体体现
数据提供方	保障数据主权，实现数据增值	数据不出域、可用不可见；精细化授权控制；可计量的数据收益
数据消费方	合规获取数据，降低使用成本	可信的数据来源；标准化的数据接口；按需付费的使用模式
监管/审计方	全链路可追溯，合规可验证	不可篡改的操作记录；链上存证的审计轨迹；第三方可独立验证
平台运营方	构建数据生态，形成网络效应	标准化的接入协议；可扩展的架构设计；丰富的应用生态

2.3 设计哲学

2.3.1 四条架构原则

VISOM WeiDAO TDS 的设计遵循四条核心架构原则，贯穿系统设计的每一个层面：

版权所有©北京中科京云控股有限公司 2026-2028

原则	含义	在系统中的体现
最小信任	不信任任何单一参与方	合约需双方签署才能激活；区块链存证不可抵赖；每个服务独立验证 Token
合约先行	数据访问由显式合约授权	无合约/合约未激活 = 无权访问；合约定义使用范围、期限、计量方式
计算近数据	数据不移动，计算移动	TEE 沙箱在数据侧执行，仅输出聚合结果；消费者提交算法，飞地内执行计算
全链路可审计	每一步操作留有不可篡改记录	审计日志入 OpenSearch + 关键事件上链；数据血缘全程追踪

2.3.2 微服务拆分策略

VISOM WeiDAO TDS 采用 11 个微服务的分布式架构，而非单体应用。这一设计决策基于以下考量：

第一，安全域隔离。数据空间场景下，不同功能模块的安全敏感度差异巨大。IAM 认证逻辑与资产存储逻辑若在同一进程，攻击面将显著扩大。通过微服务拆分，每个服务拥有独立的安全边界，可实现精细化的权限控制与攻击面收敛。

第二，独立演化节奏。合约、资产、审计、计费的业务节奏完全不同。合约模型变更缓慢，而计费规则、审计策略则可能频繁调整。按业务域垂直切分，使各服务能够独立迭代，互不干扰。

第三，故障隔离。计量服务宕机不应影响合约签署；TEE 节点异常不应阻断资产查询。微服务架构将故障影响范围限制在单个服务内，提升系统整体可用性。

VISOM WeiDAO TDS 的拆分依据是"变更频率"和"安全边界"的垂直切分，而非按技术层的水平切分。高变更频率的计费规则、审计策略与低变更频率的合约模型、资产元数据分别部署，确保系统的稳定性与灵活性。

2.3.3 共享库的边界纪律

11 个微服务共享 tds-common 基础库，但严格控制共享库的边界。tds-common 仅包含三类内容：

- **模型类**（DataAsset, Organization, User, DigitalContract）— 所有服务共识的数据模型
- **异常类**（BusinessException + ErrorCode 枚举）— 统一错误语义

版权所有©北京中科京云控股有限公司 2026-2028

- **安全过滤器**（JwtAuthFilter）— 每个服务独立验证 Token，网关不承担鉴权

共享库严格遵循"反模式防御"原则：不包含 DAO、不包含业务逻辑、不包含配置。一旦有服务需要在 common 中放置 Repository，就说明切分有误，需要重新审视架构边界。

2.4 产品优势

相较于传统数据共享方案与同类产品，VISOM WeiDAO TDS 具有以下显著优势：

技术架构先进。采用云原生微服务架构，支持弹性伸缩与高可用部署；深度融合区块链、TEE、隐私计算等前沿技术，构建多层次可信保障体系。

安全合规可靠。遵循零信任安全理念，构建纵深防御安全体系；关键操作链上存证，满足监管审计要求；支持国密算法，符合国产化安全标准。

部署灵活便捷。支持 Docker/K8s 容器化部署，提供一键启停脚本；既可私有化部署，也可 SaaS 化交付，满足不同规模企业的部署需求。

生态开放兼容。提供标准化的 API 接口与 SDK，支持多源数据接入；兼容主流区块链平台与隐私计算框架，便于与现有系统集成。

版权所有©北京中科京云控股有限公司 2026-2028

三、系统总体架构

3.1 总体架构视图

VISOM WeiDAO TDS 采用分层微服务架构设计，自下而上分为基础设施层、运营保障层、能力支撑层、核心业务层和接入层五个层次。各层职责清晰、松耦合，通过标准化接口交互，支持独立演进与水平扩展。

3.2 接入层

接入层是系统的统一入口，负责 TLS 终止、请求路由、流量控制与安全防护。采用 Nginx 作为 API 网关，监听 9080（HTTP）和 9443（HTTPS）端口，提供以下核心能力：

- **TLS 终止**：统一处理 HTTPS 请求，支持 TLS 1.3 协议，保障传输安全
- **请求路由**：根据 URL 路径将请求转发至对应微服务，支持动态路由配置
- **限流熔断**：基于 IP、用户、接口等多维度的流量控制，防止系统过载
- **请求大小限制**：默认限制 100MB，防止大文件攻击

值得强调的是，Nginx 网关不承担鉴权职责——Token 验证在每个微服务的

版权所有©北京中科京云控股有限公司 2026-2028

JwtAuthFilter 中独立执行。这是零信任原则的体现：即使网关被绕过（如 K8s Pod 间直连），鉴权依然生效。生产环境可升级为 APISIX，获得动态路由、插件体系、可观测性等增强能力。

3.3 核心业务层

核心业务层是 VISOM WeiDAO TDS 的业务核心，包含 IAM、Org、Asset、Contract 四个核心服务，构成数据空间运行的最低必要集。

IAM 服务：身份与访问管理服务，负责用户认证、Token 签发、DID 身份管理。支持 JWT 与 DID 两种身份体系，既满足传统企业身份管理需求，又支持去中心化身份认证。

Org 服务：组织与用户管理服务，维护组织架构、用户信息、角色权限。支持多租户隔离，每个组织拥有独立的用户空间与权限体系。

Asset 服务：数据资产管理服务，负责数据资产注册、元数据管理、NDI 标识分配、对象存储管理。是数据空间的"资产目录"，提供数据发现、检索、预览等能力。

Contract 服务：智能合约服务，负责合约创建、签署、激活、撤销、过期等全生命周期管理。合约是数据访问的授权凭证，无合约或合约未激活则无权访问数据。

核心业务层共享 Redis 缓存集群，通过 7 个命名空间分别缓存组织、用户、资产、合约、DID 文档等高频查询数据，显著提升系统响应性能。

3.4 能力支撑层

能力支撑层提供数据空间的关键技术能力，是"可信"能力的主要承载者。

Chain 服务：区块链适配服务，提供链上存证、链上查询等能力。通过适配器模式对接 FISCO BCOS 等底层区块链平台，将关键操作（合约签署、资产登记等）的哈希写入链上，提供不可抵赖性。

TEE 服务：可信执行环境服务，负责 TEE 飞地管理、远程证明、计算任务调度。对于最高敏感度数据，数据不离开 TEE 飞地，消费者提交算法在飞地内执行，仅返回计算结果。

Compute 服务：数据计算服务，提供数据加工、聚合分析、模型推理等计算能力。支持多种计算模式，包括直接下载（低敏感数据）、TEE 计算（高敏感数据）、联邦学习（跨机构联合建模）等。

Policy 服务：合规策略服务，提供数据分类分级、脱敏规则、访问策略等合规管理能力。支持动态策略配置，可根据数据敏感度、用户角色、使用场景等灵活控制数据访问权限。

版权所有©北京中科京云控股有限公司 2026-2028

3.5 运营保障层

运营保障层为平台运营提供支撑能力，确保系统可审计、可追溯、可计量。

Audit 服务：操作审计服务，记录所有关键操作日志，存储于 OpenSearch。支持多维度审计查询、审计报表生成，满足合规审计要求。关键事件同时上链存证，提供双重审计保障。

