采购需求

一、项目介绍

1、业务需求

鉴于“十四五”期间，区卫生健康信息化建设工作的积极探索和取得的可观成效,本次拟定继续应用先进的云计算技术，采用资源按月租用的方式，构建全委及区急救中心包括偏内网医疗卫生及偏外网互联网两类应用、3处核心数据中心机房、共55个重要的核心系统应用、7类卫健委原有机房的其他服务应用、和急救中心包括急救调度、院前急救电子病历在内的4类平台应用的底层基础设施建设。打造统一、安全、可靠、可信和可适应爆发型的互联网化的便民应用服务发展的朝阳健康云平台。

2、采购内容

依托公有云构建区域健康云底座，承载我委现在本地数据中心卫生健康信息系统，从而释放本地机房空间能效消耗、减少设备硬件采购、整合服务应用、聚集信息资源、减少运维升级维护人力及财务投入；对云平台基础设施进行改造，建设符合等保 2.0 三级要求和密码应用安全性评估的朝阳健康云平台和基层医疗卫生信息化应用。

本项目主要包括：健康云资源租用、本地运维服务、健康云应用运维三个部分，具体内容如下：

第一个方面：租用云平台云资源，包括卫健委的所有公共卫生、社区绩效考核、全民健康相关系统应用、OA 及其他自用系统等 55 个系统所用混合云资源。投标人所需的云服务资质详见评分表

第二个方面：保障本地数据中心各系统正常稳定的运行，通过相关本地运维体系的建设，结合构建集中式的服务管理模式，及时、准确、全面地反映与掌控本地数据中心各系统的运行状态，保障各系统的正常运行。

第三个方面：本项目在运维服务方面将构建整合 11 个区域信息系统的全生命周期、全流程、全方位的一体化系统运维管理体系。由于涉及的系统范围广、用户覆盖类型跨度广，需要通过统一运维管理规范、统一考核标准要求，更有抓

手的掌握各系统运维服务状况。系统的分类主要覆盖医疗卫生机构临床业务系统、医院端管理系统、疾控中心业务系统、国资管理系统、急救中心业务系统、管理办公类系统等。

序号	服务内容	备注
一	云平台及计算资源租用	
1	公有云资源（含专属云）	
2	云上网络安全服务	
二	本地运维服务	
1	云平台运维服务	
2	运维平台服务要求	
3	核心数据库运维服务	
4	一体机运维服务	
5	本地数据中心运维服务	
三	健康云应用运维服务	
1	区域卫生信息化系统运维服务	
2	区域心电系统软件运维服务	
3	区域 PACS 系统运维服务	
4	数字化流调系统运维服务	
5	紧急医疗救援中心三级急救网络系统运维服务	
6	急救电子病历系统运维服务	
7	卫生资产管理系统运维服务	
8	医院成本核算系统运维服务	
9	数字卫健协同平台运维服务	
10	OA 系统运维服务	
11	互联网诊疗应用运维服务	

3、采购要求

总体设计要求

朝阳卫生健康云（以下简称“健康云”）需要符合北京市信息化发展“十四五”规划的总体定位，满足全区卫生健康业务发展需要，统一部署，合理规划，对业务资源和系统结构进行优化，合理设计计算、存储、网络、安全等资源配置需求，改善目前资源分配不均衡、利用率低的情况。并托管卫健委所有服务端运维服务工作，包括云平台、数据库运行维护、卫健委及社区本地机房的全部系统和网络运维工作。同时构建整合 11 个区域信息系统的全生命周期、全流程、全方位的一体化系统运维管理体系，提供健康云应用运维服务。

健康云平台网络安全要求

通过安全的健康云建设，云计算环境本身的安全也需要符合国家相关网络安全标准，如《网络安全等级保护基本要求》中，明确要求云计算安全扩展要求，要求针对云计算的特点提出特殊保护，包括“基础设施的位置”，“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”等方面。本次选用的云平台也一定要严格参照网络安全等级保护三级标准作为基础要求。这里的主要技术思想包含两个层面，一方面是平台自身的安全防护要求，应确保平台不承载高于其安全保护等级的业务系统，所有的基础设施基于就近业务原则位于北京区域内，运维地点也应位于北京区域内，产生的相应配置数据、鉴别数据、业务数据、日志信息等存储数据均位于北京区域内；另一方面是云计算提供的安全产品向其上的租户系统提供相应的二级或三级配套的安全防护能力，包括但不限于通信传输、边界防护、入侵防范等安全机制，具备完善的容灾备份机制。

提供落实等保 2.0 的平台安全合规建设能力。初步建成面向卫生专网的网络安全动态监控能力。配合完成全区卫生健康机构等保 2.0 的合规性建设，配合实现各单位“一个中心三重防护”的建设，实现从等保 1.0 的被动防御向等保 2.0 的积极防御转变。配合卫生健康机构全面推进等级保护建设，针对系统全面展开定级评估，按照《信息系统安全保护等级定级指南》（GB/T 22240-2020），确定系统等保等级，根据不同保护等级要求，完善落实技术防护策略管理防护策略，

并配合第三方测评机构完成测评或备案。卫健委及其他各单位应在本单位业务/系统/网络架构发生重大变化调整时，立即对相应的系统进行重新定级评估，健康云按照调整后的等级进行等级保护建设。

利用健康云提供的安全能力配合各单位完善本单位应急响应管理制度与预案开发。配合卫健委开展云化网络安全意识水平调研摸底，启动全员网络安全意识教育工作计划。符合等保三级安全防护标准及满足近年护网实战要求的云数据中心平台可以规避包括但不限于传统数据中心存在数据泄露、身份凭证和访问管理不善、不安全的应用程序编程接口、系统漏洞、账户劫持、怀有恶意的内部人士、高级持续性威胁、数据丢失、尽职调查不足、拒绝服务、0 day 漏洞等方面存在安全威胁。

数据安全保护方面，因为数据是区域医疗信息化服务的能力源泉，是医疗信息互联互通、信息共享的基础，没有适合的存储模型与能力，就无法维持数据的可靠性。在健康云平台提供更为安全便捷的数据保护能力的同时，健康云应包含一套完整的存储及数据安全策略，帮助卫健委提升云上数据风险防御能力，实现核心及敏感数据可靠、安全、可控。通过与多种实时、离线计算框架、计算服务的对接方式，满足结构化、半结构化、非结构化等不同数据类型的海量数据存储需求，提供海量、高可靠、易扩展、高性价比、全面支持计算生态的数据湖解决方案。对数据进行全生命周期的管理，将本地存储和公共云存储无缝结合，具备智能分层、经济高效、易于管理的混合云架构下的存储资源服务能力。

健康云平台密码应用安全要求

自国务院办公厅、国家卫生健康委等部门颁布《关于促进“互联网+医疗健康”发展的意见》（国办发〔2018〕26 号）、《关于印发全国基层医疗卫生机构信息化建设标准与规范（试行）的通知》（国卫规划函〔2019〕87 号）、《关于印发全国公共卫生信息化建设标准与规范（试行）的通知》（国卫办规划发〔2020〕21 号）等政策文件以来，招标人为促进规范朝阳区医疗机构信息化建设、积极探索应用互联网等信息技术拓展医疗服务、业务管理等方面的空间和内容。

为了适应基层医疗卫生信息化建设标准，满足一体化的医疗卫生信息系统的实际需求，同时满足基层医疗卫生信息化密码应用及安全要求，招标人在建设过

程中，为积极落实国家相关政策文件的精神，结合北京市朝阳区区域卫生信息化系统的安全现状，分析系统需要依据等级保护第三级信息系统要求以及《信息系统密码应用基本要求》-GBT39786-2021 等相关标准的要求进行商用密码改造，充分利用国产密码技术保障网络安全等级保护制度和密码应用安全性评估的落实，科学合理地采用密码技术及其产品，确保核心密码技术和产品自主可控，从身份认证安全、通信传输安全、数据安全三方面进行商用密码改造，构建安全可控的密码技术支撑体系，提升平台的网络和信息安全保障能力。

