申万宏源证券有限公司

权益类场外衍生品网厅系统

实施方案

信息技术开发总部

2023/5/4

文档信息

文档编号	
创建日期	2023/5/4
作者	

修订记录

版本号	日期	描述	修改者
V0.1	2023/5/4	文档创建	刘悦

注：V1.0 为 IT 内部沟通确认的发布版，后续如果更新实施方案模板，需要提交完整的实施方案并注明变动的内容，并以 V2.0，V3.0 等整数序号发出。

1 项目目标

1.1 文档目的

项目总体方案设计是项目总体实施方案的技术部分内容，以需求说明书为输入，从应用、数据、安全、技术四个角度进行高阶架构设计，并说明项目的实施方式，估算初步的成本，是项目立项评审、概要设计的依据。

1.2 预期读者

权益类场外衍生品网厅系统前期筹备人员、需求分析人员、系统设计人员、立项评审人员、其他相关技术架构设计人员。

1.3 术语定义

信息技术应用创新产业 简称 信创

场外衍生品交易管理系统 简称 BCT

1.4 项目背景

1.4.1 需求背景

近年来，公司金融创新总部的权益类场外衍生品业务迅速发展，跻身并保持行业头部位置。在当前阶段，对于场外期权询报价、跨境互换交易等场景，仍存在需要与客户线下沟通确认的环节，对面向更多客户，尤其是海量中小规模客户的展业产生了明显的制约。

随着场外市场越发成熟，涌入很多中小客户，经调研不少中小客户利用网厅交易下单、办理业务的需求强烈，对期权个股标的产生了越来越广泛的灵活交易诉求，同时提出了大量跨境互换的诉求，同时有大量客户提出需要提升客户服务体验可查询交易信息等，行业内中信、中信建投等头部券商的衍生品网厅已相对成熟，当前我司金融创新总部互换网厅仅支持境内互换业务，迫切扩展网厅功能，整合形成期权、互换及跨境业务需要的一站式服务平台。

在互换业务方面，我司前期已经建设了互换对客网厅，但该系统当前仅能支持境内互换业务，无法支持跨境互换业务，相关业务功能行业内头部机构通常采用自主研发的方式实现，具有较强的保密需要，该部分功能建议由我司组织技术人员进行自主研发。

在期权业务方面（包括期权询报价、定价引擎整合、订单管理和持仓管理等）计划通过采购的方式扩展期权业务相关功能。同时，考虑到未来业务发展中的个性化开发需要，同时要求供应商提供相关功能源码。

我国明确提出“数字中国”建设战略，并将信创产业纳入国家战略，提出“2+8”发展体系，我司也已将系统信创改造作为信息技术建设方面的重要目标和重点工作。本项目实施过程中，将进一步对系统进行信创化改造，建设更加安全可控的衍生品网厅系统。

1.4.2 建设目标

为进一步提高公司在衍生品行业的核心竞争力，快速响应客户需求，拓展创新业务模式，基于公司业务中台信创版容器云环境，搭建一套权益类场外衍生品网厅系统，实现期权询报价与跨境互换交易等业务的网厅操作，对接现有的 BCT 衍生品管理系统、互换对冲交易系统，实现权益类衍生品业务全流程一体化管理，同时在项目建设过程中完成信创化改造。

自研跨境互换业务的网厅核心功能，实现客户的交易委托下单，交易的分配与确认，客户额度的申请，以及资金、持仓及委托信息的查询。

新增期权类功能，支持期权的询报价（含定价引擎对接）、代客询价下单、BCT 簿记对接、持仓管理等功能。

2 需求概述

2.1 业务需求

2.1.1 网厅首页

通过卡片平铺方式展示客户“合约”维度的信息，支持通过“交易主体”、“合约编号”搜索，单笔合约信息支持查看详情，包括合约层级和标的物层级信

息，支持快速交易下单操作。同时汇总展示客户的可用预付金余额、预付金余额、总合约价值。

通过列表方式展示客户“标的”维度的信息，包括标的代码、标的方向、名义数量、成本均价、估值价格、待实现权益收益等。可支持按照“标的”搜索，按照“机构+标的+方向”进行汇总展示。同时支持根据标的维度做合约查询，查看对应标的下有持仓的合约相关详细信息，包括合约编号、起始日/到期日，标的期初价格，标的名义数量等。

2.1.2 互换交易管理

互换交易功能旨在打通境内外收益互换客户端到交易系统的下单通道，包括A股、港股、美股等，目前由于系统不完善，客户下单需通过线下邮件或微信的方式通知交易员，由交易员手动下单后再通过线下的方式将成交结果回复给客户；盘后客户对成交结果进行产品分配时也需要由交易员来代为操作并手动簿记录入盘后管理系统，在最终达成交易确认书之前整个交易前-交易中-交易后链路经历了繁杂的线下沟通和手工操作过程，不仅增加了交易的复杂度，还引入了操作风险。

网厅互换交易功能一方面为客户提供一个交互友好的前端界面，从用户的交易习惯出发设计前端功能；一方面对接交易系统，打通下单渠道，支持普通单、算法单，并在交易过程中做必要的事前风控，将风险拦截在交易系统之前。通过系统化的方式，上述一系列线下手工操作转化为可跟踪、可定位、可回溯的系统功能，减少了客户与交易员之间沟通成本的同时也大大降低了风险，将客户的交易与分配行为做标准化、规范化的限制。

除此之外，网厅还为客户提供了丰富的查询、数据可视化等功能，支持不同维度客户信息的查询，如合约信息、标的信息、订单信息、成交信息、资金信息、持仓信息等，支持统计数据和实时数据的展示，为客户提供了集交易、管理、查询等功能为一体的统一门户。

