



农信银资金清算中心农信云长沙区 建设项目

公开招标文件

项目编号: RH-WTGK2023004

中国人民银行集中采购中心

2023 年 11 月

第一章

投标邀请

投标邀请

中国人民银行集中采购中心现采取公开招标的方式，就“农信银资金清算中心农信云长沙区建设项目”（项目编号：RH-WTGK2023004）邀请合格投标人进行密封投标。

本项目为非政府采购项目，遵照执行《国有金融企业集中采购管理暂行规定》（财金〔2018〕9号），参照《政府采购法》、《政府采购法实施条例》及政府采购领域相关程序及政策。

一、 招标标的

★采购清单

详细清单

本项目的整体方案由投标人提供，整体的软件及硬件由投标人进行集成适配，因此下表硬件各类目数目及配置为投标时需达到的**最低量**（不含测试、开发环境许可），具体以投标人的方案为准。

序号	类别	名称	基本要求	数量	备注
1.	网络设备	核心交换机	单台设备实配 100G 线速端口 ≥ 72 ，单块板卡 100G 接口数量 ≥ 36 ，100G 端口可以自适应成 40GE，模块满配，包含与接口数量相等 100G MPO 接口光模块，即光模块满配。	2 台	
2.		接入交换机-100G 接入	交换容量 $\geq 6.4\text{Tbps}$ ，包转发率 $\geq 2000\text{Mpps}$ ， ≥ 32 个 100 GE QSFP28 端口，模块满配	0	云网关服务器接入使用，如不使用投标人可采用本表所列其他品类交换机实现云网关接入。
3.		接入交换机-25G 接入	交换容量 $\geq 4.8\text{Tbps}$ ，包转发率 $\geq 2000\text{Mpps}$ ， ≥ 6 个 40 QSFP+/100 QSFP28 端口，模块满配， ≥ 48 个 10GE SFP+ / 25GE SFP28 端口，模块满配。	12 台	仅用于计算节点接入，其他节点接入交换机数量需投标人另行配置。

4.	接入交换机-10G接入	交换容量 $\geq 4.8\text{Tbps}$ ，包转发流 $\geq 2000\text{Mpps}$ ，配置万兆以太网 SFP+端口 ≥ 48 ，模块满配 配置 100G QSFP28/40G QSFP 端口 ≥ 6 ，模块满配	6 台	仅用于计算节点接入，其他节点接入交换机数量需投标人另行配置。
5.	接入交换机-1G接入	交换容量 $\geq 570\text{Gbps}$ ，包转发率 $\geq 140\text{Mpps}$ ， ≥ 48 个 10/100/1000Base-T 端口，模块满配， ≥ 4 个 10GE SFP+ 端口，模块满配	6 台	仅用于计算节点、网络管理接入，其他节点接入交换机数量需投标人另行配置。
6.	边界路由器	支持多核 CPU，实配控制引擎 ≥ 2 ， ≥ 16 个 10GE SFP+ 端口，LC 接口单模模块满配 ，需分布在不同板卡。	0	局域网边界使用，根据投标人方案自行确定是否需要使用。
7.	硬件防火墙	独立硬件设备，而非通过添加功能模块实现。 吞吐量 $\geq 40\text{Gbps}$ 最大并发连接数 ≥ 1200 万； 每秒新建连接数 ≥ 30 万； ≥ 8 个 10 SFP+ 端口，模块满配； (以上配置的端口均为实际可用数量，要求全部同时支持，不得存在复用端口)	4 台	边界防御， 局域网边界 2 台， 互联网接入边界 2 台
8.	云内防火墙	软硬件方案皆可； 吞吐量 $\geq 80\text{Gbps}$ 最大并发连接数 ≥ 2500 万； 每秒新建连接数 ≥ 60 万； $\geq$ 具备硬件防火墙同等功能和性能要求	1 套	云内防火墙 1 套， 根据云内 VPC 划分安全隔离要求，每个 VPC 边界使用独立防火墙防护，可采用硬件或软件防火墙实现

9.	硬件负载均衡	独立硬件设备,而非通过添加功能模块实现,具备服务器、链路、全局负载均衡功能,无需添加额外许可。 吞吐量$\geq 40\text{Gbps}$ 4 层并发$\geq 16\text{M}$ 4 层每秒新建$\geq 500\text{K}$ 7 层每秒新建$\geq 600\text{K}$ 设备同时支持服务器负载均衡、链路负载均衡、全局负载均衡,无需额外许可费用 每秒新建连接数: TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 $\geq 12000\text{TPS}$。 TLS_RSA_WITH_AES256_GCM_SHA384 $\geq 12000\text{TPS}$。 ECC-SM2-SM4-SM3 $\geq 8000\text{TPS}$; ECDHE-SM2-SM4-SM3 $\geq 8000\text{TPS}$; 吞吐量: TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 $\geq 5.6\text{Gbps}$。 TLS_RSA_WITH_AES256_GCM_SHA384 $\geq 5.6\text{Gbps}$。 SSL 最大并发连接数≥ 600000。 支持 SSL 加密,通过将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器。 支持商密 SSL 算法的单向和双向认证,至少包含以下算法:国密: SM2、SM3、SM4 算法,商密: RSA、SHA、ECDSA、ECDHE、SHA256、SHA384 算法。 "支持以下算法: TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384; TLS_RSA_WITH_AES256_GCM_SHA384; TLS_ECC_SM4_SM3。" 支持多级 CA 证书链 "支持各类标准证书的申请和导入,类型包含: RSA: 1024-bit, 2048-bit, 4096-bit; ECDSA: 256-bit、384-bit; SM2: 256-bit。" 支持 SSL 卸载,将 SSL/TLS 协议流量解密为明文后再传输至服务器,以减轻服务器性能压力。 支持 SSL 加密,通过将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器。 实配支持基于自定义策略的 DNS 解析 DNS 每秒查询能力: $\geq 1500\text{Kqps}$ 具备国家密码管理局商用密码检测中心颁布的《商用密码产品认证证书》,满足 GM/T 0028 要求。	8 台	局域网边界 2 台,互联网接入区链路负载 2 台。局域网国密 SSL 卸载 2 台,互联网国密 SSL 卸载 2 台。
----	--------	--	-----	---

10.		云内负载均衡	软硬件方案皆可； 吞吐量 $\geq 80\text{Gbps}$ ，四层新建连接数四层新建能力 ≥ 50 万 CPS；七层新建能力 ≥ 60 万 RPS。 支持同一套负载均衡集群提供内网和外网两种负载均衡创建模式，支持轮训（RR），加权轮询（WRR）、源 IP 一致性哈希，最小连接数。	1 套	云内负载均衡 1 套，为云内提供负载均衡能力。根据云内 VPC 使用边界使用独立负载均衡，可采用软件或硬件方式实现。
11.		网络入侵防护	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧入侵防护。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件
12.		Web 应用防火墙	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧 web 应用安全防护。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件
13.	网络安全设备	网络未知威胁检测	1. 旁路部署，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧未知威胁检测。 3. 软硬件方案皆可，需支持将云内流量（含云边界和云内南北向流量）镜像至硬件平台（例：网络分路器）。	1 套	需实配所需的软硬件
14.		数据加密	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及用户侧数据加密。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件
15.		密钥管理系统	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于密钥管理。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件
16.	计算型服务许可	计算节点许可	1. 运行虚拟化组件，承载虚拟机。需兼容招标人已采购的特定型号的服务器； 2. 每个许可对应 1 台物理服务器，单个许可不限制物理服务器的物理 CPU 和物理核心数量。	100	招标人已经规划详细用途，不得被投标人挪用。若其他采购项依赖该许可，投标人需额外实配。
17.		裸金属许可	1. 将物理服务器作为资源。需兼容招标人已采购的特定型号的服务器； 2. 每个许可对应 1 台物理服务器，单个许可不限制物理服务器的物理 CPU 和物理核心数量。	100	招标人已经规划详细用途，不得被投标人挪用。若其他采购项依赖该许可，投标人需额外实配。

18.	存储资源	云存储	详见 1.4.1.4	-	
19.	服务器	服务器	规格及数量要求见 1.2.2 及 1.4	115 台	
20.	备份对接设备	备份设备	详见 1.4.1.8	1 套	
21.	PaaS 软件	分布式关系型数据库服务	1. 每套实配不少于 3 台物理服务器的许可； 2. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器） 3. 单台物理服务器物理 CPU 个数和核心总数不受许可限制；	6 套	1. 该产品运行的服务器需含在云底座硬件中，提供 18 台服务器，服务器配置同 1.4.1.1.4 数据库服务器规格 A； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
22.	硬件	数据库同步工具	1. 实配不少于 50 条数据库同步链路（链路可重复使用，即源端和目标端可变化）的许可； 2. 或无限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	1 套	1. 该产品运行的服务器需含在云底座硬件中，提供不少于 3 台服务器，服务器配置同 1.4.1.1.4 数据库服务器规格 A； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）

23.	容器服务	1. 实配不少于 10 台物理服务器的许可； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）； 4. 单个 Node 节点的 CPU 个数和 CPU 核心总数不受许可限制；	1 套	1. 该产品管理端（基于 kubernetes 的 Master 端）、应用仓库、镜像仓库模块运行的服务器需含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）； 2. 运行 pod 的物理服务器不含在云底座硬件中，硬件不做报价，规格同 1.4.1.1.5 利旧服务器规格
24.	分布式缓存服务	1. 每套实配不小于 3 台物理服务器的许可； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	2 套	1. 该产品运行的服务器需含在云底座硬件中，提供 6 台服务器，服务器配置同 1.4.1.1.4 数据库服务器规格 A； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
25.	DevOps 服务	1. 实配不少于 200 个可重复使用的用户（通过用户是否激活 DevOps 服务许可的授权实现重复使用）许可，或实配不少于 500 个不可重复使用的用户许可，且支持 100 个用户同时在线，同时不限限制流水线数量； 2. 或不限限制用户许可和流水线数量的产品	1 套	该产品运行的服务器不含在云底座硬件中，硬件不做报价

26.		微服务应用平台	1. 实配不少于 300 个微服务处理节点的许可； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	1 套	1. 该产品用于运行应用系统（处理节点）的物理服务器不含在云底座硬件中，硬件不做报价，规格同 1.4.1.1.5 利旧服务器规格； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
27.		API 网关	1. 实配 3 个集群的许可，每个集群需保证高可用，单集群 TPS 不少于 6000； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	1 套	1. 该产品运行的服务器需含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
28.	云管软硬件	运维平台	含云管平台、监控平台。	1 套	含软硬件
29.		其他组件	云底座及其他组件	1 套	含软硬件
30.	技术支持与服务	技术支持与服务	3 年高级云技术支持服务，包括故障修复、预防性维护、应急保障、版本升级、性能调优、巡检、应用上云改造支持等服务。6 人年现场技术支持服务、培训服务等。	3 年	部分硬件服务年限另有要求

31.	云建设集成实施服务	线缆敷设	本项目实施所需的线缆、标签等辅材及综合布线服务。	1次	完成基本要求所列工作。
-----	-----------	------	--------------------------	----	-------------

核心产品：29. 其他组件（云底座及其他组件）

根据《中华人民共和国政府采购法》和财政部《政府采购进口产品管理办法》的有关规定，本次招标**不接受**进口产品投标。

本次招标 标的预算	项目总预算：¥51,530,000.00 本项目最高限价： <u>5153万元</u>
--------------	--

二、 招标文件发放

发放时间	2023年11月3日至2023年11月10日每天（节假日除外）
线上报名 领取	供应商前往 https://jzcg.pbc.gov.cn/ 注册并登录，在线报名并免费下载领取招标文件。 若有技术问题，咨询 010-66195993。

三、 招标公告期限

招标公告 期限	2023年11月3日至2023年11月10日（不少于5(含)个工作日）。
------------	--------------------------------------

四、 澄清截止期限及要求

澄清截止 期限	2023年11月21日16:00前
澄清文件 递交方式	由参加报名的供应商持法人代表授权书，递交纸质澄清材料并加盖单位公章。
递交地点	北京市西城区金融街国际企业大厦B座5层中国人民银行集中采购中心

五、 投标截止时间及方式

投标截止 时间	2023年11月27日14:00（北京时间）
投标文件 递交方式	投标文件应于投标截止时间前递交至开标地点，逾期送达或不符合规定的投标文件恕不接受

六、 开标时间、地点

开标时间	2023年11月27日14:00（北京时间）
开标地点	北京市西城区金融大街33号通泰大厦C座911室
	根据通泰大厦物业要求，访客进入通泰大厦需要办理人脸识别信息录入，供应商有关人员应当提前预留合理时间

七、 投标人资格要求

(一) 投标人资格条件

投标人为云平台代理商的, 还需提供云平台原厂商资格条件相关材料。

序号	分类	资格条件
1	投标人	在中华人民共和国境内依法登记的法人或其他组织, 合法运作并独立于招标人和招标代理机构, 需提供有效的营业执照复印件, 法定代表人身份证明复印件等证明文件, 并加盖公章。
2		单位负责人为同一人或存在控股、管理关系的不同单位, 不得参加同一标段/标包投标或未划分标段/标包的同一招标项目投标。需提供加盖公章的承诺函原件(格式自拟)。
3		投标人应经营状况良好, 符合《中华人民共和国政府采购法》第二十二条的规定, 且必须为未被列入信用中国网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道信用记录失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人, 否则其投标将被拒绝。 投标人必须在投标文件中提供下述资格证明文件, 否则按无效投标处理: 1、法人或者其他组织的营业执照等证明文件, 自然人的身份证明; 2、财务状况报告, 依法缴纳税收和社会保障资金的相关材料;(供应商应提供书面承诺) 3、具备履行合同所必需的设备和专业技术能力的证明材料;(供应商应提供书面承诺) 4、参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明;(供应商应提供书面承诺) 5、具备法律、行政法规规定的其他条件的证明材料。(以上均为《中华人民共和国政府采购法实施条例》第十七条之规定)
4		本项目不接受联合体投标。
5	技术	投标人资质证书要求: 无。
6		产品资质证书要求: 无
7		原厂商说明函或授权函要求: 本项目仅限于云平台原厂商投标或其授权的代理商投标。投标人若为代理商, 须获取云平台原厂商关于参与本项目投标的 授权书 , 同一代理商只能代理一个云平台原厂商的产品 同一品牌云平台厂商参与本项目的投标人(包括原厂商和代理商)数量不得超过两家, 超过两家则该云平台原厂商、原厂商的代理商投标均将被拒绝。
8		投标人须保证, 招标人在其本国使用其提供的货物时, 不存在任何已知的不合法的情形, 也不存在任何已知的与第三方专利权、著作权、商标权或工业设计权相关的任何争议。如果有任何因招标人使用投标人提供的货物而提起的侵权指控, 投标人

序号	分类	资格条件
		须依法承担全部责任,需提供书面承诺并加盖公章(格式自拟)。
9		团队人员要求: 无

(二) 云平台原厂商资格条件

序号	分类	资格条件
1	商务	在中华人民共和国境内依法登记的法人或其他组织,合法运作并独立于招标人和招标代理机构,需提供有效的营业执照复印件,法定代表人身份证明复印件等证明文件,并加盖云平台原厂商公章。
2		单位负责人为同一人或存在控股、管理关系的不同单位,不得参加同一标段/标包投标或未划分标段/标包的同一招标项目投标。需提供加盖公章的承诺函原件(格式自拟)
3		经营状况良好,符合《中华人民共和国政府采购法》第二十二条的规定,且必须为未被列入信用中国网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道信用记录失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人,否则其投标将被拒绝。 投标人必须在投标文件中提供下述资格证明文件,否则按无效投标处理: 1、法人或者其他组织的营业执照等证明文件,自然人的身份证明; 2、财务状况报告,依法缴纳税收和社会保障资金的相关材料;(供应商应提供书面承诺) 3、具备履行合同所必需的设备和专业技术能力的证明材料;(供应商应提供书面承诺) 4、参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明;(供应商应提供书面承诺) 5、具备法律、行政法规规定的其他条件的证明材料。(以上均为《中华人民共和国政府采购法实施条例》第十七条之规定)
4		资质证书要求: 无
5	技术	产品资质证书要求: 无
6		原厂商说明函或授权函要求: 无
7		团队人员要求: 无

八、 投标保证金

本项目不收取投标保证金

九、 分包投标

合同分包 本项目是否接受分包形式履行合同。□是 ■否

十、 CA 办理密钥联系方式:

具体 CA 数字证书及电子签章办理事项,详见集中采购中心互联网交易系统-“系统公告”中《关于供应商办理 CA 数字证书及电子

	签章的通知》，具体详见 https://jzcg.pbc.gov.cn/freecms/site/templet/xtgg/info/2022/36209.html
十一、 采购人及采购代理机构信息	
采购人	采购人：农信银资金清算中心有限责任公司 联系人：吴先生 电 话：010-57969696-4016 地 址：北京市丰台区南四环西路 186 号汉威国际广场二区 4 号楼 邮政编码：100166
采 购 代 理 机构	采购代理机构：中国人民银行集中采购中心； 地 址：北京市西城区金融街 35 号, 国际企业大厦 B 座 5 层 501； 邮政编码：100033； 联系方式： 李先生（文件发放、开标前咨询） 电 话：66195317； 赵女士（开、评标咨询） 电 话：6619 5465；
十二、 投标人参与开标须知	
	1、满足新冠肺炎疫情防控属地管理的相关要求。

第二章

投标人须知（包括前格式）

投标人须知前格式

投标人应按照本表要求制作投标文件。其他未尽要求，详见招标文件相关章节。

序号	内容	要求及说明
1	开标一览表、投标人资格证明文件（根据本招标文件第一章《投标邀请》七 投标人资格要求与投标文件在开标时间前提交。采购机构在开标现场拆封纸质版开标一览表并予唱标。	
2	一份纸质投标文件，电子版一份，具体要求详见采购文件。如果投标文件纸质正本与电子版不一致，以纸质正本为准。因纸质正本与电子版内容不一致而导致的不利后果由投标人承担。	
3	投标人的资格要求	详见招标文件第一章“投标人资格要求”
4	投标文件的投标有效期	不少于开标之日后 90 天。
5	投标文件构成	投标人须完整地按照招标文件提供的格式编制投标文件。投标文件应包括下列格式材料： (1) 开标一览表：见格式 1； (2) 投标书：见格式 2； (3) 法定代表人授权书：见格式 3； (4) 投标分项报价表：见格式 4； (5) 货物说明一览表：见格式 5； (6) 采购需求及技术要求逐项应答表：见格式 6； (7) 商务及合同条款逐项应答表：见格式 7； (8) 项目实施人员情况表：见格式 8； (9) 同类业务案例介绍：见格式 9； (10) 售后服务与质量保证承诺：见格式 10； (11) 投标人资格声明文件：见格式 11； (12) 投标人资质证书及其他资质证明文件：见格式 12； (13) 正版软件声明：格式见附表 13； (14) 采购需求及技术要求中规定应提交的有关技术文件材料：见格式 14； (15) 投标人关于投标文件纸质正本与投标文件电子版两者一致性的承诺书：见格式 15。 (16) 制造商授权书：见格式 16（如评分细则中要求对投标人提供的授权进行打分，则由投标人提供此表）。 (17) 第一章《投标邀请》七 投标人资格要求的有关材料：见格式 17。
6	投标人应提交的技术文件	详见招标文件第五章有关技术要求
7	投标文件可以被拒绝的其他情形	详见招标文件第二章投标人须知
8	是否接受选择性报价	否

9	投标文件的递交	详见招标文件第二章“三、投标文件编制与递交”。
10	投标报价	详见招标文件第二章“投标报价”。
11	交货时间、地点	详见招标文件第五章
12	投标资格审查	■开标结束后, 采购人应当对投标人进行资格审查, 给出审查结论。
13	相同品牌的投标人的认定	13.1 对于单一产品采购项目, 使用综合评分法的采购项目, 提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的, 按一家投标人计算, 评审后得分最高的同品牌投标人获得中标人推荐资格; 评审得分相同的, 由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格, 招标文件未规定的采取随机抽取方式确定, 其他同品牌投标人不作为中标候选人。 13.2 对于非单一产品采购项目, 多家投标人提供的核心产品品牌相同的, 采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品, 并在招标文件中载明。多家投标人提供的核心产品品牌相同的, 按 13.1 有关规定处理。
14	评标方法	■综合评分法
15	评标委员会人数	7 人
16	确认中标方式	■采购人应当自收到评标报告之日起 5 个工作日内, 在评标报告确定的中标候选人名单中按顺序确定中标人。
17	信息公示渠道	■中国政府采购网

投标人须知

一、总则

1、定义

1.1 “投标人”指响应本次招标要求进行投标的投标人。

1.2 “货物”指本招标文件要求投标人应提供的设备、软件、备品配件、工具及有关技术资料 and 材料。

1.3 “服务”指本招标文件要求投标人应承担的安装、调试、售后质量保证及技术支持、人员培训以及其他伴随服务。

2、合格的投标人

2.1 凡在中华人民共和国境内注册，符合本招标文件规定的投标人资格要求，投标人均可响应本次招标。

3、投标费用

投标人应自行承担参加本次投标所涉及的一切费用。

4、投标范围

投标人必须对本次招标标的整体投标。

5、招标文件技术指标的非限制性

本招标文件技术需求部分规定的技术指标仅说明本项目的采购需求，并没有任何限制性。投标人可以选用性能等同的设备或部件进行投标，但必须实质上满足招标文件对技术性能实质性的要求，并应在投标文件中进行相应的说明和论证。

6、招标通知方式

采购代理机构通过“投标人须知前格式”中“信息公示渠道”发布本次招标所涉及的所有公告、通知等。投标人没有接收其他形式的通知，不视为招标人没有履行通知义务。

二、招标文件

7、招标文件构成

7.1 招标文件用以阐明本项目采购货物及服务的内容与技术要求、招标投标程序和采购合同格式、条款等。

招标文件包括以下五章：

第一章 投标邀请

第二章 投标人须知

第三章 合同格式及合同条款

第四章 投标文件格式

第五章 采购需求及技术要求

7.2 投标人应认真阅读招标文件规定的事项、格式和技术要求等，如投标人没有对招标文件的实质性条款做出全面的实质性响应，则可能导致其投标被拒绝。

8、招标文件的澄清

投标人要求澄清招标文件的，请于澄清截止时间前由参加报名的供应商持法人代表授权书，向采购代理机构正式书面提出（书面文件必须加盖单位公章）。采购代理机构将予以答复，逾期提交的不予受理。

9、招标文件的澄清或者修改

9.1 采购代理机构可以对已发出的招标文件进行必要的澄清或者修改，但不得改变采购标的和资格条件。澄清或者修改应当在原公告发布媒体上发布澄清公

告。

澄清或者修改的内容可能影响投标文件编制的,采购代理机构应当在投标截止时间至少 15 日前,以书面形式通知所有获取招标文件的潜在投标人;不足 15 日的,采购代理机构应当顺延提交投标文件的截止时间。

9.2 澄清或者修改的内容为招标文件的组成部分。

三、投标文件编制与递交

10、投标文件的语言

投标人编写投标文件和往来函件应以中文书写。

11、投标文件中的计量单位

除招标文件另有规定外,投标文件的计量单位应使用中华人民共和国法定计量单位。

12、投标文件构成

详见“投标人须知前格式”中“投标文件构成”。

13、投标报价

13.1 投标人的投标报价应为投标货物在采购人指定地点交货并完成安装调试和正常运行(含售后质量保证及技术支持、培训、备件等所有伴随服务)的最终价格。

13.2 投标人必须在“投标分项报价表”中报出投标货物和服务的分项单价。对招标文件要求提供的货物和服务,而投标人未提供分项报价的视为免费提供。

13.3 采购人不接受投标人提供的选择性报价、赠送,每种货物或服务只允许有一个报价。否则,在评标时将其视为无效投标。

13.4 投标报价中的单价和总价全部采用人民币表示和结算。

13.5 除合同条款中另有规定外,投标货物和服务的分项单价在合同实施期

间不得变动。

14、投标文件的签署及规定

14.1 投标文件需清楚的标明“正本”，投标文件的正本须是打印文件（一份正本文件）。同时，投标人须随一份投标文件正本提供与其内容相同并在首页加盖《关于供应商办理 CA 数字证书及电子签章的通知》中指定供应商签发的单位电子签章的电子版本文件一份，并在首页注明电子签章签发单位（吉林省安信电子认证服务有限公司、中金金融认证中心有限公司、北京数字证书股份有限公司）。

如果投标文件纸质正本与电子版不一致，以纸质正本为准。因纸质正本与电子版内容不一致而导致的不利后果由投标人承担。

14.2.1 采购代理机构接受的投标文件电子版格式为：PDF 格式，并加盖电子签章。投标人使用 Microsoft office word 2010 以上版本编写投标文件后另存为 PDF 格式。

14.2.2 投标人在提交加盖电子签章的 PDF 格式投标文件的同时提交一份 Office Word 版本的投标文件，并自行承诺两份文件一致性。

14.3 投标文件纸质正本应由投标人法人代表或经其正式授权代表逐页签名或逐页盖单位公章。正式授权代表签字的，投标文件中需附有“法人代表授权书”。

投标文件中的盖章、公章仅指与投标人名称全称相一致的标准单位公章，而非投标专用章等其他非公章。如使用投标专用章，须提供特别说明函，明确该投标专用章作为投标文件的签章其效力等同于单位公章（该特别说明函须同时加盖投标人单位公章和投标人投标专用章）。“法定代表人授权书”必须按招标文件要求加盖与投标人名称全称相一致的标准单位公章。

14.4 投标文件不得行间插字、涂改或增删，如有修改，必须由投标人法人代表或经其正式授权代表签名或盖单位公章。

14.5 出现下列情况之一的投标文件按无效投标处理：

投标文件电子版与纸质正本均未按要求加盖《关于供应商办理 CA 数字证书及电子签章的通知》中指定供应商签发的单位电子签章或公章的；

投标人未能按招标文件要求提供投标文件纸质正本、电子版及两者一致性的书面承诺书的;

14.6 未按照招标文件要求密封的纸质或电子版投标文件, 采购人、采购代理机构应当拒收。

15、投标文件的密封、标记和递交

15.1 投标人应将开标一览表与投标文件同时递交至开标地点。

15.2 投标文件的正本应封装在独立信封中, 在信封上标明“正本”字样。

15.3 外层信封应:

(1) 写明项目名称、项目编号、投标人名称、地址和邮政编码, 并于袋口密封处加盖公章。

(2) 注明“请勿在 200 年 月 日 时 00 分(开标时间)之前启封”的字样。

15.4 外层包装没有按上述规定密封的投标文件将会被拒绝。

15.5 电报、电话、传真、邮件形式的投标文件概不接受。

16、投标文件的修改和撤回

16.1 投标人在投标截止时间前, 可以对所递交的投标文件进行补充、修改或者撤回, 并书面通知采购代理机构。补充、修改的内容应当按照招标文件要求签署、盖章、密封后, 作为投标文件的组成部分。

16.2 在投标截止时间后, 不得更改投标文件。

四、开标

17、开标

17.1 采购代理机构在招标文件第一章《投标邀请》中规定的时间和地点组织开标。投标文件中授权的投标人代表应参加开标并签名报到。

17.2 开标由采购代理机构主持，邀请投标人参加。评标委员会成员不得参加开标活动。开标时，应当由投标人或者其推选的代表检查投标文件的密封情况；经确认无误后，由采购代理机构工作人员当众拆封，宣布投标人名称、投标价格和书面修改和撤回投标的通知以及采购代理机构认为合适的其它内容。

对于未按规定格式编制或未盖单位公章的开标一览表，采购代理机构将不予唱标。

投标人不足 3 家的，不得开标。

17.3 开标过程应当由采购代理机构负责记录，由参加开标的各投标人代表和相关工作人员签字确认后随采购文件一并存档。

投标人代表对开标过程和开标记录有疑义，以及认为采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。采购代理机构对投标人代表提出的询问或者回避申请应当及时处理。投标人未参加开标的，视同认可开标结果。

18、投标人资格审查

18.1 见“投标须知前格式”中“投标人资格审查”。经审查不符合资格的投标人的投标文件，按无效投标处理，合格投标人不足 3 家的，不得评标。

18.2 投标人信用记录

信用信息查询渠道：信用中国网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道。查询截止时间为开标后资格审查时间。

信用信息查询记录和证据留存的方式：信用信息查询记录和证据必须留存，并与该采购文件一并保存。

信用信息的使用规则:对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商,应当拒绝其参与政府采购活动。

五、评标

19、组建评标委员会

19.1 采购代理机构根据招标项目的特点,并按照政府采购法律规定的原则组建评标委员会,评标委员会负责对投标文件进行审查、质疑、评估和比较。

19.2 本项目评标委员会由采购人代表和有关技术、经济等方面的专家组成。

19.3 对投标文件的审查、质疑、评估和比较以及确定中标的过程中,投标人对采购人和评标委员会成员施加影响的任何行为,都将导致其投标资格被取消。

20、投标文件的符合性审查

20.1 评标委员会应当对符合资格的投标人的投标文件进行符合性审查。即审查、评价投标文件是否符合招标文件的商务、技术等实质性要求。评标委员会将首先审查投标文件是否完整,文件签署是否合格,有无计算上的错误,投标文件是否大体编排有序且提供了招标文件要求的所有有效证明文件。投标文件有下列情况之一者将被拒绝:

- (一) 投标文件未按招标文件要求签署、盖章的;
- (二) 不具备招标文件中规定的资格要求的;
- (三) 报价超过招标文件中规定的预算金额或者最高限价的;
- (四) 投标文件含有采购人不能接受的附加条件的;
- (五) 不同投标人的投标文件由同一单位或者个人编制;
- (六) 不同投标人委托同一单位或者个人办理投标事宜;
- (七) 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人;

(八) 不同投标人的投标文件异常一致或者投标报价呈规律性差异;

(九) 不同投标人的投标文件相互混装;

(十) 法律、法规和招标文件规定的其他无效情形。

20.2 如果投标文件实质上没有响应招标文件的要求, 评标委员会将予以拒绝。

20.3 对于专门面向中小企业采购的项目, 如果评标委员会认定投标(响应、报价) 供应商不是中小微企业, 该供应商的投标(响应、报价) 按无效处理。

20.4 预留份额的采购项目或者采购包, 通过发布公告方式邀请供应商的采购项目, 符合资格条件的中小企业数量不足 3 家的, 中止采购活动, 视同未预留份额的采购项目或者采购包, 按照财库〔2020〕46 号第九条有关规定重新组织采购活动。

21、合格投标文件的修正与澄清

21.1 对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容, 评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。

21.2 投标文件报价出现前后不一致的, 除招标文件另有规定外, 按照下列规定修正:

(一) 投标文件中开标一览表(报价表) 内容与投标文件中相应内容不一致的, 以开标一览表(报价表) 为准;

(二) 大写金额和小写金额不一致的, 以大写金额为准;

(三) 单价金额小数点或者百分比有明显错位的, 以开标一览表的总价为准, 并修改单价;

(四) 总价金额与按单价汇总金额不一致的, 以单价金额计算结果为准。

同时出现两种以上不一致的,按照前款规定的顺序修正。修正后的报价按照《政府采购货物和服务招标投标管理办法》第五十一条第二款的规定经投标人确认后产生约束力,投标人不确认的,其投标无效。

21.3 投标人的澄清、说明或者补正应当采用书面形式,并加盖公章,或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。投标人不确认的,其投标无效。

21.4 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价,有可能影响产品质量或者不能诚信履约的,应当要求其在评标现场合理的时间内提供书面说明,必要时提交相关证明材料;投标人不能证明其报价合理性的,评标委员会应当将其作为无效投标处理。

22、投标文件的评价和比较

22.1 经符合性审查合格的投标文件,评标委员会将根据以下的评标原则和办法进行评标。

22.2 评标原则

(1) 评标委员会将遵循公开、公平、公正的原则,对所有投标人的投标评估都采用相同的程序和标准;

(2) 评标参照政府采购有关法律、法规以及本招标文件规定的评标办法进行;

(3) 维护招、投标双方的合法权益。

22.3 评标办法

(1) 本次评标采用综合评分法,是指投标文件满足招标文件全部实质性要求,且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

(2) 评标委员会将依据上述评标办法制定的评分细则(详见本招标文件附件部分)进行评标,计算各投标人得分并排出名次。

23、确定中标候选人

23.1 评标委员会将按照评审得分由高到低顺序排名推荐中标候选人。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

23.2 最低报价的投标人并不保证成为中标候选人。

24、编写评审报告

评审报告是评标委员会根据全体评标成员签字的原始评标记录和评标结果编写的报告。评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评标工作，与采购代理机构沟通并作书面记录。采购代理机构确认后，应当修改招标文件，重新组织采购活动。

六、中标

25、公示中标候选人

根据《国有金融企业集中采购管理暂行规定》（财金〔2018〕9号）第二十八条“采用公开招标方式的，应当按规定发布招标公告、资格预审公告，公示中标候选人、中标结果等全流程信息”，采购代理机构应当在评标委员会提交评审报告后，在“投标人须知前格式”中的“信息公示渠道”上公示中标候选人。

26、确定中标

确定中标方式详见“投标人须知前格式”中的“确认中标方式”。

如评审中出现异常或特殊情况，采购代理机构有权按照相关法律规定进行处理。

27、采购代理机构拒绝任何或所有投标的权利

为维护国家和社会公共利益,采购代理机构在签订合同之前,保留拒绝任何投标,终止以及宣布招标活动取消的权利。采购代理机构对受影响的投标人不承担任何责任,也无需向投标人解释理由。

28、中标通知书

28.1 采购代理机构应当自中标人确定之日起 2 个工作日内,在“投标人须知前格式”中的“信息公示渠道”上公告中标结果,招标文件应当随中标结果同时公告。中标、成交供应商享受财库〔2020〕46 号文件规定的中小企业扶持政策的,中标、成交供应商的《中小企业声明函》将随中标、成交结果一并公示。

28.2 中标通知书是合同的组成部分。

28.3 采购代理机构应当向中标人发出中标通知书;对未通过资格审查的投标人,应当告知其未通过的原因;采用综合评分法评审的,还应当告知未中标人本人的评审得分与排序。

七、履约

29、签订合同

29.1 采购人应当自中标通知书发出之日起 30 日内,按照招标文件和中标人投标文件的规定,与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

29.2 如果中标人没有按照上款规定与采购人签约,采购人有权按照评审报告推荐的中标候选人名单排序,确定下一个中标候选人为中标人,或重新招标。如中标供应商被发现前期采购过程中存在提供虚假材料谋取中标的行为,该供应商中标无效,按照政府采购有关法规要求处理。

29.3 招标文件、中标人的投标文件及澄清文件,均为合同的组成部分。

八、附则

30、解释权

本招标文件的解释权属于采购代理机构。

31、未尽事宜

本招标文件未尽事宜按照《中华人民共和国政府采购法》及其它有关法律法规的规定执行。

第三章

合同格式及合同条款

农信银资金清算中心 农信云长沙区建设采购合同



甲 方：农信银资金清算中心有限责任公司

地 址：北京市丰台区南四环西路 186 号汉威国际广场二区 4 号楼

邮 编：100160

联系人：_____

电 话：_____

邮 箱：_____

传 真：_____

乙 方：_____

地 址：_____

邮 编：_____

联系人：_____

电 话：_____

邮 箱：_____

传 真：_____

通用条款

甲、乙双方本着诚信公平、共同发展的原则，经协商，在平等自愿的基础上，依据《中华人民共和国民法典》及相关法律法规，就甲方向乙方采购硬件、软件及服务事宜签订本合同，以兹双方共同遵守。

第一条 乙方服务水平保证

(一) 提供的产品的技术指标符合国家或行业标准。

(二) 按本合同、招标文件、乙方投标文件及澄清文件约定时间向甲方交付全部硬件、软件产品，保证所提供的硬件、软件及相关版本型号均为原厂、原装且拥有合法知识产权及使用授权的硬件、软件，且提供硬件、软件完全符合本合同、招标文件、乙方投标文件及澄清文件及产品说明书规定的版本、质量、规格和性能的要求，满足甲方的硬件、软件采购需求，实现本合同约定目的。

(三) 采购硬件、软件涉及原厂测试的，乙方需按照技术要求通过相关厂家软件诊断验证。

(四) 硬件、软件安装调试完成后运转良好、工作正常。提供相关的技术支持，负责硬件、软件的安装、调试及甲方人员的应用培训工作。

(五) 保证向甲方提供的硬件、软件与甲方现有的技术、软硬件配置兼容，不存在因技术不配套而产生任何影响甲方系统运行、业务开展的因素。

(六) 保证其有权签署本合同，保证其拥有履行本合同所必需的资质及能力。签署本合同不侵犯包括甲方在内的任何其他方的合法权

益；保证其根据本合同约定向甲方提供服务的行为不损害包括但不限于其债权人、客户在内的任何第三方的合法权益，并保证甲方使用乙方提供的资料不受任何第三方关于侵犯专利权、著作权、商标权等知识产权的指控。任何第三方在本合同签订后提出有关侵权指控，乙方应负责与第三方交涉并承担由此引起的法律责任和所有费用。

(七) 乙方保证在事件发生后五日内及时向甲方书面通报公司重大事件并提供相关证明文件，包括但不限于：

1. 公司名称的变更、公司注册地的变更、公司注册资本的变更；
2. 公司发生并购行为；
3. 公司经营发生困难；
4. 公司涉及标的超过本合同金额或人民币壹佰万元（以二者中金额较小的为标准）的诉讼、仲裁等纠纷；
5. 公司及其关联公司发生严重声誉事件；
6. 公司资质证书过期或者吊销；
7. 公司法定代表人、高级管理人员发生风险事件（包括但不限于被公安、司法等有关机构调查、发生或者极有可能发生重大违法行为等）；
8. 其他有可能对合同产生不利影响的异常事件。

(八) 乙方应遵守甲方业务连续性管理规章制度，根据甲方要求开展信息系统突发事件分析与应急处置工作，并须在国家、主管机构、监管机构及本中心要求的重要保障时期提供重要保障服务。

(九) 乙方承诺不利用提供产品和服务的便利条件非法获取甲方用户数据、非法控制和操纵甲方用户设备，无正当理由不中断产品供应或必要的技术支持服务等。

(十) 乙方承诺提供产品和服务满足本合同、招标文件、乙方投标文件及澄清文件要求。因乙方对招标文件理解不充分导致设备、软件、服务不能满足要求采购需求的,乙方应在本合同总价款不变的前提下,无条件提供补救方案,并承担由此产生的逾期责任以及所有费用。

第二条 保密条款

(一) 乙方应对在履行本合同过程中获悉的甲方的有关数据机密、文档资料、商业秘密及甲方要求保密的其他信息(以下简称“保密信息”)严格保密,并采取相应的保密措施,乙方应指示雇员遵守保密义务,乙方及乙方雇员不得将其用于本合同以外的其他目的或披露给任何第三人。在本合同终止或解除后或甲方要求时,乙方应及时将保密信息全部返还甲方或按甲方要求作适当处理。

(二) 上述保密义务的期限至保密信息正式向社会公开之日或甲方书面解除乙方本合同项下保密义务之日止。

第三条 违约责任

(一) 逾期违约

根据本合同、招标文件、投标文件及澄清文件中各节点时间约定,乙方每逾期1天,甲方有权要求乙方支付合同总价款**0.5%**的违约金;逾期超过30天的,甲方有权单方解除本合同,乙方应按合同总价款**10%**向甲方支付违约金。因逾期给甲方造成损失,乙方就全部损失承担赔偿责任。

(二) 付款违约

如甲方自身原因导致未能按照本合同约定付款的,经乙方书面催告的30日内甲方仍未支付,每逾期一天,乙方有权要求甲方支付合

同总价款 0.5%的违约金,但违约金总额累计不超过合同总价款的10%。

(三) 维保服务违约

如乙方未能按照本合同约定时间提供《原厂维保服务承诺函》(可根据乙方内部管理需要变更该函件名称;下同)或提供内容与甲方要求不符的,甲方有权单方解除本合同,乙方应向甲方支付合同总价款30%的违约金。

维保服务期间,乙方未及时提供维保服务或乙方提供的服务与本合同约定不符的,甲方有权通过其他途径购买维保服务,由此发生的全部费用由乙方承担。乙方应自收到甲方书面账单通知之日起10个工作日内,支付相关费用。若乙方每逾期1天,甲方有权要求乙方支付相关费用0.5%的违约金。

(四) 保证违约

本合同生效后,如甲方能够证明乙方存在违反本合同“乙方服务水平保证”条款的行为(无论该等违约行为发生在本合同签订之前或之后),除非乙方采取充分的证明或保证或补救措施使甲方确信因乙方违约行为而使甲方可能遭受的不利影响已消除或得到充分补偿,否则,甲方有权拒绝接收硬件、软件、单方解除本合同,此外乙方应向甲方支付合同总价款30%的违约金。

(五) 保密违约

乙方违反本合同及《安全保密协议》所约定的其在保密方面的义务,应向甲方支付合同总价款20%的违约金,由此给甲方造成损失的,应按照甲方的实际经济损失向甲方支付赔偿金。本违约金的支付义务独立于其他违约义务。

（六）其他违约

除本合同另有约定外，任何一方违反本合同约定，违约方应向守约方支付本合同总价款 **10%** 的违约金，承担继续履行、采取补救措施等违约责任，并赔偿守约方由此遭受的损失；任何一方违反本合同约定导致本合同无法继续履行，另一方有权终止合同，并有权要求违约方承担赔偿责任。

（七）违约通知和违约限制

1. 如发生违约事件，守约方要求违约方支付违约金、赔偿金时，以书面方式通知违约方，内容包括违约事件、违约金金额、赔偿金金额、支付时间和方式等；违约方在收到上述通知后，应于 10 个工作日内书面形式答复对方，并支付违约金、赔偿金。如双方不能就此达成一致意见，将按照本合同所约定的“**争议解决**”条款解决纠纷，但任何一方不得采取非法或损害本合作项目的手段以强行收取违约金。

2. 违约方除应按照本合同项下约定承担支付违约金的责任外，还应赔偿守约方因此遭受的一切损失，包括但不限于诉讼费、仲裁费、律师费、评估费、鉴定费、审计费、公证费、保全费、保险费、差旅费。

（八）其他

除本合同另有约定外，甲方根据本合同约定单方解除合同的，乙方应自收到甲方书面解除合同通知之日起 10 日内退还此前甲方已经支付的合同费用，同时按约定金额或比例支付违约金，并赔偿由此给甲方造成的全部损失。

（九）技术转移违约

乙方未按本合同、附件 1 采购清单及服务约定及甲方要求向甲方提供技术转移相关服务，且经甲方明确提出具体要求仍不提供服务的，应按照本合同总价款的 5% 向甲方支付违约金。

第四条 不可抗力

(一) “不可抗力”指本合同签订时不能预见的、其发生与后果无法避免或克服的、妨碍任何一方全部或部分履约的所有事件，包括但不限于地震、台风、水灾、火灾、战争、交通管制、流行病、民乱、罢工，以及由于国家法律、法规、行政规章或命令等。遇有上述不可抗力的一方，必须以最快方式及时通知对方，并在不可抗力因素发生后十五日内提供不可抗力的详细情况及合同不能履行，或者部分不能履行，或者需要延期履行的理由和有效的证明文件。此项证明文件应由不可抗力发生地的公证机关出具，按其对履行合同影响的程度，由双方协商决定是否解除合同，或者部分免除履行合同的义务，或者延期履行合同。如因一方怠于通知而造成另一方损失或损失扩大的，则怠于通知的一方应负责赔偿另一方的相应损失。

(二) 受不可抗力影响的一方，应当尽可能采取合理的行为和适当的措施减轻不可抗力对履行本合同所造成的影响。没有采取适当措施致使损失扩大的，该方不得就扩大损失的部分要求免责或赔偿。如果不可抗力因素的后果影响本合同的执行超过 20 日，任何一方均有权终止本合同。

第五条 争议解决

(一) 有关本合同的任何争议，双方应首先本着相互信任、长期合作的原则，共同协商解决。协商不成，双方同意由北京仲裁委员会进行仲裁。仲裁是终局的，一经裁决对双方均具有法律效力。

(二) 除正在提交仲裁或与仲裁有关的部分外, 双方应继续履行本合同其余部分。

第六条 通知送达与到达

(一) 除本合同另有约定外, 为享有本合同约定的权利和履行本合同约定的义务或有关违约交涉而需通知另一方时, 必须采取书面形式。通知的地址为本合同首页上所述地址。合同涉及有关通知事项可按照本合同约定的通知与送达方式, 采用邮寄、直接送达、电子邮件等任一方式进行, 邮寄到达当日、直接送达、电子邮件发送当时, 即视为接到该通知。

(二) 如一方欲改变通知地址、电话、联系人、邮箱等信息时, 则应提前10个工作日以邮件方式通知另一方, 否则应自行承担送达不能的法律后果, 且非责任方按照本合同约定的通知与送达方式向其发出的任何通知均视为合法有效。

(三) 甲、乙双方同意, 在合同中约定的地址、电子邮箱, 均可作为送达仲裁文书(包括但不限于申请书、传票、举证通知书、出庭通知书、各类裁定等)的确认地址。即, 只要仲裁委员会将仲裁文书发送至甲、乙方约定的地址、电子邮箱, 即视为送达。因责任方自己提供或者确认的送达地址不准确、送达地址变更未及时告知对方, 责任方或者责任方指定的联系人拒绝签收, 导致仲裁文书未能被责任方实际接收的, 文书退回之日视为送达之日。

第七条 其他

(一) 经甲方网络安全审查预判本合同项目属于下述第 2 种情况。

1. 无需提交网络安全审查的项目。本合同经双方法定代表人/授权代表签名/盖章并加盖公章/合同专用章之日起生效。甲乙双方一致同意

不执行网络安全审查条款。

2. 需要将相关材料提交网络安全审查办公室或其委托机构判定是否需要网络安全审查的项目。

对于经网络安全审查办公室或其委托机构书面通知无需进行网络安全审查的项目,本合同经双方法定代表人/授权代表签名/盖章并加盖公章/合同专用章,且甲方收到网络安全审查办公室或其委托机构出具的无需审查的书面通知之日起生效。

对于需经网络安全审查的项目,本合同经双方法定代表人/授权代表签名/盖章并加盖公章/合同专用章,且甲方收到网络安全审查办公室或其委托机构出具的网络安全审查结论为通过的书面材料之日起生效。

(二)除本合同另有约定外,本合同至双方均履行完本合同项下全部义务且相关费用付清之日终止。

(三)本合同所列附件为本合同不可分割之组成部分,与本合同具有同等法律效力。附件内容与本合同约定冲突时,以本合同之相关约定为准。

(四)本合同未尽事宜,均需甲乙双方以书面补充协议的形式体现,并作为本合同的有效组成部分,与本合同具有同等法律效力。

(五)为营造健康营商环境,共创风清气正的合作氛围,甲乙双方签订《廉洁合作协议》(详见附件8)。

(六)本合同一式肆份,甲方、乙方各执贰份,具有同等法律效力。

(七)自甲方知道或应当知道解除事由之日起满三年,甲方在本

合同中享有的解除权消灭。

（以下为专用条款）

专用条款

甲方委托乙方按照本合同约定采购相关软件及服务, 详见《采购清单及服务要求》(附件 1)。

第一条 双方权利与义务

(一) 甲方权利与义务

1. 按照合同约定如期向乙方支付合同款项。
2. 有权对乙方的履约情况进行监督、检查及评价, 并进行风险评估或审计。
3. 按照合同约定, 做好软件初验、终验及服务验收。验收不通过时, 有权要求乙方整改直至验收通过, 并顺延相应款项支付。
4. 与乙方、原厂签订《安全保密协议》, 详见附件 9。

(二) 乙方权利与义务

1. 按本合同约定时间向甲方交付全部合同硬件、软件产品及授权使用认证。硬件、软件的产品说明书、技术资料等文件完整、清晰。
2. 配合甲方及甲方内、外部审计机构和监管机构的检查、评估或审计。
3. 配合甲方开展到货验收、集成部署验收、试运行验收、技术转移验收及终验等。验收不通过时, 应进行整改直至验收通过。
4. 负责协调硬件、软件原厂提供原厂维保服务及技术支持工作。
5. 对甲方的相关人员进行技术转移, 目标包括但不限于甲方人员能够独立、熟练地完成系统操作, 实现依据本合同所约定的目标和功能, 具体以附件 1 采购清单及服务要求为准。
6. 如软件存在重大问题或发生重要变更, 乙方应当在知道上述事件 1 个工作日内向甲方做出书面报告。

7. 按照合同的约定按时向甲方提供全额发票或等额发票。

8. 未经甲方书面同意,乙方不得任意终止或向第三方转包、分包或使其继承本合同项下的权利或义务。

9. 与甲方、原厂签订《安全保密协议》,详见附件 9。

第二条 硬件、软件交付

(一) 交付时间:

乙方应在本合同生效之日起40个工作日内向甲方交付本合同所约定的全部硬件、软件。

因乙方原因未在约定时间内完成交付的,视同乙方**逾期违约**,并按**《通用条款》违约责任条款**相关约定承担违约责任。

(二) 硬件交付:

交付地点:湖南省长沙市岳麓区福祥路

1. 设备须装置于适合运送及气候变化的坚固木箱或纸箱(以下简称箱体)内,且妥善防潮、防震、防锈、防腐蚀等。专用、特殊安装工具材料和易磨损部件应进行包装并采取保护措施。乙方需在每一包装箱/物表面显著位置以显著方式标明甲方收货人、目的地、设备名称、尺寸规格、数量、重量等内容,并对每一箱体内产品附以标签,标明其在安装图纸中的编号(如有)。另外乙方应根据产品的特点及其对装卸操作的要求在箱体显著位置以英文或中文标明“保持干燥”,“小心轻放”,“此面向上”等国际惯用图示。包装费用由乙方承担。

2. 在合同产品的包装中应附有详细的装箱单、产品质量合格证、与合同产品有关的技术材料、产品说明书及产品出厂所需的其他资料。

3. 凡由于对合同产品的包装不当或采取的防护措施不充分或运

输过程中致使产品损坏或丢失的,乙方均应负责免费更换;未完成更换前,视作乙方尚未交付;直至乙方交回合格的产品,其间延误的时间视为乙方逾期交付的时间。

4. 设备运至指定交付地点的运费及保险费等相关费用由乙方承担。

(三) 软件交付

1. 软件交付须提供合理、有效、安全的存储介质进行产品存储于提交,提交介质应防潮、防震、防锈、防腐蚀及防磁化处理等。需从固定服务资源或互联网下载的软件产品需提供有效下载地址,并保证软件下载过程安全可控。涉及软件许可授权的,应保证乙方可顺利验证通过。

2. 软件产品附有详细的软件配置清单及版本信息、产品质量合格证、与合同产品有关的技术材料、产品说明书及产品出厂所需的其他资料。

3. 凡由于软件产品交付不当或无法下载致使软件无法使用的,乙方均应负责免费解决;未解决前,视作乙方尚未交付;直至乙方交付合格可用的软件产品,其间延误的时间视为乙方逾期交付的时间。

4. 软件交付如产生运费及保险费的全部费用由乙方承担。

5. 乙方承诺拥有本合同约定软件产品完整的知识产权或者有效授权(且可转授权),**确保甲方可以永久使用本合同约定的软件产品**,且不受到任何其他方提出的侵权指控。任何其他方在本合同签订后或在甲方使用过程中提出有关侵权指控,应由乙方负责与提出方交涉并承担由此引起的法律责任和费用,给甲方造成损失的,乙方应负责赔偿。

第三条 验收

各阶段验收应按照《采购清单及服务要求》（附件 1）及本合同其他约定完成。

本合同的验收主体为农信银资金清算中心有限责任公司、本项目供应商及第三方专业机构。验收方式为现场验收或验收评审会议，验收程序为由乙方提出验收申请，甲方组织各相关部门对项目的质量、进度、范围，按照验收标准进行验收。。

（一）到货验收：

1. 时间：自设备上电试运行完成后7个日历日内，甲、乙双方按本款约定标准进行到货验收。

2. 内容：在合同签订后设备到货时间是否满足要求；软、硬件设备到货后，核对与供货通知单的品类、数目、配置是否一致；乙方协调软、硬件原厂商将箱体拆封，核对设备外包装、外观是否完好，装箱单等随机资料是否齐全；硬件设备上电试运行是否正常。

3. 标准：满足如下标准，视为验收通过，甲方、乙方、原厂商签署《到货验收单》（格式见附件 2）：

乙方应按照本合同附件 1 采购清单及服务要求第（二）部分项目实施服务要求中的第 2 项设备到货验收要求完成相关工作，并保证交付软硬件品类、数目、配置与附件 1 采购清单及服务要求一致，设备外包装、外观完好，装箱单等随机资料齐全，硬件设备上电试运行无误。

（二）集成部署验收

1. 时间：设备到货 2 个月内，乙方应按照附件 1 采购清单及服务要求第（二）部分项目实施服务要求第 3 项集成部署要求完成设

备安装及相关软件调试等集成部署工作,并自集成部署完成**2个月**内通过相关测试(验证测试要求详见附件1采购清单及服务要求第(二)部分项目实施服务要求第4项验证测试要求)后,乙方向甲方提出书面申请,甲、乙双方及原厂商进行集成部署验收。

2. 内容:生产云的设备安装和软件系统调试是否满足集成部署要求,完成时间是否满足需求;是否根据验证测试要求进行验证测试,验证测试是否通过。

3. 标准:满足如下标准,视为验收通过,甲方、乙方及原厂三方人员签署《集成部署验收报告》(格式见附件3):

