郑州商品交易所期货行业云平台采购项目前期技术参数公示

（招标编号：/）

项目所在地区：河南省,郑州市

一、招标条件

本郑州商品交易所期货行业云平台采购项目已由项目审批/核准/备案机关批准，项目资金来源为其他资金/，招标人为郑州商品交易所。本项目已具备招标条件，现招标方式为公开招标。

二、项目概况和招标范围

规模：郑州商品交易所期货行业云平台采购项目

范围：本招标项目划分为1个标段，本次招标为其中的：

(001)郑州商品交易所期货行业云平台采购项目;

三、投标人资格要求

(001郑州商品交易所期货行业云平台采购项目)的投标人资格能力要求：/;

本项目*不允许*联合体投标。

四、招标文件的获取

获取时间：从2023年06月20日 00时00分到2023年06月25日 18时00分

获取方式：本项目为前期公示，请忽略时间

五、投标文件的递交

递交截止时间：2023年06月26日 00时00分

递交方式：本项目为前期公示，请忽略时间。

六、开标时间及地点

开标时间：2023年06月26日 00时00分

开标地点：本项目为前期公示，请忽略时间

七、其他

河南招标采购服务有限公司受郑州商品交易所的委托，拟就郑州商品交易所期货行业云平台采购项目组织公开招标，现将该项目的采购需求及评审因素进行公示。

公示期限：2023年6月20日起至2023年6月25日。

所有意见应于公示期限内以书面形式，后附营业执照、法人授权委托书、法定代表人身份证明及身份证件扫描件或复印件一并加盖投标人公章递交至河南招标采购服务有限公司408办公室或发送至邮箱441301399@qq.com，逾期反馈或其他形式反馈均不予受理。

联系方式：

代理机构：河南招标采购服务有限公司

地址：郑州市金水区纬四路13号

联系人：马小利

电话：0371-65950562

附件：郑州商品交易所期货行业云平台采购项目采购需求及评审因素

八、监督部门

本招标项目的监督部门为/。

九、联系方式

招 标 人：郑州商品交易所

地　　址：/

联 系 人：/

电　　话：/

电子邮件：/

招标代理机构：河南招标采购服务有限公司

地　　址：郑州市金水区纬四路13号

联 系 人：马小利

电　　话：0371-65950562

电子邮件：/

招标人或其招标代理机构主要负责人（项目负责人）：_____（签名）

招标人或其招标代理机构：_____（盖章）

郑州商品交易所期货行业云平台采购项目采购需求及评审因素公示

采购需求

一、项目概况

为提升郑州商品交易所(以下简称郑商所)科技服务市场水平、促进期货市场业务创新和数字化转型，计划开展期货行业云建设工作。期货行业云的建设总体按照“贴近行业、全栈服务、安全可靠、持续完善”原则开展，为期货行业提供安全可靠、集约高效的数字化云基础设施服务。一是助力期货行业信息科技降本增效，二是促进期货行业数字化转型，三是促进形成期货行业集聚高效的数字技术生态圈，四是为郑商所集团数字化转型提供统一的基础算力平台。

期货行业云总体采用多地多站点部署架构，与郑商所现有交易网络、证联网等业务网络，以及互联网连通。为期货公司等行业内机构提供生产、灾备、测试等资源环境，同时也将承载郑商所集团部分互联网业务。

期货行业云采用分期建设的思路，初期重点建设郑州站点IaaS服务(计算、存储、网络、安全等)，主要承载如灾备、行情、测试等业务，通过初期的运行模式优化，为后续的容量扩容、服务能力扩展打好基础。中期增加同城灾备能力，视情况在客户聚集的其他城市增加网络接入POP点，同时扩大云服务范围(如数据库、中间件、Devops、大数据、AI等)，扩大业务承载能力(如交易、智能应用、综合办公、服务APP等)。远期着

眼于支持更多的客户群体、客群生态更加多样化，同时站点布局更加全面，运营成熟度进一步提升。

本次项目主要建设郑州单站点的IaaS服务及初步的PaaS服务，后续将持续完善多地多站点结构并完善PaaS/SaaS服务。

***二、云平台总体能力要求**

为了满足期货行业云未来持续建设和运营要求，云平台整体能力上须满足如下的功能性和非功能性指标。**本节内容必须完全响应，否则为无效投标。**

1.总体技术架构要求

（1）云平台应支持多地多中心的部署能力。

（2）云平台应支持同城双活、异地容灾等不同场景下的容灾架构，从而满足期货行业云上运行的业务应用所需的不同容灾要求。

（3）云平台及云产品应采用分布式技术架构，从而保证云平台及云产品具备在线横向扩展能力。

（4）云平台提供的云产品服务应全部采用软件（包括但不限于计算、块存储、对象存储、文件存储、虚拟网络、大数据、分布式中间件等）+通用服务器（X86服务器或采用国产CPU的服务器）实现。

（5）云平台虚拟网络应采用软SDN+Vxlan实现。

（6）云平台管控节点规模可支持不少于1000台物理服务器扩展能力。

（7）云平台应支持多租户，且支持单租户内包含多个VPC，满足单一租户内根据不同业务划分不同安全域的要求。

（8）云平台应具备对用户、多租户的全生命周期管理。

（9）云平台应提供统一的图形化管理操作界面。

（10）云平台应提供租户资源配额管理，支持自定义的配额管理、计量计费管理。

（11）云平台应支持PaaS、SaaS服务扩展能力。

（12）一云多芯：同一云平台内全面兼容x86、ARM多种芯片架构，兼容Intel、海光、鲲鹏、飞腾等CPU芯片服务器。

（13）云平台应支持主流数据库服务：包括mysql、postgres、redis、MongoDB等，具备提供自主研发数据库服务的能力，具备兼容oracle数据库服务能力。

（14）云平台应支持大数据服务：具备提供自主研发的大数据服务的能力。

2.能力指标

(1)IaaS服务能力要求

应**提供完善的**IaaS**服**务**能力**,**包括**计**算**、存**储**、网**络**、安全**、**容器等**;

1)计算服务应**包含**:**同**时**支持虚**拟**机和裸金属服**务**器形式的**弹**性供**给,**其中**弹**性裸金属服**务**器能**够实现**与云虚**拟**机同**样**的灵活供**给**和管理能力。**

2)存储服务能力应**包含**:

A. 提供安全、高可靠的对象存储服务，可通过网络随时存储和调用文本、图片、音频和视频等在内的各种非结构化数据文件；

B. 提供高性能、低时延，满足随机读写的块存储服务，使得虚机可以像使用物理硬盘一样格式化建文件系统使用；

C. 提供可共享访问、弹性扩展、高可靠以及高性能的分布式文件系统，虚拟机、容器服务等计算节点内通过标准的NFS协议挂载文件系统，并使用标准的POSIX接口对文件系统进行访问；

D. 提供一站式日志服务，可以快速完成日志数据采集、消费以及查询分析等功能，提升运维、运营效率，建立海量日志处理能力。

3)网络服务能力应**包含**:

A. 云虚拟化网络应采用软件SDN+VxLan网络技术，支持容器网络、裸机网络、云内网络的统一调度和管理能力；

B. 云网络支持与传统网络打通；

C. 云网络应支持虚拟私有网络（VPC）能力；

D. 应支持云上采用软件实现L4/L7负载均衡，支持高性能高并发的负载均衡场景和灵活多样

的负载策略；

E. 应支持为租户提供域名解析服务。

4)安全服务能力应包含：

提供等保三级安全能力以及相应的安全服务能力，包含但不限于如下安全能力（产品可以是云平台厂商适配集成的第三方产品，由云平台原厂商总体负责）：

A. 主机安全服务

B. 容器安全服务

C. 网络安全服务

D. 流量安全服务

E. 运维审计服务

F. 数据库审计服务

G. 数据加密服务

H. 安全日志分析服务

I. 统一安全管理服务

J. 可信计算安全服务

K. 数据脱敏安全服务

L. 应用安全服务

提供以上安全能力对应产品清单及产品简要说明的盖章证明材料，无相关证明材料的或者缺项的视为该指标不满足。

(2)PaaS服务能力要求

云平台应支持PaaS服务扩展能力，包括但不限于中间件、数据库、大数据、人工智能等。（产品可以是云平台厂商适配集成的第三方产品，由云平台原厂商总体负责）

提供以上PaaS服务能力对应产品清单及产品简要说明的盖章证明材料，无相关证明材料的或者缺项的视为该指标不满足。

(3)容灾与备份能力要求:

1）应支持同城容灾架构，关键数据产品支持同城三机房容灾架构且RPO≈0，支持可视化同城容灾管理平台，可实现整机房级/云产品级故障一键切换，保障业务连续稳定运行。

2）应支持异地跨城容灾架构，可以容忍区域性故障，支持可视化异地容灾管理平台，基于业务维度建立容灾资源组和容灾计划，支持多地多中心架构，具有更高的级别的业务高可用性。

3）应支持备份恢复服务能力，可以对云上的云主机、存储、大数据、数据库等多种云服务进行统一备份恢复管理，防止误删除、误操作导致的云上数据丢失。

(4)行业云服务能力

期货行业云应支持计算、存储、网络、安全、中间件、数据库、大数据的多租户服务能力。

应支持行业云统一运营门户，提供多租户、服务管理、资源配额管理、计量计费能力。

(5)一云多芯能力

支持云平台底座和资源池全链路基于通用硬件设备的方案，同时保障全平台高性能稳定运行;支持基于通用底座管理多CPU芯片架构类资源池，用户可基于芯片类型创建资源。

(6)云原生分布式应用能力支持

云平台支持提供必要的应用开发框架和服务治理能力。

3.非功能性指标

(1)云平台架构要求

云平台技术架构应与公有云采用同一技术架构体系，与投标云厂商公有云同源，须提供云平台原厂商印章的相关证明材料，如官网截图等，若投标产品云原厂商无公有云产品或无法证明投标产品与其投标产品云原厂商的公有云产品同源，则视为指标

项不满足。云平台提供整套包含部署、监控报警、备份、故障处置、安全管控等自动化运维能力，提供云平台统一运营门户及行业云运营能力。

(2)安全性要求

云平台应该提供符合GB/T 22239-2019《网络安全等级保护基本要求》标准中的云安全扩展要求的等保三级安全能力，能够通过等保三级认证，具备为行业提供大规模云资源服务所需的各项安全能力。

(3)可扩展性要求

云平台支持多地多中心多活架构，支持多可用区多活架构，云底座、云管控、云服务应具备同城双AZ容灾能力，并支持异地跨Region容灾能力。

Region作为逻辑隔离域，实现地域级别多AZ管理，同时兼顾大规模数据中心多AZ的管理需求;同一Region下，Region级的公共资源服务可实现跨AZ的高可用，包括VPC服务、云负载均衡服务、云DNS服务、对象存储服务等。

AZ作为资源故障隔离域，可承载应用完整的功能节点;AZ之间资源池完全独立，一个AZ的故障不影响其他AZ正产运行;AZ级服务为:计算服务(云主机、裸金属、容器服务)、块存储服务、Spine/leaf组网等。

(4)高可用性要求

云平台及云产品应采用分布式集群架构以保证高可用性，全平台无单点问题。

(5)可管理性要求

云平台应提供完整的管理服务能力和运营运维服务能力，应提供租户视角和运营、运维视角的统一管理门户:租户视角整合IaaS和PaaS一体化统筹设计，提供包括面向计算、存储、网络、安全、数据库、软件服务等多层面的服务目录，形成统一云门户;运

营视角提供云平台运营能力;运维视角提供对应用、计算、存储、网络、安全、容器等的统一运维管理界面，形成运维人员统一入口。

同一Region的云平台通过统一账号体系对不同AZ的运维和运营进行管理。

产品服务应提供API接口以及接入的SDK和文档。

(6)在线平滑升级、平滑资源扩容要求

支持云平台的在线平滑升级和扩容，对提供的云服务没有影响，能够正常不间断的对外提供服务，对其上的资源及服务也无影响。

三、采购需求

（一）采购清单

为确保满足郑商所期货行业云平台正常运行，投标人**应提供给招标人包括但不仅限于下表中整体云平台及所需的配套产品组件**，并提供所购置产品的永久性软件产品许可使用权，各类授权的数量应能满足本次采购需求。此次涉及的云平台软件产品和服务内容是由原厂商整体提供，整体负责。下面所列软件均由产品原厂商进行集成适配。

序号	分类	产品名称	采购数量	描述
1	弹性计算	弹性计算	4800核	提供云主机、弹性伸缩等弹性计算功能，授权规模不小于4800核（可用物理核数，对应不少于60物理服务器）
2	存储	分布式块存储	1900TB	提供分布式块存储功能，块存储物理磁盘总容量不小于1900TB
3		分布式对象存储	850TB	提供分布式对象存储功能，对象存储物理磁盘容量不小于850TB
4	网络	专有网络VP	1套	提供专有网络VPC服务，应满足本次项目

		C服务		所采购的计算规模需求
5		负载均衡软件	1套	提供四层与七层负载均衡服务，应满足本次项目所采购的计算规模需求
6		云平台DNS服务	1套	提供云平台DNS服务，应满足本次项目规模需求
7	容器服务	容器服务	1套	提供容器服务功能，授权不少于900vCPU核数
8		容器镜像服务	1套	提供容器镜像服务，支持1千个命名空间，10万个仓库配额，支撑不少于500节点并发拉取规模
9	安全服务	主机安全防护	1套	提供云主机安全防护功能，云服务器主机安全防护授权节点数应满足本次项目所采购的计算规模需求，支持不少于1500台云主机的安全防护
10		容器安全防护	1套	提供容器安全防护，授权不小于900vCPU核数
11		平台侧堡垒机	1套	提供平台侧堡垒机功能，授权不少于500个对象管理许可
12		租户侧堡垒机	1套	提供租户侧堡垒机功能，授权不少于600个对象管理许可
13		云安全管理中心	1套	提供云安全管理中心功能(包括安全管理基础功能、安全编排自动化响应、安全日志分析功能)，授权节点数应满足本次项目建设规模所需，其安全日志保存总容量不少于270TB

14		云安全流量监测	1套	提供云安全流量监测功能，支持总网络吞吐性能>=20(Gbps)， 支持总入侵检测能力>=10(Gbps)
15		云安全态势感知	1套	提供云安全态势感知服务，授权节点数应满足本次项目建设规模需求
16		漏洞扫描	1套	授权节点数应满足本次项目建设规模需求
17		应用安全防护	1套	提供应用安全防护功能，支持4万QPS
18		数据库审计	1套	支持云自建数据库、RDS数据库SQL精确审计，包含10个数据库实例授权，支持扩容
19		数据梳理及脱敏	1套	数据发现、数据梳理及数据脱敏，包含10个数据库实例授权，支持扩容
20		敏感数据保护	1套	为云数据资产提供敏感数据识别、分级、打标、审计、脱敏、异常检测等数据安全能力，授权数量不少于100台物理主机
21		应用身份服务	1套	内置5A模块，包括应用统一管控AppStore及单点登录SSO，可以实现Web、移动App及API的统一认证。支持Web应用实现SSO单点登录和开发者服务等能力。提供不少于100用户授权
22		密钥管理服务	1套	提供密钥生命周期管理、全托管的密码机，支持云平台底座的密钥管理
23		加密服务	1套	对加密机进行管理，支持云平台底座的