2.1.2.1. 互换交易委托

客户/交易员进入交易委托页面下单，可快速搜索标的，自动计算展示可用资

金及最大开仓数量。对于客户存在多个交易主体的情况，可按照指定不同比例分配进行下单。支持单笔买入、卖出及批量指令下单，批量下单方式支持通过文件上传导入。下单方式支持限价单和算法单（TWAP、VWAP、POV）等。交易页面支持交易白名单、额度信息搜索查询，可根据标的展示市场行情。同时支持查看当前资金、当前持仓、当日委托、成交记录；交易委托成功下达后，相应页面数据自动实时更新。在当日委托页面可进行撤单与批量撤单操作。因委托订单为 high-touch 模式，需交易员审批才能进入对冲台下单，对于交易员当日委托页面还支持审批与批量审批操作。

2.1.2.2. 互换交易确认

客户/交易员对当日委托的原始开仓/平仓订单，支持在盘后按交易主体/合约维度进行数量上的再次交易分配。分配后的结果需要提交交易员审批。盘后重新分配均支持单笔分配、批量分配操作，交易员确认页面也支持审批与批量审批操作。对于客户分配申请和交易员分配审批均有截止时间控制，在截止时间后不允许进行分配。审批后的订单流水会进入对冲交易清算系统，参与后续的流水对账、费用计算等流程。最终由对冲交易清算系统生成调仓文件，并导入 BCT 执行合约级别的调仓。

2.1.3 自定义期权配置管理

支持交易员灵活地自定义面向客户的期权询价及报价字段以及创建期权结构供客户发起询价。同时支持交易员配置常用的产品结构至策略库，供用户询价时进行便捷选择，如：配置香草平值看涨、雪球不追保 75-100 等策略至策略库，则对应策略将在客户的“发起询价”页面按结构列示，客户可直接点击策略，从而完成快捷询价。

2.1.4 期权询价管理

2.1.4.1. 快速询价

支持客户在“发起询价”页面实现便捷期权询价。针对权益香草和雪球期权，

支持客户同时选择多个标的（标的搜索支持拼音首字母搜索）、多个策略模板及期限，批量发起询价。在发起询价过程中，还有既定询价规模可供选择，客户可直接选择，或手动输入自己的实际询价规模。

2.1.4.2. 雪球自定义询价

支持客户在发起权益雪球结构询价时，既可以选择使用系统内展示的快速询价模板发起快速询价，又可以选择根据其实际所需要素发起自定义询价，大大提升了客户询价的可拓展性。

2.1.4.3. 询价单管理

支持查询和展示当日和历史的询价单信息，如标的、策略、到期日、询价时间、询价规模、报价价格等。同时支持买方用户查看询价单对应的历史报价记录。

2.1.5 期权报价管理

2.1.5.1. 手工报价

客户发起询价后，交易员将在“报价列表”实时查看到询价单信息。支持交易员依次手动填入报价要素对询价单进行手工报价，报价信息实时返回至客户客户端。

2.1.5.2. 多次报价

客户发起询价后，交易员将在“报价列表”实时查看到询价单信息。支持交易员依次手动填入报价要素对询价单进行手工报价，报价信息实时返回至客户客户端。

2.1.6 期权订单管理

2.1.6.1. 买方订单管理

支持客户在线下单，并支持多种进场方式，如：最新价、限价、TWAP、VWAP、收盘价等。完成下单操作后，支持用户查看当日和历史订单信息，如标的、策略、下单规模、进场价格、进场规模、进场方式、状态等。同时，支持用户修改订单以及对未确定的订单进行取消操作。

2.1.6.2. 卖方交易员订单管理

支持交易员查看当日和历史订单信息，如标的、策略、交易主体、下单规模、进场价格、进场规模、进场方式、状态等，并对订单进行确认。支持交易员对订单的下单规模、进场方式及进场价格（进场后）进行修改，同时支持交易员对未进场的订单进行取消并填写拒单原因。交易员亦可对申请取消的订单进行审核操作。如订单确认无误，支持交易员根据实际对冲情况填写对冲规模和价格等字段，完成进场。

2.1.7 期权合约簿记

交易达成时，通过网厅系统进场成交的订单，支持直接进入 BCT 管理系统。支持的结构包括欧式香草、美式香草、欧式价差、跨式、参与式期权、区间保护期权、单鲨、双鲨、保本雪球、非保本雪球、安全气囊等期权结构。

2.1.8 持仓管理

2.1.8.1. 基础查询

支持连通 BCT4 系统，客户可实时多条件查询和展示 BCT4 中客户自己的持仓。合约成交后，客户可在网厅查询持仓合约列表及持仓合约详情，如结构信息、基本交易信息等。并支持通过搜索栏筛选符合相关条件的交易。支持用户查看合约生命周期事件，如开仓、敲入敲出、平仓、结算等。

2.1.8.2. 灵活查询

支持持仓列表字段支持灵活拖拽展示，支持固定某列展示、调整列的顺序、隐藏某些列等。同时，支持买方客户分区域查看从 BCT4 获取的持仓合约详情信息，能够按结构信息、交易要素、生命周期等分区查看客户持仓详情。支持保存最近查看的交易详情，能够进行快捷切换查看。

2.1.9 风控设置

支持卖方配置网厅标的白名单。在客户发起询价时，卖方交易员可以接收位于白名单标的的询价单，并对非标的白名单内的标的询价单和订单进行拦截。

2.1.10 系统管理

2.1.10.1. 账号管理

提供维护系统各类用户信息并给用户授予角色权限、资源权限的功能。支持卖方管理员在网厅为客户创建对应的账号并关联至相应机构。支持从 BCT 同步已有的内部账号至网厅系统。并支持使用同名账号登录 BCT 后，点击对应菜单直接跳转至网厅系统，过程中无需再次输入密码。同时支持通过系统管理员创建独立的内部账号（独立的用户名及密码），进行网厅系统的登陆。

2.1.10.2. 资源组管理

支持针对不同的交易对手配置不同的数据资源。为特定用户分配资源组后，即可完成对此用户进行数据授权的操作。拥有特定资源组的用户可以以此交易主体的身份发起询价，并访问与之对应的交易数据等内容。