乙方遵照附件1采购清单及服务要求第(二)部分项目实施服务要求第3项集成部署要求、第4项验证测试要求完成相关工作。

4. 因乙方原因未在约定时间内完成集成部署、验证测试工作的,视同乙方**逾期违约**,并按《通用条款》违约责任条款相关约定承担违约责任。

(三) 项目试运行验收

1. 时间:完成集成部署验收**2个月**内,乙方应按照本合同附件1采购清单及服务要求第(二)部分项目实施服务要求第5项试点应用部署要求完成相关工作。完成试点应用部署后**4个月**内,乙方应按照本合同附件1采购清单及服务要求第(二)部分项目实施服务要求第6项系统上线要求完成相关工作。完成系统上线相关工作后,经甲方同意,双方启动项目试运行,试运行期间**3个月**,试运行期满,乙方向甲方提出申请,甲、乙及原厂三方进行试运行验收。甲方有权结合自身情况调整试点应用部署及系统上线时间,但应提前书面通知乙方。

2. 内容：农信云生产云的业务功能、技术指标是否满足要求，且项目试运行 3 个月内有无严重等级缺陷发生。

3. 标准：满足如下标准，视为验收通过，签署《试运行验收报告》（格式见附件 4）：

农信云生产云的业务功能、技术指标满足要求，乙方遵照附件 1 第（二）项目实施服务要求完成试点应用部署及系统上线，且项目试运行 3 个月内无严重等级 3 级以上（含 3 级）缺陷发生。

缺陷分类说明如下：

严重等级 1：系统无法运行。即在日常必需的功能测试和运行中，系统无法正常完成工作或无法产生正常结果。

严重等级 2：系统存在功能、性能缺陷。但系统能够运行，在某些特定环境下，无法达到性能或功能要求。

严重等级 3：系统存在功能、性能缺陷。但在生产环境中，可采用其它方式替代或弥补，并达到同样效果。

严重等级 4：微小缺陷。系统功能、性能符合要求，可以服务于用户，有局部需要改动或润色

4. 因乙方原因未在约定时间内完成试点应用部署、系统上线的，视同乙方**逾期违约**，并按《通用条款》**违约责任条款**相关约定承担违约责任。

（四）技术转移验收

1. 时间：自技术转移要求满足后 7 个日历日内，甲、乙双方进行技术转移验收。

2. 内容: 乙方是否提供了完备的云平台软硬件部署、使用、开发、测试、维护、故障处理以及对外接口开发等方面的详细的使用文档, 并使甲方相应的技术人员达到相应的技术水平。

3. 标准: 满足如下标准, 视为验收通过, 由乙方、原厂商和甲方签署《技术转移验收报告》(附件 5):

乙方遵照附件 1 采购清单及服务要求第(二)部分项目实施服务要求第 7 项完成技术转移服务, 提供了完备的技术文档, 提供了相应的培训及考试机会, 提供了必要的工具并使甲方相应的技术人员达到了如下的技术水平:

a. 能够熟练使用和维护农信云平台:

b. 能够独立进行接入交换机、计算节点、裸金属节点、容器 Node 节点、存储节点的扩容、缩容、更换等操作;

c. 具有熟练查阅各种相关技术文件及维护手册的能力;

d. 掌握农信云平台的工作原理以及基于标准接口的开发方法。

(五) 项目终验

1. 时间: 项目试运行验收通过后满 6 个月, 经乙方向甲方提出终验申请, 甲、乙双方及原厂商进行项目终验。

2. 内容: 完成质量检测认证、整体优化完善等工作后, 乙方、原厂商和甲方(必要时由第四方参加)共同组成验收小组进行项目最终验收。重点关注项目期间产生的所有问题是否得以有效解决, 终验前 6 个月内是否有严重缺陷发生, 乙方各阶段的提供的文件、文档是否符合相关要求, 各类报告是否完备合格。

3. 标准：满足以下标准，并自项目最终验收需求满足后 7 个日历日内，乙方向甲方提供《原厂维保服务承诺函》，视为验收通过，签署项目《终验报告》（附件 6）：

- a. 项目期间产生的所有问题均得以有效解决。
- b. 终验前 6 个月无严重等级 3 级以上（含 3 级）缺陷发生。
- c. 乙方提供了项目软硬件原厂提供的维保服务承诺函。

缺陷分类说明如下：

严重等级 1：系统无法运行。即在日常必需的功能测试和运行中，系统无法正常完成工作或无法产生正常结果。

严重等级 2：系统存在功能、性能缺陷。但系统能够运行，在某些特定环境下，无法达到性能或功能要求。

严重等级 3：系统存在功能、性能缺陷。但在生产环境中，可采用其它方式替代或弥补，并达到同样效果。

严重等级 4：微小缺陷。系统功能、性能符合要求，可以服务于用户，有局部需要改动或润色。

d. 各阶段所涉及的所有安装文件、源程序、构建、配置文件、相关技术文档、培训资料等均已提供，并书面保证移交的源程序编译后和线上运行的程序完全一致。

e. 具备权威部门出具的符合相关标准规范与认证的证明或报告（网络安全等级保护三级、商用密码应用安全性评估三级），优化点验收测试报告。

（六）其他：

1. 如各阶段验收中发现交付合同产品有缺陷或其他与合同约定不符合的情形，乙方应在甲方指定的期限内免费进行更换或版本升

级,直至乙方通过各阶段验收,其间延误的时间视为乙方验收逾期的时间。

2. 如出现乙方逾期的情形,甲方费用支付相应顺延,甲方就此不承担任何责任。

3. 甲方有权适当调整到货计划及验收安排,但应自本合同约定的相应截止日期前3个工作日内书面告知乙方。

4. 乙方在完成相关工作后,应积极向甲方申请验收,并配合甲方、协调原厂开展验收工作。经甲方验收不合格的,乙方应协调原厂进行整改,并尽快再次提请甲方验收。除甲方认可的情形外,经两次验收仍不合格的,均视为乙方验收逾期,每逾期一日,乙方需向甲方支付合同总价款0.5%的违约金,并承担继续履行本合同的相关义务。如逾期时间超过30天,甲方有权单方解除本合同,乙方应按合同总价款的20%向甲方支付违约金。**该违约金的支付义务独立于其它违约义务。**

第四条 服务要求

本合同约定服务内容包括但不限于维保服务、技术支持与服务以及其他采购文件要求、本合同约定、投标文件承诺的其他内容。

本项目自合同订立生效之日起开始执行,预计项目实施周期为12个自然月,验收通过后提供云平台整体3年,服务器设备5年的维保服务,实际结束时间以满足项目验收条件并且维保期结束为准,可根据实际情况延长。项目如有调整以甲方通知为准,经甲乙双方协商一致,合同期限可顺延。

(一) 维保服务

自《终验报告》签署之日起,乙方应按照《采购清单及服务要求》约定分别提供为期3年的网络设备、安全设备及软件维保服务,为期

5 年的服务器产品维保服务。在维保服务期内，如设备、软件产品非甲方原因发生故障，乙方应协调原厂提供免费上门提供售后服务。

《原厂维保服务承诺函》应加盖原厂公章，生效日期为《终验报告》签署日，有效期为 5 年（服务器及备份对接设备）、3 年（其他软硬件）。如《原厂维保服务承诺函》生效日期早于《终验报告》签署日，乙方应协调原厂在《原厂维保服务承诺函》到期但维保服务期未届满前，按照《原厂维保服务承诺函》规定标准向甲方提供同等维保服务。

（二）技术支持与服务

乙方按照甲方《采购清单及服务要求》中的需求，向甲方提供农信云技术支持与服务。

（三）服务验收

甲方以年为周期，按照本合同、《采购清单及服务要求》、《原厂维保服务承诺函》内容对乙方所有服务进行验收，验收通过的，双方签署《服务验收单》（格式见附件 7）。

第五条 合同款项

（一）合同款项

本合同总价款为¥_元整（大写：_人民币元整），其中硬件设备价款为¥_元整（大写：_人民币元整），软件产品价款为¥_元整（大写：_人民币元整），服务项价款为¥_元整（大写：_人民币元整）。价格明细见《采购清单及服务要求》（附件 1）。

本合同总价款包含硬件、软件及服务采购的所有费用，包括但不限于硬件费用、软件费用、集成服务费用、维保服务费用及相关税费。合同履行过程中，乙方不得以任何形式向甲方收取其他额外费用，合

同履行过程中另行签订补充协议的条款不受此限。

（二） 款项支付

合同价款的支付条件及支付比例（本条款中款项的支付，均须以甲方收到乙方开具的**软、硬件设备全额增值税专用发票或服务费等额发票**为前提，否则付款期限将自动向后顺延）：

1. 《到货验收单》签署后 30 个工作日内，甲方向乙方支付合同总中硬件设备总价款的 40%，即_元（大写：人民币_元整）；

2. 《集成部署验收报告》签署后 30 个工作日内，甲方向乙方支付合同中硬件设备总价款的 25%，软件产品总价款的 25%，服务项的总价款 40%，即_元（大写：人民币_元整）。

3. 《试运行验收报告》签署后 30 个工作日内，甲方向乙方支付合同中硬件设备总价款的 25%，软件产品总价款的 40%，服务项的总价款 25%，即_元（大写：人民币_元整）。

4. 《技术转移验收报告》签署后 30 个工作日内，甲方向乙方支付合同中服务项的总价款 25%，即_元（大写：人民币_元整）。

5. 《终验报告》签署后 30 个工作日内，甲方向乙方支付合同中硬件设备总价款的 5%，软件产品总价款的 20%，服务项的总价款 5%，即_元（大写：人民币_元整）。

6. 第三年《服务验收单》签署后 30 个工作日内，甲方向乙方支付合同中支付除服务器外全部硬件设备剩余总价款，软件产品总价款的 15%，服务项的总价款 2%，即_元（大写：人民币_元整）。

7. 第五年《服务验收单》签署后 30 个工作日内，甲方向乙方支付合同中支付服务器设备剩余总价款，服务项的总价款 3%，即_元（大写：人民币_元整）。

8. 发票开具的要求: 可根据合同内容开具软件、硬件类发票及服务类发票, 以软件、硬件为内容开具的发票, 发票中软件的数量必须是整数且为产品费用全额发票; 维保服务开具服务类发票。

9. 如乙方违反本合同约定, 每次付款时甲方有权直接扣除相应违约金、赔偿金金额后, 再向乙方支付剩余款项。

(三) 乙方账户信息

账户名称: _____

开户银行: _____

账 号: _____

乙方账户如有变更, 应提前 15 个工作日以书面加盖公章形式将新的账户信息通知甲方。因乙方未及时通知而造成逾期付款, 甲方不承担任何责任。

第六条 网络安全审查条款

(一) 根据网络安全审查相关管理规定, 甲方有权将本合同约定的关于软件、硬件采购等相关内容向网络安全审查办公室或其委托机构申报网络安全审查, 乙方对此表示认可、支持与配合。除经甲方网络安全审查预判无需提交网络安全审查的情况外, 甲乙双方一致认可具体是否需要网络安全审查, 以网络安全审查办公室或其委托机构书面通知为准。

(二) 乙方认可甲方因网络安全审查需要, 向网络安全审查办公室或其委托机构提供有关本合同履行的相应材料, 不违反本合同保密条款约定义务。

(三) 甲乙双方明确, 本项目需经网络安全审查的, 本合同的生效以通过网络安全审查为前提。如网络安全审查过程中, 网络安全审

查办公室或其委托机构需要乙方提供进一步说明或证明材料的,乙方应予以配合。如网络安全审查结论为不通过的,甲方应向乙方反馈网络安全审查办公室或其委托机构出具的相关书面材料,本合同自始不产生法律效力,对于乙方有过错的,应当向甲方承担赔偿责任。

(四)如网络安全审查结论为通过、但附加条件的,乙方在收到甲方反馈的网络安全审查办公室或其委托机构出具的相关书面材料后,严格对照整改,并保证在终验前完成。甲乙双方一致同意将整改情况作为终验的一个环节,如乙方在约定时间内未完成整改或未按甲方要求完成整改的,视为终验不通过。本合同自始不产生法律效力,对于乙方有过错的,应当向甲方承担赔偿责任。

第七条 其他

附件:

1. 采购清单及服务要求
2. 到货验收单(格式)
3. 集成部署验收报告(格式)
4. 项目试运行验收报告(格式)
5. 技术转移验收报告(格式)
6. 终验报告(格式)
7. 服务验收单(格式)
8. 廉洁合作协议
9. 安全保密协议

（本页无正文，为《农信银资金清算中心农信云长沙区建设采购合同》
签字页）

说明：在签署本合同时，甲方就本合同的全部条款，包括但不限于本合同所约定的网络安全审查条款的概念、内容及其法律后果已向乙方进行了明确说明和解释，各方对合同的全部条款均无疑义，并对甲、乙双方有关权利义务和责任限制或免除条款的真实含义和法律后果有准确无误的理解。

甲方（盖章）：

乙方（盖章）：

法定代表人/授权代表：

法定代表人/授权代表：

年 月 日

年 月 日

附件 1

采购清单及服务要求

(一) 采购清单

1. 生产云采购清单

产品名称	项目	子项目	列表价	折扣率	单价	数量	金额	配置
硬件	服务器							
								
	网络 按配件分项报价，光模块 计入各设备不单独列出							
								
	安全							
								

								
	小计							
PaaS 软件	软件产品、license 费用 (软件产品和纳管设备 License 分开报价, 纳管 设备按类型分开报价)							
	小计							
云底座软件	软件产品、license 费用 (软件产品和纳管设备 License 分开报价, 纳管 设备按类型分开报价)							
								
								
	小计							
服务	 小计							
								
	集成实施服务	农信云长沙 区建设集成 实施(单位: 人/天)						

	技术支持服务费用 (3 年)	现场云运维 技术支持 (2*3 人年)						
								
	维保服务 (年) 按产品类型分项报价, 维 保价格不得高于采购价格 的 12%							
	小计							
合计								

（二）项目实施服务要求

乙方应与原厂充分协商，确保下列服务在约定时间内完成。

1. 实施准备要求

（1）合同签订后，乙方安排至少 10 名乙方技术人员或制造商原厂技术人员在甲方指定地点（北京或长沙市内），在 45 天内完成设计、规划、测试等文档编写、配置验证等各项准备工作。

（2）需要对数据中心进行现场场地踏勘时，乙方应安排相应技术人员进行现场踏勘工作。

（3）乙方须编写项目实施的各类文档，并生成设备配置，项目实施时乙方需至少提交下列文档并经过甲方评审，内容必须与所提供的产品相一致，并应尽可能详细。编写的技术文档类别应包括规划设计类、方案测试类、实施类、现场测试类、上线类及运维类。规划设计类文档应完整合理，涉及机房、布线等规划的协助甲方完成，涉及系统配置的根据甲方要求完成；实施类文档能够清晰准确指导实施，实现系统集成的标准化、规范化和一致性；测试类文档覆盖全面；上线及运维类文档步骤明确、有效、可操作。

（4）文档编写人员按需参与现场实施工作。

（5）在投标的工程实施方案中应说明可提供的技术文档清单。

（6）乙方应在每批次实施前向甲方交付当批所需的完整的技术文档。

（7）提交的技术文档是按需出版或装订的，其费用应包括在该品目的基本报价中。为了培训的目的，甲方有权复制这些资料而不受限制和另付费用。

（8）乙方须按照总体技术方案编写整个项目的各类技术文档。

编写的技术文档类别应包括规划类、设计类、实施类、测试类、上线类及运维类。规划和设计类文档应完整合理；实施类文档能够清晰准确指导实施，实现系统集成的标准化、规范化和一致性；测试类文档覆盖全面；上线及运维类文档步骤明确、有效、可操作。编写的技术文档不得少于下表，但不限于下表内容：

类别	文档名称
规划设计类	《总体设计方案》
	《设备部署图》
	《详细设计》
系统测试类	《测试方案》
	《测试报告》
实施类	《硬件安装手册》
	《配置手册》
上线类	《上线操作手册》
	《上线应急预案》
运维类	《运行维护手册》
	《备件管理方案》
	《上下电手册》
	《日常值守检查表》
运营类	《运营手册》
	《用户操作指南》

(9) 本项目线缆需符合下列要求：

序号	类型	要求
1	双绞线：	★类型：Cat6A 类 S/FTP 屏蔽电缆，可以抗各种电磁干扰。 ★芯线规格：26 AWG，4 线对。 ★采用十字骨架支撑结构。 ★标准：TIA/EIA-568-D 和 ISO/IEC 11801(2002) 和 EN 50173-1(2003)。 ★工作频率：≥ 500MHz 要求。
2	LC 接口 光纤	★双纤芯跳线，方便安装，易于维护； ★规格：1.8mm 的缆径； ★光纤类型：万兆多模，OM4，LC-LC； ★标准：ANSI/TIA-568.C； ★阻燃等级：光纤跳线须采用 OFNP 外皮； ★综合布线产品必须为优质品牌的标准化产品，不接受采用 OEM 方式的厂家产品； ★认证：多模光纤跳线须提供国际权威机构 UL 出具的认证文件。
3	MPO 接口	★光缆标准：TIA-492AAAD。

	光纤	★光缆规格: 50/125μm 室内多模光纤。 ★性能等级: OM4。 ★宏弯损耗: 最大宏弯 (100 圈, 75 mm 圆轴): 850 nm 和 1300 nm 下, 最大 0.50 dB。 ★100Gbps 传输距离: 不少于 150 米; ★光缆损耗: 850 nm (3.0 dB/km) \ 1300 nm (3.0 dB/km)。 ★回波损耗: -82.1 dB (1550 nm) \ -79.6 dB (1310 nm)。 ★插入损耗: 不大于 0.35dB。 ★插头标准: ANSI/TIA-568-C.3。 ★阻燃等级: 光纤跳线须采用 OFNP 外皮。
--	----	--

2. 设备到货要求

(1) 在合同生效后 40 个工作日内设备到达甲方指定地点。

(2) 乙方按照采购配置清单, 提供完好、全新、未使用过的硬件产品; 提供完整、正版的软件介质、软件文档及软件许可。

(3) 收到甲方发出的中标通知书后, 需及时联系甲方相关人员安排到货事宜, 按照甲方的时间要求完成到货。

(4) 供货前, 应按照甲方要求, 提前准备好相关供货材料和信息 (包括设备型号、规格、数量、序列号、包装、运输人员和车辆等), 配合甲方完成到货清点、入库、拆箱检查、到货验收, 以及资产扫描和入账等工作。

(5) 乙方负责开箱验货, 检查产品到货情况。

(6) 如果乙方履行合同时不能按承诺的时间地点到货, 将以合同违约处理, 并追究乙方的有关责任。

3. 集成部署要求

(1) 在设备到货 2 个月内完成设备的安装和平台系统调试。

(2) 系统集成的主要目标是按照详细设计要求完成云系统环境搭建并能够正常运行, 确保与之相联的全部设备正常联通、设备上安装的软件正常运行并满足甲方业务运行的要求, 完成运维、运营等各类系统的集成, 按照规划完成虚拟计算池、物理计算池、存储系统及

网络的纳管 and 对接，完成云平台的搭建工作。

(3) 乙方在安装设备之前，应先对甲方的相关人员进行现场培训，并在甲方相关技术人员的监督下进行安装、检测和排除故障。乙方不得在现场安装未经甲方批准的任何设备。

(4) 按照甲方要求的时间，乙方安排工程师到现场实施本项目所有软硬件的安装调试，包括但不限于场地勘测及确认、设备到位连线、加电自检、微码升级、存储初始化、主机连接、软件安装及客户化等工作。在安装调试过程中乙方的技术人员应说明设备的安装步骤和应该注意的事项并做详细记录。

(5) 根据采购配置清单及安装调试实施方案，配合甲方对设备部件种类及数量、硬件配置、软件配置、软件介质和许可进行验收；按照甲方的要求，对所购设备进行高可用和功能验收；按照甲方的要求，对所购软件进行功能验收；根据验收结果提供验收报告。

(6) 在安装、调试过程中造成的设备损坏，一切责任由乙方承担。

(7) 在项目实施全过程中，乙方对安装、调试及验收期间的工作进度、每天的主要工作、发现的问题及解决方法均须记录在工作日志上，工作日志每天的记录双方签字确认，双方各保留一份。

(8) 乙方必须响应下列安装、调试要求，包括但不限于以下几点：

①按标书要求对其产品的性能和配置进行安装、调测检查，并做出安装、调测报告。所供设备应在合同中所规定的地点和环境下，实现正常运行并达到合同要求的性能和产品技术规格中的性能。

②完成与配套设备（包括本项目采购的其它设备、其它项目近期

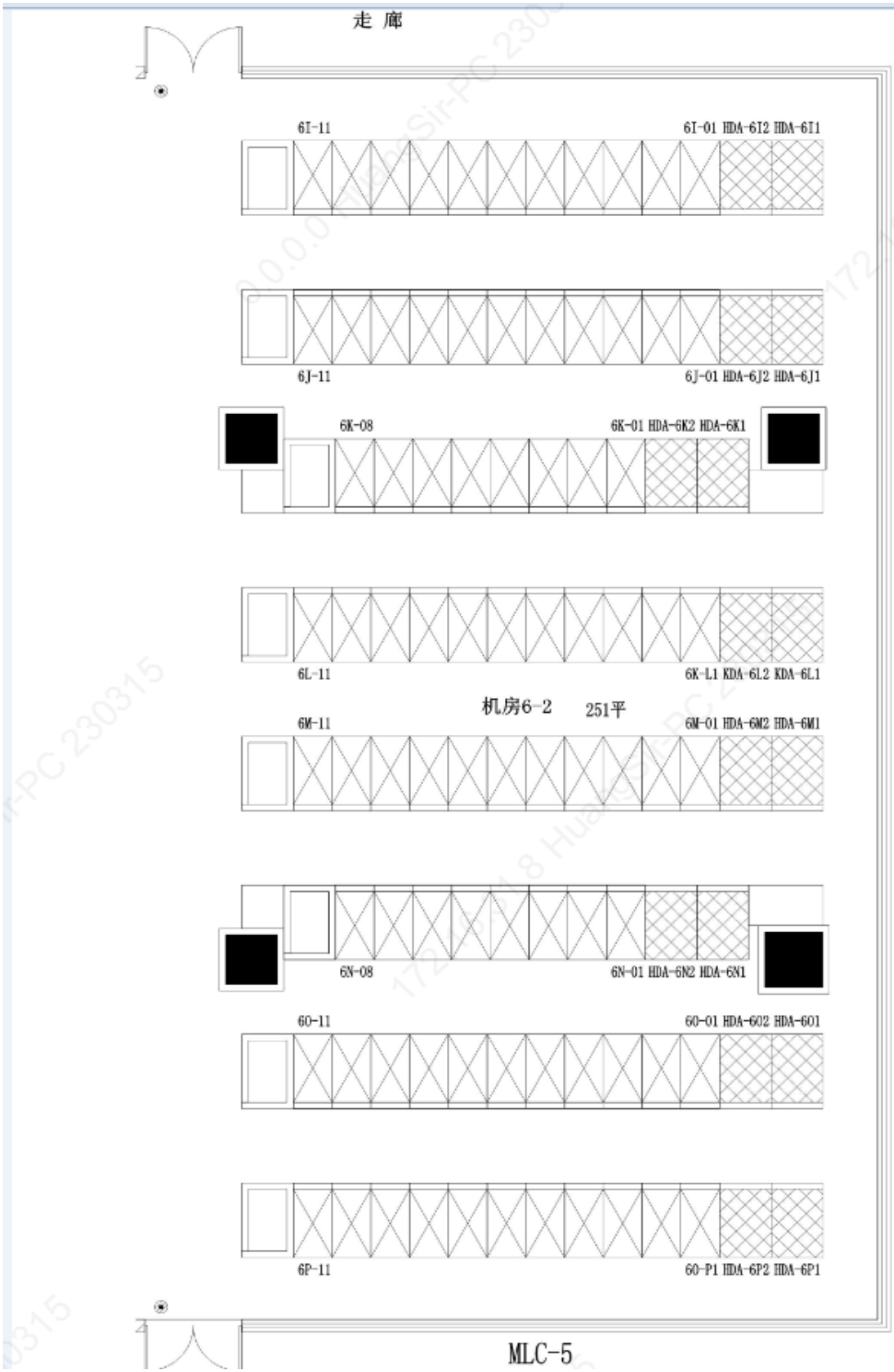
采购的设备和原有设备)的联合调试,构成整体的系统平台,进行相关的配置和系统优化调试,配合应用开发商或其他系统集成商进行应用系统安装、配置和系统优化调试等。

③当所供设备在安装、调测中出现性能指标或功能上不符合技术要求时,由乙方无附加条件解决。因缺少某些部件而导致达不到项目的设计指标,乙方须无偿提供这些部件,使项目满足设计要求。

④如安装、调测中出现不符合合同要求的质量问题时,用户保留索赔和退货的权利。

⑤完成与甲方已有服务器的适配及集成。

(9)为实现农信云农平台整体的高可行性和稳定性,保障网络的冗余性和健壮性,现结合信银机房实际情况(如下图),乙方根据产品的最佳设计实践,完成机房部署设计实施,包括但不限于以下几点:



①云平台云底座的部署遵照高可用原则，云底座和各功能组件在单列机柜电力或网络接入等故障仍保持业务可用。每组云底座服务器接入交换机不允许分拆跨机柜列部署。

②云平台网络核心交换机、互联网区域、广域网区域设备部署在

6L01-04 和 6M01-04 机柜，核心交换机分别部署 6L01-02 和 6M01-02 机柜，互联网模块网络设备部署在 6L03、6M03，局域网模块网络设备部署在 6L04、6M04，防止单列电力出现故障时整体云平台不可用。

③服务器网络接入 Leaf 交换机采用 TOR 或 EOR 部署模式（现机房机柜已具备 EDA-HDA 综合布线）。Leaf 交换机需分布在同列不同机柜，要求具备高可用原则，服务器接入采用端口聚合，物理线缆需接入不同物理交换机。服务器不允许跨列接入 Leaf 交换机。

④HDA（网络列头柜）可用空间 20U，配备 AB 双路电源，单路额定功率 3.5KW，其中单路配备国标 16A*6 个，国标 10A*8 个，C13/14*6 个。

⑤服务器机柜可用空间 46U，配备 AB 双路电源，单路额定功率 3.5KW，其中单路配备 C19/20*6 个，C13/14*14 个。

⑥计算节点、存储集群等需在满足单列机柜电源故障不影响整体云平台业务连续性要求下，自行设计物理部署。

(10)乙方保证其提供的设备中所有预装和为本项目安装的软件为具有合法版权或使用权的正版软件且无质量瑕疵，且为该产品的当前最新版本或最适合用户的版本，软件授权应无时间限制。

(11)设备安装和系统调试工作因甲方因素超出工作时间，不另行收费。

(12)项目实施过程中，如出现技术障碍、运行故障等问题，乙方有义务和责任组织、协调相关各方对问题进行快速解决。

4. 验证测试要求

(1)乙方安排技术人员和具备高级技术认证的原厂技术人员在完成系统集成一周后启动验证测试工作，并在 2 个月内完成云系统的

验证测试工作。

(2) 由乙方、原厂商和甲方（必要时由第四方参加）共同组成验证测试小组，由原厂商（必要时由第三方）提供测试方案和测试数据，经甲方确认后进行验证测试，测试内容包括但不限于软件平台功能测试、软硬件平台兼容性测试、性能测试、高可用测试、管理性测试等。

(3) 乙方应按照验证测试方案进行验证测试工作，提交测试报告，并经甲方审核。

(4) 对于需要进行完善、整改的问题，应评估问题影响，制定整改计划，并经甲方审核。

(5) 对于影响不大，不能及时完成整改的问题，经甲方同意后，可以作为遗留问题在系统后按计划进行整改。

(6) 测试结果如与验证测试小组确定的性能不符或测试结果不能确认，乙方及原厂商应在 5 个工作日内调整配置直至重新测试合格，如果测试不通过，甲方有权停止验证测试和拒验收该系统，且由乙方承担相应责任。

5. 试点应用部署要求

(1) 乙方安排不少于 5 名技术人员和具备高级技术认证的原厂技术人员在完成系统集成后 2 个月内协助甲方完成试点应用的部署工作。

(2) 乙方应提供应用迁移上云的标准解决方案及操作手册，并协助甲方制定试点应用上云部署方案及测试方案，并经甲方审核。

(3) 初步计划试点上云应用数量不大于 3 个。

(4) 乙方应协助甲方按照应用上云测试方案进行测试工作，提

交测试报告，并经甲方审核。

6. 系统上线要求

(1) 完成试点应用部署后 4 个月内，开展系统上线运行工作。
甲方有权结合自身情况调整系统上线时间，但应提前书面通知乙方。

(2) 云上线时乙方应提供技术人员及相关产品的原厂技术人员共同在上线地点进行现场技术保障，现场技术保障人员总人数不少于 10 人。乙方技术人员应具备三年以上工作经验并为本项目主要成员，可熟练配置投标系统及设备，参与至少一个以上和本项目同等规模的实施工作。原厂技术人员需具备 5 年以上工作经验，有较强的排除错误的能力，参与至少 3 个以上和本项目同等规模的实施工作。

(3) 上线期间，若发生由于乙方派遣的技术人员的技术能力或集成的系统导致的应用系统业务中断，乙方负责承担一切相关责任。

(4) 乙方须提供切实可行、操作高效、验证充分的系统上线方案，要求如下：

① 上线方案应包含上线思路、上线步骤、验证方案、流程控制以及应急回退等内容。

② 上线工作应尽可能减小对现有业务系统影响。

③ 如规定时间内遇到问题无法解决，应制定相应的应急预案和应急回退方案等。如是硬件问题，上线阶段乙方应确保备件可在 4 小时内到达用户现场。

7. 技术转移要求

7.1. 现场技术培训

(1) 乙方在设备上线之前，应对甲方的相关人员进行现场培训。

(2) 乙方应准备相关培训资料，并交付甲方。

(3) 培训内容包括但不限于设备的功能原理、配置方法和运行运维、技术支持服务, 以及软件架构、标准接口及基本开发方法等内容, 通过培训运维人员应基本掌握设备的功能原理和配置方法, 系统运维管理方式等内容, 并提供相应的工具, 使甲方相应的技术人员达到了如下的技术水平:

- a. 能够熟练使用和维护农信云平台;
- b. 能够独立进行接入交换机、计算节点、裸金属节点、容器 Node 节点、存储节点的扩容、缩容、更换等操作;
- c. 具有熟练查阅各种相关技术文件及维护手册的能力
- d. 掌握农信云平台的工作原理以及基于标准接口的开发方法

7.2. 技术资料移交

所有系统上线完成后, 乙方按甲方要求完成项目移交。项目移交工作要求如下, 包括但不限于以下内容:

(1) 乙方负责安排至少 3 名工程师参与文档交付任务。包括修订项目实施文档, 在甲方已有移交文档的模板上进行格式校对。

(2) 提交电子版 (U 盘) 文档, 移交 U 盘必须为高质量 U 盘。

7.3. 技术认证考试

乙方提供不少于 10 个云平台原厂最高等级的云计算培训、认证考试名额。

(三) 农信云技术支持与服务需求

1. 服务总体要求

序号	指标内容	要求	备注
1.	服务方要求	①在签署《终验报告》之日起, 由乙方及相关软硬件原厂商共同提供技术支持与服务, 其中云平台等主要软硬件必须由原厂商提供技术支持与服务	

		务。	
2.		②由乙方及相关原厂商组成技术支持服务团队，说明服务方式及服务内容。	
3.	服务人员要求	①服务方成立由项目经理、服务工程师等组成的专职服务项目组。	
4.		②指派有 3 年以上类似项目管理经验的人员担任项目经理，要求具有较强的组织协调能力、专业技术能力、项目管理能力、口头及文字表达清晰，负责本项目全程管理。	
5.		③质保期内，一线工程师需有 3 年以上相关技术经验，二线工程师需有 5 年以上相关技术经验，要求对工作应认真负责，具有良好的合作精神。	
6.		④服务人员需经甲方认可，未经甲方同意不能更换。如果甲方认为服务方指派的人员达不到甲方所要求，服务方应立即满足甲方提出的替换要求。	
7.		⑤服务方服务人员需身体健康，品行端正，无犯罪不良记录，无扰乱社会治安倾向。服务方对所派服务人员的各项要求负有审核管理义务。	
8.	服务期限要求	质量保证期为自经过甲方终验合格后次日起 36 个月。针对服务器、备份一体机，质量保证期为自经过甲方终验合格后次日起 60 个月。	
9.	测试开发环境支持	乙方须提供测试、开发等环境的软件授权，供甲方按需使用，且不再收取额外费用。本项目要求测试、开发等环境的软件功能、兼容性、安全性等在技术规格上生产云保持一致。	

2. 服务内容要求

2.1. 远程技术支持

服务方通过热线电话、电子邮件、传真等方式向甲方提供 7*24 小时远程技术支持，支持范围包括故障报修、问题提交、问题远程指导、分析和排除、产品功能介绍、配置、安装、调试、客户化以及使用中遇到的技术问题的咨询等，服务方需在规定时间内响应。

2.2. 现场运维技术支持

2.2.1. 驻场支持服务

驻场支持服务指乙方按要求安排云平台原厂商的技术人员，在甲方提供的办公区现场办公，提供运维支持服务。

序号	指标内容	要求	备注
1.	基本要求	提供 5×8 驻场支持服务，人员不少于 2 人，必须为资深技术人员（通过本项目云平台原厂云计算相关高级认证），工作年限不少于 3 年，服务期与质量保证期相同。	
2.	工作内容	为甲方的技术人员提供平台使用咨询服务	
3.		按甲方的流程，进行云平台的资源创建、交付	
4.		云平台的日常监控、预警、优化、故障处置服务	
5.		协助甲方进行云平台的升级、扩容等变更操作	
6.		甲方安排的其他技术工作	
7.	考核要求	1. 遵守甲方的办公管理、运维管理等制度； 2. 如提供的驻场服务人员的表现不符合项目要求，乙方项目经理需无条件在甲方提出换人要求之日起，5 个工作日内完成更换。若更换后仍不满足要求，乙方项目经理 5×8 在现场跟进，3 个工作日仍然没有明显改进，乙方项目经理的上级领导 5×8 在现场监督改进，依次类推，直到大中华	

		服务总经理（或同级别经理）5×8 在现场监督，直到完全改进。	
--	--	--------------------------------	--

2.2.2. 现场支持服务

现场支持服务指乙方提供的驻场服务以外，云平台原厂提供的各类需在甲方现场进行的支持服务。

序号	指标内容	要求	备注
1	现场支持服务	提供 7×24×4（每周 7 天，每天 24 小时，4 小时到现场）现场服务，接到支持需求必须在 30 分钟内做出回应；由于乙方或原厂商原因造成的各种软件（含集成）故障（不论涉及硬件或软件是甲方通过本次直接购置、赠送还是随机附带方式获得），均应在 4 小时内修复，如确实出现异常情况，在上述 4 小时内必须完成业务系统的恢复，提供硬件和软件环境准备，恢复生产；应提供紧急事件的快速处理服务系统，对于影响生产的紧急事件，必须在 2 小时内恢复系统。	
8.		如提供的项目服务人员态度与能力不符合项目要求，甲方提出改进要求，3 个工作日内没有明显改进，乙方项目经理 5×8 在现场监督改进，3 个工作日仍然没有明显改进，乙方项目经理的上级领导 5×8 在现场监督改进，依次类推，直到大中华服务总经理（或同级别经理）5×8 在现场监督，直到完全改进。	
9.		无附加条件提供本次采购软件产品、文档更新服务，包括：磁带、磁盘、电子邮件、U 盘等，安装或运行最新软件修订版时，	

	提供相应的技术支持和说明。如对软件有新的改进、增加新的功能或者为适应最新标准所形成的最新版本，均应及时通知并无附加条件提供介质。	
10.	提供特殊时段（国庆节、年终、重大活动、重要应用测试、投产、切换演练），以及产品安装、系统变更和迁移、系统升级等的现场支持服务。	
11.	每次现场服务后均须向甲方提交《技术服务工作报告》，对未完全解决的问题，服务工程师须至少每周与甲方工程师联系，跟踪问题，分析协商处理方案，直至问题解决。	
12.	每季度进行设备定期现场巡检，检查产品运行状况，解决运行过程中遇到的问题，分析运行记录和系统日志，提出系统管理改进建议。在每次服务完毕后5个工作日内提交服务报告，并且每年提交一次年度服务总结报告。	
13.	在甲方使用主流品牌的硬件、软件产品出现兼容性问题时，需积极配合，与有关硬件、软件厂商和甲方接洽，及时定位问题原因、寻求解决方案。若为本次采购软件原因，应及时解决。	
14.	提供各种突发事件的应急策略。	
15.	提供其他与产品相关联的服务，如产品过期EOL(End of life)，需至少提前两年通知客户。	

2.3.疑难复杂问题解决

服务方需保持 7*24 联系畅通，及时响应解决突发紧急问题；根据需要，及时到达现场进行故障恢复、问题诊断或维修，以尽快恢复设备系统可用状态。对未明确原因的故障问题和关联产品问题协助进行排查，并给出合理意见和建议。

2.4.备件保障服务（仅适用于硬件产品）

服务方备件库应满足本项目 100%的备件覆盖率（即备件库中备有维护清单中所有设备的所有备件），保证备件的品质和可用性，按服务级别提供备件保障服务，每季度主动通报一次备件情况。

针对服务器，维保覆盖整机配件。项目设备中所有故障硬盘不返厂。

2.5.应急保障服务

针对维保产品提供应急保障方案，结合应用系统需要，提供配套应急保障方案（包括应急措施和切换流程等），根据需要进行实际演练，相关应急方案需满足甲方管理流程和相关规范要求。根据需要，提供应急演练支持（包括必要的现场支持），根据甲方各环境实际运行地点，提供对应级别支持，支持地点包括长沙、北京两地三中心所在地。

2.6.预防性维护

服务方根据甲方要求，定期对设备、软件进行巡检和预防性维护，提交巡检记录，并对巡检中发现的问题给予及时修复。

2.7.产品版本信息发布和升级支持

产品版本信息包括硬件微码、软件 PTF 和新版本，以及 EOS 等所有涉及版本变化的信息。服务方需于版本信息发布后 90 天内正式通

知甲方,且产品 EOS 信息发布时间不得晚于 EOS 日期前一年。对于新发布的版本信息,服务商需提供相关介质和安装使用说明,包括但不限于新功能、所解决的问题、相关环境要求、安装方法等。服务期内甲方享有对所购买产品合法升级的权力,服务方需根据甲方需要,对升级工作提供技术支持,包括结合甲方实际使用对新版本进行评估并给出建议,配合升级和回退方案拟定、测试演练和投产支持等。同时甲方有需求对已上线系统进行配置变更时,需提供技术支持和保障服务。

2.8.移机、扩容技术支持服务

根据甲方需要,服务方为甲方提供设备系统移机技术支持服务。

如对设备进行扩容,服务方应根据甲方需要,提供技术支持,包括调试、参数定义、逻辑卷划分、数据迁移、相关功能软件工具安装、远程备灾方案的实施和调试等。

2.9.重要时段保障服务

根据甲方需要,在特殊时段(如重要会议、黄金周长假、年终决算、重大投产变更等甲方认定的特殊时段)提供 7*24 小时现场值守支持服务,以及二线 7*24 小时响应服务。并根据甲方需求,提供现场备件。

2.10. 开源软件版本维护服务

在服务期内,若该服务所涉及的开源软件发生升级情况,应提供配套的版本升级维护服务,包括开源软件升级版本的安装服务,新版本的培训,协助完成软件配置、升级测试工作等。升级的版本包括但不限于软件的小版本、大版本、跨代版本以及基本功能不变但已更换名称的软件,并按甲方要求的方式提供相应介质。升级的版本相对于

已使用的版本，要能提供平滑升级包。

2.11. 性能调优

在服务期内，对基础设施云涉及的云平台整体或组件发生性能下降时，需提供性能分析报告、性能调优方案，并协助甲方完成性能调优操作，出具性能调优报告。

2.12. 系统迁移

在服务期内，对应用系统由外部迁移至云内时，提供系统迁移改造技术支持、迁移方案和迁移计划，并协助甲方完成数据迁移及相关验证工作。

2.13. 容灾演练支持

在服务期内，对甲方统一容灾演练或单独针对云平台的容灾演练，提供云平台侧技术支持工作，并在演练结束后提供云容灾演练结果报告。

2.14. 巡检和健康检查

在服务期内根据甲方需要，提供巡检和健康检查服务，提供季度生产现场巡检制度并预先提供巡检计划，提供季度系统健康检查服务并在维护和服务之后提供相关书面报告。

2.15. 文档维护

在服务期内，根据运行维护和运营需要，对各种工程实施相关技术文档、运维运行规范指南、基础设施云运营规范、常见问题处理指南、厂商支持体系和流程指南等提供持续文档完善工作，并及时交付给甲方相关部门。

2.16. 服务标准与质量要求

2.16.1. 故障恢复要求

事件级别定义如下:

一级: 属于普通问题; 其具体现象为: 设备系统技术功能、安装或配置等事前测试和准备, 或其他显然不影响业务的预约服务。

二级: 属于较严重问题; 其具体现象为: 设备系统能继续运行且性能不受影响, 但出现报错, 存在较大安全隐患。

三级: 属于严重问题; 其具体现象为: 设备系统部分部件或功能失效、性能下降但不影响正常业务运作。

四级: 属于紧急问题; 其具体现象为: 设备系统故障导致系统停止运行、数据丢失等。

服务质量基本要求如下:

故障级别	响应时限	人员到场时限	备件到场时限 (仅限有备件服务的项目)	故障恢复时限
4 级	立即	1 小时	重要备件: 4 小时 一般备件: 24 小时	联机故障平均恢复时间不超过 20 分钟 批量中断平均恢复时间不超过 40 分钟 所有故障最长恢复时间不超过 2 小时
3 级		1 小时		
2 级		2 小时		
1 级		约定时间		4 小时之内

说明 1: 重要备件指某类备件的硬件故障导致相关设备宕机 (影响生产) 的备件; 一般备件指某类备件的硬件故障不影响生产。

说明 2: 故障恢复时间以服务方工程师被允许进行维护开始计时, 到设备系统恢复服务为止。

2.16.2. 可用性指标

完成两地三中心建设后, 整个云平台系统年可用性 $\geq 99.99\%$, 即系统故障或问题影响生产的时间, 年度内不超过 52.6 分钟。其计算公式为:

$$\text{年可用性} = \left(1 - \frac{T_{\text{down}}}{60 \times 24 \times \text{Year}}\right) \times 100\%$$

T_{down} : 影响生产的时间, 单位为分钟。

注: 年可用时间按 60 分钟*24 小时*365 天计算, 取值为万分位。

2.16.3. 问题解决率

故障发生后 24 小时内, 服务方应提交初步问题分析报告, 问题分析定位后提交最终分析报告, 报告需包括问题描述、分析情况、原因定位、可行的解决方案等内容, 提出的解决建议应具有合理性和可实施性。分析报告以甲方认可视为提交。

问题解决率: 2 日内不低于 60%, 5 日内 100% (故障发生后每 24 小时为 1 日), 双方另有约定的除外。

(四) 农信云扩容建设要求

//根据中标投标文件承诺情况补充。

(五) 其他要求

招标文件、乙方投标文件及澄清文件均作为本合同的组成部分, 本合同未列出, 但乙方在其投标文件中承诺提供的产品及服务, 乙方应按照投标文件承诺履约, 乙方未按期投标文件提供相应产品及服务的视同合同违约, 承担相应违约责任。

附件 2

到货验收单（格式）

合同名称: 农信银资金清算中心XXX合同

合同编号: _____

经验证，以下设备、软件 (符合/不符合) 采购需求:

序号	原厂 (品牌)	产品名称	型号 (版本)	序列号	详细配置 (用户数)	数量	是否包装完好
1							是 ☐ 否 ☐
2							是 ☐ 否 ☐
3							是 ☐ 否 ☐

采购管理部门经办人: 采购管理部门负责人: 实物管理部门经办人: 供货商经办人: 日期:

注：此单一式三份，采购管理部门、实物管理部门和供货商各一份。

附件 3

集成部署验收报告（格式）

合同名称	农信银资金清算中心 XXXXXX 软件及服务采购合同 (编号: _____)
验收标准	乙方遵照附件 1 采购清单及服务要求第(二)部分项目实施服务要求第 5 项集成部署要求、第 6 项验证测试要求,在设备到货 2 个月内完成生产云设备的安装和平台系统调试,按照要求完成对甲方已有设备的适配及集成,在 2 个月内完成并通过验证测试视为验收合格,三方人员签署集成部署验收报告。
验收结论	
甲方签字	日期:
乙方签字	日期:
原厂商	日期:

备注	
----	--

注： 1. 此单一式三份，甲方、乙方及原厂商各一份。
2. 采购管理部门、使用部门必须有 2 名专业技术人员参与验收。

附件 4

项目试运行验收报告（格式）

合同名称	农信银资金清算中心 XXXXXX 软件及服务采购合同 (编号: _____)
验收标准	农信云生产云的业务功能、技术指标满足要求,且项目试运行 3 个月 after 无严重等级 3 级以上(含 3 级)缺陷发生。 缺陷分类说明如下: 严重等级 1: 系统无法运行。即在日常必需的功能测试和运行中,系统无法正常完成工作或无法产生正常结果。 严重等级 2: 系统存在功能、性能缺陷。但系统能够运行,在某些特定环境下,无法达到性能或功能要求。 严重等级 3: 系统存在功能、性能缺陷。但在生产环境中,可采用其它方式替代或弥补,并达到同样效果。 严重等级 4: 微小缺陷。系统功能、性能符合要求,可以服务于用户,有局部需要改动或润色
验收结论	
甲方签字	日期:
乙方签字	

	日期:
原厂商	日期:
备注	

注： 1. 此单一式三份，甲方、乙方及原厂商各一份。
2. 采购管理部门、使用部门必须有 2 名专业技术人员参与验收。

附件 5

技术转移验收报告（格式）

合同名称	农信银资金清算中心 XXXXXX 软件及服务采购合同 (编号: _____)
验收标准	乙方按合同要求提供了完备的技术文档, 提供了相应的培训及考试机会, 提供了必要的工具并使甲方相应的技术人员达到了如下的技术水平: a. 能够熟练使用和维护农信云平台: b. 能够独立进行接入交换机、计算节点、裸金属节点、容器 Node 节点、存储节点的扩容、缩容、更换等操作; c. 具有熟练查阅各种相关技术文件及维护手册的能力 d. 掌握农信云平台的工作原理以及基于标准接口的开发方法。
验收结论	
甲方签字	日期:
乙方签字	

	日期:
原厂商	日期:
备注	

注： 1. 此单一式三份，甲方、乙方及原厂商各一份。

附件 6

终验报告（格式）

合同名称	农信银资金清算中心 XXXXXX 软件及服务采购合同 (编号: _____)
验收标准	满足以下标准,并自项目最终验收需求满足后 7 个日历日内,提供《原厂维保服务承诺函》,视为验收通过: a. 项目期间产生的所有问题均得以有效解决。 b. 终验前 6 个月无严重等级 3 级以上(含 3 级)缺陷发生。 c. 乙方提供了项目软硬件原厂提供的维保服务承诺函。 缺陷分类说明如下: 严重等级 1: 系统无法运行。即在日常必需的功能测试和运行中,系统无法正常完成工作或无法产生正常结果。 严重等级 2: 系统存在功能、性能缺陷。但系统能够运行,在某些特定环境下,无法达到性能或功能要求。 严重等级 3: 系统存在功能、性能缺陷。但在生产环境中,可采用其它方式替代或弥补,并达到同样效果。 严重等级 4: 微小缺陷。系统功能、性能符合要求,可以服务于用户,有局部需要改动或润色。

	c. 各阶段所涉及的所有安装文件、源程序、构建、配置文件、相关技术文档、培训资料等均已提供，并书面保证移交的源程序编译后和线上运行的程序完全一致。 d. 具备权威部门出具的符合相关标准规范与认证的证明或报告（安全合规认证相关要求），优化点验收测试报告。
验收结论	
采购管理部门意见	经办人 1 日期 经办人 2
使用部门意见	经办人 1 日期 经办人 2
供货商	日期:
原厂商	
备注	

注： 1. 此单一式四份，采购管理部门、使用部门、供货商及原厂商各一份。
2. 采购管理部门、使用部门必须有 2 名专业技术人员参与验收。

附件 7

服务验收单（格式）

合同名称	农信银资金清算中心 XXXXXX 软件及服务采购合同（编号：_____）
服务期数	
验收标准	完成_____, 符合《采购清单及服务要求》《原厂维保服务承诺函》与本合同约定。
确认结论	
甲方签字	日期
乙方签字	日期
备注	

注： 1. 此单一式四份，甲方、乙方各二份。
2. 采购管理部门、使用部门必须有 2 名专业技术人员参与验收。

附件 8

廉洁合作协议

甲方（采购方全称）：农信银资金清算中心有限责任公司

乙方（供应方全称）：_____

甲乙双方签署了《农信银资金清算中心 XXX 软件及服务采购合同》合同（合同编号：_____；以下简称主合同），为营造健康商业环境和建立正常商业合作关系，甲乙双方经友好协商签订本协议，并作为双方共同遵守的廉洁合作行为准则执行。

一、 甲方责任

1. 甲方有责任向乙方告知甲方廉洁合作相关规定。
2. 甲方严禁甲方人员在业务合作过程出现下列行为（包括但不限于）：

（1）商业贿赂：甲方人员收受或向乙方及乙方人员主动索要各种形式的回扣、礼品、购物卡、预付卡、会员卡、提货券、电子红包、股权、土特产、金融产品、现金、实物、证券、消费卡（券）等有价物品，或接受并参与乙方及乙方人员提供的旅游、宴请、住宿、健身、文化娱乐等活动安排及馈赠，出入私人会所及其他可能影响职务行为公正履行的活动；

（2）行贿及其他：甲方人员要求乙方或乙方人员配合或协助进行各种形式的行贿（包括但不限于提供回扣、礼品、购物卡、预付卡、会员卡、提货券、电子红包、股权、土特产、金融产品、现金、实物、证券、消费卡（券）等有价物品）、不当利益输送在内的各类违法活

动；甲方人员要求乙方或乙方人员配合或协助进行装修住房、婚丧嫁娶、配偶子女的工作安排及出国（境）、旅游等可能导致利益冲突的行为；

(3) 利益冲突：甲方人员未经甲方批准，以本人或其亲属名义于乙方或其关联单位处直接或变相参股（员工激励持股、公开市场股票投资除外）、任职、兼职或获取其它利益；

(4) 串标围标：在甲方业务范围内，甲方人员授意乙方配合进行串标或围标等违规违法行为；

(5) 资金往来：甲方人员或其亲属以任何理由向乙方（含关联单位）或乙方人员借贷资金。

3. 对于乙方举报甲方人员违反廉洁合作禁止项的情况，甲方负有保密义务，并应及时组织调查，将最终调查结果反馈乙方。

二、 乙方责任

1. 乙方应保证乙方人员了解本协议中关于廉洁合作禁止项的相关规定，并遵照执行；如乙方人员违反相关规定，视为乙方违约。

2. 乙方承诺并保证，与甲方开展合作时不存在（且在与甲方开展合作的过程中不得有）甲方在职员工或离职员工直接或变相持股或控制乙方公司或其关联单位的情形，但员工激励持股、公开市场股票投资不在前述限制。

3. 乙方及乙方人员应严格遵守以下廉洁合作约定（包括但不限于）：

(1) 严禁商业贿赂：乙方及乙方人员不得向甲方人员提供任何形式的回扣、礼品、购物卡、预付卡、会员卡、提货券、电子红包、股权、

土特产、金融产品、现金、实物、证券、消费卡（券）等有价物品或旅游、高档宴请等其他可能影响职务行为公正履行的活动；

（2）严禁行贿及其他违法：乙方及乙方人员不得接受甲方人员要求配合或协助进行各种形式的行贿（包括但不限于提供回扣、礼品、购物卡、预付卡、会员卡、提货券、电子红包、股权、土特产、金融产品、现金、实物、证券、消费卡（券）等有价物品）、不当利益输送在内违法行为的请求；乙方及乙方人员不得为甲方人员个人装修住房、婚丧嫁娶、配偶子女的工作安排及出国（境）、旅游等提供方便以及其他可能导致利益冲突的行为等；

（3）利益冲突及其他披露：若在与甲方合作时及过程中，出现以下任何情形之一的，须在相关情形发生后 10 天内，以书面方式向甲方完整、如实披露相关信息：

- ① 甲方在职员工或其亲属于乙方公司或其关联单位处直接或变相持股（注：员工激励持股、公开市场股票投资不属于乙方协议披露义务）、控制、任职、兼职、借贷资金或获取其它利益的情况；
- ② 甲方离职员工或其亲属于乙方公司或其关联单位处直接或变相持股（注：员工激励持股、公开市场股票投资不属于乙方协议披露义务）、控制、任职或兼职的情况；
- ③ 乙方法定代表人、股东、实际业务控制人、对接人两年内以其他公司名义参与甲方业务合作的情况。

（4）严禁串标围标：在甲方业务范围内，乙方及乙方人员应拒绝甲方员工授意配合进行串标或围标等违法违规操作的请求；乙方及乙方

员工不得串谋其他单位,在甲方业务中进行串标或围标等违规违法操作;

(5) 资金往来: 乙方(含关联单位)或乙方人员不得在任何情况下向甲方人员或其亲属提供无息、低息借款或高息出借资金或与甲方人员或其亲属有其他不正当的资金往来。

4. 乙方应保证向甲方提供的文件、资料、数据、陈述和口头陈述等信息的合法性、真实性、准确性和完整性;

5. 乙方有责任接受甲方对乙方在合作期间廉洁合作协议执行情况的监督,并对甲方相关调查工作主动配合;

6. 乙方有责任就甲方人员或甲方业务合作单位人员营私舞弊、弄虚作假等违反职业道德准则的行为及时向甲方举报,甲方受理举报的联系方式为:

举报电话: 010-57969734

举报邮箱: jw@nongxinyin.com

三、 违约责任

1. 如乙方或其人员违反本协议第二条乙方责任中第 2、3 款约定的,一经查实(包括但不限于被甲方核实属实,或者被司法机关或第三人核实属实的),乙方除应向甲方赔偿由此给甲方造成的损失并对乙方相关责任人员进行追责外,还承诺向甲方支付最高相当于主合同总价款 10%的违约金(具体比例由甲方视情况单方决定,乙方无条件接受);甲方将公开通报处理,并有权解除主合同且无需承担任何违约责任。如因乙方违反廉洁合作禁止项相关规定原因导致甲方解除主合同的,

甲方有权要求乙方按主合同与本协议约定承担违约责任,且甲方有权拒绝其后与乙方或其关联单位开展合作,乙方承诺不会就此提出异议,并按甲方要求承担违约责任。

2. 如乙方拒不配合甲方对乙方在合作期间内的廉洁合作监督及调查工作的,或者被证实存在隐瞒信息、提供虚假信息和伪证行为的,甲方有权视情节严重程度,对主合同的履行采取暂停支付合同款项、终止合作、追究经济损失、解除合同等措施,且无需承担任何违约责任。

3. 如乙方在合作期间内出现违反本协议约定的行为,甲方有权视情节严重程度,将乙方列入不诚信合作方名单,并在甲方内部、官方网站及公开媒体行公示。乙方承诺,甲方对公示产生的影响不承担任何责任。

四、 其他

1. 本协议是主合同的补充协议,与主合同具有同等法律效力。本协议未作约定的事项(包括但不限于争议解决方式),仍以主合同约定为准。本协议约定与主合同不一致的,以本协议为准。

2. 本协议经双方法定代表人/授权代表签名/盖章并加盖公章或合同专用章之日起生效。协议有效期与主合同一致。

甲方(盖章):

乙方(盖章):

法定代表人/授权代表:

法定代表人/授权代表:

签订日期: 年 月 日

附件 9

安全保密协议

甲方（采购方全称）：农信银资金清算中心有限责任公司

乙方（供应方全称）：_____

为保护甲方在商业和技术合作中涉及的商业秘密，维护双方的合法权益，依据国家有关法律法规和相关要求，根据甲乙双方签订的《农信银资金清算中心农信云长沙区建设采购合同》（合同编号：_____）（以下简称主合同），双方经协商一致达成以下安全保密协议。

第一条 保密信息

（一）乙方在洽谈或履行主合同过程中从甲方获得（无论在本协议生效之前或之后）的所有文档资料、软硬件和服务信息、与主合同项目相关的所有信息及在主合同项目进行过程中有关的一切中间或成果文档资料，包括但不限于以下内容：

1. 技术信息：业务需求书、操作手册、软件开发说明书、系统安装手册、部署手册、接口规范说明书、测试文档、培训文档、管理文档、源代码、各种安装程序、技术支持文档、数据、技术、方法和其他信息等；
2. 业务信息：业务人员、财务状况、经营策略、工作计划、资源消耗、通信流量等；
3. 安全信息：账号、口令、密钥、授权等用于网络、系统、进程

等进行访问的身份与权限数据,以及乙方按主合同约定履行工作职责所需要的重要、适当和必要信息。

上述信息无论是以书面、口头、电子或其他任何形式或载于何种载体,都具有保密性,仅用于主合同项目约定之用途。

(二) 主合同文本及附件内容,都具有保密性。

第二条 双方权利和义务

(一) 乙方必须严格遵守本协议,保证不向任何第三方透露任何保密信息。除为履行主合同外,未经甲方书面同意,乙方不得擅自留存、传输、使用、披露,不得以任何方式和形式将保密信息透露给第三方。

(二) 未经甲方书面同意,乙方不得将含有保密信息的任何资料以任何形式带出甲方指定工作场所,并禁止对任何信息进行复制和仿造。

(三) 当甲方以书面形式要求乙方交回所提供的保密信息时,乙方应立即交回所有书面及以其他形式存在的保密信息,包括保密信息的承载媒介及其全部复印件、复制件、影印件或摘要等。如果该保密信息属于不能归还的形式、或已经复制或转录到其他资料或载体中,则应予以永久性删除。未经甲方书面允许,乙方不得丢弃、删除、修改或处理任何含保密信息的书面的、有形或无形的资料及信息。

(四) 除非甲方明确书面授权,乙方不得认为甲方转让或授予其关于主合同项目任何信息的任何专利权、专利申请权、商标权、著作权、商业秘密或其他知识产权。

(五)乙方不得以甲方的保密信息为基础或数据来源进行衍生性研究和/或开发利用,包括但不限于不得对甲方提供的保密信息中的数据产品以及其数据进行解析、逆向工程、分解、反向编辑等;如果乙方从事任何上述衍生性研究和/或开发利用,除应按照本协议约定承担违约责任外,由衍生性研究和/或开发利用所产生的知识产权属于甲方所有。

(六)乙方对其员工的保密义务负责。乙方应保证其所有接触或可能接触保密信息的员工严格遵守本协议项下的保密义务,如因乙方员工的行为造成本协议项下的保密信息任何形式的泄露,乙方承担本协议项下的违约责任。

第三条 保密期限

保密义务的期限至保密信息正式向社会公开之日或甲方书面解除乙方本协议项下保密义务之日止。

主合同终止或提前解除的,不影响本协议效力。乙方仍需遵守本协议约定,履行其保密义务。

第四条 违约责任

(一)乙方有违反本协议的情形,无论故意与过失,应当立即向甲方报告,停止侵害,并在第一时间采取一切必要措施防止保密信息的扩散,尽最大可能消除影响。

(二)乙方违反本协议所约定的其在保密方面的义务,应按照主合同违约责任条款中保密违约条款处理。

第五条 争议解决

(一) 甲、乙双方因履行本协议所发生的一切争议, 按照主合同争议解决条款进行解决。

(二) 当产生任何争议及任何争议正在解决时, 除争议事项外, 双方应继续行使其剩余的相关权利, 履行其本协议项下的其他义务。

第六条 不弃权条款

(一) 甲方对任何上述权利或救济权的未行使或延迟行使都不代表其自动放弃, 任何单一或部分的权利或救济权的行使都不能阻碍其继续进一步行使权利或救济权; 但甲方向乙方书面明示放弃的除外。

(二) 未经其他方同意, 任何一方不得转让其在本协议项下的全部或任何部分权利。

第七条 其他

(一) 本协议自甲、乙双方法定代表人或授权代表签字/盖章, 加盖合同专用章/公章之日起生效。

(二) 本协议一式肆份, 甲、乙双方各执贰份, 具有同等法律效力。

甲方: 农信银资金清算中心有限责任公司

法定代表人/授权代表:

日期:

乙方:

法定代表人/授权代表:

日期:

第四章

投标文件格式

格式 1

开标一览表

投标人：

招标编号：

项目名称：

投标总价（人民币）

注：投标总价为投标货物在采购人指定地点交货并完成安装调试和正常运行（含售后质量保证及技术支持、培训、备件等所有伴随服务）的最终价格。

序号	投标产品	品牌及型号	备注
1			
2			
.....			

