

一、云服务内容和技术要求

1.1 总体要求（适用于包1、包2）

- (1) 本招标内容与技术要求作为投标人给出技术方案和报价的依据，采购人拥有本招标内容与技术要求的最终解释权。
- (2) 中标方必须根据本项目的各项服务技术要求，提供科学、合理、先进、可行、适合采购人实际情况的服务。
- (3) ★本次项目遵循多云异构原则，采购包1与采购包2的主要国产化产品（云管理平台、存储、核心交换机）须为不同的品牌，如采购包2排名第一的中标候选人所使用的主要产品与包1标段中标候选人所使用的主要产品品牌相同，将不具有子包2的候选人推荐资格，从具有中标候选人资格的投标人中，由排名次高的投标供应商为中标候选人，以此类推；投标人须提供规则确认函，格式自拟。
- (4) 本次政务云服务总体要求是招标人对投标人提出的基本要求，投标人可进行优化，具体投标人方案中的功能、性能可优于本次采购项目内容及技术要求。
- (5) 中标方负责本项目采购服务的部署、实施、调试、运维管理并提供相关服务。
- (6) 当云资源使用单位需要增加服务资源时，中标方须按采购人要求及时提供相应服务。
- (7) 中标方保证业务系统连续稳定运行的前提下积极开展全量业务迁移工作。涉及的业务迁移所产生的费用需中标方自行承担。
- (8) 云平台分区要求：云平台分为互联网接入区和电子政务外网区，满足弹性扩容需求，两个区域计算、存储、网络、安全防护物理独立，并根据业务需求细分业务子区，两个区域之间通过安全隔离交换系统实现数据安全交换。
- (9) 网络资源要求：云平台核心骨干设备、出口设备、骨干线路等需要支持冗余备份，云内骨干线路带宽 $\geq 40\text{Gb}$ 带宽，服务器业务 $\geq 10\text{Gb}$ 带宽。需具备虚拟路由功能，支持定制虚拟路由器的路由规则。交换机需具备虚拟化部署能力。支持用户可自定义虚拟主机的网络拓扑和

IP。实现具备虚拟机之间、虚拟机与云平台之外进行网络通信，根据业务需求可以实现虚拟机内部组网和虚拟私有网络等网络功能。

- (10) 网络安全要求：投标人需通过部署防火墙、DDOS 防护、主机安全、web 应用防火墙、安全审计、运维安全管理、日志审计等产品，为云平台建设安全通信网络、安全区域边界、安全计算环境、安全管理中心。云平台安全建设必须满足《GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求》中等级保护三级设计要求进行防护，且通过网络安全等级保护测评三级及以上。
- (11) 商用密码合规性改造要求：通过部署签名验签服务器、时间戳服务器、服务器密码机等密码产品，为云平台提供商用密码技术安全防护能力。云平台密码合规性改造必须按照《中华人民共和国密码法》和 GB/T 39786-2021《信息系统密码应用基本要求》要求，且通过商用密码应用安全性评估三级及以上。
- (12) 政务云开放要求：中标人提供的政务云平台应具备开放性，需配合招标人提供相关接口权限，主要涉及 IaaS 资源服务域名地址、网络服务域名地址、虚拟机/主机（CPU、内存、网络、磁盘）等监控采集接口权限，满足招标人各方面应用要求（例如安全、监管、存储等）。
- (13) 要求投标人提供的政务云平台与呼伦贝尔市政务外网的专用互联光纤带宽不小于 1G，以满足网络互访的要求，并提供高可靠的双线路保护措施；要求提供的政务云和互联网独享出口总带宽不少于 2G，可扩充到 20G，互联网线路提供高可靠的双线路保护措施。
- (14) ★为确保政务云平台持续稳定运行，保障政务业务系统的可用性、可靠性、先进性，投标人须明确列出所提供的政务云服务平台所涉及国产化部分软件、硬件产品的设备厂商、设备型号，并提供不少于 3 年的产品原厂质保、提供产品制造商售后服务承诺函并加盖产品制造商公章。
- (15) 若在服务期开始后，有在本次招标时未涉及的云服务需求，可双方友好协商，服务价格另行商议。

1.2 总体服务要求（适用于包1、包2）

1.2.1 服务要求及模式

1.2.1.1 服务要求

- （1） 采购服务符合工信部《基于云计算的电子政务公共平台顶层设计指南》、《信息安全技术云计算服务安全指南》和《信息安全技术云计算服务安全能力要求》等国家及行业标准、规范的政务云平台。
- （2） 为增强政务云服务支撑能力，云平台应具备 PaaS 层服务能力，PaaS 层应具备与第三方控件、模块对接能力。
- （3） 建设政务云安全管理体系和运维管理体系，为上云政务应用系统稳定持续运行提供全面支撑。
- （4） 投标人必须按照政务云管理单位要求开放云计算相关平台接口。

1.2.1.2 建设及运营模式

呼伦贝尔市本级政务云采用云服务采购的模式，由云服务商建设符合招标文件要求的政务云资源池，完成政务云平台的建设部署并通过相关测评后为招标人提供政务云服务。

政务云云平台及承载云平台所需的硬件、与政务外网互联的共享链路（非专线业务）及机房均由投标人提供，并承担相关建设和运行维护成本。

投标人应在云管理单位的指导下构建统一完整的政务云服务体系。政务云验收合格并投入使用后，云管理单位根据资源使用量支付服务费用。

1.2.1.3 采购服务要求

1.2.1.3.1 政务云专用

★投标人应承诺所提供的政务云平台必须是为采购人专用云平台，独享机房或物理隔离，具体要求如下：承诺函格式自拟，投标时提供，承诺函需包含但不限于以下内容：

- （1） 设备专用：投标人提供的云平台为呼伦贝尔市本级政务专用。本项目所提供的云平台所涉及的所有软硬件资源仅限于纳入呼伦贝尔市本级云服务范围的单位使用（由采购人确定），未经采购人允许不得提

供给其他用户使用；禁止政务云与其他未经许可的平台连通。

- (2) 管理专用：针对云平台制定完善的管理制度，不得随意开通用户及提供各类云服务。
- (3) 人员专用：投标人需配备专门的运维管理团队，未经采购人同意，不得随意变动和调用。
- (4) 专网专用，互联网区与政务外网区的云服务平台不得复用，需分别独立建设；

1.2.1.3.2 物理环境要求

呼伦贝尔市本级政务云服务平台设备需部署在符合 IDC 数据中心建设标准的机房内。

根据本项目的需要，机房相关要求如下。

- (1) 机房附近不应有污染气体、强电磁场、强震动源、强噪声源及所有危害系统正常操作或运行的因素。
- (2) 为保障政务云安全及使用方便，需要机房建设位置在呼伦贝尔市区内（海拉尔区、鄂温克旗），投标时须提供数据中心的详细地址。

1.2.1.3.3 投标人服务要求

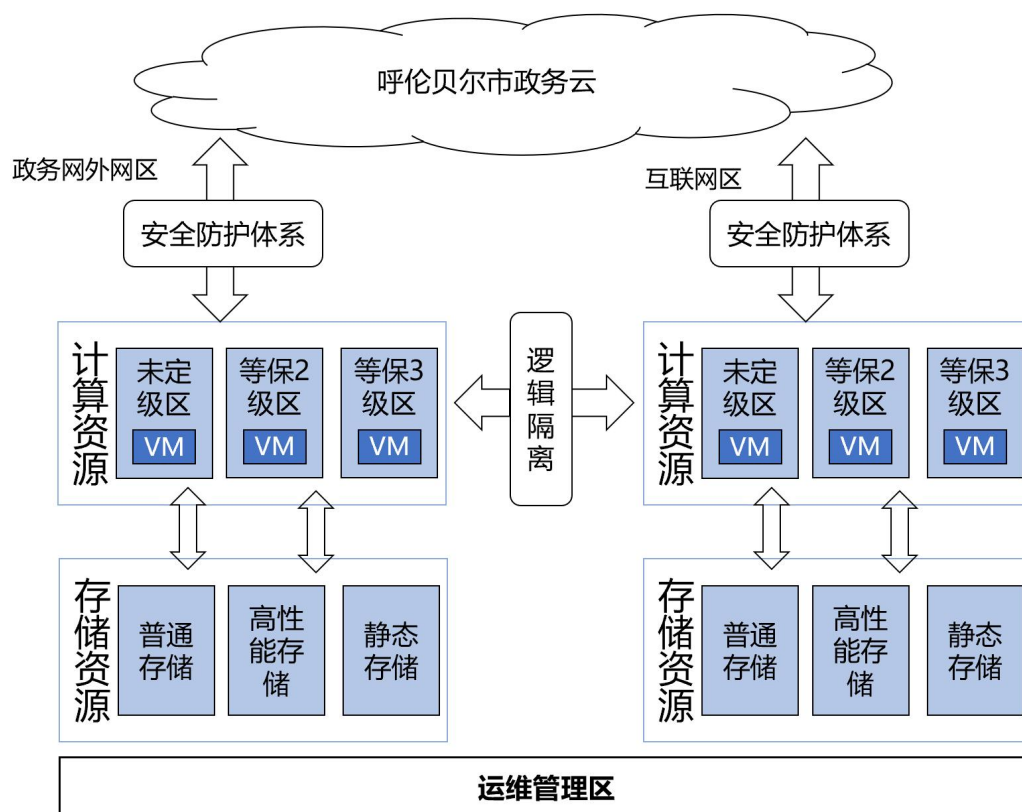
- (1) 云基础设施建设要求：提供云基础设施的网络、存储、服务器、虚拟化平台、安全服务及通信链路等。
- (2) 云平台应能提供包括计算服务、存储服务、网络服务、数据库及运维保障服务在内的服务能力。
- (3) 投标人应及时跟踪云计算发展趋势，特别是业界发生云安全相关事件时，及时报告给政务云管理单位参考。
- (4) 知识产权要求：投标人采用的云平台软件必须满足国家在知识产权方面的有关规定和要求。投标人云计算平台应采用成熟稳定的云计算平台产品。
- (5) 运维能力要求：投标人需要能够对云基础设施、平台软件和业务应用

系统提供集中运维管理、监控，包括虚拟化、服务器、存储、网络、安全等，可以实现资源利用率可视化，实现对政务云中出现的事件、问题和故障定位，实现事前 预测及告警、事中及时处理和事后可审计。

- (6) 安全责任：投标人承担机房基础设施层面（主要包括机房及通信链路）、云平台层面（主要包括物理资源、计算资源、存储资源、网络资源）以及云平台数据防篡改、防丢失的安全责任；具备实时监控云平台层面各项资源运行状态的能力；有义务配合政务云使用单位排查上云系统问题。针对迁移上云的业务需要与各使用单位确认系统安全，不会对其他业务系统造成安全攻击。
- (7) 投标人所提供的云平台须按照信息系统安全等级保护三级标准进行建设，确保通过等级保护三级安全测评，并在建设完成 1 年内通过云计算服务安全评估。
- (8) 数据保护要求：政务数据未经采购人许可不得离开政务云机房。投标人应承诺，未经采购人许可不得对云平台上的任何数据进行非法截取、加工、分析处理或提供给第三方机构。
- (9) 投标人在未经过采购人书面材料确认前提下，不能查看、修改、拷贝用户业务系统文件和数据；各业务系统、数据归属于采购人及政务云使用单位，云服务商无权支配。
- (10) 应急演练：投标人须配合采购人建立云平台应急体系，定期开展演练工作，保障灾难发生时，能够保留数据、恢复数据。投标人负责指导或协助云平台使用单位开展系统应急工作。
- (11) 系统迁移上云：云投标人须配合云使用单位完成迁移上云。投标人必须按照政务云管理单位要求开放云计算相关平台接口。投标人需接受包括第三方检测、调解，对政务云管理单位的合理要求需无条件给予配合。

1.2.1.4 政务云整体架构要求

按照政务云平台服务规范要求，划分电子政务外网和互联网两个区域，两个区域间通过安全数据交换区实现不同区域间的数据安全交换。



政务云平台内部需要划分安全隔离区，每个安全隔离区之间的访问需有统一的安全策略管理。安全区设立规划但不限于：

互联网业务区：互联网业务区主要为公众和企业提供互联网门户网站服务和政务服务，由于门户网站群分属各不同的政务部门，其安全要求各有不同，对网站和信息系统可根据不同的安全级别进行分等级防护。

公共业务区：公共业务区主要实现跨部门、跨地区的信息共享、数据交换及业务协同，提供政务部门内部的公共服务。

部门业务区：用于部署市级政府部门业务系统，可按要求部署在不同的VPC，VPC 之间采用 VPN 技术隔离。部门业务区资源池分为通用资源池和信创资源池，依据政府部门上云业务的实际需求提供通用云主机和信创云主机服务。

云资源管理区：为整个政务云系统提供云资源管理和物理资源抽象，以及日常运维所必须的运维系统和认证管理系统。通过资源管理区实现对各类云资源的实时监控、管理、预警和应急处置，并对虚拟机迁移、资源弹性扩展、业务使用情况及运维操作人员进行实时监控和审计。

投标时投标人根据对政务云的理解，结合呼伦贝尔市政府对政务云的要求，在投标文件中给出详细部署方案及拓扑图。

1.2.1.5 资源池基础要求

★包 1、包 2 所提供的政务云服务环境承载能力不得低于下列要求，并提供承诺函，格式自拟：

互联网区：

- 可用 vCPU \geq 3500vCPU，且 CPU 物理核数 \geq 1280 核
- 可用内存 \geq 10240GB
- 块存储可用容量 \geq 300TB
- 文件存储可用容量 \geq 300TB
- 互联网带宽：2*1G
- 安全：通过商用密码应用安全性评估和网络安全等级保护测评（备案等级：3 级）

政务外网区：

- 可用 vCPU \geq 3500vCPU，且 CPU 物理核数 \geq 1280 核
- 可用内存 \geq 10240GB
- 块存储可用容量 \geq 300TB
- 文件存储可用容量 \geq 300TB
- 政务外网专线带宽：2*1G
- 安全：通过商用密码应用安全性评估和网络安全等级保护测评（备案等级：3 级）