Lineage 服务：数据血缘服务，追踪数据的来源、流转、使用全链路。支持数据血缘可视化，帮助用户了解数据的来龙去脉，为数据质量评估与合规审计提供支撑。

Metering 服务：计量计费服务，按合约约定的计量方式（调用次数、数据量、计算时长等）统计使用量，生成计费账单。支持多种计费模型，为数据交易与商业化运营提供支撑。

3.6 基础设施层

基础设施层为整个平台提供基础技术支撑，采用云原生技术栈，支持 Docker/K8s 容器化部署。

组件	版本	用途
PostgreSQL	16	关系型数据库，存储业务数据，支持 JSONB 兼顾灵活性
Redis	7.4	分布式缓存，使用 Redisson 客户端，提供 7 个命名空间缓存
MinIO	最新	对象存储，存储数据资产文件，S3 兼容
OpenSearch	2.x	搜索引擎，存储审计日志，支持全文检索与分析
FISCO BCOS	最新	联盟链，提供链上存证能力，国产化合规

3.7 服务分类与依赖关系

11 个微服务按重要性可分为"核心"与"增强"两类：

层次	服务	状态	缓存	链依赖

版权所有©北京中科京云控股有限公司 2026-2028

接入	IAM	核心	Redis	--
接入	Org	核心	Redis	--
业务	Asset	核心	Redis	--
业务	Contract	核心	Redis	读写链
能力	Chain	核心	--	链适配器
能力	TEE	核心	--	--
能力	Compute	增强	--	--
能力	Policy	增强	--	--
运营	Audit	增强	--	读链
运营	Lineage	增强	--	--
运营	Metering	增强	--	--

"核心"服务是系统运行的最低必要集，构成数据空间的基础能力；"增强"服务可在核心链路完整后按需启用，根据业务场景灵活裁剪。

版权所有©北京中科京云控股有限公司 2026-2028

四、核心技术能力

4.1 分布式身份与访问控制

4.1.1 DID 去中心化身份

VISOM WeiDAO TDS 支持 W3C DID（Decentralized Identifiers）去中心化身份标准，为每个参与方（组织、用户、设备）颁发可验证的数字身份。DID 身份不依赖中心化身份提供商，身份所有者完全掌控自己的身份数据，符合数据空间"最小信任"的设计原则。

DID 身份体系的核心优势在于：

- **自主可控**：身份所有者完全掌控身份数据，可自主颁发、验证、撤销可验证凭证（VC）
- **隐私保护**：支持选择性披露，用户可只披露必要的身份属性，而非全部身份信息
- **跨域互认**：基于标准协议，不同数据空间、不同机构间的身份可互认互通
- **不可篡改**：身份与凭证基于区块链存证，具有不可抵赖性

4.1.2 JWT 认证体系

除 DID 外，VISOM WeiDAO TDS 同时支持传统的 JWT（JSON Web Token）认证体系，满足企业级应用的身份管理需求。IAM 服务负责用户认证与 Token 签发，其他服务使用同一把密钥（TDS_JWT_SECRET）独立验证 Token。

JWT 认证的设计要点：

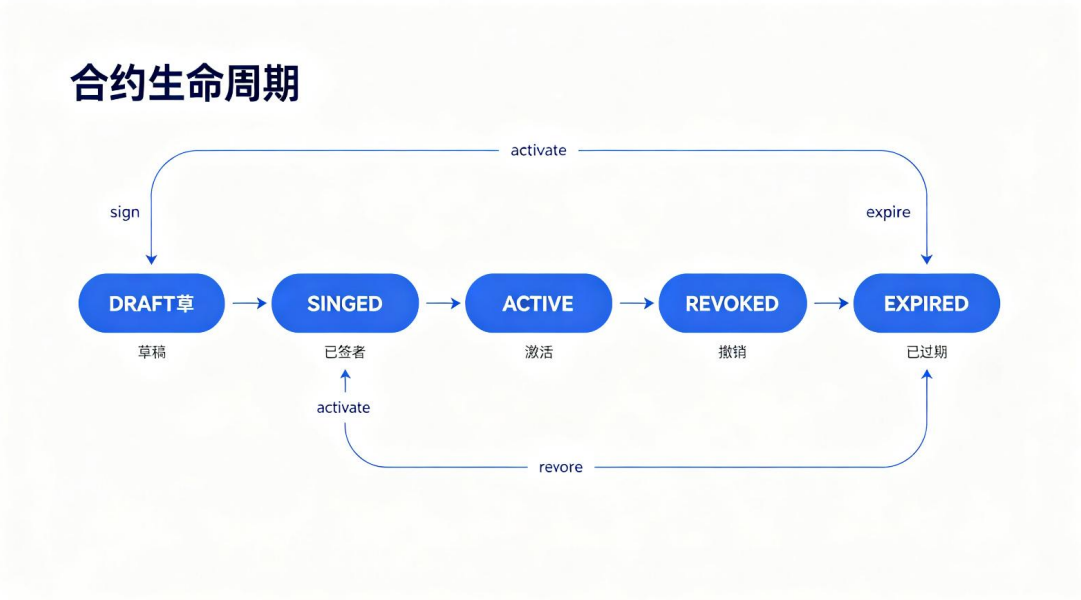
- **服务端无状态**：Token 包含所有必要信息，服务端无需查询会话状态，便于水平扩展
- **每服务独立验证**：每个微服务通过 JwtAuthFilter 独立验证 Token，网关不承担鉴权职责，遵循零信任原则
- **HS256 算法**：采用 HS256 对称加密算法，密钥仅在服务间共享，不暴露给客户端，安全性与性能兼顾
- **角色权限体系**：支持 SUPER_ADMIN、PROVIDER、CONSUMER 等多角色，实现精细化权限控制

4.2 智能合约与链上存证

版权所有©北京中科京云控股有限公司 2026-2028

4.2.1 合约生命周期管理

合约是 VISOM WeiDAO TDS 的核心授权机制，定义了数据使用的范围、期限、计量方式等条款。合约的生命周期包含 DRAFT（草稿）、SIGNED（已签署）、ACTIVE（已激活）、REVOKED（已撤销）、EXPIRED（已过期）五个状态，状态转换严格遵循状态机规则。



合约状态转换的关键规则：

- **签署（sign）**：需双方签署才能生效，每次签署触发链上存证
- **激活（activate）**：双方签署完成后可激活，激活后合约才真正生效
- **撤销（revoke）**：任何一方可在合约生效前撤销，撤销后合约不可恢复
- **过期（expire）**：到达约定的到期时间后自动过期

4.2.2 链上存证机制

合约签署等关键操作触发 FISCO BCOS 智能合约调用，将操作哈希写入区块链。链上存证不替代 PostgreSQL 中的业务记录，而是提供三重价值：

第一，不可抵赖性。签署方无法事后否认签署行为，链上记录具有密码学级别的证据效力。

第二，第三方可验证。监管节点、审计机构可以独立验证链上哈希与合约内容的一致性，无需依赖平台方。

第三，审计完整性。链上存证与 OpenSearch 审计日志构成双重审计轨迹，相互印证，提升审计可信度。

链上仅存储操作哈希，不存储业务原文——这是重要的设计权衡。既保护了商业隐

版权所有©北京中科京云控股有限公司 2026-2028

私，又提供了密码学级别的完整性证明。如需验证，只需计算原文哈希与链上哈希比对即可。

4.3 可信执行环境（TEE）

可信执行环境（Trusted Execution Environment，TEE）是 VISOM WeiDAO TDS 实现"数据可用不可见"的核心技术之一。对于最高敏感度的数据，即便合约授权了访问，数据也不离开 TEE 飞地（Enclave）。

4.3.1 TEE 工作原理

TEE 通过硬件级隔离技术，在 CPU 中划分出一块安全区域——飞地（Enclave）。飞地内的代码和数据对外部完全不可见，即使操作系统、虚拟机监控器（VMM）被攻破，也无法窃取飞地内的数据。

