**第五章 采购需求**

**一、采购标的**

1. 采购标的

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 项目描述 | 计量单位 | 数量 | 租赁期限（月） |
| 1 | 云主机服务 | vCPU（主频不低于2.4GHz） | CPU/元/月 | 516 | 12 |
| 2 | 内存 | GB/元/月 | 2056 | 12 |
| 3 | 高性能存储 | SSD高性能存储；高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | GB/元/月 | 12000 | 12 |
| 4 | 普通存储 | SATA普通存储；普通存储（单盘技术指标: 单盘IOPS 1000-3000 ） | GB/元/月 | 8100 | 12 |
| 5 | 静态存储 | 备份存储，总容量的60% 保留2副本；普通存储（单盘技术指标: 单盘IOPS 1000-3000 ） | TB/元/月 | 12 | 12 |
| 6 | 本地备份服务 | 本地备份服务，与备份存储数量相同；通过备份策略实现文件、操作系统、数据库的本地备份（不包含备份存储空间费用） | GB/元/月 | 12000 | 12 |
| 7 | 互联网链路服务 | 互联网带宽；互联网链路带宽 | MB/元/月 | 100 | 12 |
| 8 | IP地址；互联网IP地址租用服务、并提供备案服务 | IP/元/月 | 2 | 12 |
| 9 | 远程接入服务 | 每个账号结合身份验证通过VPN远程接入堡垒机维护 | 账号/元/月 | 5 | 12 |
| 10 | WAF防护 | 满足信息系统安全等级二级中恶意代码防范方面的要求：“应在网络边界处对恶意代码进行检测和清除”。web应用防火墙服务。 | IP（互联网）/元/月 | 2 | 12 |
| 11 | 国产操作系统 | 提供国产操作系统授权及相关运维支撑服务 | 套/元/月 | 22 | 12 |
| 12 | 7\*24小时监控 | 针对所有主机监控；7\*24小时监控 | 主机/元/月 | 22 | 12 |
| 13 | 云端APT服务 | 政务外网和互联网区；对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。 | 套/元/月 | 22 | 12 |
| 14 | 主机杀毒服务 | 针对所有主机杀毒服务；对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。 | 台/元/月 | 22 | 12 |
| 15 | 主机防护 | 针对数据库主机进行主机防护；主机防护：提供符合等保三级要求的主机权限管理及安全防护。 | 台/元/月 | 8 | 12 |
| 16 | 主机安全加固 | 针对所有主机每年1次；针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。 | 台/次/年 | 44 | 12 |
| 17 | 云端抗DDOS服务 | 根据流量提供云端抗DDOS服务，避免业务遭受拒绝服务攻击（攻击流量在10G以内） | 站点/元/月 | 1 | 12 |
| 18 | 网页防篡改服务 | 网页防篡改服务 | 控制点/元/月 | 2 | 12 |
| 19 | 主机日志分析 | 针对所有主机每年1次；针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况 | 台/次/年 | 22 | 12 |