				密钥管理
24	PaaS服务	数据库服务	1套	提供稳定可靠、可弹性伸缩的在线关系型数据库服务，授权不少于256核（物理核）
25	云备份服务	云备份服务	1套	提供云主机整机备份，备份总容量应不小于20TB，并支持存储类产品、大数据类产品备份功能
26	云管理平台	云管理平台	1套	授权节点数应满足本次项目建设规模需求
27		云运维管理系统	1套	授权节点数应满足本次项目建设规模需求
28		云统一运营平台	1套	授权节点数应满足本次项目建设总规模所需，要求具备多云纳管等能力，多云管理能力不少于3朵独立云纳管

注：①以上详细的软件要求和兼容性要求分别详参“软件要求”、“兼容性要求”章节内容详述；

②投标人在应答上述采购需求时，在报价明细中需明确各功能组件/产品的授权方式、授权单位、授权数量、生效容量等信息。

（二）软件要求

本项目采购的云平台及相关云产品软件需满足本章节所述的各项指标要求，对本章节软件要求中带有“★”号的指标项要求，投标人须提供相关指标项的原厂商盖章证明材料，证明材料可以使用原厂商官方网站截图、相关部门官网截图或者资质证书、产品白皮书或第三方机构检验报告、产品截图或其他相关证明材料。需要提供证明材料的指标，若出现未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

1. 云平台

云平台须具备完全自主知识产权，并具备以下相关产品资质要求：

指标项	具体要求
资质要求	*云操作系统软件著作权证明材料
	*云平台安全产品应具备公安部颁发的计算机信息系统安全专用产品销售许可证(增强级)
	★中央网信办云服务安全审查(IaaS PaaS/增强级)
	★中国信息通信研究院-可信云认证-可信金融云解决方案能力评估
	★中国信息通信研究院-可信云认证-数字基础设施一体化云平台服务能力
	★中国信息通信研究院-可信云认证-虚拟化云平台分级(先进级)
	★中国信息通信研究院-可信云认证-多云管理平台解决方案
	★中国信息通信研究院-可信云认证-金融云灾备能力评估
	★中国信息通信研究院-可信云认证-专有云能力综合水平评估(自建模式)
	★中国信息通信研究院-可信云认证-云原生能力成熟度- 技术架构检验证书，成熟度达到四级且四个领域全部达到L4+标准
	中国信息通信研究院-可信云认证-金牌运维
	中国信息通信研究院-可信云认证-研发运营(Devops)解决方案能力(先进级)
	中国信息通信研究院-可信云认证-风险管理能力(先进级)
	中国信息通信研究院-可信云认证-云服务用户数据保护能力(私有云)认证
	云平台具备《信息系统密码应用基本要求》所需的能力

注:上述各项资质要求均需提供证明材料。

2. 弹性计算

弹性计算提供一种处理能力可弹性伸缩的计算服务，提供云主机（云服务器）、弹性伸缩和资源编排服务。弹性伸缩管理服务根据业务需求和策略，自动调整其弹性计算资源大小，资源编排服务提供简化云计算资源管理的服务，可以根据模板自动完成所有资源的创建和配置，实现自动化部署及运维。

指标项	指标子项	
功能要求	云主机	支持云主机生命周期管理和维护，包括但不限于创建、启动、关闭、重启、更换操作
	IP	支持为云服务器指定IP地址创建云主机，方便运维人员进行IP的统筹管理，支持配
	镜像	支持对云主机的系统盘和数据盘创建整机镜像模板，创建的镜像包含用户的业务数
	监控	支持对云主机CPU、内存、硬盘等基础指标进行监控，同时支持对云主机系统中的各
	硬盘	单个云主机能够挂载不低于16块数据盘，单个数据盘的存储容量不小于32TB。
	资源编排	提供资源编排组件，支持按照模版规范编写资源栈模版。在模板中可以定义所需资
		支持JSON格式的资源模板，并通过此模板创建资源栈。
		支持在线查看资源编排服务支持的资源类型及各资源类型详情。
可靠性	反亲和性	★支持云主机按宿主机、机架、网络交换机物理拓扑的调度能力，提升业务的可靠
	热迁移	支持云主机热迁移，运维人员可以手工指定迁移任务的带宽限制，降低迁移流量对
	高可用	支持云主机高可用(宕机迁移)，当某台物理节点发生意外故障，在其上运行的云主
	备份	支持用户通过快照对云主机的数据进行备份，通过快照进行云服务器的数据恢复，
安全性	防ARP	支持云主机网络防ARP欺骗，云平台应阻止用户非法修改IP地址和MAC地址后发出的
	VNC访问	支持用户通过VNC方式远程访问云主机，同时支持用户设置云主机VNC密码(非系统
	硬盘加密	支持云主机磁盘密码算法加密，能够对云盘中的数据、云盘和实例间传输的数据、
	自动快照	支持设置自动快照策略，可自定义快照时间点、重复日期以及保留时长。
弹性伸缩	弹性伸缩	支持弹性伸缩功能，根据业务的需求和策略，自动调整计算资源大小，在业务需求
		支持根据配置的伸缩规则弹性扩张云主机实例，能够自动将云主机实例添加到负载
		支持指定待伸缩云主机实例的配置信息，包括但不限于实例规格、镜像类型、系统
		支持用户定时执行伸缩规则，从而实现自动扩张或者收缩计算资源，满足业务需求
		支持实时统计伸缩组内指标数据，并在统计值满足告警条件时触发告警，自动执行

3.存储

（1）分布式块存储

分布式块存储是为弹性计算虚机实例提供的存储设备，具备高性能、低时延特性，满足随机

读写需求。

指标项	
总体要求	为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。
技术架构要求	★应采用分布式存储引擎软件加通用服务器(至少支持鲲鹏ARM、海光X86 架构通用服务
功能要求	支持在不中断业务的前提下，在线变更云盘规格，满足灵活多变的业务需求。
	支持云盘在客户端缓存功能，在挂载云盘的客户端做预读缓存，节约一跳计算集群到存
	支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘;系统盘在线扩容不停业
	支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。
	单个云盘最高支持不低于32TB容量。
安全性	★支持纠删码和三副本数据冗余保护，三副本模式下，数据三副本支持分布在3个机柜或
	支持使用用户指定的KMS密钥进行加密。加密功能简单易用，无需用户构建、维护或更改

（2）分布式对象存储

对象存储是安全、低成本、高可靠的云存储服务，通过对象存储可以通过网络随时存储和调用包括文本、图片、音频和视频等在内的各种非结构化数据文件。

指标项	具体要求
总体要求	对象存储服务支持RESTful API接口、兼容AmazonS3接口，通过开发工具包SDK或直接通过RESTful API进行基础和高级对象存储操作，提供key-value键值对形式的对象存储服务。
架构要求	★应采用分布式存储引擎软件加通用服务器(至少支持鲲鹏ARM、海光X86架构通用服务器)部署技术架构实现。
功能要求	支持图片处理:包括图片格式转换、图片效果处理、添加文字或图片水印等。
	支持视频处理:对视频文件进行截帧。

	支持对象的简单上传、追加上传、下载、删除、列举、复制，获取对象的元数据、创建多段上传任务。支持列举存储空间、创建存储空间、删除存储空间、列举存储空间内对象、获取存储空间的元数据。
	支持将存储空间配置成静态网站托管模式，并通过存储空间域名访问该静态网站。支持防盗链，支持设置基于HTTP header中表头字段Referer的防盗链方法。
	支持生命周期管理、定义和管理存储空间内所有对象或对象的某个子集的生命周期、变更容量和变更归属。
	支持一朵云跨可用区、跨地域，跨两朵云之间的异步远程复制。
	支持多个集群使用统一域名对外提供服务。
	bucket以及object支持设置标签，可以基于标签设置访问权限和数据生命周期管理策略。
	支持选取内容功能，支持以SQL语句从单个CSV文件中提取记录。
	支持存储清单功能，支持根据配置的清单生成规则，以日/周为单位，对存储空间内的对象进行扫描并生成的清单报告，并存储到指定的存储空间内。在清单报告中，可导出指定对象的元数据信息。
	支持WORM功能，支持基于时间的合规保留策略，在合规保留策略的保留周期内以“不可删除、不可篡改”的方式保存和使用存储数据。
功能指标	★单个对象最大支持不小于48.8TB，单租户支持bucket数量不少于10000个；每个bucket的生命周期可容纳规则不少于1000条。
	支持存储空间监控/使用流量监控/每小时请求数；能够统计公网流入、流出流量，内网流入、流出流量；统计Get/Putobject请求数，Get/Head/Postobject成功请求数，Append/UploadPart/UploadPartCopy/Deleteobject成功请求数；服务端错误请求数、服务端错误请求占比、网络错误请求数、网络错误请求占比、客户端错误请求数、客户端错误请求占比。

安全性	支持客户端加密功能，可以使用客户端加密SDK，在本地进行数据加密，并将加密后的数据上传到对象存储;既支持云平台密钥管理系统托管的用户主密钥，也支持用户自主管理的密钥。支持服务器端的加密功能，用户能够使用密钥管理系统上创建的密钥进行加密。可以使用密码算法对bucket内保存的数据以及单独object进行加密存储。

4.网络

（1）专有网络VPC

专有网络是用户可以完全掌控自己的私有网络，例如选择IP地址范围、配置路由表和网关等

。

指标项	
总体要求	支持用户创建自己的专有网络，同时支持自定义配置IP地址、子网、路由表。支持不同V
功能要求	支持在控制台上针对VPC地址新增CIDR地址段的扩容。
	支持创建IPv4/IPv6 NAT网关，支持SNAT和DNAT配置，用于支持NAT网关绑定多个地址。
	支持不同VPC间互通，支持VPC内的云服务器通过专线与线下IDC的服务器互通要求。
	支持用户可以创建网络ACL配置入向/出向规则，进行网络访问控制功能，从而实现对一
	支持ENI弹性网卡(elastic network interface)绑定云服务器，在多个云服务器间自由
	EIP支持部署多运营商地址池，用户创建EIP的时候可以从指定运营商地址池中申请地址
	VPC支持IPV6地址，支持云主机可通过IPV6地址访问互联网的IPV6服务，支持云主机作
	支持共享VPC，支持按租户和资源集的VPC资源共享。VPC的所有者可以将VPC共享给同一
	支持第三方虚拟网络设备(如负载均衡、防火墙)的自动化部署，提供跨VPC业务流量调
	应支持单一租户创建多个VPC。
	★支持高可靠的云原生组播能力，包含云上Region内组播、云上云下组播等场景;支持
高可用要求	应具备高可用性，当一台物理服务器宕机时，不影响VPC网络正常运行，且对其他服务不
并网能力要求	当云平台内有多个VPC时，应同时支持不同VPC采用不同物理网络接口和子接口与传统

（2）负载均衡

负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。

指标项	具体要求
总体要求	负载均衡服务采用通用服务器架构实现，提供四层TCP/UDP和七层HTTP/HTTPS协议类型的服务。
架构要求	负载均衡支持IPv6，支持挂载IPv4或IPv6的后端应用服务器。
功能要求	★负载均衡支持TCP/UDP/HTTP健康检查方式。支持健康检查，自动隔离异常状态的后端应用服务器。支持健康检查端口与应用服务端口不相同。UDP健康检查支持用户自定义请求和应答字段。
	负载均衡支持公网和私网类型实例;支持私网实例绑定公网IP地址;支持ping私网负载均衡的IP地址用于VIP探活。
	四层TCP/UDP类型负载均衡支持轮询(RR)、加权轮询(WRR)、最小连接数(WLC)、一致性HASH等调度算法;七层HTTP/HTTPS类型负载均衡支持轮询(RR)，加权轮询(WRR)、最小连接数(WLC)等调度算法;TCP在上述每种调度算法均支持源地址会话保持，HTTPS/HTTPS在述每种支持的调度算法下均支持Cookie会话保持(包括植入Cookie和重写Cookie)。
	四层负载均衡支持TCP/UDP监听在后端应用服务器无插件模式下直接获取客户端源IP地址。七层负载均衡支持后端服务器应用程序通过HTTP头字段的X-FORWARD-FOR获取客户端源IP地址，支持从HTTP头字段扩展方式获取负载均衡实例Id和负载均衡VIP地址信息。
	七层负载均衡模式下支持配置域名或者URL转发策略，将来自不同域名或者URL的请求转发给不同的云主机处理。
	负载均衡支持配置性能保障型实例，针对不同的业务类型配置不同的规格，其中规格涉及并发连接数、每秒新建连接数、每秒查询请求数。支持

	单实例监听带宽配置，针对同一个VIP内不同的监听端口配置不同的带宽限制值。
	四层负载均衡支持提供主备服务器Active-Standby模式，负载均衡监听的后端添加主备两台后端应用服务器，主备服务器不需要依赖Keepalived、pacemaker等应用高可用组件。
	四层负载均衡支持集群内节点之间的session同步，在单机故障或者升级过程中，TCP长连接无影响。
	私网类型负载均衡场景下，当客户端云服务器和服务端云服务器被分配在同一个物理机host节点时，转发正常。
	负载均衡支持HTTP重定向到HTTPS。
安全性	负载均衡提供监听级别的访问控制，基于监听配置IP地址段白名单，只有在白名单中的IP地址才允许访问负载均衡。
高可用要求	集群应具备高可用性，应支持四、七层的负载均衡高可用性相互独立，当四层或七层中的某一层发生高可用切换时对另外一层不造成影响。

（3）云平台DNS服务

云平台DNS是运行在期货行业云环境的一套DNS产品，可为期货行业云的内网环境（专有云VPC网络、IDC内网）提供域名解析服务。

指标项	具体要求
总体要求	VPC私有域名转发配置管理和解析:支持域名级别的转发操作，将特定域名的解析操作转发到其他DNS服务器上进行解析;支持默认转发功能的配置，将本地不存在的所有域名的解析操作全部转发到其他DNS服务器上进行解析。
功能要求	VPC私有域名和全局域名转发配置管理和解析:支持两种转发操作模式，强制转发模式和优先转发模式。在强制转发模式下，设置只使用转发目的DNS服务器做域名解析，如果解析不到(解析超时)则返回DNS客户端查询