1.2.2 服务标准

1.2.2.1 政策及合规要求

投标人所提供的云平台应满足包括但不限于以下国家标准要求：

- 《信息安全技术信息系统安全管理要求》（GB/T 20269-2006）
- 《信息安全技术信息系统通用安全技术要求》（GB/T 20271-2006）
- 《信息安全技术操作系统安全技术要求》（GB/T 20272-2019）
- 《网络安全技术网络和终端隔离产品技术规范》（GB/T 20279-2024）
- 《信息安全技术信息系统安全工程管理要求》（GB/T 20282-2006）
- 《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
- 《信息安全技术信息系统灾难恢复规范》（GB/T 20988-2007）
- 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
- 《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）
- 《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2019）
- 《信息安全技术网络安全事件分类分级指南》（GB/T 20986-2023）
- 《信息系统密码应用基本要求》（GB/T 39786-2021）
- 《计算机场地通用规范》（GB/T 2887-2011）
- 《信息技术服务服务基本要求》（GB/T 37961-2019）
- 《信息技术服务运行维护》（GB/T 28827）
- 《信息技术云计算云服务交付要求》（GB/T 37741-2019）
- 《基于云计算的电子政务公共平台技术规范》（GB/T 33780）
- 《基于云计算的电子政务公共平台总体规范》（GB/T 34078）
- 《基于云计算的电子政务公共平台安全规范》（GB/T 34080）
- 《基于云计算的电子政务公共平台服务规范》（GB/T 34079）
- 《基于云计算的电子政务公共平台管理规范》（GB/T 34077）
- 《信息技术云计算云服务运营通用要求》（GB/T 36326-2018）
- 《信息技术云计算云服务计量指标》（GB/T 37735-2019）
- 《信息技术云计算云平台间应用和数据迁移指南》（GB/T 37740-2019）
- 《信息技术服务服务管理》（GB/T 36074）
- 《信息技术云数据存储和管理》（GB/T 31916）
- 《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）
- 《信息技术服务从业人员能力评价要求》（GB/T 37696-2019）

- 《信息安全技术云计算服务安全能力要求》（GB/T 31168-2023）
- 《信息技术云资源监控指标体系》（GB/T 37938-2019）
- 《信息技术大数据存储与处理系统功能要求》（GB/T 37722-2019）
- 《信息技术云计算分布式块存储系统总体技术要求》（GB/T 37737-2019）
- 《信息技术服务质量评价指标体系》（GB/T 33850-2017）
- 《信息技术云计算云服务级别协议基本要求》（GB/T 36325-2018）
- 《信息安全技术政府部门信息技术服务外包信息安全管理规范》（GB/T 32926-2016）

1.2.2.2 服务考核要求及惩罚条款

为加强政务云平台的可靠性与可用性，提升运营和管理服务水平，督促中标人持续提高政务云服务质量，采购人将根据政务云平台服务质量（SLA）指标相关考核评价办法对中标人的服务进行考核评价，并根据考核结果执行相应处置条款。

产品分类	服务项目	可用性目标
计算服务	云服务器	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	裸金属服务器	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
存储服务	块存储	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	文件存储	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
网络服务	服务器负载均衡	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	公网弹性 IP	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	互联网独享带宽	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	互联网共享带宽	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
大数据服务	大数据服务（平台、计算、检索、消息、列式存储）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
MPPDB 服务	MPPDB 服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
增值安全服务	日志审计服务（云主机）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月

产品分类	服务项目	可用性目标
	数据库审计服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	漏洞扫描服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	云防火墙服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	Web 应用防火墙服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	网页防篡改服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	云堡垒机	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	VPN 接入服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	应用检测服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	中间件服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
软件服务	API 网关	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	云备份服务（本地备份）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	信创数据库（软件）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
数据库服务	集中式数据库服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
	分布式数据库服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 30 分钟/月
链路服务	端到端网络链路	端到端传输网络链路可用率 $\geq 99.95\%$ ；同城机房网络时延 $\leq 1.5\text{ms}$

投标人云平台可靠性未达标扣款：

1. 服务周期内，以上各产品实例如发生故障，故障不可用时间超过 30 分钟，每发生一次，采购人有权收取该实例当月费用等额的金额作为违约金，违约金上限为服务周期内该实例费用对应金额。

2. 服务周期内，年度政务云生产中心云平台可靠性应达到 99.95%。如未达到，指标每下降 0.01%，采购人有权收取本年度结算费用的 0.05%作为违约金。政务云平台不可用认定原则包括但不限于：单云区不可用、生产中心内 10%以上应用不可用等。

3. 在服务周期内，云平台每发生 1 起安全事件，中标人应向采购人支付本年度结算费用的 2%作为违约金；每年度累积超过 3 起，采购人有权单方解除合同并收取本年度结算费用的 10%作为违约金，违约金不足以弥补采购人

损失的，中标人还应当继续补足。安全事件认定原则：被省级或国家网络安全监管机构（网信、通管、公安、国安等部门）通报云平台存在安全隐患，中标人未在 24 小时内做有效处置或应急防护措施，造成业务系统瘫痪 1 小时以上、或被恶意篡改、或敏感信息泄露的事件。

1.2.3 项目整体实施要求

1.2.3.1 实施要求

为了充分满足采购人的需求，提供更优质的服务，投标人需提供先进、科学、执行性较强的实施方案，实施方案要具备合理性、全面性，技术应用成熟领先，结合呼伦贝尔市本级政务云承载计算、存储、网络、安全、PaaS 层服务等方面的需求，实施方案具体应包括针对需求理解及运行现状分析、项目实施组织架构、项目进度计划及应急响应措施、实施管理及进度保障、培训方案及质量保障等。

实施团队：投标人须针对本项目配备实施团队，项目经理统筹负责项目组织、协调、实施、对接，应具备关键节点汇报机制。同时配备项目技术负责人、安全负责人及专业的实施人员，确保项目能够顺利的开展实施工作。

项目安装调试服务：投标人需负责本合同包政务云中心的基础环境软硬件设备设施采购、安装部署及系统集成工作。负责对接电子政务网络系统，根据业务系统所处的网络环境，对接电子政务外网、公共互联网，为处于不同网络区域提供针对性的服务。另外须按照国家相关标准，建立完善的实施保障体系，保障本合同包政务云中心云资源按时交付。

数据隔离：政务专网区域的云服务需要与其他区域服务进行物理隔离。互联网区域与政务外网区域的云服务进行逻辑隔离。同时满足对不同安全级别、不同业务、不同业务专网的需要，支持虚拟专有域功能（VPC），能够划分隔离的区域为特定的用户提供云服务，区域内的资源与其他的用户逻辑隔离，完全为该用户使用。

培训服务：投标人须提供完整的培训方案。针对云平台、政务网络等日常操作及使用，提供全面的产品介绍和产品使用培训，包括安装、配置、运维管理、常见问题处置操作等。培训内容包括基本理论、软件的安装与操作、运行管理、现场操作辅导等。培训方式应包括技术讲课、操作示范和其它必须的业务指导和技术咨询，确保培训人员对系统基本理论、技术特性、操作规范、运行规程、管

理维护等方面获得全面了解和掌握。

1.2.3.2 性能要求

服务商需制定维护管理规定，并按规定制定详细的作业计划并执行，包括但不限于维护项目、维护周期和维护要求等，同时提供 7*24 小时驻场监控值守服务，重大事件及节日进行强化保障，确保整体稳定正常运行。提供的政务云平台整体可靠性应不低于 99.95%，数据可靠性应不低于 99.99%。

云平台可靠性指业务功能正常使用所占时间比例。以云主机为例，云主机服务可用性 = $1 - \frac{\text{客户所有云主机的累计故障时间}}{\text{客户所有云主机可用时间} + \text{客户所有云主机故障时间}}$ 。当云主机服务不可用时长超过 5 分钟记为故障，云主机故障时数为所有故障时间之和。

故障处理要求：处理政务云平台发生的各类软硬件等故障，确保上层业务系统能够正常稳定运行，故障响应时间小于 10 分钟，响应及时率不低于 99.9%。

1.2.3.3 服务团队要求

投标人须安排项目经验丰富的项目经理 1 人承接本项目，负责各种重大问题的处理及重要关系的协调，全面调配投标人的技术人员、设备工具、现场采购等资源，使项目资源实现最优化配置，为本项目的顺利实施和后续高效服务提供全力支持和保障。

服务团队要求：须为呼伦贝尔市本级政务云单独建立管理组织，配置相应团队，须组建高素质、专业性强、经验丰富、稳定的专业专职服务团队，驻场服务团队总人数不少于 5 人，服务团队负责呼伦贝尔市本级政务云平台运行管理维护工作，支撑云使用单位做好业务应用运行、维护、管理工作，响应故障请求，负责呼伦贝尔市本级政务云平台的故障受理、处理、跟踪、结果汇报工作，确保平台安全、稳定、高效运行。

1.2.4 迁移服务要求

1.2.4.1 整体要求

投标人需配合需求单位对上云及迁移业务系统进行调查摸底、制定上云及迁移方案，提供架构设计咨询、指导业务系统的开发单位进行代码修改和系统部署，在系统上云迁移前期提供非代码级别的迁移支持服务。提供服务方案，应配合各需求部门做好上云及整体迁移工作。

呼伦贝尔市本级政务云承载的业务系统，均要求达到 7*24 小时不间断运行的条件；如因业务需要必须短期中断时，必须经过报备许可，仅可在规定时间段内中断。迁移过程须充分进行风险评估，完全保证呼伦贝尔市本级政务云业务的连续性和可靠性。

迁移服务：投标人在中标后，需要对现有本合同包政务云中心进行整体业务迁移。在进行迁移的过程中需要确保数据的安全与保密工作，不得造成任何数据丢失或泄露。同时在实施迁移的过程中，需要进行平滑在线热迁移，确保迁移过程中各类业务不中断，迁移期间业务系统产生的数据不丢失。投标人在保障业务连续性、数据安全的前提下，对本合同包现有政务云进行整体迁移或优化，投标人需要制定完善的迁移服务方案确保迁移成功。

在完成数据迁移后，数据归属权归采购人所有，投标人须按照采购人要求处理相关迁移遗留数据。

迁移要求：投标人在中标后须制定详细的迁移方案，获得采购人的认可和书面授权后，方可迁移。投标人需要依据现有政务云平台架构、政务网络架构进行提前组网，从而达到无缝迁移。投标人中标后需对准备迁移的云主机、业务系统进行充分调研，制定详细的迁移方案，通过专家论证并获得采购人的书面认可后，方可迁移。投标人及其参与迁移的技术工作人员需要签订保密协议。

投标人需要在中标后 50 个自然日内完成全部设备部署、业务系统迁移、测试、验收等工作，其中至少包含 1 周业务运行测试期，因投标人未完成上述工作，所产生的额外费用（包含但不限于上一期服务延期费用）由投标人承担。

投标人需保证业务系统连续稳定运行的前提下积极开展全量业务迁移工作，涉及的业务迁移所产生的费用需投标人自行承担。

迁移过程中，由于迁移方案不合理、迁移实施不规范、迁移人员操作不合规造成安全问题的，如网络受到攻击篡改，病毒感染，数据丢失泄漏事故等造成业务系统计划外中断，由迁移方（投标人）承担由此产生的相关责任及损失。

1.2.4.2 迁移方案

投标人针对本项目实际情况，提供迁移服务方案，根据呼伦贝尔市本级政务云具体情况，制定有针对性的定制化业务迁移方案。

1.2.4.3 迁移实施

根据需求进行云计算资源和网络资源的准备，为云的迁移搭建好运行环境，从而保证业务系统顺利迁移。在迁移方案及迁移环境准备完成之后，按照和采购人商定的迁移计划进行业务迁移实施。

1.2.4.4 系统测试

在系统上线前，考虑新建云平台与本合同包原有云平台、政务云网络的环境差异，需在新建的云平台上进行充分的功能验证和性能测试。

1.2.4.5 系统割接

在完成系统测试并试运行稳定后，方可对业务系统进行上线割接，原有云平台的系统停止对招标人服务，将原有业务系统切换到新建的政务云平台，业务系统开始为招标人提供服务。

1.2.5 运维要求

投标人应具备能力完善的云管平台，提供给采购人及上云单位使用，并保证后续及时升级。投标人应根据项目特点和呼伦贝尔市本级政务云管理要求，制定政务云服务相关制度、规范，明确服务流程及相关表单样式。

投标人应提供7×24小时云资源使用情况监控服务，发生云资源使用率过高或过低情况时应及时通知采购人。每月提供政务云服务报告，月报对当月政务云服务情况进行总结，包括各类云资源调整、使用及服务情况，以及日常维护、应急值守、故障处置等情况。

投标人须每月对云资源使用情况向采购人提出调整建议，其中的云资源占用率较大的重点项目，投标人需支持提供任意时间区间的云资源使用情况，并提出调整建议。投标人在服务期内，应提供5*8小时全面覆盖工作日的高级售前咨询服务，满足用户提出的技术方案咨询类、部署架构类、技术测试类等专业性技术需求。投标人对政务云实施升级、优化等调整前，应向运行管理单位报送调整方案，待方案审核通过后实施；可能影响政务云使用部门信息系统正常运行的，投标人应提前告知政务云使用部门，并制定应急预案。

投标人制定服务内容及服务标准，为采购人提供包括日常运维管理服务、定期维护管理服务、应急演练管理服务和应急响应服务在内的基本运维管理服务。提供的服务总体上应满足业务需求，确保本合同包政务云平台安全、稳定、可靠

运行。对服务器、存储设备、安全设备及平台基础软件等基础设施环境提供运维服务，切实保障本合同包政务云平台基础设施环境安全、稳定、高效的运行。

实施项目完毕后，实行 7×24 小时运行维护和响应故障工作，负责本合同包政务云平台的软硬件健康检查、平台和网络安全。指派专职接口人，负责本合同包政务云平台的故障受理、处理、跟踪、结果汇报工作。中标人需提供专业的运维服务，确保本合同包政务云平台稳定高效运转，确保本合同包政务云的信息系统安全。

投标人应建立健全配套的制度标准。可提供基于自身平台的相关标准、办法及建议，如：政务云管理办法、运维运营制度、应急预案等。

投标人建立统一的运维服务体系，制定运维服务标准和规范，为云平台提供响应及时、安全可靠的运维保障服务。

1.2.6 保密要求

(1) 服务技术支持人员不得将掌握的客户设备信息未经客户许可泄露给其他人。

(2) 服务技术支持人员任何时候不得私自打开机房内客户设备。

(3) 服务技术支持人员任何时候不得私自拷贝、更改、删除客户服务器数据。

(4) 非工作需要，服务技术支持人员不得掌握非工作范围内设备的口令。

(5) 服务技术支持人员需签订服务保密协议，未经授权禁止进入机房。

(6) 服务技术支持人员需遵守国家有关的政策、法律、法规和制度。

(7) 服务技术支持人员需要按照工作规范进行工作，凡接收到的重大服务请求，需要经用户同意才做处理。

(8) 服务技术支持人员不得向外泄漏任何业务和相关数据。

(9) 服务技术支持人员不得向外泄漏任何保密的资料。

(10) 服务技术支持人员授权，仅授权必要人员访问特定系统，避免过度授权

(11) 投标方及其服务技术支持人员不得外泄用户提供的软件系统源代码及技术文档。

1.2.7 数据安全

投标人须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利将采购人数据及其他信息进行擅自修改或透漏给第三方。