2.1.10.3. 资源组管理

系统提供管理角色配置的功能，支持获取 BCT 已有的卖方角色至网厅，并针对不同的角色配置不同的系统页面权限等。同时支持系统管理员创建新的买卖双

方角色，并对其页面权限进行配置，为用户设置与其岗位适配的角色。

2.1.11 信创支持

2.1.11.1. 注册中心信创支持

为响应国家信创国产化号召，系统设计之初，就优先从国产及开源社区进行架构选型。系统注册中心已完成国产化替代工作以及国产环境技术验证。系统服务注册中心、系统配置中心已通过阿里 NACOS 进行国产化替代。

2.1.11.2. 全面适配国产数据库 TDSQL

数据库方面，全面适配国产数据库 TDSQL，极大降低了在信创工作中对存量系统进行数据迁移、系统改造的操作难度和时间成本。同时，对系统有数据采集、数据推送需求时，其对接成本也能够显著降低。并且，该数据库在主从同步，数据拆分，弹性拓展方面拥有优秀的性能表现，为将来业务拓展和系统升级留有足够的升级空间。

2.1.12 二次开发支持

2.1.12.1. 后端灵活开发

期权后端全面采用微服务架构，用户管理，系统配置，询报价下单，BCT 集成，消息通知等多个模块均可独立部署运行，各司其职，协同工作。降低了系统的部署难度、运维成本和功能迭代周期，系统性能，稳定性更好，在业务发展速度快，需求迭代频繁的要求下，可以更加友好的进行二次开发。

2.1.12.2. 微前端灵活集成

基于 alibaba 开源技术 qiankun 构建前端基础框架与网厅主应用，网厅各子系统(期权、互换等)基于微前端技术体系开发，可做到不同业务开发团队互不影响，支持不同技术体系开发的子应用通过基础框架统一集成至主应用中，提供一

站式的用户体验、无需分别登录不同的系统。同时基于 oauth 权限管理体系可以对不同类型客户、部门/机构等做不同的页面权限控制。

2.2 非功能性需求

系统部署后能满足支撑并发用户数不低于 200 人，同时最大在线用户数 3000 人的要求。在不改变产品部署架构的前提下产品支持横向扩展以满足用户量和并发访问量增加的要求。

- ✧ 支持 5000+用户群体，3000 人同时在线，支持 200 个并发查询。
- ✧ 一般性事务响应时间不超过 5 秒，复杂查询事务响应时间不超过 20 秒。
- ✧ 每笔业务操作平均系统响应时间不超过 3 秒。
- ✧ RTO（系统恢复时间）：30 分钟内。
- ✧ RPO（系统恢复至运作允许丢失的数据量）：5 分钟内。

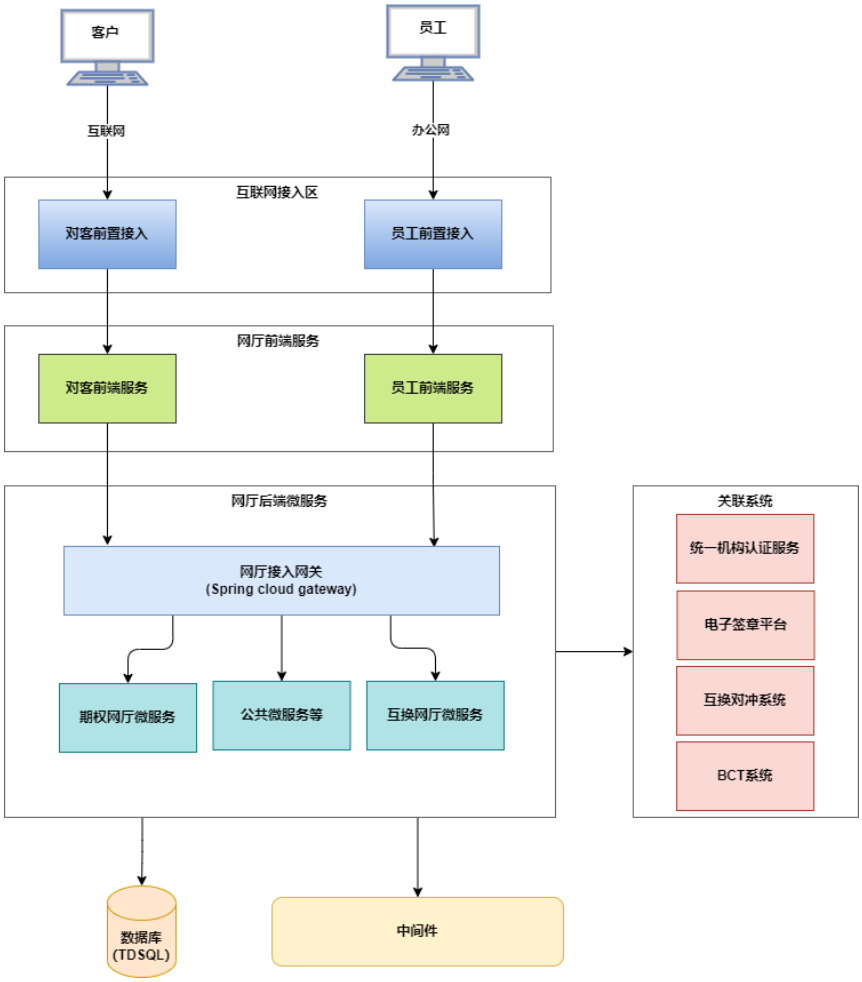
在满足当前业务需求的前提下，应充分考虑未来业务量及业务种类增长的需求，应用系统规模应具有可调性，新的软件模块、新业务的增加应尽可能在不影响系统运行的情况下实现。