	失败。在优先转发模式下，设置优先使用转发目的DNS服务器做域名解析，如果查询不到再使用本地DNS服务器做域名解析。
	VPC私有域名解析支持租户隔离的功能特性，支持权威域名的添加、修改、备注、删除、批量删除操作的功能，同时也支持根据关键字进行模糊查询，针对每个VPC都可以提供定制化的私有网络DNS解析服务配置，实现VPC粒度的租户隔离功能。
	★支持全局域名的配置管理，满足所有VPC解析同样的域名数据的基础性需求，减少管理员的配置工作。
	支持基于地理位置的全局域名调度和VPC私有域名调度，地域基于内网IP地址段的分配来标注，租户侧DNS云服务可以根据客户端访问的源IP判断地域，并把相同域名解析到不同的后端指定vip上，来实现基于地理位置的流量调度。
	内网权威域名管理和解析:支持IPV6域名解析服务。
	内网权威域名管理和解析:支持域名主机记录的添加、删除和修改操作的功能，支持的记录类型包括A、AAAA、CNAME、NS、MX、TXT、SRV、PTR、NAPTR、CAA。
	支持对地址池内的地址值进行TCP/UDP/HTTP/HTTPS/ICMP等协议的健康检查。
	地址池方面: 支持对地址池内的地址值进行TCP/UDP/HTTP/HTTPS/ICMP等协议的健康检查; 支持地址池的添加、修改、备注、删除、批量删除操作的功能，同时也支持根据关键字进行模糊查询，实现方便的应用服务集群的管理; 支持的地址类型包括IPv4地址、IPv6地址和域名，实现常用的应用服务类型的配置需求;

	支持多个地址记录的负载均衡策略配置，包括:轮询策略(全部返回ALLRR)、权重策略(加权轮询WRR)的负载均衡策略，通过该策略可以按需实现应用流量的全局负载均衡。
	数据同步管理方面: 实现调度实例、地址池、IP地址线路配置、调度域等相关调度配置数据在多个GTM的节点之间进行实时的同步。能够在少于一半节点宕机的情况下，集群可以正常工作; 实现多个GTM集群的合并，组建成一个更大范围的GTM大集群; 同时支持在单机房/多机房故障场景下，实现集群的重建，保证业务连续性; 实现多个GTM集群的合并，组建成一个更大范围的GTM大集群; 同时支持在单机房/多机房故障场景下，实现集群的重建，保证业务连续性。
	调度域方面: VPC私有域名支持配置GTM，即GTM调度域支持选择VPC私有域名; 云内全局域名支持配置GTM，即GTM调度域支持选择云内全局域名; 单云场景支持对租户域名配置GTM，数据在云内同步; 支持调度域的添加、修改、备注、删除、批量删除操作的功能，同时也支持根据关键字进行模糊查询，方便客户自定义私有的调度域。
	调度实例方面: 每个调度实例都支持配置一个客户自定义的CNAME接入域名，实现实例配置记录的解析; 支持为调度实例配置主备地址池，并结合主备地址池的健康检查结果，实现主备地址池的自动切换; 每个调度实例都支持配置多条访问策略，不同的线路(对应解析请求来源

	配置)都可以单独设置独立的访问策略，实现流量的智能调度； 支持调度实例的添加、修改、备注、删除、批量删除操作的功能，同时也支持根据关键字进行模糊查询，实现方便的调度实例的管理。
	调度线路管理方面： 支持基于客户端的源IP地址创建线路，同一个IP地址段可以归属多条线路，多线路之间支持优先级的设定和调整。

5.容器服务

（1）容器服务

容器服务提供高性能可伸缩的容器应用管理能力，支持企业级容器化应用的全生命周期管理

。

指标项	指标子项	
功能要求	多租户	★支持不同租户创建、配置和管理各自的容器集群，支持不同租户
	持久化存储的备份和还原	支持基于云盘的快照和恢复功能。
	权限管理	支持子账号的权限管理，可对集群、命名空间等层次进行权限分配
	容器网络策略管理	VPC网络模式下支持使用网络策略Network Policy，支持入口和出
	路由管理	支持Ingress服务权重配置，使流量按比例分发;支持Ingress配置
	命名空间和配额管理	支持对命名空间的CPU、内存、存储、容器组等资源设置配额。
	配置管理	支持对应用的保密字典进行集中定义和管理，保密字典支持Opaqu
	集群创建/删除	容器服务与云平台无缝对接，能够通过控制台实现集群的一键式
	多集群管理	支持多集群的统一管控。
	集群概览	提供平台看台功能，能够快速查看资源的总体运行状态，包括节点
	节点区域支持	支持工作负载节点跨可用区统一管理。
	节点类型支持	支持GPU类型节点、支持裸金属服务器。
	节点伸缩	支持从Web页面一键式手工自助添加和删除节点，伸缩过程中无需
	白屏化编排	支持页面对资源进行编排，资源包括:Deployment、StatefulSet、

	YAML编排	支持使用yaml文件创建应用，查看已部署应用的YAML文件，可修改
	实例控制	容器实例支持以webshell终端方式进行远程访问控制。
	存储管理	支持从页面上进行容器存储卷（本地存储、块存储、文件存储、对象
	容器伸缩	支持手动伸缩和弹性伸缩，支持手工调整Pod的副本数量进行横向
	GPU虚拟化	支持显存和计算单元的隔离和动态调整，同时避免虚拟化开销。
	安全容器	支持安全容器，安全容器需拥有独立的内核，具备更好的安全隔离
	日志管理	支持日志采集，对容器的标准输出日志和应用日志文件进行采集，
	边缘集群	支持创建边缘集群，支持用将地理位置分布的已有节点作为边缘节
	集群操作审计	支持查看Kubernetes集群中的事件整体概览以及重要事件（访问、时间维度查询。
	监控	支持集群、节点、应用、容器实例层面的监控，支持集成Prometheu
可靠性	Matser节点高可用	Master节点高可用支持5节点和3节点模式，5节点模式下故障2台，
	Worker节点高可用	Worker节点故障迁移时，故障节点上POD自动迁移。

（2）容器镜像服务

容器镜像服务是面向容器镜像等符合OCI标准的云原生应用安全托管及高效分发平台。容器镜像服务与容器服务应无缝集成，帮助期货行业云用户降低交付复杂度。

指标项	具体要求
制品支持种类	支持容器镜像、HelmChart、Operator等OCI制品
制品生命管理	提供高可用的容器制品管理服务，支持制品的上传、下载、删除等功能
触发器策略设置	支持对容器镜像仓库创建触发器，支持全部触发、表达式触发、Tag触发等方式，支持触发器访问记录的查看。
镜像信	支持容器镜像版本的查看，包括镜像的摘要信息、镜像大小、最后更新信息、

息查看	层信息等
镜像跨地域同步	支持跨地域镜像同步场景，支持手动触发某个镜像版本的同步；同时支持基于同步规则，支持镜像推送后自动同步
镜像跨云/跨账号同步	支持跨云及跨账号场景，支持手动触发某个镜像版本的同步；同时支持基于同步规则，支持镜像推送后自动同步
容器镜像的安全托管	提供镜像仓库管理功能，支持命名空间和镜像仓库分级管理，支持公共或私有镜像仓库，其中公共仓库可被系统所有用户访问，私有仓库只能被有权限的用户访问。
权限控制	★支持按照组织架构和项目维度的权限管理，支持RAM子账号权限管理
集成能力	可与容器服务深度集成，在容器服务平台部署应用，支持免密拉取配置，避免每次设置secret，支持可视化选择镜像仓库及版本

6.关系型数据库服务

关系型数据库是一种稳定可靠、可弹性伸缩的在线数据库服务。基于高性能存储，应支持容灾、备份、恢复、监控、迁移等方面的能力。

指标项	具体要求
总体要求	提供稳定可靠、可弹性伸缩的在线关系型数据库服务。
	产品可100%兼容MySQL。
功能要求	创建只读实例支持选择与主实例不同的VPC，满足用户网络隔离要求。
	为了满足大量读请求的应用场景，支持原生只读实例和读写分离功能，可支持不少于5个只
	提供完善的备份、恢复机制，支持手工备份和自动备份，支持物理备份和逻辑备份、逻辑备
	提供数据库自主诊断、慢查询分析，提供全面的健康状态以便用户自动化运维。

	★提供用户可独有CPU资源选择的独享型规格，提供用户可独有整台物理机器的独占型规格
	提供用户自服务门户和API接口:用户可自行创建不同规格的关系型数据库实例，并提供关
	支持业务无中断在线方式升级数据库规格及存储空间。
	支持对MySQL可视化日志管理，包括慢日志、错误日志、数据库主备切换日志等。
	支持虚拟专有网络和经典网络，可支持指定虚拟网络创建数据库实例。
安全性	具备完善的安全防护措施，支持白名单设置、SQL审计等功能。
	支持数据SSL传输加密、透明数据加密。
可靠性	采用全冗余架构，无单点故障。支持单AZ主备高可用。

7.安全服务

（1）安全通用要求

指标项	
总体要求	云平台安全防护系统应主要采用通用服务器(至少支持鲲鹏ARM、海光x86架构服务器)架构，
架构要求	云平台安全防护系统应能够实现与云平台联动，用户业务上线后即自动提供安全保障服务。
功能要求	简化内部网络地址规划，无需现场为每个云安全产品重新规划和配置内部网络。
	★应提供成熟的云安全管理平台，在云安全管理平台中提供的主机安全防护、容器安全、流
	云平台应提供基础的安全审计功能，支持的审计内容包括但不限于网络设备日志审计、用户

（2）主机安全防护

主机安全防护是针对终端进行安全检测及响应的系统。通过使用漏洞和基线配置检测消除系统弱点、预防恶意攻击，提供安全告警实时防御恶意入侵，提供安全态势分析和安全可视化界面，满足事后追溯和分析需求，用于建立完善的云环境终端安全体系。

指标项	
安全总览	支持展示重点关注的资产、漏洞、异常、配置缺陷、事件等信息。
资产中心	支持批量下发资产安全检查，数据导出，以及云外主机解绑等操作。
	支持主机软件安装的资产信息，包括具体软件资产名称、软件版本、软件安装目录、最新采集

	支持主机进程信息，包括进程名、进程路径、启动参数、启动时间、运行用户、运行权限、pid
	支持主机账户信息，包括账户名、登录权限、root权限、用户组、到期时间、上次登陆时间、最
	支持主机的计划任务，包括任务路径、执行命令、任务周期、账户名称，最新采集时间等信息
	支持中间件数据类型，包括中间件名称、类型、版本、PID、安装路径、最新扫描时间、版本验
	支持启动项数据类型，包括启动项名称、命令行、任务路径/MD5、最新采集时间。
安全预防	支持租户漏洞管理，支持主流Linux操作系统，包括Redhat、Ubuntu等。
	支持租户漏洞管理，支持WindowsServer操作系统。
	支持租户漏洞管理，Web-CMS漏洞包括支持包括但不限于74CMS、DedeCMS、Discuz、ECShop、
	支持租户漏洞管理，系统服务弱口令漏洞包括支持包括OpenSSH、MySQL、MSSQL、MongoDB、F
	支持租户漏洞管理，系统服务漏洞包括OpenSSL、SMB、RSYNC、VNC、pcAnywhere、Redis。
	支持租户漏洞管理，应用服务漏洞包括但不限于Tomcat、ApacheStruts2、ActiveMQ、Conflu th、RCE、ThinkPHP、WebLogic、WordPress、Zabbix。
	支持租户弱口令基线检检查，包括检测弱口令账号、可疑的隐藏账号、克隆账号、空密码账户
	支持租户高风险利用基线检查，包括对存在未授权访问风险的应用进行高风险利用基线检查
	支持主机维度进行资产暴露盘点，可提供资产、暴露方式、暴露组件、暴露端口、可被利用的
	支持应用维度进行资产暴露盘点，可提供暴露中间件名称、类型、版本、关联漏洞、影响资产
入侵防御	支持查杀的病毒类型:勒索病毒、挖矿程序、DDoS木马、木马程序、后门程序、恶意程序、高危
	支持进程行为拦截、进程链防御、进程二进制检测、执行脚本检测等能力。
	支持拦截勒索软件、挖矿程序、木马程序、蠕虫病毒、恶意程序、后门程序、DDoS木马、自变异
	支持检测脚本语言bash、python、perl、powershell、vbs、bat、jscript、CSharp、c。
	支持检测批量蠕虫挖矿脚本。
	支持检测开源武器化框架自动生成利用脚本(CobaltStrike、Empire、Metasploit、Nishang
	勒索防护提供对勒索诱捕以及数据恢复风险的监控能力。帮助用户拦截勒索病毒运行，排查
	★支持网站后门防护功能，支持自动拦截黑客通过已知网站后门进行的异常连接行为，并隔
	支持对常用登录地、登录IP、登录时间、登录账号、web目录进行自定义。

	支持威胁检测模块具备350+威胁检测模型，能够覆盖云上95%以上的入侵事件。并按照操作
	支持的告警类型:进程异常行为、异常登录、异常事件、敏感文件篡改、异常网络连接、异常
	支持的情报类型:恶意域名、恶意IP、暗网通信IP、中控通信IP、矿池通信IP、恶意URL、恶意
日志检索	支持登录流水、暴力破解、进程快照、网络连接、端口监听快照、账号快照、进程启动的日志
主机设置	支持云内命令行部署，云外命令行/镜像部署，云外客户端可关联供应商、Region、AZ等环境
	支持Windowsserver操作系统。
	支持主流Linux操作系统，包括Redhat、Ubuntu等。
	支持主流国产操作系统，包括银河麒麟、中标麒麟、统信等操作系统。
	支持客户端使用最低的内存和CPU运行防护工作，cpu占用峰值小于10%、内存占用峰值小于
	支持客户端使用相对高的系统内存和CPU进行防护工作，cpu占用峰值小于20%、内存占用峰
	支持智能化的规则提升告警检测引擎的敏感度，对任何可疑的入侵行为和潜在的威胁提供
	支持客户端进程及文件目录进行保护，防止黑客入侵后破坏agent。

（3）容器安全防护

容器安全防护是面向基于Docker、kubernetes的云原生容器安全统一管理运营平台。

指标项	
资产中心	支持查看集群名称/ID、集群类型、地域、服务器、创建时间、集群状态、风险等级级
	支持查看应用名称、所属集群、创建时间、风险状态及详情。
	支持查看容器组名称、命名空间、存在风险容器数/总容器数、容器组IP、服务器、集
	支持查看容器ID、告警、漏洞、容器组、服务器、风险状态及详情等信息。
	支持查看命名空间名称、集群、创建时间、风险状态等信息。
	支持查看镜像地址/标签、镜像大小、最新发现时间、风险状态等信息。
	支持镜像资产系统漏洞检查，支持主流Linux操作系统，包括Redhat、Ubuntu等。
	支持镜像资产系统服务弱口令检查，范围包括但不限于OpenSSH、MySQL、MSSQL、Mong
	支持镜像资产系统服务漏洞检查，范围包括但不限于OpenSSL、SMB、RSYNC、VNC、pcA