存放在云平台上任何资料、软件、数据等知识产权归采购人所有，投标人无权复制、传播、转让、许可或提供他人使用这些资源，不能将云平台提供给采购人未书面授权的任何委办局使用，不能运行采购人未授权的任何业务系统，否则应承担相应责任。

投标人须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利将采购人数据及其他信息进行擅自修改或透漏给第三方。

投标人还应保障采购人的数据主权，数据不得出政务云。未经允许不得对政务云上的任何数据进行非法截取、加工、分析处理或提供给第三方机构。

投标人在未经过用户邮件、书面材料确认前提下，不能查看、修改、拷贝用户业务系统文件和数据；政务云内所有设备的维修、报废等处理须经过采购人审批，在采购人监督下执行。

对正式下线和报废设备的存储介质中的全部信息进行清除，保障其中的数据得到完全清除并不可恢复，保存相应记录。

投标人服务技术支持人员运维服务时，禁止携带手机、摄像等设备，禁止拍照或录音导致信息泄露，禁止携带外部存储设备，U 盘、移动硬盘等需经安全检查后方可使用，防止感染遭受病毒。

1.2.8 合规性要求

1.2.8.1 安全规范要求

采用的软件、硬件技术和方法应充分考虑安全性要求，建立适宜的安全管理保障机制。中标方应在服务各环节提供相应的安全保障措施。

投标人提供的云服务需要符合电子政务相关的各类法律、法规、标准及其他要求。并且按照有关规定和各级监管部门的要求进行动态整改。

投标人在合同期内提供的云平台须每年通过网络安全三级等保测评并向采购人提交测评报告。

投标人在合同期内提供的云平台须每年通过一次商用密码应用安全性评估并向采购人提交测评报告。

投标人做好云服务提供、云中心运行维护、安全保障及技术支撑等各项服务工作，确保运行在云平台上的应用系统和数据安全。

1.2.8.2 兼容与可扩展性要求

根据本次购买服务的特点，投标人提供的软硬件产品及服务须具有兼容性和可扩展性。如果投标产品在软硬件产品及服务出现兼容性问题，中标方必须在采购人规定的期限内予以协商解决。

1.2.8.3 知识产权

（1）投标人应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任和费用。

（2）投标人应保证在本项目中提供的产品和服务，采购方享有合法的使用权，如有法律纠纷由投标人负责。

1.2.9 重大事件保障

中标人应具备完善的系统服务保障体系，配备足够的技术人员，在重大节假日、重大活动及业务高峰期内加大运维保障力度，保证期间系统平稳运行。

1.3 采购包1：云服务内容及技术要求

标的名称：呼伦贝尔市本级政务云采购（政务混合云 A 云）

1.3.1 采购内容

本项目为呼伦贝尔市本级政务云服务 A 云采购，呼伦贝尔政务应用已部署在云上共计 22 个部门，50 个系统，90%以上资源为商用架构，为响应国家信创政策的要求，计划分两年，对已部署在 A 云上的业务系统进行政务系统国产化环境替换，并于 2027 年底前全面实现政务云应用全栈信创改造。A 云保持现有存量资源环境的基础上，按业务系统信创改造升级为以鲲鹏、飞腾等国产化 ARM 资源环境为主，C86 架构如海光、LoongArch64 架构如龙芯等资源环境为辅助，最终实现政务业务系统的全面国产化信创升级改造。

投标人需建设基础云资源、基础安全设施等平台，满足呼伦贝尔市本级政务业务存量系统承载需求，提供包括云主机服务、镜像服务、云安全服务、商用密码服务、AI 算力云服务、云硬盘服务、IP 带宽服务、网络服务、托管服务、数据库和中间件服务、设备租赁等相关服务内容。

1.3.2 云服务清单

序号	设备及软件名称	主要性能指标	数量总计	单价(万元/年)	单位
一	计算服务				
1.1	云主机服务				
1.1.1	云主机服务 1	2 核 4G	23	0.470000	台
1.1.2	云主机服务 2	2 核 8G	106	0.870000	台
1.1.3	云主机服务 3	4 核 4G	22	0.590000	台
1.1.4	云主机服务 4	4 核 8G	120	0.930000	台
1.1.5	云主机服务 5	4 核 16G	300	1.400000	台
1.1.6	云主机服务 6	8 核 8G	40	0.800000	台
1.1.7	云主机服务 7	8 核 16G	76	1.600000	台

1.1.8	云主机服务 8	8 核 32G	300	2.900000	台
1.1.9	云主机服务 9	8 核 64G	38	4.400000	台
1.1.10	云主机服务 10	16 核 64G	162	5.700000	台
1.1.11	云主机服务 11	16 核 32G	57	3.300000	台
1.1.12	云主机服务 12	32 核 64G	20	5.060000	台
1.1.13	云主机服务 13	32 核 128G	15	9.200000	台
1.1.14	云主机服务 14	GPU 云主机性能 16C64G-2 块 16GB-T4-100GB 系统盘	3	6.400000	台
1.1.15	镜像服务	镜像服务	330	0.280000	镜像
1.1.16	操作系统	国产化服务器操作系统	650	0.280000	镜像
1.2	裸金属服务				
1.2.1	二路基础机型-国产化	CPU: 国产化 CPU, 主频 2.5GHz, 双路, 每 CPU 核数 24 核; 内存: 配置 256GB; 硬盘: 480GB SSD 硬盘*2; 2*600GB 硬盘, 网口: 4 个千兆电口, 4 个万兆光口 (含模块); RAID: 支持硬件 Raid0/1/10/5/50/6/60 等模式, 支持 JBOD, 支持 Raid 启动。	18	2.660000	台
1.2.2	二路基础机型-国产化	CPU: 国产化 CPU, 主频 2.6GHz, 双路, 每 CPU 核数 32 核; 内存: 配置 256GB; 硬盘: 480GB SSD 硬盘*2; 网口: 4 个千兆电口, 2 个万兆光口 (含模块); RAID: 支持硬件 Raid0/1/10/5/50/6/60 等模式, 支持 JBOD, 支持 Raid 启动。	9	2.660000	台
二	存储服务				
2.1	云硬盘服务				
2.1.1	普通云硬盘服务	普通云硬盘	1200000	0.000800	GB
2.1.2	对象存储硬盘服务	对象存储 OBS	90	0.210000	TB
2.1.3	海量存储服务	海量数据存储服务	3	1.600000	TB
2.2	云备份服务				

2.2.1	云备份服务 1	云备份服务	4000	0.012000	GB
2.2.2	云备份服务 2	基础云备份服务	120	0.009000	GB
2.2.3	云备份服务 3	10TB	5	3.700000	TB
三	网络服务				
3.1	云负载均衡服务				
3.1.1	应用负载均衡 1	应用负载（基础型）	9	0.430000	实例
3.1.2	应用负载均衡 2	应用负载（标准型）	9	0.842000	实例
3.2	云网络				
3.2.1	带宽 IP 专线	运营商静态互联网 IP_GL	180	0.015000	条
3.2.2	带宽 IP 专线	运营商静态互联网 IP_GL	12	0.014400	条
3.2.3	带宽 IP 专线	运营商静态互联网带宽_GL	450	0.030000	Mbps
3.2.4	带宽 IP 专线	运营商静态互联网带宽_GL	1830	0.030000	Mbps
3.2.5	带宽 IP 专线	运营商电子政务外网专线-G	3	3.166666	条
3.2.6	带宽 IP 专线	运营商静态互联网带宽_GL	3315	0.030000	Mbps
四	云安全服务				
4.1	云防火墙				
4.1.1	云防火墙 1	2C2G-IPS	30	2.110000	台
4.1.2	云防火墙 2	2C4G-IPS	9	5.280000	台
4.2	云堡垒机服务				
4.2.1	云堡垒机服务 1	500 资产	34	1.380000	台
4.3	云日志审计服务				
4.3.1	云日志审计 1	日志审计（基础版）	30	3.900000	台
4.3.2	云日志审计 2	日志审计（专业版）	3	5.660000	台
4.4	VPN 接入服务				
4.4.1	VPN 服务 1	虚拟 VPN10 个	3	1.600000	账

1					户
4.4.2	VPN 服务 2	专属网络服务基于 VPN 接入	3	1.900000	带宽
4.5	云租户安全咨询及测评服务				
4.5.1	等级保护设计咨询及测评费用	云租户测评服务	10	6.000000	套
4.5.2	密码安全设计咨询及测评费用	云租户测评服务	10	4.000000	套
4.6	WAF 防护				
4.6.1	WAF 基础防护	WAF 基础版	30	3.200000	套
4.6.2	WAF 增强防护	WAF 增强版	25	5.270000	套
4.7	网页防篡改服务				
4.7.1	网页防篡改	网页防篡改标准版	1	2.003202	套
4.8	数据库审计服务				
4.8.1	数据库审计基础服务	数据库审计基础版	15	6.000000	套
4.8.2	数据库审计专业服务	数据库审计专业版	3	12.000000	套
4.9	安全管理平台				
4.9.1	安全管理中心	安全中心能力	116	0.500000	VM
4.9.2	安全管理中心	安全中心能力	157	0.700000	VM
4.1	密码资源池服务				
4.10.1	统一资源调度服务	统一密码服务调度系统主要实现应用鉴别、计算单元虚拟化、计算资源自适应、负载均衡、密钥安全分发、密钥同步等功能，同时能提供缓存能力。	3	3.880000	套
4.10.2	加解密服务	加解密服务可以实现数据的传输或存储机密性保护，业务系统根据实际需求，自主调用该服务实现数据基于国密算法的加解密过程	3	3.500000	套

4.10 .3	签名验签服务	签名验签服务是基于数字签名技术,可以实现人员身份真实性验证、数据完整性保护及操作行为不可否认性功能,业务系统根据实际业务需求,自主调用该服务实现签名验签的过程	3	3.500000	套
4.10 .4	HMAC 服务	HMAC 服务可以实现数据的传输或存储完整性保护,业务系统根据实际需求,自主调用该服务基于国密算法 HMAC-SM3 对数据计算校验值后进行保存,读取数据时进行校验值验证达到防止数据被篡改的效果	3	3.500000	套
4.10 .5	证书解析与认证服务	用于解决用户身份鉴别的需求,保证用户身份的真实性。证书解析与认证服务支持基于 SM2 的数字证书解析,支持多 CA 多证书链模式,支持对接 OCSP 认证服务器和 CRL 列表导入,实现用户证书的在线和离线认证。	3	3.500000	套
4.10 .6	数字信封服务	数字信封服务用于不同租户、不同业务系统进行数据交换时,通过数字信封技术,保证数据的机密性、完整性和数据来源的真实性。	3	3.500000	套
4.10 .7	时间戳服务	基于 NTP 授时技术,进行时间戳服务封装,为租户应用系统提供标准格式的时间戳签发和验证服务	3	3.360000	套
4.10 .8	统一身份认证服务	支持基于数字证书的高强度身份认证服务,用于通过证书验证后实现应用系统的单点登录功能;包括统一身份管理、统一身份认证、统一身份授权、统一审计等功能	3	3.360000	套
4.10 .9	国密 https 接入服务	采用基于国密算法的 SSL 协议,基于应用层 SSL 实现技术,为租户应用系统提供国密算法的 https 安全接入服务,结合客户端国密浏览器,实现安全的 https 访问,保证应用层数据传输安全。在提供国密算法 https 接入同时,在面向公众访问场景下,可同步提供基于 RSA2048 密	3	3.360000	套

		码算法的 https 访问服务，满足普通用户使用常规浏览器访问的需求。			
4.10.10	协同签名服务	协同签名服务用于解决移动端用户身份鉴别的需求。面向开放式移动终端无法外置密码硬件介质的场景，采用密钥分割和协同签名技术，保证用户私钥安全同时，解决移动端用户身份鉴别的需求。	3	3.360000	套
4.10.11	虚拟密码机	基于底层的硬件虚拟化技术生成的虚拟密码机，作为上层密码统一服务平台的计算资源，可以提供密钥生成、数据加解密、签名验签、HMAC 等运算能力。	3	4.500000	套
4.10.12	SSL VPN 服务	通过国密 VPN 产品实现云租户的互联网 SSL VPN 接入，提供支持国密算法的 SSL 隧道加密连接服务，保证接入的实体身份真实性，通信访问过程的机密性、完整性	3	0.002000	套
4.10.13	证书服务	基于 PKI 体系签发的数字证书可以为个人和设备提供身份证明，确保人员或者设备身份真实性；智能密码钥匙可以作为个人数字证书的载体，实现客户端与服务端之间基于数字证书的身份鉴别。	3	0.010000	套
4.10.14	国密浏览器服务	为用户提供国密浏览器软件使用授权服务	3	0.015000	个
4.10.15	数字证书服务	进行电子签章有效性的认证。	3	0.005000	个
五	机房及其他服务				
5.1	IDC 机柜服务				
5.1.1	机柜租赁服务 1	机柜租赁，42U，功率 3kW	25	3.500000	个
5.1.2	机柜租赁服务 2	机柜租赁，42U，功率 5kW	12	4.500000	个
5.2	IDC 机柜服务				
5.2.1	云加速	内容分发	12	0.100000	Mb
5.2.	运维服务	7*24 小时运维服务	6	25.800000	人

3					
5.2.3	多云互联专线	10G 专线链路	3	88.000000	条

1.3.3 技术要求

1.3.3.1 云管理平台总体要求

1、**平台稳定性**：为了保障云平台稳定可靠，平台组件和产品管理组件均采用容器部署架构。

2、**厂商运维能力**：云平台厂商具备专业的售后运维支持团队，提供远程专业级统一运维中心服务，具备 7*24 小时全生命周期管理能力。

3、**平台开放性**：云平台应提供统一的标准接口，包括但不限于虚拟化平台、运营管理平台、运维管理平台、服务产品等标准接口，具备与云监管部门和第三方平台对接的能力。