3 应用架构

本章节描述系统的目标应用架构，具体包括:总体架构设计、应用功能架构、关键业务流程、相关系统交互、相关系统配合改造等。

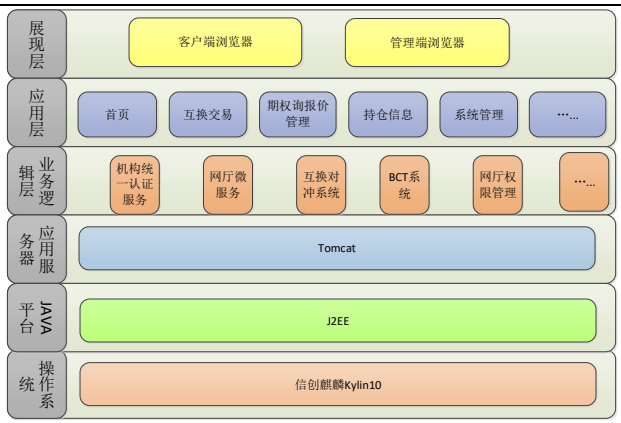
3.1 总体架构设计

权益类场外衍生品网厅系统负责场外期权和收益互换业务的对客处理和内部管理，实现权益类衍生品业务全流程一体化。系统基于信创容器云平台建设，外部客户通过互联网访问系统，内部员工通过办公网访问系统，均通过浏览器访问系统前置接入服务器，再通过前置接入服务器将请求转发至前端服务器，前端微服务通过网关进行身份认证与后台微服务进行交互；后台微服务负责处理主要业务逻辑，并与相关外部系统（包括“机构统一认证系统”、“电子签章平台”、“互换对冲系统”和“BCT 系统”）对接；其中微服务的部署复用中台现有的轻舟云集群资源，数据库采用 TDSQL，中间件集群单独申请机器部署。



权益类场外衍生品网厅系统总体架构图

3.2 应用功能架构



权益类场外衍生品网厅系统功能架构图

- 展现层：实现和最终用户的交互，通过 web 页面进行系统交互。展示层包括安全认证、操作日志等基础服务。
- 应用层：实现首页（包括合约与标的信息）、互换交易、期权询报价管理、持仓信息、系统管理等业务功能。
- 业务逻辑层：实现网厅系统的前后端功能开发以及与外部模块（机构统一认证服务、互换对冲系统、BCT 系统、网厅权限管理）之间的交互。
- 应用服务器：采用 Tomcat。
- JAVA 平台：采用 J2EE。
- 操作系统：采用信创麒麟 Kylin10。

业务功能模块如下：

功能模块		功能描述
员工端&管理端	首页	展示“合约”和“标的”维度相关信息
	互换交易	交易委托
		交易确认
	期权询报价管理	询价管理 报价管理 订单管理
	持仓信息	合约簿记 持仓展示
	系统管理	用户账号管理

		角色管理 资源组管理

3.3 关键业务流程

系统的关键业务流程主要有以下四个部分。

1）信息展示：包括首页“合约”和“标的”层面的展示、持仓信息的展示

2）互换管理：包括交易委托、交易确认等

3）期权管理：询价管理、报价管理、订单管理、合约簿记等

4）用户权限管理：用户账户管理、资源组管理和角色管理

3.4 相关系统交互

权益类场外衍生品网厅系统主要对接的外部系统有：

1) BCT 系统：负责提供相关合约和标的等相关信息，并且进行清算簿记等业务流程处理；
2) 互换对冲系统：负责提供互换交易相关的处理；
3) 机构统一门户登录认证系统：负责机构用户的权限认证及校验；
4) 电子签章系统：负责对接客户进行交易确认书等电子化签章处理；

3.5 相关系统配合改造

相关对接系统需要同步配合进行升级改造。其中 BCT 系统需要对接资金结算系统实现实时出入金管理，支持区分机构和产品类型的信息查询，增加跨境标的物基础信息（例如 lotSize）；互换对冲系统需要提供交易基础信息（例如交易日），支持资金结算额度的配置管理和交易校验，其清算模块需要同步盘后分配流水进行清算调仓。

4 数据治理

4.1 数据采集

本系统产生的相关数据，后续可根据实际需要可采集到数据中心。

4.2 数据交互

按照《申万宏源数据治理管理办法》中要求，本系统使用到的数据来源有两处：1）BCT 系统 2）互换对冲系统，产生的数据主要存放在 TDSQL 关系型数据库、内存数据库、Redis 缓存中，本系统不涉及使用其他数据或数据共享。

4.3 数据标准

系统在开发完成后，项目组向数据中心提供数据字典、表结构等，后续按照《数据治理管理办法》要求，提供本系统元数据的要素信息。

4.4 数据分类分级

本系统在开发设计过程中，按照《数据安全管理办法》的要求，对数据安全需求（访问权限、用户使用权限等）进行同步规划与设计。

本系统的数据使用、查询、导出功能，按照数据安全管理要求，按照数据安全等级为用户进行使用权限的设置。

4.5 数据安全

本系统在开发设计过程中，按照《数据安全管理办法》的要求，对数据安全需求（访问权限、用户使用权限等）进行同步规划与设计。

4.6 数据质量

不涉及

4.7 指标管理

目前本系统不产生指标数据。未来如果增加指标数据，将纳入指标体系统一管理，并填写《指标管理标准模板》中的信息项，包含指标定义、指标口径等信息。

5 安全架构

权益类场外衍生品网厅系统按照等保二级要求进行建设。系统支持外部客户与公司金融创新总部内部员工访问，支持登录 token 认证、强密码、加密存储和传输，用户权限管理符合公司规范。系统有完善的日志记录功能，出故障时候可对问题进行追溯，对关键操作需要记录日志，包含操作用户、时间、用户 ip、访问菜单、访问页面、操作以及操作结果、接口响应时间等信息，并且日志记录不能随意删除、覆盖。