VISOM WeiDAO TDS 中 TEE 的工作流程：

1. 数据提供方将加密后的数据上传至 TEE 节点，数据密钥仅提供方持有
2. 数据消费方提交计算任务（算法代码或 SQL 查询）
3. TEE 服务验证消费方身份与合约授权，通过后加载计算任务
4. 数据在飞地内解密，执行计算，仅输出计算结果
5. 计算结果返回给消费方，原始数据始终不离开飞地

4.3.2 远程证明

为确保计算确实在真实的 TEE 环境中执行，VISOM WeiDAO TDS 支持远程证明（Remote Attestation）机制。消费方可以验证：

- 计算节点确实运行在真实的 TEE 硬件上
- 飞地内加载的代码版本与预期一致
- 计算过程未被篡改

远程证明由 TEE 服务负责，通过硬件厂商提供的证明服务（如 Intel SGX 的 IAS）进行验证。验证通过后，消费方才会将计算任务提交执行。

4.4 数据资产目录与 NDI 标识

4.4.1 数据资产管理

Asset 服务负责数据资产的全生命周期管理，是数据空间的"资产目录"。数据资产包含以下核心属性：

版权所有©北京中科京云控股有限公司 2026-2028

- **基本信息**：资产名称、描述、分类、标签、提供者等
- **元数据**：数据结构、字段说明、数据格式、数据量等
- **存储信息**：存储位置、文件大小、加密方式等
- **安全属性**：数据分级、脱敏规则、访问控制策略等
- **血缘信息**：数据来源、加工历史、衍生关系等

数据资产支持多种存储后端，包括 MinIO 对象存储、PostgreSQL 数据库、外部 API 等，通过统一的抽象层屏蔽底层存储差异。

4.4.2 NDI 数据标识

VISOM WeiDAO TDS 为每个数据资产分配唯一的 NDI（National Data Identifier，国家数据标识）编码。NDI 是我国数据要素市场的统一数据标识标准，具有全国唯一性、不可篡改性、可解析性等特征。

NDI 标识的作用：

- **唯一标识**：在全国范围内唯一标识一个数据资产，便于跨域流通
- **可解析**：通过 NDI 可解析出数据资产的元数据、提供者、访问方式等信息
- **可追溯**：基于 NDI 可追踪数据的流转全链路，支持监管审计
- **互认互通**：遵循国家标准，不同数据交易场所、数据空间之间可互认互通

4.5 高性能缓存架构

4.5.1 设计背景与决策

在 v3.2 及之前版本，所有查询直接穿透到 PostgreSQL。随着数据资产登记量增长，组织和用户表的重复查询成为系统最大瓶颈——这两个实体变更频率极低，但查询频率极高，是教科书级的缓存适用场景。

VISOM WeiDAO TDS 选择 Redis + Redisson 作为分布式缓存方案，而非 Caffeine 等本地缓存方案。核心原因在于：11 个微服务分布在多个 JVM 进程中，本地缓存会导致严重的缓存一致性问题。集中式 Redis 是天然正确的选择。

维度	Caffeine (JVM 堆内)	Redisson (Redis)
多实例一致性	需额外同步机制	天然一致（集中式）
内存开销	每实例独立缓存，N×内存	共享 512MB，N×连接

版权所有©北京中科京云控股有限公司 2026-2028

失效传播	需消息广播	单点清除即全局生效
持久化	重启丢失	AOF 重启恢复
运维可见性	无独立监控	redis-cli INFO / Prometheus

4.5.2 缓存策略

缓存什么：单实体查询（getOrganization, getUser, getAsset, getContract, resolveDid），Key 为实体 ID 或唯一标识。这类查询命中率高、价值大。

不缓存什么：分页列表、聚合查询、搜索结果。这些结果集不稳定，缓存命中率低且内存消耗大。

驱逐时机：写操作成功后立即驱逐关联缓存。核心原则是"宁可多查一次数据库，绝不返回脏数据"。

全平台共设 7 个缓存命名空间，分别对应不同类型的实体：organizations、users、assets、contracts、didDocuments、assetsByNdi、contractsByOrg。

4.5.3 序列化陷阱与防护

Redisson 默认使用 JDK 序列化，所有被缓存的 Java 对象必须实现 java.io.Serializable。这是一个常见的故障点：tds-common 中的实体类新增字段或修改继承关系后，若下游服务仍从本地 Maven 仓库加载旧版 JAR，运行时会抛出序列化异常，导致所有@Cacheable 方法返回 500。

VISOM WeiDAO TDS 采取了三重防御措施：

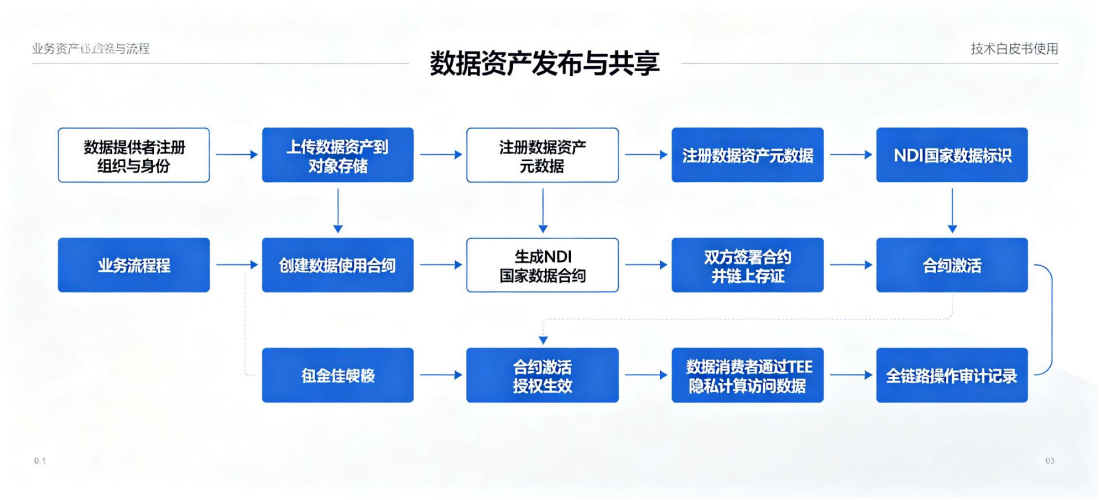
- CI/CD 中强制 mvn install -Dmaven.test.skip=true，确保所有服务使用最新版 JAR
- 启动脚本修正为 mvn install（v3.3 修订），避免编译不安装的问题
- 实体类显式声明 serialVersionUID = 1L，确保跨版本兼容

4.6 核心数据流

4.6.1 资产发布与共享流程

资产发布与共享是 VISOM WeiDAO TDS 的核心业务流程，涵盖从资产注册到数据使用的全链路：

版权所有©北京中科京云控股有限公司 2026-2028



4.6.2 缓存在流程中的角色

在资产发布与共享流程中，缓存扮演着重要角色。每一步"查询"都可能命中或回填缓存，每一步"写入"都触发相关缓存驱逐：

步骤	缓存影响
发现资产	assets::{id} 首次 MISS → 写 Redis
签署	contracts::{id} EVICT（驱逐）
激活	contracts::{id} EVICT（驱逐）
预签名	assets::{id} HIT（如果已缓存）
审计写入	不涉及业务缓存