1.3.3.2 云主机服务

1) 支持批量创建云服务器的功能。

2) 支持为云服务器绑定弹性 IP，实现业务发布功能，支持随机或指定绑定弹性 IP，支持指定或批量创建 ip 地址。

3) 支持提供云服务器生命周期管理包括创建、删除、开机、关机、重启、镜像与磁盘管理、安全组与网络管理、弹性公网 IP 管理、规格变更等。

4) 支持云服务器热迁移，可将运行中的云服务器迁移到另一台宿主机上，期间云服务器上的服务不中断。

5) ▲反亲和性，支持物理机级别。将用户的同一云服务器组中的弹性云服务器尽量分散地创建在不同的主机上。提供官网截图或功能截图或承诺函，并加盖投标人公章。

6) ▲支持计算能力的水平弹性伸缩，可根据定时、周期或监控策略，增加或减少云服务器实例。提供官网截图或功能截图或承诺函，并加盖投标人公章。

7) 支持虚拟主机的快照备份、性能监测分析、异常告警、日志管理等功能。

8) 支持用户快速定位虚拟机功能，可以支持按照虚拟机名称、IP、ID、镜像名称、运行状态、实例类型名称等多种方式快速定位虚拟机。

9) 支持根据应用系统的性能需求，灵活调整相关资源虚拟机的配置，包括调整 vCPU 个数，内存大小，磁盘卷个数，扩展磁盘卷的容量等。

10) ▲支持根据实例创建镜像时，可以选择制作系统盘镜像、数据盘镜像，或者整机镜像。提供官网截图或功能截图或承诺函，并加盖投标人公章。

1.3.3.3 镜像服务

1) 公共镜像支持的操作系统版本包括：SUSE, Debian, OpenSUSE, Fedora, Ubuntu, EulerOS, CoreOS。

2) 支持镜像共享,用户可以通过镜像共享将私有镜像在同 Region 下多个租户间实现共享。

3) ▲支持镜像导入，支持导入的镜像格式：vhd, vmdk, qcow2, qcow, qed, vhdx, raw。提供官网截图或功能截图或承诺函，并加盖投标人公章。

4) 支持通过控制台或 API 方式完成镜像的自定义管理，轻松搞定镜像管理。

5) 支持镜像在系统后端可以加密存储。

6) 支持使用弹性云服务器携带其挂载的数据盘一起创建整机镜像。支持弹性云服务器开机制作整机镜像。

7) ▲支持镜像导出，支持从 console 导出 VMDK、VHD、QCOW2 和 ZVHD 格式的镜像，自主导出。提供官网截图或功能截图或承诺函，并加盖投标人公章。

8) ▲支持通过注册镜像操作，将外部镜像 ISO 文件注册为云平台的私有镜像，通过私有镜像可以创建客户业务主机。提供官网截图或功能截图或承诺函，并加盖投标人公章。

1.3.3.4 裸金属设备租赁服务

1) ▲支持使用用户的自定义镜像创建裸金属实例自主申请裸金属批量,可以配置虚拟专有云、子网、弹性公网 IP 及公网带宽。支持查看裸金属查看 CPU、内存、网络、磁盘等监控指标；能够实现裸金属生命周期管理，包括创建、关闭、重启、删除、更换操作系统等操作，其中关闭、重启和关闭应支持批量操作，以提升管理员效率。提供官网截图或功能截图或承诺函，并加盖投标人公章。

2) 用户可以根据不同场景的业务需求进行选择不同类型的物理服务器，实现快速部署和设备管理；除裸机本地硬盘之外，也可以支持云硬盘，实现与本云内的云硬盘对接。

1.3.3.5 AI算力云服务

- 1) 支持具有针对深度学习场景的加速型弹性云服务器。
- 2) 支持 AI 资源用户专属，支持 VPC、安全组隔离、主机安全，云磁盘、硬盘备份恢复等。
- 3) 支持提供云服务器生命周期管理包括创建、删除、开机、关机、重启、镜像与磁盘管理、安全组与网络管理、弹性公网 IP 管理、规格变更等。
- 4) 支持虚拟主机的快照备份、性能监测分析、异常告警、日志管理等功能。
- 5) 支持用户快速定位虚拟机功能，可以支持按照虚拟机名称、IP、ID、镜像名称、运行状态、实例类型名称等多种方式快速定位虚拟机。

1.3.3.6 云硬盘服务

- 1) ▲支持云盘在线扩容，保障业务不中断。提供官网截图或功能截图或承诺函，并加盖投标人公章。
- 2) 支持块存储、对象存储、文件存储等存储类型。
- 3) 支持每个云硬盘存储均需要有 3 份分布于不同机架的副本，保证数据安全可靠。
- 4) 支持对云硬盘资源进行周期性全量备份，增强备份副本可靠性。
- 5) ▲支持系统盘和数据盘加密。提供官网截图或功能截图或承诺函，并加盖投标人公章。
- 6) ▲为了防止误删除数据，支持回收站功能，放入回收站的云盘可以在有效期内恢复该云盘数据。提供官网截图或功能截图或承诺函，并加盖投标人公章。

1.3.3.7 数据库和中间件服务

- 1) 支持提供多种实例类型，满足客户多种场景业务。
- 2) 支持通过安全组限制源端 IP 对文档数据库的访问权限，可以细化到端口。
- 3) 支持添加/删除/修改标签，并且为各个实例打上标签，支持通过标签筛选实例。
- 4) 支持对运行正常的主实例创建手动备份，用户可以通过手动备份恢复数据，从而保证数据可靠性。
- 5) 支持切换主备实例的可用性策略，以满足不同业务需求。可选择“可靠性优先”或者“可用性优先”两种策略。

6) 支持存量实例修改安全组，根据部署情况的变化配置网络访问控制。

7) 支持可以通过慢日志的日志明细、统计分析情况，查找出执行效率低的语句，进行优化。也可以下载慢日志进行业务分析。降低用户运维难度，提升体验感。

1.3.3.8 IP带宽服务

1) 支持与云服务器、裸金属服务器、NAT 网关灵活的绑定与解绑，带宽支持灵活调整。

2) 支持接入多家运营商带宽，按要求提供 IP 数量和带宽大小。

1.3.3.9 网络服务

1) 提供网络虚拟化功能，实现集中化网络控制和按需管理，具备弹性扩展能力，支持自动化网络部署。

2) 云平台应划分独立的业务网络、存储网络、服务产品管理调度网络、宿主机运维网络、物理节点带外管理网络等，不同网络之间逻辑隔离；业务网络和存储网络采用万兆冗余链路。

3) 支持网络拓扑管理功能，通过拓扑自定义网络结构，创建网络和虚拟机实例。

4) ▲ACL 规则支持 IP 地址组。提供官网截图或功能截图或承诺函，并加盖投标人公章。

5) 支持设置安全组，安全组规则支持配置优先级。

1.3.3.10 容灾备份服务

1) 为防止数据库误操作、关键文件误删除等操作导致业务系统崩溃，为用户提供备份上云和备份容灾服务以及文件、数据库等细颗粒度备份服务。

2) ▲支持整机崩溃一致性备份。提供官网截图或功能截图或承诺函，并加盖投标人公章。

3) 支持将备份数据跨租户共享，可以将数据快速复制给其他用户。

4) ▲支持周期性全量备份，增强备份数据可靠性。提供官网截图或功能截图或承诺函，并加盖投标人公章。

5) 勒索病毒攻击后还有可用的备份副本。

1.3.3.11 云WAF服务

1) 支持对 OWASP Top 攻击进行安全防护，支持包括 XSS、SQL 注入、命令注

入、代码注入、远程溢出攻击、Webshell 检测（上传木马）等。

2) ▲支持 CC 防御，支持基于 IP/Cookie/Referer 的源和目的限速，限速的防护动作至少要支持设置验证码、动态阻断 IP/用户一段时间，限速的响应页面支持用户自定义。提供第三方佐证材料(提供官网截图, 或功能截图，或承诺函)。

3) 提供扫描器行为统计防护功能，可根据敏感 URL 访问统计、告警统计等多种统计方法，判定扫描器攻击行为，支持相关阈值配置。

4) ▲支持返回页面的敏感信息防泄漏，例如将返回页面的身份证号码、电话号码、电子邮箱等进行匿名化。提供官网截图或功能截图或承诺函，并加盖投标人公章。

5) 支持访问审计功能，能够记录、查询所有用户对网站的访问情况。

1.3.3.12 云主机安全服务

1) 产品提供防御病毒、木马、间谍程序、后门程序等恶意代码功能，可根据不同的病毒类型采取不同的处理策略，包括清除、删除、拒绝访问、不予处理、隔离恶意程序等。

2) ▲支持口令复杂度策略检测，并使用弱口令字典对系统/应用帐户进行扫描，检测出弱口令后展示弱口令存在时长并提示用户修改，弱口令字典支持自定义。提供官网截图或功能截图或承诺函，并加盖投标人公章。

3) 支持检测口令破解攻击，可对识别出的攻击源 IP 封锁 24 小时，禁止其再次登录，防止主机因账户破解被入侵。

4) 支持清点并展示主机账号权限、所属用户组、用户目录、启动 Shell 等信息；支持清点并展示进程路径、启动参数、文件权限、文件 HASH、开放端口、软件版本等信息。

5) 支持基于特征病毒检测引擎进行服务器病毒文件的扫描，覆盖活动进程、隐藏进程、内核模块、已安装程序、动态库劫持、计划任务、开机自启动项、敏感目录、office 文件、图片、视频、执行脚本、压缩包等系统薄弱模块。

1.3.3.13 数据库审计服务

1) 支持旁路模式数据库审计功能，支持实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。

2) 支持实时审计用户对主流数据库系统所有操作（插入、删除、更新、用

户自定义操作等), 还原操作信息包括会话 ID、数据库实例、数据库类型、数据库用户、客户端 MAC 地址、数据库 MAC 地址、客户端 IP、数据库 IP、客户端端口、数据库端口、客户端名称、操作类型、操作对象类型、响应结果、影响行数、开始时间、响应结束时间、SQL 请求语句、请求结果等字段。

3) 支持展示会话的终端信息、会话的主机信息、会话的其它信息、操作信息等。

4) ▲支持审计常见数据库。提供官网截图或功能截图或承诺函, 并加盖投标人公章。

1.3.3.14 云堡垒机服务

1) ▲支持手机令牌、手机短信、USBKey、动态令牌等多因子认证形式。支持 AD 域、RADIUS、LDAP、Azure AD 用户账号远程认证。提供官网截图或功能截图或承诺函, 并加盖投标人公章

2) 支持第三方客户端运维, 包括 SecureCRT、Xshell、Xftp、WinSCP、Navicat、Toad for Oracle 等工具。

3) ▲支持一键登录多个授权资源, 多个资源可同时在一个浏览器页签运维, 开启群发键, 能够对多个资源访问同步命令输入。提供官网截图或功能截图或承诺函, 并加盖投标人公章

4) 支持命令执行记录留存, 以列表的形式展示详细的命令执行记录。

5) 支持日志管理, 涵盖登录/登出日志、文件管理日志、操作日志、密码更改日志、文件下载日志、系统状态日志、告警日志。

1.3.3.15 日志审计服务

1) 支持通过关键字、条件表达式、时间范围进行快速检索、筛选、过滤, 同时支持 SQL 语句快速检索。

2) ▲支持日志完整保留 180 天, 满足等保审计对保留时长的要求。提供官网截图或功能截图或承诺函, 并加盖投标人公章

3) 支持以图表方式(饼图、柱图、曲线图)显示当日日志数据分布情况。

4) 支持多种方式的查询检索, 包括: 告警日志检索、全文检索、日志分类检索。

5) 支持采集日志、告警、漏洞等安全数据, 对安全数据可自动化租户和资

源标识，方便按照租户维度进行审计和分析。

1.3.3.16 漏洞扫描服务

1) 支持 Web 应用漏洞扫描能力，支持扫描使用 Ajax、JavaScript、Flash 等技术构建的网站，支持扫描使用 Tomcat、Apache、Nginx、IIS 等 Web 容器部署的网站支持；支持 HTTP 和 HTTPS 协议的扫描。

2) 支持资产分组管理能力，支持自定义分组，可按照分组批量快速启动扫描。

3) 支持操作系统漏洞扫描，支持 RedHat、openSUSE15、SUSE、UOS V20、HCE2.0、EulerOS、KylinOS、Debian、Ubuntu、Windows Server。

4) ▲支持检查主机弱密码，主机弱密码字典不低于 12 种。提供官网截图或功能截图或承诺函，并加盖投标人公章。

5) 支持 SSH、Telnet、FTP、MySQL、PostgreSQL、Redis、SMB、WinRM、Mongo，memcached、SQL Server、SFTP 等常见协议、中间件的弱口令检测。

1.3.3.17 云防火墙服务

1) ▲支持基于源 MAC、源端口、目的端口、时间、域名、URL 等多个元素进行访问控制，并可针对该策略进行最大并发连接数和长连接的限制（支持 IPv4/IPv6）。提供官网截图或功能截图或承诺函，并加盖投标人公章。

2) 支持基于域名/泛域名的访问控制，添加域名组支持 URL 过滤和地址解析两种类型。

3) ▲具备 WEB 攻击防护能力，支持 SQL 注入攻击防护、XSS 攻击防护，对常见的 Web 服务器环境 Web 入侵的脚本攻击工具（websHELL）的拦截，包含 ASPX、ASP、PHP、JSP 等。提供官网截图或功能截图或承诺函，并加盖投标人公章。

4) 支持提供 AI 入侵防御引擎对恶意流量实时检测和拦截，防御木马蠕虫、注入攻击、漏洞扫描、网络钓鱼、暴力破解等攻击。

5) 支持互联网到业务的访问流量分析，包括互联网出入口流量、攻击趋势以及 TOP 访问 IP 等。

1.3.3.18 商用密码应用服务

按需提供加解密服务、完整性校验服务、签名验签服务、时间戳服务、密钥管理服务、数据库加密服务、SSL 安全网关-安全接入、SSL 安全网关-https 安

全负载、国密浏览器、手机盾签名验签、USB Key、应用密码改造咨询及指导。

1.3.3.19 机柜服务

1) 须保证用户租用的服务器设备可持续获得冷源供应，机房运行环境恒温恒湿：温度为 $23\pm1^{\circ}\text{C}$ ，相对湿度保持在 40%~55%；机柜采用精确送风方式；空调系统采取 N+1 冗余备份方式设置，无单点故障；具备专业空调维护队伍；对机房温湿度有监控措施和记录。

2) 提供满足本次政务云服务运行承载的机柜空间，每个机柜须满足双路供电，机房空间和供电在满足建设规模基础上，具备适合业务扩展的扩展能力。

1.3.3.20 托管设备技术要求

按照 U 数提供托管服务，并对托管设备提供基础网络配置及故障排查、硬件巡检服务、7x24 值守服务。

1.3.3.21 云主机服务器硬件技术要求

1. CPU \geq 2 颗 26Core CPU；主频 \geq 2.6GHz；
2. 内存 \geq 12*64GB 内存；
3. 系统盘 \geq 480G SSD；
4. 网卡 \geq 2* 25GE 光口以太网卡；

1.3.3.22 存储设备硬件技术要求

1. \geq 2 颗 12Core CPU；主频 \geq 2.4GHz；
2. 内存 \geq 4*32GB；
3. 系统盘 \geq 480G； \geq 4*3.2TB SSD； \geq 12*16TB-SATA；
4. 2* 25GE 光口以太网卡；