健康云应用运维要求

目前卫健委管理和运行的各信息应用受部署方式、架构设计不同等方面的影响，无法形成统一的信息系统安全运维管理体系，以基层医疗卫生信息系统为代表的部分重要业务应用不能有效地开展信息系统运维管理，相关制度无法落实，由此造成的各类安全隐患难以解决。建立和完善卫健委医疗卫生信息系统安全运维管理体系，以保证基层医疗卫生信息系统安全管理体系，在安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理几个方面符合国家等级保护三级要求，对互联网诊疗平台增强运维服务能力。

卫健委已经对应用进行了现代化的微服务改造，而微服务优点之一就是能够快速启动和关闭微服务实例，以响应可伸缩性和服务故障事件，微服务可以打包在虚拟机镜像中，然后开发人员可以在 IaaS 层快速部署和启动服务的多个实例。对于软件升级来说，管理员只需操作和管理统一的云平台门户，批量导入升级，大大缩短了维护升级维护的时间，降低了运维难度。并且，对于目前系统组件部署位置杂乱的情况，微服务将后台组件间相互解耦，达到分门分类、高效复用的作用。同时，资源以服务模式租赁大大降低了硬件采购的一次性投入成本浪费，释放了资金投入的灵活性。通过打造健康云，可以满足卫健委及下属分中心未来系统多年的支撑作用。健康云数据中心可以消除本地数据中心设备规格、使用寿命、技术架构等问题。云底层基础设施平台采用最新的 SDX 架构，即软件定义的计算、网络、安全、运维服务等，让由于设备单节点、单链路、单模块组件、单生产节点的风险做到最低，从而实现计算资源的高可用。构建整合 11 个区域信息系统的全生命周期、全流程、全方位的一体化系统运维管理体系，提供健康云

应用运维服务。

二、项目履约时间、地点、服务期限

1、履约时间：合同签署后 36 个小时内，云平台供应商按照招标人要求开通健康云平台账号。

2、履约地点：北京市

3、服务期限：自合同签订生效之日起四个月服务期。

三、拟订云资源服务一览表

（下表中的数量为本项目招标的基准资源与服务要求，合同生效后具体的虚拟化资源与服务的数量与内容包括但不限于下表所示）

序号	产品和服务名称	单位	数量	备注
1	云主机	台	233	
2	云硬盘（SAS）	TB	415	
3	云数据库	个	18	根据招标方需求开通供应商支持的数据库
4	物理机	台	3	
5	公网带宽	个	1	
6	云专线	条	2	
7	云备份	GB	44100	
8	云主机备份	套	27238	
9	弹性文件存储	TB	25	
10	专属云	台	4	
11	主机安全	个	200	
12	日志审计	套	1	
13	云下一代防火墙	套	3	
14	云堡垒机	套	1	400 个授权，25 并发

15	SSL VPN	套	1	含 25~45 授权
16	数据库安全审计	套	1	支持 30 个 DB 实例
17	Web 应用防火墙	个	1	
18	DDoS 清洗	套	1	
19	域名保护	套	1	
20	网页防篡改	套	1	
21	漏洞扫描	套	1	

注：投标方在投标时按照以上配置进行报价（作为价格分部分进行评标），同时，将各产品的各种典型配置的单价作为投标书内容进行报价，并出具承诺折扣函。

四、云产品清单及指标要求

重要性分为“★”、“#”和一般无标示指标。★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，无标识则表示一般指标项。

1、云主机

序号	重要性	指标项	指标要求	证明材料要求
1	#	主机性能	云主机主频支持 3.0GHz，最高支持的主频可达 4.0GHz；内网最大带宽不低于 36Gbps，最高可达 40Gbps。	是
2	#	国产化	支持海光、鲲鹏、飞腾等主流国产化云主机。	是
3		主机功能	支持云主机生命周期管理，包括：创建、启动、停止、重启、释放（或删除）；支持强制停止、强制重启、停机不收费；支持根据实际使用场景进行选型创建云主机。	
4		主机功能	支持云主机的费用管理，包括：续费、退订、购买相同配置、计费模式互转等；支持到期提醒。	
5		主机功能	支持通过公共镜像、自定义镜像（私有镜像）、共享镜像等方式创建云主机；支持基于实例创建私有镜像，支持跨用户共享镜像。	
6	#	主机功能	支持云主机挂载云盘，最多可挂载的云盘数不低于 23 块，单个云盘的最大容量不低于 32TB，单盘最大 IOPS 不低于 10W；支持云盘的卸载、挂载、扩容等；支持系统盘和数据盘加密。	是
7		主机功能	支持云主机快照和云盘（系统盘和数据盘）快照；支持创建自动快照策略，为云盘周期性地创建快照备份数据。	
8		主机功能	支持绑定弹性 IP、弹性网卡，公网 IP、私网 IP；支持限制弹性 IP 数量；支持 IPv4/IPv6 双栈网络、配置网卡多队列等。	
9	#	主机功能	支持免费主机安全基础防护，至少可以提供异常登录、暴力破解、漏洞扫描等安全功能。	是
10	#	主机功能	具备云主机统一的策略管理能力，支持云主机组功能，支持强制反亲和性、非强制反亲和性、强制亲和性、非强制亲和性策略，支持云主机动态迁入/迁出云主机组。	是
11	#	主机功能	支持云主机 HA（High Available）机制，在云主机出现故障时能够检测和自动拉起，确保业务快速恢复，恢复时长分钟级。	是
12	#	主机性能	单个弹性云主机每服务周期服务可用率不低于 99.975%；同一区域内多个可用区的弹性云主机每服务周期服务可用率不低于 99.995%。	是

2、云硬盘

序号	重要性	指标项	指标要求	证明材料要求
1		功能	支持云硬盘的续订、退订；支持转换计费方式，可实现包年包月和按需付费的互转。	
2		功能	云硬盘支持多种付费方式，包括：包年包月、按需计费。	
3	#	功能	支持为云硬盘自动或手动创建快照，创建、修改自动快照策略，可通过快照回滚云硬盘；单块云硬盘可支持 40 个手动可用快照。	是
4	#	功能	支持云硬盘的批量创建和续订，支持批量删除快照和自动快照策略。	是
5	#	功能	支持为云硬盘自动或手动创建备份；支持使用备份恢复原盘、创建新盘；支持设置备份策略，支持备份策略的启动/停止。	是
6	#	功能	支持云硬盘回收站功能，可将按需计费的云硬盘在删除后进行临时保存，以提高客户在使用过程中的容错率。	是
7	#	性能	数据可用率不低于 99.95%，数据持久性不低于 99.9999999%（9 个 9）	是
8		功能	支持创建实例时加密系统盘和数据盘，支持创建云硬盘时加密数据盘。	
9		功能	支持共享云硬盘，可将同一块云硬盘挂载至多台云主机。	

3、云数据库

序号	重要性	指标项	指标要求	证明材料要求
1		数据安全	数据安全：多种安全策略保护数据库和用户隐私，例如：VPC、子网、安全组、VPN、SSL 等	
2		数据高可	数据高可靠：数据库存储支持三副本冗余	

		靠		
3	#	规格	支持最大实例规格不低于 64 核 512G	是
4	★	服务高可用	服务高可用：全主备实例，服务可用性高。 请提供控制台支持开通主备实例的证明截图。	是
5		实例访问	实例访问：多种访问方式，包括：内网 IP 访问、公网 IP 访问、VPN 访问	
6	#	实例管理与功能	支持创建数据库时指定实例 IP 地址。	是
7			支持修改数据库实例 IP 地址，投标人须在采购需求偏离表中响应。	
8			支持分钟级实现磁盘扩容，对业务无影响。	
9			支持单机一键转主备实例。	
10		实例监控	实例监控：支持监控数据库实例 OS 及 DB 引擎的关键性能指标，包括计算/内存/存储容量使用率、I/O 活动、数据库连接数、QPS/TPS、缓冲池、读/写活动等。	
11		备份与恢复	备份与恢复：备份：自动备份、手动备份，全量备份、增量备份，备份文件的增、删、查、复制等生命周期管理。恢复：恢复到备份保留期内任意时间点（Point-In-Time Recovery，PITR）/某个全量备份时间点，恢复到新实例/原实例。	
12		日志管理	日志管理：支持查看慢 SQL 日志、错误日志等。	
13	#	支持跨 AZ 部署	可用区之间内网互通，不同可用区之间物理隔离。	是