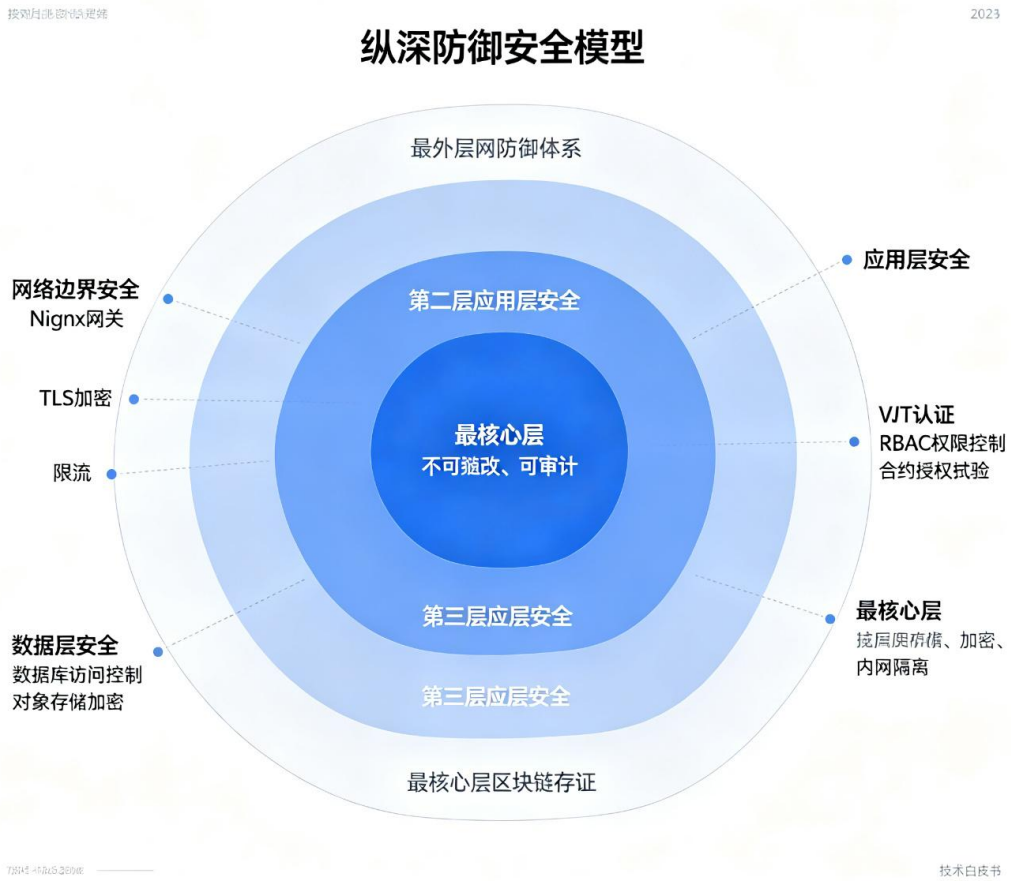
通过缓存与数据库的协同，系统在保证数据一致性的前提下，显著提升了查询性能，降低了数据库压力。

版权所有©北京中科京云控股有限公司 2026-2028

五、安全与合规体系

5.1 纵深防御安全模型

VISOM WeiDAO TDS 遵循零信任安全理念，构建多层次、纵深防御的安全体系。系统从外到内分为四个安全边界，每一层都有独立的安全防护机制，即使某一层被突破，仍有后续防线保障安全。



5.1.1 网络边界安全

最外层是网络边界安全，由 Nginx API 网关负责：

- **TLS 加密传输**：所有外部请求通过 HTTPS 访问，支持 TLS 1.3 协议，保障数据传输安全
- **流量控制**：基于 IP、用户、接口等多维度的限流策略，防止 DDoS 攻击与暴力破解
- **请求过滤**：限制请求大小（默认 100MB），过滤恶意请求，防止大文件攻击与注入攻击
- **路由隔离**：内部服务不直接暴露公网，所有请求必须经过网关转发

版权所有©北京中科京云控股有限公司 2026-2028

5.1.2 应用层安全

中间层是应用层安全，由每个微服务的 JwtAuthFilter 负责：

- **Token 独立验证**：每个微服务独立验证 JWT Token，不依赖网关鉴权。即使网关被绕过，鉴权依然生效
- **基于角色的访问控制（RBAC）**：支持 SUPER_ADMIN、PROVIDER、CONSUMER、AUDITOR 等多角色，实现精细化权限控制
- **合约授权校验**：数据访问必须验证合约状态，无合约或合约未激活则拒绝访问
- **输入校验**：所有输入参数进行严格校验，防止 SQL 注入、XSS 等常见攻击

5.1.3 数据层安全

最内层是数据层安全，由各存储组件负责：

- **PostgreSQL**：连接认证 + HikariCP 连接池化，最小权限原则分配数据库账号
- **MinIO**：对象级访问策略，预签名 URL 临时授权，数据静态加密
- **Redis**：内网绑定（bind 127.0.0.1），不暴露公网，密码认证
- **数据加密**：敏感数据存储加密，支持国密算法

5.2 数据全生命周期安全

VISOM WeiDAO TDS 对数据的采集、传输、存储、使用、共享、销毁全生命周期进行安全管控，确保数据在每个阶段都受到保护。

5.2.1 数据采集安全

- **来源可信**：数据提供者必须通过身份认证，确保数据来源可追溯
- **质量校验**：数据入库前进行格式校验、完整性校验、去重处理，确保数据质量
- **分类分级**：根据数据敏感度自动或手动分类分级，匹配相应的安全策略

5.2.2 数据传输安全

- **传输加密**：所有数据传输采用 TLS 1.3 加密，防止中间人攻击
- **预签名 URL**：文件下载使用 MinIO 预签名临时 URL，有效期可控，无需暴露永久凭证
- **完整性校验**：支持文件哈希校验，确保传输过程中数据未被篡改

5.2.3 数据存储安全

版权所有©北京中科京云控股有限公司 2026-2028

- **静态加密**：敏感数据存储加密，支持 AES-256 和国密 SM4 算法
- **访问控制**：基于角色与合约的双重访问控制，最小权限原则
- **备份恢复**：定期数据备份，支持快速恢复，保障数据可用性

5.2.4 数据使用安全

- **合约化授权**：数据使用必须经过合约授权，明确使用范围、期限、用途
- **隐私计算**：高敏感数据通过 TEE 隐私计算，实现"数据可用不可见"
- **脱敏处理**：根据数据分级与用户角色，自动进行数据脱敏

5.2.5 数据销毁安全

- **安全删除**：数据删除时彻底清除，不可恢复
- **销毁审计**：销毁操作全程记录，支持审计追溯

5.3 合规审计与追溯

5.3.1 全链路审计

VISOM WeiDAO TDS 构建了完善的审计体系，实现数据流通全链路可追溯。所有关键操作（用户登录、资产注册、合约签署、数据访问、计算任务等）均记录审计日志，存储于 OpenSearch，支持多维度查询与分析。

审计日志包含以下关键信息：

- **操作主体**：谁执行了操作（用户 ID、组织 ID、IP 地址）
- **操作对象**：操作了什么（资产 ID、合约 ID、数据范围）
- **操作类型**：执行了什么操作（查询、下载、计算、修改等）
- **操作时间**：何时执行的操作（精确到毫秒）
- **操作结果**：操作是否成功，返回结果摘要

5.3.2 链上存证审计

除了 OpenSearch 审计日志，关键操作（合约签署、资产登记、权限变更等）的哈希还会写入区块链，提供不可篡改的审计证据。链上存证与日志审计构成双重审计轨迹，相互印证，提升审计可信度。

链上存证的优势：

- **不可篡改**：区块链数据一旦上链，无法修改或删除

版权所有©北京中科京云控股有限公司 2026-2028

- **不可抵赖**：操作方无法事后否认操作行为
- **第三方可验证**：监管机构、审计机构可独立验证，无需依赖平台方

5.3.3 数据血缘追踪

Lineage 服务提供数据血缘追踪能力，记录数据从产生、流转、加工到使用的全链路关系。通过数据血缘可视化，用户可以清晰了解：

- 数据来自哪里（来源系统、原始数据）
- 数据经过了哪些加工处理（加工规则、处理过程）
- 数据被哪些方使用过（使用方、使用方式、使用时间）
- 数据衍生出了哪些新的数据产品（衍生关系、血缘链路）