| 20 | 数据库审计服务 | 针对数据库主机进行审计服务；支持Oracle、SQL-Server、DB2、MySQL、国产数据库等数据库审计。（1套为1个数据库实例）。 | 套/元/月 | 5 | 12 |
| 21 | 主机漏洞扫描(次/年) | 针对所有主机每年2次；为用户提供针对主机层面的安全扫描服务，并反馈相关结果。 | 台/次/年 | 44 | 12 |
| 22 | 密钥管理服务 | 提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理 | 套/元/月 | 1 | 12 |
| 23 | 数据加密服务 | 提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持数据库字段级或表级加密与完整性保护，支持“一字段一密钥”；支持文件数据加密与完整性保护，支持“一文件一密钥”细粒度数据加密控制； | 套/元/月 | 1 | 12 |
| 24 | 签名验签服务 | 提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护。 | 套/元/月 | 1 | 12 |
| 25 | 虚拟密码机（VSM)服务 | 基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能。密评必备产品 | 套/元/月 | 1 | 12 |
| 26 | 密码API接口服务 | 把密码调用接口进行业务级封装形成统一密码服务API和SDK，提供统一的密码API接口服务。支持业务应用的鉴别和密码服务权限控制；支持密码服务接口调度，匹配到对应的密码服务资源；支持日志采集，记录调用密码服务的详细日志。密码平台管理服务：实现对各类密码服务接口、服务订购、应用调用、应用认证、平台运行等的管理。支持租户信息管理及服务订购；支持租户密码资源配置与信息管理；支持系统管理员、安全管理员、安全审计员等的系统管理；支持密码资源状态监控、统计展示和告警管理。 | 套/元/月 | 1 | 12 |
| 27 | 数字证书服务（身份鉴别） | 提供数字证书全生命周期管理服务功能，支持用户信息注册、证书申请、证书更新申请、证书注销申请、证书冻结申请、证书解冻申请等注册审核；支持用户证书签发、证书更新、证书注销、证书冻结、证书解冻等证书管理；支持SM2等密码算法；默认1张证书送1个usbkey | 套/元/月 | 5 | 12 |
| 28 | 基于国密算法的远程安全接入 | 支持在终端与平台之间建立SSL VPN安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的HTTPS安全通道。 | 套/元/月 | 2 | 12 |
| 29 | 智能密码钥匙（身份鉴别） | PC终端密码支撑服务，PC端用户身份认证。业务系统每个用户配发一个。不含证书。 | 套/元/月 | 5 | 12 |
| 30 | SSL证书服务（应用层HTTPS） | 提供基于通配符的应用层SSL证书 | 套/元/月 | 1 | 12 |
| 31 | 应急演练服务 | 含应急预案、应急演练、应急响应、服务总结 | 项/次/年 | 1 | 12 |
| 32 | 特殊时期安全专家分析 | 主要提供与安全相关的人工服务，安全隐患分析、安全培训、应急处置服务、木马病毒分析、日志隐患分析等服务。分析报告、人工协助解决隐患、解决方案等 | 项/次/年 | 1 | 12 |
| 33 | 国产数据库 | 国产数据库管理系统 | 套/元/月 | 4 | 12 |
| 34 | 国产数据库 | 国产数据守护集群软件 | 套/元/月 | 2 | 12 |

