**采购需求**

北京互联网法院2025年度政务云平台基础资源租用服务采购项目

1. **采购标的**

1. 采购标的（货物需求一览表或简要服务内容及数量）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物或服务名称 | 数量 | 单位 |
| 1 | 云主机 | 2C4G | 5 | 台 |
| 2C8G | 1 | 台 |
| 4C8G | 136 | 台 |
| 4C16G | 8 | 台 |
| 8C16G | 56 | 台 |
| 8C32G | 4 | 台 |
| 8C64G | 1 | 台 |
| 16C32G | 26 | 台 |
| 16C64G | 9 | 台 |
| 32C64G | 6 | 台 |
| 32C128G | 1 | 台 |
| 共1860C，4252G（以上资源可根据采购人需求进行再次分配） |
| 2 | 通用型SSD | 普通存储 | 18000 | GB |
| 3 | 性能型SSD | 高性能存储 | 170000 | GB |
| 4 | 本地备份服务 | 本地备份服务 | 188000 | GB |
| 5 | 异地备份服务 | 异地备份服务 | 66560 | GB |
| 6 | 互联网链路服务 | 同时满足上、下1、互联网链路带宽；2、专线带宽： （1）北京互联网法院云机房至北京互联网法院≥500M；（2）北京互联网法院云机房至北京市高级人民法院云机房≥500M。 | 1 | 套 |
| 互联网IP地址租用服务、并提供备案服务 | 49 | IP |
| 7 | 主机负载均衡服务 | 主机负载均衡服务 | 17 | IP |
| 8 | 远程接入服务 | 远程接入服务 | 100 | 账号 |
| 9 | WAF防护 | web应用防火墙服务 | 12 | IP |
| 10 | 特定云主机深度监控及运维保障服务（7\*24小时值守） | 7\*24小时深度监测云主机资源、硬件设备监控、云平台层应急处置等内容 | 253 | 台 |

说明：本项目不接受进口产品。云主机资源可根据采购人需求进行再次分配，主机负载均衡服务、远程接入服务、WAF防护、特定云主机深度监控及运维保障服务可按照采购人要求进行调整。

2. 项目背景

根据《北京市法院信息化建设五年发展规划（2016-2020）》、《最高人民法院关于互联网法院审理案件若干问题的规定》等文件要求。2018年北京互联网法院成立以来，以北京市级政务云计算服务作为北京互联网法院信息系统的基础运行环境，承担了电子诉讼平台，门户网站、英文门户网站、微法院系统、区块链系统等11个系统的基础云资源服务。一直以来各系统运行平稳，主站访问超过3亿次，英文网站访问超过千万次。

本期要求租用市级政务云，租用计算资源、存储资源、网络资源、7\*24小时运维等服务为北京互联网法院电子诉讼平台，门户网站、英文门户网站、微法院系统、区块链系统等系统提供稳定高质量的运行环境，保障各业务系统运行稳定。

1. **商务要求**

1. 交付（实施）的时间（期限）和地点（范围）

1.1 服务时间：　签订合同后一年（履行时间：2025年6月9日至2026年 6月8日）。

自签订合同起5日内，完成采购人云上部署应用及数据迁移。

1.2 服务地点：　北京互联网法院

2. 付款条件（进度和方式）

根据北京互联网法院内控管理制度规定，该项目合同分三期支付，其中合同签订后支付项目总金额的50%作为首付款，服务满半年后，若中标人无违约行为支付项目总金额45%的款项，合同到期前一个月，且完成验收服务后，若报价人无违约行可支付剩余5%的款项。

4. 售后服务（质保期）

报价人对该项目要求配备专业人员成立售后服务团队，保障服务运维工作顺利开展；7\*24小时云资源和网络链路稳定性监控保障服务；7\*24小时IM群，快速响应，专家会诊，及时风险预警。VIP大客户专线、即时通讯客服、邮件客服，电话客服等；7\*24小时产品运维团队提供专人专家技术支持；需要配合采购人进行系统等级保护检查；需要提供上门使用指导培训。报价人应当提供详实周到的系统使用培训服务，按照采购人要求对报价人提供的产品使用开展培训并提供7\*24小时技术服务。