数据血缘为数据质量评估、合规审计、影响分析提供了重要支撑。

5.4 等保与合规认证

VISOM WeiDAO TDS 在设计与开发过程中，严格遵循国家与行业的安全合规要求，积极对接相关认证标准：

- **网络安全等级保护**：按照等保 2.0 三级要求设计，满足政企客户的安全合规需求
- **数据安全法合规**：支持数据分类分级、数据安全评估、数据出口管制等要求
- **个人信息保护法合规**：支持个人信息去标识化、目的限定、最小必要等原则
- **国密算法支持**：支持 SM2/SM3/SM4 国密算法，满足国产化安全要求
- **金融行业合规**：满足金融行业数据安全监管要求，支持金融数据安全分级

版权所有©北京中科京云控股有限公司 2026-2028

六、典型应用场景

6.1 政务数据共享与开放

6.1.1 场景背景

政务数据是国家重要的数据资源，涵盖人口、法人、地理空间、宏观经济等多个领域。推动政务数据共享与开放，是提升政府治理能力、优化营商环境、促进数字经济发展的关键举措。然而，政务数据共享长期面临"不愿共享、不敢共享、不会共享"的困境——数据安全顾虑、权责不清、技术标准不统一等问题制约了政务数据价值的释放。

6.1.2 解决方案

VISOM WeiDAO TDS 为政务数据共享提供安全可信的技术基础设施：

- **数据可用不可见**：通过 TEE 隐私计算技术，政务数据"不搬家、不出域"，各部门可在不获取原始数据的前提下进行联合查询与分析，既保障数据安全，又实现数据价值共享
- **合约化授权管理**：数据共享通过智能合约授权，明确数据使用范围、期限、用途，实现精细化、可追溯的授权管理
- **全链路审计追溯**：所有数据操作全程记录，关键操作链上存证，满足政务审计与监管要求
- **统一数据目录**：构建统一的政务数据资产目录，实现数据资源的标准化管理与快速发现

6.1.3 应用价值

通过 VISOM WeiDAO TDS 构建政务数据空间，可实现：

- **提升治理效率**：打破部门数据壁垒，实现"数据多跑路、群众少跑腿"，提升政务服务效率
- **保障数据安全**：数据不出域、可用不可见，从技术上消除数据安全顾虑
- **强化监管能力**：全链路可追溯，监管部门可实时掌握数据流转情况，提升监管效能
- **促进数据开放**：在安全可控的前提下，有序推动政务数据向社会开放，赋能数字经济发展

6.2 金融数据要素流通

版权所有©北京中科京云控股有限公司 2026-2028

6.2.1 场景背景

金融行业是数据密集型行业，数据是金融机构的核心资产。然而，金融数据涉及大量敏感信息，受严格的监管约束，数据流通面临诸多限制。一方面，中小金融机构数据积累不足，难以有效开展风控、营销等业务；另一方面，数据拥有方担心数据泄露与合规风险，不敢轻易共享数据。

6.2.2 解决方案

VISOM WeiDAO TDS 为金融数据要素流通提供安全合规的解决方案：

- **联合风控建模**：多家金融机构通过 TEE 联邦学习，在不共享原始数据的前提下联合构建风控模型，提升模型准确性
- **多头借贷查询**：通过隐私计算技术，在不泄露用户隐私的前提下查询用户在多家机构的借贷情况，防范过度授信风险
- **反欺诈协作**：金融机构间安全共享黑名单、欺诈特征等信息，联合打击金融欺诈
- **合规审计支撑**：全链路审计与链上存证，满足金融监管的数据安全与审计要求

6.2.3 应用价值

- **提升风控能力**：通过多方数据联合建模，显著提升风控模型的准确性与覆盖度
- **降低合规风险**：数据不出域、可用不可见，从技术上满足数据安全与隐私保护法规要求
- **促进普惠金融**：帮助中小金融机构获得更全面的数据支撑，提升服务小微企业与个人的能力
- **激活数据价值**：在合规前提下实现金融数据要素的市场化配置，释放数据价值

6.3 医疗健康数据协作

6.3.1 场景背景

医疗健康数据具有极高的科研与商业价值，是精准医疗、药物研发、健康管理等领域的关键生产要素。然而，医疗数据涉及患者隐私，受《个人信息保护法》《医疗卫生机构网络安全管理办法》等严格监管。医疗数据分散在各家医院、体检机构、保险公司，形成数据孤岛，难以有效利用。

6.3.2 解决方案

VISOM WeiDAO TDS 为医疗健康数据协作提供安全可信的技术平台：

版权所有©北京中科京云控股有限公司 2026-2028

- **多中心科研协作**：多家医院通过隐私计算技术联合开展临床研究，在不共享原始病历的前提下进行多中心数据分析，加速医学研究进程
- **药物真实世界研究**：药企与医院合作，利用真实世界数据开展药物疗效与安全性研究，缩短药物研发周期
- **健康管理服务**：体检机构、保险公司、健康管理公司安全共享健康数据，为用户提供个性化健康管理服务
- **医保智能审核**：医保部门与医疗机构安全共享诊疗数据，实现医保费用智能审核，防范医保欺诈

6.3.3 应用价值

- **保护患者隐私**：数据不出院、可用不可见，从技术上保障患者隐私安全
- **加速医学创新**：打破医疗机构数据壁垒，促进多中心科研协作，加速医学创新
- **降低研发成本**：利用真实世界数据开展研究，降低药物研发成本与周期
- **提升医疗质量**：通过数据驱动的精准医疗，提升诊疗效果与医疗服务质量

6.4 工业数据空间

6.4.1 场景背景

工业互联网时代，工业数据呈现爆发式增长。设备数据、生产数据、供应链数据等工业数据蕴含着巨大价值，是智能制造、工业互联网的核心要素。然而，工业数据分布在设备厂商、生产企业、供应链上下游等多个主体，数据孤岛严重，难以实现跨主体的数据协同与价值挖掘。

6.4.2 解决方案

VISOM WeiDAO TDS 为工业数据空间建设提供技术支撑：

- **设备数据共享**：设备厂商与生产企业安全共享设备运行数据，实现设备预测性维护与远程运维
- **质量协同分析**：产业链上下游共享质量数据，联合分析质量问题根源，提升整体产品质量
- **工艺优化协作**：工艺设计方与生产方通过隐私计算联合优化工艺参数，提升生产效率
- **供应链协同**：供应链上下游企业安全共享库存、物流、需求等数据，提升供应链协同效率

版权所有©北京中科京云控股有限公司 2026-2028

6.4.3 应用价值

- **提升生产效率**：通过数据驱动的工艺优化与设备运维，提升生产效率与设备利用率
- **降低运营成本**：预测性维护减少设备故障停机，供应链协同降低库存成本
- **保护商业秘密**：工艺参数、生产数据等敏感信息不出域，保护企业商业秘密
- **促进产业协同**：打通产业链数据壁垒，促进产业协同与数字化转型

6.5 供应链数据协同

6.5.1 场景背景

现代供应链体系复杂，涉及供应商、制造商、分销商、零售商等多个主体。供应链数据协同是提升供应链效率、降低成本、应对风险的关键。然而，供应链各参与方之间缺乏信任，数据共享顾虑重重——担心核心数据泄露、担心被上下游企业利用、担心数据安全责任不清等问题制约了供应链数据协同。

6.5.2 解决方案

VISOM WeiDAO TDS 为供应链数据协同构建可信数据空间：

- **需求预测协同**：上下游企业通过隐私计算联合进行需求预测，在不泄露各自商业数据的前提下提升预测准确性
- **库存共享与调度**：供应链伙伴安全共享库存数据，实现库存优化与协同调度，降低整体库存水平
- **供应商风险评估**：核心企业与金融机构安全共享供应商数据，联合评估供应商信用风险与履约能力
- **溯源与防伪**：通过区块链与数据空间技术，实现商品全链路溯源，防范假冒伪劣

6.5.3 应用价值

- **降低供应链成本**：通过需求协同与库存优化，降低库存成本与缺货损失
- **提升响应速度**：数据协同提升供应链透明度与响应速度，增强供应链韧性
- **保护商业机密**：敏感数据不出域、可用不可见，保护各参与方的商业机密
- **建立信任机制**：合约化授权与全链路审计，建立供应链参与方之间的信任机制