投标人认为需声明的情况

投标人（盖单位公章）：

格式 2

投 标 书

致：中国人民银行集中采购中心

根据贵方_____项目（招标编号：_____）招标采购货物及服务的投标邀请，授权代表_____（姓名、职务）经正式授权并代表投标人_____（投标人名称、地址）提交下列文件电子版本：

- （1）投标书；
- （2）法定代表人授权书；
- （3）投标分项报价表；
- （4）货物说明一览表；
- （5）采购需求及技术要求逐项应答表；
- （6）商务及合同条款逐项应答表；
- （7）项目实施人员情况表；
- （8）同类业务案例介绍；
- （9）售后服务与质量保证承诺；
- （10）投标人资格声明文件；
- （11）投标人资质证书及其他资质证明文件；
- （12）正版软件声明；
- （13）采购需求及技术要求中规定应提交的有关技术文件材料；
- （14）投标人关于投标文件纸质正本与投标文件电子版两者一致性的承诺书。
- （15）制造商授权书；
- （16）第一章《投标邀请》七 投标人资格要求的有关材料。

在此，授权代表声明如下：

1. 投标人已详细阅读并完全理解全部招标文件，包括澄清文件；并将按招标文件的规定履行合同责任和义务。

2. 本投标有效期为自开标之日起 90 日。

3. 投标人与采购人聘请的为此项目提供咨询服务的公司及任何附属机构均无关联。

4. 投标人同意按照采购人的要求提供与投标有关的一切数据或资料，并完全理解最低报价的投标人不一定中标的规定。

5. 与本投标有关的一切正式往来信函请寄：

地 址：_____ 邮 编：_____

电 话：_____ 传 真：_____

电子邮件地址：_____

格式 3

法定代表人授权书

本授权书声明：注册于（地址）的（公司名称）的（法人代表姓名、职务）代表本公司授权（被授权人的姓名、所在单位及职务、联系方式（包含电子邮件）、联系电话）为本公司的合法代理人，参加（项目名称）的投标，以本公司名义处理一切与之有关的事务，包括投标及中标后签订合同等有关事务。

本授权书于_____年___月___日签字生效，特此声明。

法定代表人签字（或人名章）_____

被授权人签字_____

投标人名称_____

（盖单位公章）

格式 4

投标分项报价表

投标人名称: _____ 招标编号: _____

本项目报价格式要求按照以下模板所列进行分项报价。

产品名称	项目	子项目	列表价	折扣率	单价	数量	金额	配置
硬件	服务器							
								
	网络 按配件分项报价，光模块计入各设备不单独列出							
								
	安全							
								
								
	小计							
PaaS 软件	软件产品、license 费用（软件产品和纳管设备 License 分开报价，纳管设备按类型分开报价）							
	小计							
云底座软件	软件产品、license 费用（软件产品和纳管设备 License 分开							
								

	报价, 纳管设备按类型分开报价)							
								
	小计							
服务	 小计							
								
	集成实施服务	农信云长沙区建设集成实施(单位: 人/天)						
	技术支持服务费用(3 年)	现场云运维技术支持(2*3 人年)						
								
	维保服务(年)按产品类型分项报价, 维保价格不得高于采购价格的12%							
	小计							
	合计							

服务器设备采用整机报价, 网络设备需细化至板卡、模块, 软件产品需详细列出各组件及其许可单位、限制条件(不

得具有限制招标人采购软硬件产品功能、性能发挥的隐性条件或许可)。维保服务要求单独报价,计入投标总价,且软件产品每年维保价格不得超过产品优惠后单价的 12%,同时各产品应按目录价及折扣率进行报价,合同总价应为各分项报价之和。扩容建设报表格式相同,报价要求参照前述章节相关要求。

注:1、本表中报出的各分项价格及总价应包括本招标文件要求的所有货物及服务的价格(除非本招标文件中明确规定由投标人另行报价)。

2、本招标文件要求报价而投标人在本表中未予报价的项目,将视作已包含在其他分项价格中。

格式 5

货物说明一览表

投标人名称: _____ 招标编号: _____

序号	货物的品名及型号	制造厂商	货物性能及配置	数量	单位	备注

注：各项货物详细技术性能应根据招标文件要求另页描述。

格式 6

采购需求及技术要求逐项应答表

投标人名称: _____ 招标编号: _____

序号	招标文件条目号	采购需求及技术要求	投标应答	偏 离说 明

注：针对本招标文件第五章逐条应答。

格式 7

商务及合同条款逐项应答表

投标人名称: _____

招标编号: _____

项目名称: _____

序号	招标文件条目号	招标文件的商务条款	投标文件的商务条款	偏离	说明
序号	招标文件条目号	招标文件的合同条款	投标文件的合同条款	偏离	说明

格式 8

项目实施人员情况表

姓名	性别	职称	最高学历	在本项目担当的任务
本人本项目计划时间	本人本项目计划内任务和目标			
本人以往业绩实施时间	以往业绩描述			

格式 9

同类业务案例介绍

案例名称和 合同额			
证明 材料	(附件目录, 附件应提供合同复印件等证明材料)		
项目简介及 实施情况	投标人单位 (盖单位公章)		
用户 名称		联系人	
用户 地址		电话	

注：1、每个案例填写一份表格。如业绩提供不实，将取消其投标资格。

格式 10

售后服务与质量保证承诺

项目名称:

项目编号:

序号	类别	售后服务与质量保证承诺	备注

格式 11

投标人资格声明文件

1、名称及概况:

(1) 投标人名称: _____

(2) 地址: _____

电话/传真号码: _____

(3) 成立和/或注册日期: _____

(4) 公司性质: _____

(5) 注册资本: _____

(6) 主要负责人: _____

(7) 职工人数: _____

(8) 近期资产负债情况 (到_____年__月__日止)

固定资产:

原值: _____

净值: _____

流动资金: _____

长期负债: _____

短期负债: _____

(9) 法定代表人姓名: _____

(10) 授权代表的姓名和职务: _____

(11) 上一年度的财务审计报告: _____

(12) 最近三年中的与本次招标项目类似的项目上的营业额: _____

项目名称	用 户	完成时间	项目合同总额
------	-----	------	--------

3、是否承诺近三年内，在经营活动中无重大违法记录: _____

4、是否具有良好的商业信誉和健全的财务会计制度: _____

5、是否具有履行合同所必需的设备和专业技术能力: _____

6、是否承诺投标文件电子版及纸质投标文件一致: _____

7、有关开户银行的名称和地址: _____

8、投标人认为需要声明的其他情况: _____

兹证明上述声明是真实、正确的，并提供了全部能够提供的资料和数据，

我们同意遵照贵方要求出示有关证明文件。

投标人名称: _____

授权代表姓名和职务_____

传 真_____

电 话_____

电子邮件_____

注册地址_____

开户银行_____

银行账号_____

税 号 或信用代码_____

格式 12

投标人资质证书及其他资质证明文件

应包括但不限于业务资质认证证书、代理资格证书、制造商授权及服务承诺、用户验收单或用户履约证明或其它可以证明其行业影响与品牌形象等证明材料复印件。

格式 13

正版软件声明

本公司针对本采购项目提供的任何软件均系正版软件，不会对第三方的知识产权构成侵犯。任何第三方如果提出侵权指控，由本公司与其交涉并承担由此引起的一切法律责任和费用，以及赔偿由此给采购人造成的一切损失。

特此声明。

供应商：_____（盖单位公章）

格式 14

采购需求及技术要求中规定应提交的有关技术文件材料

投标人应认真阅读本招标文件第五章“采购需求及技术要求”，并按照其规定自行拟制格式，完整提供有关产品技术说明文件、技术与服务的说明与证明材料等。

（盖单位公章）

格式 15

投标人关于投标文件纸质正本与投标文件电子版

两者一致性的承诺书

我公司系（公司名称）_____，承诺如下：

本公司针对_____（采购项目名称、项目编号）提供的投标文件纸质正本与投标文件电子版内容一致。因投标文件纸质正本与投标文件电子版内容不一致而导致的不利后果由本公司承担。

特此说明。

投标人：（公司名称）_____

（盖单位公章）

格式 16

制造商授权书

致：中国人民银行集中采购中心

作为设在_____（厂家地址）的制造_____（货物名称和/或描述）的_____（制造厂家名称）在此授权_____（投标公司名称和地址）用我厂制造的上述货物就_____采购项目的_____号招标邀请递交投标书并进行后继的合同谈判和签署合同。

根据合同条款规定，我们在此保证为上述公司就此次招标而提交的货物承担全部质量保证责任。

出具授权书的制造厂家名称：_____

单位公章：_____

格式 17

第一章《投标邀请》七 投标人资格要求的有关材料

投标人按第一章《投标邀请》七 投标人资格要求，提供相关材料。

第五章

采购需求及技术要求

一、采购需求

（一）项目概况

农信云建设的目标是基于公有云技术体系，使用国产软、硬件设备，完成两地三数据中心农信云架构的设计，功能覆盖 IaaS、PaaS、统一云管服务等主要模块，提供计算、存储、网络等基础资源和容器、数据库、安全组件等平台化服务，支持一体化运维与计量计费云能力，并实现部分业务试点上云验证。

本次农信云建设为长沙数据中心生产云落地建设。总体上分为 IaaS、PaaS、云管平台、监控平台、云安全服务等功能模块。支持统一管理，即逻辑上为“一朵云”，在不同的数据中心设置不同的 Region，支持一个管理界面同时管理多个数据中心的云平台。

（二）采购标的汇总表

1. 工作范围

完成农信云的建设，提供农信云建设所需服务器、网络设备、安全系统、云底座、IaaS、PaaS、云管、监控等产品及集成安装实施（含综合布线所需线缆、标签等）、应用上云、培训（云厂商最高级别认证培训及考试机会）、3 年维保（部分设备另行要求）等服务，并协助招标人通过网络安全等级保护三级、商用密码应用安全性评估三级认证（认证

费用招标人自理）。本项目的软、硬件产品均需通过网络安全审查。

1.1. 总则

本部分是招标人就本项目的硬件采购、软件产品授权、系统部署和技术支持服务采购向投标人发出的业务需求及技术要求。

本文所称“不少于”、“至少”、“不大于”等均包含本数；本文所称“支持”指具备相应能力；本文所称“实配”指实际提供的配置数目、能力等。

“★”代表最关键指标项，不满足该指标项将导致投标被拒绝，“#”代表重要指标项，不满足该指标项在招标评分表中会有扣分处理（扣分规则见招标评分表），其他代表一般指标项，投标人需进行应答，不涉及扣分处理。

投标人应根据本部分的要求，编写投标文件的技术部分，主要包括：

（1）技术方案：根据招标人提出的业务需求和建设目标，编写本项目建设的技术方案。内容包括但不限于技术指标、总体架构设计、云服务设计、高可用设计、安全设计、部署方案设计、运维和运营设计等。

（2）云能力说明书：根据招标人所提的技术方案，对建成的农信云进行说明，包括云服务能力、业务连续性能力、可用性能力、多云（同一云厂商）管理能力等。

(3) 项目实施方案：编写满足需求的实施方案，内容包括但不限于工程组织、项目团队、实施计划、现场测试、试点应用迁移、系统上线和技术培训等。

(4) 技术支持与服务方案：内容包括针对本项目的技术服务保障体系，服务期内因用户新需求而产生的开发服务，以及服务期内的技术支持服务等。

(5) 扩容建设方案：编写扩容建设方案，内容包括本次采购中各类软硬件设备在数量、授权、性能、应用场景的限制情况，在本次建设基础上可采取的扩容方案，扩容建设的产品报价情况等，包括本次招标询价但不实际配置的产品也应对其建设扩容方案、报价予以说明。

(6) 投标产品应用案例汇总：投标人应提供主要投标产品（包括云平台、各类 PaaS 组件产品）自 2018 年 1 月 1 日至投标截止日，具有云系统成功应用案例。

(7) 本项目所称原厂服务为：由 IaaS 和 PaaS 原厂商负责软硬件集成、维保等总体牵头协调工作。

(8) 1.2 节采购清单中分布式关系型数据库服务、数据库同步工具、容器服务、分布式缓存服务、DevOps 服务、微服务应用平台、API 网关项所要求的“含在云底座硬件中”，指运行上述 PaaS 产品的硬件需包含在云底座硬件中，相关硬件采购报价需包含在云底座硬件整体报价中，不得包含在云底座软件及 PaaS 软件的报价中。

(9) 投标人提供的数据库同步工具、容器服务、分布式缓存服务、DevOps 服务、微服务应用平台、API 网关 PaaS 产品需同时支持基于 X86 和 ARM 两种 CPU 架构的服务器；若支持两种 CPU 架构的上述产品为不同产品或版本，则需同时提供，且按照一套产品报价计费。

(10) 因投标人对需求理解不充分，导致投标产品数量不满足招标要求，投标人应无条件提供补救方案，使投标产品数量满足招标要求。

未按上述要求提供相应方案的，按投标无效处理。

1.2. ★采购清单

1.2.1. 详细清单

本项目的整体方案由投标人提供，整体的软件及硬件由投标人进行集成适配，因此下表硬件各类目数目及配置为投标时需达到的**最低量**（不含测试、开发环境许可），具体以投标人的方案为准。

序号	类别	名称	基本要求	数量	备注
1.	网络设备	核心交换机	单台设备实配 100G 线速端口 $\geq$ 72，单块板卡 100G 接口数量 $\geq$ 36, 100G 端口可以自适应成 40GE，模块满配，包含与接口数量相等 100G MPO 接口光模块，即光模块满配。	2 台	

2.		接入交换机 -100G 接入	交换容量 $\geq 6.4\text{Tbps}$, 包转发率 $\geq 2000\text{Mpps}$, ≥ 32 个 100 GE QSFP28 端口, 模块满配	0	云网关服务器接入使用, 如不使用投标人可采用本表所列其他品类交换机实现云网关接入。
3.		接入交换机-25G 接入	交换容量 $\geq 4.8\text{Tbps}$, 包转发率 $\geq 2000\text{Mpps}$, ≥ 6 个 40 QSFP+/100 QSFP28 端口, 模块满配, ≥ 48 个 10GE SFP+ / 25GE SFP28 端口, 模块满配。	12 台	仅用于计算节点接入, 其他节点接入交换机数量需投标人另行配置。
4.		接入交换机-10G 接入	交换容量 $\geq 4.8\text{Tbps}$, 包转发流 $\geq 2000\text{Mpps}$, 配置万兆以太网 SFP+端口 ≥ 48 , 模块满配 配置 100G QSFP28/40G QSFP 端口 ≥ 6 , 模块满配	6 台	仅用于计算节点接入, 其他节点接入交换机数量需投标人另行配置。
5.		接入交换机-1G 接入	交换容量 $\geq 570\text{Gbps}$, 包转发率 $\geq 140\text{Mpps}$, ≥ 48 个 10/100/1000Base-T 端口, 模块满配, ≥ 4 个 10GE SFP+ 端口, 模块满配	6 台	仅用于计算节点、网络管理接入, 其他节点接入交换机数量需投标人另行配置。
6.		边界路由器	支持多核 CPU, 实配控制引擎 ≥ 2 , ≥ 16 个 10GE SFP+ 端口, LC 接口单模模块满配, 需分布在不同板卡。	0	局域网边界使用, 根据投标人方案自行确定是否需要使用。

7.		硬件防火墙	独立硬件设备，而非通过添加功能模块实现。 吞吐量 $\geq 40\text{Gbps}$ 最大并发连接数 ≥ 1200 万； 每秒新建连接数 ≥ 30 万； ≥ 8 个 10 SFP+ 端口，模块满配； (以上配置的端口均为实际可用数量，要求全部同时支持，不得存在复用端口)	4 台	边界防御， 局域网边界 2 台，互联网 接入边界 2 台
8.		云内防火墙	软硬件方案皆可； 吞吐量 $\geq 80\text{Gbps}$ 最大并发连接数 ≥ 2500 万； 每秒新建连接数 ≥ 60 万； $\geq$ 具备 硬件防火墙同等功能和性能要求	1 套	云内防火墙 1 套，根据云 内 VPC 划分 安全隔离要 求，每个 VPC 边界使用独 立防火墙防 护，可采用硬 件或软件防 火墙实现

9.	硬件负载均衡	独立硬件设备，而非通过添加功能模块实现，具备服务器、链路、全局负载均衡功能，无需添加额外许可。 吞吐量≥40Gbps 4 层并发≥16M 4 层每秒新建≥500K 7 层每秒新建≥600K 设备同时支持服务器负载均衡、链路负载均衡、全局负载均衡，无需额外许可费用 每秒新建连接数： TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 ≥12000TPS。 TLS_RSA_WITH_AES256_GCM_SHA384 ≥12000TPS。 ECC-SM2-SM4-SM3 ≥8000TPS； ECDHE-SM2-SM4-SM3 ≥8000TPS； 吞吐量： TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 ≥5.6Gbps。 TLS_RSA_WITH_AES256_GCM_SHA384 ≥5.6Gbps。 SSL 最大并发连接数≥600000。 支持 SSL 加密，通过将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器。 支持商密 SSL 算法的单向和双向认证，至少包含以下算法：国密：SM2、SM3、SM4 算法，商密：RSA、SHA、ECDSA、ECDHE、SHA256、SHA384 算法。 "支持以下算法： TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384； TLS_RSA_WITH_AES256_GCM_SHA384； TLS_ECC_SM4_SM3。" 支持多级 CA 证书链 "支持各类标准证书的申请和导入，类型包含： RSA：1024-bit，2048-bit，4096-bit； ECDSA：256-bit、384-bit； SM2：256-bit。" 支持 SSL 卸载，将 SSL/TLS 协议流量解密为明文后再传输至服务器，以减轻服务器性能压力。 支持 SSL 加密，通过将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器。 实配支持基于自定义策略的 DNS 解析 DNS 每秒查询能力¹²⁷≥1500Kqps 具备国家密码管理局商用密码检测中心颁布的《商用密码产品认证证书》，满足 GM/T 0028 要求。	8 台	局域网边界 2 台，互联网接入区链路负载 2 台。局域网国密 SSL 卸载 2 台，互联网国密 SSL 卸载 2 台。
----	--------	--	-----	---

10.		云内负载均衡	软硬件方案皆可； 吞吐量 $\geq 80\text{Gbps}$ ，四层新建连接数四层新建能力 ≥ 50 万 CPS；七层新建能力 ≥ 60 万 RPS。 支持同一套负载均衡集群提供内网和外网两种负载均衡创建模式，支持轮训（RR），加权轮询（WRR）、源 IP 一致性哈希，最小连接数。	1 套	云内负载均衡 1 套，为云内提供负载均衡能力。根据云内 VPC 使用边界使用独立负载均衡，可采用软件或硬件方式实现。
11.	网 络 安 全 设备	网络入侵防护	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧入侵防护。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件
12.		Web 应用防火墙	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧 web 应用安全防护。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件
13.		网络未知威胁检测	1. 旁路部署，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧未知威胁检测。 3. 软硬件方案皆可，需支持将云内流量（含云边界和云内南北向流量）镜像至硬件平台（例：网络分路器）。	1 套	需实配所需的软硬件
14.		数据加密	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及用户侧数据加密。 3. 软硬件方案皆可。	1 套	需实配所需的软硬件

15.		密 钥 管 理 系 统	1. 系统采用高可用架构, 可采用 集群部署模式满足农信银云性能 要求。 2. 用于密钥管理。 3. 软硬件方案皆可。	1 套	需实配所需 的软硬件
16.	计 算 服 务 可	计 算 节 点 许 可	1. 运行虚拟化组件, 承载虚拟机。 需兼容招标人已采购的特定型号 的服务器; 2. 每个许可对应 1 台物理服务器, 单个许可不限制物理服务器的物 理 CPU 和物理核心数量。	100	招标人已经 规划详细用 途, 不得被投 标人挪用。若 其他采购项 依赖该许可, 投标人需额 外实配。
17.		裸 金 属 许 可	1. 将物理服务器作为资源。需兼 容招标人已采购的特定型号的服 务器; 2. 每个许可对应 1 台物理服务器, 单个许可不限制物理服务器的物 理 CPU 和物理核心数量。	100	招标人已经 规划详细用 途, 不得被投 标人挪用。若 其他采购项 依赖该许可, 投标人需额 外实配。
18.	存 储 资 源	云存储	详见 1.4.1.4	—	
19.	服 务 器	服务器	规格及数量要求见 1.2.2 及 1.4	115 台	
20.	备 份 对 接 设 备	备份设备	详见 1.4.1.8	1 套	

21.	PaaS 软 硬 件	分布式关 系型数据 库服务	1. 每套实配不少于 3 台物理服务器的许可； 2. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器） 3. 单台物理服务器物理 CPU 个数和核心总数不受许可限制；	6 套	1. 该产品运行的服务器需含在云底座硬件中，提供 18 台服务器，服务器配置同 1.4.1.1.4 数据库服务器规格 A； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
-----	------------------	---------------------	--	-----	--

22.	数据库同步工具	1. 实配不少于 50 条数据库同步链路（链路可重复使用，即源端和目标端可变化）的许可； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	1 套	1. 该产品运行的服务器需含在云底座硬件中，提供不少于 3 台服务器，服务器配置同 1.4.1.1.4 数据库服务器规格 A； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
-----	---------	---	-----	---

23.	容器服务	1. 实配不少于 10 台物理服务器的许可； 2. 或不限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）； 4. 单个 Node 节点的 CPU 个数和 CPU 核心总数不受许可限制；	1 套	1. 该产品管理端（基于 kubernetes 的 Master 端）、应用仓库、镜像仓库模块运行的服务器需含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）； 2. 运行 pod 的物理服务器不含在云底座硬件中，硬件不做报价，规格同 1.4.1.1.5 利旧服务器规格
-----	------	--	-----	--

24.		分布式缓存服务	1. 每套实配不小于 3 台物理服务器的许可; 2. 或不限制许可的产品; 3. 其他配套的管理类、支持类模块需支撑上述需求, 且自身部署模式具备高可用 (高可用集群各节点不可部署于同一物理服务器)	2 套	1. 该产品运行的服务器需含在云底座硬件中, 提供 6 台服务器, 服务器配置同 1.4.1.1.4 数据库服务器规格 A; 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中 (可运行在物理机或虚拟环境中, 规格同 1.4.1.1.1 计算型服务器规格 A)
25.		DevOps 服务	1. 实配不少于 200 个可重复使用的用户 (通过用户是否激活 DevOps 服务许可的授权实现重复使用) 许可, 或实配不少于 500 个不可重复使用的用户许可, 且支持 100 个用户同时在线, 同时不限制流水线数量; 2. 或不限制用户许可和流水线数量的产品	1 套	该产品运行的服务器不含在云底座硬件中, 硬件不做报价

26.		微服务应用平台	1. 实配不少于 300 个微服务处理节点的许可； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	1 套	1. 该产品用于运行应用系统(处理节点)的物理服务器不含在云底座硬件中，硬件不做报价，规格同 1.4.1.1.5 利旧服务器规格； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中(可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A)
-----	--	---------	---	-----	--

27.		API 网关	1. 实配 3 个集群的许可，每个集群需保证高可用，单集群 TPS 不少于 6000； 2. 或不限限制许可的产品； 3. 其他配套的管理类、支持类模块需支撑上述需求，且自身部署模式具备高可用（高可用集群各节点不可部署于同一物理服务器）	1 套	1. 该产品运行的服务器需含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）； 2. 其他配套的管理、支持类模块运行的服务器含在云底座硬件中（可运行在物理机或虚拟环境中，规格同 1.4.1.1.1 计算型服务器规格 A）
28.	云管软硬件	运维平台	含云管平台、监控平台。	1 套	含软硬件
29.		其他组件	云底座及其他组件	1 套	含软硬件
30.	技术支持与服务	技术支持与服务	3 年高级云技术支持服务，包括故障修复、预防性维护、应急保障、版本升级、性能调优、巡检、应用上云改造支持等服务。 6 人年现场技术支持服务 、培训服务等。	3 年	部分硬件服务年限另有要求
31.	云建设集成实施服务	线缆敷设	本项目实施所需的线缆、标签等辅材及综合布线服务。	1 次	完成基本要求所列工作。

1.2.2. 服务器数量要求

投标人应根据自身方案特点，配置国产物理服务器，在

满足 1.4 章节要求情况下，**实配**各类物理服务器**数量**不少于 115 台。

(1) 若投标人配置方案所需服务器数量大于 115 台，则需投标人自行补充相应数量服务器；

(2) 若投标人配置方案所需服务器数量小于 115 台，则须补充计算型服务器 A，使得总体服务器满足上述最低数量要求，并配置相应的计算节点许可(运行云主机)。

1.3. 农信云总体需求

1.3.1. ★总体功能要求

1.3.1.1. IaaS 总体需求

IaaS 平台可按需构建计算、网络和存储三大资源域，以云主机、裸金属的统筹管理为基础，结合 SDN+VPC、弹性 IP、负载均衡等网络技术实现灵活组网，并辅以高可靠、高容量的云硬盘、分布式文件及块存储等服务，为上层应用运行提供全面、灵活、可靠的技术支撑。基础设施不绑定硬件及品牌，支持一云多芯、应用平稳上云、云上安全，并可按需容纳足够数量的物理节点。同时，基于统一的云管平台提供核心资源的统一管理、分配调度、运营运维等能力，实现资源生成、申请、分配、使用、监控、回收的全生命周期管理，并具备精准预警、成本核算、度量评估等基础能力。具备开放性，可通过 APIs 快速构建资源及业务。

IaaS 平台依托多中心多活布局，实现区域、资源池等多层次的高可用，首先基于云管平台支持多数据中心管理，保证其相互独立同时实现中心级切换。其次提供租户隔离功能，通过计算和网络资源虚拟化、池化及调度实现底层资源的隔离，通过分布式存储系统保证数据的可靠性，为业务连续性和数据安全提供保障。

1.3.1.2. PaaS 总体需求

PaaS 平台的建设应采用开放的、可替换组件的架构。PaaS 平台应以标准化满足业务系统的多样组合、快速响应业务需求，加快应用系统的交付速度，不断助力研发路径的统一和研发质量的提升；助力信息系统建设向分布式微服务架构转型，实现应用的统一调度管理，提升系统弹性扩展及安全运行能力，提高开发和运维效率和自动化运维水平，有力支撑灾备和多活的应用场景，持续提升信息系统的业务连续性保障水平。

1.3.1.3. 云管平台总体需求

云管平台为业务、需求、开发、测试、运维等人员提供全方位、可视化和开放性的云资源供给和运营能力，具备一体化管控、自动化运维、智能化分析及个性化扩展等功能，并通过友好易用的界面提升用户体验。

云管平台统一 IaaS 和 PaaS 层管理，具备细粒度的用户、

用户组、角色和权限管理机制，方便管理人员进行组织架构管理，提高安全合规性；支持自助的、开放的、自动化、可配置、可计费的各类云资源纳管和供给服务，简化研发流程；提供基础资源、中间件、应用等云上所有服务立体化、多维度、可视化的监控能力，实现应用运维集中与统一。

1.3.1.4. 监控平台总体需求

监控平台支持监控面板跨云服务、跨实例查看监控数据，自定义展示和导出监控数据；支持对计算、存储、网络等资源的监控，并提供自定义阈值告警功能；支持跨云服务、跨地域资源分组管理功能，支持按应用系统集中监控服务器、网络设备、存储 PaaS 软件等资源，具备监控数据可视化展示，并与告警机制联动；支持对应用进行日志管理和服务调用链路追踪，并按业务需求设置告警策略；支持应用系统吞吐量、JVM、线程、SQL、响应状态等典型指标的监控和告警。

1.3.1.5. 云安全服务总体需求

云安全服务应从平台层面保障信息系统安全运行，保证信息资产的机密性，提升系统运维的自动化水平，防范安全风险漏洞。云平台应实现物理安全、网络安全、平台安全、访问控制、数据安全、业务安全、运维安全等要求，同时应满足国家相关安全标准及认证，满足监管合规要求。云平台需具备兼容其他厂商和技术的能力，避免对单一厂商、单一技术方案过分依赖而产生的安全问题。

1.3.2. ★总体指标要求

1.3.2.1. 功能性指标要求

(1) 服务能力：提供 IaaS 和 PaaS 服务能力，包括计算、存储、网络等 IaaS 服务能力，容器、中间件、数据库等 PaaS 服务能力以及相应的安全服务能力。

(2) 平台开放支持：支持对云平台的服务进行定制和扩展。

(3) 硬件支持：云平台应支持主流厂商多样化的服务器、网络设备、存储设备、安全设备，云平台应能同时支持通用 X86 和国产芯片架构服务器。同时云平台涉及的服务器、备份对接设备应支持至少三家原厂制造商，网络设备（交换机、路由器、硬件防火墙、硬件负载均衡）支持至少两家原厂制造商。

1.3.2.2. 非功能性指标要求

(1) 兼容性要求：投标人及原厂商应保证 IaaS 软件（不含固件、微码等硬件运行所需的自身软件产品）产品和 PaaS 软件产品需为同一厂商，以及项目整体方案内软硬件的兼容性。服务器及 PaaS 相关产品(1.4.3 节所有产品)需至少兼容统信 V20 1060 系列、银河麒麟 V10 服务器操作系统。

(2) 扩展性要求：支持扩展为多地多中心（至少支持

两地三中心) 布局; 支持在单数据中心扩展到不少于 3000 台物理服务器规模, 支持在单数据中心管理不少于 18000 台云主机。

(3) 业务连续性要求: 云平台的业务连续性要求在两地三中心完成建设的情况下, 应满足 $RPO \approx 0$, $RT0 \leq 30$ 分钟。

(4) 可用性要求: 云平台无单点问题, 在两地三中心完成建设的情况下, 整个云平台可用性达到 99.99%, 支持多中心多活;

(5) 可管理性要求: 提供完整的云平台管理服务能力和运营运维服务能力。产品服务需提供 API 接口以及接入的 SDK 和文档。

(6) 平滑升级要求: 支持云平台的平滑升级, 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; 具备多版本应用平滑升级过渡的能力, 最小以周为单位整合补丁。

(7) 性能要求: 满足云平台各部分不同的性能要求, 详见各章节性能指标要求。

(8) 自动部署要求: 云平台上软、硬件资源具备一键部署能力, 能够快速部署。

(9) 扩容要求: 对于本次采购的各类软硬件设备, 应说明相关授权或设备在授权、数量、性能、应用场景等方面的限制情况, 并且对于招标人后续扩容时需要配置、采购的

内容进行说明，具体要求见“扩容建设要求”章节。

(10) 临时使用授权要求：对于本次采购的各类软件产品，如果招标人需要，可无条件获得软件的临时使用授权（有效期不少于 6 个月）以供招标人临时使用；

(11) 软件许可要求：所有软件许可不区分 CPU 架构，即招标人可以自由地将软件应用到受云厂商支持的硬件架构中；

(12) 基础定制要求：云平台界面主要品牌元素使用农信银个性化 Logo、颜色等。

(13) PaaS 产品中分布式关系型数据库服务、数据库同步工具、微服务应用平台、分布式缓存服务、DevOps 服务需支持部署在非云环境中。若不满足上述需求，投标方需提供相应的方案和产品，保持非云环境技术选型与云上一致。投标人需按照招标人实际需求完成部署工作，且上述产品所享受的各项维保服务不受影响。

(14) 投标人须提供测试、开发等环境的软件授权，供招标人按需使用，且不再收取额外费用。测试、开发等环境的软件功能、兼容性、安全性等在技术规格上要求与生产云保持一致。

1.3.2.3. 云平台发展要求

(1) 自有知识产权：云技术原厂商应承诺具有本次投

标的云平台软件产品的知识产权；

(2) **云平台发展路线：**投标软件是其长期产品，未来 10 年会持续发展，若原厂商不再继续支持，应提前至少两年告知；

(3) **云平台技术体系：**在未来 10 年内，农信云平台和原厂商自身的公有云平台保持相同的技术体系；

(4) **供应链稳定：**在未来 10 年内，农信云平台保持持续支持新的硬件且相关硬件具有稳定的供应链体系（即支持特定配置的多个不同硬件厂商的硬件设备，配置要求和原厂商对应版本的公有云保持一致）；

(5) **版本升级：**在维保期内，农信云平台软件产品大小版本升级不再收取额外费用。大小版本升级需支持业务无中断升级；

(6) **适配要求：**为保证农信银自有技术平台能够适配本项目 API 网关、微服务应用平台产品。投标人需提供技术支持，直到技术平台完成上述产品的适配工作；若无法满足上述要求，投标人需提供上述产品的源码和设计文档以满足技术平台适配需求（源码版本需和农信云上产品版本保持一致）。

1.3.2.4. 其他要求

(1) 投标人及原厂商须以本次采购的云平台满足相关

安全标准及资质要求为前提提供相应的技术方案、软硬件资源。如因投标人及原厂商提供的技术方案、软硬件资源导致本次采购的云平台无法满足需求书规定的相应安全合规要求, 招标人有权向其追偿因此受到的损失。

(2) 投标人及原厂商须确保其所提供的软硬件的厂商按照需求书要求提供相应的服务, 并就服务的结果承担相应担保责任。

(3) 投标人未经招标人许可, 不得将该项目分包给其他服务商。

(4) 因产品测试不一定能实时、全部反映出生产上的问题, 因此招标人保有对一旦发现所购产品在实际接入生产环境运行后发现性能没有达到采购要求书中要求后追究投标人相关责任的权利。投标人需根据实际情况, 为用户提供用户认可的优化解决方案, 期间产生的费用由投标人自行承担。

(5) 投标人需确保本次提供的软、硬件产品需通过网络安全审查, 未通过网络安全审查则合同不生效。

1.3.3. ★安全合规要求

投标人及原厂商须协助招标人, 使得云平台云满足以下标准、认证(相关认证费用及组织工作由招标人自理, 投标人应无条件配合认证工作)及审查验收要求:

等级保护:

GB 17859-1999 计算机信息系统安全保护等级划分准则;

GB/T 25058-2010 信息安全技术信息系统安全等级保护实施指南;

GB/T 25070-2010 信息安全技术信息系统等级保护安全设计技术要求

系统定级:

GB/T 22240-2008 信息安全技术信息系统安全等级保护定级指南

技术标准:

GB/T 20270-2006 信息安全技术网络基础安全技术要求

GB/T 20271-2006 信息安全技术信息系统通用安全技术要求

GB/T 20272-2006 信息安全技术操作系统安全技术要求

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

JR/T 0166-2018 云计算技术金融应用规范技术架构

JR/T 0167-2018 云计算技术金融应用规范安全技术要求

JR/T 0168-2018 云计算技术金融应用规范容灾

商用密码应用安全性评估 FAQ (第二版) 第 21、22 条要

求。

管理标准:

GB/T 22239-2019 信息安全技术信息系统安全等级保护基本要求

安全合规认证:

网络安全等级保护三级

商用密码应用安全性评估三级。**审查及验收:**

网络安全审查。

1.3.4. ★设计要求

1.3.4.1. 技术方案要求

以国家相关政策及法规为指导，结合金融行业标准管理办法、金融信息化现状及实际应用，从实际要求出发，以国产化软硬件为数字底座，建设一个安全、高效实用的农信云平台。方案设计必须按照“高安全、高性能、高可用、高可扩展、高可管理”的原则建设和管理。

农信云平台方案设计应遵循以下总体规划原则：

（1）高安全性：本项目提供的云平台需遵循行业安全规范，设计安全防护保证客户数据中心安全，达到 GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求 和 JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引等级保护三级要求，重点保障网络安全、主机安全、虚拟化安全、应用安全和数据安全。

(2) 高性能性：本项目建设的农信云，为农信银及农信机构各类应用提供集中运营管理的数字底座，实现资源共享，体现以云计算为核心实现“共性平台+应用子集”集约化建设的总体思路，最终实现高性能算力。

(3) 高可用性：本项目提供的农信云平台需从硬件设备冗余、链路冗余、应用容错等方面充分保证整体系统的可用性；同时云平台需采用分布式架构，从整体系统上提高可靠性，降低系统对单设备可靠性的要求。

(4) 高扩展性：本项目提供的云平台资源需要根据业务应用工作负荷要求进行弹性伸缩，IT 基础架构应与业务系统松耦合，在业务系统进行容量扩展时，只需增加相应数量的 IT 硬件设备，即可实现系统的灵活扩展。

(5) 高可管理性：本项目提供的云平台应符合国家金融行业云平台技术标准和规范。需采用经过大规模商用实践检验的架构方案和软硬件产品选型，采用符合 ITIL 规范的 IT 管理方案，保障方案的成熟性和可管理性。

1.3.4.2. 资源设计要求

(1) 本项目完成长沙生产云建设，长沙数据中心用于提供计算服务的虚拟资源池服务器和裸金属服务器数量不少于 100，不含配套存储、PaaS、云管、网络、安全等系统的服务器，详见采购清单。

(2) 建设 2 个全闪块存储资源池，每个块存储资源池可用容量不小于 150TB（三副本后）。

(3) 建设 1 套文件存储和 1 套对象存储，文件存储可用容量不小于 100TB，对象存储可用容量不小于 300TB。

1.3.4.3. 网络设计要求

1.3.4.3.1. 数据中心网络要求

(1) 数据中心架构：数据中心全部网络建设满足容灾架构，内部网络链路和设备须采取冗余架构；云平台应支持与主流厂商硬件或软件 SDN，通过 SDN 技术实现网络虚拟化，构建网络资源池。

(2) 数据中心专线：同城数据中心间网络：招标人初步计划采用裸光纤连接。异地数据中心间网络：招标人初步计划采用多条运营商专线连接。

(3) 数据中心设备：数据中心配套的网络设备(如交换机、路由器等)以及配套的防火墙等安全设备，均需要满足冗余架构。

1.3.4.3.2. 网络容量和标准

1.3.4.3.2.1. 网络容量

(1) 核心交换机支持在线扩容至部署 3000 台服务器的能力；

(2) LEAF 交换机下联 25G 光口或 10G 光口，上联 100G

光口，单台 LEAF 交换机上联 SPINE，端口数量不少于 4 个，LEAF 到 SPINE 的收敛比不大于 3:1，LEAF 交换机应不少于 48 个端口，服务器与 LEAF 交换机之间通过双网卡绑定，逻辑层隔离平台管理和租户业务网络平台，不同平面间设置不同 Qos 策略；

1.3.4.3.2.2. 网络标准

区域划分：农信云的网络划分包括但不限于以下六个模块（相关设备均需投标人提供）：

（1）核心模块：提供各模块之间数据高速转发能力；

（2）局域网接入模块：提供农信云接入传统数据中心网络及广域网，部署服务器负载均衡，国密 SSL 卸载设备，该区域负载均衡、防火墙等设备为松耦合设计，单台设备故障无需负载均衡、防火墙等联动切换；

（3）互联网接入模块：提供农信云接入农信银互联网接入模块，部署链路负载均衡，国密 SSL 卸载设备，该区域负载均衡、防火墙等设备为松耦合设计，单台设备故障无需负载均衡、防火墙等联动切换；

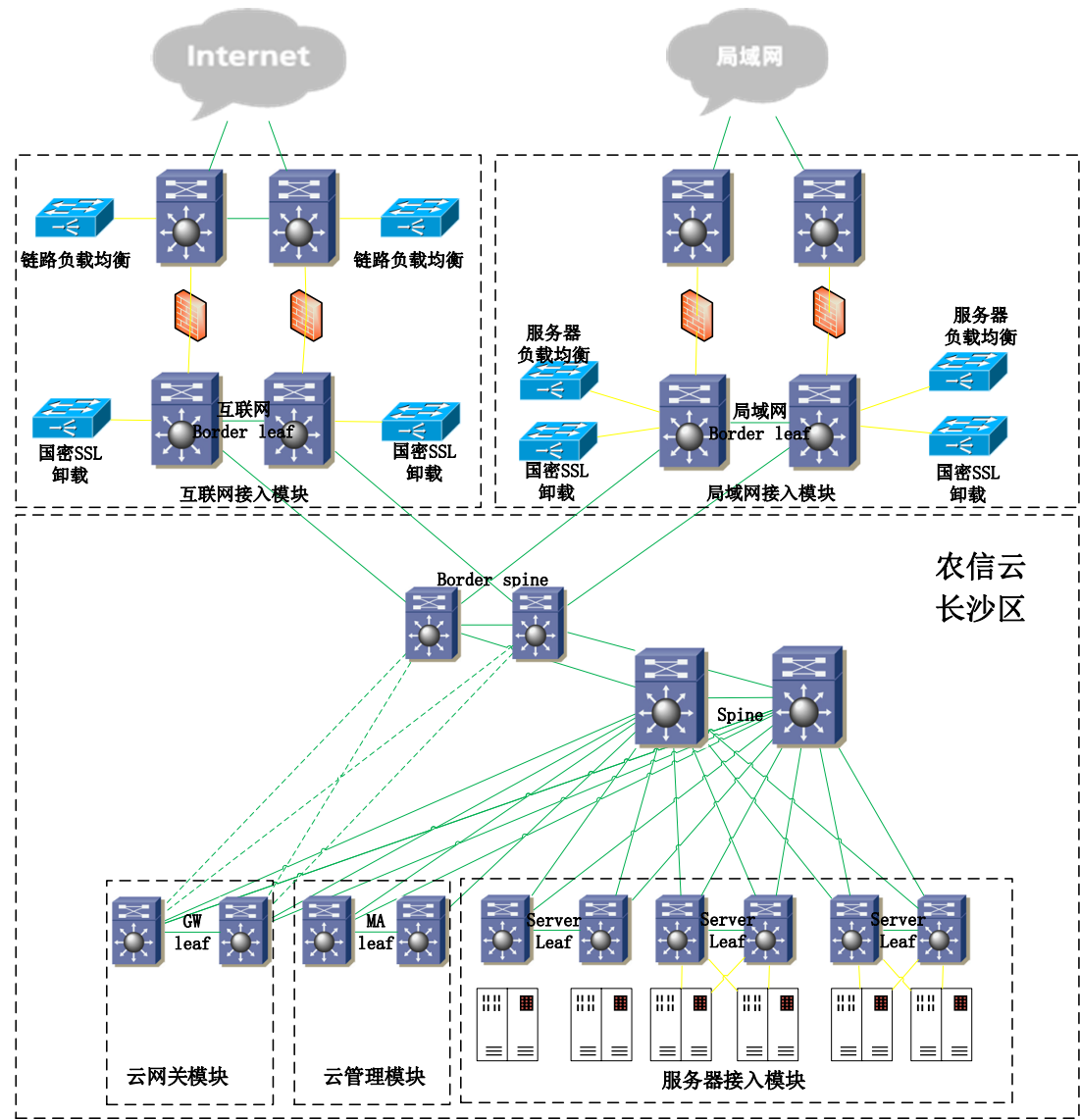
（4）服务器接入模块：提供计算、存储、数据库等资源部署；

（5）云管理模块：提供云内设备带外管理及管理组件部署；

（6）云网关：提供云内 VPC、NTP、DNS、四层负载、七

层负载等网络相关服务能力。

参考网络拓扑示意图如下，投标人应根据方案，满足上述模块设计要求。



1.4. 农信云各模块详细需求

1.4.1. 硬件设备要求

(1) 以下章节描述的硬件数目为各投标人投标时需达到的最低量，各投标人应在确保满足本次业务和技术需求的

前提下，进行实际配置。

(2) 本次投标人所采用的产品可适配所投云产品。

(3) 网络和安全设备方面除特别标注软硬件方案皆可外，均应采用硬件解决方案。若采用软件解决方案（可通过云平台一种或多种产品满足相应能力，或另行提供相应的专业化软件满足相应能力。如采用专业化软件，应已经获得授权，无需额外采购），应配套额外增加的相应服务器资源，避免占用业务系统所需的服务器资源。

1.4.1.1. 国产服务器规格

为保证可维护性和兼容性，投标人根据各资源池要求配置相应的国产服务器。

1.4.1.1.1. 计算型服务器规格 A

序号	服务器规格 1		服务器
			指标要求
1.	规格	高度	机架式，高度 $\leq$ 2U
2.	★CPU	CPU 数量	配置 $\geq$ 2 颗
3.		CPU 规格	须为国产 CPU，规格二选一： (1) ARM 架构，单颗不小于 64 核、基础频率不小于 2.6GHz； (2) X86 架构，单颗不小于 32 核、线程数不小于 64、基础频率不小于 2.2GHz。
4.	★内存	内存槽	槽位数 $\geq$ 16 个
5.		内存容量	配置 DDR4 或 DDR5 RDIMM 内存，频率 $\geq$ 2933MHz，单根内存条 $\geq$ 32G，内存容量 $\geq$ 512G。
6.	★硬盘 I/O	硬盘槽位	支持 $\geq$ 8 个 NVME 硬盘槽位

7.		硬盘种类	支持 2.5 寸 SAS、SATA 接口的 HDD（机械硬盘）、SSD（固态硬盘）、NVME 硬盘（固态硬盘）。所有硬盘支持热插拔。
8.		硬盘容量	配置 ≥ 1 块 480GB SSD, 5 年内 DWPD 不小于 1; 配置 ≥ 0 块 3.2TB NVME SSD, 5 年内 DWPD 不小于 3; 数据硬盘类型（HDD 或 SSD）和数量按需配置。
9.		HBA	配置 ≥ 0 块（各云厂商根据自身实际情况按需配置） 支持配备 SAS/SATA HBA 卡, SAS 端口速率 $\geq 12\text{Gb/s}$, SATA 端口速率 $\geq 6\text{Gb/s}$, 不得采用多 HBA 方式扩展磁盘, 所有 SAS/SATA 硬盘通过 HBA 扩展连接, 并保证用于本地系统安装 480G SATA SSD 硬盘盘序优先靠前;
10.		RAID	配置 ≥ 0 块（各云厂商根据自身实际情况按需配置） 支持 RAID 0、RAID 1、RAID 5、RAID 6、RAID 10 等。
11.	★网络	以太网通道	配置 ≥ 2 块 $\geq 25\text{G}$ 双口光口网卡（含光模块）; 千兆网卡≥ 0 块,（各云厂商根据自身实际情况按需配置）
12.	★软件	软件兼容性	至少兼容银河麒麟 V10、统信 1060e
13.	★管理	管理	独立 BMC 管理口, 支持 IPMI 2.0、KVM over IP, Redfish;
14.	★其他	电源、风扇、导轨	风扇冗余; 配备服务器导轨; 电源冗余, 通过 80plus 白金认证, 按招标人需求配置电源线。
15.	★维保	维保服务	提供 ≥ 5 年原厂金牌 7x24H 设备保障和技术支持服务

1.4.1.1.2. 存储型服务器规格 A

序号	服务器规格 1		服务器
			指标要求
1.	规格	高度	机架式, 高度 $\leq 2\text{U}$
2.	★CPU	CPU 数量	配置 ≥ 2 颗