1. **技术要求**

1. 基本要求

本项目采购标的的总体要求及需满足的国家相关标准、行业标准、地方标准或者其他标准、规范如下：

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 合规性★ | 不得转包此项目，需开具带有投标人公章的不转包项目承诺书。 |
| 可用区★ | 本项目要求针对中国大陆地区，云厂商需提供跨城域的异地可用区，需出具带有投标人公章的有效证明材料。 |
| 网络接入★ | 中标后需满足投标人云机房专线至北京互联网法院、投标人云机房至北京市高级人民法院云机房专线，带宽皆不低于500M，需要开具带有投标人公章的承诺书。 |
| 平台开放性要求# | 支持用户自服务门户、命令行和open API，并向用户提供统一门户、统一服务和跨省备份，需出具有效证明材料（如API手册、web页面截图等）。 |
| 认证合规★ | 云平台需具备信息安全等级保护三级或以上等级的认证，需出具带有相关行政部门的有效证明材料。 |
| 云计算平台信息安全★ | 投标人须承诺数据的私有和安全，保证数据私密性，即投标人承诺在未获允许的情况下，不得使用我方在云上产生和使用的数据，不得提供给第三方，保证云平台产生的数据不会被挖掘，不会被用于广告或其他商业目的，需要开具带有投标人公章的承诺书。 |

2. 服务内容及要求/货物技术要求

本项目采购标的需满足的技术、服务要求如下，投标人需提供有效的证明材料、设计方案，满足采购标的的性能、功能等基本要求。

2.1服务要求

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 售后支持★ | 售后工程师提供全年7\*24小时的电话，工单及IM实时支持，30分钟快速响应，需要开具带有投标人公章的承诺书。 |
| 迁入服务支持★ | 本项目涉及的应用系统为采购人在用的生产系统，因此业务连续性是首要保障需求。如发生政务云迁移，投标人应承担以下服务：协助北京互联网法院部署在云上的应用服务商并联系原有云服务商配合做好迁移工作，并承担期间发生的全部费用（包括但不限于迁移测试阶段的云资源费用，第三方对业务系统的部署、调试费用等）。以上需要开具带有投标人公章的承诺书。 |

2.2主机要求

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 可用性要求# | 按内存不复用方式分配资源，要求CPU主频≥2.4GHz，云主机SLA，对于单实例单可用区维度，云主机的服务可用性不低于99.97%；单地域多可用区维度，云主机的服务可用性不低于99.97%，需出具承诺书，需出具带有投标人公章的承诺书。 |
| 性能要求 | 支持双路服务器，可以基于服务器的每路CPU进行独立调度，同时支持两路RAID卡和两路网卡的独立调度，以提升云主机的性能。 |
| 操作要求# | 支持调整CPU核数、内存大小；支持镜像：官方/私有/共享镜像，支持导入、导出、共享/取消共享、整机镜像，需提供操作关键步骤截图。 |
| 动态资源扩展# | 支持对云主机扩展和收缩策略的灵活配置，能够根据云主机CPU、内存等参数动态的克隆云主机或删除云主机以满足业务量大时使用多个云主机提供服务、业务量少时使用少量云主机提供服务的业务需求，整个过程不需要人工干预，同时支持对业务云主机组的统一负载监控和负载状态展示，需提供操作关键步骤截图。 |
| 资源开通方式# | 支持灵活的资源开通方式，支持直接开通，也支持按部门或云服务设置为审批模式，通过审批流程开通资源。直通模式和审批模式可以依据业务交叉设置，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 资源混部# | 云平台应支持ECS、容器、数据库同一资源池部署，即同一物理机可以同时创建ECS、容器和数据库实例。需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 安全要求# | 安全组、SSH安全密钥、IAM访问权限控制、实时监控报警、节点故障自动恢复，支持租户删除云主机，放入回收站，并可从回收站恢复云主机。需提供操作关键步骤截图。 |
| 登录访问限制# | 支持配置云服务器ECS的登录访问控制，支持IP黑白名单、会话超时时间、连续登录失败锁定用户、密码强度设置等功能，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 兼容性要求# | 云平台采用云原生技术实现，支持ECS、容器、数据库等多个云服务在一个Kubernetes集群调度与管理，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 可维护性# | 支持单虚拟机实例升级Qemu，支持多个Qemu版本的虚拟机同时运行，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 技术支持# | 支持同一集群内同时运行多种体系架构CPU虚拟机，同一资源池支持多种体系架构CPU，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。同时，在与采购人缔约期间，如采购人要求“XC”升级，投标人应无偿在云侧进行相关支持，如支持集群内X86、ARM架构服务器并存等，需要开具带有投标人公章的承诺书。 |