5.1 监管要求、安全等级与风险类型

系统遵照相关安全要求，如《证券公司信息技术管理规范》、信息安全等级保护二级要求，以及以下相关安全要求：

数据验证：系统中接收的所有参数和数据包都要有准确性、完整性、合法性验证。

权限控制：有完善的权限控制方案，避免恶意提权、暴力破解。

日志记录：有完善的日志记录功能，出故障时对问题进行追溯。

安全检测：系统上线前要进行有效的安全检测，检测范围包括但不限于：用户恶意提权、暴力破解、SQL 注入式攻击、弱口令账户、绕过验证、目录遍历、文件上传、跨站脚本攻击、缓冲区溢出等。

5.2 身份和访问管理

用户分为两类：公司员工和外部客户。公司员工通过北京和上海的办公网访问管理端，限定访问用户源 IP；外部客户可通过互联网访问对客端，不限制用户源 IP。

5.3 权限管理

1）系统支持按角色赋权、为用户配角色的权限管理模式，支持增加、修改、删除、查询角色的功能。

2）系统权限管理由角色管理员和用户管理员完成，设置角色管理员角色及用户管理员角色，角色管理员负责新建角色、为角色分配菜单；用户管理员负责开设操作员用户并为其分配角色。

3）系统中的“角色设置、为角色赋权”与“用户维护、为用户授予角色”的功能菜单相互独立。

4）需有一个用户只能分配一个角色的单选控制。

5）不得直接为用户赋菜单权限。

6）系统不设自带角色、默认权限以及权限间的捆绑，超级用户（admin）不作日常使用。

7）系统对用户的登录、退出以及与权限变动有关的操作进行记录，具有对记录的分类查询功能。

8）对于内部管理端，以人力资源名册中的员工工号作为登陆用户号，支持设置对应员工姓名，字符长度可满足实际需求。

5.4 安全审计

有完善的日志记录功能，日志包括系统 elk 日志和 tdsql 中存储的用户操作日志。出故障时候可对问题进行追溯排查。对系统的关键操作有日志记录，包含操作用户、时间、用户 ip、访问菜单、访问页面、操作以及操作结果、接口响应时间等信息，并且日志记录不能随意删除、覆盖。

记录方式：elk 文件记录和 tdsql 日志表

审计方式：可以通过 elk 文件检索和 sql 查询语句提供审计相关查询、统计功能

日志保存策略：elk 日志保留 1 年以上，tdsql 日志永久保存

5.5 数据完整性和保密性

系统中敏感信息的安全管理做到存储安全、传输安全、访问安全、安全审计。

- 存储安全

系统的信息存储主要依托基础技术平台和数据库的安全策略，防止数据的非授权访问和修改。

- 传输安全

在数据传输上采用传输前加密及传输时加密两种方式。传输前系统可对敏感数据进行初次加密，如密码传输前使用 AES 方式进行加密处理，在传输时使用

SSL 加密技术进行数据传输。

密码加密存储，密码仅仅在登录时提供，认证之后所有的通信全部基于一个系统生成的、有时效的 token 完成；浏览器与服务器之间的通信全部经过 https 加密

5.6 网络安全

- 最小化对互联网的暴露，管理端仅供办公网访问
- 系统仅包含 WEB 页面，无对外发布 Restful API
- 系统不访问互联网
- F5 到前置机、前置机到容器云对外服务、容器云工作节点到 tdsql 实例、nacos 集群、mq 集群、redis 集群，均需开通防火墙

5.7 系统安全

- 操作系统、中间件、数据库版本，使用标准版本
- 使用的管理员账号非缺省，使用复杂密码
- 管理员账号归信息技术保障部管理
- 管理员通过堡垒机登录服务器

5.8 供应链安全

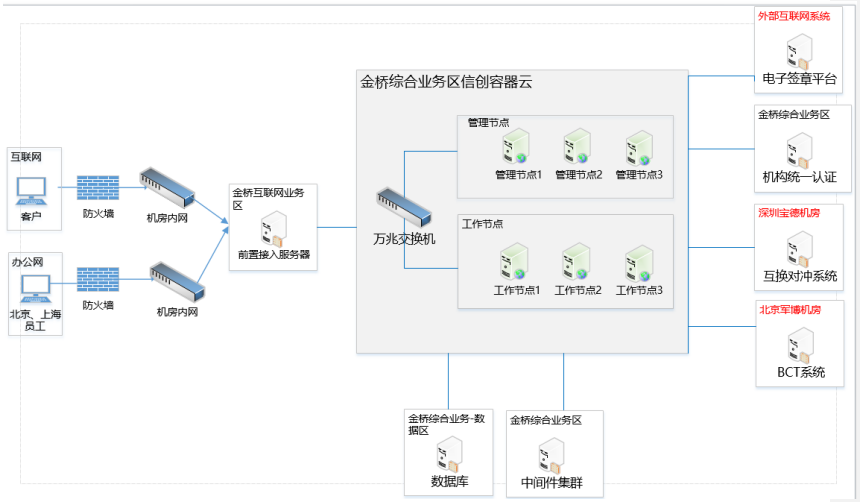
- 制品的交付方式：升级包，包括镜像、配置文件、升级手册、厂商测试报告
- 采用的制品安全检测：容器云自带镜像扫描

5.9 其他安全措施

无

6 技术架构

6.1 物理架构



权益类场外衍生品网厅系统物理架构图

说明：权益类场外衍生品网厅系统部署在金桥机房，复用业务中台的信创容器云与 TDSQL 数据库的资源。

1）前置接入服务器采用信创虚拟机资源，中间件集群为非信创虚拟机资源（注册中心 Nacos，消息队列 RabbitMQ，缓存 Redis 在集群资源外单独申请机器部署）；