版权所有©北京中科京云控股有限公司 2026-2028

七、性能与可伸缩性

7.1 性能指标与基准

VISOM WeiDAO TDS 在设计与开发过程中，始终将性能作为核心考量因素。通过缓存优化、连接池管理、异步处理等多种技术手段，确保系统在高并发场景下仍能保持稳定的响应性能。

7.1.1 连接池预算

系统对各类资源连接进行精细化管理，确保资源利用效率与系统稳定性的平衡。

资源	每服务	× 服务数	总计
HikariCP 到 PostgreSQL	max 5, min 2	11	~55 连接
Redisson 到 Redis	~24	11	~264 连接

PostgreSQL 默认 max_connections = 100，55 个连接在安全范围内，留有充足余量应对突发流量。Redis 单线程模型处理 264 个连接无压力——每个连接的健康检查是 O(1)的，不会成为性能瓶颈。

7.1.2 缓存命中率预期

缓存是提升系统性能的关键手段。在稳态运行下，各缓存命名空间的预期命中率如下：

缓存命名空间	预期命中率	依据
organizations	> 95%	组织信息极少变更，查询频率高
users	> 90%	用户变更频率低，认证查询频繁
contracts	> 80%	合约签署/激活时驱逐，其余时间稳定
assets	> 85%	资产发布后较稳定，查询频繁
didDocuments	> 99%	DID 文档几乎不变，解析查询频繁

版权所有©北京中科京云控股有限公司 2026-2028

通过 Redis 缓存，高频查询请求可直接从缓存返回，大幅降低数据库压力，提升系统整体吞吐量。

7.2 水平扩展能力

VISOM WeiDAO TDS 采用云原生微服务架构，支持水平扩展，可根据业务需求灵活调整资源规模。

7.2.1 无状态服务扩展

核心业务服务（IAM、Org、Asset、Contract 等）均为无状态设计，会话信息存储在 Redis 中，支持水平扩展。在 K8s 生产部署中，核心服务默认配置 2 副本，可根据负载自动扩缩容。

当副本数增加时：

- **缓存命中率不变**：所有副本指向同一 Redis 实例，缓存集中管理
- **数据库连接数线性增加**：需关注 PostgreSQL 连接上限，必要时升级数据库规格或引入连接池中间件
- **Redis 连接数线性增加**：264 × 副本系数，Redis 单实例可轻松支撑

7.2.2 缓存层扩展

当前采用 Redis 单实例架构，512MB / 1GB 内存可支撑 10 万级缓存键，满足中小规模部署需求。当缓存容量或性能成为瓶颈时，可演进到以下架构：

- **Redis 哨兵模式**：实现主从复制与自动故障转移，消除缓存单点，提升可用性
- **Redis Cluster**：数据分片存储，突破单实例内存与性能上限，支撑大规模部署

7.2.3 数据库扩展

PostgreSQL 作为核心数据存储，可通过以下方式扩展：

- **读写分离**：主库负责写入，从库负责查询，提升读性能
- **分库分表**：按组织或业务域分库分表，支撑超大规模数据量
- **NewSQL 迁移**：极端场景下可迁移到 TiDB 等分布式 NewSQL 数据库

7.3 高可用设计

VISOM WeiDAO TDS 在架构设计中充分考虑高可用性，确保系统稳定可靠运行。

7.3.1 服务高可用

版权所有©北京中科京云控股有限公司 2026-2028

- **多副本部署**：核心服务多副本部署，单实例故障不影响整体服务
- **健康检查**：Spring Actuator 提供健康检查端点，K8s 根据健康状态自动调度
- **优雅启停**：支持优雅上下线，确保请求处理完整，避免数据丢失

7.3.2 数据高可用

- **数据库主从**：PostgreSQL 主从复制，主库故障可快速切换
- **对象存储多副本**：MinIO 支持纠删码与多副本，数据可靠性有保障
- **定期备份**：支持全量与增量备份，可快速恢复数据

7.3.3 链路高可用

- **网关集群**：Nginx 网关集群部署，避免单点故障
- **服务熔断降级**：非核心服务故障时自动降级，保障核心链路可用
- **限流保护**：多维度限流机制，防止系统过载雪崩

版权所有©北京中科京云控股有限公司 2026-2028

八、运维与部署体系

8.1 部署架构

VISOM WeiDAO TDS 支持多种部署方式，可根据企业规模与 IT 基础设施灵活选择。

8.1.1 部署模式

部署模式	适用场景	特点
Docker Compose	开发测试、小规模部署	部署简单、资源占用少、一键启停
Kubernetes	生产环境、中大规模部署	高可用、弹性伸缩、自动化运维
私有化部署	对数据安全要求高的政企客户	数据完全可控、可定制化集成
SaaS 服务	中小企业、快速上线需求	开箱即用、按需付费、免运维

8.1.2 一键启停脚本

VISOM WeiDAO TDS 提供完善的部署脚本，支持一键启停与状态监控：

```bash
部署脚本使用示例 cd deploy/scripts
./start.sh                    # 启动基础设施 + 11 个服务 + 前端
./status.sh --watch           # 实时监控面板
./restart.sh --backend --rebuild   # 重新编译并重启后端
./stop.sh                     # 停止所有服务
```

脚本化部署大幅降低了部署门槛，开发人员可在几分钟内搭建完整的开发测试环境。

8.2 可观测性体系

VISOM WeiDAO TDS 构建了完善的可观测性体系，覆盖基础设施、中间件、应用等多个层次，确保系统运行状态可监控、可追溯、可诊断。

版权所有©北京中科京云控股有限公司 2026-2028

层次	工具	覆盖范围
基础设施	Prometheus (:9090)	容器 CPU/内存/网络、节点资源使用率
Redis	redis-cli INFO / Prometheus Exporter	缓存命中率、内存使用、连接数、QPS
应用	Spring Actuator /actuator/health	每服务健康状态、接口响应时间、错误率
审计	OpenSearch (:9200)	全量操作日志、审计查询、合规报表
日志	logs/tds-*.log	集中日志目录，支持 ELK/EFK 集成

8.2.1 监控告警

通过 Prometheus + Grafana 构建统一监控面板，实时展示系统运行状态。支持多维度告警规则，当系统出现异常时（如服务宕机、响应超时、错误率飙升、资源使用率过高等），及时通过邮件、短信、企业微信等渠道通知运维人员。

8.2.2 日志管理

所有服务日志统一输出到 logs 目录，按服务与日期分割。支持集成 ELK/EFK 日志分析平台，实现日志的集中收集、检索与分析，便于问题排查与安全审计。

8.2.3 链路追踪

v3.5 版本计划引入 OpenTelemetry 全链路追踪，实现请求在各微服务间的调用链路可视化，帮助开发人员快速定位性能瓶颈与错误根源。

8.3 数据库迁移与版本管理

VISOM WeiDAO TDS 采用 Flyway 进行数据库版本化管理，确保数据库 schema 的可追溯与可重现。

8.3.1 Flyway 迁移机制

迁移文件存放在 db/migrations/目录，遵循

 版权所有©北京中科京云控股有限公司 2026-2028

V<major>.<minor>.<patch>__description.sql 命名规范，与平台版本号对齐。Docker 启动时自动执行未应用的迁移脚本，确保数据库 schema 与应用版本保持一致。

Flyway 的核心优势：

- **版本化管理**：每个 schema 变更都有对应的版本号，可追溯、可回滚
- **自动执行**：应用启动时自动检测并执行未应用的迁移，无需人工操作
- **幂等安全**：已执行的迁移不会重复执行，确保数据库状态一致
- **多环境一致**：开发、测试、生产环境使用相同的迁移脚本，保证 schema 一致性