4、物理机

序号	重要性	指标项	指标要求	证明材料要求
1		功能	支持 VPC 网络和自定义网络通过 VPC 内的私有网络，实现裸金属服务器和云服务器之间、裸金属服务器和裸金属服务器之间的网络互通。	

2		功能	弹性裸金属支持云硬盘的挂载、卸载和扩容等操作，支持连接文件存储和对象存储，满足对弹性存储的要求。	
3		功能	支持国产化操作系统。	
4		功能	支持国产化服务器，包括鲲鹏、海光等国产化架构。	
5		功能	支持 GPU 物理机，支持的 GPU 卡包括 A100、A800、H800、昇腾 910B 等。	
6		功能	支持绑定、解绑、删除辅助弹性网卡；支持挂载多块弹性网卡。	
7		功能	弹性裸金属支持弹性网卡，支持单网卡多私有 IP。	
8	#	功能	裸金属服务器支持动态 Raid 配置，用户在开通时根据需求选择合适的 Raid 类型，以满足不同的存储配置需求。	是

5、共享带宽

序号	重要性	指标项	指标要求	证明材料要求
1		功能	支持按需按带宽、包年包月计费。	
2		功能	支持绑定云主机、物理机、负载均衡、NAT 网关等实例。	
3	#	功能	支持出/入方向流量、带宽监控和查询。	是
4		功能	支持出/入方向流量监控支持自动刷新。	
5	#	功能	支持 IPv4/IPv6。可以绑定 IPv6 双栈网卡，让 IPv6 公网 IP 复用带宽。	是
6		功能	弹性 IP 移出共享带宽时，可配置移出时的带宽。	

6、云专线

序号	重要性	指标项	指标要求	证明材料要求
1	#	性能	云专线端口带宽支持 10G/40G/100G。	是
2		功能	支持费用管理，包括：订购、续订、退订等	
3	#	功能	支持独享和共享物理端口模式。	是
4	#	功能	支持 IPRAN、PON、OTN、CN2、MSTP、IP 虚拟专网等多种专线类型接入。	是
5	#	功能	支持 IPV4 单栈通信、IPV6 单栈通信、IPV4/IPV6 双栈通信。	是
6	#	功能	支持多条物理专线接入，可选择主备、负载方式，支持配置优先级。	是
7	#	功能	支持端口聚合。	是
8		功能	支持端口限速、端口带宽升降配。	
9	#	功能	支持一条物理专线同时访问多个 VPC。	是
10	#	功能	支持多条物理专线同时访问同一个 VPC。	是
11	#	功能	支持健康检查实现链路探测及路由快速收敛。	是
12		性能	云专线端口每服务周期的可用性不低于 99.95%	

7、云备份

序号	重要性	指标项	指标要求	证明材料要求
1		功能	支持备份客户端订购、续订、扩容	
2		功能	支持备份存储库订购、续订、扩容、退订	

3		功能	支持创建、删除、查看、修改备份计划	
4	#	功能	支持云主机中的目录/文件备份	是
5		功能	支持基于策略的周期性自动备份，最小备份周期为 1 小时	
6		功能	支持用户手工触发备份	
7		功能	支持备份数据重删（删除多余的重复数据）	

8、云主机备份

序号	重要性	指标项	指标要求	证明材料要求
1	★	功能	支持全量备份或增量备份可以将云主机的数据恢复至备份副本所在时刻的状态。请提供官方文档介绍的证明截图。	是
2		功能	支持通过云主机备份数据申请新云主机。	
3		功能	支持云主机的全量和增量备份。	
4		功能	支持周、天的备份周期设置，支持按数量、时间、永久策略进行备份保留。	
5		功能	备份数据可跨 AZ 恢复。	

9、弹性文件存储

序号	重要性	指标项	指标要求	证明材料要求
1	#	功能	支持 NFS v3 v4.1 和 CIFS SMB v2.1、v3.0 协议，满足不同操作系统环境的需要。	是
2	#	功能	支持 SFS Turbo 标准型、SFS Turbo 性能型、SFS Turbo 标准型专属规格，满足不同用户场景的需要。	是

3		功能	支持创建、删除、搜索、筛选、挂载、名称修改等文件系统管理功能。	
4		功能	支持文件系统容量调整，支持文件系统扩容。	
5		功能	支持创建、修改、查询、删除等权限组管理功能，最大支持 20 个权限组。	
6	#	功能	支持文件系统快照，用于文件系统恢复与备份。	是
7		功能	支持文件系统服务端加密，支持 KMS 加密。	
8		功能	数据存储采用多副本、纠删码等冗余模式，单存储节点损坏不会导致数据丢失。	
9		功能	支持 IPv4 和 IPv6 网络访问文件存储服务。	
10	#	功能	服务可用性达 99.95%，数据持久性达 99.99999999%（10 个 9）。	是

10、专属云

序号	重要性	指标项	指标要求	证明材料要求
1		计算隔离	独享计算资源池，部署在独立的物理集群中，确保云主机资源运行在物理隔离的专属计算资源池内。	
2		灵活部署	支持多区域，多可用区，多计算集群部署，集成对接专属分布式存储，用户可自配置网络，提供安全组策略，方便用户构建立体防护网络。	
3		灵活创建	用户可指定不同专属计算池，不同专属物理机进行弹性云主机创建。	
4		资源管控	用户可以查看专属计算集群下的物理机列表和计算资源总量和消耗量以及物理机上弹性云主机的列表，用户能直观的查看和管理计算资源。	

11、主机安全

序号	重要性	指标项	指标要求	证明材料要求
1		功能	支持的操作系统：Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、win xp 、win 7、win 8、win 10、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、Ubuntu 14 +等。	
2	★	功能	支持对防护资产的CPU使用率、内存使用率、磁盘使用情况、网络上下行流量进行性能监控，并支持对性能监控项设置阈值，达到阈值后告警；支持对CPU、内存达到一定阈值时客户端进行熔断。请提供功能界面证明截图。	是
3	#	功能	支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。	是
4	#	功能	识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。	是
5	#	功能	可对渗透的收尾阶段的数据清除行为进行识别和阻断	是
6	#	功能	支持防端口扫描，锁定恶意的端口扫描，并记录告警。	是
7	#	功能	支持网站漏洞防护，防护内容包括SQL注入、XSS攻击、应用程序漏洞及自定义规则	是
8		功能	支持智能检测并防御CC攻击，并可进行高、中、低三档设置。	
9		功能	支持病毒立即处理，对于无法普通隔离的病毒文件进行处理并加入隔离区，或动态移动到信任区。	

10		功能	支持文件实时监控，在文件执行、文件修改、存储介质连接时可自动触发病毒扫描。	
11		功能	支持病毒库、Windows 补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级。	
12	#	功能	篡改规则：支持基于目录、进程、IP、用户等进行设置篡改规则	是
13	#	功能	支持对屏幕拍照泄密数据的行为进行溯源。	是
14	#	功能	提供专门的挖矿风险评估功能。	是