	支持镜像资产应用服务漏洞检查，中间件范围包括但不限于Tomcat、ApacheStruts2 tuatorunauth、RCE、ThinkPHP、WebLogic、WordPress、Zabbix。
	支持镜像资产弱口令检查，包括检测弱口令账号、可疑的隐藏账号、克隆账号、空密
	支持镜像资产高风险利用基线检查，对存在未授权访问风险的应用进行高风险利用基
	支持镜像资产镜像恶意样本查杀，查杀病毒类型包括:勒索病毒、挖矿程序、DDoS木马
CI/CD安全	支持镜像安全扫描系统漏洞检查，支持主流Linux操作系统，包括Redhat、Ubuntu等。
	支持镜像安全扫描系统弱口令检查，包括OpenSSH、MySQL、MSSQL、MongoDB、FTP、VSF
	支持镜像安全扫描系统服务漏洞检查，包括OpenSSL、SMB、RSYNC、VNC、pcAnywhere、
	支持镜像安全扫描应用服务漏洞检查，包括Tomcat、ApacheStruts2、ActiveMQ、Conf CE、ThinkPHP、WebLogic、WordPress、Zabbix。
	支持镜像安全扫描弱口令基线检查，包括:检测弱口令账号、可疑的隐藏账号、克隆账 FTP登录。
	★支持镜像安全扫描高风险利用基线检查，对存在未授权访问风险的应用进行高风险
	支持镜像安全扫描高风险利用基线检查，包括身份鉴别、服务配置、密码泄漏等类型
	支持镜像安全扫描镜像恶意样本检查，查杀的病毒类型:勒索病毒、挖矿程序、DDoS木
容器运行时防护	容器运行安全支持查杀的病毒类型:勒索病毒、挖矿程序、DDoS木马、木马程序、后门
	支持立即扫描:立即下发扫描任务，支持按资产分组下进行策略下发。
	支持周期性扫描:设定扫描周期，扫描指定资产分组下的选定的服务器。
	支持进程行为拦截、进程链防御、进程二进制检测、执行脚本检测等能力。
	支持拦截勒索软件、挖矿程序、木马程序、蠕虫病毒、恶意程序、后门程序、DDoS木马
	支持检测脚本语言bash、python、perl、powershell、vbs、bat、jscript、CSharp、c。
	支持检测批量蠕虫挖矿脚本。
	支持检测开源武器化框架自动生成利用脚本(CobaltStrike、Empire、Metasploit、N
	支持网站后门防护功能，支持自动拦截黑客通过已知网站后门进行的异常连接行为，

	威胁检测模块具备不少于350个威胁检测模型。并按照操作系统、分析对象、攻击手法
	支持的告警类型:进程异常行为、异常登录、异常事件、敏感文件篡改、异常网络连接
	支持云威胁情报，能够有效识别资产中的潜在威胁。威胁情报可以对威胁信息的相关
	支持的情报类型:恶意域名、恶意IP、暗网通信IP、中控通信IP、矿池通信IP、恶意URL
日志检索	提供进程快照、端口监听快照、进程启动的日志查询。

（4）流量安全监测

流量安全监测是通过流量镜像的方式对出入期货行业云环境的所有网络流量进行逐包检测分析和DDoS攻击检测，支持对可疑的网络访问行为进行一键封禁。

指标项	具体要求
部署模式	网络威胁检测响应系统支持旁路部署模式，支持云网络到互联网、云网络到企业内网流量中的攻击行为。
多租户	★支持云原生多租户部署模式，一套集群支持检测不同租户的流量，并支持每个租户账单独立查看安全告警，支持租户配置安全策略，租户配置的阻断策略和白名单仅对租户生效。
检测性能	单集群要求支持最少20G流量，且支持横向扩展。
流量统计	支持根据网络流量大小统计出从互联网、IDC IP地址访问云内主机的流量排名(TOP5或TOP10)，应用类型的分布，支持云内主机网络访问流量的排名。支持查看最近1小时、24小时、7天3个维度的统计数据。
	支持根据网络流量大小统计云内主机到云外的流量排名(TOP5或TOP10)，应用类型的分布，支持云内主机对外网络访问流量的排名。支持查看最近1小时、24小时、7天3个维度的统计数据。
互联网边界	支持查看从互联网边界到云VPC内的流量统计和流量列表。支持查看最近1小时、24小时、7天3个维度的统计数据。

	支持查询互联网边界到云VPC内单个IP地址的网络流量大小、访问目的IP数、应用类型数、会话数进行排序。
	支持查询单个IP的网络访问记录详情，查看IP地址关联的云主机资产，历史网络会话记录。支持查看最近1小时、24小时、7天3个维度的统计数据。
	支持对可疑的网络访问行为进行一键封禁，禁止可疑IP地址出和入方向的网络访问。
内网边界	支持查看从内网边界到云VPC内的流量统计和流量列表。支持查看最近1小时、24小时、7天3个维度的统计数据。
	支持查询内网边界到云VPC内单个IP地址的网络流量大小、访问目的IP数、应用类型数、会话数进行排序。
	支持查询单个IP的网络访问记录详情，查看IP地址关联的云主机资产，历史网络会话记录。支持查看最近1小时、24小时、7天3个维度的统计数据。
	支持对可疑的网络访问行为进行一键封禁，禁止可疑IP地址出和入方向的网络访问。
入侵检测	支持DNStunnel、PowerShell等异常连接行为检测。
	支持对Microsftsharepoint、Dynamics365、OracleWebLogicServer、Apache、CMS等应用的远程代码执行漏洞利用行为进行检测。
	支持对远程代码执行、远程命令执行的攻击行为进行检测。
	支持远程文件包含和本地文件包含攻击行为检测。
	支持检测SQL注入攻击行为，可以防护常见的SQL注入攻击行为和SQL注入盲注行为。
	web攻击，支持目录遍历、目录穿越、任意文件上传、任意文件读取、SSRF、CSRF等web类攻击的检测。
	支持AWVS、Acunetix、masscan、Nessus、nmap、BurpSuite、ZedAttack、appscan、WVS、tangscan、eEye等扫描器的恶意扫描行为进行检测。

	支持针对WordPress、MicrosoftSharePoint、OracleApplicationServer、Apache、WebCMS、Nginx、OracleDB、MySQL、ES等服务的数据泄漏攻击行为进行检测。
	dos攻击检测，支持检测针对web、MySQL、FTP、Samba、OpenLDAP、Redis等服务的拒绝服务攻击行为。
	支持暴力破解攻击行为检测。
	支持常见缓冲区溢出攻击行为检测。
	支持webshell上传攻击行为检测，发现中国菜刀、恶意文件上传。
	支持跨站脚本攻击行为的检测。
恶意软件	支持蠕虫病毒行为的检测，防止蠕虫病毒在网络中下载、传播、通信。
	木马行为检测，支持对FireEye、BlackRAT、SoreFang、Azorult、Rifdoor等数百种后门软件的通信行为进行检测。支持webshell远控通信检测。
	挖矿行为检测，支持对DecredMiner、xmrig等主机挖矿软件行为进行检测，发现消耗主机资源的挖矿行为。
	勒索软件，支持buran、clop、yatron、samsam、badrabbit等勒索软件家族的检测。
	反弹Shell，支持检测linux、windows操作系统中存在的反弹shell行为。
威胁告警	系统支持对检测到的攻击行为生成攻击告警，通过告警详情可查看攻击的IP、类型、威胁等级等基本信息、攻击payload和请求响应报文，支持下载原始pcap包进一步分析。同时还支持查看攻击命中的检测规则以及攻击的原始告警列表。
威胁检索	告警支持按攻击类型、威胁等级、攻击来源IP、被攻击资产IP、HTTP响应码、XFF代理、域名、规则ID、攻击结果、告警来源、部门、标签、防护状态字段进行日志检索。
威胁响应	威胁日志支持一键封禁IP、一键加白等操作，实现对告警的快速处理。

白名单管理	支持白名单策略，加白后不再产生告警。
封禁日志	命中防护策略的流量，会生成封禁日志。封禁日志支持查看流量的源、目的、攻击次数、命中的策略ID，以及命中的规则的名称。支持修改策略的防护动作。
攻击者画像	从攻击者的视图对入侵者的基础信息、威胁情报、攻击手法、攻击目标、攻击过程进行统一的分析展示。
	支持查看攻击过程的详情，支持攻击详细信息的payload和pcap包下载。
网络层防护策略	支持四层防护策略，根据基于源IP、目的IP及端口设置流量观察与阻断策略。
威胁情报	威胁情报开关，支持启用威胁情报对网络流量中的恶意访问流量进行阻断。
应用层防护策略	支持应用层防护策略，基于HTTP报文的字段内容设置观察与阻断策略。
	支持web应用检测配置，对包括webshell上传、SQL注入、跨站脚本、代码执行、CRLF、本地文件包含等多种攻击行为检测。支持启用和禁用web应用检测规则。
端口扫描欺骗策略	支持端口扫描欺骗策略，可添加需要防护的IP和端口，对恶意端口扫描行为进行欺骗。
地址簿管理	支持IP地址簿管理，可以批量管理IP地址，并在防护策略中引用地址簿。
DNS行为分析	支持DGA域名和DNS隧道检测功能，检测可疑DNS请求并产生告警。支持自定义检测时间范围、请求次数、域名总长度。支持可以域名数量和趋势的统计。
加密流量分析	支持SSL加密流量特征检测，发现加密流量中的恶意软件通信行为特征并产生告警。
日志查看	支持查看1小时、4小时、8小时、24小时、7天、30天的流量日志和安全事件日志。

日志检索	支持选择日志中需要展示的字段，并对任意字段内容添加检索条件。
	支持日志导出，支持PCAP包导出。
网络抓包	支持网络TCP/UDP/ICMP抓包分析，支持双向抓包

（5）态势感知

态势感知提供整体安全威胁概览信息，包括总体安全评分、防护资产状态、待处理风险告警、已处理风险等态势信息。提供安全大屏、安全告警处理、攻击分析等内容的展示。

指标项	指标子项	具体要求
总体要求	总览	提供整体安全威胁概览信息，包括总体安全评分、防护资产状态、待处理风险告
功能要求	大屏展示	★提供基于态势感知的大屏展示，包括资产、漏洞、基线、攻击来源、攻击分布等
	攻击分析	支持防密码暴力破解攻击事件的发现，可对黑客进行暴力破解的行为进行实时
		支持定向攻击分析，比对云平台数据，分析出定向的应用攻击和定向暴力破解。
	应用白名单	支持应用白名单功能，针对未经白名单授权的程序进行监控告警，可监控进程名
	资产中心	提供资产中心管理页面，包括服务器资产和云产品资产，展示的信息包括不限于

（6）漏洞扫描

漏洞扫描是结合人工智能技术发现安全风险的智能安全产品，根据设置的已知资产结合漏洞扫描的资产学习模型，对资产进行分析，准确分辨资产来源，发现未知资产，结合漏洞扫描的漏洞检测覆盖能力，及时发现未知的安全风险。

指标项	具体要求
资产管理	支持资产状态检测，资产自动收集、识别资产上线、下线和更新等状态。
	支持资产导入功能，包括域名资产、主机资产、网站资产，实时查看导入进度。
	支持以饼图、柱状图、趋势图等形式展示资产综合状况，支持从资产类型、漏洞类型、主机存活状态、服务类型等角度展示。

	支持大数据分类算法，能够建立精准的资产识别模型，提高识别的精准度。能够识别的服务类型包括但不限于CMS网站应用、数据库服务应用、服务中间件、开源框架、商用软件，识别数量不低于500种。
	支持包括防火墙、交换机、路由器、服务器、应用系统等各类资产识别，资产指纹总数不少于5000条，并支持自动对资产所属设备类型进行归类展示。
	支持主机资产发现，采用TCP_SYN、ICMP_ECHO、UDP、TCP_ACK、SCTP等多种方式，同时支持IPV6扫描，并支持探活端口设置，全天候巡检发现资产更新并展示。
	支持主机资产的内外网识别，同时获取资产存活/更新状态、关联域名、操作系统、端口、服务、中间件、地理位置、漏洞信息、WAF、CDN、指纹、来源、扫描时间等信息。
	支持VPC侧扫描自动导入虚拟云主机资产，可手工添加扫描目标IP。
	支持自定义nameserver、IP/域名矫正，分析域名资产解析状态，获取域名资产whois详细信息。
	支持网站、主机可用性监控，设定监控相关参数，包括但不限于监控目标、监控频率、请求方法、响应时长上限、响应码及丢包率等信息。
	支持通过自定义分组、负责人、手机、邮箱、标签、资产来源及变动等属性对资产进行业务化管理。
	支持资产更新分析，自动收集资产更新前后信息，并针对更新内容进行重点对比展示。
	支持自定义导出资产综合报表和资产报表，导出格式包括但不限于Word、Html、Excel等。
弱口令	支持运维弱口令检测功能，包括mysql、SSH、FTP、Redis等主流服务口令检测。弱口令字典可以自定义设置。

漏洞发现	系统漏洞库能够覆盖常见的操作系统漏洞、软件漏洞、最新的网站框架应用漏洞等，能够针对操作系统 以及Web漏洞进行检测，漏洞标准兼容CVE、CNVD等 。
	支持CMS应用漏洞、运维安全漏洞、弱口令、Web漏洞、基线监控、合规漏洞等风险检测。
	针对云平台产品的漏洞，支持漏洞原理性插件检测，分析风险危害并给出相应建议。
	★支持突发事件应急检测，能够针对单个或多个漏洞进行指定资产范围内的风险发现。
	支持自定义资产白名单，系统对白名单内资产不进行资产监测或风险扫描。
	支持设置资产巡检周期，自定义扫描周期、扫描开始/结束时间、扫描速率、探活发包协议、端口策略、漏洞类型、User-Agent等信息。
	支持资产发现和漏洞扫描的可视化展示，显示巡检周期数、巡检进度、巡检状态等。
风险分析	支持资产风险分析，包括但不限于未修复、已修复风险、已确认、待确认、已忽略等不同风险维度展示，同步展示漏洞数量趋势、风险生命周期等信息。
	支持漏洞风险TOPN展示，包括但不限于应用漏洞、运维安全风险、风险资产、弱口令等。
	支持通过资产指纹进行漏洞分析，并从资产的类型、服务版本、漏洞类、漏洞严重程度等多个维度进行关联分析。
	支持漏洞风险分析，包括但不限于风险概述、风险地址、风险类型、风险描述、风险危害、风险细节、修复建议以及原始请求与响应等信息。
	支持漏洞闭环管理，能对漏洞进行确认、忽略。