1.3.3.23 网络安全设备技术要求

防火墙：吞吐量 \geq 20Gbps；IPSec 吞吐量 \geq 15Gbit/s；并发连接数 \geq 800 万；新建连接数 \geq 30 万/秒；支持入侵防御(IPS)、防病毒(AV)、数据防泄漏(DLP)、上网行为管理/审计。

交换机： \geq 24*10GE SFP+接口； \geq 4*40GE QSFP+接口； \geq 2*交流电源； \geq 2*风扇模块。

1.4 采购包2：云服务内容及技术要求

标的名称：呼伦贝尔市本级政务云采购（全栈信创云 B 云）

1.4.1 采购内容

为引入竞争机制，提升政务云整体服务质量，降低服务采购成本，同时积极响应国家信创政策，同步引入一家全栈信创云服务商，提供全栈国产化信创环境和服务；B 云以当前技术环境下，从技术架构兼容性、迁移成本、应用适配性更优的国产 C86 架构资源环境为主，以鲲鹏、飞腾等 ARM 资源环境为辅助，以承载呼伦贝尔市本级行政部门新增业务系统的上云需求。根据呼伦贝尔政务系统上云 3 年规划调研结果，拟将自 B 云运营后的新上线政务系统，以及 2026 年规划的政务一体化大数据平台等部署在 B 云，同时承载部分 A 云现有业务系统国产化改造，将改造适配难度低，对 C86 国产化环境适配更优的业务系统迁移至 B 云。

1.4.2 云服务清单

序号	设备及软件名称	主要性能指标	数量	单价（万元）	单位
一	计算服务				
1.1	国产化 C86 架构云主机服务				
1.1.1	云主机服务 1	国产 C86 架构，2 核 4G	24	0.420000	台
1.1.2	云主机服务 2	国产 C86 架构，2 核 8G	72	0.720000	台
1.1.3	云主机服务 3	国产 C86 架构，4 核 4G	12	0.528000	台
1.1.4	云主机服务 4	国产 C86 架构，4 核 8G	60	0.828000	台
1.1.5	云主机服务 5	国产 C86 架构，4 核 16G	144	1.440000	台
1.1.6	云主机服	国产 C86 架构，8 核 16G	48	1.656000	台

	务 7				
1.1.7	云主机服务 8	国产 C86 架构，8 核 32G	144	2.880000	台
1.1.8	云主机服务 9	国产 C86 架构，8 核 64G	12	4.812000	台
1.1.9	云主机服务 10	国产 C86 架构，16 核 32G	48	3.312000	台
1.1.10	云主机服务 11	国产 C86 架构，16 核 64G	12	5.196000	台
1.1.11	云主机服务 12	国产 C86 架构，32 核 64G	12	5.976000	台
1.1.12	云主机服务 13	国产 C86 架构，32 核 128G	12	9.516000	台
1.2					
1.2.1	二路国产化基础机型	CPU: 国产架构 CPU, 主频 2.7GHz, 双路, 每 CPU 核数 64 核; 内存: 配置 256GB; 硬盘: 480GB SSD 硬盘*2; 4*3.84TB SSD 硬盘网口: 4 个千兆电口, 2 个万兆光口 (含模块); RAID: 支持硬件 Raid0/1/10/5/50/6/60 等模式, 支持 JBOD, 支持 Raid 启动。	6	6.720000	台
1.2.2	二路国产化架构基础机型	CPU: 国产架构 CPU, 主频 2.7GHz, 双路, 每 CPU 核数 64 核; 内存: 配置 512GB; 硬盘: 480GB SSD 硬盘*2; 网口: 4 个千兆电口, 2 个万兆光口 (含模块); RAID: 支持硬件 Raid0/1/10/5/50/6/60 等模式, 支持 JBOD, 支持 Raid 启动。	3	6.720000	台
二	存储服务				
2.1	云硬盘服务				
2.1.1	普通云硬盘服务	云硬盘服务 1GB	606550	0.000700	GB
2.1.2	文件存储服务	NAS 存储服务 1TB	600	0.570000	TB
2.2	云备份服务				

2.2.1	云备份服务 1	定时备份服务 1TB	300	0.680000	TB
三	网络服务				
3.1	云负载均衡服务				
3.1.1	应用负载均衡 1	应用负载均衡	22	0.430000	实例
3.2	云网络				
3.2.1	云网络 1	互联网带宽	1400	0.014400	Mb
3.2.2	云网络 2	互联网 ip	110	0.022000	个
四	云安全服务				
4.1	云防火墙				
4.1.1	云防火墙 1	云防火墙（基础版）	30	3.300000	台
4.2	云堡垒机服务				
4.2.2	云堡垒机服务	管理不低于 50 点资产	30	2.000000	台
4.3	云日志审计服务				
4.3.1	云日志审计 1	日志审计（基础版）	30	3.300000	台
4.4	VPN 接入服务				
4.4.1	VPN 服务 1	SSLVPN	30	0.037500	账户
4.4.2	VPN 服务 2	IPSEC VPN	30	0.013500	带宽
4.5	云 DDOS 防护服务				
4.5.1	DDOS 防护 1	DDoS 增强型	6	7.700000	套

4.6	WEB 网站实时防护服务				
4.6.1	WEB 网站基础防护	WEB 防护（基础版）	30	2.600000	套
4.7	WAF 防护				
4.7.1	WAF 基础防护	WAF（基础版）	30	2.600000	套
4.8	网页防篡改服务				
4.8.1	网页防篡改	网页防篡改	30	4.500000	套
4.9	数据库审计服务				
4.9.1	数据库审计基础服务	数据库审计（基础版）	30	3.100000	套
4.10	密码资源池服务				
4.10.1	统一资源调度服务	统一密码服务调度系统主要实现应用鉴别、计算单元虚拟化、计算资源自适应、负载均衡、密钥安全分发、密钥同步等功能,同时能提供缓存能力。	12	3.880000	套
4.10.2	加解密服务	加解密服务可以实现数据的传输或存储机密性保护,业务系统根据实际需求,自主调用该服务实现数据基于国密算法的加解密过程	12	3.500000	套

4.10.3	签名验签服务	签名验签服务是基于数字签名技术，可以实现人员身份真实性验证、数据完整性保护及操作行为不可否认性功能，业务系统根据实际业务需求，自主调用该服务实现签名验签的过程	12	3.500000	套
4.10.4	HMAC服务	HMAC服务可以实现数据的传输或存储完整性保护，业务系统根据实际需求，自主调用该服务基于国密算法HMAC-SM3对数据计算校验值后进行保存，读取数据时进行校验值验证达到防止数据被篡改的效果	12	3.500000	套
4.10.5	证书解析与认证服务	用于解决用户身份鉴别的需求，保证用户身份的真实性。证书解析与认证服务支持基于SM2的数字证书解析，支持多CA多证书链模式，支持对接OCSP认证服务器和CRL列表导入，实现用户证书的在线和离线认证。	12	3.500000	套
4.10.6	数字信封服务	数字信封服务用于不同租户、不同业务系统进行数据交换时，通过数字信封技术，保证数据的机密性、完整性和数据来源的真实性。	12	3.500000	套
4.10.7	时间戳服务	基于NTP授时技术，进行时间戳服务封装，为租户应用系统提供标准格式的时间戳签发和验证服务	12	3.360000	套
4.10.8	统一身份认证服务	支持基于数字证书的高强度身份认证服务，用于通过证书验证后实现应用系统的单点登录功能服务；包括统一身份管理、统一身份认证、统一身份授权、统一审计等功能	12	3.360000	套
4.10.9	国密https接入服务	采用基于国密算法的SSL协议，基于应用层SSL实现技术，为租户应用系统提供国密算法的https安全接入服务，结合客户端国密浏览器，实现安全的https访问，保证应用层数据传输安全。在提供国密算法https接入同时，在面向公众访问场景下，可同步提供基于RSA2048密码算法的https访问服务，满足普通用户使用常规浏览器访问的需求。	12	3.360000	套
4.10.10	协同签名服务	协同签名服务用于解决移动端用户身份鉴别的需求。面向开放式移动终端无法外置密码硬件介质的场景，采用密钥分割和协同签名技术，保证用户私钥安全同时，解决移动端用户身份	12	3.360000	套

		鉴别的需求。			
4.10.11	虚拟密码机	基于底层的硬件虚拟化技术生成的虚拟密码机，作为上层密码统一服务平台的计算资源，可以提供密钥生成、数据加解密、签名验签、HMAC 等运算能力。	12	4.500000	套
4.10.12	SSL VPN 服务	通过国密 VPN 产品实现云租户的互联网 SSL VPN 接入，提供支持国密算法的 SSL 隧道加密连接服务，保证接入的实体身份真实性，通信访问过程的机密性、完整性	9	0.005000	套
4.10.13	证书服务	基于 PKI 体系签发的数字证书可以为个人和设备提供身份证明，确保人员或者设备身份真实性；智能密码钥匙可以作为个人数字证书的载体，实现客户端与服务端之间基于数字证书的身份鉴别。	12	0.010000	套
4.10.14	国密浏览器服务	为用户提供国密浏览器软件使用授权服务	220	0.015000	个
4.10.15	数字证书服务	进行电子签章有效性的认证。	220	0.005000	个
4.11	云租户安全咨询及测评服务				
4.11.1	等级保护设计咨询及测评费用	云租户测评服务	15	6.000000	套
4.11.2	密码安全设计咨询及测	云租户测评服务	15	4.000000	套

	评费用				
五	数据库服务				
5.1	国产化数据库	企业版	16	11.362900	套
5.2	分布式数据库	1核/月/台	1000	0.050000	套
5.3	分布式数据库	2GB/月/台	3072	0.016300	套
六	操作系统服务				
6.1	操作系统	国产操作系统，提供主流国产操作系统统信 V20、麒麟 V10 的租用、安装、技术支持服务。	520	0.500000	套
七	中间件服务				
7.1	国产化中间件	具备 Web 应用、EJB 应用、虚拟主机、应用服务器集群、身份认证、日志审计等基础工作，提供类库管理、集成环境管理、图形化监控、配置、垃圾回收配置等功能，支持实例部署、数据库连接服务，为业务系统提供运行环境。	17	2.410000	套
八	大数据服务				
8.1	大数据服务	提供离线数据进行存储与计算。包括：运维与监控管理、用户与权限管理、多集群管理、日志管理、集群高可用、集群容灾备份、数据存储服务、离线计算引擎、流式计算引擎、NoSQL 数据库、全文检索数据库、Redis 内存数据库、Kafka 消息队列	31	3.600000	套
九	机房及其他服务				
9.1	IDC 机柜服务				
9.1.1	机柜租赁服务 1	机柜租赁，42U，功率 3kW	6	3.500000	个
9.1.2	机柜租赁服务 2	机柜租赁，42U，功率 5kW	6	4.500000	个

9.2	IDC 机柜服务				
9.2.1	云加速	内容分发	3	0.080000	Mb
9.2.2	IDC 专线	带宽 1G 专线	3	3.100000	条
9.2.3	运维服务	7*24 小时运维服务/年	3	26.000000	人
9.2.4	多云互联专线	10G 专线链路	3	88.000000	条
9.3	硬件设备租赁服务				
9.3.1	4G 吞吐防火墙	国产化防火墙产品，采用国产化 CPU，支持 15 个千兆电接口，6 个千兆光接口，2 个万兆光接口，3 个 Combo 电接口，2 个扩展槽位；1TB 硬盘；IPS/AV/URL 组合特征库升级服务；	6	1.400000	台
9.3.2	10G 吞吐防火墙	国产化防火墙产品，采用国产化 CPU，5GE+4SFP，2 个接口扩展槽位灵活扩展，1TB 硬盘；IPS/AV/URL 组合特征库升级服务；	6	4.000000	台
9.3.3	20G 吞吐防火墙	国产化防火墙产品，采用国产化 CPU，5GE+4SFP，2 个接口扩展槽位灵活扩展，1TB 硬盘；IPS/AV/URL 组合特征库升级服务；	6	5.000000	台
9.3.4	堡垒机	国产化堡垒机，采用国产化 CPU 硬件 2U 硬件架构，16GB 内存，4TB 硬盘容量，标准配置 6 个以太网千兆电口、4 个以太网千兆光口，支持 2 个接口扩展槽位，支持太网千兆或万兆接口扩展能力；为用户提供了全面的运维管理体系和运维能力，保障运维过程的安全 图形会话并发数：200 字符会话并发数：700 可管理资产数：300 6*GE 电口、4*GE 光口，2 个接口卡扩展槽	6	4.000000	台

9.3.5	网闸	国产化网闸，采用国产化 CPU 吞吐性能：900Mbps 系统整体时延：1ms 并发连接数 80W 固化接口形态及插槽：内网 6 电+4 千兆光，1 串口，外网 6 电+4 千兆光+1 串口，2 USB，1 液晶屏	6	3.500000	台
9.3.6	日志审计	国产化日志审计，采用国产化 CPU 2U 高机架式硬件架构，CPU：8 核；内存：16G，硬盘：标配 4T 3.5 寸 SATA 盘；接口 2*GE（电）：4 个扩展槽，可选配不少于（4*GE 电+4*GE 光）/8*GE 电/8*GE 光/4*10GE，电源标配：2*350W 事件入库性能 3500EPS. 支持 32 个日志源	6	1.600000	台
9.3.7	数据库审计	国产化数据库审计，采用国产化 CPU SQL 平均处理性能：5Wqps，SQL 峰值处理性能：6Wqps 入库速度：6Wqps，日志存储数量：40 亿条 吞吐：600Mbps，2 电口+4 扩展槽 支持 Oracle、MySQL、SQLServer、DB2、Sybase、Informix 等主流数据库协议的解析。支持 SQLServer2005 及以上版本的加密数据库账号的解析，支持达梦、人大金仓、神通、高斯 DB、南大通用等国产数据库协议的解析，支持 PostgreSQL、Greenplum、Cache 等专用数据库协议的解析，支持主流大数据平台数据库/NoSQL 库的解析与审计，包括 HBase、Hive、MongoDB、Elasticsearch、Redis 等	6	3.400000	台
9.3.8	WEB 应用防护	国产化 WEB 应用防护，采用国产化 CPU 吞吐性能：1.5G 新建连接数：4W 并发连接数：60W 5*GE 电口，支持 BYPASS，4*GE 光口，支持扩展插槽 支持网页防篡改，支持 Web 攻击防护功能，包括命令注入攻击，组件漏洞防护、Web 扫描防护、XPath 注入防护、XML 注入防护、SSI 注入防护、JOSN 注入防护、LDAP 注入防护、webshe11	6	3.600000	台