12、日志审计

序号	重要性	指标项	指标要求	证明材料要求
1	#	主备切换	支持系统主备切换，在主机工作时，部署备机实时心跳监控主机状态，发生意外时主备替换，避免因意外导致的数据丢失，提高设备稳定性。	是
2	#	国产化	支持系统采集国产化操作系统日志，包括但不限于：中标麒麟、银河麒麟、统信等。	是
3	#	日志接入	支持系统规则自适应日志接入，仅输入 IP 范围及端口即可自动匹配相应规则，完成日志自动接入。	是
4	#	日志转发	支持系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息。	是
5	#	自定义查询	支持系统自定义查询条件，可指定多个查询条件进行组合查询，并可将查询条件存储为快速检索模板。	是
6	#	事件分类	支持系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别。	是
7		重复归并	支持对收集到的重复日志进行归并，以减少日志存储资源消耗	
8		日志过滤	支持自定义配置将用户不关心的日志进行过滤	
9		统一处理	系统应能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据	
10		提取方式	系统应支持正则、KV、CSV、格式串等多种灵活的提取方式	

11		监控配置	系统应支持对资产进行监控配置，包含资源监控、采集监控、采集限速等	

13、云下一代防火墙

序号	重要性	指标项	指标要求	证明材料要求
1	#	安全策略	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、数据过滤、文件过滤、AV、URL 过滤和 APT 防御等）统一界面进行安全策略配置。	是
2	#	策略优化	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。	是
3	#	入侵防御	支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。	是
4	#	抓包分析	支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证。	是
5	#	病毒检测	支持基于文件协议、邮件协议（SMTP/POP3/iMAP)、共享协议（NFS/SMB）的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。	是
6	#	防泄露	支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证号、信用卡号、银行卡号、手机号等类型进行匹配。	是
7		报文捕获	支持基于接口及 IP 的报文捕获，并将捕获到的报文生成 Wireshark（一种网络封包分析软件）可识别的.cap 后缀文件，保存到本地或外部服务器，供用户分析诊断出入设备的流量。	
8		报文示踪	支持报文示踪功能，支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和连接数限制等）对报文的处理过程，通过查看报	

			文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。	
9		故障诊断	支持 IPsec 故障诊断功能，应支持至少三种诊断模式：数据流、接口、IP 地址。用于检测 IPsec 连接的状态，当 IPsec 连接发生故障时，可以协助用户排查 IPsec 配置中的问题，并提供可能的原因。	

14、云堡垒机

序号	重要性	指标项	指标要求	证明材料要求
1	#	状态统计	支持用户状态统计：支持用户账号状态统计，至少包含用户账号上次登录时间、已禁用的用户账号、用户账号有效期等。	是
2	#	角色划分	支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。支持自定义用户权限。	是
3	#	组织架构	支持按部门组织架构（至少 5 个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。	是
4	#	客户端	支持 Windows/Mac 操作系统下 C/S 架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。	是
5	#	自动登录	支持设备帐户和密码的自动登录、手工登录、二次自动登录模式。	是
6		运维管理	支持 B/S 架构进行堡垒机运维管理，至少支持使用 IE、谷歌、火狐等浏览器打开堡垒机的 Web 页面直接调用 mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX 等本地运维客户端工具；	
7	#	实时监控	实时监控：支持对文件传输会话的实时监控	是

8		运维规则策略	运维规则策略：支持通过基于时间、IP/IP 段、用户/用户组、主机组、主机账号、命令控制策略等组合访问控制策略，授权用户可访问的目标设备	
9		二次审批	对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录；并且管理员在审批时可以设置审批有效期，及在有效期内是否不限制登录次数。	
10	#	批量登录	支持批量登录字符设备功能：能自动生成 SecurCRT/Xshell 工具的批量登录文件，实现在工具中批量自动登录多台设备	是
11		运维方式	H5 运维方式：支持 ssh、telnet、rlogin、rdp、vnc 协议的 H5 运维，无需本地运维客户端工具	
12		定期修改	支持定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能	

15、SSL VPN

序号	重要性	指标项	指标要求	证明材料要求
1	#		支持国际商用加密算法，用户可根据业务系统重要程度按需选择加密算法和密钥长度。通过标准加密算法保障数据传输安全。	是
2		易用性	可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP 地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果。	
3			支持文档 WEB 化管理，用户可通过任意浏览器，对存储服务器的文件进行管理操作（包括：上传、下载、删除、重命名、剪切、复制、粘贴、新建文件目录），而不需要额外安装 FTP、文档共享软件等应用程序客户端。	
4	#		提供独立日志中心，可以详细记录接入用户的访问行为，确保用户的访问过程可追溯。同时可以提供详尽报告，作为网络规划的依据。此外日志中心具备管理员权限分级功能，提高了管理安全性。	是

5		权限、服务器安全	产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。	
6			针对服务器地址保护方面，可支持 SSLVPN 资源列表界面上的用户授权资源隐藏；针对 B/S 应用，可进行 URL 地址伪装，防止服务器真实 IP 地址泄露	
7	#	身份认证	产品必须支持 Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 。	是
8			针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果。	

16、数据库安全审计

序号	重要性	指标项	指标要求	证明材料要求
1		部署方式	支持通过安装agent 的方式进行旁路审计	
2		关系型数据库	支持Oracle（包括21C版本）、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ、Vertica、Tidb、PolarDB、PolarDB-X、达梦、金仓等主流数据库的审计	
3	#	非关系型数据库	支持MongoDB、Hbase、Hive、Impala、Elastic Search、HDFS、Canssandra、greenplum、LibrA、graphbase、cache、Redis、HANA、ArangoDB、Neo4j、OrientDB等非关系型数据库审计	是
4		主流业务协议	支持主流业务协议HTTP、HTTPS、Telnet、FTP的审计	
5		操作审计	支持数据库操作类、表、视图、索引、存储过程等各种对象的所有SQL操作审计	
6	#	审计信息	审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集	是
7		双向审计	支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小	
8	#	内置规则	产品具有内置规则，规则类型有sql注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警；	是

9		审计规则	可自定义审计规则，审计规则至少支持18个条件；	
10	#	安全规则	支持内置安全规则单独升级	是
11		查询功能	具有高效的查询性能，后台采用全文检索引擎检索	
12	#	过滤规则	支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单	是
13		审计查询	支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询；	
14	#	检查条件	设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源IP、目的IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想；	是
15	#	告警分析	支持告警分析功能，告警支持按照源IP和数据库账号对SQL模板维度进行排行，支持在页面一键去除规则、添加规则白名单	是
16		模板库	系统内置多种报表模板库，报表类型不少于20种；	
17		综合报告	支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；	
18		性能分析	支持性能分析，准确提炼出SQL语句执行频率和执行时间异常的报表；	

19		信息钻取	支持报表页面信息钻取	
20		报表导出	支持HTML、PDF、PNG等格式的报表导出	
21	#	告警日志	可依据客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志；	是

17、Web应用防火墙

序号	重要性	指标项	指标要求	证明材料要求
1		吞吐量	提供的产品应用层吞吐量不能小于 1000 Mbps，最大并发连接数（http）不能低于 100 万，每秒最大新建连接数（http）不低于 26000。	
2	#	HTTP	支持 HTTP 1.0/1.1，且可根据现网环境配置协议降级。	是
3	#	白名单机制	支持基于规则体系构建黑名单安全策略和自学习白名单机制；支持基于智能用户行为识别的动态防护机制；产品自学习应该能够支持 host,url,http method,请求响应码，请求参数名称及其对应的值，cookie 参数名称及其对应值等信息。	是
4	#	黑名单机制	支持基于规则体系构建黑名单安全策略和自学习白名单机制；支持基于智能用户行为识别的动态防护机制；产品自学习应该能够支持 host,url,http method,请求响应码，请求参数名称及其对应的值，cookie 参数名称及其对应值等信息。	是
5	#	攻击防护	支持 ARP 攻击防护，支持 MAC 地址绑定。	是
6	#	五元组	支持基于五元组（源 IP 地址、目的 IP 地址、源端口、目的端口、协议类型）及接口的网络层访问控制功能。	是