2. 项目背景/项目概述

根据《北京市市级政务云管理办法》文件中“上云为常态，不上云为例外”的政策要求，北京市公安局人口基层总队需进行人口总队信息管理平台系统入云工作。为了巩固前期工作成果，本项目继续租用北京市级政务云的计算服务、存储服务、网络服务等各类服务，保障已入云系统安全，实现系统在云长期稳定的运行。

本次采购政务云基础服务为人口总队信息管理平台提供云上平台基础计算、存储、网络、安全等政务云资源及服务。

**二、商务要求**

1. 交付（实施）的时间（期限）和地点（范围）

服务周期：1年。

交付地点：招标人指定。

交付实施：合同签订后1周内完成服务交付，如涉及系统迁移需保证在服务交付期间完成系统迁移工作。

2. 付款条件（进度和方式）

合同签订生效后15个工作日内，甲方向乙方支付合同总价的50%；合同到期后，乙方按照合同约定内容完成义务后，甲方向乙方支付合同剩余的50%。

3. 售后服务（质保期）

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求投标人根据业务周期性特点，提供必要的运维值守服务，包含所有云主机的运维维保和远程值守以及定期的巡检服务，包含重要时间节点的重保服务，保证在业务高峰期内系统平稳运行，服务期1年。

**三、技术要求**

1. 基本要求

符合《北京市市级政务云管理办法》文件中“上云为常态，不上云为例外”的政策要求；

提供云上平台基础计算、存储、网络、安全、密码等政务云资源及服务。

2. 服务内容及要求/货物技术要求

2.1采购标的需满足的性能、材料、结构、外观、质量、安全、技术规格、物理特性等要求；

**2.1.1 云计算技术需求**

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| 基本需求 | 云主机资源支持弹性调整，可提供弹性扩展CPU、内存及数据盘磁盘，实例可用性达99.99% |
| 支持虚拟机的跨物理服务器的在线迁移 |
| 虚拟机支持秒级启动功能 |
| 支持用户自主制作镜像功能 |
| 支持用户自主访问、操作自服务平台 |
| 支持实时监控功能 |
| **#**支持云主机深度监控能力，结合深度监控服务提供云主机CPU、内存、磁盘、网络相关资源使用率分析，能够清晰判别资源使用率数值及变化情况，如1天内变化；并支持自动巡检能力，可快速获取巡检时刻资源使用率。提供演示系统链接及管理工具截图证明文件。  |
| **#**通过《云计算服务安全要求 第一部分：通用安全要求》核验，达到增强级要求。（提供通过相关检验的证明材料复印件并加盖证明材料持有人公章，证明材料持有人与投标人必须完全一致。）） |

**2.1.2云存储技术需求**

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| 基本要求 | 提供块存储服务：普通性能存储，读写IOPS：1000-3000 |
| 提供块存储服务：高性能存储，读写IOPS： 3000-20000 |
| 提供对象存储服务：静态存储，读写IOPS：1000-3000 |
| 投标人支持对象存储技术，采用基于服务器本地硬盘提供对象存储资源池，云平台支持通过Web界面对对象存储文件夹进行增删改查（提供所投产品此项要求的系统截图或其他有效证明文件） |
| 本地数据零丢失，提供备份数据内容 |
| 支持NFS，CIFS，SAMBA等协议，可进行跨平台文件共享 |
| 支持存储快照，对系统盘、磁盘数据生成备份，快速恢复数据 |
| 支持云磁盘的创建、删除、挂载到一个特定的虚拟机，作为用户的数据盘使用，支持逻辑卷快照及恢复，支持逻辑卷按需扩容 |
| **#**块存储服务符合《云计算服务协议参考框架》要求（提供相关证明材料复印件并加盖证明材料持有人公章，证明材料持有人与投标人必须完全一致。） |
| **#**对象存储服务符合《云计算服务协议参考框架》要求（提供相关证明材料复印件并加盖证明材料持有人公章，证明材料持有人与投标人必须完全一致。） |

**2.1.3云平台技术需求**

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| 基本要求 | 云平台应具备不低于99.99%可用性标准，可支持用户自主配置主机、存储、网络、安全等资源，支持定制化开发 |
| 支持数据中心资源动态调度，可根据业务压力随时调整虚拟机数量，停机时间可控制在秒级 |
| 支持对虚拟机CPU、内存、存储、带宽进行实时监控，并支持自定义告警规则 |
| 支持用户自定义虚拟主机专用网络或VLAN，并支持7层和4层的软件负载均衡  |
| 支持虚拟机的跨物理服务器的在线迁移 |
| 支持用户自主进行虚拟资源的新建、添加、删除、启动、停止、资源释放和回收 |
| 支持多种虚拟机调度模式，松散调度、紧凑调度、高可用调度等调度策略。其中高可用调度策略开放给云的租户 |
| 支持云平台租户自行指定云主机的网卡IP |
| **#**云服务器、负载均衡(SLB)、云解析(DNS) 、对象存储(KS3)、API 网关、Web 应用防火墙(WAF) 、高防弹性 IP(KEAD) 、文件存储 KFS、对等连接(Peering)、云数据库 MySQL、托管 Hadoop(KMR)通过云服务IPv6支持能力测评，（提供通过相关检验的证明材料复印件并加盖证明材料持有人公章，证明材料持有人与投标人必须完全一致。） |
| **#**通过《云平台网络能力评估方法 第4部分：云组网》检验。（提供通过相关检验的证明材料复印件并加盖证明材料持有人公章，证明材料持有人与投标人必须完全一致。） |