		防护			
9.3.9	路由器	国产化路由器，采用国产化 CPU 双主控、冗余电源 交换容量：670Gbps，包转发率： 360Mpps 16*10GE (SFP+)，16*GE (RJ45)+4*25GE 光接口	6	1.900000	台
9.3.10	漏洞扫描	国产化产品，采用国产化 CPU，系统 漏扫&数据库&基线漏扫最大并发扫描 IP 总数：60 系统漏扫&数据库&基线漏扫最大并发 扫描任务数：6 Web 漏扫最大并发扫描站点数：5 口令猜解并发：4 4*GE 电口，4*GE 光口，支持扩展插槽 支持国产操作系统、数据库的扫描， 国产操作系统包含中标麒麟、凝思、 华为欧拉、深度、红旗、中兴新支点， 国产数据库包括神通、人大金仓、南 大通用、达梦。	6	4.300000	台
9.3.11	入侵防御	国产化入侵防御，采用国产化 CPU 吞吐性能：网络层 15G、全威胁 5G 新建连接数：10 万/秒 并发连接数：500 万 配置 5*GE，支持 Bypass、4*SFP 光口， 2 个接口扩展槽位	6	4.800000	台
9.3.12	24 口 千兆 电接 入交 换机	国产化交换机，采用国产化 CPU，配 置 28 个 10/100/1000BASE-T 端口，8 个 1G/10G BASE-X SFP Plus 端口；	6	0.260000	台
9.3.13	48 口 千兆 电接 入交 换机	国产化交换机，采用国产化 CPU，配 置 48 个 10/100/1000BASE-T 电口，6 个 1G/10G BASE-X SFP Plus 端口	6	0.340000	台
9.3.14	48 端 口万	国产化交换机，采用国产化 CPU，配 置 48 个 1/10G SFP Plus 端口，2 个	6	2.450000	台

	兆交换机	QSFP 端口，4 个 100G QSFP28 端口，双电源；支持 TAP 功能			
9.3.15	48 千兆光交换机	国产化交换机，采用国产化 CPU，配置 48 个 100/1000Base-X SFP 端口，4 个 1G/10GBase-X SFP Plus 端口，支持 1 个扩展槽位，冗余电源及风扇模块	6	1.500000	台
十	智算服务				
10.1.1	人工智能大语言模型服务	支持基于大语言模型（如 DeepSeek、Qwen、LLaMA 等）的文字处理。模型参数 500B	30000	0.004000	Tokens
10.1.2	人工智能大语言模型服务	支持基于大语言模型（如 DeepSeek、Qwen、LLaMA 等）的文字处理。模型参数 30B	30000	0.003000	Tokens
10.1.3	大模型 DS 满血 GPU 服务器租赁服务	支持 Deepseek 671B 满血 1、配置 2 颗国产化 CPU（2.6GHz/48 核）； 2、16*64G DDR5 内存； 3、4*3.84T SSD 硬盘，2*960G SSD 硬盘； 4、8 块国产化昆仑芯 P800 GPU 卡模组（单卡 96GB 显存）； 5、2 个 25G 光口（含 25G 光模块）； 6、冗余电源、风扇，滑轨；	2	40.000000	台

1.4.3 技术要求

★投标人承诺本次项目所有投入使用的硬件设备为新出厂设备，且出厂日期不早于本项目合同签约日期前 3 个月，并提供承诺函（格式自拟）。

1.4.3.1 云管理平台总体要求

1、平台稳定性：

为了保障云平台稳定可靠，平台组件和产品管理组件均采用容器部署架构。

▲为了保障云平台安全可靠，要求云平台采用国产自研架构，非基于OpenStack 开源架构开发，拥有自主知识产权。提供厂商承诺函并加盖厂商公章。

▲云平台管理集群具备高可用机制，对云平台管理集群其中一个节点进行掉电/关机或重启操作，不影响云平台业务的正常运行；云管平台全部宕机或版本升级，都不会影响业务转发面正常运行。提供厂商承诺函并加盖厂商公章。

▲云平台管理集群多 AZ 集群高可用部署方案及多 Region 容灾机制，实现在多 AZ、多 Region 场景下的管理平台高可用部署方案，在云管宕机后，能够在另外一个 AZ/Region 及时拉起云管平台，不影响云管平台正常运行。提供厂商承诺函并加盖厂商公章。

2、厂商运维能力：

云平台厂商具备专业的售后运维支持团队，提供远程专业级统一运维中心服务，具备 7*24 小时全生命周期管理能力。

▲云平台具备资源的闲置/瓶颈分析能力，可分别列出当前闲置或瓶颈的资源信息，支持默认判定算法，也支持自定义设置资源指标监控项、监控判定阈值，监控判定时长等判定条件。提供功能截图和供厂商承诺函并加盖厂商公章。

▲运管平台支持计算视角、存储视角、网络视角等不同维度的拓扑图展示能力，支持展示全网服务器、交换机、防火墙等物理设备状态、监控、告警信息，能够展示计算集群主机和虚拟机关系图、存储拓扑云硬盘挂载关系图、网络设备连接关系图等。提供功能截图并加盖厂商公章。

▲支持 Overlay 网络流量监控与分析能力，流量分析提供了对云内 VPC 网络流量的详细分析，包括服务分析，展示服务端 IP 及其流量分布流统计；展示 IP 之间的互访关系；异常会话统计，展示源 IP 端口到目的 IP 端口的异常连接列表等能力。提供功能截图并加盖厂商公章。

3、平台开放性：云平台应提供统一的标准接口，包含但不限于虚拟化平台、运营管理平台、运维管理平台、服务产品等标准接口，具备与云监管部门和第三方平台对接的能力。

4、平台兼容型：▲云平台管理服务器支持分别基于鲲鹏、飞腾、海光 CPU 部署，计算节点支持基于鲲鹏、飞腾、海光 CPU 部署。

1.4.3.2 云主机服务

1. 用户可以通过管理控制台批量申请云主机。支持多种规格的云主机类型，包括通用型、计算型、内存型、高主频、本地盘型、GPU 型等。申请云主机时可以定义所需操作系统类型、镜像、云主机规格、数据盘规格。可自定义云主机网卡 IP 及安全组，云主机支持配置 IPv6、IPv4 或双栈网络，支持为存量 IPv4 云主机补充下发 IPv6 地址。可以为云主机选择自定义密码、随机密码或密钥对登录。
2. 支持云主机生命周期管理，用户申请云主机后，可以通过管理平台对云主机执行开机、关机、重启、删除、远程登录、整机快照、重置密码、克隆、挂载光驱等；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；也可以根据云主机实例名称、实例 ID、公网 IP、私网 IP、标签、运行状态以及操作系统等快速查找、过滤云主机。
3. ▲具备弹性扩展能力，可以对虚拟机 CPU、内存、硬盘进行热添加。为提高性能、业务连续性，需同时满足 DPDK 加速、支持 DPDK 虚拟机热添加。提供厂商承诺函并加盖厂商公章。
4. ▲支持云主机 HA。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。支持 Web 页面配置 HA 功能的开启和关闭。提供厂商承诺函并加盖厂商公章。
5. ▲支持将已创建虚拟机加入启动集，启动集支持强制反亲和性和非强制反亲和性策略。提供厂商承诺函并加盖厂商公章。
6. 云主机支持标签管理，可以为云主机添加一个或多个标签，并通过标签筛选虚拟机，支持不同的角色分别管理云主机标签。
7. 支持云主机迁移，实现计算资源、存储资源的迁移；支持云主机热迁移，可在不同代 CPU 资源池中进行云主机热迁移；支持云主机在宿主机不关机状态下进行冷迁移；支持界面化执行迁移操作，支持迁移到由用户指定的目标可用区和主机。
8. ▲云平台支持在虚拟机创建时，配置虚拟机启动后自动运行的脚本。提供功能截图和厂商承诺函并加盖厂商公章。

1.4.3.3 镜像服务

1. ▲虚拟机镜像支持除了支持公共镜像、私有镜像以外，还支持共享镜像方式，即用户可以将自己的私有镜像共享给其他特定的用户使用。支持自定义镜像，以公有镜像为模板，创建定制镜像。提供厂商承诺函并加盖厂商公章。
2. ▲虚拟机和裸金属镜像服务应支持业界主流操作系统的版本(64 位)及后续新版本，包括 ubuntu14 及以上版本、Debian，麒麟，UOS 等。提供功能截图和厂商承诺函并加盖厂商公章。
3. 支持镜像管理，可以查看镜像基本信息，包括镜像名称、操作系统、适用主机类型（虚拟化/非虚拟化）、镜像大小、磁盘容量等；支持镜像双可用区同步和跨可用区部署。
4. ▲私有镜像双 AZ 同步，跨 AZ 部署。提供厂商承诺函并加盖厂商公章
5. ▲云平台支持不同账号共享镜像，租户创建自定义镜像，可将虚拟机镜像进行共享给指定租户，被共享租户可进行接受共享镜像操作。提供功能截图和厂商承诺函并加盖厂商公章。
6. 支持云主机运行状态下通过数据盘快照恢复数据盘数据。

1.4.3.4 裸金属设备租赁服务

1. ▲支持使用用户的自定义镜像创建裸金属实例自主申请裸金属批量，可以配置虚拟专有云、子网、弹性公网 IP 及公网带宽。支持查看裸金属查看 CPU、内存、网络、磁盘等监控指标；能够实现裸金属生命周期管理，包括创建、关闭、重启、删除、更换操作系统等操作，其中关闭、重启和关闭应支持批量操作，以提升管理员效率。提供厂商承诺函并加盖厂商公章。
2. 用户可以根据不同场景的业务需求进行选择不同类型的物理服务器，实现快速部署和设备管理；除裸机本地硬盘之外，也可以支持云硬盘，实现与本云内的云硬盘对接。

1.4.3.5 云硬盘服务

1. 提供云硬盘服务，可弹性扩展的虚拟块存储设备，为总站相关应用

提供系统盘及数据盘资源。可以在线进行操作，使用方式与传统服务器硬盘完全一致，可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据持久化存储。

2. 支持块存储、对象存储、文件存储等存储类型。
3. 支持每个云硬盘存储均需要有 3 份分布于不同机架的副本，保证数据安全可靠。
4. ▲支持对存储配置进行厚置备和精简置备的设置。提供第三方测试报告并加盖厂商公章。

1.4.3.6 数据库和中间件服务

1. ▲支持 Kafka、RabbitMQ、ActiveMQ、RocketMQ、TongWeb 等多种消息队列实现虚拟机自动化安装部署功能。提供厂商承诺函并加盖厂商公章。
2. 支持提供多种实例类型，满足客户多种场景业务。
3. 消息队列提供丰富多样的消息类型，支持普通消息、顺序消息、分布式事务消息、定时消息功能。支持消息队列的回收站管理。
4. 支持 DM8 数据库的自动安装、部署、实例下发及实例删除，参数修改与参数模板管理，对 DM 数据库表空间管理
5. 支持 DM8 数据库实例删除后，可选择放入回收站，预防数据丢失。对删除之后的表进行回站，必要的时候可以恢复
6. 支持 KingBase8 数据库的自动安装、部署、实例下发及实例删除，参数修改与参数模板管理，对 schema 进行管理
7. ▲云平台应具备应用视角故障精准定位能力，具备链路追踪、链路告警和链路分析等功能，即时了解服务健康度，链路日志联动分析，业务监控，Skywalking 实例管理，环境分析，自动监测异常事件、事件快照，秒级找到异常的微服务，掌控业务流量。提供功能截图证明和供厂商承诺函并加盖厂商公章。

1.4.3.7 网络服务

1. 支持提供虚拟私有云（VPC）服务，可以为云上租户提供一个专属、私密、隔离的网络环境。用户可以自主管理 VPC 网络环境，包括对

VPC 实例的增删改查、自定义 IP 地址范围、网段、路由表等，也可以结合弹性伸缩和弹性公网 IP 搭建自己的业务系统。

2. ▲支持 IPv4/IPv6 双栈，在 VPC 详情支持查看 VPC 内拓扑，图形化拓扑展示当前 VPC 的子网等信息。VPC 支持在单可用区和多可用区部署子网。提供功能截图证明和厂商承诺函并加盖厂商公章
3. 支持云主机的弹性网卡切换/迁移 VPC 功能，切换时支持手动指定或自动分配 IP 地址。
4. 支持 VPC 多出口能力，VPC 支持灵活配置 NAT 模式的互联网出口、三层路由直通出口、公网出口，多出口支持灵活映射到同一出口网关或不同的出口网关设备，支持横向扩展出口网关设备，同时出口网关支持使用软件形态或硬件形态承载。
5. 提供安全组服务，支持为云主机提供安全访问控制策略，并支持对安全组规则的增删改查操作，支持安全组规则的导入/导出，支持 IPv4/IPv6 双栈。支持同一弹性云主机实例的弹性网卡与主网卡可以属于不同的安全组。
6. 云管理平台能够提供云负载均衡服务，申请时可以指定负载均衡的规格。云负载均衡支持 UDP、TCP、HTTP、HTTPS 等多种网络协议，支持加权轮询、加权最小连接、源地址 Hash 等多种负载均衡算法。支持连接限制和会话保持，支持基于 PING、TCP、HTTP、HTTPS 的健康检查。
7. ▲支持通过软件和硬件两种不同形态提供 NAT 网关能力，NAT 网关服务组件具备高可用能力，避免单点故障。提供厂商承诺函并加盖厂商公章。
8. ▲支持申请/批量申请弹性公网 IP，支持弹性公网 IP 绑定云主机、裸金属、负载均衡、NAT 网关、辅助网卡、高可用虚拟 IP 等资源。提供功能截图证明和厂商承诺函并加盖厂商公章。