8.3.2 数据迁移策略

对于涉及数据迁移的版本升级，采用"双写+灰度"的策略：

1. 新增字段或表，新旧代码同时兼容
2. 灰度发布，逐步切换到新逻辑
3. 全量切换后，清理旧字段与冗余数据

这种策略确保升级过程对业务无感知，降低升级风险。

8.4 运维最佳实践

8.4.1 日常运维

- **定期备份**：数据库与对象存储定期备份，备份数据异地存储
- **容量监控**：监控磁盘、内存、连接数等资源使用情况，提前扩容
- **安全补丁**：及时修复安全漏洞，更新依赖组件版本
- **日志轮转**：配置日志自动轮转与清理，避免磁盘占满

8.4.2 故障处理

- **故障自愈**：K8s 自动重启异常 Pod，服务自动恢复
- **降级预案**：非核心服务故障时自动降级，保障核心业务可用
- **快速回滚**：支持版本快速回滚，降低发布失败影响
- **应急预案**：针对数据库故障、缓存雪崩、网络中断等场景制定应急预案

版权所有©北京中科京云控股有限公司 2026-2028

九、技术栈选型

9.1 技术选型原则

VISOM WeiDAO TDS 在技术选型过程中，始终遵循以下原则：

- **成熟稳定优先**：优先选择经过大规模生产验证的成熟技术，降低技术风险
- **社区生态活跃**：选择社区活跃、文档丰富的开源项目，便于问题排查与持续演进
- **团队技术栈匹配**：结合团队技术背景，选择团队熟悉的技术，提升开发效率
- **国产化兼容**：支持国产操作系统、数据库、中间件，满足信创要求
- **可扩展性**：选择具备良好扩展性的技术架构，支撑业务持续发展

9.2 核心技术栈

技术选择	版本	备选方案	选择理由
Spring Boot	3.3.5	Quarkus, Micronaut	团队熟悉度高、生态成熟、Spring Cache 无缝集成、社区资源丰富
Redisson	3.36	Lettuce, Jedis	唯一内置 Spring Cache 自动配置的客户端，统一全平台 Redis 访问，支持分布式锁等高级特性
PostgreSQL	16	MySQL 8, MongoDB	强 schema 约束符合"数据资产"场景（schema 即合约），JSONB 兼顾灵活性，支持复杂查询与事务
MinIO	最新	Ceph, HDFS	S3 兼容、单二进制部署、K8s 友好、性能满足中小规模需求、运维简单
FISCO BCOS	最新	Hyperledger Fabric	国产化合规、单节点开发模式零配置、Java SDK 原生、国内社区活跃

版权所有©北京中科京云控股有限公司 2026-2028

Nginx	最新	APISIX, Envoy	开发/测试环境部署最简单，性能稳定可靠；APISIX 已预留为生产升级路径
OpenSearch	2.x	Elasticsearch	开源友好、与 ES 兼容、功能丰富、满足审计日志检索需求
JDK 序列化	-	Jackson JSON, Protobuf	与 Spring Cache 默认行为一致，无需额外配置；可升级到 Kryo 提升性能
Flyway	最新	Liquibase	简单易用、与 Spring Boot 集成好、满足数据库版本管理需求

9.3 关键技术选型详解

9.3.1 为什么选择 PostgreSQL 而非 MySQL

在关系型数据库选型上，VISOM WeiDAO TDS 最终选择了 PostgreSQL 16，主要基于以下考量：

第一，强 schema 约束更符合数据资产场景。数据空间的核心是"合约"，schema 本身就是合约的一部分。PostgreSQL 的强类型系统与丰富的约束能力，能够更好地保证数据一致性与完整性。

第二，JSONB 兼顾灵活性。对于元数据、扩展属性等半结构化数据，PostgreSQL 的 JSONB 类型提供了与 MongoDB 相当的灵活性，同时保持关系型数据库的事务与查询能力。

第三，复杂查询支持更好。PostgreSQL 对复杂 SQL、窗口函数、CTE 等特性的支持更完善，能够更好地支撑审计、统计分析等复杂查询场景。

第四，国产化生态完善。PostgreSQL 在国内有大量的开源社区与商业支持，基于 PostgreSQL 的国产数据库（如人大金仓、瀚高）也较为成熟，便于信创适配。

9.3.2 为什么选择 Redisson 而非 Lettuce

项目原本的计量服务（metering）已使用 Redisson。统一整个平台到同一个客户端有多重收益：

- **减少依赖碎片化**：一种客户端，一套连接池，一类序列化方式，降低维护成本
- **Spring Cache 自动集成**：Redisson 的 redisson-spring-boot-starter 自动集成

版权所有©北京中科京云控股有限公司 2026-2028

Spring Cache 抽象，配置简单

- **高级数据结构支持**：支持分布式锁、RMap、RAtomicLong 等高级数据结构，为后续分布式能力铺路
- **连接池优化**：Redisson 的连接池管理比 Lettuce 更成熟，在高并发场景下表现更稳定

9.3.3 为什么选择 FISCO BCOS

在联盟链选型上，VISOM WeiDAO TDS 选择了 FISCO BCOS，主要基于国产化与易用性的考量：

- **国产化合规**：FISCO BCOS 是国内主导的联盟链平台，符合国家区块链技术标准与监管要求
- **开发友好**：单节点开发模式零配置，快速搭建开发测试环境，提升开发效率
- **Java SDK 原生**：官方提供完善的 Java SDK，与 Spring Boot 技术栈无缝集成
- **国内社区活跃**：国内社区活跃，文档与案例丰富，问题响应及时

9.4 国产化适配

VISOM WeiDAO TDS 积极适配国产化技术栈，满足政企客户的信创需求：

- **操作系统**：支持麒麟、统信等国产操作系统
- **数据库**：支持人大金仓、达梦、瀚高等基于 PostgreSQL 的国产数据库
- **中间件**：支持东方通、金蝶等国产应用服务器
- **密码算法**：支持 SM2/SM3/SM4 国密算法，满足密码应用安全要求
- **芯片架构**：支持 x86、ARM、龙芯、鲲鹏等多种 CPU 架构

通过全面的国产化适配，VISOM WeiDAO TDS 能够满足政府、金融、能源等关键行业的信创建设需求。

版权所有©北京中科京云控股有限公司 2026-2028

十、生态与合作

10.1 生态战略

可信数据空间是数据要素市场化的基础设施，其价值与网络效应直接相关——接入的参与方越多、数据资源越丰富，平台的价值就越大。因此，VISOM WeiDAO TDS 始终坚持开放合作的生态战略，致力于构建共建共享共赢的数据要素生态体系。

VISOM WeiDAO TDS 的生态战略遵循三个核心原则：

- **开放兼容**：遵循国家标准与行业规范，提供标准化接口，支持多源异构数据接入，兼容主流技术栈
- **共建共享**：与合作伙伴共同建设数据空间生态，共享技术成果与商业机会
- **价值共赢**：构建合理的价值分配机制，让生态参与各方都能从中获益

10.2 技术生态

10.2.1 标准化对接

VISOM WeiDAO TDS 积极对接国家与行业标准，确保平台的开放性与互操作性：

- **数据标识标准**：支持 NDI 国家数据标识，实现跨平台数据互认
- **DID 身份标准**：遵循 W3C DID 标准，支持去中心化身份互认
- **隐私计算标准**：支持 TEE、联邦学习等多种隐私计算技术标准
- **区块链标准**：遵循区块链参考架构、智能合约等国家标准
- **数据安全标准**：符合数据分类分级、数据安全能力成熟度等标准

10.2.2 技术合作伙伴

VISOM WeiDAO TDS 与各类技术厂商建立深度合作，共同完善技术生态：

基础设施厂商：与云厂商、服务器厂商、操作系统厂商合作，优化平台在各类基础设施上的部署与性能表现。

隐私计算厂商：与 TEE 厂商、联邦学习厂商、安全多方计算厂商合作，整合多种隐私计算技术，提供更丰富的计算能力。

区块链厂商：与各类联盟链平台对接，支持多链部署与跨链互操作。

安全厂商：与安全厂商合作，整合身份认证、数据加密、安全审计等能力，提升平台整体安全水平。

版权所有©北京中科京云控股有限公司 2026-2028

10.2.3 开源社区

VISOM WeiDAO TDS 计划逐步开源核心组件，回馈开源社区：

- 开源数据空间核心协议与 SDK，降低接入门槛
- 参与开源社区建设，贡献代码与最佳实践
- 举办技术沙龙与开发者大会，促进技术交流
- 建立开发者社区，培育数据空间技术人才