**2.1.4备份服务技术需求**

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| 基本要求 | 采用B/S架构；支持生产端主流操作系统LINUX/Windows 平台；支持多种数据库类型包括Oracle、MS SQL Server、Mysql等，并且支持这些数据库的所有版本； |
| 基于服务器操作系统层，旁路监测被保护数据每次磁盘I/O的变化。实时监测每一笔磁盘写I/O操作，并以事件日志的方式记录。恢复时基于事件日志可以做任意时刻数据恢复； |
| 生产端到灾备端数据传输时要基于字节级实时数据传输而非存储块级； |
| 支持实时、定时两种备份方式；支持一对一、一对多、多对一、级联、双向等部署方式，且在多对一复制时备份端只需配置一套备份端软件； |
| 服务器主机层做应用/数据库高可用，不依赖于某个具体的硬件平台； |
| 支持主机/备机之间实时数据同步，基于主机被保护数据每一笔磁盘I/O操作，以字节的方式高效的传输到备机进行数据同步； |
| 支持缓存和断点续传机制。当备份端硬件故障或网络传输异常中断时，自动缓存生产端数据库的新增数据，系统或网络故障恢复后自动实现断点续传； |
| 图形化管理方式，无需命令行操作； |

**2.1.5扩展服务技术需求**

1. 采购要求
2. 国产操作系统

按照采购人的有关管理规定及需求，提供国产操作系统租用、安装及维护，并协助安装采购人提供的商用操作系统，配合开展维护等工作。

1. 云端APT防护服务

按照采购人的有关管理规定及需求，提供对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。

1. 主机杀毒服务

按照采购人的有关管理规定及具体需求，提供主机杀毒服务。对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。

1. 主机防护

按照采购人的有关管理规定及具体需求，提供主机防护服务。针对数据库主机进行主机防护；主机防护：提供符合等保三级要求的主机权限管理及安全防护。

1. 主机安全加固

按照采购人的有关管理规定及具体需求，提供主机安全加固服务。针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。

1. 云端抗DDOS服务

按照采购人的有关管理规定及具体需求，提供云端抗DDOS服务。根据流量提供云端抗DDOS服务，避免业务遭受拒绝服务攻击（攻击流量在10G以内）

1. 网页防篡改服务

按照采购人的有关管理规定及具体需求，提供网页防篡改服务。

1. 主机日志分析

按照采购人的有关管理规定及具体需求，提供主机日志分析服务。利用云主机日志分析技术对云主机日志进行分析、管理及合规性存储，增强云主机日志方面的监管能力。

1. 数据库审计服务

按照采购人的有关管理规定及具体需求，提供数据库审计服务。对入云业务系统的数据库进行日常操作审计，需支持Tdsql、Oracle、SQL-Server、DB2、MySQL等数据库审计。

1. 主机漏洞扫描

按照采购人的有关管理规定及具体需求，提供主机漏洞扫描服务。包含但不限于主机层面、数据库层面、应用层面的安全扫描，并反馈相关结果。

1. 特殊时期安全专家分析

按照采购人的有关管理规定及具体需求，提供特殊时期安全专家分析服务。主要提供与安全相关的人工服务，安全隐患分析、安全培训、应急处置服务、木马病毒分析、日志隐患分析等服务。分析报告、人工协助解决隐患、解决方案等。