1.4.3.8 IP带宽服务

1. 支持与云服务器、裸金属服务器、NAT 网关灵活的绑定与解绑，带

宽支持灵活调整。

2. 支持接入多家运营商带宽，按要求提供 IP 数量和带宽大小。

1.4.3.9 容灾备份服务

1. 支持飞腾 1500/2000+/ S2500/5000C、鲲鹏 916/920/920X、海光 3G/4G、龙芯 MIPS/LoongArch、申威 SW64 等国产服务器平台的备份客户端、备份管理服务端软件和介质存储服务器端软件均支持基于龙芯、飞腾、海光、兆芯、申威、华为鲲鹏架构下的银河麒麟、中科方德、UOS 统一操作系统等国产操作系统
2. 备份客户端支持龙芯 LoongArch64 架构下的 UOS 统一操作系统。
3. 支持备份域间的备份集复制，为各类业务备份数据提供全面的数据保护。
4. 支持国产主流的数据备份恢复，包括但不限于达梦（DM）、人大金仓（Kingbase）、南大通用（GBase）、GBase 8a MPP、神舟通用（ShenTong）、优炫（UXDB）、瀚高（HighGo）、虚谷、openGauss、Vastbase（海量）、许继电气 SG-RDB-PG、GoldenDB、HotDB、AntDB（亚信）、FusionDB、MogDB、TDSQL PostgreSQL 版、TDSQL MySQL 版、GaussDB（DWS）和 GaussDB（for openGauss）、GoldenDB、OceanBase、磐维、巨杉（SequoiaDB）、万里（GreatDB）、HBase、TiDB、崖山（YashanDB）等数据库。支持 Linux OS、Windows OS、文件、NAS NDMP、Hadoop、Hive、HBase、FusionInsight HD、Cloudera CDH、对象存储、Exchange、Domino 备份集的备份域间复制。
5. 支持 K8s、VMware、Hyper-V、CAS、FusionCompute、HCS、HCSO、OpenStack、CloudOS、RHV、XenServer、InCloud Sphere、SmartX、ZStack、品高云、CNware 虚拟化备份集的备份域间复制。
6. 支持对备份域间复制的备份集，在目标域再进行池复制，用于跨域复制的数据归档、上云、异地保护等场景。
7. 支持达梦数据库数据库、用户、模式、表等逻辑备份和恢复，且支持单节点、主备集群（DMMSC）、大规模并行处理集群（DMMPP）、共

享存储集群（DMDSC）、读写分离集群（DMRWC）达梦分布式数据库（DMDPC）等架构。支持达梦数据库 DM6、DM7、DM8 版本备份与恢复。

8. 支持神舟通用数据库的物理备份，备份过程无需在数据库服务器上运行单独的脚本，备份数据无需在服务器上缓存，并通过备份软件管理界面即可配置备份策略和作业的管理。支持运行在龙芯、飞腾、海光、兆芯架构上的神舟通用数据库的流式备份和恢复。支持神舟通用数据库的完全备份、增量备份、差异备份功能，有效兼容神舟通用数据库的单机、双机、读写分离集群环境；

1.4.3.10 云防火墙服务

1. 支持静态路由、策略路由、RIP、OSPF、BGP、IS-IS 等路由协议
2. 支持一对一、多对一、多对多等多种形式的 NAT，支持 DNS、FTP、H.323、RTSP、ILS、PPTP、SIP、SQLNET、MGCP、RSH、ICMP 差错报文、TFTP、RTSP、SCTP、XDMCP、NBT、SCCP、HTTP 等多种 NAT ALG 功能。NAT 地址池支持动态探测和可用地址分配。
3. 实现 IPSec、L2TP、GRE VPN、SSL VPN 等功能。支持 SSL 的版本包括 TLS1.0、TLS1.1、TLS1.2、TLS1.3
4. 支持一体化安全策略，能够基于源/目的安全域、源 IP/MAC 地址、目的 IP 地址、地区、服务、时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置
5. 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。
6. ▲支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项，提供功能截图证明和厂商承诺函并加盖厂商公章

1.4.3.11 云WAF服务

1. 提供 Web 攻击防护，包括命令注入攻击，组件漏洞防护、Web 扫描防护、XPath 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、webshe11 防护
2. 提供 Web 业务加固防御功能，提供弱密码检测、CGI 安全、跨站请求伪造等防御功能
3. 支持检测并清洗的攻击类型：IP 攻击，TCP 攻击，UDP 攻击，ICMP 攻击，DNS 攻击，HTTP 攻击等多种 DDoS 攻击类型
4. 支持 SQL 注入、XSS 跨站攻击的语义分析检测，同时支持语义分析算法和特征检测算法的切换
5. ▲支持业务合规流程控制，防止非法用户通过不合规流程请求（提供产品 web 界面配置截图，及提供第三方检验报告证明，并加盖厂商公章）
6. ▲支持非法 URL 外联检测功能，针对特定外联 URL 进行监控或阻断，并且支持自定义 URL 地址（提供产品 web 界面配置截图，及提供第三方检验报告证明，并加盖厂商公章）

1.4.3.12 云堡垒机服务

1. 支持双因素组合认证，可以将两种认证方式自定义组合为全新的认证方式
2. 支持用户标签视图管理，可根据自定义的筛选条件快速统计出符合条件的账户信息
3. 支持资源、用户、操作三个维度审计智能检索
4. 支持对通过 RDP 协议登录到目标资源后的剪贴板控制，可限制剪贴板的文件上行、字符上行、文件下行、字符下行操作
5. ▲支持按不同属性对资产进行多级分类并自动生成树状结构的资源视图（提供产品 web 界面配置截图，及提供第三方检验报告证明）

1.4.3.13 数据库审计服务

1. 支持达梦、人大金仓、神通、高斯 DB、南大通用等国产数据库协议的解析
2. 支持 PostgreSQL、Greenplum、Cache 等专用数据库协议的解析
3. 支持主流大数据平台数据库/NoSQL 库的解析与审计，包括 HBase、Hive、MongoDB、Elasticsearch，Redis 等
4. 支持 UTF-8、GBK、GB2312、UNICODE、UTF-32/16/16BE/16LE、ISO-8859-1、US-ASCII 等编码方式。
5. ▲支持对操作语句中的 IP、账号、操作、操作对象进行业务翻译，支持按照业务语句模板进行操作语句翻译（提供界面截图证明，并加盖厂商公章）
6. ▲支持对审计到的敏感信息进行隐秘操作，防止信息二次泄密（提供界面截图证明，并加盖厂商公章）

1.4.3.14 日志审计服务

1. 支持按照日志按资产类型分布、日志设备采集分布、日志等级分布进行整体图表展示，并且支持下钻查看详细信息
2. 支持自定义采集日志类型，可以选择采集全部类型或者部分类型的日志
3. 支持在原始日志查询，输入原始日志中任意信息、选定任意时间进行内容查询匹配
4. 支持默认展示网元操作日志设备 IP 分布、审计日志类别分布、安全日志攻击日志类型分布、安全日志设备名称分布、安全日志严重等级分布、安全策略日志目的 IP 分布内容
5. ▲支持在日志查询过滤条件中选择性针对关注的字段结果进行统计，针对统计的结果进行排序，并支持快捷添加为过滤条件。（提供第三方检测报告佐证并加盖厂商公章）
6. ▲支持 NAT 溯源取证专题功能模块，查找内网资产真实 IP，并能够查看相对应的安全风险，支持针对 NAT 转换源 IP、目的 IP、溯源时间信息进行溯源，针对溯源结果以溯源业务链的方式呈现。（提供

第三方检测报告佐证并加盖厂商公章)

1.4.3.15 漏洞扫描服务

1. 支持 Web 漏洞扫描，漏洞规则依据 OWASP 定义的常见 TOP10Web 漏洞进行分类
2. 支持目前主流协议弱口令检测，包含 TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP
3. 支持基线核查功能
4. 支持主流数据库漏洞的检测，应包括但不限于：Oracle、Sybase、SQLServer、DB2、MySQL、Postgres、Informix、达梦、南大通用、人大金仓、神通等。
5. ▲支持自动探测指定 IP 段的未知 Web 站点（提供界面截图证明，并加盖厂商公章）

1.4.3.16 商用密码应用服务

按需提供加解密服务、完整性校验服务、签名验签服务、时间戳服务、密钥管理服务、数据库加密服务、SSL 安全网关-安全接入、SSL 安全网关-https 安全负载、国密浏览器、手机盾签名验签、USB Key、应用密码改造咨询及指导。

1.4.3.17 云主机安全服务

1. 一体化管理，统一客户端，统一服务端提供病毒防护、检测响应、运维管控、基线核查、漏洞管理、虚拟补丁等多重防护能力。
2. 产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁；
3. 可基于 ATT&CK 架构识别攻击阶段，并呈现排名考前的受威胁主机
4. 支持 USB 外设进行管理，提供允许、禁用的控制能力，包括光驱、打印机、扫描仪、手机/平板、红外等设备
5. 支持在线、离线两种更新方式
6. ▲对于恶意文件处理措施至少支持三种以上（提供界面截图证明，并加盖厂商公章）
7. ▲支持对补丁的扫描任务和修复任务进行管理（任务的新建，启用，

停用，编辑，删除），支持设置周期性的扫描修复任务（提供界面截图证明，并加盖厂商公章）

1.4.3.18 机柜服务

须保证用户租用的服务器设备可持续获得冷源供应，机房运行环境恒温恒湿：温度为 $23 \pm 1^{\circ}\text{C}$ ，相对湿度保持在 40%~55%；机柜采用精确送风方式；空调系统采取 N+1 冗余备份方式设置，无单点故障；具备专业空调维护队伍；对机房温湿度有监控措施和记录。

提供满足本次政务云服务运行承载的机柜空间，每个机柜须满足双路供电。

1.4.3.19 托管设备技术要求

按照使用机柜高度 U 为单位提供托管服务，并对托管设备提供基础网络配置及故障排查、硬件巡检服务、7x24 值守服务。

1.4.3.20 云主机服务器硬件技术要求

1. CPU： ≥ 2 颗国产 CPU，单 CPU 主频 $\geq 2.7\text{GHz}$ ，单 CPU 核心数 ≥ 64 ， ≥ 128 线程，符合安全可靠测评 II 级；
2. 内存： $\geq 16*64\text{GB}$ DDR5
3. 系统盘： $\geq 2*480\text{GB}$ SATA SSD
4. PCI 扩展：最多提供 ≥ 10 个标准 PCIe 5.0 插槽
5. GPU 扩展：可配置 ≥ 4 块双宽或 ≥ 8 块单宽 GPU 卡
6. 电源：双电源；
7. 网络：支持 ≥ 1 个管理接口， ≥ 4 个 GE 电接口， ≥ 6 个 10GE 光接口

1.4.3.21 存储设备硬件技术要求

1. CPU： ≥ 2 颗国产架构 CPU，单 CPU 主频 $\geq 2.5\text{GHz}$ ，单 CPU 核心数 ≥ 32 ， ≥ 64 线程，符合安全可靠测评 II 级；
2. 内存： $\geq 128\text{GB}$ DDR5
3. 硬盘： $\geq 2*480\text{GB}$ SATA SSD， $\geq 2*3.2\text{TB}$ NVMe SSD， $\geq 12*16\text{TB}$ SATA SSD
4. PCI 扩展：最多提供 ≥ 10 个标准 PCIe 5.0 插槽；
5. 电源：支持双电源；

1.4.3.22 网络安全设备技术要求

1.4.3.22.1 核心交换机：

1. CPU、交换芯片、内存均为国产芯片，且 CPU 芯片在国家安全可靠测评名录中
2. 交换容量 $\geq 2700\text{Tbps}$ ，包转发率 $\geq 230000\text{Mpps}$ ；
3. 正交无中板架构，独立交换网板插槽数量 ≥ 6 ，业务槽位数量 ≥ 4 ，电源、风扇、主控、交换网板等关键部件冗余
4. 端口密度：配置 40G QSFP+ 光口 ≥ 36 ，10G SFP+光口 ≥ 48
5. ▲10G/25G/40G/100G/400G 端口时延均 $< 1.2\mu\text{s}$ ，提供第三方测试报告并加盖厂商公章。
6. ▲支持 TAP 能力，满足安全管理平台、审计系统等同时采集数据的需求，可支持 TAP 同源同宿功能，报文截断功能，源端口标识功能，支持 TAP 基于端口的 M:N 模型功能，M:N 模型下最大 M 口规格 ≥ 512 ，N 口规格 ≥ 512 ，提供第三方测试报告并加盖厂商公章。
7. 支持 RDMA、RoCE v2、PFC、ECN 等无损以太网特性；
8. 支持虚拟化技术，支持一虚多，可虚拟成 ≥ 16 台逻辑交换机；支持多虚一，支持 DRNI/M-LAG 跨设备链路聚合及 DRNI/M-LAG 升级功能，保证业务不中断。
9. 数量要求：政务外网区 ≥ 2 台，互联网区 ≥ 2 台。

1.4.3.22.2 万兆业务交换机

1. CPU、交换芯片均为国产芯片，且 CPU 芯片在国家安全可靠测评名录中
2. 交换容量 $\geq 4.8\text{Tbps}$ ，包转发率 $\geq 2000\text{Mpps}$ ；
3. 电源、风扇等关键部件冗余，风扇模块 ≥ 5 ；
4. 端口密度：配置 100G QSFP28 光口 ≥ 8 ，10G SFP+光口 ≥ 48 ；
5. ▲10G 端口时延 $< 3\mu\text{s}$ ；100G 端口时延 $< 1\mu\text{s}$ ，提供第三方测试报告并加盖厂商公章。

6. ▲支持 TAP 能力，满足安全管理平台、审计系统等同时采集数据的需求，可支持 TAP 同源同宿功能，报文截断功能，源端口标识功能，支持 TAP 基于端口的 M:N 模型功能，M:N 模型下最大 M 口规格 ≥ 120 ，N 口规格 ≥ 120 ，提供第三方测试报告并加盖厂商公章。
7. 支持 RDMA、RoCE v2、PFC、ECN 等无损以太网特性；
8. 整机缓存 $\geq 36\text{MB}$ ，MAC 表项 $\geq 704\text{K}$ ；
9. ▲支持全端口 256bits MACsec 加密，支持国密认证，支持可信计算，提供第三方测试报告并加盖厂商公章。

1.4.3.22.3 存储网交换机：

1. CPU、交换芯片、为国产芯片，
2. 电源、风扇等关键部件冗余；
3. 端口密度：配置 100G QSFP28 光口 ≥ 4 ，40G QSFP+ 光口 ≥ 2 ，10G SFP+光口 ≥ 48 ，
4. 10G/40G/100G 端口时延均 $\leq 1.03\mu\text{s}$
5. ▲支持安全扩展能力，可根据实际业务需求灵活扩容防火墙、入侵防御等至少 5 种及以上安全业务模块。提供佐证材料，并加盖厂商公章。