序号	重要性	指标项	指标要求	证明材料要求
7		检测处理	支持对 HTTP 协议合法性进行验证，支持对 HTTP 协议的 URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理。	
8	#	控制策略	支持 HTTP 访问控制功能，可以提供针对 HTTP 元素和客户端的组合访问控制策略。支持对多种 HTTP 方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY 、 MOVE 、 OPTIONS 、 PROPFIND 、 PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT。	是
9	#	盗链防护	提供盗链防护，应采用 Referer 和 Cookie 算法。	是
10	#	注入防护	支持对注入（包括 SQL 注入、LDAP 注入、XPATH 注入及命令行注入）、XSS、SSI 指令、路径穿越、远程文件包含、WebShell 防护。	是
11		CSRF 防护	支持 CSRF（跨站请求伪造）防护，并支持 WEB2.0 CSRF 防护。	
12	#	安全检测	支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell 、 Linux shell 、 Power shell(windows Script File) 、 Java shell、Asp shell、Perl shell、Python shell 及 Ruby shell，同时可支持源 IP 封禁、Session 封禁和 UA 封禁。	是
13		限制策略	支持非法下载防护，可以根据文件大小、MIME 类型及文件扩展名灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等）。	
14		防护算法	支持 Cookie 安全机制，包括 Cookie 加密和 Cookie 签名的防护算法。支持过期兼容时间配置以及*配置。	
15		安全策略	支持信息泄露防护，提供针对服务器状态码进行过滤和伪装的安全策略。	
16		内容过滤	支持内容过滤，提供恶意代码过滤功能。	

序号	重要性	指标项	指标要求	证明材料要求
17		隐私检测	支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换。	
18		SOAP 校验	支持 XML 防护，包括 XML 基础校验、Schema 校验以及 SOAP 校验。	

18、DDoS清洗

序号	重要性	指标项	指标要求	证明材料要求
1		防护协议	支持 TCP、UDP、ICMP 网络协议防护，如 SYN Flood ，ACK Flood，空连接等。	
2		报文过滤	支持对 Ping of Death、Tear Drop、LAND、Fraggle 等畸形报文进行过滤，判断报文合法性，丢弃异常请求。	
3		黑白名单	可针对 IP，IP 段，IP 端口，URI，METHOD，请求地区，请求参数，请求头部，请求协议等维度进行组合，设置白名单和黑名单，对请求进行拦截和放行，保证客户网站不受未知访问。	
4		特定统计	支持针对特定报文（十余种粒度组合），选择 URL、ARGS、Header、Cookie、UA、IP 其中一个或两个粒度进行频率统计，并设置对应的处理动作，以对高频请求进行控制。	
5		CC 告警	支持自定义 CC 攻击告警策略，对持续时长、QPS 峰值、攻击次数进行监控和告警。	
6		自动接入	支持 HTTP、HTTPS、HTTP2 协议的域名进行自助接入配置。 支持自定义回源 HTTP 请求头。 支持多个源站或域名回源，并对源站设置层级和权重。 支持指定回源协议或配置跟随协议。 支持请求强制跳转，即将请求的 HTTP 强制 302 跳转至 HTTPS 进行请求。	

19、域名保护

序号	重要性	指标项	指标要求	证明材料要求
1			对域名池中需要监控的域名信息进行定期的采集和对比，发现域名解析异常后，及时通知，确保使用方在第一时间获取域名解析错误的告警提示。	
2			域名因遭到劫持或误操作等原因导致业务不可用时，可通过域名快速修正服务，秒级完成使用方电信全网缓存 DNS 服务器的刷新动作，同时可实现微信自主操作，确保域名得到快速修正。。	

20、网页防篡改

序号	重要性	指标项	指标要求	证明材料要求
1		网页文件自动同步功能	系统可以从本地或异地备份文件夹自动同步到监测目录内。	
2		支持多虚拟主机 / 目录的并发同步	系统支持多虚拟主机 / 目录的并发同步功能。	
3		网站管理	可支持对 web 服务器的远程维护管理功能，如远程接管、远程唤醒、远程关机、远程用户注销等。	
4		网页分类	支持对各类网页文件分类。	

21、漏洞扫描

序号	重要性	指标项	指标要求	证明材料要求
1			支持 IPv4 和 IPv6 环境的部署和扫描	

2			许最大并发扫描≥60 个 IP 地址，允许最大并发任务≥10 个任务，支持无限 IP 授权扫描。	
3			产品应支持多路扫描功能，可以同时对多个隔离业务子网进行扫描。	
4			支持检测的漏洞数大于 250000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准，并提供 CVE Compatible 证书。	
5			产品支持对系统漏洞扫描、web 漏洞、配置合规进行检查和综合分析，可输出同时包含漏洞扫描和配置核查结果的报表。	
6			同时支持远程扫描和采用 SMB、SSH、Telnet、RDP、HTTP、HTTPS、WinRM 等协议对 Windows、Linux 等系统进行登录扫描。	
7	#		提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。	是
8	#		支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞。	是
9	#		具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、RDP、SSH、Telnet、SQL SERVER、MySQL 、Oracle、Sybase、DB2、MongoDB、Memcached、Redis 、PostgreSQL 、HighGo 、UXDB 、Kingbase 、STDB 、FTP、SFTP、ActiveMQ、POP3、Tomcat、SMTP、IMAP、Onvif、RTSP、 SNMP、SIP、Vmware ESXi、HTTP Digest、Weblogic、Elasticsearch、Websphere 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。	是
10	#		支持认证信息管理，可将系统登录信息、配置检查模板进行统一管理和配置，提供登录信息导入功能，无须每次下任务时进行配置。可跟堡垒机联动获取账户的密码，支持登录信息的批量更新和全部更新。	是
11	#		支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。	是
12	#		支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义。	是
13	#		支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容。	是

14	#		支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析,并可在线查看同一 IP 的多次历史扫描结果。	是
	#		提供灵活的报表自定义，可定制报表标题、封面 logo、报表页眉和页脚、报表各章节显示内容	是

五、本地运维服务清单及指标要求

重要性分为“★”、“#”和一般无标示指标。★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，无标识则表示一般指标项。

投标人应提供详细的系统技术支持和售后服务体系说明，包括服务的对象、内容、方式、时间等,并能够根据招标方业务需要进行服务及级别的调整和完善。请详细说明如下要求满足的程度,提供服务响应偏离表并说明各项服务的满足情况。需要在投标人提供的售后服务承诺函中详细体现，否则均认定为不满足该项要求。

序号	指标项	规格要求		重要性	证明材料要求
1	云平台运维服务要求	提供 7×24×365 热线电话支持，提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。		#	是
		提供 7×24×365 云产品工单支持，解答客户在使用中的问题。提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。		#	是
		提供 7×24×365 故障实时响应支持。提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。		#	是
		两会以及安全日历定义的		#	是

		重保日提供重保服务			
		提供支持相应的API与SDK，帮助文档、云社区/消息订阅等服务			
		提供在线培训课程			
		提供1名专属驻场技术服务经理,提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。		#	是
		提供并保证能够联系到客户专属联系人，联系人在明确故障后立即进行反馈。投标人须在采购需求偏离表中响应。		#	是
		提供资深技术专家团队二线支持进行部署与故障处理。投标人须在采购需求偏离表中响应。		#	是
		提供对第三方软件支持，配置指导及协助故障排除等			
		提供架构咨询服务，包括但不限于： 分析业务系统特点，根据业务系统数据规模、用户量、访问量、业务特点协助客户完成需求评估、产品选型和资源规划，完成应用上云方案和部署建议。 系统需要做改造的场景下，提供上云改造方案建议，提供面向互联网、高并发、海量数据的企业 IT 架构设计与咨询。 针对不同的业务场景设计系统迁云方案，包括应用迁移（镜像迁移，直接部署），系统容量设计，云上高可用设计，负载均衡设计，同城容灾方案，域名配置等。 针对客户场景设计基于关系型数据库(ORACLE/MySQL/MSSQL 等)到云平台的数据库迁移方			