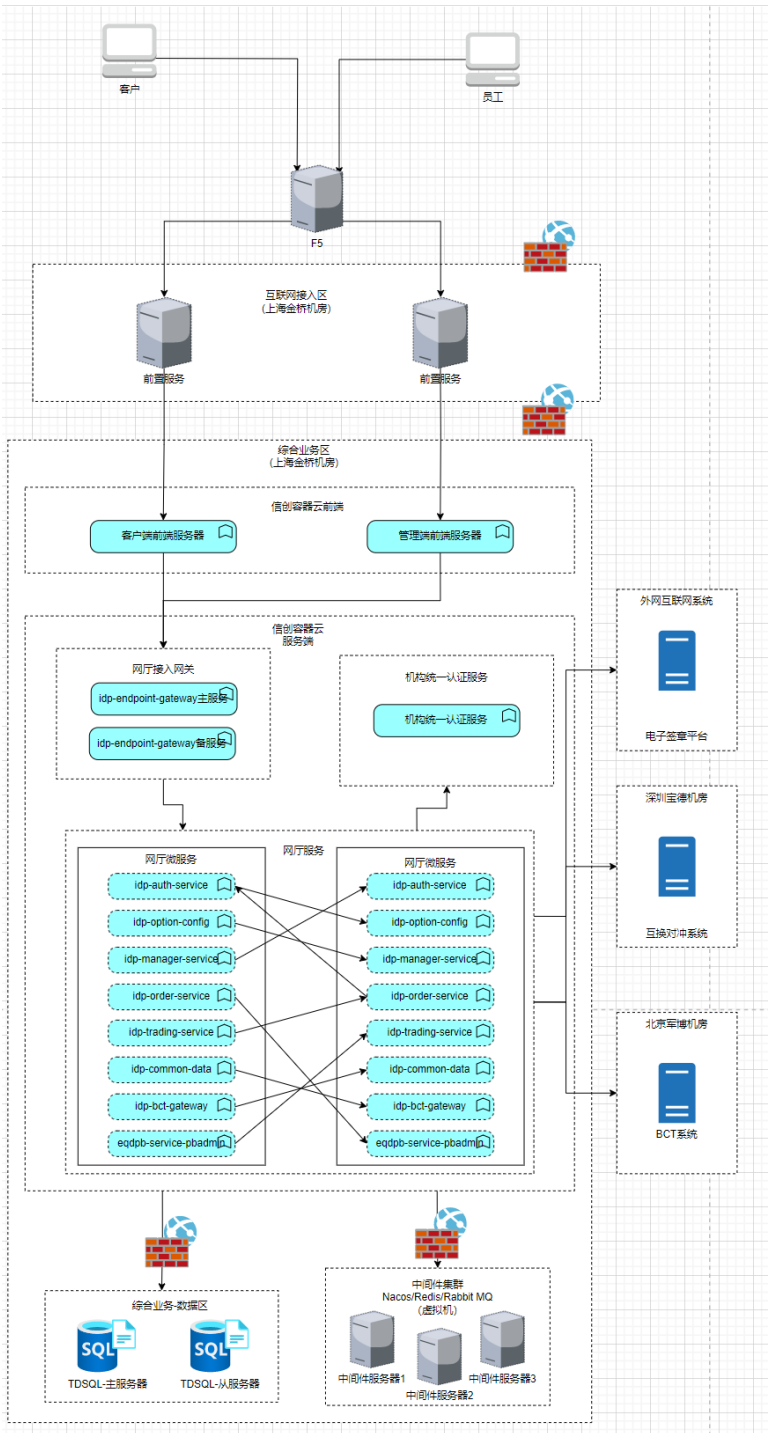
2）网络结构上前置接入服务器在互联网业务区，其他服务节点均在综合业务区；

3）本系统挂载域名后通过 web 服务对外提供访问，用户分为外部客户与公司内部员工，外部客户通过互联网访问系统，内部员工通过北京和上海的办公网访问；

4）数据库复用业务中台已有的 TDSQL 集群资源，采用一主两备模式运行，确保高可用。

6.2 功能部署架构

平台的应用功能主要分为两部分：客户端和员工端部分。


客户
员工
F5
互联网接入区
(上海金桥机房)
前置服务
前置服务
综合业务区
(上海金桥机房)
信创容器云前端
客户端前端服务器
管理端前端服务器
信创容器云
服务端
网厅接入网关
idp-endpoint-gateway主服务
idp-endpoint-gateway备服务
机构统一认证服务
机构统一认证服务
网厅微服务
网厅服务
网厅微服务
idp-auth-service
idp-option-config
idp-manager-service
idp-order-service
idp-trading-service
idp-common-data
idp-bct-gateway
eqdpb-service-pbadm
idp-auth-service
idp-option-config
idp-manager-service
idp-order-service
idp-trading-service
idp-common-data
idp-bct-gateway
eqdpb-service-pbadm
外网互联网系统
电子签章平台
深圳宝德机房
互换对冲系统
北京草博机房
BCT系统
综合业务-数据区
SQL
SQL
TDSQL-主服务器
TDSQL-从服务器
中间件集群
Nacos/Redis/Rabbit MQ
(虚拟机)
中间件服务器1
中间件服务器2
中间件服务器3

外部客户通过互联网访问系统，内部员工通过办公网访问系统，均通过浏览器经 F5 转发至系统前置接入服务器，再通过前置接入服务器上部署的 nginx 将请求转发至前端服务器，前端微服务通过网关进行身份认证与后台微服务进行交互；后台微服务负责处理主要业务逻辑，并与外部系统对接；其中微服务的部署复用中台现有的轻舟云集群资源，数据库采用 TDSQL，中间件（注册中心 Nacos，消息队列 Rabbitmq，缓存 Redis）在集群资源外单独申请机器部署。

6.3 系统软件平台

6.3.1 操作系统

平台名称	操作系统名称	操作系统版本	备注
ARM 容器云	麒麟	V10	
X86 服务器	麒麟	V10	

6.3.2 数据库

服务器种类	数据库版本	硬件平台	操作系统及版本
TDSQL	8.0	ARM	麒麟 V10

TDSQL 参数模板：

参数	建议值	需求值	参数说明
实例版本	8.0	8.0	目前可选版本为 5.7 和 8.0
LVS 端口		15101	应用连接的两台负载均衡地址的端口号 ，建议和开发、测试环境一致；填表前跟信息技术保障部沟通后确定
PROXY 端口		15101	三台网关服务器的端口号，建议和开发、测试环境一致，填表前跟信息技术保障部沟通后确定
DB 端口		默认	多台数据库服务器的端口号，建议和开发、测试环境一致，填表前跟信息技术保障部沟通后确定
实例类型	集中式	集中式	有集中式、分布式实例可选