1.4.3.22.4 安全网关

1. 设备整机所使用的全部 CPU 芯片和交换芯片均为国产化品牌芯片；
2. 设备采用控制、数据、业务相互解耦分离的全分布式架构，主控引擎、采用硬件槽位分离的独立硬件模块，支持业务和接口扩容模块数量 ≥ 4 ；
3. 主控引擎需采用独立且可热插拔的硬件模块形态，占用专用的硬件槽位，数量 ≥ 2 ，支持 1+1 冗余备份，保障热插拔无丢包；
4. 具备可插拔冗余电源模块，电源模块 ≥ 2 ，可插拔冗余风扇模块，风扇模块 ≥ 2 ；
5. ▲吞吐量 $\geq 200\text{ Gbps}$ ；并发连接数 ≥ 6000 万；新建连接数 ≥ 130 万

/秒；开启 IPS 和 AV 功能后，设备吞吐性能 $\geq 36\text{Gbps}$ ，提供佐证材料，并加盖厂商公章；

6. 支持 100G QSFP28 光接口 ≥ 2 , 10G SFP+光接口 ≥ 14 ；含 IPS/AV/URL 特征库升级服务；
7. 支持虚拟防火墙功能：支持虚拟防火墙的创建、设置、停止、删除功能；虚拟防火墙数量 ≥ 2048 个；
8. 设备支持完善的 NAT66 功能，支持 IPv6 源地址转换、IPv6 目的地址转换、IPv6 双向地址转换等 NAT66 能力；
9. 支持防病毒检测功能，支持对 IPv4、IPv6 的报文进行病毒检测并输出日志；设备本地支持病毒特征库数量 ≥ 600 万种；
10. 支持超过 23000 种入侵防御特征库；
11. ▲支持 IPSEC VPN 功能，支持 IPSEC 智能选路功能，支持 SM2/SM3/SM4 国密加密算法，提供佐证材料，并加盖厂商公章；
12. 支持全面的 IPv4/IPv6 路由能力；
13. 支持对流经的文件传输、HTTP 网页流量，解析文件内容、HTTP 网页内容并进行过滤，支持对涉及指定关键词内容的文件传输行为或 HTTP 访问行为进行过滤管控，从而降低数据泄露风险；
14. 政务外网区 ≥ 4 台，互联网区 ≥ 4 台。

1.4.3.23 主要租赁设备技术要求

1.4.3.23.1 4G吞吐防火墙：

1. 国产化防火墙产品，采用国产化 CPU；
2. 整机吞吐量 $\geq 4\text{G}$ ，并发连接数 ≥ 250 万，每秒新建连接数 ≥ 4 万；
3. 支持国密 SM2、SM3、SM4 算法；
4. 支持 ≥ 16 个千兆电接口， ≥ 6 个千兆光接口， ≥ 2 个万兆光接口， ≥ 4 个 Combo 电接口， ≥ 1 个 Console 接口， ≥ 2 个扩展槽位； $\geq 1\text{TB}$ 硬盘；2*交流电源, 含 IPS/AV/URL 组合特征库升级服务；
5. 具备网络安全专用产品安全检测证书

1.4.3.23.2 10G吞吐防火墙

1. 国产化防火墙产品，采用国产化 CPU
2. 整机吞吐量 $\geq 10\text{G}$ ，并发连接数 ≥ 400 万，每秒新建连接数 ≥ 10 万；
3. 支持国密 SM2、SM3、SM4 算法；
4. 100GE 光接口 ≥ 2 ，10GE 光接口 ≥ 8 ，GE 光接口 ≥ 8 ，GE 电接口 ≥ 16 ，接口扩展槽位 ≥ 2 个，1TB 硬盘；2*交流电源，IPS/AV/URL 组合特征库升级服务；
5. 要求具备网络安全专用产品安全检测证书

1.4.3.23.3 20G吞吐防火墙：

1. 国产化防火墙产品，采用国产化 CPU；
2. 整机吞吐量 $\geq 20\text{G}$ ，并发连接数 ≥ 1000 万，每秒新建连接数 ≥ 15 万，支持国密 SM2、SM3、SM4 算法；
3. 100GE 光接口 ≥ 2 ，10GE 光接口 ≥ 8 ，GE 光接口 ≥ 8 ，GE 电接口 ≥ 16 ，接口扩展槽位 ≥ 2 个，1TB 硬盘；2*交流电源，IPS/AV/URL 组合特征库升级服务；
4. 要求具备网络安全专用产品安全检测证书

1.4.3.23.4 堡垒机：

1. 国产化堡垒机，采用国产化 CPU；
2. 硬件 2U 硬件架构， $\geq 16\text{GB}$ 内存， $\geq 4\text{TB}$ 硬盘容量；
3. 支持 GE 电口 ≥ 6 ，GE 光口 ≥ 4 ；
4. 接口卡扩展槽 ≥ 2 个，支持以太网千兆或万兆接口扩展能力；为用户提供了全面的运维管理体系和运维能力，保障运维过程的安全；
5. 图形会话并发数 ≥ 200 ，字符会话并发数 ≥ 700 ，可管理资产数 ≥ 300 ；
6. 支持图形操作的关键事件切片，管理员点击任意切片，即可直接定位到对应操作片段；
7. 支持资源、用户、操作三个维度审计智能检索，其中在操作检索层面，支持多关键字检索，检索结果直接定位到相关操作片段，并能将多个会话的操作片段进行一键合并和基于时间的操作排序重组；

8. 要求具备网络安全专用产品安全检测证书

1.4.3.23.5 网闸

1. 国产化网闸，采用国产化 CPU
2. 采用“2+1”模块结构设计，包括内端机、外端机和隔离交换等模块组成，实现协议隔离和信息交换
3. 吞吐性能 $\geq 900\text{Mbps}$ ，系统整体时延 $< 1\text{ms}$ ，并发连接数 $\geq 80\text{W}$
4. 内网支持 ≥ 6 千兆电接口， ≥ 4 千兆光；
5. 外网支持 ≥ 6 千兆电接口， ≥ 4 千兆光；
6. 具备 TCP、UDP、FTP 等协议定制应用数据交换，支持 FTP 文件双向同步功能
7. 要求具备网络安全专用产品安全检测证书

1.4.3.23.6 日志审计

1. 国产化日志审计，采用国产化 CPU
2. 机架式硬件架构，高度 $\leq 2\text{U}$ ，提供 $\geq 8*\text{GE}$ 电接口， $\geq 4*\text{GE}$ 光接口， ≥ 4 个扩展槽，可按需扩展 GE 电/GE 光/10GE 光接口，电源标配： $2*350\text{W}$
3. CPU ≥ 8 核；内存 $\geq 16\text{G}$ ，硬盘 $\geq 4\text{T}$ 3.5 寸 SATA 盘， $\geq 128\text{TB}$ SSD 硬盘
4. Syslog 文本日志入库性能 $\geq 5000\text{EPS}$ ，二进制日志入库性能 $\geq 10000\text{EPS}$ ；
5. 支持 ≥ 128 个日志源，最大支持 ≥ 512 个日志源；
6. 要求具备网络安全专用产品安全检测证书

1.4.3.23.7 数据库审计

1. 国产化数据库审计，支持国产化操作系统，采用国产化 CPU
2. 支持 ≥ 4 类数据库，支持数据库类型扩容；
3. SQL 平均处理性能 $\geq 5\text{Wqps}$ ，SQL 峰值处理性能 $\geq 6\text{Wqps}$
4. 入库速度 $\geq 6\text{Wqps}$ ，日志存储数量 ≥ 80 亿条

5. 吞吐 $\geq 3000\text{Mbps}$, $\geq 8\text{GE}$ 电接口, $\geq 4*\text{GE}$ 光接口, ≥ 4 扩展槽
6. 支持 Oracle、MySQL、SQLServer、DB2、Sybase、Informix 等主流数据库协议的解析。支持 SQLServer2005 及以上版本的加密数据库账号的解析, 支持达梦、人大金仓、神通、高斯 DB、南大通用等国产数据库协议的解析, 支持 PostgreSQL、Greenplum、Cache 等专用数据库协议的解析, 支持主流大数据平台数据库/NoSQL 库的解析与审计, 包括 HBase、Hive、MongoDB、Elasticsearch、Redis 等
7. 支持自动发现镜像流量中的活跃数据库。支持自定义发现范围, 包括数据库类型、IP 地址、端口范围。
8. 支持 UTF-8、GBK、GB2312、UNICODE、UTF-32/16/16BE/16LE、ISO-8859-1、US-ASCII 等编码方式。
9. 要求具备网络安全专用产品安全检测证书

1.4.3.23.8 WEB应用防护

1. 国产化 WEB 应用防护, 采用国产化 CPU, 支持国产化操作系统
2. 应用层吞吐性能 $\geq 1.5\text{G}$,
3. HTTP 新建连接数 ≥ 4 万, HTTP 并发连接数 ≥ 60 万, HTTPS 并发连接数 ≥ 11 万, 保护网站站点数量无限制
4. $\geq 8*\text{GE}$ 电口, 支持 BYPASS, $\geq 4*\text{GE}$ 光口, 支持扩展插槽 ≥ 4
5. 支持网页防篡改, 支持 Web 攻击防护功能, 包括命令注入攻击, 组件漏洞防护、Web 扫描防护、XPath 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、webshell 防护;
6. 支持业务合规流程控制, 防止非法用户通过不合规流程请求, 对 web 服务器进行攻击;
7. 支持 SQL 注入、XSS 跨站攻击的语义分析检测, 同时支持语义分析算法和特征检测算法的切换
8. 要求具备网络安全专用产品安全检测证书

1.4.3.23.9 路由器

1. 设备满足国产化要求, 设备关键核心芯片 (CPU、转发芯片) 采用

国产化芯片，设备 CPU 满足安全可靠测评名录；

2. 双主控双转发架构、可插拔电源模块 ≥ 4 ；
3. 交换容量 $\geq 670\text{Gbps}$ ，包转发率 $\geq 360\text{Mpps}$ ；
4. 配置 $\geq 14 \times 10\text{GE (SFP+)}$ ， $\geq 14 \times \text{GE (RJ45)}$ ， $\geq 4 \times 25\text{GE}$ 光接口；
5. 设备子卡业务板槽位数 ≥ 6 ，支持子卡热插拔；
6. ▲支持 SM1/SM2/SM3/SM4 国密算法，提供证明材料并加盖制造商公章；
7. 支持 MACSEC 保障业务数据在网络中的安全传输；
8. 满足 IPv6+技术演进需求，支持 IPv6、支持 NAT66；
9. 具备中华人民共和国工业和信息化部颁发的电信设备进网许可证。

1.4.3.23.10 漏洞扫描

1. 国产化产品，采用国产化 CPU
2. 系统漏扫&数据库&基线漏扫最大并发扫描 IP 总数 ≥ 60
3. 系统漏扫&数据库&基线漏扫最大并发扫描任务数 ≥ 6
4. Web 漏扫最大并发扫描站点数 ≥ 5 ，口令猜解并发 ≥ 4
5. 支持 $\geq 4 \times \text{GE}$ 电口， $\geq 4 \times \text{GE}$ 光口，支持扩展插槽 ≥ 2
6. 系统应支持检测的系统漏洞数 ≥ 20 万，覆盖 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq 多种漏洞标准。
7. 支持国产操作系统、数据库的扫描，国产操作系统包含中标麒麟、凝思、华为欧拉、深度、红旗、中兴新支点，国产数据库包括神通、人大金仓、南大通用、达梦。
8. 支持主流数据库漏洞的检测，应包括但不限于：达梦、南大通用、人大金仓、神通、SQLServer、DB2、MySQL、Postgres、Informix 等；
9. 系统应支持目前主流协议弱口令检测，包含 TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP ；
10. 要求具备网络安全专用产品安全检测证书

1. 4. 3. 23. 11 入侵防御

1. 国产化入侵防御，采用国产化 CPU
2. 专业入侵防御设备，非下一代防火墙产品；接口扩展槽位 ≥ 6 ，支持扩展 100G 接口；支持可插拔冗余电源模块；支持 ≥ 2 个硬盘扩展槽位；
3. 吞吐性能：网络层吞吐 $\geq 15\text{G}$ 、全威胁吞吐性能 $\geq 5\text{G}$ ，新建连接数： ≥ 10 万/秒，并发连接数： ≥ 500 万
4. 配置 $\geq 5*\text{GE}$ （支持 Bypass）， $\geq 4*\text{SFP}$ 光口，2 个接口扩展槽位
5. 支持一体化安全策略，能够基于源/目的安全域、源 IP/MAC 地址、目的 IP 地址、地区、服务、时间、用户/用户组、应用层协议、五元组、内容安全（WAF、IPS、防病毒、数据过滤、文件过滤、URL 过滤和 APT 防御等）统一界面进行安全策略配置，提供第三方测试报告证明；
6. 入侵攻击特征库数量 ≥ 24000 、病毒特征库数量 $\geq 600\text{W}$ 、Web 攻击特征库 ≥ 6000 ，提供第三方测试报告证明；
7. 支持虚拟入侵防御功能：支持虚拟入侵防御的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；可独立管理，独立保存配置；具备独立会话管理、路由等功能。提供第三方测试报告证明；
8. 要求具备网络安全专用产品安全检测证书

1. 4. 3. 23. 12 24口千兆电接入交换机

1. 国产化交换机，采用国产化 CPU
2. 交换容量 $\geq 670\text{Gbps}$ ，包转发率 $\geq 170\text{Mpps}$
3. 支持 ≥ 28 个千兆电口， ≥ 6 个万兆光业务端口；
4. 支持双电源；
5. 支持 IPv4 静态路由；
6. 支持 SNMP 功能

1. 4. 3. 23. 13 48口千兆电接入交换机

1. 国产化交换机，采用国产化 CPU；
2. 交换容量 $\geq 670\text{Gbps}$ ，包转发率 $\geq 200\text{Mpps}$ ；
3. 支持 ≥ 48 个千兆电口， ≥ 6 个万兆光业务端口；
4. 支持双电源；
5. 支持 IPv4 静态路由；
6. 支持 SNMP 功能

1. 4. 3. 23. 14 48端口万兆交换机

1. 国产化交换机，采用国产化 CPU
2. 交换容量 $\geq 4.8\text{Tbps}$ ，包转发率 $\geq 2000\text{Mpps}$ ；
3. 电源、风扇等关键部件冗余；
4. 配置 100G QSFP28 光口 ≥ 4 , 40G QSFP+光口 ≥ 2 , 10G SFP+光口 ≥ 48 ,
10G/40G/100G 端口时延均 $\leq 1.03\mu\text{s}$ ；
5. 支持 TAP 功能

1. 4. 3. 23. 15 48千兆光交换机

1. 国产化交换机，采用国产化 CPU，
2. 交换容量 $\geq 2.4\text{Tbps}$ ，包转发率 $\geq 650\text{Mpps}$ ；
3. 支持 ≥ 48 个 GE SFP 端口， ≥ 4 个 10G SFP+端口，
4. 支持冗余电源