1. 达梦数据库

按照采购人的有关管理规定及具体需求，提供数据库服务

1. 商业密码服务

按照采购人的有关管理规定及具体需求，提供商业密码服务

1. 技术指标要求

（1）云端APT防护服务

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 云端APT防护服务 | 提供基于云端的APT防护能力，对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁，有效发现APT攻击中探测期、入侵期、潜伏期、退出期等不同阶段的安全攻击，具备URL异常检测、沙箱检测、异常流量分析等能力。提供APT防护服务，实现恶意代码检测、恶意软件检测及攻击溯源。无论已知还是未知恶意样本，后台都能提取出恶意行为的特征，形成特征库或策略库，并通过中心管理分发到前端。前端接收安全策略，对相应规则进行拦截，并形成整体防御体系。 |

（2）主机杀毒服务

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 防病毒要求 | 提供基于云平台集成的杀毒软件，对云主机进行定期的病毒查杀，杀毒软件采用集中控制，云主机端无需安装代理软件，病毒库升级采取控制端统一下发的方式，对网络性能无影响。采用轻量级Agent部署，无需依赖虚拟化平台API即可实现安全防护；客户端支持手动从控制中心获取安装，也可通过管理控制中心批量远程安装；客户端对windows类、linux类的物理服务器、虚拟服务器、桌面云具备相同的防护和部署。产品应至少支持VMware 、Ctrix、Microsoft 、Huawei、H3C、浪潮等国内外主流虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理。 |

（3）主机安全加固

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 安全隐患排查与整改 | 支持对信息系统和IT基础设施存在的安全漏洞和隐患进行排查和处置，提高安全防护水平。 |
| 安全基线核查 | 支持项目概况范围（不包括终端）中的主机系统、应用系统、网络设备和数据库管理系统等资产进行安全基线核查，检测在安全现状、安全配置、防护能力、恢复能力等方面的详细情况。 |
| 渗透测试 | 支持应用系统、外网网络进行定期的渗透测试，挖掘存在的安全漏洞，找出系统的安全短板，以此评估目标系统的安全性。 |
| 安全整改与加固 | 支持信息安全风险评估、安全基线核查、漏洞扫描和渗透测试等技术手段全面的评估的结果，对发现的信息资产安全漏洞、隐患、威胁等进行整改和加固，提高信息系统安全保障能力。 |
| 应用加固 | 支持修补漏洞、增强安全配置、调整系统架构和提升安全策略等方式进行系统整体加固和安全优化，提高系统的安全性和抗攻击能力，将整个系统的安全状况维持在较高的水平，减少安全事件发生的可能性和可能造成的损失。 |

（4）主机漏洞扫描

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 扫描能力 | 支持Windows、Linux域扫描技术，利用域管理员权限使扫描更深入、更准确。 |
| 支持大华、海康等视频监控类设备扫描。 |
| 支持多种协议口令猜测，包括SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM等。 |
| 支持设置口令猜测间隔0-300秒。 |
| 支持对主流数据库的识别与扫描，包括：Oracle、Sybase、SQL Server、DB2、MySQL等，支持对数据库漏洞进行扫描和修复。 |
| 资产管理 | 支持以txt、csv、dat、xls等格式进行资产列表的导入。 |
| 产品升级、维护 | 支持实时提醒当前的系统消息，包括报表下载消息、升级内容消息、日志下载消息等。支持控制台功能，可以通过控制台对系统进行操作和设置，例如重启和关闭系统、修改系统和网络配置、查看漏扫引擎状态并提供网络诊断工具。 |