2.3存储要求

|  |  |
| --- | --- |
|  指标项 | 招标要求 |
| 可靠性要求# | 为确保数据可靠性，云平台关键组件支持多副本方式部署，不存在单点故障隐患，支持纠删码，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 性能要求# | 提供SSD云硬盘、需要支持云硬盘形式的系统盘卸载和挂载、具备多挂载点、高并发性、高可靠性等特点；需支持在线调整性能级别，无需停机或迁移数据；需支持文件存储；需提供操作关键步骤截图。 |
| 快照要求# | 支持通过快照链特性将同一块云硬盘的所有快照组成的关系链，每个关系链的节点表示云硬盘的一份快照，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 使用要求# | 支持服务器扩展，扩容过程中不影响对外服务；系统整体架构无单点故障，支持在线更换坏盘、热备盘；支持更换实例的系统盘，更换系统盘前后，实例的IP、MAC地址保持不变，需提供操作关键步骤截图。 |
| 安全要求# | 支持对云盘数据进行加密持久化保存，加密算法支持国际通用AES256和国密SM4，能够实现不同存储节点的数据差异不超过5%，整个集群空间利用率达95%以上。需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |

2.4网络要求

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 支持SDN或OVS | 能通过SDN控制器实现对物理网络设备或OVS虚拟网元等自动化配置。 |
| 组网模式# | 支持VLAN或基于VXLAN的其他技术组网模式。支持VPC互通（若成交后必须满足北京互联网法院与北京市高级人民法院云主机互通），需出具带有投标人公章的承诺书。 |
| IP地址重叠 | 支持租户IP地址重叠及支持子网跨AZ，如涉及服务迁移可保持云内网IP不变。 |
| 云防火墙服务 | 云管理平台能够提供云防火墙服务。 |
| IPV4/6双模 | 支持IPV4/6双模配置。 |
| IP管理# | 公网IP：支持增删改查、绑定和解绑资源、调整带宽及支持无预设的CIDR块，需提供操作关键步骤截图。 |
| 安全性# | VPC隔离、子网级ACL一级防护，实例级安全组二级防护、支持高可用路由，需提供操作关键步骤截图。 |
| 专有网络VPC# | VPC内支持同时创建标准型子网与直通型子网，VPC直通型子网支持访问外网，VPC标准型子网可通过EIP/NAT网关访问外网。需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 负载均衡 | 支持无负载均衡实体的负载均衡服务，提供软件定义的全可用区不低于3层网络负载均衡，兼具高性能且支持大额并发；应用负载均衡支持TCP\UDP\HTTP\HTTPS等多种协议的不同端口侦听服务。 |
| 域名转换 | 涉及域名于公网IP映射关系需对DNS进行配置。支持智能解析，提供基于物理位置或者基于权重的智能返回。 |