（7）应用安全防护

应用安全防护（Web应用防火墙）通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP攻击，过滤海量恶意访问，避免应用资产数据泄露，保障应用的安全与可用性。

指标项	具体要求
协议识别和解码	★支持http、https协议流量识别，具备http协议深层解码能力，支持递归解码，解码方式包括:URL解码、JSON解码、Base64解码、16进制转换、斜杠反转义、XML解析、PHP反序列化解析、UTF-7解码等。
攻击检测	支持SQL注入攻击检测，通过解析http协议中payload内容，识别符合sql语句的特征，评估威胁等级并阻断。
	支持SQL非注入型攻击检测，如完整SQL语句执行。
	支持XSS注入检测，通过分析Html片段的DOM结构，解析存在的JS片段，进行分析，根据分析结果评估威胁等级并阻断。
	支持非XSS注入型攻击检测，如完整Html页面。
	支持信息泄露检测，检测内容包括测试文件、备份文件、代码仓库和服务器敏感文件等。
	支持WebShell检测功能，通过检测上传文件的特征和分析访问行为，检测Web请求是否存在上传WebShell或调用WebShell的行为，实现告警和阻断。
	支持反序列化攻击检测，支持PHP、JAVA语言的反序列化攻击检测，能够识别相关程序语言的序列化流并进行分析、解码，进行告警和阻断。
	支持CSRF和SSRF检测，通过分析Payload代码特征，告警并阻断相关请求。
	支持机器人检测和防御，能够识别扫描器检测、爬虫检测、非浏览器请求。
	支持深度检测功能，可在站点详情中的防护配置页面开启深度检测，即使该请求已在检测过程中已被判断为拦截，仍可继续进行所有攻击检测模块的检测，完整地记录攻击检测信息记录，便于进行更完整的分析。
	支持文件上传、文件包含攻击检测。

	支持代码注入、命令注入攻击检测，支持检测上传文件中是否包含Java、Php代码注入信息。
	支持服务器响应信息检测，防止响应错误信息包含服务器列目录、SQL报错、服务器异常信息等。
	支持CC攻击防护，通过限制IP和Session实现对异常访问行为的限制，并内置Session系统。
	支持智能语义分析引擎，不需配置规则即可完成对XSS、SQL注入、命令注入、SSRF、CSRF、PHP反序列化、Java反序列化、文件上传、PHP代码注入、Java代码注入等攻击类型的检测，在功能界面上可以以开关方式控制以上Web应用攻击检测引擎。
	自定义规则的攻击类型可配置超过35种。
	具备0day漏洞防护能力，实现告警和拦截。
	支持本地可存储的威胁情报防护，威胁情报数据可完全存储在设备中使用。
	支持威胁情报规则，包含【威胁情报置信度】、【情报等级】、【威胁标签】、【最近发生时间】作为规则匹配条件。
	支持网页防篡改能力。
	消除误报功能配置中规则的使用范围支持自动化添加站点或者域名筛选功能。
业务管理	提供准确有效的攻击行为分级策略，包括低危、中危和高危，在拦截日志中明确体现。
	攻击检测日志应包含完整的事件信息，包括攻击类型、风险等级、攻击向量、完整请求信息等，支持报警日志下载。
	攻击检测日志可配置UTF-8/GBK编码。
	支持按源IP聚合的方式展示攻击检测日志，支持进行聚合时间、展示条数的配置。

	支持点击统计数据可跳转到对应的日志详情。
	支持防护策略(策略模版)筛选。
	支持在界面查询各个防护策略生效的站点列表和不使用防护策略的站点列表。
	VPC侧添加站点vip支持自定义。
	创建站点时，支持自定义vip输入校验。
	添加防护站点，回源到指定实例，支持按实例名称搜索功能。
	支持访问IP溯源，能够从Socket、X-Forwarded-For和任意Http头中获取访问源IP。
	支持站点全量访问日志的完整记录功能，属性包括:站点信息、访问地址、源IP、请求方法、响应码、请求开始时间;查看详情功能提供分类查看日志详情，可分为访问日志详情、请求检测信息、响应检测信息、HTTP响应展现。
	支持站点列表表头字段自由配置。
	支持实时防护状态监控，包括但不限于实时请求数、攻击数、拦截数和检测耗时。
	支持定时或手动生成报告，可筛选报告类型和自定义配置报告内容。
	支持Cookie防篡改，可配置三种防护方式，结合“观察”和“拦截”两种响应方式。
	支持IP组功能，进行配置的模块包括:自定义规则-匹配条件、访问频率控规则、不限制这些用户以及源IP获取方式-信任IP。
	访问频率限制规则的观察模式，为对满足访问控制规则的请求信息进行日志记录，不生效限制动作。
	提供EIP和SLB-inner配置API接口，以支撑WAF EIP接入防护。
	支持站点创建的权限操作:租户不具备添加站点功能的操作权限，可以对已创建的站点进行防护规则的配置。

	允许同一个站点在互联网侧、VPC侧分别配置。
Web应用管理	支持SSL证书卸载功能，能够上传证书实现加密协议检测。
	支持批量替换证书。
系统管理	支持用户名、证书登录。
	系统用户支持启用/禁用。
	支持Syslog日志外发。
性能要求	单检测节点http每秒处理请求数能力>=20,000
	单检测节点https每秒处理请求数能力>=5,000
	数据延迟小于5ms

（8）数据库审计

数据库审计实现自建数据库、云数据库服务访问过程和行为的审计。

指标项	指标子项	
部署方式	部署方式	部署agent插件来获取网卡的流量：1）自建数据库（虚拟云主机）方式
		可以实时监控agent CPU使用率、内存使用率、传输包个数。
		agent参数支持自定义，支持IP、CPU占用率、内存占用率、本地缓存大
		支持WEB界面管理插件，支持插件的配置、唤醒、挂起、中断、升级等操
功能要求	协议支持	★支持Oracle、SQL Server、PostgreSQL、MySQL、MongoDB、MariaDB等
		支持Teradata、Cache、人大金仓、达梦、神通、南大通用、华为Guass等
		支持RDS MySQL、RDS SQL Server、RDS PostgreSQL、RDS MariaDB、RDS
		支持访问来源信息：客户端IP、端口、数据库名称、数据库用户、OS用
		支持SQL语句信息：SQL标识、操作类型（DDL、DML、DCL等）、影响行数
		支持数据库告警功能，支持对根据IP、账号、客户端工具名、时间等定
		支持数据库漏洞扫描。
	结果集审计	支持按照策略进行结果集审计。

		支持通过返回行数和内容大小控制返回结果集大小，降低系统开销。
	安全审计	内置安全特征库规则，如SQL注入、缓冲区溢出、权限提升、数据泄露、
		应具备漏洞攻击规则库，漏洞攻击规则应至少包括：漏洞名称、CVE标识
		支持识别口令猜解攻击，以及在同一个会话里，相同IP、数据库用户的
	审计策略	可自定义审计策略，规则各条件之间支持与或非逻辑关系。
		结果集审计支持全局开启，也支持按照具体策略进行结果集审计开启的
		告警数量需支持最大告警数量限制，超过告警阈值之后便不告警。
	审计查询	支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命
		支持将常用的查询条件保存成固定查询模板，方便后续快速查询。
		支持对查询结果中可能存在的敏感数据进行掩码处理，防止敏感数据泄
		支持对查询结果以CSV文件格式导出到本地。
		支持SQL语句自定义业务化语言翻译。
	统计报表	系统提供多种报表模型，分别基于全库、数据库组和单库维度进行展现。
		支持合规性报表，如PCI、等级保护、SOX法案等专项报表展现。
		支持专项报表展现，针对风险、性能、访问源、账户等信息做专项报表
		支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种
		支持按日、周、月等时间周期生成报表。
		支持报表数据后台定期预生成，保障报表数据展现速度。
		支持将报表按指定的时间推送至指定管理员的邮箱。
		报表支持以Word、PDF、HTML等格保存到本地。
	会话分析	支持会话级检索和详情展现：包括在线的并发会话、活跃会话、失败登
		支持失败登录会话查询和统计：包括客户IP、数据库用户、操作系统用
	统计信息环比	获取同一数据库不同时间段及不同数据库同一时间段的SQL语句量和会话
	行为建模	可基于单个数据库建立学习期，默认学习期内行为可信认，学习期结束
	数据管理	日志备份与恢复管理，支持审计日志数据的备份与恢复，支持自动备份
		支持SYSLOG方式进行审计数据外送。

	IP别名管理	支持客户端IP别名设置，针对不同客户端IP自定义别名展现。
	分组管理	支持IP地址、数据库用户、时间、对象、应用用户分组，并且分组对象
	告警管理	风险告警内容支持触发规则风险内容，并支持根据风险等级高、中、低

（9）数据梳理及脱敏

数据梳理及脱敏包括数据梳理和数据脱敏两个主要功能。数据梳理对资产安全状况摸底及资产管理工作，做到对风险预估和异常行为评测，避免核心数据遭破坏或泄露的安全事件。数据脱敏对敏感数据进行屏蔽、随机替换、乱序处理和加密，将敏感数据转化为虚构数据，隐藏真正的隐私信息，为数据的安全使用提供基础保障。

指标项	指标子项	
功能要求	敏感数据自动发现	系统应支持敏感信息的自动发现能力，系统具有内置敏感数据特征库，能对身、回乡证等敏感信息自动识别。
		系统能读取数据库或txt、csv等文件内容，根据内容和内置敏感数据特征规则
	数据库类型	支持多种数据源，包括:Oracle、SQL Server、MySQL、PostgreSQL等多种数据
	脱敏方式支持	系统支持自定义、图形化操作的脱敏规则和脱敏方式，支持UNICODE标准、中文
	脱敏任务管理	支持对脱敏任务进行停止、启动、重启，并且支持任务并发，充分利用系统资源
	自定义函数	对有特定业务需求的敏感数据可通过自定义发现函数实现和自定义脱敏函数

（10）敏感数据保护

敏感数据保护关注云端数据安全，通过智能化的手段识别敏感数据，基于业务需求实现自动分类分级，并在此基础上通过敏感数据脱敏进行保护、结合数据异常行为检测和智能安全审计，做到数据安全可见、可控和合规。

指标项	
数据识别	支持基于内置及用户自定义的识别规则，实现针对敏感数据的识别能力。提供对结嵌套文件），支持OCR技术识别图片敏感数据。
	支持对授权范围内的数据资产进行自动扫描，并在完成扫描后持续监控数据资产

	内置数据分类分级模版，用户可基于内置模板通过来定制属于自己的分级分类模
	支持敏感等级的增加、删除、修改，最多可设置10级敏感等级，支持手工订正识别
数据资产分析	资产地图:支持统计敏感数据、异常事件等数据安全态势数据，动态展示数据流转
	用户帐号分析:支持RDS实例账号和RAM账号的总用户数、休眠用户数、活跃用户数
	权限分析:支持定位各租户账号对相应数据资产的权限，并支持对持有数据资产权
	支持对资产进行全面分析，通过资产管理和安全保障、异常和审计事件、敏感数据
	支持对资产有危害性的操作分析报表，提供入侵防范与监控、恶意代码监控、安全
数据资产授权	支持一键发现并接入云上数据资产，支持免输入密码一键授权数据识别、数据脱敏
数据审计	支持资产的实例、库、账号、源IP地址、返回行数、时间等日志信息，用户可通过搜
	支持数据资产命中审计规则的结果、命中规则的操作类型和操作账号等日志信息。
	支持数据资产的安全审计功能，提供了包括审计规则命中结果、审计规则检测的资
	支持内置与自定义的审计规则。内置数据库、OSS审计规则，数据库审计规则包含
数据泄漏风险检测	支持对预置与自定义的异常事件进行集中化的处理，提供基于部门账号、事件类型
	支持内置与自定义的异常事件规则。对于内置规则，支持集中化的规则启用与相关
数据脱敏	支持生产数据向开发测试环境脱敏转存，避免直接访问敏感数据带来的数据泄漏
	支持用户为指定敏感数据、敏感字段配置相应的脱敏算法、脱敏方式，并保存成脱
	支持动态脱敏功能，您可以通过调用ExecDatamask接口对数据进行动态脱敏。
	支持6大类共30种常见的脱敏算法，包括哈希、遮盖、替换、变换、加密及洗牌，能够

（11）应用身份服务

应用身份服务实现构建一套统一、高效、安全的统一身份认证平台，满足现有业务系统传统WEB端及未来移动端等多领域需求，提升对内、对外网上业务服务能力。

指标项	具体要求
操作日志	支持根据账户、应用、日志类型进行日志查询，并提供日志导出、设计报表功能。
进出日志	提供账户级别的登录、退出日志。

应用列表	支持应用查询以及应用的启用/禁用、查看详情、修改等功能。
添加应用	支持JWT/OAuth/OIDC/SAML/CAS协议应用的创建。
应用授权	支持应用、账户维度的授权管理。
权限系统	管理自身系统权限，也可以管理第三方应用的二、三级授权。
分类管理	提供分类创建功能，进行账户的分类管理。
机构及组	支持组织机构、账户的创建以及AD、LDAP、SCIM接口等方式同步数据。
账户管理	针对账户的管理功能，不限于启用/禁用、重置密码、启用/禁用二次认证等功能。
RADIUS	支持对接RADIUS实现对防火墙、堡垒机、WIFI等设备的统一认证。
认证源	支持接入外部认证源。
证书管理	为用户分配手机、PC端两个证书，实现双向TLS认证。
个性化设置	允许管理员设置公司的基本信息，包括图标、登录页等。
安全设置	支持配置密码策略、短信、邮件网关;支持配置OTP认证;对接UEBA、实人认证等。

（12）密钥管理服务

密钥管理服务是一款云上密钥管理产品，基于商用密码机，为云产品和云上用户应用提供符合国密要求的云原生密钥管理服务和轻量级的应用加密服务。针对本项目提供云平台底座需要的密钥管理服务能力。

指标项	具体要求
密钥管理	提供密钥创建、启用、禁用、计划删除、BYOK等功能。
签名	提供数据对称、非对称加解密，签名等功能。
安全性	支持通过密钥版本化和定期轮转来加强密钥使用的安全性。
容器部署	支持容器部署。

（13）加密服务

加密服务是一款云上密码机资源管理服务，通过密码机硬件虚拟化技术，提供云平台需要的加密服务能力，为用户提供弹性、安全、稳定的云密码机实例服务。

指标项	具体要求
实例管理	提供底座云密码机实例的开通、配置、释放、删除等功能。
HSM管理	提供添加HSM、配置网络、漂移HSM、升级HSM、重载HSM等功能。
VSM管理	提供VSM网络配置、导出镜像、升级、重启等功能。
	管理VSM管理的数据影像，可以用于恢复操作。
兼容性	提供通过国密检测认证的云密码机。