（5）主机日志分析

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 日志采集 | 满足支持新增Lotus Domino的日志采集任务；新增CheckPoint的日志采集任务。 |
| 日志审计中心可以集中对独立安装的日志采集器进行统一管理，能够对日志的解析策略进行统一下发。 |
| 部署要求 | 支持单级部署和级联部署，支持分布式部署。 |
| 资产管理 | 满足系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表； 满足能够根据收到的事件的设备地址自动识别新的资产并自动添加到资产库中。 |
| 工作台 | 满足系统内置基本的仪表板。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为用户建立不同维度的仪表板。满足仪表板中的每个显示区域都能够放大、缩小、拖动。 |
| 日志管理 | 满足日志可加密压缩传输 支持加密压缩方式转发，定时转发。满足支持日志源管理功能，对断点日志源可以产生告警。  |
| 日志范式化 | 满足范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址、目的MAC地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成。满足产品界面支持范式化文件的导入导出功能。 |
| 日志分析 | 满足系统需内置不同分析场景，包括各种实时分析场景、历史统计场景、实时统计等。并支持支持自定义场景。满足可以手工对选中日志进行告警或者加入观察列表中。 满足自定义事件查询策略，基于事件类型的查询条件不少于10大项50小项。满足可以对选中的日志提供在线/离线地图定位、视网膜图、事件拓扑图等多种分析工具。可以显示一段时间的动态日志移动图，能够在图上显示每个时间切片的日志数量、等级，并能够在图上显示每秒事件数。用户点击每个时间切片，可以查看该切片内的日志。 |
| 关联分析 | 满足提供基于图形化方式的规则编辑器；规则可导入导出。满足在编辑规则条件的时候，可以针对事件属性引用规则、应用资产属性、引用资源。 |
| 综合显示 | 满足能够显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，事件EPS曲线。 |

（6）数据库审计服务

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 审计协议 | 支持Tdsql、Oracle、SQL-Server、DB2、MySQL等数据库审计。 |
| 支持高斯（Gauss）、人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) 等数据库进行审计。 |
| 支持MongoDB、Redis、Hbase、hive、ES等数据库进行审计。 |
| 支持FTP、Rlogin、Radius、NFS、X11等协议审计。 |
| 审计能力与效果 | 系统应内置规则集，对数据库DML、DCL、DDL等语句及FTP、Telnet等协议中的命令进行归类，便于用户定制审计策略。 |
| 审计策略支持时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件。 |
| 审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件（非正则表达式方式）。 |
| 提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别。 |
| 支持对数据库DML、DCL、DDL语句的审计。 |
| 审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件。 |
| 审计策略支持时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件。 |
| 支持对数据库绑定变量方式访问的审计。 |
| 支持访问数据库的源主机名、源主机用户的审计。 |
| 支持SQL操作响应时间的审计。 |
| 支持Select操作返回行数和返回内容的审计。 |
| 支持对超长SQL语句的审计。 |
| 支持访问数据库的源主机名、源主机用户、SQL操作响应时间、数据库操作成功、失败的审计。 |
| 支持频次告警，某一操作在周期时间内达到设定的次数阀值即可告警，周期事件和次数可按需配置。 |
| 支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计。 |
| 支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的SQL操作审计。 |
| 支持Telnet协议的审计，能够审计用户名、操作命令、命令响应时间、返回码等。 |
| 支持对FTP协议的审计，能够审计用户名、命令、文件、命令响应时间、返回码等。 |
| 支持审计网络邻居的用户名、读写操作、文件名等。 |
| 支持审计NFS协议的用户名、文件名等。 |
| 支持审计Radius协议的认证用户MAC、认证用户名、认证IP、NAS服务器IP。 |
| 支持对针对数据库的XSS、SQL注入攻击行为进行审计。 |
| 支持对Oracle数据库状态的自动监控，可监控会话数、连接进程、CPU和内存占用率等信息。 |
| 业务关联审计 | 支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯。 |
| 支持实时关联，实时显示关联结果，无需时候手动查询。 |
| 数据库异常行为审计 | 支持根据网络数据流自动建立数据库操作行为基线。 |
| 智能发现 | 满足数据库审计支持用户数据库中敏感信息的自动发现，方便针对敏感信息配置针对性的审计策略。 |
| 满足敏感信息发现支持探测器和正则表达式两种方式，探测器至少包含：姓名、地名、银行卡、身份证、IP地址、密码等多种探测器。 |
| 事件查询统计与报表 | 满足支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多IP登录、上下班操作量对比异常、操作响应时间分析。 |
| 满足支持疑似暴力破解、疑似撞库攻击场景的操作异常分析；行为周期与阀值可按需定义。 |
| 查询需支持返回全部符合条件的结果，无上限限制。 |
| 可支持sql语句关键字查询，查询结果包含该关键字的sql语句。 |
| 第三方扩展接口与联动功能 | 支持与Web应用防火墙（WAF）的联动，可对WAF上报的应用系统攻击实现场景还原展示。 |
| 支持与APT检测产品的联动，对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件。 |