3.		CPU 规格	须为国产 CPU，规格二选一： (1) ARM 架构，单颗不小于 32 核 (2) X86 架构，单颗不小于 32 核
4.	★内存	内存槽	槽位数≥16 个
5.		内存容量	配置 DDR4 或 DDR5 RDIMM 内存，频率≥2933MHz，单根内存条≥32G，所有物理内存品牌型号一致，内存容量≥256G。
6.	★硬盘 I/O	硬盘槽位	支持≥12 个硬盘槽位
7.		硬盘种类	支持 2.5 寸 SAS、SATA 接口的 HDD（机械硬盘）、SSD（固态硬盘）、NVME 硬盘（固态硬盘）。所有硬盘支持热插拔。
8.		硬盘容量	配置≥1 块 480GB SSD, 5 年内 DWPD 不小于 1； 配置≥1 块 NVME SSD 数据盘， 8TB≥单盘容量≥3.2TB，5 年内 DWPD 不小于 3。
9.		HBA	配置≥0 块（各云厂商根据自身实际情况按需配置） 支持配备 SAS/SATA HBA 卡，SAS 端口速率≥12Gb/s，SATA 端口速率≥6Gb/s，不得采用多 HBA 方式扩展磁盘，所有 SAS/SATA 硬盘通过 HBA 扩展连接，并保证用于本地系统安装 480G SATA SSD 硬盘盘序优先靠前；
10.		RAID	配置≥0 块（各云厂商根据自身实际情况按需配置） 支持 RAID 0、RAID 1、RAID 5、RAID 6、RAID 10 等。
11.	★网络	以太网通道	配置≥2 块≥25G 双口光口网卡（含光模块）； 千兆网卡≥0 块，（各云厂商根据自身实际情况按需配置）
12.	★管理	管理	独立 BMC 管理口，支持 IPMI 2.0、KVM over IP, Redfish；
13.	★其他	电源、风扇、导轨	风扇冗余；配备服务器导轨；电源冗余，通过 80plus 白金认证，按招标人需求配置电源线。

14.	★维保	维保服务	提供≥5年原厂金牌7x24H设备保障和技术支持服务。所有硬盘不返厂。
-----	-----	------	------------------------------------

1.4.1.1.3. 存储型服务器规格 B

序号	服务器规格 2		服务器
			指标要求
1.	规格	高度	机架式, 高度≤2U
2.	★CPU	CPU 数量	配置≥2 颗
3.		CPU 规格	须为国产 CPU, 规格二选一: (1) ARM 架构, 单颗不小于 32 核 (2) X86 架构, 单颗不小于 32 核
4.	★内存	内存槽	槽位数≥16 个
5.		内存容量	配置 DDR4 或 DDR5 RDIMM 内存, 频率≥2933MHz, 单根内存条≥32G, 所有物理内存品牌型号一致, 内存容量≥256G。
6.	★硬盘 I/O	硬盘槽位	支持≥12 个硬盘槽位
7.		硬盘种类	支持 2.5 寸 SAS、SATA 接口的 HDD (机械硬盘)、SSD (固态硬盘)、NVME 硬盘 (固态硬盘)。所有硬盘支持热插拔。
8.		硬盘容量	配置≥1 块 480GB SSD, 5 年内 DWPD 不小于 1; 配置≥2 块 NVME SSD, 单盘容量≥3.2TB, 5 年内 DWPD 不小于 3; 配置≥12 块 SATA 硬盘, 单盘容量≥8TB。
9.		HBA	配置≥0 块 (各云厂商根据自身实际情况按需配置) 支持配备 SAS/SATA HBA 卡, SAS 端口速率≥12Gb/s, SATA 端口速率≥6Gb/s, 不得采用多 HBA 方式扩展磁盘, 所有 SAS/SATA 硬盘通过 HBA 扩展连接, 并保证用于本地系统安装 480G SATA SSD 硬盘盘序优先靠前;

10.		RAID	配置 ≥ 0 块(各云厂商根据自身实际情况按需配置) 支持 RAID 0、RAID 1、RAID 5、RAID 6、RAID 10 等。
11.	★网络	以太网通道	配置 ≥ 2 块 $\geq 25G$ 双口光口网卡(含光模块); 千兆网卡 ≥ 0 块,(各云厂商根据自身实际情况按需配置)。
12.	★管理	管理	独立 BMC 管理口,支持 IPMI 2.0、KVM over IP, Redfish;
13.	★其他	电源、风扇、导轨	风扇冗余;配备服务器导轨;电源冗余,通过 80plus 白金认证,按招标人需求配置电源线。
14.	★维保	维保服务	提供 ≥ 5 年原厂金牌 7x24H 设备保障和技术支持服务。所有硬盘不返厂。

1.4.1.1.4.数据库服务器规格 A

序号	数据库型服务器规格		服务器
			指标要求
1.	规格	高度	机架式,高度 $\leq 2U$
2.	★CPU	CPU 数量	配置 ≥ 2 颗
3.		CPU 规格	须为国产 CPU,规格二选一: (1) ARM 架构,单颗不小于 64 核、基础频率不小于 2.6GHz; (2) X86 架构,单颗不小于 32 核、线程数不小于 64、基础频率不小于 2.2GHz。
4.	★内存	内存容量	配置 DDR4 或 DDR5 RDIMM 内存,频率 $\geq 2933MHz$,单根内存条 $\geq 32G$,所有物理内存品牌型号一致,内存容量 $\geq 1024G$ 。
5.	★硬盘 I/O	硬盘槽位	支持 ≥ 8 个 NVME 硬盘槽位
6.		硬盘种类	支持 2.5 寸 SATA SSD (固态硬盘)、NVME 硬盘 (固态硬盘)。所有硬盘支持热插拔。

7.		硬盘容量	配置 ≥ 2 块 480GB SATA SSD, 5年内 DDPD 不小于 1; 配置 ≥ 4 块 NVME SSD, 单盘容量 ≥ 3.2 TB, 5年内 DDPD 不小于 3;
8.		HBA	配置 ≥ 0 块(各云厂商根据自身实际情况按需配置) 支持配备 SAS/SATA HBA 卡, SAS 端口速率 ≥ 12 Gb/s, SATA 端口速率 ≥ 6 Gb/s, 不得采用多 HBA 方式扩展磁盘, 所有 SAS/SATA 硬盘通过 HBA 扩展连接, 并保证用于本地系统安装 960G SATA SSD 硬盘盘序优先靠前;
9.		RAID	配置 ≥ 0 块(各云厂商根据自身实际情况按需配置) 支持 RAID 0、RAID 1、RAID 5、RAID 6、RAID 10 等。
10.	★网络	以太网通道	配置 ≥ 2 块 ≥ 25 G 双口光口网卡(含光模块); 千兆网卡 ≥ 0 块, (各云厂商根据自身实际情况按需配置)
11.	★管理	管理	独立 BMC 管理口, 支持 IPMI 2.0、KVM over IP, Redfish;
12.	★软件	软件兼容性	至少兼容银河麒麟 V10、统信 1060e
13.	★其他	电源、风扇、导轨	风扇冗余; 配备服务器导轨; 电源冗余, 通过 80plus 白金认证, 按招标人需求配置电源线。
14.	★维保	维保服务	提供 ≥ 5 年原厂金牌 7x24H 设备保障和技术支持服务。所有硬盘不返厂。

1.4.1.1.5.利旧服务器规格

序号	型号	备注
1	新华三 R4900G3、R4950G3	详细配置参见 1.8.1 章节
2	浪潮 NF5280M6、CS5280H、CS5260F	
3	联想 ThinkServer SR658H V2	
4	待采购服务器	

1.4.1.1.6.其他要求

投标人提供的服务器应为同一品牌，服务器 CPU 应为同一品牌。

投标人提供的服务器的硬盘，相同品牌型号的形态应保持一致。招标人可在不通知中标方和服务器原厂商的情况下，在服务器之间，自行调换空闲的硬盘，所享受的各项服务不受影响。

在不影响平台整体架构和安全的情况下，招标人可将投标人提供的服务器自由应用在其他环境中，所享受的各项服务不受影响。

1.4.1.2. 网络设备规格

投标人配置的网络设备参数配置不低于本节要求，所投设备为市场主流产品及型号。

序号	设备类型	业务用途
1.	核 心 交 换 机	支持最终扩容至不少于 3000 台各类服务器部署的接入能力，当前实配至少 900 台各类服务器的接入能力。
2.	接 入 交 换 机-25G 接 入	满足各类设备接入（采购清单中的 100G/25G/10G/1G 接入交换机的最低数量用于保障云内所有各类设备的接入，总体交换机具体数量由投标人根据技术方案自行配置。）
3.	接 入 交 换 机-10G 接 入	
4.	接 入 交 换 机-1G 接 入	
5.	防 火 墙	局域网边界 2 台（硬件），互联网接入边界 2 台（硬件）。云内防火墙 1 套（根据云内 VPC 划分安全隔离要求，每个 VPC 使用边界使用独立防火墙防护，可采用硬件或软件防火墙实现），功能、性能、冗余性均需满足要求。

6.	负载均衡	互联网接入负载均衡 2 台（硬件），局域网负载均衡 2 台（硬件）。国密 SSL 卸载 4 台（硬件）。 云内负载 1 套（根据云内 VPC 划分安全隔离要求，每个 VPC 使用负载均衡功能，可采用硬件方式或软件负载均衡实现） 功能、性能、冗余性均需满足要求。
----	------	--

1.4.1.2.1. 交换机

1.4.1.2.1.1. 国产核心交换机

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	设备架构要求	多级交换架构，能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离
2.		设备板卡要求	要求交换网板槽位数 ≥ 6 ；在交换矩阵能够满足 N+1 冗余情况下，本次配置交换机矩阵模块数量 ≥ 6 ；
3.			支持并配置主控冗余引擎模块
4.		★设备端口配置	单台设备实配 100G 线速端口 ≥ 72 ，单块板卡 100G 接口数量 ≥ 36 个，100G 端口可以自适应成 40GE，模块满配，包含与接口数量相等 100G MPO 接口多模光模块，即光模块满配）。
5.		★设备扩展性要求	业务插槽数 ≥ 8
6.	性能及容量指标	★设备端口处理性能	配置的全部端口支持全线速 2 层、3 层转发
7.		★设备交换容量	$\geq 640\text{Tbps}$
8.		★数据包转发能力	$\geq 230000\text{Mpps}$
9.		★端口转发延迟	端口与端口之间 $\leq 8\mu\text{s}$
10.		路由条目数	$\geq 64\text{K}$

11.		★性能指标验证要求	对于以上性能及容量指标,若用户测试环境没有足够资源进行验证,原厂商应提供相应的测试环境并由用户现场验证在容量到达指标时的设备运行状态与指标相符
12.	功能性要求	端口特性要求	所有物理端口可以直接配置为三层路由端口,配置IP地址,需提供官方文档链接证明
13.		★二层特性要求	支持MSTP(IEEE 802.1s)≥62个实例
14.			支持巨型帧(9216 Bytes)
15.		★三层特性要求	IP V4: 支持静态路由, RIP V2, OSPF V2, ISIS,BGP,PBR
16.			IP V6: 支持静态路由, OSPF V3, ISIS,BGPv6, PBR
17.			支持BFD(支持BGP, ISIS,OSPF,RIP,VRRP,PIM等)
18.			等价路由支持≥32条,端口不在同一机箱也可捆绑为一组实现负载均衡
19.		组播功能要求	支持PIM V2 SM, SSM, MSDP, IGMP V2, V3,组播路由≥4K
20.		安全功能要求	单板卡ACL条目数≥20K
21.			支持控制平面保护
22.			支持标准和扩展第二层ACL: MAC地址、协议类型等
23.			支持标准和扩展第三到四层ACL: IPv4和v6、ICMP、TCP、UDP等
24.			支持扩展的ACL、MAC地址、端口ACL(PACL)、VLAN ACL(VACL)和路由ACL(RACL);
25.			支持DHCP Snooping,ARP检测和IP Source Guard
26.			支持Private VLAN(PVLAN)等相应技术
27.		环路检测及保护要求	支持BPDU保护、Root保护、环路保护
28.		★链路状态检测要求	支持单向链路检测特性用于检测光纤或铜缆以太网链路路上的故障
29.	高可用及可靠性要求	业务不间断升级	支持不间断业务在线软件升级

30.		故障隔离要求	支持对交换机操作系统每个进程的故障隔离, 系统进程可进行状态化或无状态化重启, 不影响其他进程
31.		★电源及风扇	支持 N+1, N+N 电源冗余, 支持最大电源数 ≥ 4 , 配置电源模块不少于 4 个
32.			支持风扇冗余, 最大风扇托盘数 ≥ 2
33.		引擎冗余要求	支持主控模块冗余, 主控冗余时模块间支持状态化故障切换;
34.		热插拔要求	支持主控引擎拔出 0 丢包
35.			★支持矩阵拔出 0 丢包
36.		链路高可用要求	实配的所有端口支持以太网端口捆绑技术 (IEEE 802.3ad)
37.			必须支持跨机箱链路捆绑 (端口不在同一机箱也可捆绑为一组实现负载均衡)
38.		★网关协议	支持 VRRP
39.	监控及管理要求	★管理协议要求	支持 SNMP V1/V2/V3
40.		带外管理端口要求	提供独立的 100/1000M 的带外网络管理接口
41.		登陆方式	支持 telnet 和 SSHV2 登陆方式, 支持通过命令行等方式进行配置和管理。
42.		★监控项目要求	支持通过 snmp 直接采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、NTP 状态等设备运行状态
43.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由翻动、地址冲突等)
44.			支持向外部 SNMPTrap 服务器发送告警信息, 告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由翻动、地址冲突等)
45.		★认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权

46.		网管性能及容量监控要求	支持端口流量等性能监控,并对设备指标中所涉及的性能指标提供监控方法;
47.		链路关键路径	支持并提供通过 Rping 或者 NQA 等方式提供对远端指定路径的监控,所采购的网络整机设备如不能使用 Rping 实现统一的链路连通性探测,则中标人需提供与现有网管平台兼容的链路连通性管理解决方案。
48.		时钟同步要求	支持 NTP 时间同步
49.		可编程管理要求	优选设备本身自带内嵌事件管理功能,可依据系统事件自定义触发动作,通过事件管理器可调用设备本身的所有命令,如接口命令、路由、策略路由、ACL 和 QoS 等。
50.		★流量镜像要求	支持 SPAN, ERSPAN, 具备对端口、VLAN 的流量镜像功能;
51.		流量统计要求	提供 Netflow/Netstream 功能,通过提供 Netflow、Netstream、sflow 中任意一种或多种功能,通过上述功能检测网络病毒,实配 Netflow、Netstream、sflow 中任意一种或多种硬件统计板卡或芯片实现:
52.			每张实配线卡支持 Netflow、Netstream、sflow 中任意一种或多种表项 $\geq 128K$
53.			支持采样 (Sampling)
54.			支持 L2 Netflow、Netstream、sflow 中任意一种或多种
55.			支持通过端口镜像流量后,使用开源抓包工具 (如 Wireshark),可在线对报文进行分析。
56.		配置自动备份	提供设备配置自动备份的方法 (命令行交互方式或者其他方式),定期自动备份到外部服务器
57.		系统故障检测要求	系统自检测发现端口、芯片、板卡、矩阵的丢包等影响数据转发的问题时,具备自我屏蔽、隔离功能
58.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可
59.		Overlay 技术支持	所有实际配置端口硬件支持 VXLAN,支持 VXLAN Bridging 和 Routing 功能或相应技术。

60.		数 据 中 心特性	必须支持 IEEE DCB 或 CEE,支持 DCBX 协议(IEEE 802.1AB)
61.		★产 品 成 熟 度 要求	CPU 芯片须为国产,产品剩余生命周期不低于 7 年。

1.4.1.2.1.2. 国产接入交换机-100G 接入

序号	指标分类	技术指标	要求
1.	设备硬件 及端口要求	★硬件规格	电源 1+1 备份, 风扇 N+1 备份
2.			端口缓存 $\geq 32\text{M}$
3.			支持前后、后前风道
4.		★端口配置要求	≥ 32 个 100 GE QSFP28 端口, 根据组网模式, 满配与接口相对应 MP0 的多模模块。
5.			(以上配置的端口均为实际可用数量, 要求全部同时支持, 不得存在复用端口)
6.	容量及性能指标	★交换容量	交换容量 $\geq 6.4\text{Tbps}$, 以官网所列最低参数为准
7.		★转发性能	包转发率 $\geq 2000\text{Mpps}$, 以官网所列最低参数为准
8.		MAC 地址表	MAC 表容量 $\geq 256\text{K}$, 支持动态 MAC、静态 MAC 和黑洞 MAC 表项
9.		ARP 表项	ARP 表容量 $\geq 90\text{K}$
10.		FIB 表项	IPv4 FIB 表容量 $\geq 256\text{K}$
11.		二层功能	支持 IEEE 802.1q, IEEE 802.1p, IEEE 802.1w(RSTP), 802.1s(MSTP), IEEE 802.3ad(LACP)
12.		三层功能	支持静态路由、BGPv4、OSPF、RIP、IS-IS, 支持 BGP 的 EVPN 扩展, 支持 IPV6
13.		DC 特性	支持 VXLAN GW 支持 OpenFlow+Netconf 的 VXLAN 集中式控制平面 支持 EVPN 分布式网关 提供配套的 VXLAN Controller 支持大二层网络

14.		★QoS	支持对端口接收报文的速率和发送报文的速率进行限制, 限速粒度 $\leq 10\text{Kbit/s}$ 支持报文的 802.1p 和 DSCP 优先级重新标记 每端口支持的输出队列数 ≥ 8 支持灵活的队列调度算法, 可以同时基于端口和队列进行设置, 支持 SP、DRR、SP+DRR 或 WRR、SP+WRR 等队列调度方式
15.	高可用及可靠性要求	可靠性	链路故障切换需要小于 20ms, 因此设备需要支持 BFD (Bidirectional Forwarding Detection) $\leq 5\text{ms}$ 检测间隔
16.			支持 VRRP、VRRP 负载分担、BFD for VRRP
17.		安全性	支持 IP+MAC+PORT 的绑定
18.			支持 DHCP Snooping, 防止欺骗的 DHCP 服务器
19.			支持黑洞 MAC、动态 ARP 检测、ARP 防攻击
20.		无损以太	在支持分布式存储的场景下, 设备具备零丢包技术能力
21.		配置和维护	支持 Telemetry
22.			★支持 SNMP V1/V2/V3、Telnet、SSH
23.			支持缓存的微突发检测
24.	监控及管理要求	★监控项目要求	支持通过 snmp 直接采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、NTP 状态等设备运行状态
25.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障, 端口翻动, 路由协议邻居状态变化, 地址冲突等)
26.			支持向外部 SNMPTrap 服务器发送告警信息, 告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由协议邻居状态变化、地址冲突等)
27.		★认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权
28.		网管性能及容量监控要求	支持端口流量等性能监控, 并对设备指标中所涉及的性能指标提供监控方法;
29.		链路关键路径	支持并提供通过 Rping 或 NQA 等方式提供对远端指定路径的监控, 所采购的网络整机设备如不能实现统一的链路连通性探测, 则中标人需提供与现有网管平台兼容的链路连通性管理解决方案。

30.		时钟同步要求	支持 NTP 时间同步
31.		★流量镜像要求	支持 N 对 1 (N>1) 的端口镜像;
32.			支持本地端口镜像 (SPAN), 增强远程端口镜像 (ERSPAN), 支持跨网段的端口镜像;
33.		流量统计要求	支持网络流量分析功能, 支持 NetStream/sflow;
34.		配置自动备份	提供设备配置自动备份的方法 (命令行交互方式或者其他方式), 定期自动备份到外部服务器
35.		系统故障检测要求	系统自检测发现端口、芯片、板卡、矩阵的丢包等影响数据转发的问题时, 具备自我屏蔽、隔离功能
36.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可
37.		★产品成熟度要求	CPU 芯片须为国产, 产品剩余生命周期不低于 7 年。

1.4.1.2.1.3. 国产接入交换机-25G 接入

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	★硬件规格	电源 1+1 备份, 风扇 N+1 备份
2.			支持前后、后前风道
3.		★端口配置要求	≥6 个 40 QSFP+ / 100 QSFP28 端口, 100G MPO 多模模块满配
4.			≥48 个 10GE SFP+ / 25GE SFP28 端口, 25GE LC 多模模块满配
5.			(以上配置的端口均为实际可用数量, 要求全部同时支持, 不得存在复用端口)
6.	容量及性能指标	★交换容量	交换容量≥4.8Tbps, 以官网所列最低参数为准
7.		★转发性能	包转发率≥2000Mpps, 以官网所列最低参数为准
8.		MAC 地址表	MAC 表容量≥256K, 支持动态 MAC、静态 MAC 和黑洞 MAC 表项
9.		ARP 表项	ARP 表容量≥160K
10.		FIB 表项	IPv4 FIB 表容量≥256K

11.		二层功能	支持 IEEE 802.1q , IEEE 802.1p , IEEE 802.1w(RSTP) , 802.1s(MSTP) , IEEE 802.3ad(LACP)
12.		三层功能	支持静态路由、BGPv4、OSPF V2 、RIPv2、IS-IS, 支持 BGP 的 EVPN 扩展, 支持 IPV6
13.		★DC 特性	支持 Vxlan, 且支持 BGP EVPN 特性
14.		★QoS	每端口支持≥8 队列;
15.			支持端口的流量限制;
16.			支持 CAR、Remark 等动作;
17.			支持 SP、DRR、SP+DRR 或 WRR、SP+WRR 等队列调度方式
18.			支持 WRED、尾丢弃等拥塞避免机制;
19.	高可用及可靠性要求	可靠性	链路故障切换需要小于 20ms, 因此设备需要支持 BFD (Bidirectional Forwarding Detection) ≤ 5ms 检测间隔
20.			支持 VRRP、VRRP 负载分担、BFD for VRRP
21.		安全性	支持方式 Dos、arp 攻击和 ICMP 攻击
22.			支持 IP、MAC、端口和 VLAN 的组合绑定
23.			支持端口隔离
24.			支持 AAA、Radius 和 TACACS 认证
25.			支持 RMON
26.		★无损以太	在支持分布式存储的场景下, 设备具备零丢包技术能力
27.		★配置和维护	支持 Telemetry
28.			支持 SNMP V1/V2/V3、Telnet、SSH
29.			支持缓存的微突发检测
30.	监控及管理要求	★监控项目要求	支持通过 snmp 直接采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、NTP 状态等设备运行状态
31.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障, 端口翻动, 路由协议邻居状态变化, 地址冲突等)
32.			支持向外部 SNMPTrap 服务器发送告警信息, 告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由协议邻居状态变化、地址冲突等)
33.		认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权

34.		网管性能及容量监控要求	支持端口流量等性能监控，并对设备指标中所涉及的性能指标提供监控方法；
35.		链路关键路径	支持并提供通过 Rping 或 NQA 等方式提供对远端指定路径的监控，所采购的网络整机设备如不能使用 Rping 实现统一的链路连通性探测，则中标人需提供与现有网管平台兼容的链路连通性管理解决方案。
36.		时钟同步要求	支持 NTP 时间同步
37.		★流量镜像要求	支持 N 对 1 (N>1) 的端口镜像；
38.			支持本地端口镜像 (SPAN)，增强远程端口镜像 (ERSPAN)，支持跨网段的端口镜像；
39.		流量统计要求	支持网络流量分析功能，支持 NetStream/Netflow/sflow；
40.		配置自动备份	提供设备配置自动备份的方法（命令行交互方式或者其他方式），定期自动备份到外部服务器
41.		系统故障检测要求	系统自检测发现端口、芯片、板卡、矩阵的丢包等影响数据转发的问题时，具备自我屏蔽、隔离功能
42.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可
		★产品成熟度要求	CPU 芯片须为国产，产品剩余生命周期不低于 7 年。

1.4.1.2.1.4. 国产接入交换机-10G 接入

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	★设备端口配置	配置千兆/万兆以太网 SFP+端口≥48，10G LC 接口多模模块满配
2.			配置 100G QSFP28/40G QSFP 端口≥6，100G MPO 多模模块满配
3.		★端口特性要求	支持在两芯多模光纤上传输 40G 信号以实现未来从 10G 到 40G 的平滑升级
4.		风扇进出风结构要求	端口前进风

5.	性能及容量指标	★设备端口处理性能	配置的全部端口支持全线速2层、3层转发
6.		★设备交换容量	$\geq 4.8\text{Tbps}$
7.		★数据包转发能力	$\geq 2000\text{Mpps}$ (64B 报文, 二层、三层转发均要求达到该指标)
8.		★端口转发延迟	$\leq 12\mu\text{s}$
9.		MAC 地址表	$\geq 256\text{k}$
10.		★缓存buffer要求	$\geq 16\text{MB}$
11.		★性能指标验证要求	对于以上性能及容量指标, 若用户测试环境没有足够资源进行验证, 原厂商应提供相应的测试环境并由用户现场验证在容量到达指标时的设备运行状态与指标相符
12.	功能性要求	★二层特性要求	支持 IEEE 802.1Q VLAN 封装, VLAN 数量 ≥ 4096 , 支持快速 PVRST 或 MSTP, PortFast, BPDU ROOT Guard
13.		★三层特性要求	支持在物理端口、虚拟端口配置 IP 地址
14.			支持 $\geq 32\text{K}$ IPv4, $\geq 8\text{K}$ IPv6 单播路由
15.			支持 $\geq 8\text{K}$ IPv4 多播路由
16.			支持静态、RIP、OSFP、ISIS、BGP 等路由协议以及 PBR 策略路由
17.			支持 VRF, 数量 $\geq 4\text{K}$ 个
18.			支持 ECMP 多路径 ≥ 32 , 实现负载分担
19.		★虚拟化特性要求	硬件支持 VXLAN 桥接和路由 bridge 和 routing
20.			支持多合一虚拟化, 实现跨机箱的以太网链路捆绑, 路由/交换控制和转发平面均为双活机制
21.		QoS 要求	每端口支持 ≥ 8 个单播/多播队列
22.			支持单播、组播、广播抑制;
23.		安全功能要求	支持三层、四层的 ACL;
24.			支持 VLAN 内的 ACL (VACL) 访问控制;
25.		环路检测及保护要求	支持 BPDU 保护、Root 保护、环路保护

26.		★链路状态检测要求	支持单向链路检测特性用于检测光纤或铜缆以太网链路上的故障
27.	高可用及可靠性要求	★电源及风扇	配置冗余热插拔电源和风扇
28.		★网关协议	支持 HSRP 或 VRRP
29.	监控及管理要求	★管理协议要求	支持 SNMP V1/V2/V3
30.		带外管理端口要求	提供独立的 100/1000M 的带外网络管理接口
31.		登陆方式	支持 telnet 和 SSHV2 登陆方式, 支持通过命令行、Web 等方式进行配置和管理。
32.		★监控项目要求	支持通过 snmp 直接采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、NTP 状态等设备运行状态
33.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级(对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由翻动、地址冲突等)
34.			支持向外部 SNMPTrap 服务器发送告警信息, 告警按照对系统影响性进行分级(对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由翻动、地址冲突等)
35.		★认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权
36.		网管性能及容量监控要求	支持端口流量等性能监控, 并对设备指标中所涉及的性能指标提供监控方法;
37.		链路关键路径	支持并提供通过 Rping 或 NQA 等方式提供对远端指定路径的监控, 所采购的网络整机设备如不能使用 Rping 或 NQA 实现统一的链路连通性探测, 则中标人需提供与现有网管平台兼容的链路连通性管理解决方案。
38.		★时钟同步要求	支持 NTP 时间同步
39.		可编程管理要求	支持支持内嵌的基于事件的网络自动化管理功能, 通过监控 Syslog、设备硬件状态、路由 Track 等, 预先进行配置, 实现自动化网络管理

40.		★流量镜像要求	支持至少4个并发的SPAN和ERSPAN流量镜像,支持1个Session进程多个源端口及多个目的端口
41.		配置自动备份	提供设备配置自动备份的方法(命令行交互方式或者其他方式),定期自动备份到外部服务器
42.		系统故障检测要求	系统自检测发现端口、芯片、板卡、矩阵的丢包等影响数据转发的问题时,具备自我屏蔽、隔离功能
43.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可
		★产品成熟度要求	CPU芯片须为国产,产品剩余生命周期不低于7年。

1.4.1.2.1.5. 国产接入交换机-1G接入

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	★硬件规格	固定接口交换机
2.			电源1+1备份
3.			支持前后、后前风道
4.		★端口配置要求	≥48个10/100/1000Base-T端口,模块满配
5.			≥4个10GE SFP+端口,LC接口多模模块满配
6.			(以上配置的端口均为实际可用数量,要求全部同时支持,不得存在复用端口)
7.	性能及容量指标	★交换容量	交换容量≥570Gbps,以官网所列最低参数为准
8.		★转发性能	包转发率≥140Mpps,以官网所列最低参数为准
9.		MAC地址表	≥32K
10.		路由条目数	路由表≥16K
11.	功能性要求	端口特性要求	实配单机和板卡支持端口在二层和三层模式中灵活切换,二层模式下可归属到任意VLAN,三层模式下可直接配置IP地址
12.		二层特性要求	★支持4K VLAN;支持QinQ、Super VLAN;支持STP/RSTP/MSTP;
13.			支持跨设备链路聚合,要求配对设备有独立的控制平面,不能用堆叠等多虚一技术实现
14.		★三层特性要求	支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议

15.		组播功能要求	支持组播协议, 支持 PIM-SSM, 支持 IGMP V3
16.		★QoS 要求	至少具备 8 个队列; 支持 SP, DWRR, SP+DWRR 或 WRR、SP+WRR 调度方式; 支持出方向的端口限速, 限速粒度 64K; 提供广播风暴抑制功能; 双向流限速
17.		安全功能要求	支持 DHCP Snooping trust, 防止私设 DHCP 服务器;
18.			支持 DHCP Option 82;
19.			支持 DHCPv4 Server、Relay 和 snooping
20.			支持 MFF/IPSG/DAI
21.			支持 BPDU guard
22.		环路检测及保护要求	支持 BPDU 保护、Root 保护、环路保护
23.		链路状态检测要求	支持单向链路检测(DLDP), 有效的防止网络中单通故障的发生
24.	高可用及可靠性要求	★电源及风扇	支持并配置 1+1 冗余电源以及风扇框 1+1 冗余
25.		热插拔要求	支持电源、风扇热插拔
26.		链路高可用要求	端口支持以太网端口捆绑技术 (IEEE 802.3ad)
27.		★网关协议	支持 VRRP、VRRP 负载分担
28.	监控及管理要求	★监控项目要求	支持通过 snmp 直接采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、NTP 状态等设备运行状态
29.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级(对影响设备正常运行的软硬件报错, 如硬件故障, 端口翻动, 路由协议邻居状态变化, 地址冲突等)
30.			支持向外部 SNMPTrap 服务器发送告警信息, 告警按照对系统影响性进行分级(对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、路由协议邻居状态变化、地址冲突等)
31.		★认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权
32.		网管性能及容量监控要求	支持端口流量等性能监控, 并对设备指标中所涉及的性能指标提供监控方法;

33.		链路关键路径	支持并提供通过 Rping 或 NQA 等方式提供对远端指定路径的监控, 所采购的网络整机设备如不能使用 Rping 实现统一的链路连通性探测, 则中标人需提供与现有网管平台兼容的链路连通性管理解决方案。
34.		时钟同步要求	支持 NTP 时间同步
35.		★流量镜像要求	支持 N 对 1 (N>1) 的端口镜像;
36.			支持本地端口镜像 (SPAN), 支持跨网段的端口镜像;
37.		★流量统计要求	支持网络流量分析功能, 支持 NetStream/Netflow/sflow;
38.		配置自动备份	提供设备配置自动备份的方法(命令行交互方式或者其他方式), 定期自动备份到外部服务器
39.		系统故障检测要求	系统自检测发现端口、芯片、板卡、矩阵的丢包等影响数据转发的问题时, 具备自我屏蔽、隔离功能
40.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可
		★产品成熟度要求	CPU 芯片须为国产, 产品剩余生命周期不低于 7 年。

1.4.1.2.2. 国产边界路由器

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	★处理器要求	支持多核 CPU
2.		功能或功能板卡配置	★实配控制引擎≥2
3.			所有母板和子卡均可后向兼容
4.		交换模块要求	支持万兆口自适应千兆口
5.		★设备接口要求	≥16 个 10GE SFP+ 端口, LC 接口单模模块满配, 需分布在不同板卡。
6.		端口功能要求	物理端口具有路由能力
7.		设备出风要求	设备散热方式采用前后或左右风道散热方式

8.	性能及容量指标	★设备处理性能	交换容量 $\geq 20\text{Tbps}$
9.		转发性能	包转发能力 $\geq 3600\text{Mpps}$
10.		★端口性能	每槽位提供不少于 10 个 10GE 端口实配;
11.		★性能指标验证要求	对于以上性能及容量指标,若用户测试环境没有足够资源进行验证,原厂商应提供相应的测试环境并由用户现场验证在容量到达指标时的设备运行状态与指标相符
12.		★路由协议要求	支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议
13.		★BFD 功能	支持 BFD 功能,包括 BFD for 静态路由/OSPF/ISIS/LDP/BGP/RSVP/PIM/IP-TRUNK/Eth-TRUNK/VRRP/IPv6,支持多跳 BFD 功能
14.		★QOS 服务要求	完善的 HQoS 机制,每线路板可提供先进调度和拥塞避免技术;
15.			提供精确的流量监管和流量整形功能;
16.			提供定义复杂规则的功能,支持流细粒度鉴别;
17.			支持 MPLS HQoS,全面保证 MPLS VPN、VLL 和 PWE3 的 QoS 调度;
18.			提供基于 DiffServ 和 MPLS TE 的 DS-TE;
19.			支持面向 TE 隧道的 QoS。
20.		NAT 功能要求	地址池方式 PAT; 地址池方式 NOPAT(支持 TCP,UDP,ICMP; 两次 NAT (支持 TCP,UDP,ICMP 以及其他特殊协议连接);
21.		VPN 功能要求	支持 MPLS TE,支持 P2MP-TE/mLDP,支持 MPLS/BGP VPN,符合 RFC2547 协议;
22.			支持三种跨域实现方式,支持与 Internet 业务集成;
23.			支持基于 Martini、Kompella 方式的 MPLS L2 VPN,支持 VPLS/VLL 等多种二层 VPN 技术,支持异种介质互联;
24.			支持组播 VPN;
25.		MPLS 功能要求	支持 MPLS L3 VPN, VRF 数量 $\geq 4\text{K}$
26.		安全要求	支持 ACL 报文过滤;
27.			支持 URPF;
28.			支持 GTSM;
29.			支持 DHCP Snooping;
30.			支持防 ARP 攻击、防 DOS 攻击;

31.			支持 MAC 地址限制、MAC 与 IP 绑定;
32.			支持 SSH、SSH v2;
33.			支持 NetStream 和 IPSec 技术。
34.	高可用及可靠性要求	★电源及风扇要求	支持并配置冗余电源及风扇
35.		★热插拔要求	所有组件可热拔插。
36.		★设备主控引擎要求	冗余主控引擎
37.			主备引擎要求分布在不同槽位
38.		★在线业务升级要求	支持 ISSU 在线业务升级支持
39.		冗余网关协议要求	支持 VRRP
40.	监控及管理要求	管理端口要求	支持 Console、telnet、SSH 等登陆方式;
41.		★登陆方式	支持 telnet、SSHv2 登陆方式, 支持通过命令行、图形化配置软件等方式进行配置和管理。
42.		★网管设备监控要求	支持 SNMPv1、v2、v3, 通过 snmp 直接采集 CPU 使用率/内存利用率、板卡状态、主备工作状态、电源/风扇状态、设备温度等设备运行状态
43.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级
44.			支持向外部 SNMPTrap 服务器发送告警信息, 告警按照对系统影响性进行分级
45.		配置自动备份	提供设备配置自动备份的方法(命令行交互方式或者其他方式), 定期自动备份到外部服务器
46.		★链路关键路径	支持 NQA 等链路检测协议, 确保广域链路发生故障时, 上层的协议能够及时收敛, 减少因链路故障导致的业务中断时间;
47.		认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权
48.		流量分析采集和数据输出要求	支持 NetStream 或类似的流量采集功能
49.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可

		★产品成熟度要求	CPU 芯片须为国产, 产品剩余生命周期不低于 7 年。
--	--	----------	------------------------------

1.4.1.2.3. 硬件防火墙

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	★硬件架构	设备形态≤3U; 支持交流双电源; 支持风扇可插拔;
2.		★端口配置要求	≥8 个 10SFP+ 端口, LC 接口多模模块满配; (以上配置的端口均为实际可用数量, 要求全部同时支持, 不得存在复用端口)
3.	性能及容量指标	★整机性能	吞吐量≥40Gbps 最大并发连接数≥1200 万; 每秒新建连接数≥30 万;
4.		性能指标验证要求	对于以上性能及容量指标, 若用户测试环境没有足够资源进行验证, 原厂商应提供相应的测试环境并由用户现场验证在容量到达指标时的设备运行状态与指标相符
5.	功能性要求	★部署功能要求	必须支持透明、路由、混合、旁路 4 种工作模式
6.		★虚拟防火墙功能	≥32
7.		安全区域功能	支持安全区域管理, 可基于接口、VLAN 划分安全区域
8.		安全策略要求	能够基于时间、用户/用户组、应用层协议、IP 地址、端口、域名组、URL 分类、协议 TCP/UDP/SCTP/ICMP、统一界面进行安全策略配置
9.			支持最大访问策略数量不少于 5000 条。
10.		★三层路由功能要求	支持 IPv4、IPv6 的静态路由
11.			支持基于会话的原路回包功能, 可设置优先于路由策略而通过会话表中的入接口进行回包
12.			支持基于源 IP、目的 IP、服务类型、应用类型、用户(组)、接口、DSCP 优先级的策略路由
13.		IPv6 功能	★支持 IPv6 功能
14.			支持 IPv6 over IPv4 GRE 隧道
15.		★NAT 功能要求	支持双向 NAT, 多对一、一对多、多对多和一对一等多种方式的地址转换

16.		应用层识别要求	具备对应用程序的识别和控制能力。应用程序特征库不少于 5000 种, 并支持在线更新
17.			在国内有应用特征库开发团队, 并提供国内地址的应用升级服务
18.		流量控制要求	可支持基于应用层协议设置流控策略, 包括设置最大带宽、保证带宽、协议流量优先级等
19.			支持流量整形
20.		★防火墙状态同步要求	支持 HA 模式下的状态同步: 包括 Session 同步, NAT 同步, IPSec SA 同步
21.		安全防护要求	抗 DDOS 攻击: 支持抵御下所列所有攻击类型, 包括: DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke
22.			支持对 HTTPS, POP3S, SMTPS, IMAPS 加密流量代理解密后, 并进行内容过滤, 审计, 安全防护
23.		DNS 防护要求	支持 DNS 透明代理
24.			支持 DNS 代理黑白名单功能, 用户可通过该功能过滤域名查询请求, 保护 DNS 服务
25.	高可用及可靠性要求	★电源冗余要求	支持并配置双冗余电源
26.		★双机热备要求	支持主备方式和双主方式的双机热备
27.		版本升级不中断要求	要求支持版本升级实现向下兼容, 支持不中断的版本升级
28.		接口绑定要求	可在透明、路由模式下支持多条链路带宽进行捆绑
29.	监控及管理要求	★管理协议要求	支持 SNMP V1/V2/V3
30.		监控项目要求	支持通过 snmp 直接采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、failover 状态、新建连接数、并发连接数等设备运行状态
31.			支持向外部 syslog 服务器发送日志信息, 日志告警按照对系统影响性进行分级 (对影响设备正常运行的软硬件报错, 如硬件故障、端口翻动、地址冲突、温度等, 以及影响设备运行、容量指标的告警, 如端口、芯片、板卡的丢包、流量冲高超过阈值的监控)

32.		认证及审计要求	支持以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权
33.		流量和分析要求	支持将数据镜像到设备自身的其余接口,用于抓包分析
34.		★时钟同步要求	支持 NTP 时间同步
35.		其他管理要求	具备 WEB 认证功能,可支持本地数据库,以及 LDAP、Radius 和 Windows AD 域联动的第三方认证方式。
36.	其他要求	★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可
		★产品成熟度要求	CPU 芯片须为国产,产品剩余生命周期不低于 7 年。

1.4.1.2.4. 硬件负载均衡

序号	指标分类	技术指标	要求
1.	设备硬件及端口要求	★基本指标	吞吐量 $\geq 40\text{Gbps}$ 4 层并发 $\geq 16\text{M}$ 4 层每秒新建 $\geq 500\text{K}$ 7 层每秒新建 $\geq 600\text{K}$ 每秒新建连接数 TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 $\geq 12000\text{TPS}$ 。 TLS_RSA_WITH_AES256_GCM_SHA384 $\geq 12000\text{TPS}$ 。 ECC-SM2-SM4-SM3 $\geq 8000\text{TPS}$; ECDHE-SM2-SM4-SM3 $\geq 8000\text{TPS}$; 吞吐量 TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 $\geq 5.6\text{Gbps}$ 。 TLS_RSA_WITH_AES256_GCM_SHA384 $\geq 5.6\text{Gbps}$ 。 SSL 最大并发连接数 ≥ 600000 。 支持 SSL 加密,通过将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器。 支持商密 SSL 算法的单向和双向认证,至少包含以下算法: 国密: SM2、SM3、SM4 算法, 商密: RSA、SHA、ECDSA、ECDHE、SHA256、SHA384

			算法。 "支持以下算法： TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384； TLS_RSA_WITH_AES256_GCM_SHA384； TLS_ECC_SM4_SM3。" 支持多级 CA 证书链 "支持各类标准证书的申请和导入, 类型包含： RSA: 1024-bit, 2048-bit, 4096-bit； ECDSA: 256-bit、384-bit； SM2: 256-bit。" 支持 SSL 卸载, 将 SSL/TLS 协议流量解密为明文后再传输至服务器, 以减轻服务器性能压力。 支持 SSL 加密, 通过将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器。 实配支持基于自定义策略的 DNS 解析 DNS 每秒查询能力: $\geq 1500\text{Kqps}$
2.		★端口类型	实配至少 4 个万兆以太网 LC 光口及配套多模模块； 实配至少 4 个 10/100/1000M 以太网电口
3.	高可靠性	★可靠性	实配冗余电源； 实配支持冗余功能: 支持主备方式和双主方式的双机热备； 实配支持连接镜像和会话保持镜像功能；
4.	功能性要求	支持 IEEE 协议	支持 Spanning Tree (IEEE 802.1d)；VLAN (IEEE802.1q)；链路聚合 (IEEE802.3ad) 协议；
5.		★IPv6	支持
6.		★链路负载均衡支持	支持链路负载, 提供针对多条出口线路的链路负载均衡功能, 实现 inbound 和 outbound 流量的均衡调度, 以及链路之间的冗余互备
7.			支持入向链路负载均衡(Inbound)算法, 应包括但不限于以下算法: 轮询算法(RR)、加权轮询算法(WRR)、就近性算法 (PROXIMITY)。(提供界面证明、配置管理手册)
8.		★广域网负载均衡	设备支持广域网负载 GSLB 功能, 且具备全局负载均衡算法, 包括但不限于以下算法: 轮询算法(GRR)、加权轮询算法(VWRR)、连接溢出(GCO)、最小连接数(GLC)、IP 优先(IP0)、全

			局就近性算法 (PROXIMITY)、区域算法 (REGION)、DPS 等算法; 可实现应用级别的健康检查功能,支持数据中心互备
9.		★对域名的负载均衡	要求能配置域名作为后台服务器。应用交付控制器应该根据配置的域名自动定期进行解析,将解析后得到的 IP 地址作为后台服务器。当域名解析的 IP 地址发生变化的时候,能够自动将新解析的 IP 地址作为后台服务器进行负载均衡;
10.		★DNS 防火墙功能	支持对 DNS 协议的安全防护,如防 DNS Flooding; 支持 DNS 缓存,提高对 DNS 请求的相应速度;
11.		统一 DNS 管理	统一 DNS 管理,将智能解析服务和标准 DNS 服务两种功能和二为一;
12.		★管理特性	支持灵活的带宽管理; 实配支持 Console、Telnet/SSH、HTTP/HTTPS 管理方式; 实配支持 SNMP v2/v3 管理方式; 所有实配的功能均可由 SSH 命令行方式完成,提供完整的命令行手册; 实配支持 TACACS+ AAA 认证; 实配支持 NTP 时钟;
13.		★路由协议	实配支持静态 IP 路由, OSPF, RIP V1, RIP V2; 实配支持虚地址的健康路由注入 (Route Health Injection);
14.		虚拟化支持	支持虚拟化负载均衡; 支持对业务端口划分 Vlan,使不同 Vlan 的数据流能够通过被测设备访问目标服务器;
15.	其他要求	原厂实施	软件版本升级时,可无条件获得新软件的许可使用权; 要求配置与其他设备连接的配件; 提供符合 IEC 标准的电源线; 产品必须提供配置清单、设备实配的外观彩页。
16.		★证书要求	具备国家密码管理局商用密码检测中心颁布的《商用密码产品认证证书》,满足 GM/T 0028 要求
17.		★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可

		★产品成熟度要求	CPU 芯片须为国产，产品剩余生命周期不低于 7 年。
--	--	----------	-----------------------------

1.4.1.2.5. 云内防火墙

序号	指标分类	技术指标	要求
1.	性能及容量指标	★整机性能	混合包吞吐量 $\geq 80\text{Gbps}$ 最大并发连接数 ≥ 2500 万； 每秒新建连接数 ≥ 60 万；
2.		性能指标验证要求	对于以上性能及容量指标，若用户测试环境没有足够资源进行验证，原厂商应提供相应的测试环境并由用户现场验证在容量到达指标时的设备运行状态与指标相符
3.		接口要求	接口速率在 10G 以上，需匹配云内整体网络架构设计。
4.	功能性要求	★安全策略要求	能够基于协议、IP 地址、端口、统一界面进行安全策略配置（提供功能截图）
5.			支持最大访问策略数量不少于 5000 条。
6.		★三层路由功能要求	支持 IPv4、IPv6 的路由
7.		★IPv6 功能	支持 IPv6 功能
8.	高可用及可靠性要求	★冗余要求	支持并实配多设备冗余，不存在单点故障，保障网络冗余性。
9.		版本升级不中断要求	要求支持版本升级实现向下兼容，支持不中断的版本升级
10.		集群要求	多设备集群，避免单点故障，保障网络冗余性。
11.	监控及管理要求	管理协议要求	支持 SNMP V1/V2/V3
12.		监控项目要求	支持通过采集 CPU 使用率/内存利用率、电源/风扇状态、设备温度、端口状态/流量/错包、failover 状态、新建连接数、并发连接数等设备运行状态
13.			支持向外部 syslog 服务器发送日志信息，日志告警按照对系统影响性进行分级（对影响设备正常运行的软硬件报错，以及影响设备运行、容量指标的告警，如端口、芯片、板卡的丢包、流量冲高超过阈值的监控）

14.		认证及审计要求	以 RADIUS 或 TACACS 方式的进行 AAA 认证并对命令进行认证、审计和授权
15.		流量和分析要求	支持将数据镜像,用于抓包分析
16.		#时钟同步	支持 NTP 时间同步
17.		其他管理要求	#具备 WEB 认证功能,可支持本地数据库,以及 LDAP、Radius。 ★支持运管平台对接。
18.	其他要求	★特性要求	若使用硬件产品响应,CPU 芯片须为国产,且需每个 VPC 部署独立设备,并符合冗余性要求; 若使用软件产品响应需部署在国产 CPU 芯片的设备中,可为全部 VPC 提供相应功能,同时符合冗余性要求,部署软件产品的设备由投标人提供。
19.		★许可	以上条款所要求配置的端口和功能的应包含涉及的相应许可

1.4.1.2.6.云内负载均衡

序号	指标	要求
1.	★总体要求	提供 4 层 TCP/UDP 和 7 层 HTTP/HTTPS 协议类型的服务。接口速率在 10G 以上,需匹配云内整体网络架构设计。
2.		支持并实配多设备冗余,不存在单点故障,保障网络冗余性。
3.		吞吐量 $\geq 80\text{Gbps}$,四层新建能力 ≥ 50 万 CPS;七层新建能力 ≥ 60 万 RPS。
4.		负载均衡支持 IPv6,支持挂载 IPv4 或 IPv6 的后端应用服务器。
5.	★架构要求	若使用硬件产品响应,CPU 芯片须为国产,且需每个 VPC 部署独立设备,并符合冗余性要求; 若使用软件产品响应需部署在国产 CPU 芯片的设备中,并可为全部 VPC 提供相应功能,同时符合冗余性要求,部署软件产品的设备由投标人提供。
6.	★负载均衡算法	同一套负载均衡集群提供内网和外网两种负载均衡创建模式,支持轮训(RR),加权轮询(WRR)、源 IP 一致性哈希,最小连接数。

7.		1. 支持 tcp 的网络层健康检查 2. 支持对应用接口或域名路径的返回状态码健康检查
8.	★健康检查	1. 支持 HTTP 模式下对应用返回的字符串比对的健康检查 2. 支持 udp 模式下对应用返回的字符串比对的健康检查
9.		支持 DB 返回值的健康检查
10.		支持 websocket 返回值的健康检查
11.	★健康检查与隔离恢复	1. 对服务器池中服务器进行健康检查自动隔离与恢复 2. 对服务器池中服务器进行手动隔离与恢复 3. 对 VS 监听进行手动隔离与恢复
12.	★挂载多种后段服务器	支持挂载虚拟机, 弹性网卡主 IP, 辅助私网 IP, 云内传统网络 IP, 云外 IP
13.	★四层会话保持	四层监听支持轮训 (RR), 加权轮询 (WRR)、源 IP 一致性哈希, 最小连接数下均支持开启基于源 IP 的会话保持
14.	七层会话保持	★七层监听支持轮训 (RR), 加权轮询 (WRR), 最小连接数负载均衡算法下均支持基于 Cookie 植入或重写的会话保持
15.		★基于源 IP 的七层会话保持
16.		★基于 Header 信息的七层会话保持
17.	★端口映射	支持对外提供服务端口与后台服务器端口不一样时, 仍可以进行端口映射
18.	监听转发	支持开启监听转发, 用于将 HTTP:80 监听的流量转发到 HTTPS:443 监听, 以实现 HTTP 协议强制跳转 HTTPS
19.		支持配置转发策略, 支持按域名和 URL 转发
20.	★七层基础调度	基于 HTTP 包头字段的负载均衡转发
21.		基于 HTTP 标头 User-Agent 进行转发
22.	七层高级调度	基于 Cookies 的负载均衡转发
23.		基于 HTTP Method 的负载均衡
24.		基于 HTTP 查询参数进行转发
25.		重写或返回固定响应
26.		隐藏服务器资源信息
27.	★HTTPS 认证	HTTPS 支持单向/双向认证
28.		7 层负载均衡前端协议支持 HTTPS2.0
29.	SSL 卸载	1. 支持卸载 SSL 证书 2. 支持卸载国际证书, 国密证书以及同时配置国际和国密证书
30.	★SNAT 能力	1. 支持源地址转换 (SNAT) 功能 2. 支持通过源地址转换 (SNAT) 解决跨网络区域 (经典 TOVPC) 访问问题 3. 提供在跨网络区域 (经典 TOVPC) 获取客户端真实源地

		址的解决方案
31.	★负载均衡流量转发模式	支持 NAT 隧道 LB 转发模式, 保证流量来回路径一致且后端直接获取真实客户端 IP
32.		支持为数据产品提供客户端-LB-服务端回程流量三角转发模式
33.		支持FAST-BYPATH转发模式负载均衡对部分高性能数据类分布式云产品如为对象存储提供高速转发模式 1. 客户端到服务端的首包经过负载均衡集群 2. 客户端和服务端的后续通信 bypaas 负载均衡代理直接通信 3. 客户端(支持自动重连)和服务端连接失败后支持重新负载均衡并重新建连
34.	★IPV6 能力支持	1. 支持 IPV6 转 IPV6 2. 支持 IPV6 转 IPV4
35.	★四层监听协议后端健康检查	TCP,UDP 监听模式下均支持对后端服务器端口进行健康检测探活以判断应用端口是否 UP,支持设置的健康检查端口和应用主进程服务端口不相同
36.		UDP 监听模式下支持主动向应用发送探测包通过检查自定义内容是否符合自定义预期判断应用程序是否健康
37.		TCP,UDP 监听模式下均支持对后端服务器端口进行健康检测探活以判断应用端口是否 UP,支持设置的健康检查端口和应用主进程服务端口不相同
38.		支持隔离非健康状态的后端服务器并可设置健康检查端口,静态页面,应用健康检查接口,检查周期,超时时间,健康阈值和不健康阈值
39.	★七层监听协议后端健康检查	1. 支持基于网络层的健康检查,能周期性地对目标服务器进行 tcp 协议的健康检查,判断后台服务器的可用状态 2. 支持基于应用层的健康检查,可配置健康检查路径和健康检查域名,通过 HTTP HEAD 方式,周期性地向后台服务器发起请求,并将返回结果与预期结果进行对比,来判断后台服务器的可用状态 3. HTTP/HTTPS 监听模式下均支持对后端服务器端口进行健康检测探活以判断应用端口是否 UP,支持设置的健康检查端口和应用主进程服务端口不相同
40.	获取真实 IP	四层监听模式下后端 realserver 为虚拟网络的虚拟机时,虚拟机操作系统无需额外安装插件即可抓包直接获取真实客户端源 IP 地址
41.		★七层监听模式下在报文中插入附加 HTTP 字段获取高级信息包括但不限于 (1)通过 X-Forward-For 头字段获取客户端真实源 IP 地址