		案，最小化数据库迁移的停机时间。 针对客户场景设计基于非结构化存储（图片/视频/文件等）数据到云平台的迁移方案，提供相应的全量迁移方案和系统改造支持。 云上的网络设计与规划，包括专有网络，混合云架构，专线或 VPN 实施方案设计，专有网络内包括 IP 地址规划，虚拟交换机规划，路由策略规划，安全组规划等，确保初始方案符合安全、网络业务互通及弹性扩展的要求。 根据应用系统对停机时间的要求制定业务割接方案，包括演练、业务正式割接、业务回滚方案等，从方案保障系统割接的顺利进行。			
		提供重大活动保障服务，每年 2 次，根据招标方申请的时间提供			
		定期组织与客户技术研讨，定时优化整体服务能力与方案，针对业界突发事件（如安全漏洞、病毒），主动联系招标方协助处置干预			
		产品相关的技术问题和故障诊断 与云平台资源相关的操作或问题系统的诊断。 API 和 SDK 问题的故障诊断			
		提供在紧急、重大事件发生时的人工应急服务及重保方案，配备专门团队紧密配合项目实施工作，包括但不限于： 非工单流程的应急响应； 业务应急预案设计； 应急风险评估与优化； 应急服务分析和总结报告； 针对不同级别的系统故障，			

		给出明确的响应时间和故障解决周期故障发生后，根据投标人与招标方后期规划的核心与非核心系统设计提供不同的响应处理时间和反馈处理结果服务： 核心系统不可用时间＜2 小时 非核心系统不可用＜10 小时			
		协助完成新老应用系统的割接，确保迁移上云后的应用系统可以稳定、高效的在运行在云平台上。			
		投标人应熟悉中标方云平台的各项功能，配合进行调整部署拓扑、产品配置等。投标人须在采购需求偏离表中响应。		#	
		需配合第三方测评单位完成等保三级测评相关工作。投标人须在采购需求偏离表中响应。		★	是
		对服务有关内容承诺保密，保证所有资料不外泄。 投标方工作人员在进行维护的相关操作时，应当遵守招标方的相关运行维护规定，并在事前征得招标方同意。投标人须在采购需求偏离表中响应。		★	是
2	运维平台服务要求	具备完全自主知识产权，避免潜在的版权纠纷，具有产品软件著作权；		#	是
		提供资产管理的服务，服务支持主机、网络设备、中间件、软件等计算机资源管理。覆盖网络、IaaS、PaaS、SaaS 以及应用服务。 支持单独和批量维护资产信息，导出资产信息；支持各类软硬件和系统资产管理，如主机，网络、安全设备，组件，应用，链路等。			

		提供资产监控的服务，服务支持网络层监控、IaaS 层监控、PaaS 层监控、SaaS 层监控、应用服务监控、日志监控、链路监控。			
		提供监控告警的服务，服务支持配置告警执行的作业计划、告警接收人、告警消息模板等内容，并支持邮件、短信、语音等多种告警推送方式。			
		提供资产巡检的服务，服务支持通过界面化操作自动执行周期性、重复性、未来性的任务，支持定义任务内容和任务执行时间。			
		提供健康报告的服务，服务支持对资源生成系统健康报告，支持按每天/周/月定期生成报告发送给指定接收人。服务支持通过图表等方式展示，掌握系统运行状况的变化趋势，识别潜在风险，提出预防建议。			
		提供大屏展示的服务，服务支持网络层面、基础设施、链路状况、资产指标等的大屏展示。			
		提供远程管理的服务，服务支持远程操作的资源各项信息，可以在线打开主机终端，进行文件的远程传输以及远程执行脚本任务。			
		提供流程管理的服务，服务支持内置告警流程，产生告警之后可以同步产生工单，同时支持自定义表单，自定义流程，进行工单的流转。			
3	核心数据库运维服务要求	数据库专家对云数据库实例针对容量、性能、容灾、安全等维度进行全方位的健康诊断，出具专业的健康诊断报告，为采购人决策管理提供依据。需提供健康诊		#	是

		断报告模板证明。投标人须在采购需求偏离表中响应。			
		数据库专家提供在线护航服务，为数据库应用系统进行性能和风险评估，并提供对应的优化或扩容方案，提供数据库维护方面专业建议，共同保障渡过业务高峰期。			
		数据库专家现场保驾护航，为用户的数据库应用系统进行性能和风险评估，参与配合进行数据压测演练，提供数据库优化方面专业建议，在业务高峰期共同保障数据库系统平稳运行。			
		数据库专家应急响应，提供紧急救援服务，帮助快速解决数据库服务不可用、性能瓶颈、数据丢失等问题。 提供 7x24 小时紧急救援。			
		针对数据库版本管理及补丁升级提供服务方案。包括：版本管理定义及补丁升级服务类型、版本管理及补丁升级服务内容、版本管理及补丁升级服务流程。			
		针对数据库安全管理及加固服务要求，提出服务方案。包括：数据库安全评估、数据库安全评估扫描结果甄别、安全加固、基线检查服务。投标人须在采购需求偏离表中响应。		#	是
4	一体机硬件运维服务要求	提供 7×24 小时电话、电子邮件、咨询服务。			
		技术支持要求：提供硬件更换服务及软件支持服务。提供一体机主要硬件的检测及损坏硬件的更换服务，运行于一体机数据库的故障处理、性能优化、数据迁移、备份恢复、补丁分析管理、安装部署等技术支持服务。			

		应急支持服务：在重要时间窗口、应用系统重大升级时提供现场技术支持服务。			
		定期巡检要求：提供以月度为单位周期对一体机软硬件进行健康状况检查			
		服务响应时间：根据故障紧急程度不同，应按以下时限完成故障处理： 紧急故障：立即响应并在 20 分钟内登录系统，1 小时内修复故障。 严重故障：立即响应并在 30 分钟内内登录系统，4 小时内修复故障。 一般故障：接到故障通知后，30 分钟内登录系统，24 小时内修复故障。			
5	本地数据中心运维服务要求	值守要求：采用驻场服务方式，提供 1 名驻场工程师；服从招标方的调度和安排，接受服务单位的监督。提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。		★	是
		技术支持要求：提供 7*24 小时的远程技术支持；提供 7*24 小时的电话技术支持；提供 5*8 小时的现场支持服务。提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。		#	是
		定期巡检要求：运维工程师定期完成服务范围内各系统的巡检，并按月度提交运维工作报告。			
		突发事件处理：遵守招标方应急响应机制，对突发事件及时汇报和处理。			
		服务响应时间：要求提供专用报修电话技术咨询，如果电话技术支持不能解决问题，将派出技术人员到现场		#	是

		协助解决，根据系统故障的程度提供不同的响应时间和故障排除时间： 一般故障，响应时间≤4 小时，故障排除时间≤8 小时； 严重故障，响应时间≤2 小时，故障排除时间≤4 小时； 系统紧急故障，响应时间≤15 分钟，故障排除时间≤2 小时。 提供售后服务承诺函中必须包含此内容以证明。投标人须在采购需求偏离表中响应。			

六、健康云应用运维清单及要求

对朝阳区 11 个系统进行运维服务，对业务系统运维展开统一运维管理，兼顾业务系统应用价值和数据价值。系统范围广、用户覆盖跨度广，需要通过统一运维管理规范、统一考核标准要求，更有抓手的掌握各系统运维服务状况。运维系统主要覆盖医疗卫生机构临床业务系统、医院端管理系统、疾控中心业务系统、国资管理系统、急救中心业务系统、管理办公系统。

1. 区域心电系统软件

朝阳区现运行的“区域心电图系统”区域内设立 3 个中心医院，连接区域内社区卫生服务中心、社区卫生服务站，为下属社区卫生服务中心提供静息心电，动态心电的远程会诊服务，实现区域内分诊落地的实施，让病人在社区就能享受到三甲医院的诊断服务，动态优化医疗资源。系统主要功能为：常规心电图和动态心电图检查和远程诊断服务；其运行环境为：Windows PC，其应用范围为：常规心电图和动态心电图。