（14）堡垒机服务（含平台侧和租户侧）

堡垒机为云平台侧和租户侧的资产的运维提供完整的审计回放和权限控制服务。基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的4A统一管理方案，通过账号管理、身份认证、授权管理、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

指标项	
系统用户管理	支持用户安全策略功能，如密码最小长度、密码使用限期、密码复杂度要求、密码重
	支持用户/用户组的多级架构管理，可以复制、剪切、粘贴、移除用户/用户组，实现用
	支持用户的移交功能，可以将用户的群组属性和权限交接给其它用户。
	支持多种认证方式:本地静态密码认证、RADIUS认证、LDAP认证、AD域认证。
	支持认证方式全局设定。支持单一用户认证方式设定;支持多种认证方式组合。
主机资产管理	支持常用的运维协议:SSH、TELNET、RDP、SFTP。
	支持主机/主机组的多级架构管理，可以复制、剪切、粘贴、移除主机/主机组，实现主
	支持主机连接性测试，验证主机的连接协议及相关账号密码的正确性，支持配置定期
	支持自动发现主机，可设定检测网段和服务端口进行扫描。
访问授权管理	支持通过基于时间、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字
	支持对重要设备启用登录审核策略:运维人员须向管理员申请登录，管理员允许之后
	支持对重要设备启用登录备注策略:运维用户访问设备时必须先填写该次访问的目的

	支持对重要命令进行实时审核:运维人员执行命令后，系统响应动作包括:实时审批、
	支持粗放式访问授权策略:授权条件仅基于运维用户(用户组)和目标主机IP地址段，
	支持登录预处理命令设置:登录成功后，自动执行指定的操作命令。
	支持协同会话功能，支持运维空闲会话时间全局设置限制功能。
运维方式支持	Web访问方式:支持使用浏览器直接调用H5控件实现运维操作;支持Web页面调用DB2c
	Web访问方式:支持运维用户个人保存未托管的目标主机账号密码;支持运维用户快速
	Web访问方式:支持批量启动目标主机;支持批量在目标主机组上执行脚本文件。
审计记录及检索	资源菜单访问方式:支持使用Windows远程客户端连接堡垒机图形化资源菜单(支持M
	客户端访问方式:支持使用SQLManager、Navicat、ISQLW、DBVisualizer、mstsc、Xsh
	支持对RDP屏幕文字内容、标题窗口、键盘输入的记录和搜索定位。
	支持全字段搜索审计日志，只需通过关键信息快速搜索定位。
	支持将常用查询条件设定成模板，供多次引用。
	支持日志关联分析，可直接关联到日志同个会话中的所有操作日志。
	支持会话录像在线回放、定位回放及下载后使用官方专用客户端离线回放。
密码安全管理	支持按设备、数据库、系统帐号、计划执行时间、改密周期、密码策略、改密结果发送
	支持随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并能
	支持手工执行改密功能。
	支持改密结果自动发送至密码管理员或FTP上传;支持手工下载全部或部分主机密码
	支持自动改密结果报表。
	支持系统操作日志的查询和统计。
系统管理	提供在线排错工具:ping、telnet、tracerroute。
	支持启停运维协议服务。
	支持邮件、短信、syslog等输出接口配置。

（15）云安全管理中心（含安全日志分析和自动编排）

云安全管理中心提供数据集中整合、资产及业务风险评估、智能分析检测、安全生态协同等能力，支撑云环境中的日志审计查询、高级持续性威胁检测及溯源、云主机资产监控管理、实时威胁处置、自动化安全编排等场景下的安全运营需求，帮助打造云环境的全方位、全生命周期的立体化安全运营中心。

指标项	技术要求
运营中心	支持安全告警总数、处置闭环率、处置动作占比、告警风险级别、告警数据源、告警类型分布、TOP10攻击源IP、TOP10被攻击IP等告警数据统计。
	支持发生时间、攻击IP、被攻击IP、告警类型等多维度条件进行安全告警聚合，并以聚合列表的形式呈现，支持查看安全告警详细证据信息。
	支持通过主机安全、网络安全、应用安全的API接口进行安全告警的响应处置
	支持时间范围、告警数据源、告警类型、告警级别、处置状态、自定义标签等多维度条件的安全告警筛选查询，并保存为安全告警快速筛选条件。
态势监控	支持云环境全局新发现网络攻击、异常行为、安全脆弱性、防护组织、TOP5(或TOP10)遭受攻击组织、TOP5(或TOP10)待处理异常行为、TOP5(或TOP10)待处理脆弱性等数据统计呈现。
	支持云主机保护在线率、新增云资产分布、防护资产类型分布等数据统计。
	支持网络攻击类型分布及最新网络攻击事件、异常行为类型分布及最新异常行为、安全变化趋势等数据的统计呈现。
风险分析	支持云环境全局威胁事件集中呈现，包括威胁名称、威胁类型、ATT&CKID、威胁描述、处置建议、网络协议、源/目的IP及端口、匹配已知威胁情报、域名、文件名、进程信息等关键信息。
	支持威胁事件风险判定的证据信息，并按照KillChain各阶段进行映射关联。

	支持威胁事件一键转换为响应事件，将威胁事件相关信息导入到响应编排中心。
	支持时间范围、攻击源/目的IP、威胁事件级别、威胁类型、攻击阶段、自定义标签等多维度条件的筛选查询。
	支持云平台和租户侧资产的违规安全配置基线集中呈现，包括基线名称、风险分类、风险等级、受影响资产、资产归属组织、基线详细描述等信息。
	支持租户侧资产安全漏洞信息集中呈现，包括由漏洞名称、漏洞类型、漏洞等级、CVEID、受影响资产、资产归属租户、修复建议、处理状态、解决方案等信息。
	支持租户侧租户、流量方向、租户各IP及相应流量大小的统计信息呈现。
资产管理	支持云平台资产信息的采集，并以列表的形式进行呈现，包括服务器名称/ip、操作系统、异常行为、在线状态等信息。
	支持资产IP、用户UID、主机地域、内网IP、在线状态、主机UUID、主机别名等基础信息查看。
	支持资产异常行为详细信息查看，包括异常等级、异常名称、异常类型等信息。
	支持基于服务器名称或Ip地址进行资产筛选查询，支持一键导出资产信息列表。
	支持租户侧云主机或虚拟化资产的信息采集，包括云主机、云数据库、云存储、负载均衡、弹性外网IP和Tunnel等资产实例信息。
	支持资产类型分布、近一日新增资产、公网开放资产类型等信息统计。
	★云主机资产以列表形式集中呈现，包括IP公/私网地址、所属组织/单位、所属VPC、运行状态、操作系统、是否为新增、可疑安全组、安全告警、脆弱性风险、网络攻击、Agent状态、快照、内存、磁盘等信息，支持单资产详细

	网络攻击、异常行为、脆弱性风险的信息查看。
	云存储资产以列表方式集中呈现，包括云存储实例名称、组织、磁盘占用、是否为新增、访问权限、referer配置等信息。
	云负载均衡资产以列表方式集中呈现，包括ID/名称、IP地址、组织、是否为新增、运行状态、监听端口等信息，支持单资产详细网络攻击、异常行为、脆弱性风险的信息查看。
	云弹性外网IP资产以列表方式集中呈现，包括ID/名称、运行状态、是否为新增、带宽，支持单资产详细网络攻击、异常行为、脆弱性风险的信息查看。
	支持多维度条件的资产筛选查询，支持一键导出资产详细信息列表。
响应编排	支持通过流式告警、定期任务、人工执行剧本生成案件，支持查看案件内关联的数据信息。
	支持联合作战室和机器人助手，针对告警和恶意行为进行调查和阻断。
	支持安全处置经验知识库。
	内置丰富的日常安全告警处置和联动封禁等自动化安全运营剧本。
	支持通过拖拽和配置方式，自定义业务场景的剧本。
	内置安全组件实体，可进行各种安全资源的调度，下发动作执行动作指令。
日志管理	基于审计日志的任意字段及内容进行统计计数、最大值、最小值、平均数、总和等统计，并以柱状图、折线图、饼图、单值图、表格的形式进行呈现。
	支持基于时间范围、所属组织、数据源、日志字段、日志内容等条件进行全局标准化日志的检索查询。
	支持通过关键字与/或/非/大于/小于/等于等逻辑表达式进行日志检索查询，支持关键字模糊匹配查询，并支持保存为快速日志查询条件。
	日志查询结果支持结构化数据列表和Syslog格式数据列表的呈现方式，所有日志字段支持灵活自定义和字段累加统计。

	支持查看平台侧审计时间范围内，指定日志源的审计日志查询。
	支持关键字和JsonDSL两种日志查询方式。
	基于日志查询结果可自定义统计计算窗口，并在日志概览中进行呈现。
	审计日志支持一键导出到Excel。
	支持安全网元日志源的内置接入，同时支持第三方产品日志源通过Syslog方式的手动配置接入。
	支持主机安全、云安全流量监测、Web应用防火墙、堡垒机等安全网元内置日志解析模板，同时支持第三方安全网元内置日志解析模板。
	支持新建日志解析模板，以完成第三方接入日志自动化解析，支持Json、JsonArray、JsonCut、JsonArrayCut、grok、keyValue等日志拆分解析方式，同时支持解析日志的时间戳格式化、添加字段、删除字段、脚本格式化等格式化处理。
	支持脚本或手动选择进行标准化日志字段关系映射。
	支持指定日志源外发标准化日志到其他第三方服务器。
报表管理	支持生成指定租户的数据报表日报、周报和月报，并发送到指定邮箱。
	支持生成数据报表任务的查看和数据报表在线下载。
	支持以列表的形式进行报表生成任务管理。
规则管理	支持内置关联分析规则，包括威胁名称、威胁级别、威胁类型、攻击阶段、ATT&CKID、威胁描述和处置建议等属性信息，并支持规则自定义。
	自定义关联条件支持以顺序发生和同周期内发生两种关联时序，可基于日志范围、源/目的IP、日志字段、周期内日志数量等属性条件进行关联。
	支持以列表的形式进行关联检测规则管理，支持威胁级别、威胁类型、威胁名称等多维度条件进行规则筛选查询。
	支持手动添加IP封禁策略到云安全流量监测，并支持IPv4和IPv6协议，支持

	源/目的IP、目的端口、封禁时长、封禁类型等策略属性配置。
运营管理	支持审计，可查看指定时间7天以内的日志概览统计，包括原始日志趋势、审计事件趋势、审计风险分布、危险事件分布、存储用量、审计类型等。
	支持云平台数据库、主机、网络设备用户操作事件采集、审计、查询，包括资源管理事件、数据库攻击、错误事件、更改事件、访问事件、资源管理事件、权限事件和账号事件。
	审计日志支持按指定时间搜索和趋势呈现，支持基于关键参数值进行筛选查询。
	支持审计规则配置、查询、管理，规则配置支持审计类型、审计对象、操作类型、操作风险级别等属性，并按照发起者、目标、命令、结果、原因的关键字等于、包含、正则匹配审计日志。
	支持指定审计类型、审计对象、风险等级的审计日志告警配置，并向指定邮箱发送告警通知。
	支持审计日志自动化归档、导出下载管理。
	支持以txt格式批量导入IP地址及地理位置对应关系。
事件调查	支持基于安全管理中心告警事件自动执行剧本，并生成案件。
	定期设置定期任务，在特定的日期和时间周期性地执行剧本，生成任务。实现周期性的安全调度。
	支持人工手动触发剧本，开始事件调查。
	支持查看本周和今日新增的案件数，统计平台内所有待处置的案件，统计平台自动响应案件数。
	支持展示平台内所有案件的列表。通过案件名称、案件状态、部门、案件创建日期对案件进行检索。
	支持人工新建案件，主动开启事件调查。批量修改案件状态。

	支持以对话的交互方式在联合作战室中下发指令，发送协同消息。
	支持多人在联合作战室中协同工作，发送消息、共享安全告警信息和事件调查的结果，实现安全事件的协同处置。
	联合作战室中集成了机器人助手，支持通过机器人对案件执行剧本，实现对安全事件的快速响应。
	能够自动提取案件中的IP地址、文件记录等实体，可以对实体下发各种命令，并能对实体状态持续跟踪。
	安全事件中执行的所有动作的记录。
	支持查看和执行的定期任务。查看任务执行记录和输出的数据。
	支持自定义作战室中的响应动作，并在作战室中调用，扩容事件响应的场景。
自动编排	内置日常运营巡检、护网封禁、资产信息富化等不少于5个剧本。
	支持可视化的拖拽的方式在线编辑剧本。
	支持用户创建自定义剧本，设置剧本启动的类型。
	支持在剧本内引用子剧本。
	支持对剧本进行断点调试，设置剧本中的动作为调试点，剧本运行到调试点之后停止，可以随时测试剧本设置和流程是否正常。
	支持通过复制的方式创建剧本，查看剧本运行情况，启用、禁用剧本。
	支持查看剧本的执行结果，查看剧本每个节点的输出记录。
	支持开始、结束、数据汇聚、数据过滤、等标准动作。
	支持接入自定义安全资源。
	支持安全资源动作管理，设置自定义资源支持的编排动作以及动作的参数。
	支持在线调试自定义动作的python代码。
知识管理	情报概览可以查看平台内生成的情报总数、已封禁情报数、已解封情报数。

	情报管理页面展示通过自动剧本或手动执行动作封禁的所有威胁指标。
	手动添加本地自定义情报。
	支持将本地的自定义情报推送到网络威胁检测产品、web应用防火墙(WAF)安全设备，实现情报的全网快速封禁。
	可以查看通过对恶意指标执行的封禁策略，可以解封或添加新的封禁策略。
	允许用户创建和管理知识库。支持列表知识库和二维表知识库。
	允许用户人工或通过剧本向知识库中添加IP地址、文本、数字等信息。用于记录安全事件调查过程中产生的知识。
系统管理	允许用户配置系统功能所需的公共参数，如多租户信息、钉钉token等
	支持通过流式数据接入同一安全厂商的安全管理中心的安全事件源，实时响应告警。
	显示剧本执行日志，可以查看剧本的执行记录、运行条件、输入数据等。

7.云备份服务

提供云主机整机备份与恢复服务。

指标项	
兼容性	支持本地、异地多场景的备份统一管理。 支持对云数据库、存储、大数据等产品进行统一备份和恢复管理。备份可以兼容Intel、海
架构	支持ENI弹性网卡(elastic network interface)绑定云服务器，在多个云服务器间自由迁
云主机备份	★以虚拟机整机(云硬盘)、文件维度备份，支持按照虚拟机操作系统中的文件路径进行备