		(2)通过 X-Forward-Proto 头字段获取 LB 的监听协议 (3)通过 Id 头字段获取 LB 实例 ID (4)通过 Ip 头字段获取 LB 实例 IP 地址
42.	内网 GTM 全局负载均衡功能	支持调度线路管理,可根据客户端请求 IP 地址进行分组,不同分组按解析策略解析至不同地址池
43.		支持地址池管理功能,支持地址池内地址健康检查
44.		支持主备地址池设置,主地址池内 ip 健康检查全部或部分失败后,自动切换到备地址池
45.		DNS 设备支持 TCP、UDP、ICMP、HTTP、HTTPS 的健康检查探测功能
46.		智能解析服务通过区分不同的客户端访问源 IP 归属,将域名访问请求根据自定义规则解析返回不同的 IP 地址或 IP 地址池
47.	★监控指标项	支持监控负载均衡器,监控项包括但不限于端口流入和流出带宽、端口新建连接数、端口流入和流出数据包数、端口活跃连接数、端口非活跃连接数、端口并发连接数、端口丢弃连接数、端口丢弃流入数据包数、端口丢弃流出数据包数、端口丢弃流入带宽和端口丢弃流出带宽等
48.	运维排障	1. 支持完善的前后端抓包命令集 2. 支持提供一键故障自动诊断工具 3. 支持健康检查告警
49.	★日志功能	1. 四层和七层均支持日志记录功能 2. 支持在日志平台上设置保存时间,最长保留时间为永久保留 3. 四层和七层均支持提供接口上送日志至司内运维系统
50.	数据统计和报表功能	1. 支持数据统计功能,web 界面可以查看历史 30 天的系统性能数据 2. 支持报表功能

1.4.1.3. ★网络安全设备规格

序号	设备名称	备注
----	------	----

1.	网络入侵防护	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧入侵防护。 3. 软硬件方案皆可。若使用硬件产品响应，CPU 芯片须为国产，若使用软件产品响应需部署在国产 CPU 芯片的设备中，部署软件产品的设备由投标人提供。
2.	Web 应用防火墙	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧 web 应用安全防护。 3. 软硬件方案皆可。若使用硬件产品响应，CPU 芯片须为国产，若使用软件产品响应需部署在国产 CPU 芯片的设备中，部署软件产品的设备由投标人提供。
3.	网络未知威胁检测	1. 旁路部署，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及租户侧未知威胁检测。 3. 软硬件方案皆可，硬件方案需支持将云内流量（含云边界和云内南北向流量）镜像至硬件平台（例：网络分路器）。若使用硬件产品响应，CPU 芯片须为国产，若使用软件产品响应需部署在国产 CPU 芯片的设备中，部署软件产品的设备由投标人提供。
4.	数据加密	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于平台侧及用户侧数据加密。 3. 软硬件方案皆可。若使用硬件产品响应，CPU 芯片须为国产，若使用软件产品响应需部署在国产 CPU 芯片的设备中，部署软件产品的设备由投标人提供。
5.	密钥管理系统	1. 系统采用高可用架构，可采用集群部署模式满足农信银云性能要求。 2. 用于密钥管理服务。 3. 软硬件方案皆可。若使用硬件产品响应，CPU 芯片须为国产，若使用软件产品响应需部署在国产 CPU 芯片的设备中，部署软件产品的设备由投标人提供。

1.4.1.4. ★存储资源池配置

1.4.1.4.1. 基本要求

每个数据中心配置 4 个存储资源池，分别为 2 个块存储资源池、1 个对象存储资源池、1 个文件存储资源池，投标

人所投产品需满足 1.4.1.1 章节服务器规格要求，并在此要求基础上，按照后续章节具体要求进行配置。

鉴于硬盘制造商的特殊度量标准，硬盘的实际可用容量小于标称容量（以 3.2TB 的固态盘为例，实际可用容量小于 3TB）。为保证招标人权益，1.4.1.4 章节所提到存储资源池的容量均为实际可用容量。

1.4.1.4.2.块存储资源池

1. 设计要求：建设 2 个全闪存块存储资源池，存储资源池 ≥ 3 副本。单个资源池存储容量不少于 450TB（三副本前）和 150TB（三副本后），物理服务器数量不少于 9 台。

2. 配置需求：

序号	配置项	配置需求
1.	台数	不少于 9 台，所有服务器配置一致。
2.	基础规格要求	满足 1.4.1.1.2 章节存储型服务器规格 A 配置要求
3.	其他要求	许可覆盖所有实配容量

1.4.1.4.3.对象存储资源池

1. 设计要求：建设一个对象存储资源池，采用 3 副本或 EC 模式，每个资源池存储容量不少于 300TB（用户实际可用），存储资源池物理服务器数量不少于 6 台。

2. 配置需求：

序号	配置项	配置需求
1.	台数	不少于 6 台，所有服务器配置一致。
2.	基础规格要求	满足 1.4.1.1 章节存储型服务器规格 A 或存储型服务器规格 B 配置要求
3.	其他要求	许可覆盖所有实配容量

1.4.1.4.4. 文件系统存储资源池

1. 设计要求：建设一个文件系统存储资源池，采用 3 副本或 EC 模式，每个资源池存储容量不少于 100TB（用户实际可用），存储资源池物理服务器数量不少于 4 台。

2. 配置需求：

序号	配置项	配置需求
1.	台数	不少于 4 台，所有服务器配置一致。
2.	基础规格要求	满足 1.4.1.1 章节存储型服务器规格 A 或存储型服务器规格 B 配置要求
3.	其他要求	许可覆盖所有实配容量

1.4.1.5. ★业务计算资源池配置

本项目平台配置 2 类业务计算资源池，分别为虚拟化资源池、裸金属资源池，投标人所投产品需满足 1.4.1.1 章节服务器规格要求。

1.4.1.5.1. 虚拟化资源池

需求如下：

序号	配置项	配置需求
1.	基础规格要求	兼容服务器规格 1.4.1.1 中列出的相关型号
2.	许可数量	100 个(有 50 个用于招标人已采购的联想服务器)
3.	架构要求	可根据 CPU 架构、服务器数量等划分集群
4.	其他要求	1. 投标人不得在配置方案中挪用招标人已有服务器； 2. 兼容 1.4.1.1.5 章节中指定用途规格的服务器，若配置不满足云厂商技术要求，投标人需提供改造需要的服务器原厂零配件（含 5 年原厂金牌维保服务），并包含在投标报价中。

1.4.1.5.2.裸金属资源池

需求如下:

序号	配置项	配置需求
1.	基础规格要求	兼容服务器规格 1.4.1.1 中列出的所有型号
2.	许可数量	100 个 (使用招标人已采购的服务器)
3.	其他要求	1. 投标人不得在配置方案中挪用招标人已有服务器; 2. 兼容 1.4.1.1.5 章节中指定用途规格的服务器, 若配置不满足云厂商技术要求, 投标人需提供改造需要的服务器原厂零配件 (含 5 年原厂金牌维保服务), 并包含在投标报价中。

1.4.1.6. 云底座资源要求

1.4.1.6.1. 设计要求

云底座资源从逻辑上包括网络服务资源池、安全服务资源池、云管资源池等, 各资源池采用虚拟化方式或裸金属方式由投标人具体方案决定, 4 个资源池说明如下:

类别	资源池	业务用途	合计
云底座	云管资源池	本地云管和资源调度等管理组件部署, 支撑统一登录、监控、告警、可视化、资源调度等管理控制服务。	1 套
	网络服务器资源池	部署各类软件定义的网络服务, 主要包括网络控制、虚拟路由交换服务、虚拟防火墙、NAT 网关、VPC 网关等各类网关服务、弹性 IP 和软负载服务等。	1 套
	安全服务资源池	该种服务器不同的配置类型不应超过三种 部署各类软件定义的安全服务, 包括安全运营中心、入侵防护、威胁检测、应用防火墙、堡垒机等, 服务器配置和规模按需部署。	1 套
	PaaS 服务资源池	部署 PaaS 层各类软件, 主要包括微服务平台、数据库、数据库同步工具、容器、分布式缓存、API 网关等	1 套

上述云底座资源池划分方式为逻辑划分，投标人可根据自身最佳实践进行技术方案设计，不用严格区分上述资源池，云底座相关功能、资源可以混合部署，但不得使用业务资源池相关资源。

1.4.1.6.2.★配置要求

云底座资源采用服务器基础规格应统一，云底座资源服务器配置需求如下表。

云管资源池、PaaS 服务资源池：

序号	配置项	配置需求
1.	★数量	由投标人整体方案决定，本次 实配 的云底座类设备配置及数量应满足支持不少于 500 台计算类物理服务器的规模，后续通过横向扩容应能够支持 3000 台计算类物理服务器的规模。
2.	★基础规格要求	按需使用 1.4.1.1.1 及 1.4.1.1.4 中列出的服务器，若招标人对某采购项有特定要求，以特定要求为准。

安全服务资源池：

序号	配置项	配置需求
1.	★高可用性要求	部署的安全服务要求提供高可用性，且不同的安全服务之间不共享物理服务器资源。
2.	★基础规格要求	按需使用 1.4.1.1.1 及 1.4.1.1.4 章节中的服务器，若招标人对某采购项有特定要求，以特定要求为准。

网络服务资源池：

序号	配置项	配置需求
1.	★数量	由投标人整体方案决定，本次 实配 的云底座类设备配置及数量应满足支持 500 台计算类物理服务器、的规模，后续通过横向扩容应能够支持 3000 台计算类物理服务器的规模。
2.	★基础规格要求	按需使用 1.4.1.1.1 及 1.4.1.1.4 中列出的服务器，若招标人对某采购项有特定要求，以特定要求为准。

1.4.1.7. ★网络安全服务要求

本项目云平台安全需要接入农信银已有的堡垒机、漏洞扫描、主机安全、签名验签、加密机等系统（对于密评要求，需满足对接农信银加密机），农信银已有的安全系统清单如下表：。

序号	设备名称	数量	备注
1.	堡垒机	——	1. 满足云平台数据中心运维安全审计要求（本地数据中心系统已完成旁路部署）。 2. 用于平台内基础资源的安全管控，包含网络策略收敛改造费用。 3. 使用农信银现有堡垒机系统（品牌：江南科友），集成方案需说明满足要求的前置条件。
2. 2	漏洞扫描	——	1. 满足云平台数据中心漏洞扫描要求（本地数据中心系统已完成旁路部署）。 2. 用于平台侧及用户侧漏洞扫描服务，包含网络策略收敛改造费用。 3. 使用农信银现有漏洞扫描系统（品牌：长亭科技），系统集成方案需说明满足要求的前置条件。
3.	主机安全	——	1. 满足云平台数据中心主机安全（本地数据中心系统已完成旁路部署）。 2. 用于平台侧主机及终端安全管控服务，包含网络策略收敛改造费用。 3. 使用农信银现有主机威胁检测系统（品牌：长亭科技），集成方案需说明满足要求的前置条件。
6.	数据加密	——	1. 满足云平台数据中心数据安全（本地数据中心系统已完成旁路部署）。 2. 用于平台侧及用户侧数据加密服务，包含系统平台对接、网络策略收敛改造费用。 3. 使用农信银现有加密机、签名验签平台，集成方案需说明满足要求的前置条件。

1.4.1.8. ★备份对接设备要求

投标人须实配若干台备份一体机（或同等功能设备），与招标人的磁带库对接（磁带库配置见 1.8.2），数量不少于 2 台，满足高可用要求。

该设备可不被云平台纳管，但须接入云平台网络，能进行云内主机与裸金属的文件备份。客户端许可不少于 700 个。单台设备须满足：

序号	规格		设备
			指标要求
1.	CPU	CPU 数量	配置≥2 颗
2.		CPU 类型	须为国产 CPU，ARM 或 X86 架构
3.	内存	内存槽	配置 DDR4 或 DDR5 RDIMM 内存，内存容量≥256GB。
4.	硬盘 I/O	硬盘槽位	支持≥12 个硬盘槽位
5.		硬盘容量	配置若干块数据盘，raid6 后可用容量≥100TB，并配置≥100TB 容量许可。
6.		HBA	配置≥4 个 16Gb FC HBA 端口
7.		RAID	至少支持 RAID6
8.	网络	以太网通道	配置≥8 个 25G 网口； 配置≥2 个千兆网口

9.	管理	管理	1. 支持通过图形化向导管理界面按设定好的步骤完成备份管理服务端的账号生成、存储池创建、系统自备份的配置，客户端注册和客户端权限划分等功能的开通，减少服务端部署的初始化复杂度，多台备份一体机可组成集群，集群中一台或多台服务器无法提供服务时剩余正常备份一体机可接管所有备份任务。 2. WEB 管理界面支持多语言，支持告警功能：依据预先设定的告警条件，当备份软件，备份任务，备份存储设备等发生异常时，触发告警提示，或邮件告警通知，支持报表统计和报表导出功能：报表数据来源涵盖作业，作业数量，作业历史，备份成功率，警报，存储资源等。
10.	兼容性	软硬件兼容性	1. 支持本项目云厂商提供的数据库的备份恢复； 2. 支持招标人已有数据库的备份恢复，详细列表见 1.8.3 章节； 3. 虚拟化支持：支持 KVM 平台。

11.	其他功能	其他功能	1. 重复数据删除：支持源端重删和目标端重删技术，支持固定块、变长块的数据重删技术。 2. 文件支持：支持在线文件备份，包含：全量备份、增量备份与合成备份。支持对单文件/目录进行细颗粒度的合成备份和恢复。 3. LAN_Free 功能：支持采用 LAN-Free 方式对文件，数据库，操作系统和虚拟化平台进行数据备份，支持 D2D2T 模式。 4. 远程复制功能：支持备份数据的远程复制，通过使用灾备端的备份数据恢复应用系统，以及本机或异机上的恢复。支持对远程复制设置带宽上限设定，数据传输加密，断线重连等规则，支持将重复数据删除后的备份数据直接复制到容灾端存储。 5. 支持多通道技术，备份通道数设置范围为 1~255，可根据客户端资源情况调整备份通道数量。可接入客户机数量不受限制。 6. 支持将备份一体机中备份的数据归档至磁带库中，并从磁带库中恢复数据。 7. 支持对象存储、Hadoop HDFS 的在线备份和恢复。
12.	电源	电源、风扇	电源冗余，通过 80plus 白金认证，按需配置电源线；风扇冗余。
13.	维保	维保服务	提供≥5 年原厂金牌 7x24H 设备保障和技术支持服务

1.4.2. IaaS 详细需求

1.4.2.1. 配置要求

本功能需求配置，相关软件授权应满足本项目本期建设全部建设规模需要，内容包含但不限于如下需求：

序号	服务名称	简述
1.	★云主机服务	云主机服务为用户提供一种可弹性伸缩的计算服务，根据业务需要，用户可随时创建或释放任意多台云主机，提升运维效率。

2.	★裸金属服务	裸金属是云平台可以为用户提供的独享高性能物理裸机,用户拥有完全的物理设备管理权限,同时可以结合弹性公网 IP 等灵活组网,并与云主机服务内网互通,灵活应对用户多种复杂场景的业务要求。
3.	★弹性伸缩服务	弹性伸缩是用户根据业务要求,通过策略自动调整其业务资源的服务。用户可以根据业务要求自行定义伸缩策略,从而降低人为反复调整资源以应对业务变化和负载高峰的工作量,节约资源和人力运维成本。
4.	★镜像服务	镜像是一个包含了软件及必要配置的云主机或裸金属服务器模版,包含操作系统或业务数据,还可以包含应用软件(例如,数据库软件)和私有软件。
5.	★云硬盘服务	云硬盘服务是一种安全可靠的弹性存储服务,作为云主机的扩展存储部件,为云主机数据存储提供高可用、高容量存储服务。
6.	★文件存储服务	弹性文件服务提供按需扩展的高性能文件存储,为弹性云主机,容器,裸金属服务器提供共享访问。
7.	★对象存储服务	对象存储服务提供稳定、安全、高效以及高扩展存储服务,支持文本、多媒体、二进制等任何类型的数据存储,支持数据多地域跨集群的存储。
8.	★分布式块存储服务	分布式块存储指通过存储系统软件将服务器本地存储资源组织起来,构建全分布式存储池,通过标准接口对外提供块存储云硬盘服务
9.	★云备份服务	云备份服务提供云内数据备份,含云主机操作系统内目录、文件的备份。
10.	★虚拟私有网络服务	虚拟私有网络服务 VPC(Virtual Private Cloud) 是一个用户能够自定义的虚拟网络。通过 VPC,用户可以灵活设置网络地址空间,实现私有网络隔离,多个虚拟网络之间(同城、跨城)稳定高速对等互通。

11.	★弹性负载均衡服务	弹性负载均衡服务通过将同一区域的多台云主机虚拟成一个组,设置一个内网或外网的服务地址,将前端并发访问转发给后台多台云主机服务器,实现应用程序的流量均衡,性能上实现业务水平扩展。负载均衡服务还通过故障自动切换及时地消除服务的单点故障,提升服务的可用性。
12.	★弹性 IP 服务	弹性 IP (EIP) 为用户提供弹性的云外网络带宽服务。
13.	★云解析服务	云解析服务,是基于高性能 DNS 系统和 IP 调度技术,提供稳定、高效、安全灵活的 DNS 解析以及流量调度服务,包含内网 DNS 服务。
14.	★NAT 网关服务	NAT 网关 (NAT Gateway) 为虚拟私有云内的云主机服务、裸金属服务,或者通过云专线/VPN 接入虚拟私有云的本地数据中心的服务器,提供网络地址转换服务,使多个云主机、裸金属、本地服务器可以共享弹性公网 IP 访问 Internet 或使其提供互联网服务。
15.	★跨地域 VPC 互通服务	跨地域 VPC 互通服务为用户提供一种能够快速构建跨区域 VPC 之间以及云上多 VPC 与云下多数据中心之间的高速、优质、稳定的网络能力。
16.	★云专线服务	云专线为用户搭建本地数据中心与云上 VPC 之间的专属连接通道。
17.	★支持 VPN 服务	虚拟专用网络服务 (Virtual Private Network, 以下简称 VPN), 用于在远端用户和虚拟私有云 VPC 之间建立一条安全加密的公网通信隧道。当用户作为远端用户需要访问 VPC 的业务资源时,用户可以通过 VPN 连通 VPC。
18.	★IPV6 支持	硬件设备和软件产品须支持 IPV6。

1.4.2.2. 性能要求

整体性能要求:

序号	指标名称	指标要求
1.	★单 AZ 能纳管的物理节点规	≥3000

序号	指标名称	指标要求
	模	
2.	单台云主机创建耗时	≤100s
3.	★单台云主机快照恢复耗时	≤2 分钟
4.	★租户自助创建一个裸金属实例耗时	≤60 分钟
5.	★云硬盘单盘创建耗时	≤10s
6.	云硬盘单盘快照创建耗时	≤1 分钟
7.	云硬盘单盘快照恢复耗时	≤1 分钟

云硬盘性能：

序号	云硬盘类型	高性能云硬盘
1.	★访问时延	小于 5ms
2.	★磁盘大小	1GB-10TB
3.	★数据可用性	99.99%
4.	★单盘最大吞吐	150MB/s
5.	★单盘 IOPS	≥6000

网络性能：

序号	云服务	指标名称	要求
1.	★虚拟私有网络服务	VPC 内虚拟机互通网络延时	≤3ms
2.		VPC 间虚拟机互通网络延时 (含云内防火墙)	≤5ms
3.	★弹性负载均衡服务	四层最大并发链接数	50 万 CPS
4.		七层最大并发链接数	60 万 CPS
5.		数据请求分发延迟	≤2ms
6.	★DNS	域名解析 QPS	70000QPS

应用性能要求：

序号	指标名称	要求
1.	承载应用交易并发数	类似如下场景：按照单个单元配置：1 台流水数据库（10C，132G），5 台 bap 节点虚机器（10C、32G）组成 1 个单元，单个单元并发交易量 ≥1000TPS，随着单元数扩容，平台可支持并发数 ≥10000TPS

2.	★通用交易链路平均耗时（仅云平台内部）	类似如下场景：交易链路通过 外联网关节点->业务处理节点->数据库节点->内联网关节点 整体耗时<50ms
3.	★云平台内部节点间通讯平均耗时	<5ms

1.4.2.3. 功能要求

需提供如下 IaaS 云服务，包括但不限于：云主机、裸金属、弹性伸缩、镜像服务、云硬盘、文件存储、对象存储、分布式块存储、虚拟私有云、备份、弹性负载均衡、弹性 IP、云解析、NAT 网关、跨地域 VPC 互通、云专线、IPV6 等服务能力，并支持 VPN 服务能力。

1.4.2.3.1. 云主机服务

序号	指标名称	要求	备注
1.	★创建、删除、启动、关闭、查看	用户可以创建、删除、启动、关闭、查看（含批量）云主机。	
2.	★调整规格	用户可以根据业务需要，进行规格变更，升级、降级 vCPU、内存。	
3.	★挂载/卸载磁盘	云主机创建成功后，可以根据要求，将已有云硬盘挂载给云主机，或创建新的磁盘，然后再挂载至云主机。同时，也可将磁盘从云主机中卸载。	
4.	★挂载/卸载网卡	可为云主机挂载多个网卡。也可将已经挂载在云主机中的网卡卸载。	

5.	# 标 签 管 理	为云主机添加标签，可以方便用户识别和管理拥有的云主机资源。	
6.	★反亲和性	反亲和性指的是同一组云主机尽量分散地创建在不同的宿主机上，提高业务的可靠性。	
7.	★用户数据注入	在创建云主机时，应提供用户初始化的能力	
8.	★密码和密钥对	云主机登录时需要进行身份验证，可以通过密码、密钥对来完成。用户可以对密码进行重置。	
9.	★配置、更改安全组	安全组创建后，用户可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云主机出入方向网络流量进行访问控制，当云主机加入该安全组后，即受到这些访问规则的保护。	
10.	★云主机冷/热迁移	支持云主机冷/热迁移，支持批量迁移。运维人员可以手工指定迁移任务的带宽限制，降低迁移流量对正常业务的干扰。	
11.	★宕机疏散	当承载云主机的节点发生宕机时，平台应有将该节点上的云主机自动疏散至其它节点的能力。	
12.	# 云 主 机 备 份	当服务器出现故障或者人为错误导致数据误删时，可以自助快速恢复数据。支持基于多云硬盘一致性快照技术的备份服务，并支持利用备份数据恢复服务器数据。同时支持全量备份和增量备份。	
13.	★云主机快照	云平台支持用户对已创建的虚拟机实例进行全量或增量快照备份服务，并提供多种备份策略。用户可以根据已有快照恢复已创建的虚机实例，或创建新的虚机实例。	

14.	★服务器兼容	支持部署通用 X86、国产 ARM 和 X86 服务器。	
-----	--------	------------------------------	--

1.4.2.3.2.裸金属服务

序号	指标名称	要求	备注
1.	★裸金属管理	支持创建、删除、启动、关闭纳管的裸金属服务器设施。	
2.	#裸金属纳管	支持纳管用户已经部署的物理服务器	
3.	★重装操作系统	提供重装裸金属服务器的操作系统能力。重装完成后：裸金属服务器系统盘的磁盘类型不变（仅限快速发放裸金属服务器）。裸金属服务器的 IP 地址不变。	
4.	★密钥对与密码	支持密钥对或密码的方式进行登录	
5.	★操作系统支持	支持银河麒麟 V10，支持统信 V20 1060 系列等常见镜像	
6.	#IP 配置	支持手动指定 IP 地址，支持单网卡配置多个同网段 IP 地址。	

1.4.2.3.3.弹性伸缩服务

弹性伸缩服务功能包括但不限于以下内容：

序号	指标名称	要求	备注
1.	★伸缩组生命周期管理	支持创建，修改，删除，启停，查询伸缩组	
2.	★设置最大、最小、期望实例数	支持设置伸缩组最大实例数和最小实例数，保证伸缩组在任何情况下，实例数均不会超过最大实例数和最小实例数的范围，同时可以使伸缩组的实例数始终自动保持和期望实例数相同	
3.	资源标签	资源标签，通过标签的形式将自定义数据分配给每个伸缩组内的虚拟机，可以对组内的虚拟机进行组织和管理	

4.	★伸缩配置生命周期管理	支持创建、查询、删除伸缩配置	
5.	★伸缩策略生命周期管理	创建、修改、删除、启停、查询伸缩策略,	
6.	★伸缩策略动作定义	伸缩策略支持定义触发动作, 可设置增加, 减少	

1.4.2.3.4. 镜像服务

镜像服务的功能包括但不限于以下内容:

序号	指标名称	要求	备注
1.	查询镜像列表	根据不同条件查询镜像列表信息	
2.	★镜像生成	可通过云主机、快照、云硬盘制作镜像	
3.	★镜像导出	用户可以将自己的私有镜像导出到本地, 或导出至对象存储再下载至本地。	
4.	★私有镜像	支持对云主机、系统盘、数据盘, 制作成自定义镜像, 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据, 可用于快速发放包含用户业务数据的新弹性云主机。	
5.	★公共镜像	包含常见的操作系统, 能够提供简单方便的镜像自助管理功能, 对所有用户可见。	
6.	自定义镜像上传	用户可以上传自定义的镜像	
7.	★国产操作系统支持	支持银河麒麟、统信等操作系统	

1.4.2.3.5.云硬盘服务

云硬盘服务的功能包括但不限于以下内容:

序号	指标名称	要求	备注
1.	★云硬盘	支持创建、删除、查看、挂载、卸载	
2.		支持在线扩容	
3.		支持基于已有云硬盘创建云硬盘快照/备份,支持通过云硬盘快照/备份回滚源云硬盘,支持通过云硬盘快照/备份创建新云硬盘	
4.		支持不同的后端存储介质(如 SATA 与 SSD 盘混合、纯 SSD 盘),云硬盘服务应具备提供多种不同性能规格的云硬盘类型的能力	
5.		支持云硬盘备份的后端数据存储池不同于云硬盘本身的后端数据存储池	

1.4.2.3.6.文件存储服务

功能包括但不限于以下内容:

序号	指标名称	要求	备注
1.	★弹性文件存储服务	支持创建、删除、查看、挂载、卸载等操作	
2.		支持 NFS 等主流协议,为弹性云服务器提供跨 AZ 和 VPC 的文件访问,支持多个弹性云服务器并发访问;	
3.		支持访问权限控制,支持文件系统访问规则的添加、修改、删除	

1.4.2.3.7.对象存储服务

对象存储服务的功能包括但不限于以下内容:

序号	指标名称	要求	备注
1.	对象存储	★支持多重冗余分布式架构,避免单点故障隐患;	
2.		★支持数据 SSL 加密传输,控制每个单独文件的读写权限,并支持数据完整型校验;	

3.		★提供界面、命令行、API 等多种途径对存储对象进行批量操作；	
4.		★支持文件追加上传、断点续传下载。	
5.		★支持存储桶的创建、列表、查看、删除	
6.		★支持对象的上传、列举、删除	
7.		支持通过桶策略、对象策略、acl 规则等方式对存储桶和对象的访问权限进行管理	
8.		★支持服务端加密	
9.		★支持多版本控制	
10.		★支持日志管理	
11.		★支持生命周期管理	
12.		支持云监控上展示流量统计和请求次数等指标	

1.4.2.3.8.块存储服务

分布式块存储服务的功能包括但不限于以下内容：

序号	指标名称	要求	备注
1.	分布式块存储服务	★支持 SSD、SSD+SSD 和 HDD 等多种规格分布式存储，以满足不同业务场景需求；	
2.		★支持弹性可扩展，可在线扩容存储容量，满足业务数据扩容需求；	
3.		★支持多副本冗余，能够保证任何一个副本故障时快速进行数据迁移恢复，避免单一硬件故障导致数据丢失；	
4.		★支持主动隔离，当出现单节点或单块硬盘故障时，自动将其从集群内隔离出来；	
5.		支持对接不同类型计算资源域，包括弹性云服务器资源域。	
6.		支持日志管理	
7.		★支持生命周期管理	
8.		支持云监控上展示流量统计和请求次数等指标	

1.4.2.3.9.虚拟私有网络服务

虚拟私有网络服务功能包括但不限于以下内容：

序号	指标名称	要求	备注
----	------	----	----

1.	★私有网络	应支持创建私有网络、修改私有网络基本信息、删除私有网络。	
2.	★子网	子网是虚拟私有云下管理云资源的网络平面，云资源都部署在子网内。应支持为虚拟私有云创建新的子网、修改子网网络信息和删除子网。	
3.	★路由表	路由表中定义路由规则，路由规则用于将目标网段的流量路由至指定的目的地。支持添加自定义路由规则，将指定目标网段的流量路由至指定目的地。云系统应提供管理路由表的功能：如添加自定义路由、查询路由、修改路由和删除路由。	
4.	★安全组	应提供管理安全组和安全组规则的功能：创建安全组、删除安全组、添加安全组规则、快速添加多条安全组规则、复制安全组规则、修改安全组规则、删除安全组规则、查看弹性云主机的安全组、变更弹性云主机的安全组、云资源加入/移出安全组等，并支持批量导入导出安全组规则。	
5.	★网络 ACL (虚拟防火墙服务)	网络 ACL 是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。应提供管理网络 ACL 和网络 ACL 规则的功能并支持批量导入导出规则。	
6.	★对等连接	对等连接是指两个 VPC 之间的网络连接。应支持用户可以使用私有 IP 地址在两个 VPC 之间进行通信，就像两个 VPC 在同一个网络中一样。同一区域内，用户应可以在自己的 VPC 之间创建对等连接，也可以在自己的 VPC 与其他帐户的 VPC 之间创建对等连接。应可以创建同一账户或不同账户下的对等连接，查看、修改、删除对等连接，查看和删除对等连接路由等。同时支持跨 region 的对等连接。	

1.4.2.3.10. 备份服务

序号	指标名称	要求	备注
----	------	----	----

1.	★ 备份类别	支持备份云主机操作系统内的文件、目录	
2.	★ 备份目的地	支持备份到文件系统存储或对象存储	

1.4.2.3.11. 弹性负载均衡服务

弹性负载均衡服务功能包括但不限于以下内容：

序号	指标名称	要求	备注
1.	★支持公网和私网负载均衡	公网负载均衡器可通过公网 IP 对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端云主机进行处理。私网负载均衡器通过私网 IP 对外提供服务，将来自同一个 VPC 的客户端请求按照指定的负载均衡策略分发到后端进行处理。	
2.	★支持轮询/最少连接/源 IP 分发策略	负载均衡应支持轮询、最小连接、加权轮询、加权最小连接和源 IP 等算法。	
3.	★支持四层（TCP/UDP）和七层负载均衡（HTTP/HTTPS）	四层负载均衡：支持 TCP 和 UDP 协议，监听器收到访问请求后，将请求直接转发给后端服务器。七层负载均衡：支持 HTTP 和 HTTPS 协议，监听器收到访问请求后，需要识别并通过 HTTP/HTTPS 协议报文头中的相关字段，进行数据的转发。七层负载均衡应支持加密传输、基于 Cookie 的会话保持等高级功能。	
4.	★支持会话保持	会话保持功能应可以识别客户与服务器之间交互过程的关联性，在作负载均衡的同时，还保证一系列相关联的访问请求会保持分配到同一台服务器上。	

5.	★支持按域名和 URL 转发	通过添加转发策略支持自行设定的域名和 URL, 将来自不同域名或者不同 URL 的请求转发到不同的后端服务器组处理。此功能应支持协议类型为 HTTP、HTTPS 的监听器。	
6.	★支持访问控制	支持通过添加白名单的方式控制访问负载均衡的监听器的 IP, 能够设置允许特定 IP 访问, 而其他 IP 不许访问。	
7.	支持后端服务器为裸机	后端服务器应支持裸金属服务器。	
8.	支持双向认证	支持对通信双方的身份都做认证, 以确保业务的安全性。除了配置服务器的证书之外, 还需要配置客户端的证书, 以实现通信双方的双向认证功能。	
9.	支持按监听器粒度监控相关指标	云平台提供的云监控服务, 可以对弹性负载均衡器的运行状态进行日常监控。用户可以通过管理控制台, 直观地查看弹性负载均衡器的各项监控指标。	
10.	★HTTP 重定向到 HTTPS	支持将 HTTP 访问重定向至 HTTPS, 客户端 HTTP 的访问请求, 后端服务器返回 HTTPS 的响应。	
11.	跨可用区流量分发	支持将业务流量分发到不同可用区的云主机。	
12.	★负载均衡器管理	创建、修改、启停、删除、查看负载均衡器	
13.	监听器管理	创建、修改、删除、查看。	
14.	后端服务器管理	添加、修改、删除、查看后端服务器, 允许添加 IP 地址。	

15.	健康检查管理	通过健康检查来判断后端服务器是否可用。对于四层（TCP）和七层（HTTP/HTTPS）监听器，用户可以配置 TCP 健康检查；对于四层（UDP）监听器，默认配置 UDP 健康检查；对于四层（TCP）和七层（HTTP/HTTPS）监听器，用户可以配置 HTTP 健康检查；添加、关闭健康检查，支持端口、检查周期、超时时间、检查路径、最大重试次数等配置。	
16.	★证书管理	支持两种类型的证书，服务器证书和 CA 证书。创建、更换证书，查看证书关联的监听器等。	
17.	标签管理	通过给云资源打标签，快速查找具有某标签的云资源，可对这些资源标签统一进行检视、修改、删除等操作，方便用户对云资源的管理。为负载均衡器、监听器等添加标签，修改和删除标签。	

1.4.2.3.12. 弹性 IP 服务

弹性 IP 服务功能包括但不限于以下内容：

序号	指标名称	要求	备注
1.	★绑定/解绑到云主机	绑定到云主机,实现云主机连接公网,并支持解绑。	
2.	绑定/解绑到裸金属	绑定到裸金属,实现裸金属连接公网,并支持解绑。	
3.	★绑定/解绑到 NAT 网关	绑定到 NAT 网关, NAT 网关通过与弹性公网 IP 绑定,可以使多个云主机(弹性云主机、裸金属服务器、云桌面等)共享弹性公网 IP 访问 Internet 或使云主机提供互联网服务,并支持解绑。	
4.	上下行带宽配置	支持配置上下行带宽限制。	

1.4.2.3.13. 云解析服务

云解析服务功能包括但不限于以下内容:

序号	指标类别	指标名称	要求	备注
1.	公网域名解析	公网域名	DNS 服务应支持托管通过域名注册商注册的域名, 并为域名提供 Internet 网络的解析服务。DNS 提供创建、修改、删除、查看公网域名等基本操作。	
2.		域名级别	DNS 服务应支持创建的域名级别为主域名以及主域名的一级子域名。如果域名后缀为一级 (例如 .com), 支持创建主域名 (例如 example.com)、子域名 (www.example.com); 如果域名后缀为两级 (例如 .com.cn), 支持创建主域名 (例如 example.com.cn)、子域名 (例如 www.example.com.cn)	
3.		记录集	记录集是一组资源记录, 用于定义域名的解析类型以及解析值。DNS 服务应支持为公网域名添加 A、CNAME、MX、AAAA、TXT、NS 以及 PTR 等类型的记录集, 还支持修改、删除、查看、暂停以及启用记录集。	
4.		域名找回	当域名已经被其他租户创建时, DNS 应支持域名所有者找回域名。	
5.		泛解析	DNS 服务应支持为主域名的所有子域名添加记录集, 为所有子域名提供解析服务。	
6.		TTL	DNS 服务应支持设置解析记录在本地 DNS 服务器的缓存时间。	
7.		权重	当域名有多条某一类型的解析记录时, DNS 服务应支持根据权重数值选择解析记录, 权重数值越高, 优先级越高。	
8.		批操作	DNS 服务应支持批量删除域名列表中的公网域名。	

9.	★ 内网域名解析	内网域名	DNS 服务应支持创建在关联 VPC 内生效的内网域名，并为域名提供内网 DNS 解析服务。DNS 提供创建、修改、删除、查看内网域名等基本操作。	
10.		关联 / 解关联 VPC	DNS 服务应支持为内网域名关联或者解关联 VPC。	
11.		记录集	记录集是一组资源记录，用于定义域名的解析类型以及解析值。DNS 服务应支持为内网域名添加 A、CNAME、MX、AAAA、TXT、PTR 等类型的记录集，还支持修改、删除以及查看记录集。	
12.		泛解析	DNS 服务应支持为内网域名的所有子域名添加记录集，为所有子域名提供解析服务。	
13.		TTL	DNS 服务应支持设置解析记录在本地 DNS 服务器的缓存时间。	
14.		批操作	DNS 服务应支持批量删除域名列表中的内网域名。	
15.	★ 反向解析	反向解析	DNS 服务应支持通过弹性 IP 获取该 IP 地址指定域名的反向解析服务。DNS 服务提供创建、修改以及删除反向解析。	
16.		TTL	DNS 服务应支持设置解析记录在本地 DNS 服务器的缓存时间。	
17.	权限	权限管理	用户可以使用统一身份认证服务对其所拥有的云解析服务进行权限管理，以满足企业基于组织划分、职能划分设置不同的访问权限。	
18.	配额	配额调整	为防止资源滥用，云平台应限定各类资源的配额，对用户的资源数量和容量做限制。如用户最多可以创建多少公网域名、内网域名、记录集或者反向解析。如果当前资源配额限制无法满足使用需要，支持用户申请扩大配额。	

1.4.2.3.14. NAT 网关服务

NAT 网关服务功能包括但不限于以下内容：

序号	指标名称	要求	备注
1.	★SNAT	支持 SNAT, 支持多个云主机通过同一公网 IP 主动访问互联网。	
2.	★DNAT	支持 DNAT, 支持绑定到 NAT 网关, NAT 网关通过与弹性公网 IP 绑定, 可以使多个云主机 (弹性云主机、裸金属服务器等) 共享弹性公网 IP 访问 Internet 或使云主机提供互联网服务。	
3.	流量告警	可以设置自定义流量告警, 当指标超过一定阈值时自动告警, 告警消息通过电子邮件、短信等方式发出, 帮助用户提前预警风险。	
4.	★管理	NAT 网关、SNAT 规则 DNAT 规则管理, 包含创建、查看、修改、删除等	
5.	批量操作	支持批量操作。	

1.4.2.3.15. 云专线服务

云专线服务功能包括但不限于以下内容:

序号	指标名称	要求	备注
1.	★物理专线	连接云与本地数据中心的物理线路连接, 在用户的数据中心和云专线网络接入点间建立网络连接。支持添加、查看、修改、删除	
2.	网络地址转换 (NAT)	网络地址转换是对专线两端 IP 冲突问题的一种解决方案。用户可以在专线网关上配置网络地址转换规则, 网络地址转换(NAT)包含 IP 转换和 IP 端口转换两种。	
3.	★专线共享	应支持多个租户共享专线并支持用户自助化	
4.	★专线接入安全防护	应具备专线链路上的安全防护措施	

1.4.2.3.16. IPV6 支持

硬件设备和软件产品须支持 IPV6:

序号	指标名称	要求	备注
----	------	----	----

序号	指标名称	要求	备注
1.	IPv6 弹性公网 IP 管理	支持申请 IPv6 弹性公网 IP、开启和关闭 IPv6 转换、配置安全组等。	
2.	★云主机动态获取 IPv6 地址	如果当前云主机使用 IPv4，那么启用 IPv6 后，云主机可在双栈模式下运行，即云主机可以拥有两个不同版本的 IP 地址：IPv4 地址和 IPv6 地址，这两个 IP 地址都可以进行内网/公网访问。	
3.	★负载均衡服务 IPv6	负载均衡支持 IPv6 网络。	
4.	★DNS 服务 IPv6	DNS 服务支持 IPv6 网络。	

1.4.2.3.17. 跨地域 VPC 互通服务

跨地域 VPC 互通服务功能包括但不限于以下内容：

序号	指标名称	要求	备注
1.	★跨区域 VPC 互通	跨区域的多虚拟私有云（VPC）互通的业务，需要提供安全、稳定、高性能、高可靠的网络连接能力。	
2.	服务管理	添加、查看、修改、删除、关联带宽设置。	
3.	#区域间带宽管理	查看、修改、删除域间带宽，查看区域间带宽监控数据。	

1.4.2.3.18. VPN 服务

支持 VPN 功能，使用户作为远端用户需要访问 VPC 的业务资源时，用户可以通过 VPN 连通 VPC。VPN 连接通过公网加密技术，将 VPN 网关与远端网关关联，使本地数据中心与虚拟私有云通信，更快速、安全的构建云环境。投标人所投产品须支持 VPN 服务，本期项目不提供 VPN 服务。

序号	指标名称	要求	备注
1.	★VPN 网关管理	支持创建、查看、删除、修改 VPN 网关	

2.	★VPN 连接管理	支持创建、查看、删除、修改 VPN 连接	
3.	★监控	新增、查看、删除监控指标和数据，并可以设置告警规则	

1.4.3.PaaS 详细需求

1.4.3.1. 分布式关系型数据库服务

1.4.3.1.1.★配置要求

(1) 分布式关系型数据库支持多中心多活架构，为了保证物理层面的高可用，要求副本部署在不同的物理机节点、机架。

(2) 本功能要求配置相关软件授权及需要单独配套的硬件设备满足上述要求。

1.4.3.1.2.功能及性能要求

数据库提供 Web 界面进行配置、操作数据库实例，为用户提供可靠的数据备份和恢复、完备的安全管理、完善的监控、轻松扩展等功能支持。

序号	指标名称	要求	备注
1.	★实例类型	支持可视化部署分布式关系型数据库实例。	
2.	数据库功能要求	★①数据库以分布式架构进行设计，数据库容量和性能不足时，只需要添加服务器，即可线性扩展数据库容量和性能。	
3.		★②语法上 DDL，DML，DCL 支持 SQL92、SQL99、SQL2003 标准。	
4.		★③支持事务处理、MVCC 多版本控制、死锁机制，事务处理系统具备原子性、一致性、隔离性、持久性。	

5.		★④支持整数、精确浮点数、字符串、时间、枚举、集合、大对象等多种数据类型，时间类型能精确到毫秒、微秒为单位存储和读取。	
6.		★⑤支持表、序列、自增字段对象。	
7.		⑥支持视图、自定义函数、游标等数据库对象。	
8.		#⑦支持分区表、唯一索引、复合索引、主键（支持多字段）等。	
9.		★⑧至少支持 utf8、gb18030 字符集，支持校验规则区分大小写。	
10.		⑨支持批量表级压缩。	
11.		★⑩支持初始化时表分区功能。	
12.		⑪支持上线后表分区维护功能。	
13.		★⑫支持 SQL 预处理 Prepared Statements 功能。	
14.		★⑬支持标准 SQL 语法，支持数据的多数据分片自动路由与聚合，支持跨库的 select、update、delete、insert、常见聚合函数（如 sum、count、avg、min、max 等）、支持跨库的 distinct、order by、group by、having、子查询、分页查询、join、union 等。	
15.		★⑭具备 OLTP 环境高并发情况下的完善锁机制，至少支持行级锁。	
16.		★⑮具备不同隔离级别，支持 read committed 及以上隔离级别。	
17.		★⑯兼容第三方客户端，包括但不限于 JDBC、ODBC 等。	
18.	#虚拟租户	可以在一组物理集群中，虚拟出多个相互资源隔离的数据库租户；每个租户都可为业务系统提供完整的数据能力。	
19.	★支持水平拆分	支持水平拆分，即将一个表的数据分散到多个物理独立的数据库服务器中，多个分片组成一个逻辑完整的数据库表。数据库性能随着水平拆分可近线性增长。	

20.	★支持集群分区表	支持在分布式集群（即水平拆分情况下），仍然支持数据库分区能力，即将大表的数据分成小的子集，但逻辑上仍然是一张完整的表。	
21.	★支持广播表	支持小表同步复制到每个分片节点，解决分布式数据库下 join 等问题。	
22.	★自增长序列	支持分布式自增长序列，提供全局唯一ID。	
23.	★多地多中心架构	支持多地多中心架构，无论是数据节点或是管理节点都支持跨机房部署，主实例在同城其他中心或者异地配置灾备实例。	
24.	#灾备参数	要求同城数据中心可选强同步，数据强一致，保证 rpo≈0，rto 小于 60 秒；要求跨地域灾备 rpo 分钟级，rto≤30 分钟。	
25.	数据备份	★①支持设置策略定期对数据进行整体备份，可以设置备份地点、备份启动时间、保存时间等，支持备份压缩功能。备份方式至少支持全量备份和增量备份。	
26.		②支持通过备份一体机或备份软件方式将备份文件离线存储到磁带库中。	
27.	从机增备	支持通过从机进行增量备份，减轻主机负担。	
28.	#自助恢复	支持数据库的恢复操作（或称为回档），系统可以通过备份恢复指定节点数据。	
29.	★性能要求	①分布式数据库：单集群（3 台物理服务器，配置见 1.4.1.1.4） 每秒事务请求数（QPS）：50000 及以上 q/s；每秒事务处理数（TPS）：5000 及以上；连接数：11000 及以上。	
30.	数据库引擎升级—新实例	数据库服务可在线升级版本，升级完成后新建实例可以选择使用新版本和旧版本。	
31.	数据库引擎升级—旧实例	数据库服务可在线升级版本，升级过程中原有数据库实例不中断，升级完成后数据不丢失。	

32.	★实例规格扩容	对既有实例（租户）的计算资源规格进行扩充，不影响原有数据。规格扩充后可以在分钟级恢复。	
33.	数据库账户角色	支持对不同账号分配不同角色，不同角色可以承担不同权限，如财务，运维，超级管理员等。	
34.	SQL 优化建议	支持业务对 SQL 进行优化评估，包括评估语法逻辑，查询效率等，以协助业务优化 SQL。	
35.	★慢查询分析	支持对慢日志（SQL）进行聚合分析，以协助业务优化业务 SQL。	
36.	慢速删除	当用户执行 drop table 或者 alter table.drop partition 时，避免 IO 波动影响数据库性能。	
37.	SQL 防火墙	内置 SQL 防火墙，SQL 防火墙通过匹配规则阻断非法 SQL。	
38.	#数据库审计	可扩展数据库审计模块，以对用户操作数据库实例进行审计。审计模块采用旁路形式，以减少对数据库的性能影响。	
39.	访问控制	支持访问控制（对于用户和权限进行控制，权限至少可划分为管理类、监控类、数据操作类权限）。	
40.	★操作审计	对管理员操作数据库管理系统记录日志，以进行审计。	
41.	防止误删元数据	只允许通过规定登录方案的授权用户删除存储元数据的库表，以便防止用户误操作导致业务不可用。	
42.	★支持 SSL 加密	支持数据库服务器与客户端建立 SSL 加密连接，避免数据被窃听。	
43.	★数据加解密	①支持敏感数据加解密，加解密支持国密算法，或支持通过集成加密机的方式实现数据加解密。	
44.		②支持数据加密存储和解密导出。	
45.	数据恢复日志	支持数据恢复日志文件查询和下载。	

46.	数据库监控	★①支持对数据库实例的全部关键指标进行实时监控（具备展示大盘），包括底层的节点，实例，关键模块以及包括数据库层面的访问监控、负载监控、查询缓存监控、表监控等。具体指标包括但不限于（CPU、内存、存储空间、活动连接数、慢 SQL 语句、锁情况溯源、非活动连接数、网络 IO、qps、tps、容量、库大小等信息）。	
47.		②支持表级粒度的容量信息展示	
48.		★③提供监控历史数据查看功能，支持回溯数据库某一时间段的运行情况。	
49.		★④可出具分析文档，如诊断日志等。	
50.	★告警策略	①对重要的、影响数据库可用性的指标实现告警通知的功能，可依据告警阈值进行分级告警，每个告警项的阈值可根据数据库运行情况来修改。	
51.		②提供告警项可选功能，根据不同运行情况的数据库选择最合适的告警项来监控数据库，防止产生大量不必要的告警项。	
52.		③支持告警项可定制化，可视化添加、更改、删除数据库的告警项，支持自定义告警，可定义异常的监控指标项、故障时间、告警方式等进行配置。具体指标包括但不限于（CPU、内存、存储空间、连接数、活动连接数、死锁、网络 IO、qps、tps）。	
53.		④支持自定义告警格式，支持短信、告警平台等方式推送告警信息。	
54.		⑤支持查看全局告警信息，可筛选查看特定的数据库告警信息。	
55.		⑥支持查看历史告警信息，可以手工方式忽略某些特定的告警信息，可以批量删除告警信息。	
56.		⑦告警功能需提供标准接口，允许其他外部系统访问调用监控告警数据，满足中心告警信息统一管理的总体规划。	

57.	统计分析	提供数据库实例、表等维度的操作量及数据量的统计分析。	
58.	错误日志	★①支持记录管理系统和数据库本身的错误日志。	
59.		②支持错误日志的自定义策略查询（如严重级别、时间区间等）	
60.	★集群全局视图	支持对数据库集群资源、告警的全局视图展示，可扩展展示到大屏。	
61.	实例管理	★①实例变更一键式图形化操作。支持新增、管理、销毁数据库实例；支持对实例做必要的运维管理操作，包括但不限于：设置实例全局读写模式，设置数据库参数，新增、管理、删除数据库账号，查询实例各组件监控和告警情况，查询该实例异常会话。	
62.		②配置实例虚拟 IP，配置租户之间的实例 CPU/IO 隔离模型与隔离参数，	
63.		③支持对实例进行备份，对实例进行回档恢复等。	
64.	★全局运营监控能力	支持对全部实例关键组件包括但不限于：计算节点（Proxy）、存储节点（DB）、接入层（LB 或者同样功能组件）等进行全局监控，并优先展示异常实例情况。	
65.	★管理或调度系统监控与管理	支持对集群所需的主要管理或调度系统进行监控，并优先展示异常情况。可以支持一些常见的运维管理操作。	
66.	★数据迁移工具（同构）	支持本地部署数据库迁移工具，支持同构数据库（本数据库）间数据迁移。	
67.	数据迁移工具（异构）	★①支持本地部署数据库迁移工具，支持异构数据库mysql和云上数据库间（本数据库）的数据不停服迁移。	
68.		#②支持本地部署数据库迁移工具，至少支持农信银资金清算中心现有数据库，如 DB2 与云上数据库（本数据库）的数据不停服迁移。	
69.	★数据归档	支持将数据归档到中心大数据平台，如支持主流的 ETL 拉取数据或推送到Kafka。	

70.	★集群管理	支持图形化界面一键式新增、修改、删除数据库集群实例。	
71.	智能巡检工具	★①智能巡检定期为数据库提供可靠性、可用性、性能、可维护性方面的全方位健康检查。	
72.		②根据巡检结果, 给出相应的优化建议	
73.	智能诊断工具	提供 7 * 24 小时实时数据库异常诊断分析, 从规格配置、SQL 分析、业务逻辑、使用合理性等维度给出建议和优化措施。	
74.	数据库安全工具	支持区分 IP、用户的白名单功能; 支持 SQL 黑名单、sql 注入攻击拦截 (如支持拦截无 WHERE 条件或恒真条件的 UPDATE 和 DELETE 等涉及数据库安全的数据库操作, 及可图形化在线配置和动态加载生效)。	

1.4.3.2. 数据库同步工具

序号	指标名称	要求	备注
1.	数据同步	★①增量数据(增删改)支持单向同步、双向同步。	
2.		#②增量数据(增删改)支持双 A 同步、多对一同步、一对多同步。	
3.		★③支持同机房、跨机房数据库间的同步。	
4.		★④支持历史数据全量同步。	
5.		★⑤数据库之间数据同步支持异步方式。	
6.		★⑥支持动态或重启后数据重定向(例如转换库名和表名)。	
7.		★⑦支持断点续传	
8.		★⑧支持动态或重启后增加数据表的复制。	
9.		★⑨数据同步支持加密传输。	
10.		⑩数据同步支持压缩传输。	
11.		★⑪支持各类常用数据库字符集, 如 utf8、gb18030 等	

12.		★⑫支持主流的关系型数据库（如MySQL、1.4.3.1 章节的云上关系型数据库）。	
13.	数据回环	双向同步和双 A 同步，避免数据回环（A 同步到 B 的数据，在 B 同步到 A 时不可再同步到 A）。	
14.	★数据一致性保障	同步后两边数据保持最终一致性；当两边数据不一致（因网络延迟导致）时，应有策略保证同步后数据的一致性。	
15.	可配置	支持按实例、数据库、表、字段同步数据（前端可配置）。	
16.	★数据监控	①支持监控同步状态（停止、运行）、同步进度、同步延迟时间等。	
17.		②统一监控页面，显示所有系统的数据同步监控结果。	
18.		③可配置告警通知。	
19.	数据对比	①支持单向同步、双向同步的一致性校验：支持数据条数、数据状态等详细比对结果的展示。	
20.		②支持一对多的一致性校验：支持数据条数、数据状态等详细比对结果的展示。	
21.		③支持双 A 同步的一致性校验：支持数据条数、数据状态等详细比对结果的展示。	
22.		④支持数据比对结果落数据库。	
23.		⑤展示结果支持下载。	
24.		⑥双向冲突的数据，支持触发告警（通过数据比对）。	
25.	#数据同步完整性检查	数据同步网络传输过程出现网络抖动、丢包等情况，具备重传重试机制。	
26.	ddl 同步	★①支持 drop table/alter table /rename table 的同步（单边支持即可）。	
27.		★②支持单向同步、双向同步、一对一同步。	
28.		③支持一对多同步。	

29.	性能需求	#①异地数据中心(物理距离>1000KM), 带宽 10M/s, 在 TPS 低于 100 时, 单向同步延迟时间不超过 2s, 双向同步延迟时间不超过 5s(存在大事务、大字段等特殊情形除外)。	
30.		②日交易量和流水大小: 日交易量 > 一亿笔, 每条流水不超过 40KB (根据支付清算系统得出), 日间延迟最大不超过 2 分钟。	
31.		★③吞吐量 90W/min (delete/insert/update 操作)。	
32.		④TPS 在 1500 下同步带宽不大于 10M/S, 同步延迟 10s 以内(存在大事务、大字段等特殊情形除外)。	
33.		⑤同步线程 CPU 使用率应控制 10%以下 (包括源端和目的端)。	
34.		★⑥数据同步需支持削峰功能, 支持流量控制。	
35.		★⑦支持按任务或链路进行资源分配, 防止系统雪崩。	
36.	★高可用需求	①数据同步过程中, 若源和目标数据库发生主从切换, 同步任务应支持主从手动切换。	
37.		②工具支持部署在非数据库主机上。	
38.		③数据库同步工具自身具备高可靠保障机制。	
39.		④同步程序出现异常, 支持告警及自动重启 (持续监测程序状态)。	