（7）安全隐患分析

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 安全隐患分析要求 | 按照采购人的有关管理规定及具体需求，提供安全隐患分析服务。包括外部访问、系统维护、资源使用等信息汇总。提供系统安全分析，包括可疑访问、恶意访问、安全试探、异常访问数据分析等安全隐患的预警性分析。 |

（8）密码应用服务

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| 密码应用服务 | 云平台安全运维服务-互联网基于国密算法的远程安全接入，支持在终端与平台之间建立SSL VPN安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的HTTPS安全通道。 |
| 云平台安全运维服务-互联网密钥管理服务，提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理 |
| 云平台安全运维服务-互联网数据加密服务，提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持数据库字段级或表级加密与完整性保护；支持文件数据加密与完整性保护，支持细粒度数据加密控制，支持数据加密吞吐率100Mbps； |
| 云平台安全运维服务-互联网签名验签服务，提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护，支持SM2签名速度不低于700次/秒。 |
| 云平台安全运维服务-互联网虚拟密码机（VSM)服务，基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能，每实例2C4G。 |
| 云平台安全运维服务-互联网密码API接口服务，把密码调用接口进行业务级封装形成统一密码服务API和SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。 |
| 云平台安全运维服务-互联网数字证书服务，提供数字证书全生命周期管理服务功能，支持用户信息注册、证书申请、证书更新申请、证书注销申请、证书冻结申请、证书解冻申请等注册审核；支持用户证书签发、证书更新、证书注销、证书冻结、证书解冻等证书管理；支持SM2等密码算法 |
| 云平台安全运维服务-互联网智能密码钥匙（usbkey），PC终端密码支撑服务，PC端用户身份认证。业务系统每个用户配发一个。 |
| 云平台安全运维服务-互联网SSL证书，符合国密算法的单域名SSL证书 |

**2.1.6其他技术需求**

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| 政务云技术架构要求 | **#**投标人所使用云平台需采用基于OpenStack主流版本且经过厂商深度定制的云平台软件，资源虚拟化通过KVM技术实现。(提供所投产品此项要求的系统截图或其他有效证明文件) |
| 政务云存储技术要求 | 投标人所使用云平台支持基于通用X86服务器本地硬盘的计算存储融合架构部署分布式存储资源池，底层支持三副本数据冗余（提供所投产品此项要求的系统截图、三方证明或其他有效证明文件。） |
| 政务云资源及服务管理要求 | 云服务商提供招标人可自服务的云资源可视化管理能力，实现：云主机数量、vCPU数、内存数、磁盘数统计，云资源分配量趋势分析，云资源分布分析（互联网及政务外网分布情况、操作系统类型分布情况、云主机状态分布等），提供演示系统链接及管理工具截图证明文件。 |
| **#**云服务商提供招标人可自服务的云资源可视化管理能力，支持按资源分布进行业务资源用量分析并支持排序；支持按云主机数量进行业务系统分析并支持排序；提供演示系统链接及管理工具截图证明文件。 |
| **#**云服务商提供招标人可自服务的云资源可视化管理能力，支持业务探活能力，能够根据业务系统服务IP地址、服务链接进行业务健康状态探测，展示系统运行状态，如正常、异常等，提供演示系统链接及管理工具截图证明。 |
| **#**云服务商提供招标人可自服务的云资源可视化管理能力，支持云效率分析展示能力，能够清晰展示云效率总值以及云效率变化轨迹图，时刻掌握系统云资源使用情况，并能够清晰展示不同系统云效率情况。提供演示系统链接及管理工具截图证明。 |