运维服务要求：

1、针对业务系统由于硬件、软件更换、生产大楼搬迁等原因需要进行业务系统迁移等情况，由工程师现场对业务系统进行重新部署、数据导入，使系统恢复正常运行状态。

2、根据需求，在发生核心业务系统不可用事件时，提供紧急救援服务，最大

限度确保业务连续性及数据完整性。如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。针对这种情况设计了突发事件应急策略。

2. 数字化流调系统

主要针对朝阳区疾病预防控制中心的数字化流调系统进行运维服务，运维服务内容包括软件和硬件两部分服务，1）软件主要是：运行系统的保障性维护(日常监测、定期巡检、电话支持、系统软件补丁升级)、处理突发应急事件、系统性能优化服务、数据服务；2）硬件主要是：硬件系统的运行状态和故障情况、配置信息、定期巡检、可用性情况和健康指标。系统主要功能包括常规监测（报告卡管理、传染病病例订正、访视任务管理等）、流行病学调查（流调任务响应管理、流调个案管理、公共卫生事件管理、样本采集检测管理、协作任务管理等）、基础报表管理、统计分析、系统管理等内容。

运维服务要求：

1、根据系统功能和网络运行环境调整，对系统代码和配置进行调优，及时修正系统运行中出现的问题。

2、针对运行过程中发现的程序问题，及时予以改正，根据用户要求对系统功能进行完善并测试，并在使用过程中更改 Bug，应形成书面分析报告文件，提交客户验收确认。

3、突发应急事件处理：为保证系统的连续运行，成立安全、系统、主机等资深专家在内的应急响应小组，制定响应预案和流程，并在应急事件发生时进行及时处理，保护关键业务免收重大故障或灾难的影响。

3. 医院成本核算系统

主要对朝阳区 4 家区属公立医院的成本核算系统进行维护服务，保证朝阳区属医院成本核算软件与北京市卫健委关于区县成本 36 家试点医院科室成本核算软件版本一致，并同步进行软件升级和系统优化。在提供医院成本核算系统运维服务过程中，对医院相关人员进行业务指导和咨询；排除医院成本核算系统运行中发生的故障、修复软件 BUG、维护系统日志、解决软件使用过程中的问题。服

务的四家区直属医院是：北京市朝阳区第一中西医结合医院、北京市朝阳区第三医院、北京市朝阳区妇幼保健院、北京市朝阳区双桥医院，运维服务的系统是医院成本核算系统。

运维服务要求：

1、排除医院成本核算系统运行中发生的故障、修复软件 Bug、维护系统日志、解决软件使用过程中的问题。

2、工作时间内提供 5*8 小时的客户服务热线（电话回访、电话技术支持等），当系统出行严重故障时，提供现场支持服务。

4. 卫生资产管理系统

主要针对朝阳区卫生国有资产管理中心的资产管理系统进行运维服务，结合区财政局、区卫生健康委等主管部门对本区卫生系统资产管理工作需要，为确保资产管理业务应用系统正常稳定运行，各项操作服务正常使用，业务流程顺利执行，避免数据损坏、丢失。需要提供运维服务工作，主要包括：系统升级、功能优化改造、运行保障、数据定期备份、用户培训等，保障系统正常稳定运行。

运维服务要求：

1、重点服务期运维保障服务。在两会期间、各节假日等重要时期，提供系统服务关停、系统运维服务、系统重启等服务。对系统运行状态监控服务，保障系统稳定运行等工作。

2、运维服务安全管理。根据卫健委信息管理安全工作要求，对系统出具的安全整改已经，对资产管理系统进行系统安全相关的维护工作，并且根据安全管理要求整改措施的相关规定进行调整，确保系统安全稳定。

5. 紧急医疗救援中心三级急救网络系统

主要对北京市朝阳区紧急医疗救援中心 120 指挥调度系统（以下简称“朝阳 120 系统”），提供运维服务。运维服务内容主要为朝阳 120 系统软硬件设备的提供日常维护、定期维护（每星期提供一次系统巡检服务）、故障处置，应急保障等。

运维服务要求：

1、维护管理服务进行故障响应。7*24 小时保障，系统出现运行故障时 2 小时内到达现场排查，提供解决方案，恢复正常运行。软件故障排除时间不超过 24 个小时，硬件故障排除时间不超过 48 小时。

2、设备终端故障响应。按照故障申报维修方式进行维保，故障报修 4 小时内处理完毕，出具故障处理报告。

6. 区域卫生信息化系统

自 2011 年以来的持续建设，为满足和保障朝阳区社区医疗机构日常基本医疗和公共卫生工作的开展需要和管理需要，在区域卫生信息化方面有将近 50 个系统需要定期维护。这些系统与社区日常工作开展息息相关，一旦出现问题或者瘫痪，将对会严重影响社区业务开展，造成不必要的经济损失和不良的社会影响。另外，根据国家、北京市、朝阳区的各项政策要求，需要对各系统内的系统进行持续性改进和完善，让所建系统和资源最大程度被使用因此，才能更的支持社区基本医疗与公共卫生工作的顺利开展，保障卫计委对社区考核及监管工作的顺利进行，支持家医签约、双向转诊，医养结合等各项工作顺利开展。提供各项运维工作的服务，满足系统日常维护需求，及时解决系统运行中的各种问题，保障系统正常运行。服务范围：北京市朝阳区卫生健康委员会下属 53 家社区卫生服务机构；软件范围：为已实施部署的系统进行维护，清单如下：

序号	用户单位	系统
1.	朝阳区社区卫生服务中心	门诊挂号收费信息系统
2.		门诊医生工作站
3.		门诊药房信息系统
4.		门诊医技执行系统
5.		入出院与住院结算系统
6.		病区护士站信息系统
7.		住院医生工作站

序号	用户单位	系统
8.		药库管理信息系统
9.		住院药房信息系统
10.		医保接口系统
11.		管理员维护信息系统
12.		多媒体导医台
13.		物资管理系统
14.		自助挂号系统
15.		自助择医系统
16.		综合服务台
17.		检验信息系统
18.		社区卫生服务机构检验条码管理系统
19.		社区卫生服务中心综合管理平台
20.		区域体检系统
21.		社区公共卫生服务系统
22.		社区卫生服务中心中医药服务综合管理系统
23.		社区卫生服务机构门诊分诊系统
24.		社区卫生服务机构医技预约系统
25.		社区卫生服务机构血透接口
26.		社区卫生服务机构全自动发药机接口
27.	朝阳区社区卫生服务	社区卫生服务绩效考核平台

序号	用户单位	系统
28.	管理中心	区域处方考核管理系统
29.		朝阳区社区卫生服务常规监测数据报送平台
30.		社区卫生服务中心综合管理平台
31.		互联网诊疗医院接口
32.	朝阳区卫生信访中心	朝阳区卫生信访信息管理平台
33.		朝阳区计生信访信息管理系统
34.		北京市朝阳区卫生计生信访留证系统
35.	朝阳区社区卫生服务中心、区属二级以上医院	数据共享与交换平台
36.		健康档案EHR管理系统
37.		区域双向转诊系统
38.		二级医院HIS接口
39.		社区服务中心 HIS 系统接口
40.	朝阳区中医科	社区卫生服务机构中医药工作管理平台

运维服务要求：

在线故障响应：配置 3 名专职人员提供 24 小时在线故障响应服务，工作时间响应时间不超过 10 分钟，非工作时间响应时间不超过 30 分钟。重大故障处理时间不超过 24 小时，一般故障处理时间不超过 1 周。

现场故障响应：现场部署人员负责处理客户故障，重大故障提供 7*24 小时现场处理响应，处理周期不超过 24 小时，一般故障提供 5*8 小时现场处理响应，处理周期不超过 1 周。