1.4.3.3. 容器服务

(1) 云容器服务提供容器基础设施服务, 需要为用户提供托管的容器引擎服务。容器引擎需基于 Kubernetes (V1.20+, 紧跟社区版本升级) 构建, 赋予租户按需完成容

器引擎集群的动态创建、自动扩缩容、集群监控运维、容器镜像管理、容器化工作负载管理等能力。

(2) 云容器引擎需集成云平台基础设施, 如租户 VPC 网络、各类存储资源, 并提供与云产品集成一体化的集群管理、工作负载管理、网络管理、存储管理、权限管理、镜像仓库、日志监控等功能模块和服务。云容器引擎服务功能包括但不限于以下内容:

序号	指标名称	要求	备注
1.	★支持创建容器引擎集群	在操作界面上, 可一键创建容器引擎集群, 支持自动安装常用集群管理工具, 例如 kubectl 或同功能工具等。	
2.	★支持对 ETCD (或同等功能) 数据进行备份和恢复	支持对集群配置信息所在 ETCD 数据进行备份和恢复, 防止升级或容灾切换演练造成的数据丢失。	
3.	★支持可控的容器和计算节点的二级弹性伸缩	支持容器和计算节点的二级弹性伸缩, 支持丰富的 HPA 自动弹性伸缩策略, 控制台上可以提供基于 CPU、内存、硬盘、网络等多种触发策略。	
4.	★容器平台组件高可用	容器管理平台所有组件具备高可用性。	
5.	★跨同城 AZ 高可用	支持跨同城 AZ 高可用。	
6.	界面提供 RBAC 全部功能	界面提供配置 RBAC 以对用户角色的权限进行访问控制、准入控制, 所有组件的 token 认证。	
7.	#镜像扫描	应支持扫描镜像中的漏洞等安全风险。	
8.	★支持 CNI 网络模型	支持多种 CNI 网络配置, 包含二层方案 (例如 flannel-vxlan) 和三层方案 (例如 calico), 或者其他技术实现	

		VPC 隔离。	
9.	界面支持对容器引擎集群 DNS 和域名的配置	在操作界面上, 支持对应用的 DNS 和域名进行配置。该域名可以从容器集群外访问, 路由至集群内的 service, 功能上类似于 Kubernetes 的 ingress。	
10.	★集群外至集群内路由	在操作界面上, 支持集群外路由至集群内的功能, 类似于 Kubernetes 的 ingress。	
11.	东西向和南北向的流量监控	支持对东西向和南北向网络流量分别进行监控。	
12.	应用发布	支持灰度、蓝绿、滚动等应用发布方式, 提供开箱即用的方案。(可以在容器服务实现, 也可以通过微服务平台实现)。	
13.	★支持市场上主流的集中式和分布式存储	支持存储类型包括但不限于: 块存储、对象存储、文件存储(本地存储和 NFS)。	
14.	★支持对持久卷进行管理操作	在操作界面上, 支持对持久卷进行增、删、查、改操作。	
15.	支持 PVC、storageclass 等资源的管理	在操作界面上, 支持 PVC、storageclass 等资源的创建删除修改查询。	
16.	应用仓库 (类似 Helm)	在操作界面上, 支持配置和管理应用仓库。	
17.	#镜像仓库	在操作界面上, 提供镜像仓库 (如 harbor) 的配置、安装和部署 (如果 DevOps 组件提供镜像仓库, 可以忽略)。	
18.	★镜像仓库高可用	镜像仓库与容器集群解耦, 独立于容器集群。	
19.	★容器负载均衡	支持基于 ingress (或类似服务) 实现容器集群负载均衡。	
20.	存储管理	支持对接及管理容器多存储访问类型: 块存储、文件存储及本地存储。具备统	

		一的接入管理体验及统一的存储配置管理平面。	
21.	应用管理	支持 Deployment、StatefulSet、Job、CronJob、DaemonSet 等 Kubernetes 的工作负载对象部署。	
22.	多集群管理	提供集群的生命周期管理能力, 包括: 集群的自动化创建、集群扩缩容与集群销毁等能力。	
23.	多租户管理	提供基于 VPC 的集群级租户能力, 实现租户独占集群; 提供集群内细粒度的资源分配能力, 结合权限控制和命名空间实现命名空间级的资源配额与环境隔离。	

1.4.3.4. 分布式缓存服务

序号	指标名称	要求	备注
1.	兼容 redis	#实例需要兼容 redis3.0 版本及以上, 支持版本升级 (小版本升级时应用端不用更新客户端)。	
2.		★具备 redis 主要功能	
3.	★缓存功能	①支持但不限于字符串 (strings)、散列 (hashes)、列表 (lists)、集合 (sets)、有序集合 (sorted sets) 等数据类型。	
4.		②支持事务。	
5.		③允许为每一个 key 设置不同的过期时间, 支持配置 key 过期策略, 支持批量设置 key 过期时间。	
6.		④支持 pipelining 管道策略, 将多个命令合并成一次操作。	
7.		⑤支持快速大量数据插入 (mass insertion)。	
8.	自动主备切换	主从和集群版支持自动主备切换, 支持故障自动识别、切换不中断业务, 支持故障修复回切。	

9.	★可扩展性	支持平滑的纵向和横向扩缩容。	
10.	★部署方式	至少支持两种模式部署，供不同业务连续性等级应用选择： 集群部署（集群各分片 slot 需部署于不同物理服务器）。 哨兵模式。	
11.	管理—新建销毁	支持图形化用户新建实例、销毁实例等操作。	
12.	管理—启停	支持图形化用户启动、重启、修改密码、修改配置。	
13.	★管理—多 AZ	支持图形化管理多个 AZ 的缓存实例。	
14.	管理—可视化	①支持图形化显示当前实例相关的概要信息。	
15.		②提供集中化、图形化界面的配置、管理、监控功能。	
16.	管理—命令行	支持命令行管理功能。	
17.	★备份	①主备和集群版本支持手动备份，支持设置备份策略并自动生成备份。	
18.		②支持数据在线持久化保存。	
19.	★监控告警—多维度告警	支持多维度监控和告警，至少包括重启或停机、CPU 冲高、内存用量等。	
20.	文档	产品介绍文档、产品使用指南、SDK 参考文档、相关协议文档、常见问题文档。	
21.	★从备份恢复	主备和集群版支持从备份恢复实例。	
22.	★访问控制	①对于用户和权限进行控制，权限至少可划分为管理类、监控类、数据操作类权限。	
23.		②主备和集群版支持黑或白名单设置，例如通过 IP 地址等设置访问实例的策略。	
24.		③支持连接密码配置。	
25.	集群管理	★①支持集群、支持数据自动分片。	
26.		②主从复制或多副本机制。	
27.		#③支持跨地域集群数据同步。（或无条件提供同类工具实现该需求）	
28.		★④具备集群防脑裂功能。	
29.	★消息管理	支持消息的订阅和发布（Pub/Sub）。	

30.	★性能要求	吞吐量： 每秒事务请求数（QPS）：100000 及以上 q/s。 当数据库连接数在 60000 时，可维持 50000 q/s。	
-----	-------	---	--

1.4.3.5. DevOps 服务

提供一站式云端研发运维一体化 DevOps 平台。需要一套开箱即用的方案，满足开发面板—代码仓库—代码检查—构建—镜像仓库—镜像安全检查—制品仓库—制品包检查—生产部署—度量管理的整体流程以及对应的 CICD 工具和过程反馈工具。除了上述功能外重点关注流水线并发条数、是否占用资源池、流水线处理单元的资源配置、流水线出错后的排查难易程度。

序号	指标名称	要求	备注
1.	★需求管理—支持敏捷模式和看板模式管理工作项	支持敏捷模式或看板模式管理工作项。	
2.	需求管理—支持迭代管理	迭代能够关联到工作项。	
3.	需求管理—需求拆分	提供需求条目化、精细化、细粒度拆分的功能。	
4.	需求状态	支持自定义需求状态。	
5.	需求管理—工作项支持关联到代码评审和测试案例	工作项支持关联到代码评审和测试案例。	

6.	项目管理—项目自定义统计报表和报告	丰富的自定义统计报表，同时支持预置优秀实践自定义报表，按需多重维度自定义；快速自定义生成项目进展报告。	
7.	★项目管理	支持任务工时、看板。	
8.	度量管理—度量指标	①支持维度的度量指标，度量指标类型覆盖过程指标及结果指标，支持对度量数据的管理，对历史度量数据有明确的管理规则，支持度量指标按照需求定期更新。	
9.		②支持交付过程中各种度量数据的收集、统计、分析和反馈，支持可视化查看数据指标的度量报告，支持度量指标的有效反馈机制，持续优化度量指标分类。	
10.	度量管理—指标维度	①版本管控数据：代码提交数、提交频率、提交时间分布等。	
11.		②构建管理数据：构建频率、时长、成功率、修复时长等。	
12.		③代码管理数据：代码行数、复杂度、重复率、覆盖率等。	
13.		④版本发布管理数据：版本发布时长、频率及前置时间等。	
14.		⑤制品部署管理数据：部署时长、成功率、回滚率等。	
15.	★代码管理—支持新建多个代码仓库	支持一个项目或组织新建多个代码仓库。	
16.	★代码管理—git 仓库支持 ssh 访问和 https 访问	git 仓库支持 ssh 访问和 https 访问。	
17.	代码管理—支持浏览 git 仓库文件和目录内容	支持选择分支、标签、commitid 进行浏览。	
18.	★代码管理—权限管理	支持代码仓库角色权限细粒度设置和管理，角色至少包括（开发者、管理者、项目所有者等）。支持代码仓库项目、分支创建、tag 创建和管理，支持代码克隆、提交、修改、合并等权限，支持默认和自定义权限分配。	

19.	★代码管理-代码仓库支持在线编辑、提交文件	代码仓库支持在线编辑、提交文件。	
20.	★代码管理-支持分支管理	在线创建、删除分支。	
21.	代码管理-支持标签管理	在线创建、删除标签。	
22.	代码管理-支持显示 commit 关系图	支持显示 commit 关系图。	
23.	代码管理-显示每个仓库的统计信息	支持提交数据统计信息的显示。	
24.	★代码合并-支持 merge request 合并模式	支持 merge request 合并模式。	
25.	代码合并-支持在线进行代码评审	支持在线进行代码评审。	
26.	代码合并-评审意见有是否解决状态	评审意见有是否解决状态，可通过评论支持。	
27.	代码合并-查看每个评审信息	包括所有评审意见、文件对比、提交列表。	
28.	代码合并-支持多个评审人员	支持多个评审人员。	
29.	代码合并-支持指定合并人员	支持指定合并人员。	
30.	代码合并-支持评审员打分	支持评审员打分，可通过评论支持。	
31.	★代码权限-代码库权限管理	可以设置指定角色的用户才可以对代码仓库进行读、写、分支操作。	
32.	代码检查-管理代码检查任务	任务新建、任务执行、任务结果展示。	

33.	代码检查—提供默认 C/C++语言检查模板	提供默认 C/C++语言检查模板。	
34.	★代码检查—提供默认 Java语言检查模板	提供默认 Java 语言检查模板。	
35.	代码检查—提供默认 Python语言检查模板	提供默认 Python 语言检查模板。	
36.	代码检查—支持 JavaScript语言检查	支持 JavaScript 语言检查。	
37.	代码检查—支持 CSS 语言检查	支持 CSS 语言检查。	
38.	代码检查—支持 Web 语言检查	在线检查工程中的 HTML/JSP 代码。	
39.	代码检查—支持 Android (Gradle) 语言检查	支持 Android (Gradle) 语言检查。	
40.	代码检查—支持 GO 语言检查	支持 GO 语言检查。	
41.	代码检查—支持自定义规则或者自定义规则集	支持自定义规则或者自定义规则集。	
42.	代码检查—显示检查问题	包括问题列表、问题分严重级别。	
43.	代码检查—显示检查出的代码度量	圈复杂度、代码重复率、有效代码行数。	
44.	代码检查—支持设置质量门禁	按不同级别的问题数。	
45.	代码检查—支持代码安全检查	用代码安全检查规则集，对自己的代码进行代码安全风险和缺陷检查，生成报告。	
46.	代码检查—支持集成外部安全检查工具	提供方便机制集成外部代码安全检查工具。	

47.	代码检查—支持安全扫描	具备基本的应用程序安全性测试, 查找和修复可利用的 Web 应用程序漏洞。	
48.	代码检查—支持集成外部安全动态扫描工具	提供方便机制集成外部动态扫描工具。	
49.	构建管理—管理构建任务	任务新建、任务执行、任务结果展示。	
50.	★构建管理—构建任务支持界面化编辑	提供标准步骤模板, 并可编辑个性化内容。	
51.	构建管理—构建任务权限管理	不同角色赋予任务操作的不同权限。	
52.	构建管理—构建任务结果通知	通过短信、社交软件(对接中心内部 EM)通知。	
53.	★构建管理—支持主流语言编译功能	支持 Java、C、C++、NodeJs、Python、Go 等主流编译构建语言。	
54.	★构建管理—支持主流构建标准	支持 Maven、Gradle、Yarn、Cmake 等主流构建标准。	
55.	★发布管理—支持私有 maven 制品库和 npm 制品库	支持私有 maven 制品库和 npm 制品库。	
56.	发布管理—支持私有容器镜像制品库	支持私有容器镜像制品库。	
57.	发布管理—支持私有文件夹式发布物管理	支持私有文件夹式发布物管理。	
58.	★部署管理—管理部署任务	任务新建、任务执行、任务结果展示。	
59.	部署管理—管理主机和主机组	管理主机和主机组。	

60.	部署管理—管理部署任务步骤	提供标准步骤模板，并可编辑个性化内容。	
61.	部署管理—支持自定义部署步骤	支持自定义步骤。	
62.	部署管理—支持部署任务权限管理	支持部署任务权限管理。	
63.	★部署管理—部署任务执行结果通知	部署任务执行结果通知。	
64.	发布管理—支持文件夹式发布物管理	支持文件夹式发布物管理。	
65.	★流水线—支持流水线在线编辑	增删改流水线、流水线执行。	
66.	流水线—支持流水线复制	支持流水线复制。	
67.	流水线—流水线执行结果通知复制	流水线执行结果通知复制。	
68.	流水线—支持流水线模板管理	支持流水线模板管理。	
69.	文档管理—支持在线知识库	支持在线知识库。	
70.	文档管理—支持文件夹式文档	支持文件夹式文档。	
71.	文档管理—支持API文档	支持API文档。	
72.	测试管理—支持测试用例管理	多层次测试案例。	
73.	测试管理—测试用例内容	步骤、处理人。	

74.	测试管理—支持测试用例关联到需求工作项	支持测试用例关联到需求工作项。	
75.	测试管理—测试任务管理	新建删除计划。	
76.	测试管理—测试任务内容	关联测试案例、负责人。	
77.	测试管理—测试任务执行	每个案例可输入执行结果（通过与否）、可输入每个执行步骤的结果文本。	
78.	测试管理—支持自动化 http/https 接口测试案例管理	多层次测试案例。	
79.	测试管理—接口测试案例编辑	在线编辑 url 和 head，返回值。	
80.	测试管理—接口测试案例多个 url 组合	支持多个 url 请求组合形成一个案例。	
81.	仓库功能	①DevOps 服务提供代码仓库（Git 类型）、容器镜像仓库（如 harbor）、制品仓库（如 Nexus）等功能。	
82.		②开源软件可信源管理和发布门禁（对发布二方包支持版本控制）。	

1.4.3.6. 微服务应用平台

需要一套开箱即用的方案，满足注册中心、配置中心、服务治理、微服务网关、监控、链路追踪、服务网格等功能。

序号	指标名称	要求	备注
1.	★底层资源要求	①基于 Java 语言的产品兼容 OpenJDK1.8 及以上版本	
2.	★微服务基础功能—基础能力	提供微服务开发框架，支持微服务注册、发现、通信、治理、配置统一管理等基础能力。	

3.	微服务基础功能—语言	支持 Java、Go、C、C++ 等开发语言。	
4.	#微服务基础功能—框架	支持 spring-boot/spring cloud/dubbo/SpringMVC/Service Mesh 等编程框架或微服务架构体系。	
5.	微服务基础功能—框架	支持 REST/RPC (dubbo/http/https) 等多种服务通信协议, 支持协议可扩展, 通信性能不低于 10 万 TPS。	
6.	微服务基础功能—本地调试	支持本地调试。	
7.	微服务基础功能—异步调用	支持全链路的异步调用(不包含数据库连接)。	
8.	微服务基础功能—泛化调用	支持泛化调用。	
9.	★微服务治理—负载均衡	支持轮询、随机等负载策略, 同时支持配置的动态更新。	
10.	★微服务治理—服务路由	支持路由规则, 路由规则决定了服务消费者的调用目标, 即规定了服务消费者可调用哪些服务提供者。	
11.	微服务治理—容错策略	①failover: 失败后自动切换其他服务器, 支持配置重试次数。	
12.		②failfast: 失败立即报错, 不再重试。	
13.		③forcereturn: 强制返回策略, 不真正地进行远程调用服务提供端, 而是在服务消费端直接按规则返回结果。	
14.	★微服务治理—服务鉴权	①服务认证支持公私钥认证、黑白名单、token 认证等一种或多种。	
15.		②支持报文加密, 支持 SSL/TLS。	
16.	微服务治理—注册发现功能	★①支持微服务的注册、注销、发现、心跳、更新等功能。	
17.		★②支持多注册中心发布和订阅功能。	
18.		③支持注册信息的本地缓存和高可用机制。	
19.		★④支持主流注册中心(如 zookeeper、nacos 等一种或多种)的适配, 或无条件提供同类工具迁移到云上注册中心。	
20.	微服务治理—注册发现可用性	注册中心支持万级服务实例注册, 集群同步时保证服务注册功能可用。	

21.	微服务治理 — 配置中心	①支持应用上线后的配置,支持配置运行时修改并生效,支持配置信息本地缓存。	
22.		★②支持和主流配置中心(如Nacos等)的适配,或无条件提供同类工具迁移到云上配置中心。	
23.	微服务治理 — 服务查询	①支持基于服务名称、服务描述等条件查询。	
24.		②支持按应用、微服务和实例三个维度展示服务列表。	
25.		③支持以拓扑图方式展示微服务基本信息,以及依赖关系。	
26.	微服务治理 — 流量控制	#①支持按服务粒度限流,支持线程池、信号量等一种或多种限流策略。	
27.		②支持开发者扩展自定义的限流逻辑,超过流量限制后既可以拒绝服务,也能够延缓处理。	
28.		③支持服务提供方限流。	
29.	微服务治理 — 熔断降级	#①可设置自动熔断策略,策略包含:窗口请求数、熔断触发故障率、熔断时长等。	
30.		②熔断后可在治理界面上查看到熔断状态为Open;熔断时长过期后可自动回复。	
31.		③支持按服务粒度和接口粒度降级,支持手工或自动降级。	
32.	微服务治理 — 多中心多分组	服务支持多中心,多分组,多版本配置和管理,支持灾备切换。	
33.	微服务治理 — 灰度发布	①支持使用接口任意参数(例如用户群组、用户类别、用户所属区域等等)定义微服务灰度发布规则。	
34.		②配合API网关等实现应用全链路灰度发布。	
35.	微服务治理 — 故障隔离	支持按接口设置线程池进行隔离。	
36.	★微服务治理 — 兼容 Spring Cloud	全面兼容Spring Cloud微服务开发框架,提供稳定可靠的Spring Cloud的应用运行环境,采用Spring Cloud框架编写的應用,可以无缝部署到本平台上。	
37.	#微服务治理 — 兼容 dubbo	全面兼容Dubbo框架,提供稳定可靠的Dubbo的应用运行环境,采用Dubbo框架编写的應用,可以无缝部署到本平台上。	

38.	Service Mesh—支持非侵入式	实现非侵入式接入已有微服务。	
39.	Service Mesh—支持虚机和容器	支持虚机和容器的迁移过渡。	
40.	Service Mesh—支持语言	支持接入 Java、python、C 等语言开发的微服务。	
41.	Service Mesh—平滑升级	支持 sidecar 的平滑升级,应用调用平滑迁移。	
42.	开放兼容性要求—开源框架	要求微服务框架已开源,提供源代码,可以在线下使用。	
43.	开放兼容性要求—多种模式	微服务开发模式(服务注册)支持 SpringMVC, 透明 RPC 等开发模式。	
44.	开放兼容性要求—主流开源产品	产品支持兼容如 nacos、xxljob 等业界主流的开源产品。	
45.	开放兼容性要求—应用平滑迁移	现有 spring-boot 应用少量改动即可接入微服务治理。	
46.	#开放兼容性要求—支持多种 web 容器	支持主流的开源和商用 web 容器。如 Tomcat、Jetty、Undertow、TongWeb 等。	
47.	开放兼容性要求—多种运行环境	微服务应用支持多种运行环境,如虚拟机、物理机和容器。	
48.	微服务监控—服务告警	支持依照自定义规则(如告警阈值)和事件等级,对微服务的异常情况进行报警和通知,并支持指定人员。	
49.	微服务模板构建	在微服务平台快速生成基于某微服务框架的工程源码,帮助设计人员快速构建微服务程序。	
50.	操作审计日志	对微服务平台的操作,进行记录和查看。	
51.	API 列表	基于 swagger 等提供微服务的 API 列表。	
52.	错误注入	支持注入错误或者超时等事件,方便服务的异常测试。	
53.	★安全功能	①支持集成国密认证的加密机或工具(可通过集成外部加密设备方式),实现微服务间报文的加密解密、加签验签、证书认证等基本安全功能。。	

54.		②流水、日志不能涉及敏感信息,需符合数据安全分级指南。	
55.	输入校验	可配置根据参数类型、参数值进行接口输入校验。	
56.	部署模式	支持单元化部署。	

1.4.3.7. API 网关

序号	指标名称	要求	备注
1.	★底层资源要求	①基于 Java 语言的产品兼容 OpenJDK1.8 及以上版本	
2.	API 测试需求	①支持 http/https 请求,可以自定义请求头、请求体 Body、请求参数 Query。并返回完成的响应报文。	
3.		②提供对接的 Mock 服务或直连自定义的服务。	
4.	★API 日常管理	支持基本信息维护以及管理。	
5.	API 版本管理	支持对于发布在不同环境的 API 进行版本管理,可以直接切换历史版本替换现有环境里的版本。	
6.	API 分组管理功能	支持创建、修改、删除 API 分组等其他管理功能。	
7.	#报文支持	支持主流的 XML、Json 报文协议。	
8.	内外部接口适配	具备内部接口转换适配能力,屏蔽对外接口差异,提高系统接口兼容性。例如版本差异。	
9.	★请求路由	支持基于权重路由、动态路由等路由规则。	
10.	★负载均衡	支持轮询、随机、权重、hash、一致性 hash 等多种负载均衡策略,且具备负载均衡策略定制化开发集成的能力(也可通过微服务或 mesh 实现该功能)。	
11.	★流量管理	①从入口流量为切入点,支持接口级限流、降级、自适应保护等(也可通过微服务或 mesh 实现该功能)。	
12.		②支持多种流量过滤策略,如协议校验、黑白名单管理。	

13.	自动分配二级域名	用于测试 API。	
14.	绑定域名	支持绑定自定义域名及 SSL 证书信息。	
15.	Mock 服务	支持配置 Mock 服务数据, API 创建选择后端服务直接选择返回的 Mock 数据, 支持响应头设置等。	
16.	后端服务配置	支持 url 路径配置、响应超时配置、负载均衡配置。	
17.	★ 签名认证防重放攻击	支持 SM3 算法签名 (可通过集成国密设备), 对请求报文进行签名, 防止报文篡改。	
18.	★ 支持 HTTPS 协议, 支持 SSL 加密	支持 HTTPS 协议, 支持上传 SSL 文件。	
19.	创建 IP 访问控制策略	支持创建 IP 黑白名单策略。	
20.			
21.	IP 访问策略与 API 绑定	将 IP 访问策略与 API 进行绑定并生效。	
22.	跨域访问	支持跨域访问。	
23.	VPC 授权	VPC 指定给 API 网关权限使用, 在创建 API 时, 可以选择已经授权的 VPC。	
24.	#微服务授权	支持 OAuth2、JWT、AK/SK 等一种或多种认证授权标准、框架。	
25.			
26.	微服务集群调用	微服务 API 具有与 API 同等功能, 并支持绑定微服务集群。	
27.	★高可用	支持集群部署。	
28.	性能	底层支持异步非阻塞模式, 提高 API 网关吞吐量。	
29.	运维管理	支持 API 网关集群扩缩容, 支持元数据直接导入或导出到请求或应答报文。 提供图形化 API 管理。	
30.	开放功能 API	将涉及的 API 网关操作接口化, 即无需通过 API 网关界面也可以通过接口调用相关功能。	

1.4.4. 云管平台详细需求

云管平台所具备功能只要能满足下述需求即可, 无需严

格遵守指标名称所包含要求的结构层次关系。

1.4.4.1. 云管整体需求

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、智能化运维、精细化运营及个性化扩展等核心竞争力，简化 IT 基础设施的管理使用成本，提升 IT 基础设施的可用性和易用性。一体化管控核心在于管理平台的一体化设计和多模块打通，包括统一的用户认证、角色管理、租户管理、权限管理、审批流程、日志管理、资源调度、监控大屏等平台基础功能和服务。

云管理平台提供统一操作入口，主要由统一管理平台、运营平台、运维平台、监控平台等模块组成，为不同的角色用户提供全面的云管理能力。

1.4.4.1.1. 统一管理平台

序号	指标名称	要求	备注
1.	★统一管理平台	为用户提供云中所有云产品和服务和云资源实例的自主管理能力，包括资源监控、资源操作等	
2.	★统一 IaaS 服务	提供包含计算、存储、网络等方面的 IaaS 层云服务，构建稳定、完备的底层资源架构体系。	
3.	★统一资源管理	提供包含创建、删除、配置等资源管理能力，满足全方位、多场景的资源管控需求	
4.	资源编排	通过资源编排模板实现多类型资源的自动化部署，提升资源创建效率并规范资源创建流程	
5.	★资源监控	通过指定告警规则，对资源运行使用情况进行监控告警，有效保障了资源运行的稳定性	

6.	资源变更	对资源归属的组织、资源集进行变更操作，满足因组织架构调整而需要对资源进行迁移的需求	
7.	★统一 PaaS 服务	提供云平台一体化的PaaS全生命周期管理界面包含：数据库、中间件、微服务、容器等组件。为打造敏捷云原生应用提供便利支持。	
8.	规格管理	通过规格管理，可控制资源创建时对规格类型的选择，实现对资源供给的灵活配置	

1.4.4.1.2.运营平台

运营平台为用户提供云中所有云产品的运营管理能力，包括组织管理、权限管理、计量计费、统计分析及服务管理等。

1.4.4.1.2.1. 用户/租户/权限管理

序号	指标名称	要求	备注
1.	★组织管理	支持组织列表中的组织名称来自定义组织排序。 支持自定义组织名称创建组织，组织名称可多次修改。 支持查看组织信息，展示当前组织下的资源集列表、用户列表、用户组列表。 支持变更组织归属、删除组织。	

2.	用户管理	支持查看系统用户列表和历史用户列表。 支持创建和删除用户,创建时可选择组织、角色和登录策略,一个用户可被赋予多个角色。 支持修改当前用户的用户信息、用户角色、用户组和登录策略。 支持查看重置密码。 支持对系统用户进行禁用和激活操作。	
3.	权限管理	提供角色创建、权限点控制、角色授权等服务。实现不同用户对资源可见性和资源管理权限 有不同的分配能力	
4.	用户组管理	支持创建和删除用户组,创建时可选择组织和角色授权,一个用户组可被赋予多个角 色。 支持修改用户组的角色授权。 支持为用户组添加或删除用户。 支持修改用户组名。	
5.	个人中心	支持查看当前用户个人基本信息和系统消息接收方式。 支持修改个人基本信息、登录密码和系统消息接收方式。	
6.	角色管理	支持查看角色信息,展示当前角色管理权限、应用权限、菜单权限和授权人员的授权 详情。 支持创建自定义角色,可根据需要选择权限。 支持修改自定义角色的基本信息和相关权限。支持激活和禁用角色	
7.	数据权限管理	支持对消息队列、对象存储、日志服务、容器服务、密钥管理服务实例进行数据授权,根据需要选择是否开启相关权限。 支持查看当前组织的用户列表,可查看用户权限。	
8.	访问控制管理	支持查看访问策略信息。 支持创建和修改访问策略,不支持修改默认策略。 支持删除未绑定用户的非默认策略。	

1.4.4.1.2.2. 资源用量计量计费

序号	指标名称	要求	备注
1.	★计量计费	1、从组织、资源集等维度提供资源计量功能，并可制定灵活计费策略进行计费管理。 2、支持将云环境里运行的资源实例数量按照时间维度、组织维度、资源集维度和区域维度进行统计展示和导出。 3、支持查看计费系统当前已有和正在使用的计费计划、计费策略、计费规则数量，以及计费计划和计费策略的生效时间。	
2.	计费策略	支持查看计费策略列表，还可查看指定计费策略的详细信息。支持创建、修改、克隆、删除计费策略，不支持删除默认计费策略。	
3.	计费规则	支持查看计费规则列表，还可查看指定计费规则详细信息。 支持查看、创建、修改、克隆、删除计费项，一条计费规则中应至少包含一个计费项。支持创建、修改、克隆、删除计费规则，不支持删除默认计费规则。	
4.	计费计划	支持查看计费计划列表，还可查看指定计费计划的详细信息。支持创建、修改、克隆、删除计费计划，不支持删除默认计费计划。	
5.	统计分析	提供针对组织、资源集的资源使用量和使用费用的统计分析的能力。	

6.	账单管理	支持从组织、资源集、资源等不同维度进行账单统计管理。 支持查看云产品账单概览,提供图表展示近6个月的云产品消费趋势、TOP10云产品消费分布、全部云产品消费详情。 支持查看、导出云产品账单统计和账单明细。 支持查看组织和资源集账单概览,提供图表展示近6个月的组织消费趋势、TOP10资源集消费分布、组织消费详情。 支持查看、导出组织和资源集账单统计和账单明细。 账单计费明细:支持按云产品查看、导出计费明细账单。	
----	------	--	--

1.4.4.1.2.3. 配置管理

序号	指标名称	要求	备注
1.	服务目录	支持自定义服务目录,通过编辑服务目录的上下架实现对服务目录的灵活管控。	
2.	配置管理	提供安全策略、个性化配置、菜单管理等方面的配置能力,满足不同场景需求。	
3.	配额管理	为组织、资源集设置不同资源的配额,控制组织所用资源总额,有效提高资源分配使用效率。	
4.	★配置导出	支持导出云内各类资源实例的列表清单	

1.4.4.1.2.4. 资源管理

资源管理提供开通和监管资源的能力,通过管理资源集、配置所需资源监控项,帮助用户清晰地了解各资源的使用情况,异常时及时避险。

序号	指标名称	要求	备注
----	------	----	----

1.	资源服务开通	支持开通 IaaS+PaaS(弹性计算、存储、网络、数据库、中间件、安全等)多种云服务和资源。	
2.	★资源集管理	支持使用自定义名称创建资源集，资源集名称可多次修改。 支持通过组织或资源集名称查找资源集信息，展示当前资源集下的资源列表和成员列表。 支持为当前资源集添加或删除成员，成员可以是用户或用户组。当一个成员被删除后，该成员不再拥有访问该资源集的任何权限。 支持删除资源、成员皆为空的非默认资源集。	
3.	仪表盘	支持模块调整和布局调整，可根据需要选择配额概览、全部资源实例数量、历史资源数量、资源负载、报警、我的管理、区域分布，并以图表方式展示，通过拖动模块调整页面布局。	
4.	云监控	支持查看各云服务单台实例的监控图表和报警规则。 支持针对当前云服务实例创建报警规则。 支持查看报警历史列表、报警规则列表、报警规则详情。 支持通过产品的监控指标设置报警规则监控项的阈值，监控项在满足报警条件时会发送报警通知。 支持启用、暂停、修改、删除报警规则。	

1.4.4.1.2.5. 合规审计

序号	指标名称	要求	备注
1.	★日志审计	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。	
2.	运维审计	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。	
3.	审计报告	审计报告功能，针对日常用户的操作、权限信息、任务运行信息等提供报告展示	

1.4.4.1.3. 全面开放与集成

提供可视化 API 门户、标准 API 接口，以及多语言 SDK。
提供页面级别的集成和个性化配置。

1.4.4.1.4. 资源审批流程

支持云资源使用人员在发起资源的申请、创建、变更、维护、扩容、缩容等资源操作时，系统将根据预设的审批流程自动发起申请审批流程。申请流程将自动流转到对应的审批人进行审批操作，待流程审批通过后，系统将自动对申请的资源发起变更操作。相关资源包括，VPC 网络、NAT 网关、弹性 IP、DNS 服务、块存储、对象存储、文件存储、云主机、分布式数据库、缓存数据库、数据传输工具、容器、微服务、API 网关等。

1.4.4.1.5.统一日志管理

日志服务要求能够为用户提供云上日志服务。用户除了可通过日志服务实现日志采集、存储、实时查询分析功能外,还支持对接流计算与数据仓库等能力。功能包括但不限于以下内容:

序号	指标内容	要求	备注
1.	★总体要求	针对实时日志类数据一站式服务,无需开发就能快捷完成日志数据采集、消费、投递以及实时查询分析等功能,提升运维、运营效率,建立海量日志处理能力	
2.	可视化	可视化分析支持线图、柱状图、环图、地图、词云、TreeMap 常见图表,支持构建图层,支持拓扑图构建,支持外部矢量图导入,支持 markdown, 图表自适应分辨率显示,支持全屏模式	
3.	数据消费	支持 Storm/Flink/SparkStreaming 方式消费数据;支持 Java/Python/Go 程序流式消费数据	
4.	数据采集	支持多种 SDK 采集服务端日志数据,包括 Log4J、LogBack、PHP、C++、Java、Go、.net、ios/android、Python/Logging Handler 9 种 SDK。	
5.	数据采集	日志采集工具支持使用分隔符、正则表达式对文本文件内的日志采集、支持 syslog 协议、Kubernetes 日志采集	
6.	查询分析	支持 json、文本、数值等数值类型查询、支持 json 格式中文本自动构建索引、支持对数据进行全文查询、支持多个条件组合查询 (And、Or、Not)、支持原始日志中上下文查询 (前后 N 行)	
7.	查询分析	支持日志聚类、变点检测、极大值检测、时序预测、时序聚类智能查询分析	
8.	加密存储	日志服务支持通过密钥管理服务对数据进行加密存储,提供数据静态保护能力。支持使用 托管密钥进行加密。支持通过用户自带密钥 (BYOK) 加密。	
9.	日志安全	提供常规的日志管理服务,支持数据采集、标	

	审计	准化接入、日志检索、日志处理等功能，实现云内日志集中、解析和审计。	
--	----	-----------------------------------	--

1.4.4.2. IaaS 云管需求

1.4.4.2.1.VPC 网络管理

序号	指标内容	要求	备注
1.	网络规划	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 VPC 之间的安全隔离。	
2.	IPv6	VPC 支持 IPV6 地址，支持 ECS 可通过 IPV6 地址访问互联网的 IPV6 服务，支持 ECS 作为服务端 IPV6 地址提供给互联网 IPV6 客户端访问，同时支持云服务器设置 IPV6 公网仅主动出规则，即经 IPV6 地址可主动访问 IPV6 网络，外部 IPV6 终端主动发起的访问不通。	
3.	弹性网卡	支持弹性网卡绑定云服务器。	
4.	VPC 互通	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。	
5.	VPC 共享	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 共享给同一组织的租户。	
6.	CIDR 地址	支持在控制台上针对 VPC 配置多个 CIDR 地址段；支持新 CIDR 地址段的扩容。	
7.	网络 ACL	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，从而实现对一个或多个子网流量的访问控制。	

1.4.4.2.2.NAT 网关服务

序号	指标内容	要求	备注
1.	SNAT	支持 SNAT，支持多个云主机通过同一公网 IP 主动访问互联网。	
2.	DNAT	支持 DNAT，支持绑定到 NAT 网关，NAT 网关通过与弹性公网 IP 绑定，可以使多个云主机共享弹性公网 IP 访问 Internet 或使云主机	

		提供互联网服务。	
3.	管理	NAT 网关、SNAT 规则 DNAT 规则管理，包含创建、查看、修改、删除等	

1.4.4.2.3.弹性公网 IP 服务

序号	指标内容	要求	备注
1.	地址池	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。	
2.	绑定/解绑到云主机	支持为云主机绑定/解绑弹性公网 IP	
3.	绑定/解绑到弹性网卡	支持为 ENI 绑定/解绑弹性公网 IP。	
4.	绑定/解绑到 NAT 网关	支持为 NAT 网关绑定/解绑弹性公网 IP。	
5.	绑定/解绑到负载均衡	支持为云负载均衡绑定/解绑弹性公网 IP。	

1.4.4.2.4.DNS 域名解析服务

序号	指标内容	要求	备注
1.	私有域名转发管理	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 服务器上解析	
2.	全局域名转发管理	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	
3.	多租户隔离	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	
4.	IPv6	内网权威域名管理和解析：支持 IPV6 域名解析服务	
5.	主机记录	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	
6.	全局域名调度	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。	
7.	负载均衡策略	支持基于权重策略(加权轮训 WRR)的负载均衡策略，通过该策略可以按需实现内网应用的全局负载均衡	
8.	健康检查	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。	

1.4.4.2.5.块存储服务

序号	指标内容	要求	备注
1.	生命周期管理	支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能	
2.	在线扩容	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务	

1.4.4.2.6.对象存储服务

序号	指标内容	要求	备注
1.	生命周期管理	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。	

2.	对象管理	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。	
3.	图片处理	支持原生图片处理服务: 创建图片处理规则、图片格式转换、图片效果处理、添加文字或图片水印、高级编辑自定义图片处理样式等, 提供控制台截图证明。	
4.	视频处理	支持对视频文件进行视频截帧	
5.	防盗链	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。	

1.4.4.2.7.文件存储管理

序号	指标内容	要求	备注
1.	命名空间	支持多个文件系统组成全局命名空间, 提供管理界面功能截图。	
2.	文件归档	支持将 NAS 指定文件或目录归档到对象存储, 可以按照不同时间段规则进行选择性的归档。提供管理界面功能截图。	
3.	容量管理	支持目录级容量管理	

1.4.4.2.8.云主机管理

序号	指标内容	要求	备注
1.	IP 规划	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, 支持配置 IPv6/IPv4 双栈网络, 云主机实例可自动获取 IPv6 地址进行内网通信。	
2.	生命周期管理	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、更换操作系统, 其中创建、启动、关闭、重启应支持批量操作, 提升管理员操作效率。	
3.	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。	

4.	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据，可用于快速发放包含用户业务数据的新弹性云主机。	
5.	宕机迁移	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，在其上运行的云主机能够在其他正常的物理节点上重新启动，保障业务的连续性。	
6.	云盘加密	支持云主机磁盘国密算法加密，能够对云盘中的数据、云盘和实例间传输的数据、云盘创建的所有快照进行加密处理，保障数据的安全性。	
7.	备份恢复	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；	

1.4.4.2.9. 云主机弹性管理

序号	指标内容	要求	备注
1.	伸缩组管理	支持伸缩组的创建、删除、修改、启用、停用等生命周期管理。	
2.	监控指标	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，自动执行伸缩规则，动态调整伸缩组内的云主机的实例数量，监控指标包括但不限于 CPU 使用率、内存使用率、内网出流量、内网入流量等。	
3.	伸缩配置	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、系统盘、数据盘、自定义数据等。	
4.	弹性扩展	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均衡实例的后端服务器组和数据库实例的访问白名单中。	
5.	伸缩规则	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，满足业务需求的同时又能控制成本。	

1.4.4.2.10. 统一管理视图

序号	指标名称	要求	备注
----	------	----	----

1.	资源池管理	支持各级管理员（例如部门、组）在自身资源池范围内为用户或用户组审批并分配资源（包括虚拟机、容器、数据库、中间件等）。	
2.	资源申请	①包括微服务、中间件、数据库等产品的单实例（VM 和容器）、集群（VM 和容器）的申请，申请页包括环境配置（机房、开发、测试、生产等环境）、基本配置（包括 cpu、内存、硬盘、网络带宽、网络地址和域名等）、安全配置（安全认证、安全策略等）以及产品定制化配置（例如消息队列、缓存、数据库的个性化配置）。	
3.		②支持根据资源申请需求内容自动化供应资源。	
4.		③用户/租户可方便查看已申请的资源信息，包括但不限于资源详细信息、申请时间、申请人、资源失效日期、计费情况等。	
5.	资源控制台	①分组管理已申请的实例资源，包括实例的扩容、基本和个性化配置修改，实例启动、重启、关机，实例安全认证、安全策略管理，实例续租、退还。	
6.		②资源镜像（虚拟机）管理，可以创建、启动及销毁资源镜像。	
7.		③在线远程连接工具，通过内嵌的远程登录工具来登录虚拟机或容器。	
8.	资源弹性管理	①实例配置：按照实例维度配置需要弹性伸缩实例的硬件资源、网络资源和环境信息等。	
9.		②启动配置：为伸缩实例配置启动和关闭策略，并支持展示、搜索实时和历史实例伸缩信息。	
10.	安全管理	展示、新建、修改、删除安全策略，包括 IP、端口、协议的访问权限。	
11.	资源配置策略管理	管理各条线或项目的资源分配策略。	
12.	资源审计	支持资源审计展示和各类报表生成导出。	
13.	资源计费	①云平台支持资源的计量计费，可以支持对资源进行消费情况的计费。	
14.		②管理员可以为不同的服务配置不同的费率，可以查看历史定价情况进行参考，并可以查看各个组织的费用情况。	

15.		③支持将费用报告导出或定时发送到用户通知中心。	
16.		④支持管理员或运营人员自定义计量计费报表,可以指定数据中心、区域的哪些对象生成表格或者图表方式的计量计费报表,可以定时发送到用户通知中心。	

1.4.4.2.11. 备份管理

序号	指标名称	要求	备注
1.	可视化管理平台	具备独立的可视化异地备份管理平台。	
2.	备份选择	支持本地备份;支持备份到另一朵云或独立的对象存储设备;	
3.	备份策略	存储备份支持重删、压缩技术,用以减少 I/O 传输量和云备份存储量	
4.	备份恢复	支持常规恢复和云重建恢复,云重建恢复用于应对生产云发生灾难性故障导致重建场景的数据恢复。	
5.	备份计划	支持自定义备份计划;支持创建、启动、停止备份计划;支持备份日志、备份记录查看。按备份策略执行备份,按以天为单位的时间间隔进行周期性备份,可设置备份时间和保存时长	
6.	恢复任务管理	支持按备份记录或按时间节点进行恢复;支持创建、启动、停止、和查看恢复任务;支持查看恢复实例的日志信息。	

1.4.4.3. PaaS 云管需求

1.4.4.3.1. 关系型数据库管理

序号	指标名称	技术要求	备注
1.	统一访问	提供统一数据库页面访问入口,避免使用人员直接填写数据库账号密码。	
2.	细粒度权	支持细粒度权限管理策略,支持库、表等数据库对象	

	限管控	粒度, 查询、导出、修改等运维操作粒度的精细化管理。	
3.	便捷权限管理	提供友好的用户与权限查看、管理功能, 支持自定义分配纳管数据库中不同的用户权限, 支持权限有效期管理, 可到期自动回收、可主动按时间周期授予、可主动按需随时回收	
4.	灵活可控的审批流程	支持单个实例级别配置不同的安全规则, 自定义审批流程与策略, 提供借口或对接中心现有流程管理系统。	
5.	操作可审计可溯源	提供系统内人员所有操作的记录和审计; 审计功能, 对用户的登录、登出、SQL 操作、表结构变更、表数据变更、导入、导出、流程审批、用户修改等操作及操作是否成功都有记录, 支持用户操作日志的查询	
6.	查询超时控制	支持单个实例级别设置查询超时时间, 避免慢 SQL 影响数据库性能	
7.	全表扫描限制	支持全局设置数据库大表扫描阈值, 表大小超过阈值后不允许全表扫描的查询 SQL 执行计划确保有走上索引才可发起; 支持自定义 SQL 审核策略, 如禁止手动输入执行全表扫描、no where 语句等, 如需操作可通过审批流程。	
8.	全局查询总行数限制	支持全局设置每次查询的返回行数	
9.	单用户单天查询总管控	支持全局设置每个用户每天的查询总次数、查询返回总行数上限, 遇到阈值后发出告警给系统管理员评估	
10.	语法正确性保障	提供统变更统一管理, 支持语法正确性校验、行数校验、变更类型校验后提交“数据变更”工单流程	

11.	定时调度支持	数据库变更可立即执行、定时执行，操作内容包括 SQL 语句执行、参数修改、数据库重启等操作。	
12.	变更完整性支持	数据变更可支持完整性执行，全工单执行成功则成功，遇到失败则全部回滚	
13.	备份保障	对 update、delete 的内容在变更前，支持自定义策略生成数据备份，更新不符合预期时可快速回滚恢复。	
14.	性能前置检查	支持设置变更前环境检查策略，在数据库变更执行前会校验数据库当前负载，若过高则中断调度并返回	
15.	变更缓冲保障	数据库变更执行后会自动 sleep 相应时间，避免瞬间更新过多造成主备复制、磁盘 IO 的延迟	
16.	协同变更	支持人员在线协同变更，避免人员单点影响变更进度	
17.	可视化结构设计	支持可视化展现包括集群、实例、数据库等多个粒度的架构。	
18.	可视化数据库表管理	提供图形化的数据库创建与管理集群、实例、数据库、表空间、数据库表的创建与管理功能	
19.	可视化 SQL 查询管理	提供友好的 SQL 查询调试功能，并提供图形化的执行计划展示，对展示的慢 SQL 提供参考优化建议	
20.	可视化导入导出管理	提供友好的数据导入导出运行界面以及查看状态与进度的界面	
21.	可视化 SQL 查询管理	提供 SQL 窗口、SQL 命令行、表数据管理、SQL 智能提示、SQL 格式化、自定义 SQL、SQL 模板、SQL 执行计划、导入导出等管理功能	
22.	可视化数据库对象管理	提供库、表、同义词等对象管理功能	

23.	SQL 代码审核	代码涉及增删改查的 SQL 可通过 SQL 审核进行 review, 确保没有 SQL 注入、不合规 SQL、无索引 SQL 发布上线	
24.	多角色权限管理	支持以集群、实例、数据库等粒度为维度的数据库岗用户权限管理功能, 根据自定义用户权限模板, 进行用户权限分配与检查。	
25.	系统用户管理	系统内置用户组管理策略, 对系统功能进行细粒度管理, 根据开发、测试、运维管理等不同使用场景设置多类别的用户组。	

1.4.4.3.2. 数据库同步工具管理

序号	指标名称	要求	备注
1.	数据同步	可视化配置数据库的同步设置	
2.	任务管理	在数据同步任务运行过程中, 用户可在线新增或移出所需同步的对象, 而无需重新创建任务	
3.	运行日志	提供应用实时运行日志的 Web 界面可视化展示, 任务出错时, 展示错误信息及处置建议。	
4.	数据校验	支持对迁移/同步的源端和目标端数据进行全量校验, 并对校验结果进行可视化展现	
5.	告警监控	完善的监控体系。数据同步提供同步作业状态、同步延迟的报警监控功能。用户可以根据业务敏感度, 自定义同步延迟报警阈值、配置任务告警。	
6.	系统用户管理	系统内置用户组管理策略, 对系统功能进行细粒度管理, 根据开发、测试、运维管理等不同使用场景设置多类别的用户组。	
7.	操作可审计可溯源	提供系统内人员所有操作的记录和审计; 审计功能, 对用户的登录、登出、配置修改等操作及操作是否成功都有详细的记录, 可以通过日志审计功能, 进行用户操作日志的查询, 可详细操作记录	

1.4.4.3.3. 分布式缓存管理

序号	指标内容	要求	备注
1.	实例管理	提供多种规格的缓存数据库实例, 支持实例的创建、	

		重启、释放、备份等管理操作, 支持在控制台清除全部数据和清理过期数据; 支持实例的网络隔离	
2.	会话管理	支持实例会话管理, 可查看会话列表, 具体操作, 执行耗时等信息, 可对会话进行批量 kill 等管理操作	
3.	缓存分析	支持缓存分析, 支持查看 key 在内存的占用和分布信息, 支持大 key 分析	
4.	持久化	同时支持 RDB 和 AoF 持久化机制, 支持可视化设置 AoF 落盘开关, 保障数据丢失最小化	
5.	备份	支持可视化的实例手动和自动备份, 支持自动备份策略设置, 支持主从、集群版等多种形态实例的原地恢复, 克隆实例, 支持备份集下载	
6.	域名修改	支持域名访问和域名修改, 支持端口号修改, 避免默认端口号扫描风险	
7.	权限设置	支持多账号, 支持设置读写、只读权限, 最小化授权提供更高安全保障	
8.	白名单设置	支持可视化白名单设置, 提供灵活的安全访问管理能力	
9.	多角色权限管理	支持以集群、实例、数据库等粒度为维度的数据库用户权限管理功能, 根据自定义用户权限模板, 进行用户权限分配与检查。	
10.	系统用户管理	系统内置用户组管理策略, 对系统功能进行细粒度管理, 根据开发、测试、运维管理等不同使用场景设置多类别的用户组。	
11.	操作可审计可溯源	提供系统内人员所有操作的记录和审计; 审计功能, 对用户的登录、登出、配置修改等操作及操作是否成功都有详细的记录, 可以通过日志审计功能, 进行用户操作日志的查询, 可详细操作记录	

1.4.4.3.4. 容器管理

序号	指标内容	要求	备注
1.	集群操作审计	①支持查看集群中的事件整体概览以及重要事件（访问、命令执行、删除资源、访问保密字典等）的详细信息。；	
2.		②支持查看集群中常见的计算资源、网络资源以及存储资源的操作统计信息。操作包括创建、更新、删除、访问。支持查看集群中某类资源的详细操作列表	
3.		③支持自定义时间维度查询。	

4.	日志管理	支持容器实例日志查看和应用日志采集	
5.	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,可修改已部署 yaml 配置	
6.	容器伸缩	支持可视化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伸缩,支持配置容器资源阈值进行容器实例的自动伸缩。	
7.	容器存储管理	支持从页面上进行容器存储卷(本地存储、块存储、文件存储、对象存储)的生命周期管理	
8.	容器实例远程控制	容器实例支持以终端方式进行远程访问控制	
9.	白屏化编排	支持页面对资源进行编排,资源包括: Deployment、StatefulSet、DaemonSet、Job、CronJob 等	
10.	组件生命周期管理	支持可视化容器服务组件安装、卸载、升级等生命周期管理能力。	
11.	节点伸缩	支持自助添加和删除节点,伸缩过程中无需人工干预。支持通过弹性伸缩组自动创建工作节点并加入集群。支持设定缩容规则触发后自动下线工作节点。	
12.	节点区域支持	支持工作负载节点跨可用区统一管理	
13.	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自助创建和删除集群。	
14.	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、组件、应用的运行状态,集群的事件记录以及集群的当前的资源使用情况。	

1.4.4.3.5.微服务平台管理

序号	指标内容	要求	备注
1.	应用生命周期管理	提供可视化分布式应用管控平台,对应用进行生命周期管理,包括但不限于应用的创建、部署、启动、扩容、停止和下线。	
2.	服务网格管理	支持服务网格的创建、修改、组件安装卸载及服务列表和详细信息的查看。 服务注册、灰度发布、负载均衡、会话保持、流量限制、故障注入、服务熔断、服务间认证、服务鉴权等管理操作。	
3.	全链路流量控制	支持 SpringCloud、Dubbo 框架的全链路流量控制操作,可以快速灵活地创建一个流量控制环境,将具有	

		一定特征的流量路由到目标版本应用。	
4.	定时弹性	支持应用集群配置定时弹性,指定时间触发弹性策略,实现自动扩缩	
5.	日志审计	支持审计功能。对所有用户的所有操作能够记录在案,并提供审计日志的查询界面。	
6.	实时日志	提供 Web 界面形式查看实例中应用的实时日志。	
7.	日志目录	添加日志文件和目录,并支持在线查看。	
8.	服务鉴权	在分布式服务框架控制台上可以创建和管理服务鉴权规则。根据鉴权规则,被调用方将可开闭允许或禁止调用方调用其接口,进行服务调用的安全管控。	
9.	服务隔离	支持在一个租户下通过命名空间隔离的方式实现多套环境并存,命名空间提供服务名在注册中心的逻辑隔离。	
10.	离群实例摘除	创建和管理离群摘除策略。当策略被触发时应用实例将被自动摘除。	
11.	灰度发布管理	支持灰度发布应用。发布过程支持分批操作以保证业务连续性,且分批过程可以指定手动或自动触发。支持按内容和按比例的比例发布策略。发布应用的过程中支持配置启动命令、环境变量和应用生命周期管理。	
12.	配置中心管理	支持应用维度配置管理,提供可视化的方式进行配置管理,配置中心支持在线、准实时变更服务配置,支持配置文件的多版本管理维护。	

1.4.4.4. 应用云管需求

序号	指标名称	要求	备注
1.	虚拟机应用发布	①提供应用全生命周期的 DevOps 自动化支持,关联应用所属的基础资源	
2.		②提供应用服务实例模型,同一应用可以有不同服务实例作为发布单元进行管控,之间提供安全组、白名单、VPC 网络等技术实现的隔离。	
3.		③提供应用的发布、回滚,用户可以对需要发布的应用编辑依赖关系、调整服务器分组,并选择部署策略等	