实例名	跟业务相关,便于识别	eqd_pb	建议使用业务相关名称缩写
赤兔用户	跟业务相关,便于管理	无	建议使用业务相关名称缩写
是否区分大小写	0	0	lower_case_table_names = 1 时，mysql 会先把表名转为小写，再执行操作,大小写不敏感，设置为 0 则大小写敏感
是否记录未使用索引的语句	1	1	是否记录未使用索引的语句,建议开启(但可能会导致 slow log 文件体积较大)
是否启用 lvs	是	是	建议启用，需申请两台 lvs 服务器设备及 3 个 IP,可实现 proxy 层面的高可用
主备同步模式	一主一备,实时同步	一主两备,实时同步	默认采用一主一备，若有其他需求请说明(可配置单备机)
备份要求	物理/逻辑备份，保存周期	物理备份,30 天	默认每个工作日物理备份全备，保留两周，备份方式数据量超过 200G 推荐物理备份，规模较小可以选择逻辑备份

6.3.3 中间件

中间件名称	版本	硬件平台	操作系统及版本
Redis	6.2.9	X86 虚拟机	麒麟 V10
Rabbitmq	3.9.4	X86 虚拟机	麒麟 V10
Nacos	2.0.4	X86 虚拟机	麒麟 V10

6.4 系统硬件平台

开发测试环境包括开发环境、测试环境各一套，容器云配置、数据库配置、中间件（Redis、Nacos、RabbitMQ）配置与生产相同。

生产环境和测试环境配有 F5 进行请求的转发。开发环境没有用到 F5 资源。

同时为了保证服务的负载均衡和高可用,生产环境和测试环境的 9 个无状态的微服务（共有 14 个微服务）均进行了多台容器的部署。

6.5 网络流量

网络带宽是指在一个固定的时间内（1 秒），能通过的最大位数据。bps 即 bit/s（比特/秒）是描述网络带宽的单位。请求数据传输引发的网络容量需求估算方法如下：

网络带宽 = 单位分钟峰值请求量 / 60 * 每笔请求数据包数 * 数据包平均字节长度 * 8 * 网络开销冗余系数。

根据业务量估算，1 年和 3 年后，预估业务量峰值分别为 1000 笔每秒和 3000 笔每秒，每笔请求的客户、产品信息总计约 20 个字段，假设每个字段平均长度为 30 字节。按每个通讯报文因报文头、MAC 等其他要素需要增加 360 字节估算，实际通讯流量需要考虑网络协议的开销按经验还需增加 20%，由此推算联机交易每秒网络流量峰值为：

1 年：1000*（20*30+360）*1.2*8/1024/1000=9Mbps

3 年：3000*（20*30+360）*1.2*8/1024/1000=27Mbps

网厅服务器和数据库服务之间网络流量峰值和联机网络流量峰值相当。

目前和第三方连接共用网络，占用网络带宽较小。

6.6 存储

数据库存储空间

权益类场外衍生品网厅系统是新建业务系统，故分别预估未来 1 年和 3 年的存储容量。业务量根据用户数以及涉及到的合约、标的来评估。

初步预估，生产环境集中存储需求如下：

用途	存储分类	容量大小（GB）
主数据库	在线存储	50
备数据库	在线存储	50

说明：数据库采用高可用技术实现可用保护。备库是指高可用保护中和主库对应的备库。

6.7 备份

1）镜像备份

容器云对历史镜像会存放在镜像仓库里，可以随时还原到指定版本。

2）业务数据备份

按照数据库模板进行备份即可，重大操作前也会进行手动备份。

6.8 高可用性设计

应用名称	权益类场外衍生品网厅系统
系统架构	B/S
应用分类	内部管理类+对外业务类
系统部署位置	金桥机房综合业务区（容器云） 金桥机房互联网业务区（前置服务）
应用重要程度	非重要系统
应用本地高可用性	前置服务器高可用 应用实例容器云高可用 数据库服务 1 主 2 备高可用 中间件 Redis、Nacos、RabbitMQ 采用集群模式部署
灾备等级	RTO：30 分钟 RPO：5 分钟
灾备架构分类	两点容灾

结合权益类场外衍生品网厅系统的 RTO、RPO 要求，建议选择两点容灾的方式，提升数据的安全性和可用性。

6.9 运维监控

运维监控通过集中监控和智能运维平台实施，至少包括基础性能监控、数据库监控、普通应用程序监控、业务监控、重要时点巡检监控等。

6.9.1 基础性能监控

本项目使用容器云平台，可以使用平台相关监控手段和数据。

6.9.2 数据库监控

本项目使用的数据库为保障部提供的标准数据库。

6.9.3 普通应用程序监控

本项目系统日志被采集并推送到日志平台供监控，同时，用户的操作日志也被记录到数据库中可供管理端查询。

6.9.4 业务数据监控

重要业务数据如合约、标的、资金和额度信息等，均可以通过管理端查看，也可以使用 SQL 语句从数据库查询。

6.9.5 重要时点巡检监控

暂不涉及。

6.10 应急方案

为保证本系统业务顺利运作，最大限度保障不间断运营，针对各类易发或潜在系统风险，对于系统特制定以下应急策略。

应用服务节点：应用服务运行于信创容器云平台中，服务异常后平台可自动拉起异常实例，基本无需人工干预。

数据库服务：系统采用 TDSQL 数据库，支持主备多实例多分片的数据复制和实时同步，主备切换后完成主从自动选举，节点恢复加入集群后分片数据自恢复。

前置服务：采用集群模式，F5 做负载，任一节点故障后，其他节点正常工作。

中间件： Redis、Nacos、RabbitMQ 均采用集群模式部署，任一节点故障后，其他节点正常工作。

7 实施方式

7.1 实施阶段

表7-1 项目实施时间计划

项目子环节	编号	工作任务目标	完成时间
1.项目基本建设	1.1	需求提出	T日
	1.2	项目立项	T+4周
	1.3	实施方案通过评审	T+8周
	1.4	完成功能开发	T+16周
	1.5	完成测试	T+24周
	1.6	完成业务验收	T+28周
2.项目投产	2.1	生产环境部署	T+30周
	2.2	系统上线试运行	T+32周
	2.3	系统正式上线	T+36周
3.项目收尾	3.1	完成项目评审与结项	T+40周