8.云管理平台

（1）多云管理平台

多云管理平台提供全方位的云资源供给、运维和运营管理能力，具备一体化管控、自动化运维、智能化分析功能。

指标项	指标子项	具体要求
功能要求	配额告警	配额支持查看历史告警。
	资源监控与告警	提供云环境中的云产品资源实例提供租户级的资源监控能力，提供云产品资源实例提供租户级的告警通知能力。
	资源运营分析	支持以组织和资源维度统计资源报表、配额报表和云监控报表，支持异步导出的各类统计分析报表。
	资源集管理	支持创建/修改/删除/查询资源集。 支持查看/跳转到资源集所有的资源实例，通过资源集管理用户、用户组。 支持对于region和集群，设置不同的名称，便于管理。
	配额管理	支持对于不同的region区域，设置每个云产品可以使用的资源量； 支持对于不同的地域区域，设置不同组织可以使用的云产品的配额总量。
	云产品资源管控	提供IaaS/PaaS/SaaS类云产品及服务的资源操作控制台
	工作台功能	提供用户登陆后的工作台，显示角色相关的关键运营数据。
	用户管理	创建/修改/删除/恢复/禁用/激活/查询用户、查询/修改/重置密码、变更归属、角色授权、用户组管理、登录策略设置。
	用户组管理	支持创建/修改/删除/查询用户组、添加/删除用户；支持用户组与角色关联。
	组织和资源池配置	支持配置云环境的地域和集群与组织的映射关系，查看地域和集群资源使用情况。
	组织管理	支持创建/修改/删除/级联删除/查询组织、变更资源组织归属。支持通过组织查看、删除、导入用户信息。

	规格管理	支持云环境中云产品的可用规格的录入/禁用/启用/查看管理。
	角色管理	★提供角色创建、修改、删除、禁用功能;支持自定义业务角色，设置角色所具有的操作权限，并将角色管理给相关用户;支持复制/查询角色，支持设置角色所能查看的首页仪表盘布局，以及相应的可视化控件。
	计量管理	按时间/按组织维度计量、计量报表查询、计量报表导出。
	资源分析	提供资源分析仪表盘，支持按类型、地区、性能、告警、利用率等多种维度的资源实力数据图形化展示以及关键数据的报表导出功能。
安全性	密码策略管理	提供统一的用户密码策略配置，支持强密码、密码有效时间以及锁定策略。
	日志管理	提供日志审计功能，保留所有用户的操作日志，并支持日志的过滤和导出功能。
	登录策略管理	创建/修改/删除/禁用/激活登录策略、支持白名单、支持黑名单、关联用户、关联组织;支持按照登陆时间和IP地址的白名单/黑名单策略;支持设置能看见并使用这个登陆策略的组织。
易用性	个性化设置	支持设置默认语言、风格/主题颜色/品牌信息个性化。
	多语言管理	提供多语言切换功能，默认支持简体中文、繁体中文和英文，并支持设置默认显示语言。
	菜单管理	支持创建、自定义、删除、启用、删除自定义菜单功能

（2）云运维管理系统

云运维管理系统提供一个统一的运维界面，包括基础设施运维、云产品和云服务运维以及业务运维。运维服务管理框架包含了IT运维服务全生命周期管理方法、管理标准和规范、管理模式、管理支撑工具、管理对象以及基于流程的管理方法。

指标项	具体要求
产品运维管理	支持第三方ISV的接入配置更改、增加、删除。
	支持通过跳转的方式便捷地访问第三方ISV界面。
产品资源管理	支持展示云平台部署产品概览，包括部署云产品总数，集群总数。图形化展示产品软件部署状态。
	支持看出每个集群的详细信息，包括集群名称，所属产品，集群状态，机器数量，告警数量。支持按产品名称、集群名称，集群状态查询集群。
任务管理	支持任务管理，支持展示系统中任务的整体运行情况。
	在运行面板区域，查看当前系统中等待介入、运行中、失败和已完成任务数量的统计信息，单击各统计数值，会跳转到对应的任务页面。
	在运行中的任务区域，查看最近24小时内正在运行中的任务。
	在脚本创建区域，支持可以通过单击或拖拽方式快速创建脚本，支持上传shell以及python脚本。
	在最近7天运行情况区域，查看最近7天任务的运行趋势。
	支持修改任务的灰度策略即调整机器的执行批次。
	支持删除不再使用的任务。
	支持手动执行方式，在任务创建成功后，按照手动启动该任务。
	支持当任务中存在断点并运行到断点时，任务将暂停等待人工确认，只有人工确认后任务才能继续执行。
	支持查看任务的执行情况。
分布式存储运维	分布式存储总览:支持显示存储集群服务器数量、总容量、使用空间百分比、文件数量以及异常服务器/异常磁盘数量。
	分布式存储集群管理:显示存储集群服务器节点详细信息，应包括服务器状态、磁盘数量、坏盘数量、总容量、已使用量。
	数据重分布:在存储集群扩容、缩容、服务器故障等场景下，支持系统自动

	进行数据在服务器间的平均分布，支持手动进行数据重新分布。
对象存储运维	可以统计对象存储Bucket数量，Object数量，可以查看最新数量和按时间段显示增长趋势。
库存管理	支持云主机、存储资源等云产品的库存情况查看，云产品库存详情中主要提供按区域、实例类型和日期分页查询某类实例在某个日期的库存情况。
服务器资源管理	支持以IDC机房、机柜维度查看服务器列表和详细信息，展示每个机柜内服务器数量和服务器告警状态，可查看每台服务器的状态、详细信息、报警信息和监控信息，监控信息包括CPU使用率、磁盘使用率、内存使用率、主机流量、磁盘IO等。
	支持以软件部署角度查看各个产品所在的物理服务器进行监控查看，可以按地域、产品、集群查看服务器列表和服务器详细信息。
	支持服务器信息导出。
服务器运维	支持对服务器进行操作系统层面诊断，包括内存使用率、时间同步、kernel故障、磁盘IO负载、删除文件异常、异常网络数据包、TCP链接状态异常、网卡异常、网络丢包等常见异常。
物理平台管理	支持按照区域、产品、集群等逐层展开左侧的导航树，查看某个产品某个服务所在的机器列表。
	支持按照主机名、IP地址、设备功能角色或SN号搜索并查看某个物理机。
	支持按产品维度查看该物理机的基本信息及监控与报警情况。不同等级告警应采用不同颜色标识。
	支持新增物理机并显示在机柜图中。
	支持将所有物理机相关的信息导出至本地，用于线下查看。 支持导出所选结构树中的服务器信息
网络资源管理	支持显示云平台物理网络拓扑，支持显示网络设备网元和互联链路，网络设备和互联链路应支持按颜色区分链路状态。

	点击网元和互联链路可以查看详细信息。
	可以动态拓扑和基准拓扑，动态拓扑可以动态刷新拓扑状态，基准拓扑表示网络的目标状态，不进行动态刷新。 支持显示展示网络状态与基准拓扑的拓扑偏移量，帮助运维人员快速进行网络状态的调整。 支持把拓扑更新到基准拓扑。
自动化运维	支持云平台运维工作自动化，可向批量资源完成运维操作，提供基础设施，云环境，操作系统，应用层的自动化运维能力。 (1)脚本管理，提供脚本库存放运维脚本，支持系统内置脚本，并支持运维人员自定义和导入脚本。 (2)软件包管理:提供软件仓库能力，可以上传和下载软件包，支持压缩包，JAR包等格式。 (3)运维作业:支持运维作业定义，运维作业可以手动触发和定时触发。支持在作业中中定义执行的脚本或软件包，以及执行主机列表，任务支持灰度设置。 (4)运维流程编排:支持图形化方式编排运维流程，可以运维人员把一系列运维操作定义为“流程”，流程中可以定义触发方式，包括手动触发和定时触发，支持在流程中添加操作任务节点，节点可以包括执行任务节点，可以执行脚本或软件包，可以设置执行任务的节点资源，包括服务器主机或容器资源，任务支持灰度设置。
运维大盘	支持统计每个Region的告警汇总，按严重等级展示。
	支持显示多Region的相关告警、库存和资源信息支持图形化展示云主机服务、对象存储服务等产品的库存百分比。
	支持统计每个Region的物理资源。
告警管理	支持根据监控项类型、产品、服务、等级、状态、开始日期、结束日期及过滤

	内容来进行过滤查询。
	支持查看告警源详情，如告警说明、参考信息、影响范围及处理步骤等。
	支持告警处理(如处理、处理完成、事件跟踪、上报ITIL等)导出告警列表里的告警信息支持告警屏蔽，在告警屏蔽的添加页面，配置需要屏蔽的告警筛选项，支持为已屏蔽的告警解除屏蔽。
	支持搜索关键字查询，如集群、产品、服务、等级、状态、监控项名称等，单击查询，可查询到相应的告警事件。
	单击各色块可跳转至对应的告警事件页面可以根据业务需要，查询、添加、修改以及删除告警联系人和联系人组。
	支持导出历史告警列表。
运维安全	支持运维角色管理，可以按产品进行角色授权支持设置运维IP白名单配置。
	支持Linux命令拦截规则，可以设置拦截命令，拦截风险提示，拦截规则，拦截规则可以为通过，禁止，二次确认，校验码校验等。
	支持运维命令审计，审计应包括登录，登出，执行命令等。记录操作人，操作时间，操作机器，执行结果信息。
	支持对操作视频回放。
系统管理	支持用户管理、用户组管理、双因素认证、角色管理、部门管理、菜单管理、Region授权管理、云操作系统日志、操作日志、授权信息。统一账号管理&角色权限管理，只需要登录到云平台运维系统中，就能实现对云平台所有的组件进行运维或者免登录跳转运维。

（3）云统一运营平台

云统一运营平台提供期货行业云面向租户用户运营云产品和云服务所需的功能，包括运营云门户、统一资源管理、统一运营管理，包括资源管理、配额管理、订单管理、审批管理、计量计费、资源分析、资源总览等功能要求，以支撑期货行业云运营体系建设。

指标项	
主要功能	★运营平台包括运营云门户、统一资源管理、统一运营管理，包括资源管理、配额管理
首页	展示云管业务整体介绍信息，包含：云产品展示云产品目录，产品文档及服务支持入口
服务介绍	展示已发布的云产品服务介绍信息，包含名称、概要介绍、详细功能介绍、产品文档，
登录注册	支持自行注册租户账号，注册后可以自主进行登录。
用户管理	支持按部门创建用户。
	新建用户时，支持随机生成强密码。
	支持用户首次登陆时强制修改密码。
	支持通过用户密码策略来限制用户密码长度、密码强度。
	管理员可重置其他用户密码。
组织管理	支持以树形结构展示部门列表及部门中的用户成员。
	支持无限级添加下级部门。
	支持按部门筛选用户。
权限管理	支持灵活的功能权限组装成角色。
	支持按角色纬度的人员权限分配。
	支持按部门、项目限定管理权限范围。
租户管理	支持租户多租户的定义。
	支持租户级别的数据隔离，包括：租户内部资源监控、资源申请、资源操作。
概览	支持展示当前当前用户信息、待办信息、常用导航设置、资源概览、信控实例情况概览
资源申请管理	支持资源开通申请创建，填写资源开通配置信息提交资源开通申请。
	支持申请单查看，根据权限展示全部、租户的申请单，展示申请单详细信息、当前状态
	支持用户待办，处理待用户处理的申请单明细，用户可以进行审核、结单操作。
	支持根据时间周期统计资源申请单汇总数据，展示对应周期的申请单明细
	提供云产品服务费用的价格计算器，通过价格计算器能够测算出来具体需要的费用
工单管理	支持提交工单，对待处理的工单进行处理，查看全部工单详情信息。

	支持根据多维度的查询条件查询工单，展示全部工单。
	支持创建技能组，编辑技能组基础信息，支持添加、删除技能组的人员。
	支持定义工单类型，编辑工单的字段信息，设置工单的任务，配置工单流转规则。
消息通知	支持设定发布通知公告信息，可设定通知时间，支持编辑和删除。
	支持查看通知内容，展示全部通知信息。
	支持查看全部系统消息，标记系统消息的阅读状态。
资源水位大盘	支持展示云产品的关键核心项的已使用量和剩余量级，剩余百分比
服务管理	支持服务目录创建，各个云服务可将对应的服务注册到服务目录中，可自定义项目包
	支持服务目录编辑，可以修改服务目录的名称、描述和图标，支持对目录启用、停用操
	支持服务目录删除，可以删除空的服务目录，有服务的服务目录不可删除。
	支持创建服务，配置服务信息关联云产品、计费策略、审批流程。
	支持服务编辑、启用/停用控制，启用的服务禁止编辑。
	支持自定义配置表单信息，表单可关联外部数据。
	支持编辑和删除表单，已关联服务的表单不能删除。
	支持审批流程定义，节点可按照部门、用户设定指定人员。
	支持审批流程编辑和删除，可编辑流程基础信息、流程链路和审批节点，启用和关联
资源管理	支持查看已开通的云产品信息，有实例的产品的实例明细，可对对应实例进行基础的
	支持计算、存储、数据库、网络、中间件、大数据、安全等产品的查看及管理入口展示
项目管理	支持创建项目，项目归属于对应的部门，可查看项目关联资源信息。
产品管理	支持自动同步已接入云环境的产品信息，包含产品基础信息及组件属性。
	支持产品编辑，可以修改产品名称、图标及描述，配置产品组件属性及关系。
	支持控制产品的启用和停用。
账户管理	支持调整账户的额度，划分设定信用额度，控制账户的启停状态，展示账户的操作日
	支持查询账户明细，展示账户资金的变动明细记录。
	支持对账户进行充值，包含线下汇款和线上支付充值方式进行充值。

订单管理	支持生成服务订购的订单信息，订单记录服务信息、支付信息、服务开通状态。
	支持取消订单，未支付的订单可以进行取消。
	支持对订单进行支付，通过收银台对订单进行付款。
支付管理	支持支付管理，支持根据订单金额创建支付单，信用卡支付。支持配置管理支付渠道
账单管理	支持月度账单的统计展示，包含消费汇总金额信息和云产品汇总金额信息。
	支持日/月账单，包括:产品、单价、优惠金额、结算、用量。
发票申请管理	支持发票基础信息及收票地址的编辑维护，可自主维护开票信息。
	支持提交发票申请，计算可开票费用，发票开票和退票审核，线下邮寄信息维护。
计费策略	支持新建计费策略，包含关联的云产品、折扣、付费类型、对应计费项请假模块的详
	支持计费策略的编辑和修改，控制计费策略的启用和停用，启用状态的计费策略不可
资源分析	支持按全部和项目展示资源分析数据，包括:实例总数、资源剩余量、产品运行效率、
	支持资源实例的详细分析，包括:实例的基础配置信息规格、部门、项目，实例具体运
多云管理	支持多云管理;支持添加/修改/删除同构云地址和账号;提供仪表盘展示多个专有云