2.5安全要求

|  |  |
| --- | --- |
|  指标项 | 招标要求 |
| 基础防护# | 能够有效抵御 SYN Flood、UDP Flood、ACK Flood、ICMP Flood 等各种常见DDoS 攻击，需出具带有投标人公章的承诺书。 |
| WEB 应用防火墙# | 支持 SQL 注入攻击、XSS 攻击防护、Web 应用扫描防护、文件读取/包含攻击、命令/代码执行攻击、敏感文件探测、恶意扫描攻击、恶意/ 后门文件攻击、XML 注入攻击、目录遍历攻击、Web 插件漏洞防护。 支持不同种规则等级或自定义防护动作。支持配置防护动作，需提供操作关键步骤截图。 |
| 支持白名单、黑名单配置，可匹配 URI、IP、Cookie、Geo、Header，匹配方式以及后续执行动作，需提供操作关键步骤截图。 |
| 针对Bot管理模块支持防爬场景化配置功能。可以基于实际业务场景对防爬规则进行自定义，更有针对性地对业务进行爬虫风险防护，防爬规则至少支持JS验证脚本、安全滑块、SEO优化、基于IP和session的限速，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 支持域名、来源地区、日志类型、方法、动作、URL、状态码组合条件查询。支持请求时间、源 IP、请求 ID、来源地区、方法、动作、 URL、恶意负载、攻击详情、状态码、状态标识的查看，需提供操作关键步骤截图。 |
| 安全运营中心# | 支持安全运营大屏，可根据选择的时间维度查看基于攻防实战演进安全能力，提供量化安全运营指标，包含：确认风险处置率、安全事件平均发现时间（MTTD）、平均响应时间（MTTR）、平均止血时间以及自动化处置率，同时提供实时攻击源统计能力，包含：新增攻击IP、已封禁IP。以及攻击源处置监控实时信息、攻击炮图、工单状态统计风险处置率部门排名。同时支持自定义安全大屏logo，需提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 支持分类统计各类资产（云主机、容器、物理服务器、网站）在线数量统计，通过进行资产扫描，对外暴露的端口和应用进行看板可视化呈现，可以直观呈现当前资产，存活公网 IP 数量、开放端口数量、暴露端口及应用类型数量，并可以支持自定义违规端口和应用。支持进行攻击源 IP 统计分析，包括攻击总次数，攻击 IP 总数，并支持按照攻击源检测引擎进行分类统计分析，支持周期化检测分析，支持自定义规则制定聚合攻击网段排名，呈现攻击源 IP 地址位置分布，需出具带有投标人公章的承诺书。 |
| 自动化攻击溯源：可自动化关联告警、风险资产、进程、攻击IP等信息，根据入侵场景，自动化分析出风险资产的入侵链路图，需提供操作关键步骤截图。 |
| 主机安全# | 支持同一个控制台统一管理云主机，服务器，容器，支持模糊检索、筛选、开启防护、查看主机资产信息、安全风险等功能，方便用户快速管理服务器，需提供操作关键步骤截图。 |
| 对于重保、护网等场景，系统默认自带 200+条规则，至少覆盖可疑命令、后门进程、代理软件调用、清理痕迹、agent威胁操作、渗透常用工具、远程文件执行、操作敏感文件、访问恶意下载源、修改关键文件、进程异常写文件、进程异常shell等告警子分类，也可根据用户真实场景自定义进程链检测规则。进程链层级至少支持5 级或者支持设置第一级和最后一级设定，对进程命令行做威胁匹配，需提供操作关键步骤截图。 |
| 堡垒机# | 通过堡垒机实现对纳管服务器的访问控制，通过主机，账号，资源管理功能，实现人与设备，资源的隔离。通过定义不同的运维策略，实现对运维人员的登陆 IP，操作指令，登陆时间段进行限制，保证对服务器资源的访问安全，可控，需提供操作关键步骤截图。 |
| 通过敏感指令拦截功能，对定义好的高危指令进行拦截，阻止高危指令的执行，需提供操作关键步骤截图。 |
| 通过实时监控功能远程监管操作者当前正在进行的操作，一旦发现操作者有不当或违规的行为，具备及时响应措施，需提供操作关键步骤截图。 |
| 告警查询# | 可支持数据库操作命令（包括select、create等14个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（含开始结束日期）等，提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 汇总统计# | 实现对所有违规事件出现频率进行图形化的汇总统计分析，并提供对汇总结果的实时查询功能；可以对客户端使用的程序、客户端IP、用户名进行图形化排名展示，并生成报表，提供国家认可的第三方权威机构出具的测试报告作为证明材料。 |
| 访问控制 | 身份&权限管理：支持主账号（租户账号）、子账号、角色（用户角色、服务角色、联合身份角色）。 |
| 抗脆弱演练方案# | 结合系统编写抗脆弱演练方案及演练脚本。一次/年，需要开具带有投标人公章承诺书。 |

3. 验收标准

在合同约定的服务期剩余10个工作日内，对投标人服务情况进行验收，投标人应配合采购人进行项目验收及提交项目相关资料。验收合格后，采购人向投标人支付项目尾款。验收不合格且拒不接受整改的，采购人依法保障自身合法权益。

4. 其他要求

投标人应保证：在与采购人缔约、履约及履约结束后，投标人及投标人的工作人员(或通过第三人)不得以任何形式向采购人的工作人员行贿，包括但不限于提供金钱、回扣或其他利益，或就相关利益作出允诺，以获得缔约机会、抬高合同价款、降低合同履行标准。如存在上述情形，一经查实，采购人有权解除本合同，投标人还应向采购人支付相当于本合同已履行金额30%的违约金，如给采购人造成其他损失，投标人还应赔偿采购人的其他损失。投标人承担上述违约责任，不影响投标人和相关人员承担刑事责任。

采购人工作人员如有向投标人索要贿赂情形，投标人应及时向采购人或纪检监察机关举报。