10.3 产业生态

10.3.1 行业合作伙伴

VISOM WeiDAO TDS 与各行业的龙头企业合作，共同推进行业数据空间建设：

政务领域：与地方政府、政务服务机构合作，建设政务数据共享与开放平台，提升公共数据开发、开放能力。

金融领域：与银行、保险、证券等金融机构合作，建设金融数据要素流通平台，赋能金融创新与风险防控。

医疗领域：与医院、药企、科研机构合作，建设医疗健康数据空间，促进医学研究与精准医疗。

工业领域：与制造企业、工业互联网平台合作，建设工业数据空间，推动智能制造与产业升级。

10.3.2 数据交易场所合作

VISOM WeiDAO TDS 与各地数据交易场所建立合作，为数据交易提供可信流通技术支撑：

- 提供数据资产登记、确权、评估等技术能力
- 提供数据可信流通与交付技术方案
- 提供数据使用计量与计费技术支撑
- 提供合规审计与监管技术手段

通过与数据交易场所的合作，共同构建规范有序的数据要素市场。

10.3.3 科研与学术合作

VISOM WeiDAO TDS 与高校、科研院所建立产学研合作关系：

版权所有©北京中科京云控股有限公司 2026-2028

- 联合开展数据空间关键技术研究
- 共同制定技术标准与行业规范
- 培养数据要素领域专业人才
- 共建联合实验室与创新中心

10.4 生态赋能计划

为推动生态繁荣发展，VISOM WeiDAO TDS 推出生态赋能计划：

技术赋能：为合作伙伴提供技术培训、认证支持、解决方案咨询等服务，帮助合作伙伴快速掌握数据空间技术。

商业赋能：与合作伙伴共享市场机会，联合拓展客户，共同打造行业解决方案。

品牌赋能：通过市场活动、媒体宣传、案例推广等方式，提升合作伙伴的品牌影响力。

资本赋能：对接投资机构，为优质生态创业项目提供资本对接与孵化支持。

通过全方位的生态赋能，与合作伙伴共同成长，共建繁荣的数据要素生态。

版权所有©北京中科京云控股有限公司 2026-2028

十一、演进路线

11.1 版本演进策略

VISOM WeiDAO TDS 采用"小步快跑、持续迭代"的版本演进策略，每个版本聚焦特定的主题，逐步完善平台能力。版本号遵循语义化版本规范（Semantic Versioning），主版本号代表架构级变更，次版本号代表功能增强，修订号代表 bug 修复与性能优化。

演进路线的规划遵循以下原则：

- **价值导向**：每个版本都聚焦为用户创造实实在在的价值，不做无意义的功能堆砌
- **架构先行**：先夯实基础架构，再扩展上层功能，确保系统的稳定性与可扩展性
- **标准对齐**：紧跟国家与行业标准，确保平台的合规性与互操作性
- **生态共建**：与合作伙伴共同规划路线图，吸纳社区反馈，共建共享

11.2 当前版本（v3.3）— 缓存就绪

v3.3 是当前发布的稳定版本，主题是"缓存就绪"，重点解决系统性能瓶颈问题。

核心特性：

- Redis/Redisson 全平台集成，统一分布式缓存方案
- 4 个核心服务（IAM、Org、Asset、Contract）启用 Spring Cache
- 7 个缓存命名空间，精细化缓存管理
- 完善的缓存驱逐策略，保证数据一致性
- K8s 部署清单与资源规划，支撑生产级部署
- 修复 JDK 序列化陷阱，完善 CI/CD 流程

适用场景：中小规模数据空间建设、开发测试环境、POC 验证项目

11.3 近期规划（v3.4）— 分布式增强

v3.4 计划于 2026 年 Q3 发布，主题是"分布式增强"，重点提升系统的分布式能力与高可用性。

规划特性：

- **Redisson 分布式锁**：防止合约并发签署、资产重复注册等并发问题
- **Redis 哨兵模式**：实现 Redis 主从复制与自动故障转移，消除缓存单点

版权所有©北京中科京云控股有限公司 2026-2028

- **缓存预热策略**：服务启动时加载热点数据，避免冷启动缓存击穿
- **分布式事务**：引入 Seata 等分布式事务框架，保证跨服务数据一致性
- **接口幂等性**：完善接口幂等性设计，防止重复提交

目标：支撑更大规模的并发访问，提升系统稳定性与可靠性

11.4 中期规划（v3.5）— 网关升级

v3.5 计划于 2026 年 Q4 发布，主题是"网关升级"，重点提升接入层能力与可观测性。

规划特性：

- **Nginx → APISIX 迁移**：动态路由、插件体系、更丰富的流量控制能力
- **全链路追踪**：引入 OpenTelemetry，实现请求全链路追踪与性能分析
- **统一监控面板**：Grafana 统一监控面板，整合基础设施、应用、业务指标
- **告警体系完善**：多维度告警规则、多渠道通知、告警收敛与降噪
- **API 网关安全**：WAF、防爬虫、API 鉴权增强等安全能力

目标：提升平台的可观测性与运维效率，支撑生产级运维需求

11.5 远期展望（v4.0）— 多方数据空间

v4.0 计划于 2027 年发布，主题是"多方数据空间"，重点实现跨组织、跨平台的数据空间互联互通。

规划特性：

- **跨组织 DID 互认**：支持不同数据空间之间的身份互认与信任传递
- **分布式合约引擎**：多链协同、跨链合约，支撑多方数据协作
- **隐私计算联邦节点**：支持联邦学习、安全多方计算等隐私计算技术
- **数据空间互联协议**：制定并实现数据空间互联标准，实现跨平台数据流通
- **数据资产跨境流通**：支持数据跨境安全评估与合规流通

目标：构建全国乃至全球范围的数据空间网络，实现数据要素的大规模流通与价值释放

11.6 长期愿景

展望未来，VISOM WeiDAO TDS 将持续演进，致力于成为数据要素市场化的关键基础设施：

- **技术领先**：持续跟踪前沿技术，保持技术架构的先进性与竞争力

版权所有©北京中科京云控股有限公司 2026-2028

- **标准引领**：积极参与国家与行业标准制定，引领数据空间技术发展方向
- **生态繁荣**：构建开放共赢的产业生态，让更多参与方共享数据要素红利
- **价值释放**：通过技术创新，充分释放数据要素价值，赋能数字经济高质量发展

数据是数字经济时代的核心生产要素，可信数据空间是释放数据要素价值的关键基础设施。中科京云伟道可信数据空间（VISOM WeiDAO TDS）以"合约化授权、隐私计算、链上存证、全链路审计"为核心技术特征，构建了"数据可用不可见、可控不可改、全程可追溯"的数据流通环境，为数据要素市场化配置提供了安全、高效、可信的技术解决方案。

本白皮书系统阐述了 VISOM WeiDAO TDS 的设计理念、系统架构、核心技术、安全体系与应用实践。我们相信，通过技术创新与制度创新的协同推进，可信数据空间将在政务、金融、医疗、工业、供应链等多个领域发挥重要作用，打破数据孤岛，释放数据价值，推动数字经济高质量发展。

数据要素市场的建设是一项长期而艰巨的任务，需要政府、企业、科研机构等多方力量的共同参与。中科京云伟道愿与各界合作伙伴一道，秉持开放合作的理念，共同推进可信数据空间技术创新与产业应用，共建繁荣的数据要素生态，为数字中国建设贡献力量。

北京中科京云控股有限公司

2026 年 6 月

版权所有©北京中科京云控股有限公司 2026-2028