2.2采购标的需满足的服务标准、期限、效率等要求；

投标人须利用监控系统或人工对硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。提供7\*24小时热线支持服务，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在2小时内到达运维现场提供服务。系统发生宕机问题时，投标人应在15分钟内响应，故障处理完毕后提供相关系统宕机报告。

2.3为落实政府采购政策需满足的要求；

无

2.4采购标的的其他技术、服务等要求；

**2.4.1故障响应服务**

投标人应当提供高效的系统维护服务，有效防范系统风险，投标人需保持7\*24小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在2小时内到达运维现场提供服务。系统发生宕机问题时，投标人应在15分钟内响应，故障处理完毕后提供相关系统宕机报告。

**2.4.2重点保障要求**

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求投标人根据业务周期性特点，提供必要的运维值守服务，包含所有云主机的运维维保和远程值守以及定期的巡检服务，包含重要时间节点的重保服务，保证在业务高峰期内系统平稳运行。

**2.4.3安全及保密要求**

投标人须严格遵守招标人的相关信息安全规定，本项目涉及人员须与投标人签订保密协议，项目中标后本项目服务人员须与招标人签订针对本项目的保密协议，投标人应选派具有良好职业道德的人员参与和从事本项目工作，不得利用系统维护服务时的便利对招标人数据及其他信息擅自修改或透漏，投标人须承担相关保密责任。

2.5需由投标人提供设计方案、解决方案或者组织方案的采购项目，应当说明采购标的的功能、应用场景、目标等基本要求。

根据本次项目采购需求及内容，提供安全服务方案、项目组织实施方案、售后服务方案、落实ESG理念的工作措施等。

2.6项目团队

项目经理不少于1人，需为本科及以上学历，具备10年（含）以上的工作经验，并具有信息系统项目管理师证书。

技术负责人1人，需为本科及以上学历，具备10年（含）以上的工作经验，须同时具有系统架构设计师（高级）证书、系统分析师（高级）证书、软件设计师（中级）及以上证书。

质量管理专员1人，需为本科及以上学历，具备 10 年（含）以上的工作经验，同时具有质量管理体系内审员证书、系统集成项目管理工程师证书（中级）、信息系统项目管理师（高级）证书。

其他项目人员，除项目经理、技术负责人、质量管理专员外，需配备不少于5名成员，每位成员均具备5年（含）以上项目实施经验，并具有有效的信息系统项目管理师证书/系统架构设计师证书/CISP证书

投标人须设立驻场运维工程师，在采购人现场办公，作息时间与采购人同步，实时响应工作时间内需求及故障处置。

投标人须利用监控系统或人工对硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。

投标人负责设立技术支持热线，并安排专人值守，提供7\*24小时热线支持服务。投标人针对采购人要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据采购人要求配合开展相关维护服务。

投标人应指派专业技术能力较强的驻场工程师1人，驻场工程师职责范围包括根据甲方要求配合开展相关维护服务、资源协调服务，协助用户开展政务云的日常运行管理工作。

3. 验收标准

投标人所提供资源应满足北京市级政务云的服务要求。保证合同期内系统安全稳定运行，云平台整体可用性不低于99.99%，数据可靠性不低于99.9999%（须提供测试报告）;不因硬件故障导致服务中断12小时。

服务期满前30个工作日开始对合同项目进行验收。投标人应当在招标人指定的验收日前向招标人提交验收报告。验收报告的内容包括但不限于，合同规定的各项服务清单，各系统设备运行情况。

项目完成后，由招标人组织验收。

4. 其他要求

如果属于政务信息系统项目，其采购需求还应当符合《政务信息系统政府采购管理暂行办法》（财库〔2017〕210号）的相关要求