***（三）兼容性要求**

此要求为必须完全响应，否则视为无效投标。具体要求如下：

1.服务器兼容性

要求云平台可兼容主流服务器厂商（比如：浪潮、新华三、超聚变、中科可控等）的服务器，需提供云平台厂商官网发布的服务器兼容证明（不少于3家）。

芯片要求兼容Intel、飞腾、鲲鹏、海光等主流CPU芯片，需提供不少于3个的兼容证明。

2.网络设备兼容性

要求兼容主流网络设备厂商（比如：新华三、华为、紫光恒越等）的网络设备，需提供云平台厂商官网发布的网络设备兼容证明（不少于3家）。

（四）服务要求

应提供给招标人包括但不仅限于下表中所需的服务内容：

序号	服务类别	服务名称	描述
1	建设实施服务	期货行业云建设规划服务	要求云平台原厂商根据期货行业云建设的场景化需求，进行建设方案设计与交付，包括:需求分析、方案规划、方案实施、试运行保障方案等内容。
2		期货行业云部署服务	要求云平台原厂商提供期货行业云建设的项目管理及实施、测试、并网等工作内容，包括:IDC工勘、硬件设备上架方案规划、综合布线规划设计、云平台部署、云平台测试等内容，并负责配合招标人组织相关的第三方厂商完成云平台建设的整体集成工作。
3		期货行业云测试服务	要求云平台原厂商提供期货行业云正式投产前对云平台的高可用测试、性能测试以及安全测试，包括:测试方案规划、现场测试、安全加固等内容。
4		期货行业云培训服务	要求云平台原厂商提供不少于6次(每次不少于0.5天)云平台产品使用及运维技能相关的原厂培训服务。培训的形式包括现场培训、线上培训等。
5		试运行运维支持服务	要求云平台原厂商在本项目在试运行期间(3个月)提供不少于1人的现场运维支持服务，用于期货行业云在正式投产前的平台使用及业务支持。
6	运营支持服务	期货行业云运营支持服务	要求云平台原厂商结合期货行业云实际建设情况，依托期货行业云统一运营平台，协助招标人建立行业云对外运营能力。
7	等保咨询服务	期货行业云等保咨询服务	要求云平台原厂商根据国家及行业的等级保护相关政策和标准要求，结合期货行业云平台实际，为招标人提供等级保护合规咨询服务。

8	软件维保服务	软件许可更新与技术支持	要求投标人自期货行业云平台通过终验之日起，提供所有软件产品原厂商1年技术支持和售后服务。在上述质量保证期内，提供7×24小时的原厂服务响应，应按需提供软件升级原厂商现场支持服务。
9		技术支持服务	要求投标人提供原厂技术支持服务，包括故障应急、风险推送、变更支持、疑难问题支持、现场运维团队管理等，及每个季度提供1次的现场技术交流及巡检。本服务除故障应急提供7×24小时响应，其他服务以5×8工作日为主。
10	运维服务	驻场服务	要求云平台原厂商提供满足招标人要求的不少于1年、不少于3人(5×8，至少1名专职安全运维人员)驻场工程师，参与期货行业云的日常值班、巡检、应急等日常运维工作。
11		专家服务	要求提供云平台原厂商不少于30人天的运维专家支持服务和不少于30人天的安全专家支持服务。

注：投标人在应答上述采购需求时，在报价明细中需明确各服务项目的报价单位、报价数量等信息，涉及人力投入的，需列明拟投入人员数量清单、工时及单价。

*（五）其他要求

1. 交货日期要求：合同签订之日起10个工作日内完成安装介质及授权文件的交付；在甲方部署环境就绪后的30个日历日内，完成系统的集成部署。

2.为确保期货行业云建设和运营的可持续性，投标人应合理报价，在报价明细清单中，服务费应和软件授权费分开报价。并须提供以下承诺(若投标人不是云平台原厂商，则须同时提供云平台原厂商的承诺文件)：一是五年内项目扩容(包括另外新建)本次采购清单内的功能时，承诺所需的费用单价不高于此次投标报价，且无额外费用；二是软件维保服务价格不超过总体投标报价(不含运维服务、软件维保费用)的20%；三是服务期满后，承诺五年内每年续签服务所需费用单价不高于此次投标报价。此要求为必须完全响应，否则因报价不完整导致无效投标。

评审因素

(一)商务部分

1.案例情况

2020年1月1日以来(以合同签订时间为准),投标人的项目业绩案例。

证券期货交易所及其下属技术公司案例,每1个案例得　　分;其他案例每个得分。

注:①案例合同中云平台软件授权与服务部分的总金额不小于人民币1000万元,否则该案例无效;②同一采购单位案例金额可累加至不少于1000万元计算得分,但同一采购单位合格案例只能按照1个有效业绩计算得分;③案例中云厂商及其云产品应与本次所投产品一致,方为有效案例。

说明:投标文件中须提供案例证明材料:①提供的合同复印件应能清晰展示云产品名称、规格等;②同时附验收或其它可说明项目正常运行的证明材料。

2.资质证书

序号	证明材料
1	具备CMMI5资质认证
2	具备CSASTAR(云安全管理体系)认证
3	具备ISO27017(云服务信息安全管理体系)认证
4	在公有云领域具备公安机关颁发的金融云信息系统公安全等级保护备案证明(四级及以上)

根据投标人以上资质证书获得情况,进行评价:

具备3-4个,得　分;

具备1-2个，得　分；

具备0个，得 分。

(二)技术部分(　分)

1.方案讲解(　分)

投标人基于对项目需求的理解，对项目方案进行现场讲解。对方案讲解情况进行评议:一档得　分，二档得　分，三档得　分。未讲标或讲解人员不符合要求的，不得分。

讲述要求:

- 讲述时长:不得超过 10分钟;
- 讲述形式: PPT形式;
- 讲述次序: 现场抽签;
- 讲解人员要求:为拟派驻本项目的项目经理。

2.技术参数(　分)

根据投标文件中提供的技术偏离表评分:完全满足招标文件要求的，得　分;每项核心技术要求(标注"*"指标)负偏离视为无效投标，每项重要技术指标(标注"★"指标)负偏离扣　分，每项一般技术指标负偏离扣　分，扣完为止。参见"软件要求"的偏离情况进行打分。

3.实施方案(　分)

在充分理解期货行业云建设的项目背景需求的前提下，参考云计算业界先进、主流实践，形成技术先进、安全合规的技术方案。

(1)云平台建设实施方案（ 分）

技术方案中应涵盖软硬件系统部署集成以及运营、运维体系与流程建设相关内容，包含但不限于服务器、网络设备、IaaS、PaaS等云平台所有相关软硬件的部署集成，以及期货云运营体系流程建设、运维体系流程建设、应急处置流程建设等方面；评标委员会根据相关内容的完整性、专业性、可操作性、针对性等进行综合评价。

方案完整、专业性强、可操作性强，得 分；

方案较完整、专业性较强、可操作性较好，得 分；

方案待完善、专业性待提高、操作性一般，得 分；

无此内容不得分。

(2)服务方案（ 分）

技术方案应包括专业服务(包括但不限于“服务要求”章节中“建设实施服务”、“运营支持服务”和“等保咨询服务”的要求)，保障云平台的顺利实施、安全运行和优质对外服务的相关内容;评标委员会根据相关内容的完整性、专业性、可操作性、针对性等进行综合评价。

方案完整、专业性强、可操作性强，得 分；

方案较完整、专业性较强、可操作性较好，得 分；

方案待完善、专业性待提高、操作性一般，得 分；

无此内容不得分。

(3)项目管理方案（ 分）

技术方案中应包含项目组织结构、人员、项目计划及项目管理相关内容。评标委员会根据相关内容的完整性、专业性、可操作性、针对性等进行综合评价。

方案完整、专业性强、可操作性强，得 分

方案较完整、专业性较强、可操作性较好，得 分；

方案待完善、专业性待提高、操作性一般，得 分；

无此内容不得分。

4.服务方案及质量保障措施（ 分）

在满足招标人的服务要求及标准的前提下，对云平台原厂商服务能力并结合投标人对服务要求（参见“服务要求”章节）的响应情况进行评议。

（1）服务团队（ 分）

投标人须针对本项目成立服务团队、指定项目经理，项目开展过程中需更换项目成员的，须经招标人同意。投标人提供的项目服务团队需满足以下条件，如有一条不满足，本项不得分。

1）如投标人非云平台原厂商，则服务团队须包括原厂商人员；

2）项目团队至少应包括以下关键人员：云计算工程师、系统架构师、系统工程师、网络工程师、CISP认证人员等；

3）拟派驻项目经理须为云平台原厂商人员，需要具备信息系统项目管理师（高级）证书以及云计算相关证书，至少具有5年从业经历，担任过云平台（不少于150节点或项目金额不少于1500万元）项目经理职位；投标文件中须提供项目经理服务过的类似项目合同案例或项目验收等证明文件（需显示项目经理姓名，非合同案例的证明文件还

需显示建设方印章，否则案例无效）、资质证书复印件等资质、能力证明材料，并提供原厂商为其缴纳社保的证明材料。

4）除项目经理外，其他关键岗位人员须为云平台原厂商人员或原厂商认证的人员，且至少具备3年相关行业从业经历。投标文件中须附资质、能力证明材料。非原厂商人员的，项目团队人员明细须加盖原厂商印章，并同时提供原厂商认证证明文件。

投标文件中须列明项目团队人员明细、职责分工，并提供人员简历、工作经历、资质证书等证明材料，在满足采购人对服务团队要求的前提下，对投标人的服务团队的服务能力包括团队人员构成、项目关键岗位人员履历、从业经历、资质水平等情况，并结合投标人对服务团队要求的响应情况进行综合评议。

拟派驻本项目服务团队整体服务能力强，人员结构组成合理，关键岗位人员专业资质和实践经验优，得 分

拟派驻本项目服务团队整体服务能力较强，人员结构组成较合理，关键岗位人员专业资质和实践经验良，得 分

拟派驻本项目服务团队整体服务能力较弱，人员结构组成不够合理，关键岗位人员履历一般，得 分

无此内容不得分。

（2）售后服务（含免费维保期内服务）（ 分）

在满足采购人服务要求及标准的前提下，对售后服务方案，内容包括：技术支持力量、保修期内服务承诺、知识转移方案、培训方案、培训课程等，并结合投标人对服务要求（参见“服务要求”章节）的响应情况进行评议。

售后服务方案全面科学、实施性强，得 分；

售后服务方案较全面科学、实施性较强，得 分；

售后服务方案整体较弱，得 分；

无此内容不得分。

(3)其他服务承诺(分)

投标文件中，投标人基于对本项目的理解程度，并结合本项目实际，在招标文件要求的基础上提供增值服务书面承诺，**若投标人不是云平台原厂商，则须同时提供云平台原厂商的承诺文件，否则相关承诺按无效处理(不得分)。**

1)投标人承诺免费为招标人提供期货行业云市场推广服务(如:客户引流、产品推介等)，评标委员会根据服务方案的业务价值、可行性、针对性以及与本项目的契合度进行综合评价；

服务方案可操作性强，业务价值优，得 分；

服务方案可操作性较好，业务价值良，得 分

服务方案可操作性一般，业务价值一般，得 分

无此内容或承诺无效不得分。

2)投标人承诺，若招标人云平台对本次采购内容扩容(包括新建)建设时，投标人可针对软件、实施等服务给予进一步的采购价格优惠，并注明优惠力度及措施;针对服务方案的可操作性和业务价值等进行评议。

优惠方案可操作性强，业务价值优，得 分；

优惠方案可操作性较好，业务价值良，得 分

优惠方案可操作性一般，业务价值一般，得 分

无此内容或承诺无效不得分。

3)针对投标文件中维保期满后与软件维保服务(参见“服务要求”章节中“软件维保服务”)的价格承诺进行评价，以服务采购时的软件合同清单为准。

承诺维保期满后，软件维保服务价格不超过总体合同费用(不含运维服务、软件维保费用)的10%(含)，得 分；

承诺维保期满后，软件维保服务价格占比总体合同费用(不含运维服务、软件维保费用)的10%(不含)-12%(含)，得 分

承诺维保期满后，软件维保服务价格占比总体合同费用(不含运维服务、软件维保费用)的12%(不含)-15%(含)，得 分

承诺维保期满后，软件维保服务价格超过总体合同费用(不含运维服务、软件维保费用)的15%，得 分。

4)投标人基于对本项目的理解程度，并结合本项目实际承诺提供其他有价值免费业务承诺。评标委员会根据相关承诺的业务价值、可操作性进行评价，承诺可操作性强、业务价值优的，得 分。

无此内容或承诺无效，或被评标委员会判定承诺操作性不强、不具针对性、业务价值低，不得分。

5.成本合理性评价(分)

(1)本期成本合理性评价(分)

投标人根据本项目要求及格式提供本项目采购产品及服务详细报价清单，评标委员会根据清单填写情况及相关产品价格的合理性进行综合评价。

采购清单详细、规范，建设成本合理，得 分；

采购清单较为详细、规范，建设成本较为合理，得 分；

采购清单基本符合要求，建设成本基本合理，得 分；

(2)云平台后期拓展及其成本合理性评价（ 分）

投标人根据对本项目的理解，制定本项目未来功能拓展方案，规划远期功能拓展方向，提出功能需求拓展(至少应包括PaaS、SaaS功能)、安全加固等方面的建议;提供达到规划方案所需的功能采购清单，清单内容应包括主要功能名称、功能(规格)描述、计价单位、采购单价、优惠折扣等，并承诺招标人的采购优惠价格不高于清单价格，若投标人不是云平台原厂商，则须同时提供云平台原厂商的承诺文件。评标委员会根据规划方案的可行性、功能采购清单的丰富性、建设成本等情况进行综合评议。

规划方案方案可操作性强，功能采购清单丰富，建设成本合理，得 分

规划方案方案可操作性较强，功能采购清单较为丰富，建设成本较为合理，得 分

规划方案方案可操作性低，功能采购清单简略，建设成本基本合理，得 分

无此内容不得分。

(三)报价部分（ 分）

评分基准值:当有效投标报价大于5家时,去掉一个最高报价与一个最低报价后,评标基准值等于剩余有效报价的算术平均值;当有效投标报价小于等于5家时,评标基准值等于所有有效投标报价的算术平均值。

价格分计算:

(1)投标人投标报价等于评标基准值的,得 分;

(2)投标人投标报价低于评标基准值 %以内的,每低1%,在 分的基础上加 分比例进行加分,满分 分;

(3)投标人投标报价低于评标基准值超过 %的,每低1%,在 分的基础上扣 分比例进行扣分,扣完为止;

(4)投标人投标报价高于评标基准值的,每高1%,在 分的基础上扣 分比例进行扣分,扣完为止;

(5)投标价格与评标基准价偏差率不足1%时,按比例计算,分值计算最终保留两位小数(第3位四舍五入)。