7.2 项目组成员

角色	部门	人员
项目组长	金融创新总部	李斌冰
项目副组长	金融创新总部	贺远宁
	信息技术开发总部	靳赟婷
项目经理	信息技术开发总部	刘悦
业务经理	金融创新总部	孟磊
		肖骁
		梁祖韬
		岳天泽
产品经理	信息技术开发总部	刘悦
开发经理	信息技术开发总部	胡睿
		王通杰
运维管理员	信息技术保障总部	高攀
测试经理	信息技术开发总部	李跃
项目监理	信息技术开发总部	陈新

8 预算及成本

8.1 项目预算

本项目费用预算 338.5 万元。硬件复用中台信创容器云的硬件资源及虚拟机资源，无硬件费用。软件及实施费用包括购买网厅基础模块与期权功能模块（含源码），并对场外衍生品网厅进行整体信创化改造，预计费用 225 万元。跨境互换的个性化需求，具有我司较为独特的展业模式，由金融创新总部与信息技术开发总部派出骨干人员负责核心功能开发，前端界面与周边功能开发建议外购部分技术支持力量，相关工作量预计为 32 人月。以 3.4 万/人月的开发人力单价计算，该部分涉及费用预计不超过 110 万元。

类型	内容	预算（万元）
软件及实施费	跨境互换个性化开发（技术支持服务）	110
	期权业务功能模块（含网厅信创改造适配）	225
	麒麟 V10 操作系统授权（5 套）	3.5
硬件费用	复用业务中台信创容器云与 TDSQL 数据库资源	0
	虚拟机 5*4C16G200G（约 3 万元，计入信创云扩容项目）	0
总计		**338.5**

8.2 成本承担以分摊原则

项目成本承担对象：金融创新总部

成本分摊原则：100%

9 软硬件清单

物理主机	用途	环境主要配置	操作系统版本	数据库/中间件版本	高可用方式
信创虚拟机-海光	Nginx-互联网接入	4C-16G-500G	信创海光 Kylin10	--	Nginx keepalived
容器云	后端对客端&后管端服务	4C-16G-500G	信创麒麟 Kylin10	--	容器云内部实现高可用

格式化表格

容器云	推送服务	4C-16G-500G	信创麒麟 Kylin10	--	容器云内部实现高可用
容器云	文档服务	4C-16G-500G	信创麒麟 Kylin10	--	容器云内部实现高可用
容器云	动态配置服务	4C-16G-500G	信创麒麟 Kylin10	--	容器云内部实现高可用
容器云	融券管理	4C-16G-500G	信创麒麟 Kylin10	--	容器云内部实现高可用
分布式数据库集群虚拟机	TDSQL 数据库	硬盘 50G	信创麒麟 Kylin10	Mysql 8.0	一主两备
中间件虚拟机（容器云外单独部署）	Redis	4C-16G-500G*3	信创海光 Kylin10	Redis6.2.9	Redis 集群
中间件虚拟机（容器云外单独部署）	Rabbitmq	4C-16G-500G*3	信创海光 Kylin10	RabbitMQ3.9.4	MQ 集群部署
中间件虚拟机（容器云外单独部署）	Nacos	4C-16G-500G*3	信创海光 Kylin10	Nacos2.0.4	Nacos 集群部署

9.1 生产/测试环境

由于项目生产/测试需要，需要如下资源(生产/测试环境下表中的 9 个微服务每个均需要配置为两个，以便于负载均衡和确保服务的高可用)：

环境名称	用途	操作系统	CPU（core）	内存（G）	共享存储（G）	数量
容器云	用户校验	信创麒麟 Kylin10	4	16	500	2
容器云	网厅前端-对客端	信创麒麟 Kylin10	4	16	500	2
容器云	网厅前端-后管端	信创麒麟 Kylin10	4	16	500	2

容器云	调用 BCT 服务	信创麒麟 Kylin10	4	16	500	2
容器云	公共数据模块	信创麒麟 Kylin10	4	16	500	2
容器云	期权网厅对外网关	信创麒麟 Kylin10	4	16	500	2
容器云	期权网厅下单服务	信创麒麟 Kylin10	4	16	500	2
容器云	期权配置服务	信创麒麟 Kylin10	4	16	500	2
容器云	期权网厅询报价管理	信创麒麟 Kylin10	4	16	500	2

9.2 开发环境

由于项目开发需要，需要如下资源(开发环境下表中的 9 个微服务无需主备)：

环境名称	用途	操作系统	CPU（core）	内存（G）	共享存储（G）	数量
容器云	用户校验	信创麒麟 Kylin10	4	16	500	1
容器云	网厅前端-对客端	信创麒麟 Kylin10	4	16	500	1
容器云	网厅前端-后管端	信创麒麟 Kylin10	4	16	500	1
容器云	调用 BCT 服务	信创麒麟 Kylin10	4	16	500	1
容器云	公共数据模块	信创麒麟 Kylin10	4	16	500	1
容器云	期权网厅对外网关	信创麒麟 Kylin10	4	16	500	1
容器云	期权网厅下单服务	信创麒麟 Kylin10	4	16	500	1
容器云	期权配置服务	信创麒麟 Kylin10	4	16	500	1
容器云	期权网厅询报价管理	信创麒麟 Kylin10	4	16	500	1

10 后续方案细化的关注点

无