4.		④提供分组发布、灰度发布、单机房发布、蓝绿发布等多种灵活的部署策略	
5.		⑤提供单元化部署的逻辑分区管理，定义服务通信边界，具备无损发布、高可用应用架构（包括同城双活、异地多活）、容灾切换和切回等能力。	
6.		⑥蓝绿发布，支持不同分组（如单元、环境等）部署应用，实现不同分组下应用并行发布，提供灵活的发布策略，支持应用的引流验证。	
7.		⑦支持发布包管理，展示当前应用的发布包相关信息，包括应用名、发布包个数、版本、发布包创建时间、负责人等。	
8.		⑧通过技术栈来管理应用在发布部署时需要安装的软件包以及要执行的部署脚本	
9.	自动化运维	①以应用视角提供模板化运维编排能力，提供批量重启，上线，下线，静态资源部署，初始化服务器等多种运维操作	
10.		②可以选择系统提供的或自定义的VM运维部署脚本	
11.		③提供录入，执行用户自定义的运维命令和脚本通道	
12.		④支持虚拟机、负载均衡、虚拟网络VPC，虚拟交换机、安全组等基础资源进行管理	
13.		⑤操作记录和审计，查看每个操作的任务日志，对执行失败的操作进行重试	
14.	容器集群管理能力	①集群创建与升级：集群可视化部署和升级，支持通过前端页面进行新集群的创建，包括网络、master和node数量、日志组件等	
15.		②集群运维管理：支持集群详情查看，节点扩缩容，	

		节点标签设置，不可调度/恢复调度/驱逐 pod， kubectl 客户端访问	
16.		③命名空间管理：支持命名空间创建/删除，添加标签；支持命名空间资源配额	
17.		④镜像管理：私有镜像中心，支持命名空间创建， 镜像构建、镜像上传和拉取等	
18.		⑤镜像构建：支持从代码仓库构建容器镜像；支持 从制品包（如 jar 等）构建容器镜像	
19.		⑥访问服务：提供集群内和多集群负载均衡和 service 访问能力；	
20.		⑦IP 地址管理：可查看各 IP 池的 IP 使用情况，以 及 IP 的使用对象	
21.		⑧安全隔离：支持主机、命名空间、pod 不同维度的 网络策略配置，可按需管控集群内、集群外的安全 访问策略	
22.		⑨Pod 管理：支持容器的删除功能、可通过浏览器直 接登陆容器、终端日志查看	
23.		⑩日志采集：支持集群组件、主机和应用业务的日 志采集	
24.		⑪监控采集：支持集群、命名空间、主机、工作负 载等多维度监控数据采集	
25.	应用发布 管理能力	①镜像发布：支持以镜像的形式发布到容器平台	
26.		②流水线对接：提供 OpenAPI 对接主流 CICD 流水线 工具作发布单部署创建	
27.		③应用服务：创建应用服务，并进行容器应用服务 发布，可提供灰度发布能力。提供发布审计，可进 行版本管理对历史版本进行回退。	

28.		⑤访问配置：进行服务访问配置设置，例如统一接入实例，负载均衡等	
29.		⑥热更新：支持快捷更新容器，使应用实例原地热升级，无需重启 pod	
30.		⑦分组发布：精细化发布控制，可对应用实例进行多策略分组，实现实例级灰度，配合暂停功能，提升发布控制力度	
31.		⑧发布单审计：发布过程强管控，可实时查看发布状态，相关步骤和关键日志信息	
32.		⑨运维单审计：运维过程强管控，可实时查看运维操作，相关步骤，如 Pod 重启等	
33.		⑩发布过程可应急回滚：支持分组暂停、支持应急回滚至历史版本	
34.		⑪版本 diff 比较：支持多版本间配置进行比较	

1.4.5. 监控平台详细需求

1.4.5.1. 整体监控要求

提供统一的运维入口，支持通用运维、产品运维、安全合规和系统配置等功能，简化日常运维操作，提升运维效率。

（1）支持云内全部组件的监控覆盖，可实现监控策略配置、告警规则配置、告警查询、策略管理、信息推送管理。支持图形化配置、展示界面。

（2）支持与其他已建运维管理系统对接需求（包括但

不限于配置管理系统、集中监控平台）。支持将统计分析结果、原始采集数据或整理后的数据及时发送给其他运维管理系统，需提供清晰、标准的数据调用方式，数据类型包括但不限于性能数据（指标数据）、告警数据、配置数据、日志数据等。

（3）支持云内日志管理，包括日志采集、日志分析、日志检索、日志查看、日志导出等。

（4）支持监控组件自监控，实时对云平台整个监控系统的运行状态进行监控，异常时推送告警通知。

（5）支持审计日志。

（6）支持与其他运维管理系统的集成对接。。

1.4.5.2. 平台监控要求

序号	功能	功能需求描述
1.	统一门户入口	建立直观、真实的运维展现门户，综合展现用户 IT 环境中的服务器、存储、网络和安全设备、操作系统、数据库等各种 IT 资源运行情况以及运维技术人员的日常运维管理工作情况，有效的展示内部 IT 资源运行情况、性能状况等，满足不同人员对系统直观了解的需求，实现全平台监控统一化、数据的可视化。
2.	告警管理	1、告警概览:展示按照告警级别维度统计告警数量，显示 TOP10 告警和 TOP10 告警源。 2、告警列表:支持查看和处理当前所有告警，根据需求自定义查询所需查看的告警信息，并以 Excel 报表格式导出。 3、告警设置:支持设置告警联系人。 支持系统默认模板或自定义告警模板，可根据实际需求

序号	功能	功能需求描述
		调整告警触发规则。支持设置告警通知通道,并按设置的推送参数推送告警信息,并支持通过钉钉、邮件远程推送告警信息。支持添加和解除告警屏蔽规则。
3.	巡检管理	1、一键巡检:支持启动系统预置巡检和自定义巡检任务。支持查看近期巡检结果。 2、巡检大盘:展示近期巡检状态、数据总览、巡检项的异常分布与总体趋势、巡检任务记录、巡检问题和最新巡检报告。 3、巡检报告:支持查看所有巡检报告,以便了解系统的问题或故障情况。 4、巡检场景配置:支持查看、新增、修改和删除巡检场景配置。 5、巡检记录查询:支持查询系统巡检记录及相关巡检报告。支持停止运行中的巡检任务。 6、巡检项查询:展示所有巡检项的详情信息。 7、巡检数据包配置:支持导入和导出巡检数据包。
4.	运维编排	支持查看主机资源(包括物理机、容器和虚拟机)信息,包括主机名称、IP地址、集群名称、操作系统等。 支持查看容器资源信息,包括服务角色名称、类型、宿主机名称、宿主机IP地址、项目名称、集群名称和服务名称等。 提供常用默认脚本库,支持自定义脚本,并支持查看、修改、导入和导出脚本。 脚本库是用于存放各个功能的脚本。脚本内容支持Python和Shell格式。 支持根据运维场景自定义运维作业,并支持查看、修改、执行、导入、导出和删除运维作业。 运维作业是针对运维资源、软件、脚本的功能集合,将不同功能脚本按照定义的顺序在不同目标主机或容器

序号	功能	功能需求描述
		上执行。 支持自定义流程编排，并支持查看、修改、运行、导入、导出和删除审核流程，并通过图形化展示流程编排包括的操作任务及整体流程。 流程编排是将一系列有逻辑的动作(包括脚本和作业)组成一个自动化运维任务。 支持运维作业管理，包括创建、导入、查看、导出、修改、执行和删除运维作业。 支持查看、删除运维作业执行历史记录，支持终止作业，查看执行报告以及下载结果 支持查看任务执行结果。支持查看各种自动化运维操作的日志。
5.	安全运维	(1) 支持运维角色管理，可以进行角色授权。支持设置运维 IP 白名单配置。 (2) 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、禁止等 (3) 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。
6.	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。 1、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。 2、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。 3、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。 4、在最近 7 天运行情况 区域，查看最近 7 天任务的运行趋势。” 5、支持修改任务的灰度策略即调整机器的执行批次。 6、支持删除不再使用的任务 7、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。 8、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。 9、支持查看任务的执行情况

序号	功能	功能需求描述
7.	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。
8.	报表管理	对硬件设备、网络设备、系统、中间件等的性能、可用容量指标通过采集方式可定制化生成相应报表,每日定时发送至制定管理员。
9.	工单管理	支持与已有流程管理平台对接,提供平台工单的管理,包括但不限于服务工单、内部工单、事件工单等。
10.	故障隔离	具备对云平台软硬件故障的自动发现和隔离能力。
11.	故障自愈	具备对云平台软硬件故障的自动检测和恢复能力。
12.	日志管理	1、平台需要支持各模块服务节点的状态监控和实时日志展示。 2、支持审计日志管理功能,包括可以查看(按操作、类型、名称、时间)、搜索、备份;能够对云管平台的审计日志归档、日志下载、归档记录。
13.	系统性能	支持不低于100个用户同时使用平台,每个数据中心纳管服务器节点数不少于3000个且用户页面响应时间不超过3s;批量纳管服务器节点不少于1万个,并可扩展。
14.	可视化运维	提供图形化界面的运维管理工具,具有可视化实时监控、自动化运维、报警、参数管理、集群管理、租户管理、日志管理、健康巡检等功能
15.	大屏展示	支持云平台运营大屏,支持预置大屏和自定义大屏。预置应至少包括租户云资源、云网络监控、云安全监控、云告警监控、多区域云资源等大屏,全方位多维度实时展示混合云的运行和资源使用状态。自定义大屏应提供可视化大屏在线编辑器,支持自定义数据来源,自定义

序号	功能	功能需求描述
		每个内容的不同呈现形式（例如柱状图、饼图、仪表盘、地图等），支持拖拽方式，所见即所得，快速实现业务数据大屏的个性化定制。
16.	接口要求	1、支持开放所有的 REST API。 2、支持对 API 的权限授权及认证。 3、提供完备的 REST API 文档。
17.	多租户管理	1、提供多级租户体系，支持灵活的组织架构管理。 2、支持为下级的租户分配不同的资源配额和资源访问权限，服务授权。 3、支持查看租户各云服务的资源使用、消费情况记录。
18.	监控和告警	1、基础设施监控，支持对数据中心服务器、存储以及网络设备等硬件设备进行统一监控管理，提供告警、资源和性能等全方位监控能力，提供监控大屏展示，帮助用户对于硬件问题进行快速定位和处理故障。 2、云资源监控，提供云资源告警、资源和性能等全方位监控能力，帮助用户对于云资源保障问题进行块定界定位。 3、操作系统监控，支持对各种操作系统 CPU、内存、IO 等性能数据采集以及监控展示。 4、对网络互联关键路径提供对连通性探测的探测监控，及时发现设备僵死等情况下的网络异常并生成对应告警。 5、应用监控，支持对应用性能指标的管理。 6、能对接短信、EM 等外部平台。 7、自定义大屏，根据需求自定义大屏展示；实现对其他专业监控系统的告警等信息进行统一纳管。 8、集中式告警统计，以告警对象为中心，从多个维度辅助分析，提升故障定界效率。 9、重复告警汇聚，将指定周期内上报的重复告警汇聚到同一个告警下，以减少海量重复告警对运维的干扰。 10、告警相关性分析，通过定义告警之间的根源衍生关系，在监控或查看告警时可以将衍生告警过滤掉，只关注要处理的根源告警。

1.4.5.3. IaaS 监控要求

序号	功能	功能需求描述
1.	资源与配置管理	1、产品维度: 支持从云产品维度查看云平台全部资源, 包括各产品及其集群、服务、服务角色、虚拟机详情。支持对目标服务角色进行重启 SR 操作。支持对目标服务角色进行安全运维操作。 2、机房维度: 支持查看机房中的机柜、服务器相关信息。支持查看物理机监控信息并查看、修复和删除报警信息。 3、网络维度: 支持查看云平台中的全部网络设备的基准拓扑信息。支持查看云平台中的全部网络设备的实时拓扑信息。 4、资源标签: 支持关注资源的添加、查看和删除。支持资源标签的添加、查看、绑定、删除。 5、提供统一的资源配置管理, 包括但不限于信息增删改查、服务器开机/关机/重启、服务器带外管理等。 6、提供包括资源使用情况(资源包括但不限于云主机、存储)。
2.	库存管理	库存分析, 支持查看各资源统计数据产品 (Vcpu、vMemory、裸金属服务器、云硬盘、弹性 IP 等分配量及总量, 以及容量风险分布。
3.	分布式存储运维	(1) 分布式存储总览: 支持显示存储集群服务器数量, 总容量, 以及异常服务器/异常磁盘数量。 (2) 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。 (3) 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。
4.	服务器运维	支持对服务器进行操作系统层面监控, 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, 网络丢标等常见异常。
5.	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。
6.	指标监控	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 CPU、内存进行监控, 为用户提供系统级、主动式、细粒度监控服务。 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, 自动执行伸缩规则, 动态调整伸缩组

序号	功能	功能需求描述
		内的云主机的实例数量，监控指标包括但不限于 CPU 使用率、内存使用率、内网出流量、内网入流量等。
7.	流量监控	支持存储空间监控/使用流量监控/每小时请求数；能够统计公网流量、流出流量，内网流入、流出流量；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。
8.	容器监控	支持集群、节点、应用、容器实例层面的监控，支持集成 Prometheus 服务的能力，为集群提供全方位监控大盘
9.	监控和告警	1、基础设施监控，支持对数据中心服务器、存储以及网络设备等硬件设备进行统一监控管理，提供告警、资源和性能等全方位监控能力，提供监控大屏展示，帮助用户对于硬件问题进行快速定位和处理故障。 2、云资源监控，提供云资源告警、资源和性能等全方位监控能力，帮助用户对于云资源保障问题进行界定定位。 3、操作系统监控，支持对各种操作系统 CPU、内存、IO 等性能数据采集以及监控展示。 4、对网络互联关键路径提供对连通性探测的探测监控，及时发现设备僵死等情况下的网络异常并生成对应告警。 5、应用监控，支持对应用性能指标的管理。 6、能对接短信、EM 等外部平台。 7、自定义大屏，根据需求自定义大屏展示；实现监控系统的告警等信息进行统一纳管。 8、集中式告警统计，以告警对象为中心，从多个维度辅助分析，提升故障定界效率。 9、重复告警汇聚，将指定周期内上报的重复告警汇聚到同一个告警下，以减少海量重复告警对运维的干扰。 10、告警相关性分析，通过定义告警之间的根源衍生关系，在监控或查看告警时可以将衍生告警过滤掉，只关注要处理的根源告警。

1.4.5.4. PaaS 监控要求

云平台提供的 PaaS 产品具备跟云平台为一体的统一监

控能力。

序号	指标名称	要求	备注
1.	服务监控	所有云平台提供的 PAAS 产品均具备监控能力，并提供跟云平台一体化的监控平台，实时监控 PAAS 产品服务状态，可图形化显示监控核心指标信息。 在发生异常时实时报警，支持不限于邮件、短信等方式。	

1.4.5.4.1.关系数据库监控

序号	指标名称	要求	备注
1.	监控界面	提供图形化界面的数据库运维管理工具，具有可视化实时查看：集群运行状态、CPU 用量、数据用量、磁盘 IO 量、数据写入量、SQL 查询量。并针对预设监控水位指标，自动报警。	

1.4.5.4.2.分布式缓存监控

序号	指标名称	要求	备注
1.	监控界面	支持秒级粒度监控，支持自定义监控项，包括基础监控(cpu, 内存, qps, 命中率, keys, expiredkeys 等)、string, hash 等常见类型监控，事务，订阅等监控	

1.4.5.4.3.容器监控

序号	指标名称	要求	备注
1.	监控界面	支持集群、节点、应用、容器实例层面的监控，支持集成 Prometheus 服务的能力，为集群提供全方位监控大盘	
2.	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、组件、应用的运行状态，集群的事件记录以及集群的当前的资源使用情况。	

1.4.5.4.4.微服务组件监控

序号	指标名称	要求	备注
1.	高可用监控	微服务基础组件的高可用监控，显示当前集群的可用状态包括，注册中心、配置中心、Api 网关、流量管理等	
2.	流量性能监	微服务基础组件的流量负载和运行负载情	

	控	况包括，注册中心、配置中心、Api 网关、流量管理等	
--	---	----------------------------	--

1.4.5.5. 应用监控服务

提供云上监控服务，分为管理端和后台，监控服务管理端并入云管平台。监控服务后台包括指标度量（Metric）、日志服务（Log）、链路追踪服务（trace）等模块，各模块需基于主流技术标准和规范。用户可通过指标监控服务实现应用资源使用状态、系统吞吐量、JVM 指标等全局化展示应用健康度；通过日志服务实现敏捷构建日志聚合分析功能，并基于云管平台实现日志多维度查询和图形化展示；通过链路追踪构建分布式应用各模块节点运行详情。同时，各模块通过告警策略设置与告警机制联动。

1.4.5.5.1. 分布式链路

提供分布式链路集成控制台，图形化展示整个调用的执行过程，展现形式包括时序图，展现内容包括 HTTP、RPC、数据库访问、缓存访问；图形化展示应用分组内及分组间链路统计信息，并能通过链路日志关联应用业务日志。

序号	指标内容	要求	备注
1	全链路应用拓扑	持续自动发现全局应用间调用，以及对中间件的依赖调用架构关系，绘制完整的全局拓扑；	

		在拓扑中展示节点和连线异常状态，帮助用户更快感知到故障问题	
2	应用性能分析	支持导入导出配置模板	
		展示所选节点的黄金指标统计（比如吞吐量、平均响应时、错误率、满意度等）趋势和指标明细，并默认提供 Service（RPC 调用）、SAL（RPC 调用）、CAL（缓存调用）、DAL（数据库调用）、HttpClient、HttpServer 等节点调用类型指标统计；	
3	多维链路查询	展示所选节点的黄金指标统计（比如吞吐量、平均响应时、错误率、满意度等）趋势和指标明细，并默认提供 Service（RPC 调用）、SAL（RPC 调用）、CAL（缓存调用）、DAL（数据库调用）、HttpClient、HttpServer 等节点调用类型指标统计；	
		支持基于应用->上下游应用->接口等逐层下钻分析，建立由底层到上层间的数据关联信息，从而深度分析分布式场景下的影响应用性能的问题根因	
4	链路详情	提供系统间调用的链路图、拓扑图等，清晰全方位的展现系统间调用的交互、性能和异常信息	
		支持接入多类型日志数据源，将链路和业务日志进行关联，增强链路上的业务信息	

1.4.5.5.2.业务实时监控

提供海量日志实时分析解决方案，能够以日志、REST 接口、Shell 脚本等作为数据采集来源，提供设备层、应用层、业务层等各种视角的监控能力，为线上系统可用率提供有效保障。提供对中间件的监控，如分布式服务注册中心、分布式消息服务、分布式调度服务、分布式事务服务等组件的监控告警能力。同时提供数据统计的监控产品类型，用于配置个性化的业务监控项，可视化，丰富的可视化 Dashboard。

序号	指标名称	要求	备注
1	业务监控	支持对应用系统的业务日志进行灵活拉取和切割，并按多种维度聚合数据，使用监控像使用 SQL 一样简单； 具备秒级/分钟级 多 Key、常用服务指标、单笔统计 TOP 等最佳实践业务监控模版，帮助用户快速创建业务指标； 提供灵活丰富的自定义大盘能力，基于业务指标提供一套完整的业务实时分析及预警能力； 支持个性化的、非标的业务监控场景，例如交易量，并提供文件夹方式管理和分类业务监控	
2	应用监控	提供应用分析能力，当应用发布成功后，可自动将应用监控起来，并以各种维度和视角的监控大盘展示，以此满足应用研发	

		或运维人员对应用的监控，保证应用的运行稳定性； 支持同时对容器应用和经典应用统一监控； 提供对应用从内到外的多样监控指标，如服务指标、系统指标、JVM 指标、端口探测等，真正实现应用全方位可观测 按照应用单实例、单机房、单元化等视角对监控指标进行多视角聚合，从多维视角发现业务连续性和稳定性	
3	一站式分析	基于元数据实现对应用的指标、链路和日志数据的一站式整合分析； 实现从应用 > 服务 > 实例 > 主机的上卷下钻的多维关联分析，迅速找到异常故障点	
4	主机监控	支持同时对物理机和虚拟机的统一监控； 提供对主机的系统指标、端口探测等监控能力；提供常见的指标统计模板（如分钟统计/无 key，分钟统计/多 key，秒级统计，分钟统计等）	
5	日志查询	支持精确查询、模糊查询、全文查询和关键字段查询，以及日志上下文查询	
6	链路关联	支持选中日志中的链路 tracerid 字段后，将提示用户是否需要根据该 tracerid 查询并跳转到链路详情	
7	Livetail	从最新的日志数据中提取出关键信息，以便快速分析出异常原因。提供日志数据实	

		时监控的交互功能 LiveTail，针对线上日志进行实时监控分析，减轻运维压力。	
8	日志快照	支持将常用查询保存为快捷历史，一键将查询历史条件导入再次查询	
9	日志采集存储	支持按照应用指定日志路径采集，以及提供采集全套流量监控，保证日志数据采集的完整性；日志数据支持自定义持久化存储时间，提供更灵活和高可靠的存储保证	
10	日志转储	支持按照应用指定日志路径采集，以及提供采集全套流量监控，保证日志数据采集的完整性；日志数据支持自定义持久化存储时间，提供更灵活和高可靠的存储保证	
11	日志下载	支持选择一段时间范围的日志按 CSV、TXT 等格式下载导出	
12	告警模版	为了提升配置告警效率，提供创建告警模版，基于模版选择生效对象可快速批量创建告警规则	
13	告警规则	支持灵活的为监控对象配置自定义告警规则和 PQL 告警规则当规则条件被触发时，规则中的每个触发对象都将产生一条告警事件，并为通知对象发送告警消息，以提醒用户采取必要的解决措施	
14	告警事件	告警事件是一个告警对象从触发到恢复的全生命周期管理，具有唯一事件 ID；当规则被触发后，产生告警，在恢复之前，所有产生的告警都属于这一事件	
15	告警恢复	告警防抖机制，告警规则只有连续 N 个检	

		测周期都触发，会产生一个告警记录，当告警规则在连续 N 个检测周期都不触发，会产生一个告警恢复记录	
16	告警静默	若告警规则一直处于触发状态，首次触发告警后，静默期后才会发送第二次告警信息；若据恢复正常，会收到数据恢复通知并解除告警；若数据再次触发告警，则会再次发送告警信息。	
17	告警暂停/开启	由于某些暂定原因需对规则暂停告警，暂停期内将不会进行检测和产生告警	
18	配置模版	提供监控告警配置模板功能，支持将应用和自定义监控告警以配置模板(JSON 文件)导出，然后一键导入其他环境。如该环境已部署同名应用，则监控告警配置即生效，帮助投产运维更加高效便捷和一致	
19	元数据管理	采集强依赖应用系统和主机元数据，通过控制台将监控告警配置和生效对象元数据自动下发给 agent，agent 才可以采集对应的可观测性数据提供元数据模型和元数据实例的信息展示，帮助用户更好的运维和排查监控数据问题；并具备手动录入和导入元数据信息，以及提供自定义 API 接口对接第三方系统的 CMDB	
20	Agent 管理	RMS Agent 管理分为容器和经典两部分组成，容器 agent 为 daemonset 方式自动部署到 Kubernetes 集群每个主机上；经典 agent 通过控制台手动批量将 RPM 包方	

		式部署到每个主机上，该部分主机可以是物理机、VMWare 虚拟机、ECS 等；Agent 管理提供对 Agent 的部署、升级，以及状态信息的查看，帮助用户更好的运维监控 agent	
21	低资源占用	在完成大量数据可靠采集和传输的同时，保证对宿主机的 CPU、内存等资源的使用限制和极低占用率	
22	数据计算和存储	支持分钟级对万台设备的实时监控和在线持续聚合数据，智能分级存储存放策略，时序数据库保证数据容量可控和弹性扩缩平台	
23	高可用	支持双机房容灾架构，组件多实例运行，数据库多副本同步，并提供自监控、故障自动恢复等能力	
24	兼容多框架协议	监控方面原生采集 Sofa 框架日志的业务和服务指标，也支持采集符合 Open-Metrics 的 prometheus 指标，并都作为统一标准格式存储为时序数据；链路方面原生应用进行无缝对接，用户的业务代码无需任何修改即可轻松接入，也支持接收 zipkin、skywalking 等符合 Open-Tracing 的链路数据，统一生成应用拓扑和链路追踪	
25	开放自主	所有组件皆为自研可控，并经过大规模生产验证；提供完善的产品功能和数据的 OpenAPI，可更好的和第三方系统集成对	

		接	
--	--	---	--

1.4.6. 云安全服务详细需求

1.4.6.1. 安全要求

安全服务产品采用软件或硬件解决方案。若采用软件解决方案，需支持云安全管理功能，能对云上提供对安全资源的统一调度和管理，实现安全设备从创建到激活、配置、删除全生命周期的管理。同时能够提供云平台组织管理、 workflow 管理、自助界面等功能，实现从安全资源的申请、审批到部署的自动化。如采用硬件方案服务器资源不可占用业务需求所需的服务器资源。

1.4.6.2. ★云平台安全要求

投标人及原厂商须提供以下安全服务，以满足安全要求。

序号	类别	功能点	详细描述
1.	基础安全	网络安全	提供安全防范措施保障云边界安全，包括但不限于安全网络安全区域防护、互联网/专线入口防护以及云环境下的区域隔离等维度。
2.		平台安全	1. 平台具备一定的自我防护能力，能对平台代码层及运行时的漏洞检测，能对平台依赖运行的中间件、数据库、操作系统等安全补丁、安全漏洞情况进行监控、检测。 2. 平台应对所有的用户输入进行校验，防止 SQL 注入和 XSS 跨站脚本攻击。

3.		身份安全	采取有效措施保护身份鉴别信息安全，在对身份鉴别信息进行加密处理时，应采取有效措施防止登录重放攻击。身份认证时，应防止暴力猜解。平台管理端的用户登录需支持标准认证协议，包含但不限于 Radius、Oauth 等。
4.		密码安全	(1) 用户名应支持数字字符、字母、下划线等常用字符。 (2) 用户口令应支持数字、字母以及其他至少三种以上字符要求，提高系统登录安全。 (3) 用户口令长度至少为 8 个字符以上。 (4) 密码在系统中的存储应采用加密方式，避免被轻易获取。 (5) 应具备密码输入达到一定次数时拒绝登录，由系统管理员重置密码。
5.		访问控制	1. 应建立严格的安全访问控制机制，防止匿名用户未授权访问。严格控制用户权限最小化。 2. 重要操作时，应对用户权限进行校验，防止水平越权操作。重要操作时，对用户权限进行校验，防止垂直越权操作。 3. 软件服务隔离，云平台软件服务在多租户应用模式下，应保障完全隔离。防止出现恶意用户就能直接访问他人的软件服务，改变其软件服务设置，即非授权用户可能突破隔离屏障，访问、窃取、篡改其他用户的数据。
6.		会话安全	平台应确保管理员登录云管平台会话安全，应防止会话固定攻击。应保证客户端 Cookie 信息的安全性。应对会话并发进行限制。应提供会话的安全退出机制。
7.		安全审计	1. 能对云平台的南北流量进行分析防护，能对 VPC 之间的东西向流量进行管控； 2. 具备用户操作日志的记录功能，保障整个云平台审计，以满足运行及行为审计要求，支持对平台的用户侧操作及管理员侧操作能进行审计，做到有据可查、高效分析、完整回溯的目标对操作及安全事件进行追溯和防御，审计功能应贯穿网络层、宿主机层、云主机层、数据层等全方位审计。

8.		流量镜像	支持将云内流量（南北向）镜像至本地数据中心硬件平台（例：网络分路器）
9.		资产统计	能对云内资产进行梳理统计。
10.	IaaS 平台安全	安全组	1. 主机安全组：安全组中支持设置出方向、入方向规则，这些规则会对安全组内部的云主机出入方向网络流量及端口进行访问控制，当云主机加入该安全组后，即受到这些访问规则的保护。 2. 网络安全组：提供管理安全组和安全组规则的功能：创建安全组、删除安全组、添加安全组规则、快速添加多条安全组规则、删除安全组规则、查看弹性云主机的安全组、变更弹性云主机的安全组、云资源加入/移出安全组等，并支持批量导入导出安全组规则。
11.		安全审计	通过平台日志进行审计，审计内容至少包括虚拟机删除、重启、配置安全策略；
12.	PaaS 平台安全	镜像快照保护	支持识别容器镜像中的漏洞及安全风险，并对相关信息进行展示
13.		访问控制	提供严格访问控制功能，控制用户对数据库的访问，支持权限最小化管控。
14.		安全部署	PaaS 应用软件部署前应具备有效的安全测试认证，包含整体安全检测、代码安全检测。

1.4.6.3. 安全设备及服务要求

（1）**服务要求：**包含现场安装，调试，提供培训；含 3 年内维保服务、软件版本升级服务与各类特征库升级服务；包含每季度一次上门巡检服务。

（2）**配置要求：**安全设备或服务的数量和配置需根据厂商整体方案进行适配性调整，厂商需对功能、性能、扩展要求等方面进行说明。

1.4.6.3.1. 网络入侵防护系统

序号	项目	指标项	功能要求
1	网络入侵防护系统	★ 特性要求	1. 若使用硬件产品响应需符合冗余性要求； 2. 若使用软件产品响应需并符合冗余性要求，部署软件产品的设备由投标人提供。
2		流量管控	★具备实时采集流入、流出目标网络的所有流量数据包的能力。
3			具备实时关联和分析 Web 请求与响应数据包的能力。
4			具备关联多个实时和缓存数据包的能力。
5			具备 TCP 流分片实时组包和分析的能力。
6			★具备对采集的数据包进行协议解析能力，能够监视的协议至少包括：以太网帧、IP（v4/v6）、TCP、UDP、HTTP、DNS、ICMP 等。
7			★支持安全违规行为监控，包括平台违规和租户违规等违反国家网络安全相关法律法规的行为持续监控，如挖矿、黄赌毒反动页面、Web 敏感数据明文信息传输、对外漏洞攻击等。
8			系统应提供安全检测告警报表，详细记录检测结果数据，至少包含：发现时间、拦截下发状态、威胁等级、威胁类型、协议类型、攻击源 IP、攻击源端口、HOST、CGI、攻击目标 IP、攻击目标端口、告警详情信息、PAYLOAD 等。
9			针对安全检测告警报表，支持对安全检测告警数据进行精确检索、模糊检索以及多条件组合检索。
10			支持对 VLAN、IPv4、IPv6 报文的入侵防护。
11		安全响应与处置	当发现异常行为、非法连接等情况时，系统支持自动拦截，防止黑客进入目标网络。
12			★能够防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等。
13			★提供自动拦截开关，用户可以自定义自动拦截开启或关闭状态。

14		★1. 支持检测未知 C&C 通道（隐蔽通道）功能，能够提供 C&C 通道的危险级别、建立时间、IP 地址和端口等 C&C 通道信息。 2. 支持弱口令检测功能； 3. 支持病毒库，支持对业界主流协议如 HTTP、FTP、SMTP、POP3、IMAP 等进行病毒检测和查杀，支持对压缩文件进行病毒查杀。
15		针对拦截日志报表，支持对拦截数据进行精确检索、模糊检索以及多条件组合检索。
16	安全管 控	支持对来访的源 IP，或被访问的 URL、域名、目的 IP 添加黑名单规则，执行 TCP 连接会话拦截或仅产生告警观察。
17		支持对来访的可信源 IP，或被访问的可信 URL、可信域名、可信目的 IP 添加白名单规则，加白放行。
18		支持黑白名单规则的有效期限设置，当规则过了有效期之后，规则自动失效。
19		★支持黑白名单单个规则或多个规则的停用、启用、删除。
20		支持黑白名单规则的批量导入、导出。
21		支持对黑白名单规则进行精确检索、模糊检索以及多条件组合检索。
22		支持与其他第三方检测设备联动，通过拦截 API，第三方检测设备可增加 IP 黑名单规则，实现拦截。
23		针对第三方检测设备下发的 IP 黑名单规则，提供查询和停用操作，支持对规则进行精确检索、模糊检索以及多条件组合检索。
24		支持对全部或指定第三方检测设备的拦截 API 的调用权限进行停用和启用操作。
25	日志存 储	告警日志存储时长不小于 1 年。
26	报 告 生 成	系统应能生成详尽的安全检测、安全处置报告，并以图表形式展示，至少应包含：拦截次数、拦截源 IP 数、拦截趋势、安全告警数、威胁等级分布、告警类型分布、攻击源 TOP 排行、产生告警最多域名/IP TOP 排行、告警趋势等。
27		系统应具有浏览安全检测、安全处置报告的功能。

28			安全检测、安全处置报告应可输出成方便管理员阅读的文本格式,包括但不限于 PDF、Word、EXCEL 文件等。
29		系 统 管 理	支持 IP 威胁情报库,包括但不限于 IP 的地理位置、属性等。
30			支持系统异常监控,发生异常后,监控会上报异常生成故障日志报表,至少包含:故障时间、故障 IP、故障类型、故障详细说明等。
31			支持定期升级威胁签名库、病毒库,遇到重大安全事件,支持即时升级。
32		系 统 用 户 鉴 别	系统应在用户登录系统执行任何与安全功能相关的操作之前对用户身份进行鉴别。
33			系统应在用户鉴别尝试失败连续达到指定次数后,阻止用户进一步进行尝试。
34			针对用户的登录、增删改等相关操作,系统应记录系统操作日志,并提供查询和审计。
35		★ 性 能 参 数	支持多节点部署,因系统出现业务延迟或中断需采用集群模式部署; 防护模式下,应用层吞吐量 $\geq 8\text{Gbps}$,网络层吞吐量 $\geq 40\text{Gbps}$,IPS 吞吐量 $\geq 2.3\text{Gbps}$,每秒新建会话 ≥ 15 万,最大并发连接数 ≥ 400 万; 支持在界面上配置 bypass 状态。
36			支持配置的黑名单规则可达 10 万条,白名单规则可达 5000 条。
37			支持通过 API 下发的 IP 黑名单规则可达 10 万条。
38			每秒最大会话数 20 万。
39		统 一 管 控	支持跨 region,跨 AZ 统一管控。 支持透明直路部署模式、旁路部署模式;支持 IDS/IPS 混合部署方式,实现部分接口旁路检测,部分接口对直路防护。

1.4.6.3.2.Web 应用防火墙

序号	项目	指标项	要求/规格名称	指标要求
1	Web 应用	性能要求	★高可用	支持多节点部署,因系统出现业务延迟或中断需采用集群模式部署,支持水平扩展。

2	防 火 墙	★ 特 性 要 求	1. 若使用硬件产品响应需符合冗余性要求; 2. 若使用软件产品响应需符合冗余性要求, 部署软件产品的设备由投标人提供。
3		★ 协 议 要 求	支持 ipv4 和 ipv6
4		★ 性 能 指 标	防护网站对象个数不少于 1000 个 防护模式 (可集群部署) 下每秒新建连接数 ≥ 6 万, 最大并发连接数 (http) ≥ 150 万 最大时间维持数: 可一直持续 日志吞吐量 ≥ 800 条/s 防护模式下网络层吞吐量 $\geq 10\text{Gbps}$, HTTP 吞吐量 $\geq 4\text{Gbps}$ 数据延迟小于 5ms
5		统一管控	1. 支持跨 region, 跨 AZ 统一管控。 2. 可统一进行特征库更新、策略编辑、告警展现、日志集中收集存储、系统监控 (接口流量、CPU、内存利用率) 等; 3. 支持 Syslog、API 与其他设备联动 (例: 网络安全态势感知平台)。
6		★ 云 服 务 支持	同时支持运营侧, 租户侧的全部管理功能界面。 支持在界面上配置 bypass 状态

7	业务特性	★Web 攻击防护	1. 具备 Web 应用攻击检测引擎, 支持文件包含攻击、抵御注入式攻击 (包含 SQL 注入、系统命令注入、Cookie 注入攻击)、信息泄露攻击、跨站脚本(XSS)、网站扫描、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为并阻断。 2. 具备识别与阻断方序列化攻击检测行为并阻断, 包含 PHP、JAVA 等反序列化攻击; 3. 支持识别和防护跨站脚本攻击、防盗链、应用 DOS 攻击的能力; 4. 支持 CC 等应用层 DDoS 防护, 可以阻断 http/https flood 攻击或者将攻击 IP 加入黑名单; 5. 能详细记录攻击事件的 HTTP 请求头信息, 含请求的 URL、User-Agent、POST 内容、cookie 等所有的请求头内容; 能详细记录服务器响应头信息, 服务器响应内容; 6. 能针对 CSRF 和 SSRF 检测, 告警并阻断相关请求;
8		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、斜杠反转义、XML 解析、PHP 反序列化解码等。
9		支持虚拟补丁	针对业界爆发的高危 web 漏洞, 提供快速分析漏洞、向引擎下发漏洞防御规则的支持, 保障 0day 漏洞及时在 waf 打上虚拟补丁;
10		支持多维度 CC 防御	支持多维度 CC 防御, 包括但不限于 IP/Cookie/Referer, 用户可选粒度更细, 更灵活
11		支持数据防爬虫/自定义策略/安全审计	提供恶意爬虫检测能力。
12			支持用户设置 IP 黑白名单, 添加基于正则表达式、关键字以及自定义等规则, 提供用户根据自己的业务特点以及防护日志来灵活设置安全策略。

13				支持应用控制策略日志记录, 包含安全策略的变更时间、变更类型和策略变更用户, 并对变更内容记录日志, 方便策略的管理和运维。
----	--	--	--	--

1.4.6.3.3. 网络未知威胁检测

序号	项目	指标项	要求/规格名称	指标要求
1	网络未知威胁检测	业务特性	★ 基本功能	1. 络威胁检测响应系统支持旁路部署模式。 2. 支持云网络到互联网、云网络到本地数据中心内网流量中的攻击行为。
2			★ 特性要求	1. 若使用硬件产品响应需符合冗余性要求; 2. 若使用软件产品响应需并符合冗余性要求, 部署软件产品的设备由投标人提供。
3			★ 日志检索	1. 支持查看近 1 小时、24 小时、7 天、30 天的流量日志和安全事件日志。 2. 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、防护状态字段等进行日志检索。

4			★网络威胁分析	1. 支持利用威胁情报检测或阻断, 支持与原厂威胁情报中心联动, 可在系统上查看情报基本信息、相关样本、关联 URL、可视化分析等。 2. 支持检测针对 WEB 应用的检测和配置, 包括但不限于 Webshell 上传、SQL 注入、XSS、跨站请求伪造、暴力破解等攻击。 3. 支持其他类型的 WEB 攻击, 如目录遍历、弱口令、权限绕过、信息泄露、文件包含、文件写入攻击等检测。 4. 支持基于程序的攻击检测, 如 TCP 代理程序、HTTP 代理程序、挖矿、勒索病毒等; 支持多种攻击检测, 能更全面的从流量中发现威胁, 包括但不限于 CobaltStrike、Empire 后渗透工具、Metasploit、Invoke-Psexec 命令执行、goproxy 隧道通信、反弹 shell、Nmap(全协议)、冰蝎、哥斯拉、GoBy、SYN 半开链接扫描等。 5. 支持基于工具特征的 Webshell 检测, 能通过系统调用、系统配置的操作来及时发现威胁; 如: 冰蝎、中国菜刀、小马上传工具、小马生成器等。 6. DNS 隧道检测, 检测可疑 DNS 请求并产生告警。登录行为分析检测, 暴力破解、异常登录、特权账号登录、弱口令、明文传输; 数据库异常行为检测。 7. 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。
5			★性能指标	1. 流量吞吐不少于 40Gbps (可多台集群部署); 2. 为进一步溯源取证, 告警日志存储时间不少于 1 年;
6			★网络抓包	支持网络 TCP/UDP/ICMP 抓包, 支持双向抓包, 提供包含攻击来源、攻击时间及试图利用的攻击方式攻击等必要信息。

7			资产管理	1. 支持自动从流量中识别云内资产信息包含：IP、端口等； 2. 支持对资产进行录入（包括：资产 IP、资产名称、分类、责任人等），系统自动根据录入的网段发现资产信息，同时支持根据分组过滤资产列表，支持对资产打标签，支持根据标签过滤资产列表。
8			统一管控	1. 支持跨 region，跨 AZ 统一管控。 2. 提供丰富的 API 接口，支持以 API 或者 syslog 与其他相关系统（例：网络安全态势感知系统）对接。
9			★ 攻击展示	1. 从攻击者的视图对入侵者的基础信息、威胁情报、攻击手法、攻击目标等进行分析展示。 2. 支持查看攻击过程的详情，支包括 payload 和 pcap 包。
10			★ 黑白名单策略	支持黑白名单策略配置，可根据黑白名单进行侦测或排除。支持基于源 IP、目的 IP 及端口设置流量观察与阻断策略； 支持 web 配置相关检测规则； 支持白名单策略，加白后不再产生告警。

1.4.6.3.4.数据加密及密钥管理

序号	项目	指标项	要求/规格名称	指标要求
1	数据加密	业务特性	★ 总体要求	基于虚拟化技术，提供虚拟密码机功能； 支持虚拟金融数据密码机、服务器密码机、签名验签服务器等多种形态的密码设备； 产品具有国密局产品型号证书； 产品支持平台和业务系统通过密评； 支持与主流的平台厂商对接或提供接口，对接案例不少于三家。
2			★ 特性要求	1. 若使用硬件产品响应需符合冗余性要求； 2. 若使用软件产品响应需符合冗余性要求，部署软件产品的设备由投标人提供。
3			统一管控	支持跨 region，跨 AZ 统一管控。
4			基本密钥管理	1、用户可创建、启用、禁用、删除、别名、修改用户主密钥，完成对用户主密钥的生命周期管理； 2、用户可创建、加密、解密数据密钥。

5		一 键 集 成 加 密	提供与其他云服务如对象存储、一键集成加密能力	
6		专 属 加 密 能 力	可提供独享网络、带宽、加密卡资源的专属加密能力	
7		★ 国 密 算 法 支 持	采用国家密码管理局批准的硬件芯片实现各类密码算法，保证算法的高安全性； 对称算法：支持国产 SM1/SM4 算法、以及国际通用算法 DES、3DES、AES； 摘 要 算 法：支持国产 SM3 和通用 SHA1/SHA256/SHA384/SHA512 等算法； 非对称算法：支持国产 SM2、RSA(1024-4096)、ECC(NIST P256、BRAINPOOLP256、FRP256)等算法。	
8		密 钥 使 用 审 计	审计密钥所有的非查询类操作	
9		跨 租 户 密 钥 访 问 授 权	租户可以把自己的密钥授权给其他租户使用，并可以指定其详细的使用权限，还可以随时撤销授权	
10		密 钥 多 Project 管理	支持多 project 特性，用户在不同 project 下的资源是相互隔离的	
11		用 户 导 入 密 钥	租户可以把自己的密钥导入到 KMS 系统，使其和其他用户主密钥一样被 KMS 管理	
12	性 能 要 求	整 机 性 能	★ 国 密 指 标	1、SM2 产生≥80000 次/秒 2、SM2 签名≥80000 次/秒 3、SM2 验签≥60000 次/秒 4、SM3 摘要(tps)≥180000 次/秒 5、SM4 加解密(tps)≥180000 次/秒 实配物理设备至少为 2 台，保证设备冗余性，整体性能要达到如上指标。
			国 际 指 标	1、RSA2048 产生≥80 次/秒 2、RSA2048 签名≥20000 次/秒 3、RSA2048 验签≥60000 次/秒 实配物理设备至少为 2 台，保证设备冗余性，整体性能要达到如上指标。

1.4.6.4. ★云与本地数据中心交互的安全需求

在本期项目建设中，云与本地数据中心交互的安全功能通过云平台安全接入服务实现，主要是与本地数据中心融合，包括云上主机安全、主机资源托管（堡垒机）、漏洞扫描、数据加密（加密机、签名验签服务器）等。投标人应按本功能要求进行相关服务。

1.4.6.4.1. 主机安全

通过在云上服务器侧部署 HIDS 插件（农信银已部署，需配合开通到云下管理节点网络访问关系），对服务近源开展资产（进程级）梳理、账号口令、应用程序信息、漏洞信息、Webshell 等安全监测，深化资产梳理。将云上主机纳入本地数据中心立体安全监测框架，应对 APT 等不断进化的网络安全攻击。

1.4.6.4.2. 堡垒机系统

本地运维时，应对运维人员进行身份认证，并对运维过程进行安全审计，主要通过云平台接入本地数据中心堡垒机系统（农信银已部署堡垒机，需配合开通到云下管理节点网络收敛访问关系）进行实现，该系统针对运维人员进行统一认证，对运维人员操作虚拟机进行全程监控与审计。

1.4.6.4.3. 漏洞扫描

云平台支持云主机漏洞扫描（农信银已部署漏扫平台，需配合开通到云下管理节点网络访问关系），利用本地数据

中心分布式扫描器对云内不同网络区域及业务进行资产和应用漏洞发现

1.4.6.4.4. 数据安全

保障云上业务数据安全，安全接入服务应支持云平台与本地数据中心业务数据之间交互数据进行加解密、数字签名及验证等操作以及基于数字证书的身份认证功能。

(1) 可提供完善的密码产品解决方案，包括加解密、数字签名验签等，能够配套管理具备国密局认证的相关安全设备，提供对接平台外设备的 API 接口。

(2) 能够提供云外密码安全产品的联通，安全接入服务应支持云平台与本地数据中心业务数据之间交互数据进行加解密、数字签名验签以及编押核押等操作，同时保证网络联通的时效性（同一数据中心稳定状态下，平台内调用平台外密码设备的延时为毫秒级别及以内）。

1.4.6.4.5. 身份安全

云平台身份安全接入服务，通过对接本地数据中心多因素认证系统实现用户名的动态口令认证，认证方式包括软硬令牌，支持标准的认证协议，包含但不限于 Radius、Oauth、Ldap 等。

1.5. ★农信云项目实施服务要求

1.5.1. 项目各阶段工作要求

1.5.1.1. 实施准备要求

(1) 合同签订后, 中标人安排至少 10 名中标人技术人员或制造商原厂技术人员在招标人指定地点(北京或长沙市内), 在 45 天内完成设计、规划、测试等文档编写、配置验证等各项准备工作。

(2) 需要对数据中心进行现场场地踏勘时, 中标人应安排相应技术人员进行现场踏勘工作。

(3) 中标人须编写项目实施的各类文档, 并生成设备配置, 项目实施时中标人需至少提交下列文档并经过招标人评审, 内容必须与所提供的产品相一致, 并应尽可能详细。编写的技术文档类别应包括规划设计类、方案测试类、实施类、现场测试类、上线类及运维类。规划设计类文档应完整合理, 涉及机房、布线等规划的协助招标人完成, 涉及系统配置的根据招标人要求完成; 实施类文档能够清晰准确指导实施, 实现系统集成的标准化、规范化和一致性; 测试类文档覆盖全面; 上线及运维类文档步骤明确、有效、可操作。

(4) 文档编写人员按需参与现场实施工作。

(5) 在投标的工程实施方案中应说明可提供的技术文档清单。

(6) 中标人应在每批次实施前向招标人交付当批所需的完整的技术文档。

(7) 提交的技术文档是按需出版或装订的, 其费用应

包括在该品目的基本报价中。为了培训的目的, 招标人有权复制这些资料而不受限制和另付费用。

(8) 中标人须按照总体技术方案编写整个项目的各类技术文档。编写的技术文档类别应包括规划类、设计类、实施类、测试类、上线类及运维类。规划和设计类文档应完整合理; 实施类文档能够清晰准确指导实施, 实现系统集成的标准化、规范化和一致性; 测试类文档覆盖全面; 上线及运维类文档步骤明确、有效、可操作。编写的技术文档不得少于下表, 但不限于下表内容:

类别	文档名称
规划设计类	《总体设计方案》
	《设备部署图》
	《详细设计》
系统测试类	《测试方案》
	《测试报告》
实施类	《硬件安装手册》
	《配置手册》
上线类	《上线操作手册》
	《上线应急预案》
运维类	《运行维护手册》
	《备件管理方案》
	《上下电手册》
	《日常值守检查表》
运营类	《运营手册》
	《用户操作指南》

(9) 本项目线缆需符合下列要求:

序号	类型	要求
1	双绞线:	★类型: Cat6A 类 S/FTP 屏蔽电缆, 可以抗各种电磁干扰。 ★芯线规格: 26 AWG, 4 线对。 ★采用十字骨架支撑结构。 ★标准: TIA/EIA-568-D 和 ISO/IEC 11801 (2002)

		和 EN 50173-1(2003)。 ★工作频率: $\geq 500\text{MHz}$ 要求。
2	LC 接口 光纤	★双纤芯跳线, 方便安装, 易于维护; ★规格: 1.8mm 的缆径; ★光纤类型: 万兆多模, OM4, LC-LC; ★标准: ANSI/TIA-568.C; ★阻燃等级: 光纤跳线须采用 OFNP 外皮; ★综合布线产品必须为优质品牌的标准化产品, 不接受采用 OEM 方式的厂家产品; ★认证: 多模光纤跳线须提供国际权威机构 UL 出具的认证文件。
3	MPO 接口 光纤	★光缆标准: TIA-492AAAD。 ★光缆规格: 50/125 μm 室内多模光纤。 ★性能等级: OM4。 ★宏弯损耗: 最大宏弯 (100 圈, 75 mm 圆轴): 850 nm 和 1300 nm 下, 最大 0.50 dB。 ★100Gbps 传输距离: 不少于 150 米; ★光缆损耗: 850 nm (3.0 dB/km) \ 1300 nm (3.0 dB/km)。 ★回波损耗: -82.1 dB (1550 nm) \ -79.6 dB (1310 nm)。 ★插入损耗: 不大于 0.35dB。 ★插头标准: ANSI/TIA-568-C.3。 ★阻燃等级: 光纤跳线须采用 OFNP 外皮。

1.5.1.2. 设备到货要求

(1) 在合同签订后 40 个工作日内设备到达招标人指定地点。

(2) 中标人按照采购配置清单, 提供完好、全新、未使用过的硬件产品; 提供完整、正版的软件介质、软件文档及软件许可。

(3) 收到招标人发出的中标通知书后, 需及时联系招标人相关人员安排到货事宜, 按照招标人的时间要求完成到

货。

(4) 供货前, 应按照招标人要求, 提前准备好相关供货材料和信息(包括设备型号、规格、数量、序列号、包装、运输人员和车辆等), 配合招标人完成到货清点、入库、拆箱检查、到货验收, 以及资产扫描和入账等工作。

(5) 中标人负责开箱验货, 检查产品到货情况。

(6) 如果中标人履行合同时不能按承诺的时间地点到货, 将以合同违约处理, 并追究中标人的有关责任。

1.5.1.3. 集成部署要求

(1) 在设备到货 2 个月内完成设备的安装和平台系统调试。

(2) 系统集成的主要目标是按照详细设计要求完成云系统环境搭建并能够正常运行, 确保与之相联的全部设备正常联通、设备上安装的软件正常运行并满足招标人业务运行的要求, 完成运维、运营等各类系统的集成, 按照规划完成虚拟计算池、物理计算池、存储系统及网络的纳管和对接, 完成云平台的搭建工作。

(3) 中标人在安装设备之前, 应先对招标人的相关人员进行现场培训, 并在招标人相关技术人员的监督下进行安装、检测和排除故障。中标人不得在现场安装未经招标人批准的任何设备。

(4) 按照招标人要求的时间, 中标人安排工程师到现场实施本项目所有软硬件的安装调试, 包括但不限于场地勘测及确认、设备到位连线、加电自检、微码升级、存储初始化、主机连接、软件安装及客户化等工作。在安装调试过程中中标人的技术人员应说明设备的安装步骤和应该注意的事项并做详细记录。

(5) 根据采购配置清单及安装调试实施方案, 配合招标人对设备部件种类及数量、硬件配置、软件配置、软件介质和许可进行验收; 按照招标人的要求, 对所购设备进行高可用和功能验收; 按照招标人的要求, 对所购软件进行功能验收; 根据验收结果提供验收报告。

(6) 在安装、调试过程中造成的设备损坏, 一切责任由中标人承担。

(7) 在项目实施全过程中, 中标人对安装、调试及验收期间的工作进度、每天的主要工作、发现的问题及解决方法均须记录在工作日志上, 工作日志每天的记录双方签字确认, 双方各保留一份。

(8) 中标人必须响应下列安装、调试要求, 包括但不限于以下几点:

①按标书要求对其产品的性能和配置进行安装、调测检查, 并做出安装、调测报告。所供设备应在合同中所规定的地点和环境下, 实现正常运行并达到合同要求的性能和产品

技术规格中的性能。

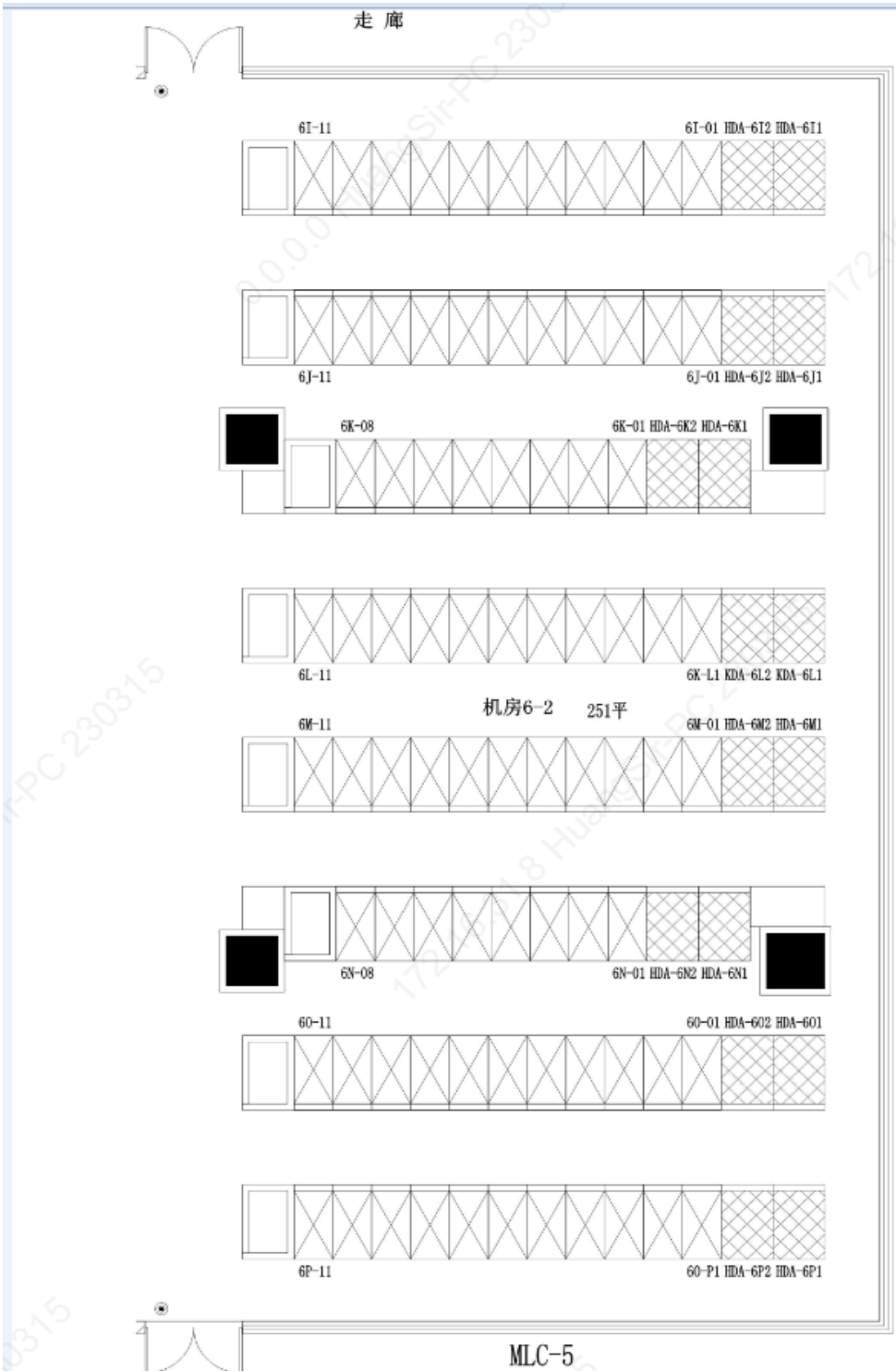
②完成与配套设备（包括本项目采购的其它设备、其它项目近期采购的设备和原有设备）的联合调试，构成整体的系统平台，进行相关的配置和系统优化调试，配合应用开发商或其他系统集成商进行应用系统安装、配置和系统优化调试等。

③当所供设备在安装、调测中出现性能指标或功能上不符合技术要求时，由中标人无附加条件解决。因缺少某些部件而导致达不到项目的设计指标，中标人须无偿提供这些部件，使项目满足设计要求。

④如安装、调测中出现不符合合同要求的质量问题时，用户保留索赔和退货的权利。

⑤完成与招标人已有服务器的适配及集成，各类服务器的规格详见1.8章节。

（9）为实现农信云平台整体的高可行性和稳定性，保障网络的冗余性和健壮性，现结合农信银机房实际情况（如下图），投标人并根据自身的最佳设计实践，完成机房部署设计实施，包括但不限于以下几点：



①云平台云底座的部署遵照高可用原则，云底座和各功能组件在单列机柜电力或网络接入等故障仍保持业务可用。

每组云底座服务器接入交换机不允许分拆跨机柜列部署。

②云平台网络核心交换机、互联网区域、广域网区域设备部署在6L01-04和6M01-04机柜，核心交换机分别部署6L01-02和6M01-02机柜，互联网模块网络设备部署在6L03、6M03，局域网模块网络设备部署在6L04、6M04，防止单列电力出现故障时整体云平台不可用。

③服务器网络接入Leaf交换机采用TOR或EOR部署模式（现机房机柜已具备EDA-HDA综合布线）。Leaf交换机需分布在同列不同机柜，要求具备高可用原则，服务器接入采用端口聚合，物理线缆需接入不同物理交换机。服务器不允许跨列接入Leaf交换机。

④HDA（网络列头柜）可用空间20U，配备AB双路电源，单路额定功率3.5KW，其中单路配备国标16A*6个，国标10A*8个，C13/14*6个。

⑤服务器机柜可用空间46U，配备AB双路电源，单路额定功率3.5KW，其中单路配备C19/20*6个，C13/14*14个。

⑥计算节点、存储集群等需在满足单列机柜电源故障不影响整体云平台业务连续性要求下，自行设计物理部署。

（10）中标人保证其提供的设备中所有预装和为本项目安装的软件为具有合法版权或使用权的正版软件且无质量瑕疵，且为该产品的当前最新版本或最适合用户的版本，软件授权应无时间限制。

(11) 设备安装和系统调试工作因招标人因素超出工作时间, 不另行收费。

(12) 项目实施过程中, 如出现技术障碍、运行故障等问题, 中标人有义务和责任组织、协调相关各方对问题进行快速解决。

1.5.1.4. 验证测试要求

(1) 中标人安排技术人员和具备高级技术认证的原厂技术人员在完成系统集成一周后启动测试验证工作, 并在 2 个月内完成云系统的验证测试工作。

(2) 由中标人、原厂商和招标人(必要时由第四方参加)共同组成验证测试小组, 由原厂商(必要时由第三方)提供测试方案和测试数据, 经招标人确认后进行测试, 测试内容包括但不限于软件平台功能测试、软硬件平台兼容性测试、性能测试、高可用测试、管理性测试等。

(3) 中标人应按照验证测试方案进行测试工作, 提交测试报告, 并经招标人审核。

(4) 对于需要进行完善、整改的问题, 应评估问题影响, 制定整改计划, 并经招标人审核。

(5) 对于影响不大, 不能及时完成整改的问题, 经招标人同意后, 可以作为遗留问题在系统后按计划进行整改。

(6) 测试结果如与验证测试小组确定的性能不符或测

试结果不能确认，中标人及原厂商应在 5 个工作日内调整配置直至重新测试合格，如果测试不通过，招标方有权停止验证测试和拒验收该系统，且由乙方承担相应责任。

1.5.1.5. 试点应用部署要求

（1）中标人安排不少于 5 名技术人员和具备高级技术认证的原厂技术人员在完成系统集成后 2 个月内协助招标人完成试点应用的部署工作。

（2）中标人应提供应用迁移上云的标准解决方案及操作手册，并协助招标人制定试点应用上云部署方案及测试方案，并经招标人审核。

（3）初步计划试点上云应用数量不大于 3 个。

（4）中标人应协助招标人按照应用上云测试方案进行测试工作，提交测试报告，并经招标人审核。

1.5.1.6. 系统上线要求

（1）完成试点应用部署后 4 个月内，开展系统上线运行工作。招标人有权结合自身情况调整系统上线时间，但应提前书面通知中标人。

（2）云上线时中标人应提供技术人员及相关产品的原厂技术人员共同在上线地点进行现场技术保障，现场技术保障人员总人数不少于 10 人。中标人技术人员应具备三年以

上工作经验并为本项目主要成员，可熟练配置投标系统及设备，参与至少一个以上和本项目同等规模的实施工作。原厂技术人员需具备 5 年以上工作经验，有较强的排除错误的能力，参与至少 3 个以上和本项目同等规模的实施工作。

(3) 上线期间，若发生由于中标人派遣的技术人员的技术能力或集成的系统导致的应用系统业务中断，中标人负责承担一切相关责任。

(4) 中标人须提供切实可行、操作高效、验证充分的系统上线方案，要求如下：

① 上线方案应包含上线思路、上线步骤、验证方案、流程控制以及应急回退等内容。

② 上线工作应尽可能减小对现有业务系统影响。

③ 如规定时间内遇到问题无法解决，应制定相应的应急预案和应急回退方案等。如是硬件问题，上线阶段中标人应确保备件可在 4 小时内到达用户现场。

1.5.2. 技术转移要求

1.5.2.1. 现场技术培训

(1) 中标人在设备上线之前，应对招标人的相关人员进行现场培训。

(2) 中标人应准备相关培训资料，并交付招标人。

(3) 培训内容包括但不限于设备的功能原理、配置方

法和运行运维、技术支持服务，以及软件架构、标准接口及基本开发方法等内容，通过培训运维人员应基本掌握设备的功能原理和配置方法，系统运维管理方式等内容，并提供相应的工具，使招标人相应的技术人员达到了如下的技术水平：

- a. 能够熟练使用和维护农信云平台：
- b. 能够独立进行接入交换机、计算节点、裸金属节点、容器 Node 节点、存储节点的扩容、缩容、更换等操作；
- c. 具有熟练查阅各种相关技术文件及维护手册的能力
- d. 掌握农信云平台的工作原理以及基于标准接口的开发方法

1.5.2.2. 技术资料移交

所有系统上线完成后，中标人按招标人要求完成项目移交。项目移交工作要求如下，包括但不限于以下内容：

（1）中标人负责安排至少 3 名工程师参与文档交付任务。包括修订项目实施文档，在招标人已有移交文档的模板上进行格式校对。

（2）提交电子版（U 盘）文档，移交 U 盘必须为高质量 U 盘。

1.5.2.3. 技术认证考试

投标人提供不少于 10 个云平台原厂最高等级的云计算培训、认证考试名额。

1.6. ★农信云技术支持与服务需求

1.6.1. 服务总体要求

序号	指标内容	要求	备注
10.	服务方要求	①在签署项目最终验收报告之日起, 由中标人及相关软硬件原厂商共同提供技术支持与服务, 其中云平台等主要软硬件必须由原厂商提供技术支持与服务。	
11.		②由中标人及相关原厂商组成技术支持服务团队, 说明服务方式及服务内容。	
12.	服务人员要求	①服务方成立由项目经理、服务工程师等组成的专职服务项目组。	
13.		②指派有 3 年以上类似项目管理经验的人员担任项目经理, 要求具有较强的组织协调能力、专业技术能力、项目管理能力、口头及文字表达清晰, 负责本项目全程管理。	
14.		③质保期内, 一线工程师需有 3 年以上相关技术经验, 二线工程师需有 5 年以上相关技术经验, 要求对工作应认真负责, 具有良好的合作精神。	
15.		④服务人员需经招标人认可, 未经招标人同意不能更换。如果招标人认为服务方指派的人员达不到招标人所要求, 服务方应立即满足招标人提出的替换要求。	

16.		⑤服务方服务人员需身体健康，品行端正，无犯罪不良记录，无扰乱社会治安倾向。服务方对所派服务人员的各项要求负有审核管理义务。	
17.	服务期限要求	质量保证期为自经过招标人终验合格后次日起 36 个月。针对服务器、备份一体机，质量保证期为自经过招标人终验合格后次日起 60 个月。	

1.6.2. 服务内容要求

1.6.2.1. 远程技术支持

服务方通过热线电话、电子邮件、传真等方式向招标人提供 7*24 小时远程技术支持，支持范围包括故障报修、问题提交、问题远程指导、分析和排除、产品功能介绍、配置、安装、调试、客户化以及使用中遇到的技术问题的咨询等，服务方需在规定时间内响应。

1.6.2.2. 现场运维技术支持

1.6.2.2.1. 驻场支持服务

驻场支持服务指中标人按要求安排云平台原厂商的技术人员，在招标人提供的办公区现场办公，提供运维支持服务。

序号	指标内容	要求	备注
16.	基本要求	提供 5×8 驻场支持服务，人员不少于 2 人，必须为资深技术人员（通过本项目云平台原厂云计算	

		相关高级认证），工作年限不少于 3 年，服务期与质量保证期相同。	
17.	工作内容	为招标人的技术人员提供平台使用咨询服务	
18.		按招标人的流程，进行云平台的资源创建、交付	
19.		云平台的日常监控、预警、优化、故障处置服务	
20.		协助招标人进行云平台的升级、扩容等变更操作	
21.		招标人安排的其他技术工作	
22.	考核要求	1. 遵守招标人的办公管理、运维管理等制度； 2. 如提供的驻场服务人员的表现不符合项目要求，投标人项目经理需无条件在招标人提出换人要求之日起，5 个工作日内完成更换。若更换后仍不满足要求，投标人项目经理 5×8 在现场跟进，3 个工作日仍然没有明显改进，投标人项目经理的上级领导 5×8 在现场监督改进，依次类推，直到大中华服务总经理（或同级别经理）5×8 在现场监督，直到完全改进。	

1.6.2.2.2.现场支持服务

现场支持服务指中标人提供的驻场服务以外，云平台原厂提供的各类需在招标人现场进行的支持服务。

序号	指标内容	要求	备注
1	现场支持服务	提供 7×24×4（每周 7 天，每天 24 小时，4 小时到现场）现场服务，接到支持需求必须在 30 分钟内做出回应；由于投标人或原厂商原因造成的各种软件（含集成）故障（不论涉及硬件或软件是招标人通过本	

	次直接购置、赠送还是随机附带方式获得），均应在 4 小时内修复，如确实出现异常情况，在上述 4 小时内必须完成为业务系统的恢复，提供硬件和软件环境准备，恢复生产；应提供紧急事件的快速处理服务系统，对于影响生产的紧急事件，必须在 2 小时内恢复系统。	
23.	如提供的项目服务人员态度与能力不符合项目要求，招标人提出改进要求，3 个工作日内没有明显改进，投标人项目经理 5×8 在现场监督改进，3 个工作日仍然没有明显改进，投标人项目经理的上级领导 5×8 在现场监督改进，依次类推，直到大中华服务总经理（或同级别经理）5×8 在现场监督，直到完全改进。	
24.	无附加条件提供本次采购软件产品、文档更新服务，包括：磁带、磁盘、电子邮件、U 盘等，安装或运行最新软件修订版时，提供相应的技术支持和说明。如对软件有新的改进、增加新的功能或者为适应最新标准所形成的最新版本，均应及时通知并无附加条件提供介质。	
25.	提供特殊时段（国庆节、年终、重大活动、重要应用测试、投产、切换演练），以及产品安装、系统变更和迁移、系统升级等的现场支持服务。	
26.	每次现场服务后均须向招标人提交《技术	

	服务工作报告》，对未完全解决的问题，服务工程师须至少每周与招标人工程师联系，跟踪问题，分析协商处理方案，直至问题解决。	
27.	每季度进行设备定期现场巡检，检查产品运行状况，解决运行过程中遇到的问题，分析运行记录和系统日志，提出系统管理改进建议。在每次服务完毕后 5 个工作日内提交服务报告，并且每年提交一次年度服务总结报告。	
28.	在招标人使用主流品牌的硬件、软件产品出现兼容性问题时，需积极配合，与有关硬件、软件厂商和招标人接洽，及时定位问题原因、寻求解决方案。若为本次采购软件原因，应及时解决。	
29.	提供各种突发事件的应急策略。	
30.	提供其他与产品相关联的服务，如产品过期 EOL (End of life)，需至少提前两年通知客户。	

1.6.2.3. 疑难复杂问题解决

服务方需保持 7*24 联系畅通，及时响应解决突发紧急问题；根据需要，及时到达现场进行故障恢复、问题诊断或维修，以尽快恢复设备系统可用状态。对未明确原因的故障问题和关联产品问题协助进行排查，并给出合理意见和建议。

议。

1.6.2.4. 备件保障服务（仅适用于硬件产品）

服务方备件库应满足本项目 100%的备件覆盖率（即备件库中备有维护清单中所有设备的所有备件），保证备件的品质和可用性，按服务级别提供备件保障服务，每季度主动通报一次备件情况。

针对服务器，维保覆盖整机配件。项目设备中所有故障硬盘不返厂。

1.6.2.5. 应急保障服务

针对维保产品提供应急保障方案，结合应用系统需要，提供配套应急保障方案（包括应急措施和切换流程等），根据需要进行实际演练，相关应急方案需满足招标人管理流程和相关规范要求。根据需要，提供应急演练支持（包括必要的现场支持），根据招标人各环境实际运行地点，提供对应级别支持，支持地点包括长沙、北京两地三中心所在地。

1.6.2.6. 预防性维护

服务方根据招标人要求，定期对设备、软件进行巡检和预防性维护，提交巡检记录，并对巡检中发现的问题给予及时修复。

1.6.2.7. 产品版本信息发布和升级支持

产品版本信息包括硬件微码、软件 PTF 和新版本，以及 EOS 等所有涉及版本变化的信息。服务方需于版本信息发布后 90 天内正式通知招标人，且产品 EOS 信息发布时间不得晚于 EOS 日期前一年。对于新发布的版本信息，服务商需提供相关介质和安装使用说明，包括但不限于新功能、所解决的问题、相关环境要求、安装方法等。服务期内招标人享有对所购买产品合法升级的权力，服务方需根据招标人需要，对升级工作提供技术支持，包括结合招标人实际使用对新版本进行评估并给出建议，配合升级和回退方案拟定、测试演练和投产支持等。同时招标人有需求对已上线系统进行配置变更时，需提供技术支持和保障服务。

1.6.2.8. 移机、扩容技术支持服务

根据招标人需要，服务方为招标人提供设备系统移机技术支持服务。

如对设备进行扩容，服务方应根据招标人需要，提供技术支持，包括调试、参数定义、逻辑卷划分、数据迁移、相关功能软件工具安装、远程备灾方案的实施和调试等。

1.6.2.9. 重要时段保障服务

根据招标人需要，在特殊时段（如重要会议、黄金周长

假、年终决算、重大投产变更等招标人认定的特殊时段) 提供 7*24 小时现场值守支持服务, 以及二线 7*24 小时响应服务。并根据招标人需求, 提供现场备件。

1.6.2.10. 开源软件版本维护服务

在服务期内, 若该服务所涉及的开源软件发生升级情况, 应提供配套的版本升级维护服务, 包括开源软件升级版本的安装服务, 新版本的培训, 协助完成软件配置、升级测试工作等。升级的版本包括但不限于软件的小版本、大版本、跨代版本以及基本功能不变但已更换名称的软件, 并按招标人要求的方式提供相应介质。升级的版本相对于已使用的版本, 要能提供平滑升级包。

1.6.2.11. 性能调优

在服务期内, 对基础设施云涉及的云平台整体或组件发生性能下降时, 需提供性能分析报告、性能调优方案, 并协助招标人完成性能调优操作, 出具性能调优报告。

1.6.2.12. 系统迁移

在服务期内, 对应用系统由外部迁移至云内时, 提供系统迁移改造技术支持、迁移方案和迁移计划, 并协助招标人完成数据迁移及相关验证工作。

1.6.2.13.容灾演练支持

在服务期内，对招标人统一容灾演练或单独针对云平台的容灾演练，提供云平台侧技术支持工作，并在演练结束后提供云容灾演练结果报告。

1.6.2.14.巡检和健康检查

在服务期内根据招标人需要，提供巡检和健康检查服务，提供季度生产现场巡检制度并预先提供巡检计划，提供季度系统健康检查服务并在维护和服务之后提供相关书面报告。

1.6.2.15.文档维护

在服务期内，根据运行维护和运营需要，对各种工程实施相关技术文档、运维运行规范指南、基础设施云运营规范、常见问题处理指南、厂商支持体系和流程指南等提供持续文档完善工作，并及时交付给招标人相关部门。

1.6.3.服务标准与质量要求

1.6.3.1. 故障恢复要求

事件级别定义如下：

一级：属于普通问题；其具体现象为：设备系统技术功能、安装或配置等事前测试和准备，或其他显然不影响业务的预约服务。

二级：属于较严重问题；其具体现象为：设备系统能继续运行且性能不受影响，但出现报错，存在较大安全隐患。

三级：属于严重问题；其具体现象为：设备系统部分部件或功能失效、性能下降但不影响正常业务运作。

四级：属于紧急问题；其具体现象为：设备系统故障导致系统停止运行、数据丢失等。

服务质量基本要求如下：

故障级别	响应时限	人员到场时限	备件到场时限（仅限有备件服务的项目）	故障恢复时限
4 级	立即	1 小时	重要备件：4 小时 一般备件：24 小时	联机故障平均恢复时间不超过 20 分钟 批量中断平均恢复时间不超过 40 分钟 所有故障最长恢复时间不超过 2 小时
3 级		1 小时		
2 级		2 小时		
1 级		约定时间		4 小时之内

说明 1：重要备件指某类备件的硬件故障导致相关设备宕机（影响生产）的备件；一般备件指某类备件的硬件故障不影响生产。

说明 2：故障恢复时间以服务方工程师被允许进行维护开始计时，到设备系统恢复服务为止。

1.6.3.2. 可用性指标

完成两地三中心建设后，整个云平台系统年可用性 $\geq$

99.99%，即系统故障或问题影响生产的时间，年度内不超过52.6分钟。其计算公式为：

$$\text{年可用性} = \left(1 - \frac{T_{\text{down}}}{60 \times 24 \times \text{Year}}\right) \times 100\%$$

T_{down} ：影响生产的时间，单位为分钟。

注：年可用时间按60分钟*24小时*365天计算，取值为万分位。

1.6.3.3. 问题解决率

故障发生后24小时内，服务方应提交初步问题分析报告，问题分析定位后提交最终分析报告，报告需包括问题描述、分析情况、原因定位、可行的解决方案等内容，提出的解决建议应具有合理性和可实施性。分析报告以招标人认可视为提交。

问题解决率：2日内不低于60%，5日内100%（故障发生后每24小时为1日），双方另有约定的除外。

1.7. ★农信云扩容建设要求

1.7.1. 扩容建设方案

投标人应编写扩容建设方案，包括以下内容：

（1）对本次采购的各类软硬件设备在数量、授权、性能、应用场景等方面的限制情况进行说明，如某项功能的授权限制，如当前配置下云平台性能瓶颈预计等。

（2）在本次建设基础上可采取的扩容方案及采购配置，包括以下扩容建设场景：

序号	指标内容	要求	备注
1.	计算资源扩容	单站点计算资源扩容需求时, 扩容设计及采购配置;	
2.	存储资源扩容	单站点存储资源扩容需求时, 扩容设计及采购配置;	
3.	网络资源扩容	单站点网络资源扩容需求时, 扩容设计及采购配置;	
4.	新建数据中心	新建站点需求时, 建设设计及采购配置(与本次数据中心建设同等规模, 需考虑数据中心同步、切换等需求, 同步列明所需的相关组件名称及价格, 满足本项目扩展性相关要求。);	
5.	PaaS 扩容	各 PaaS 功能扩容需求时, 扩容设计及采购配置;	
6.	云底座扩容	当前配置下云底座支持能力及扩容建设要求。	
7.	定制开发服务	按招标人需求的云功能优化、系统对接等开发服务。 每 8 小时计为 1 人天, 节假日与工作日计量标准相同。 对于云系统日常资源调整、系统升级、bug 修复等工作应由投标人无附加条件提供, 不计入定制开发服务。	

1.7.2. 扩容建设报价要求

序号	指标内容	要求	备注
----	------	----	----

1.	报价要求	投标人应在扩容建设方案中提供扩容建设报价，相关产品的单价价格不得高于本次采购的实际价格。	
2.		招标人有权在本次采购成交后 3 年内以不高于投标人扩容建设报价的价格采购报价产品，采购数量不受限制。	
3.		对于招标人在本次采购中提出了技术要求但不进行实际配置的产品，投标人报价应与本期配置的各产品的价格相同。	
4.		投标人进行报价时应说明报价计算方式及计量单位，如果有达到一定采购量、采购金额可以享受更高优惠或者可以买断的，应予以说明。	
5.		对于需要配置软、硬件等多种产品才能实现的功能，投标人应以该功能为整体单位进行整体报价，并对其中所需的软、硬件等细项分别报价。	
6.		定制开发服务按人天报价	

1.8. 其他信息

1.8.1. 招标人已有服务器

序号	制造商	型号	基本配置	备注
1.	浪潮	NF5280M6	2*英特尔金牌可扩展三代处理器、 256GB+ DDR4 内存、 2*2.5 寸 SATA SSD 固态硬盘、 3*10Gb 英特尔 X710 双口网卡、 不少于 2 个千兆网卡、 2*16Gb 双口 HBA 卡、	支持作为裸金属服务器、容器 Node 节点。

			1* LSI 12Gb/s 超级电容 RAID 卡、	
2.	浪潮	CS5280H	2*海光 7285 处理器、 256GB+ DDR4 内存、 2*2.5 寸 10Krpm 1.2TB SAS 硬盘 2*千兆网口、 2*10Gb 英特尔 X710 双口网卡 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡	支持作为裸金属服务器、容器 Node 节点。
3.	浪潮	CS5260F	2*飞腾 S2500 处理器 256GB DDR4 内存、 2*2.5 寸 10Krpm 1.2TB SAS 硬盘 2*千兆网口、 3*10Gb 英特尔 82599 ES 双口网卡 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡	支持作为裸金属服务器。
4.	联想	ThinkServer SR658H V2	2*海光 7285 处理器、 256GB+ DDR4 内存、 2*2.5 寸 SATA SSD 硬盘、 1*2.5 寸 3.2TB NVME 固态硬盘 4*千兆网口、 2*25Gb Mellanox CX-5 双口网卡、 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡	须作为计算节点，支持作为裸金属服务器、容器 Node 节点。
5.	联想	ThinkServer SR658H V2	2*海光 7285 处理器、 256GB+ DDR4 内存、 2*2.5 寸 960GB SATA SSD 硬盘、 4*千兆网口、 2*10Gb 英特尔 X710 双口网卡、 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡	支持作为裸金属服务器、容器 Node 节点。
6.	新华三	UniServer R4900 G3	2*英特尔金牌可扩展二代处理器、 256GB+ DDR4 内存、 2*2.5 寸 10Krpm 1.2TB SAS 硬盘、 3*10Gb 英特尔 X710 双口网卡、 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡、	支持作为裸金属服务器、容器 Node 节点。
7.	新华三	UniServer R4900 G3	2*海光 7285 处理器、 256GB+ DDR4 内存、 2*2.5 寸 10Krpm 1.2TB SAS 硬盘、 4*千兆网口、	支持作为裸金属服务器

			2*10Gb 英特尔 X710 双口网卡、 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡	
8.	类型 1	N/A	2*海光 7380 处理器、 512GB DDR4 内存、 2 块 480GB SSD、 2*3.2TB NVME 固态硬盘、 4*千兆网口、 2*10Gb 英特尔 X710 双口网卡、 2*25Gb Mellanox CX-5 双口网卡、 2*16Gb 双口 HBA 卡、 1* LSI 或 PMC 超级电容 RAID 卡	支持作为计算节点、裸金属服务器、容器 node 节点。
9.	类型 2	N/A	2*英特尔金牌可扩展三代处理器、 256GB+ DDR4 内存、 2*2.5 寸 SATA SSD 固态硬盘、 2*10Gb 英特尔 X710 或 Mellanox 双口网卡、 2*16Gb 双口 HBA 卡、 1* LSI 超级电容 RAID 卡	支持作为裸金属节点
10.	类型 3	N/A	2*海光三号处理器 256GB+ DDR4 内存、 2 块 2.5 寸 SATA SSD、 2*10Gb 英特尔 X710 或 Mellanox 双口网卡、 1* LSI 或 PMC 超级电容 RAID 卡	支持作为裸金属节点

1.8.2. 招标人已有磁带库

品牌	型号	配置
昆腾	scalar i6000	scalar i6000 Quantum Scalar i6000 LTO Control Module (CM3), no tape drives, no expansion modules 昆腾磁带库 scalar i6000 控制主柜*1 Quantum Scalar i6000 and AEL6000 IBM LTO-8 Tape Drive Module, 8Gb Native Fibre Channel, Dual Port 昆腾磁带库 scalar i6000 LTO8 驱动器*12 Quantum Scalar i6000 and AEL6000 Active Vault 许可 for extension module Enables Active Vault functionality in the system. Provides the

		ability to create Active Vault system-managed partitions. This feature can use un许可 d slots, but Expansion Modules must be ordered to provide the necessary physical slot capacity. Support will be provided by the existing system warranty/service contract. Active Vault does not require Partitioning and a Partitioning 许可 is not included. This is a library-based 许可, not a drive 许可 and cannot be transferred to another library. 昆腾磁带库 scalar i6000 Vault 非主控柜槽位控制许可*1 Quantum Scalar i6000 and AEL6000 Control Module (CM3) and Drive Ready Expansion Module (DREM3) Redundant Power (2N) 昆腾磁带库 scalar i6000 冗余电源 *1 Quantum Scalar i6000 and AEL6000 Storage Expansion Module (SEM3), no tape drive support 昆腾磁带库 scalar i6000 扩展柜库体*1 Quantum Scalar i6000 Partitioning Option 许可 Key 昆腾磁带库分区许可*1
--	--	---

1.8.3. 招标人已有的数据库

序号	数据库	版本
1	DB2	9.7 及以上
2	MySQL	5.6 及以上
3	OceanBase	2.2 及以上
4	TD-SQL	10.3.17 及以上
5	MongoDB	3.2 及以上

2. 具体采购需求明细

表 1：采购货物清单

序号	是否核	货物名称	单位	数量	到货地点	维保期要求
----	-----	------	----	----	------	-------

	心产品					
1.	否	核心交换机	台	不少于 2	长沙	3 年
2.	否	100G 交换机	台	不少于 0	长沙	3 年
3.	否	25G 交换机	台	不少于 12	长沙	3 年
4.	否	10G 交换机	台	不少于 6	长沙	3 年
5.	否	1G 交换机	台	不少于 6	长沙	3 年
6.	否	边界路由器	台	不少于 0	长沙	3 年
7.	否	硬件防火墙	台	不少于 4	长沙	3 年
8.	否	云内防火墙	套	不少于 1	长沙	3 年
9.	否	硬件负载均衡	台	不少于 8	长沙	3 年
10.	否	云内负载均衡	套	不少于 1	长沙	3 年
11.	否	入侵检测	套	1	长沙	3 年
12.	否	Web 应用防火墙	套	1	长沙	3 年
13.	否	网络未知威胁检测	套	1	长沙	3 年
14.	否	物理服务器	台	不少于 115	长沙	5 年
15.	否	备份对接设备	套	1	长沙	5 年
16.	否	数据加密	套	1	长沙	3 年
17.	否	密钥管理系统	套	1	长沙	3 年
18.	否	计算节点许可	个	100	长沙	3 年
19.	否	裸金属节点许可	个	100	长沙	3 年
20.	否	块存储许可	TB	300	长沙	3 年
21.	否	文件存储许可	TB	100	长沙	3 年
22.	否	对象存储许可	TB	300	长沙	3 年
23.	否	分布式关系型数据库服务	套	6	长沙	3 年
24.	否	数据同步工具	套	1	长沙	3 年

25.	否	容器服务	套	1	长沙	3 年
26.	否	分布式缓存服务	套	2	长沙	3 年
27.	否	DevOps	套	1	长沙	3 年
28.	否	微服务平台	套	1	长沙	3 年
29.	否	API 网关	套	1	长沙	3 年
30.	否	运维平台	套	1	长沙	3 年
31.	是	云底座及其他组件	套	1	长沙	3 年
32.	否	技术支持类服务	套	1	-	3 年
33.	否	集成实施类服务	套	1	-	-
34.	否	集成实施辅材	套	1	-	-

表 2：交付成果

序号	项目	单位	数量	备注
1.	云平台系统及软、硬件清单	1	套	采购需求所列产品
2.	CMMI5 过程域文档和项目资料	1	套	见 1.5.2.2
3.	完成云平台相关培训	1	套	
4.	完成上云试点应用上线	1	套	
5.	满足本采购需求的云平台及其维保服务	1	套	包含硬件服务器维保

（三）★项目进度要求

（1）服务类：本项目自合同订立生效之日起开始执行，预计项目实施周期为 12 个自然月，验收通过后提供云平台整体 3 年，服务器设备 5 年的维保服务，实际结束时间以满足项目验收条件并且维保期结束为准，可根据实际情况延长。项目如有调整以买方通知为准，经甲乙双方协议一致，

合同期限可顺延。

本项目下各里程碑节点具体如下：

序号	里程碑节点	具体工作内容	进度要求	备注
1.	签订合同	双方签订合同	T0	
2.	实施准备	编写实施相关材料，勘察数据中心	T0+2 个月	编写的技术文档类别应包括规划类、设计类、实施类、测试类、上线类及运维类
3.	设备到货	设备运抵现场	T0+2 个月	
4.	系统集成实施	设备安装调试，云平台搭建	T0+4 个月	
5.	系统验证测试	系统测试、等保、渗透、密评	T0+6 个月	
6.	试点系统上云	协助完成试点应用上云验证	T0+8 个月	
7.	系统上线	完成云平台投产和功能验收	T0+12 个月	

备注：上表中“日”“月”“年”均为日历年月日。

（四）★项目实施地点

湖南省长沙市或甲方指定的其他地点。

（五）项目技术要求

本技术要求共有“★”指标 7 项，“#”指标 0 项，“△”指标 0 项。

序号	重要性	指标要求	是否提供证明材料及方式
1.	★	项目经理提供每周不低于 5*8 小时驻场服务，非工作时间或节假日可提供电话支持服务，紧急情况可快速赴现场处理	提供承诺书，并加盖投标人或云平台原厂商公章
2.	★	投标人需提供云平台整体 3 年，硬件服务器等 5 年的维保服务	提供承诺书，并加盖投标人或云平台原厂商公章

3.	★	在项目验收前提供不少于 40 课时云平台培训	提供承诺书, 并加盖投标人或云平台原厂商公章
4.	★	云平台原厂商 IaaS 和 PaaS 软件产品必须为同一厂商	提供承诺书, 并加盖云平台原厂商公章
5.	★	云平台原厂商 PaaS 主要软件产品(分布式关系型数据库、分布式缓存、容器服务、微服务平台) 必须有实际运行于云上的应用案例	提供合同关键页复印件(包括合同首页、体现产品内容页、盖章页、验收标准及甲、乙双方已签署验收通过的验收报告(或其他可证明云上运行的材料))作为有效证明文件, 需加盖投标人或云平台原厂商公章
6.	★	云平台原厂商 PaaS 产品(1.4.3 包含产品, 除 DevOps 外) 必须具备软件著作权	提供著作权证明材料(有效期内复印件加盖云平台原厂商公章, 著作权证明材料可按产品单独提供, 也可多个产品共用同一证明材料)
7.	★	云平台原厂商需具备成熟的公有云产品和运营经验	提供公有云运营侧用户登录成功截图(截图需加盖云平台原厂商公章)和有效期内《中华人民共和国增值电信业务经营许可证》(互联网数据中心业务)(提供证书复印件并加盖云平台原厂商公章)

(六) ★履约验收方案

1. 验收主体

采购人 农信银资金清算中心有限责任公司

采购人拟邀请 (☒ 本项目供应商 ☒ 第三方专业机构

☐ 专家 ☐ 服务对象)

2. 验收时间

到货验收时间：自设备上电试运行完成后 7 个日历日内；

集成部署验收时间：设备到货 2 个月内，中标人应按照项目实施服务要求中集成部署要求完成设备安装及相关软件调试等集成部署工作，并自集成部署完成 2 个月内通过相关测试（验证测试要求项目实施服务要求项验证测试要求）后，中标人向招标人提出书面申请，招标人、中标人双方及原厂商进行集成部署验收。

项目试运行验收时间：完成集成部署验收 2 个月内，中标人应按照实施服务要求中试点应用部署要求完成相关工作。完成试点应用部署后 4 个月内，中标人应按项目实施服务要求系统上线要求完成相关工作。完成系统上线相关工作后，经招标人同意，双方启动项目试运行，试运行期间 3 个月，试运行期满，投中标人向招标人提出申请，中标人、招标人及原厂三方进行试运行验收。招标人有权结合自身情况调整试点应用部署及系统上线时间，但应提前书面通知中标人方。

技术转移验收时间：自技术转移要求满足后 7 个日历日内；

项目最终验收时间：项目试运行验收通过后满 6 个月，经中标人向招标人提出终验申请，中标人、招标人双方及原

厂商进行项目终验。

质量保证期：针对服务器、备份对接设备，质量保证期为自项目最终验收合格后次日起 60 个月，其他软硬件为自项目最终验收后次日起 36 个月。

合同履行期限：自合同签订之日起至合同全部权利义务履行完毕之日止。

上述为计划日期，若验收不通过顺延。

3. 验收方式

现场验收或验收评审会议。

4. 验收程序

由中标人提出验收申请，招标人组织各相关部门对项目的质量、进度、范围，按照验收标准进行验收。

5. 验收内容

项目各阶段验收应按照合同中“验收”章节及合同其他约定完成。

（1）到货验收

在合同签订后设备到货时间是否满足要求；软、硬件设备到货后，核对与供货通知单的品类、数目、配置是否一致；中标人协调软、硬件原厂商将箱体拆封，核对设备外包装、

外观是否完好, 装箱单等随机资料是否齐全; 硬件设备上电试运行。

(2) 集成部署验收

生产云的设备安装和软件系统调试是否满足集成部署要求, 完成时间是否满足需求; 是否根据验证测试要求进行验证测试, 验证测试是否通过。

(3) 项目试运行验收

农信云生产云的业务功能、技术指标是否满足要求, 且项目试运行3个月内有无严重等级缺陷发生。

(4) 技术转移验收

中标人是否提供了完备的云平台软硬件部署、使用、开发、测试、维护、故障处理以及对外接口开发等方面的详细的使用文档, 并使招标人相应的技术人员达到相应的技术水平。

(5) 项目最终验收

完成质量检测认证、整体优化完善等工作后, 中标人、原厂商和招标人(必要时由第四方参加)共同组成验收小组进行项目最终验收。重点关注项目期间产生的所有问题是否得以有效解决, 终验前6个月内是否有严重缺陷发生, 中标人各阶段的提供的文件、文档是否符合相关要求, 各类报告是否完备合格。

6. 验收标准

(1) 到货验收

满足如下标准, 视为验收通过, 签署到货验收报告:

中标人应按照项目实施服务要求中的设备到货验收要求完成相关工作, 并保证交付软硬件品类、数目、配置采购清单及服务要求一致, 设备外包装、外观完好, 装箱单等随机资料齐全, 硬件设备上电试运行无误。。

(2) 集成部署验收

满足如下标准, 视为验收通过, 签署集成部署验收报告:

中标人遵照实施服务要求集成部署要求、验证测试要求完成相关工作。

(3) 项目试运行验收

满足如下标准, 视为验收通过, 签署试运行验收报告:

农信云生产云的业务功能、技术指标满足要求, 且项目试运行 3 个月 after 无严重等级 3 级以上 (含 3 级) 缺陷发生。

缺陷分类说明如下:

严重等级 1: 系统无法运行。即在日常必需的功能测试和运行中, 系统无法正常完成工作或无法产生正常结果。

严重等级 2: 系统存在功能、性能缺陷。但系统能够运行, 在某些特定环境下, 无法达到性能或功能要求。

严重等级 3: 系统存在功能、性能缺陷。但在生产环境中, 可采用其它方式替代或弥补, 并达到同样效果。

严重等级 4: 微小缺陷。系统功能、性能符合要求, 可以服务于用户, 有局部需要改动或润色

(4) 技术转移验收

满足如下标准, 视为验收通过, 由中标人、原厂商和招标人签署技术转移验收报告:

中标人按实施服务要求中技术转移要求提供了完备的技术文档, 提供了相应的培训及考试机会, 提供了必要的工具并使招标人相应的技术人员达到了如下的技术水平:

- a. 能够熟练使用和维护农信云平台:
- b. 能够独立进行接入交换机、计算节点、裸金属节点、容器 Node 节点、存储节点的扩容、缩容、更换等操作;
- c. 具有熟练查阅各种相关技术文件及维护手册的能力
- d. 掌握农信云平台的工作原理以及基于标准接口的开发方法。

(5) 项目最终验收

满足以下标准, 并自项目最终验收需求满足后 7 个日历日内视为验收通过, 签署项目最终验收报告:

- a. 项目期间产生的所有问题均得以有效解决。
- b. 终验前 6 个月无严重等级 3 级以上 (含 3 级) 缺陷发生。
- c. 中标人提供了项目软硬件原厂提供的维保服务承诺函。

缺陷分类说明如下:

严重等级 1: 系统无法运行。即在日常必需的功能测试和运行中, 系统无法正常完成工作或无法产生正常结果。

严重等级 2: 系统存在功能、性能缺陷。但系统能够运行, 在某些特定环境下, 无法达到性能或功能要求。

严重等级 3: 系统存在功能、性能缺陷。但在生产环境中, 可采用其它方式替代或弥补, 并达到同样效果。

严重等级 4: 微小缺陷。系统功能、性能符合要求, 可以服务于用户, 有局部需要改动或润色。

c. 各阶段所涉及的所有安装文件、源程序、构建、配置文件、相关技术文档、培训资料等均已提供, 并书面保证移交的源程序编译后和线上运行的程序完全一致。

d. 具备权威部门出具的符合相关标准规范与认证的证明或报告(网络安全等级保护三级、商用密码应用安全性评估三级), 优化点验收测试报告。

7. 其他事项

1. 如各阶段验收中发现交付合同产品有缺陷或其他与合同约定不符合的情形, 中标人应在招标人指定的期限内免费进行更换或版本升级, 直至中标人通过各阶段验收, 其间延误的时间视为中标人方逾期交付的时间。

2. 如出现中标人逾期的情形, 招标人费用支付相应顺

延，招标人就此不承担任何责任。

3. 招标人有权适当调整到货计划及验收安排，但应自本合同约定的相应截止日期前 3 个工作日内书面告知中标人。

4. 中标人在完成相关工作后，应积极向招标人申请验收，并配合招标人方、协调原厂开展验收工作。经招标人验收不合格的，中标人应协调原厂进行整改，并尽快再次提请招标人验收。除招标人认可的情形外，经两次验收仍不合格的，均视为中标人逾期，每逾期一日，招标人需向中标人方支付合同总价款 0.5%的违约金，并承担继续履行本合同的相关义务。如逾期时间超过 180 天，招标人方有权单方解除本合同，中标人方应按合同总价款的 20%向招标人支付违约金。

（七）派驻实施人员简历格式要求

针对本项目投标方拟派驻的实施人员，提供固定的人员派遣格式，同时附简历，供投标方填写，格式如下：

序号	本项目任职	姓名	学 历	专 业	执业或职业资格证明			备注
					证书名称	级别	编号	

二、供应商资格条件

(三) 投标人资格条件

投标人为云平台代理商的，还需提供云平台原厂商资格条件相关材料。

序号	分类	资格条件
10	投标人	在中华人民共和国境内依法登记的法人或其他组织，合法运作并独立于招标人和招标代理机构，需提供有效的营业执照复印件，法定代表人身份证明复印件等证明文件，并加盖公章。
11		单位负责人为同一人或存在控股、管理关系的不同单位，不得参加同一标段/标包投标或未划分标段/标包的同一招标项目投标。需提供加盖公章的承诺函原件（格式自拟）。
12		投标人应经营状况良好，符合《中华人民共和国政府采购法》第二十二条的规定,且必须为未被列入信用中国网站 (www.creditchina.gov.cn)、中国政府采购网 (www.ccgp.gov.cn) 渠道信用记录失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人，否则其投标将被拒绝。 投标人必须在投标文件中提供下述资格证明文件，否则按无效投标处理： 1、法人或者其他组织的营业执照等证明文件，自然人的身份证明； 2、财务状况报告，依法缴纳税收和社会保障资金的相关材料； (供应商应提供书面承诺)

序号	分类	资格条件
		3、具备履行合同所必需的设备和专业技术能力的证明材料；（供应商应提供书面承诺） 4、参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明；（供应商应提供书面承诺） 5、具备法律、行政法规规定的其他条件的证明材料。（以上均为《中华人民共和国政府采购法实施条例》第十七条之规定）
13		本项目不接受联合体投标。
14		投标人资质证书要求：无。
15		产品资质证书要求：无
16	技术	原厂商说明函或授权函要求： 本项目仅限于云平台原厂商投标或其授权的代理商投标。投标人若为代理商，须获取云平台原厂商关于参与本项目投标的 授权书 ，同一代理商只能代理一个云平台原厂商的产品 同一品牌云平台厂商参与本项目的投标人（包括原厂商和代理商）数量不得超过两家，超过两家则该云平台原厂商、原厂商的代理商投标均将被拒绝。
17		投标人须保证，招标人在其本国使用其提供的货物时，不存在任何已知的不合法的情形，也不存在任何已知的与第三方专利权、著作权、商标权或工业设计权相关的任何争议。如果有任何因招标人使用投标人提供的货物而提起的侵权指控，投标人须依法承担全部责任，需提供书面承诺并加盖公章（格式自拟）。
18		团队人员要求：无

（四）云平台原厂商资格条件

序号	分类	资格条件
8	商务	在中华人民共和国境内依法登记的法人或其他组织，合法运作并独立于招标人和招标代理机构，需提供有效的营业执照复印件，法定代表人身份证明复印件等证明文件，并加盖云平台原厂商公章。
9		单位负责人为同一人或存在控股、管理关系的不同单位，不得参加同一标段/标包投标或未划分标段/标包的同一招标项目投标。需提供加盖公章的承诺函原件（格式自拟）

序号	分类	资格条件
10		经营状况良好,符合《中华人民共和国政府采购法》第二十二条的规定,且必须为未被列入信用中国网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道信用记录失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人,否则其投标将被拒绝。 投标人必须在投标文件中提供下述资格证明文件,否则按无效投标处理: 1、法人或者其他组织的营业执照等证明文件,自然人的身份证明; 2、财务状况报告,依法缴纳税收和社会保障资金的相关材料;(供应商应提供书面承诺) 3、具备履行合同所必需的设备和专业技术能力的证明材料;(供应商应提供书面承诺) 4、参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明;(供应商应提供书面承诺) 5、具备法律、行政法规规定的其他条件的证明材料。(以上均为《中华人民共和国政府采购法实施条例》第十七条之规定)
11	技术	资质证书要求:无
12		产品资质证书要求:无
13		原厂商说明函或授权函要求:无
14		团队人员要求:无

三、最高限价设置

本项目是否设置最高限价, ☐ 不设置, ☒ 设置: 5153 万元

附件：

评分细则

一、评标办法与分制

本项目评审采用综合评分法，百分制，标准分为 100 分（不含加分）。

二、评分方法与评审原则

1、评标委员会评委根据本细则所列评分标准，对各投标人进行独立评分。
各评委对投标人的评分进行算术平均得出投标人最终得分，并据此对投标人进行排名推荐中标候选人。

2、评审中应遵循“质优价廉者优先”的综合评审基本原则。

三、评分标准（见下表）

■综合评分法，选择该评审规则的理由：本项目为系统建设项目，需要从商务、产品、技术、服务进行综合评估服务商能力。

价格分分值_40_分，商务分分值 15 分，技术分分值_45_分，合计 100 分：

序号	评审项	评审因素	分值参考	评分细则
----	-----	------	------	------

序号	评审项	评审因素	分值参考	评分细则
一	价格评分	报价情况	40	【客观分】 1. 评审价：评审价=含税的投标总价； 2. 评审基准价：满足招标文件要求且最低的有效评审价； 3. 价格分计算：评审价=评审基准价的投标人，价格最低的满分；其他投标人的价格分按照以下公式计算，并精确到小数点后两位：价格得分=（评审基准价/投标人的评审价）×本项分值。
二	商务评分	企业综合实力	2	【主观分】 根据云平台原厂商的企业整体实力、组织架构和信誉状况、社会影响力等方面进行综合评审，优秀得2分，较好得1分，一般得0分。
		企业资质	3	【客观分】 云平台原厂商具备 ISO22301（业务连续性管理体系认证）、ISO27001、ISO27017、ISO27018、ISO27701、CSA STAR 证书，每具有1项得0.5分，满分3分。提供证书复印件。 证明文件：须提供有效期内的认证证书复印件，并加盖原厂商公章。
		同类项目业绩	10	【客观分】 投标人所投云平台产品自2018年1月1日至今同类项目（至少包含IaaS和PaaS组件）成功实施案例进行打分的案例情况，要求节点数超过500个（同一案例可多个合同累计），每个有效案例得2分。要求如下： 1. 需提供合同关键页复印件（包括合同首页、体现项目内容页、签署日期页、盖章页、验收标准及甲、乙双方已签署验收通过的验收报告（或其他可证明项目已成功实施的材料））作为有效证明文件； 2. 相同法人单位（包括同一集团公司下的分公司）的业绩视为一个有效案例；
三	技术评分	技术要求	10	【客观分】 1. 根据所投云产品原厂商提供的可信云认证证书评分（www.kexinyun.org.cn），内容需涵盖私有云平台（或专有云平台）、云存储（块存储或对象存储至少具备其一）、数据库、负载均衡、云安全，全部具备得5分，每缺1项扣1分，扣完

序号	评审项	评审因素	分值参考	评分细则
				为止。（需提供证书复印件、证书所属主体与所投产品、所投产品原厂商的关系说明，并加盖云产品原厂商公章。） 2. 使用所投云平台产品的项目通过国家网络安全等级保护三级测评，提供备案证明及测评报告并加盖原厂商公章，得4分，通过国家网络安全等级保护四级测评，提供备案证明及测评报告并加盖原厂商公章，得5分，其它不得分。（本项得分以通过等级保护测评最高等级为准，不同时加分）
		实施团队	10	【客观分】 根据投标人和云平台原厂商实施人员团队（提供的人员在后续审查通过后，须实际参与项目现场实施工作）情况进行打分： 1. 项目经理：每个投标人均需指定一位云平台原厂商人员担任项目经理，3年以上工作经验，至少有2个和本项目同等规模（单数据中心计算节点数量不小于100个）的项目经历（并在其中担任项目经理）。上述要求若不能同时满足，则本项得0分。在满足上述要求的基础上，按照如下标准，进行评分： （1）拥有5年或以上金融行业项目相关领域工作经验得1分； （2）拥有4（含）年以上5（不含）年以下金融行业项目相关领域工作经验得0.5分； （3）项目经理主导过4个金融行业云建设项目经验（相同法人单位（包括同一集团公司下的分公司）的项目视为同一个项目），得2分。 （4）项目经理主导过3个金融行业云建设项目经验（相同法人单位（包括同一集团公司下的分公司）的项目视为同一个项目），得1分。 本项得分（1）、（2）两项不可同时得分，（3）、（4）两项不可同时得分。 2. 投标人需提供符合要求的项目实施团队，实施团队中云平台原厂商人员要求如下： （1）实施团队提供至少2名专家，要求具备所投云平台最高级别认证并主导设计过至少2个金融

序号	评审项	评审因素	分值参考	评分细则
				行业的 IaaS 私有云项目, 得 3 分, 否则得 0 分; (2) 实施团队需提供至少 4 名高级工程师与至少 4 名中级工程师, 满足得 4 分, 否则不得分; 其中, 专家、高级工程师、中级工程师的标准为: 专家: 本科毕业或以上, 8 年及以上工作经验, 5 年及以上金融行业经验; 至少在 2 个总部级项目中担任架构师。 高级工程师: 本科毕业或以上, 5 年及以上工作经验, 3 年及以上金融行业经验; 具有所投云平台产品相关认证, 至少参与过 2 个以上金融行业同类项目的实施。 中级工程师: 本科毕业或以上, 3 年及以上工作经验, 至少参与过 1 个以上同类项目的实施。 注: (1) 投标人应提供实施人员团队名单和人员简历 (格式见招标文件《拟派人员信息表》); (2) 投标人和原厂商人员, 须提供本单位自 2020 年 10 月 1 日起至今任意连续 3 个月为其缴纳的社保证明, 并加盖本单位公章 (否则不予认可)。 (3) 上述所有人员的金融行业工作年限、项目经验应在个人简历中列出 (原厂商人员的简历须加盖原厂商公章); 涉及资质认证的, 须提供证书复印件 (原厂商人员的资格认证须加盖原厂商公章); (4) 对于项目团队成员的个人简历所列内容, 评标委员会和甲方保留进一步审查的权利。
		实施方案	10	【主观分】 对投标人提供的集成实施方案进行评价: 方案中需包括总体设计方案, 综合布线设计方案, 物理部署规划方案, 实施计划与里程碑, 各阶段交付物清单等相关内容。比较各投标人提交的实施方案的完整性、安全性和专业性等方面进行打分。 (此项内容不得超过 50 页, 超过 50 页不得被评为一般优秀及以上) 特别优秀 10 分, 较为优秀 9, 一般优秀 8. 特别良好 7 分, 较为良好 6, 相对良好 5, 一般良好 4, 一般 3, 较为一般 2, 及格 1, 不及格 0。

序号	评审项	评审因素	分值参考	评分细则
		维保及扩容价格	5	【主观分】 根据投标人对本次采购云平台软维保期结束后 3 年（含）内的维保价格以及后续对云平台软、硬件扩容方案的响应情况，根据扩容方案完整性，价格越低，方案越优，综合进行评分。 特别优秀 5 分，优秀 4 分，良好 3 分，较好 2，一般 1，较差 0 分。
		非实质性偏离	10	【客观分】 每有一项#不满足或负偏离扣 0.5 分，需在偏离表中提出偏离，未在偏离表中提出偏离则视为完全响应，本项最多扣 10 分。
四	总分		100 分	

★代表最关键指标，不满足该指标项将导致投标被拒绝； #代表重要指标，全部满足或优于该指标得 10 分，共计 27 项。

属于主观评价的指标包括（列出详细的指标编号）：

企业综合实力、实施方案、维保及扩容价格

属于客观评价的指标包括（列出详细的指标编号）：

报价情况、企业资质、同类项目业绩、技术要求、实施团队、非实质性偏离