网络安全服务：根据用户需求，及时解决系统所涉及的网络安全

事件。

7. 区域 PACS 系统

朝阳区区域 PACS 系统从 2011 年开始启动建设，截止 2018 年共建设五期，已覆盖朝阳区 42 家社区卫生服务中心和 8 家会诊医院（朝阳医院、中日友好医院、安贞医院、垂杨柳医院及区属二级医院）组成的医联体单位。各个医联体单位紧密结合，社区卫生服务中心每天将病人影像和报告进行上传，通过区域 PACS 系统进行远程会诊服务，三甲医院大夫每天在线对社区病人影像进行在线处理，并将报告回传给各医联体社区卫生服务中心。区域 PACS 系统前期分期分段建设，包含应用系统、操作系统、数据库系统等几部分的建设实施，本项目对区域 PACS/RIS/BROKER 系统提供运维服务、故障修复等工作。

朝阳区区域 PACS 系统从 2011 年开始启动建设，截止 2018 年共建设五期，已覆盖朝阳区 42 家社区卫生服务中心和 8 家会诊医院（朝阳医院、中日友好医院、安贞医院、垂杨柳医院及区属二级医院）组成的医联体单位。各个医联体单位紧密结合，社区卫生服务中心每天将病人影像和报告进行上传，通过区域 PACS 系统进行远程会诊服务，三甲医院大夫每天在线对社区病人影像进行在线处理，并将报告回传给各医联体社区卫生服务中心。区域 PACS 系统前期分期分段建设，包含应用系统、操作系统、数据库系统等几部分的建设实施。区域 PACS 系统做为区域医疗主要核心业务之一进行持续运行，为保障区域 PACS/RIS/BROKER 系统的稳定可靠运行，区域 PACS/RIS/BROKER 系统的运维、故障修复等工作就具有相当必要性，需要专业团队进行系统运维。

运维服务要求：

1、故障处理。第一时间提供解决方案进行处理，确保不发生责任事故造成信息系统业务应用服务中断，处理完毕后提交《故障处理报告》，提供预防故障的建议。

2、紧急救援服务。根据需求，在发生核心业务系统不可用事件时，提供紧急救援服务，最大限度确保业务连续性及数据完整性。

8. 急救电子病历系统

主要工作保障业务系统正常运行，维护云端服务端业务应用正常运行，解决急救医护人员关于业务系统中遇到的问题，指导日常应用。根据管理科室要求，评估完善性维护需求，根据协商结果进行开发支持服务。朝阳区卫生信息化建设院前急救网络信息平台（一期）主要是是以电子病历为核心的急救业务应用，涉及到中心业务科室，以及各急救站医生日常急救任务的电子病历业务应用。运维系统模块如下：

序号	系统名称	系统简介
1	移动通信监护系统（移动工作站）	医生移动工作站客户端 APP（安卓版），急救医生可通过本客户端在移动平板电脑上书写电子病历、查看患者电子健康档案信息、显示调度受理信息、生命体征、急救收费、任务导航、医疗辅助决策、三方音视频。
2	结构化院前急救电子病历管理系统	急救电子病历工作站软件(WEB 版)，急救医生可通过本 WEB 端完成电子病历的书写及打印，各站审核人员完成病历审核，中心管理科室可进行病历质控、病历数据统计报表查询等功能。
3	急救综合管理平台	实现急救人员、药品耗材、财务收费、车辆及指挥调度任务的综合管理页面查询。
4	院前急救信息平台	具备个人、医务人员、医疗机构、术语字典信息的增查删改；接收患者、电子病历、院前任务、其他业务等文档，并将文档存储到文档存储库中。对院前任务产生的检查图像数据、音视频信息进行分类，编码，对应各类事件中提供调阅。对事物创建、处理、管理；对各层级操作用户集中管理；对管理信息和网络运行信息进行专项管理。具备调用区域卫生信息平台的个人注册服务调用、医疗卫生人员注册服务调用、医疗卫生机构（科室）注册服务调用、医疗卫生术语注册服务调用、健康档案调阅服务调用、病历文档上传服务调用、病历数据查询服务调用等功能，实现与区域卫生信息平台的数据共享。
5	系统接口	实现与北京急救中心指挥调度系统的对接，获取调度任务，实现平台与车载心电监护仪互通。

6	市 120 电子病历传输接口	实现实时上传朝阳急救已经审核的电子病历中的核心数据到北京急救急救中心电子病历系统中。
7	市 120 院前院内衔接接口	与北京急救中心院前院内衔接平台完成数据对接。
8	市 120 院前院内衔接移动端 APP 适配	在医生移动工作站当中适配北京急救中心院前院内衔接数据填报内容，可将朝阳急救患者开通绿色通道中的患者信息，送往医院，生命体征等信息采集传送到北京急救中心院前院内系统，最终呈现在目标医院显示终端。

运维服务要求：

1、由于操作系统故障引起的问题，协助进行处置，恢复系统服务正常运行。

2、由于平台服务端故障，首先进行最快服务恢复，对于系统产生日志进行分析，给出系统故障原因分析报告，给出解决方案。

3、由于用户操作不当产生的故障，协助客户根据提供的使用过程信息进行分析，协助作出故障分析。

4、由于客户端软件、硬件环境、网络通信变化产生的故障，及时响应协助进行分析，解决故障问题。

5、发生故障时，对应用日志进行分析，给出解决方案。

9. 数字卫健协同平台

通过提供数字协同操作平台服务、网络及安全服务、智能低代码搭建等服务，基于现有业务需求和流程管理需求，打造专属于朝阳区卫生健康委员会的统一数字化协同办公平台，统一办公入口、统一沟通能力、统一工作协同，实现相关用户线上高效协同，提升流程管理能力与业务工作效率。一是在长期运行以来，通过精准组织架构联通了卫健委与关联组织，实现统一沟通管理；二是通过搭建用户管理和业务管理流程，提升部门、人员间的沟通与协同效率；三是基于专属安全等功能，实现用户行为、业务数据、文件数据等安全管控，保障相关数据安全，真正形成了更加高效数字化的协作网络。

运维服务要求：

1、售后服务实行 24 小时服务，若使用的产品发生故障，售后服务部可及时

派人到现场解决问题。

2、跟踪应用系统问题，确保它们都有适当的解决方案。反应时间的定义为卫健委提出问题和本单位对问题反馈之间的时间。卫健委因系统故障造成的紧急服务要求，本公司保证立即响应，如果现场技术人员及工程师不能解决问题，保证本单位的后方支持团队第一时间到达现场排除故障，最大限度地降低故障的危害。

10. OA 系统

北京市朝阳区卫生健康委员会目前建设有自己的协同办公系统（以下简称 OA 系统），该系统是朝阳区信息化建设与推进的重要组成部分。服务内容包括：系统的基础运维服务、基于 OA 系统的深度应用和公文管理系统运维工作，保证 OA 系统的日常稳定运行、公文流转顺畅以及系统数据完整安全。确保一旦出现故障，能够快速排除，减少对工作带来的各种影响,将业务的中断时间降到最低。

运维服务要求：

出现故障后，会最大限度保护好数据，做好故障恢复的文档。

11. 互联网诊疗平台

北京朝阳区互联网诊疗系统是北京市朝阳区推动“互联网+医疗”智慧化发展的核心平台，旨在通过数字化手段优化医疗资源配置、提升居民就医体验、缓解基层医疗压力。该系统自 2023 年 1 月正式落地，目前已覆盖朝阳区多家三甲医院和全部社区卫生服务中心，并持续扩展功能与服务范围。要求对互联网诊疗应用进行日常运维，保障服务的连续性，在系统功能变更或升级时，不影响业务正常运营。出现故障，能够及时响应，快速排除，减少对业务带来的各种影像，将业务中断的损失降到最低。

运维服务要求：

1、在线故障响应：配置 2 名专职人员提供 24 小时在线故障响应服务，工作时间响应时间不超过 10 分钟，非工作时间响应时间不超过 30 分钟。重大故障处理时间不超过 24 小时，一般故障处理时间不超过 1 周。

2、现场故障响应：现场部署人员负责处理客户故障，重大故障提供 7*24 小时现场处理响应，处理周期不超过 24 小时，一般故障提供 5*8 小时现场处理响

应，处理周期不超过 1 周。

3、网络安全服务：根据用户需求，及时解决系统所涉及的网络安全事件。