采购需求

第一章 概述

1、项目背景

参照《北京市数字经济促进条例》、《北京市市级政务云管理办法》和《北京市市级政务云服务指南》等相关法律法规以及政策文件精神要求，政务云按照“统筹规划、适度超前、分级管理、资源共享”的原则建设和管理，除公安、国家安全等部门以及涉密和信息安全等级保护四级（含）以上信息系统外，区级各单位现有信息系统应逐步迁移至政务云，凡政务云已具备服务能力的，软硬件原则上不再新购。

为实现集约化建设和管理，充分发挥北京市西城区级政务云（以下简称政务云）的作用，为政务大数据应用奠定基础，为区属行政事业单位提供计算、存储、网络等云服务。西城区政务云平台 2013 年初步建成，截至目前已实现“三域、三池、两平台”的架构，三域分别为政务外网域、互联网域和测试域；三池分别为北区二龙路办公区资源池、卫健委办公区资源池及天宁一号资源池；两平台为全区统一的云平台安全监管一体化平台和云备份迁移管理平台。同时，2024 年基于信创云架构的信创云正式上线试运行，标志着“政务一体云”进入全面换“芯”阶段。截至 2025 年 8 月底共承载全区 184 个业务系统（包含国产云平台、信创云平台的系统总数），共计 1133 台虚拟机，涉及委办局街道共计 59 个。

西城区政务云参考市级政务云模式，引入云服务商，采用“云服务商投资建设，通过政府采购方式购买云计算服务（参照最新政采目录），由云服务商在西城区政府指定的数据中心和指定的时间内完成政务云平台信创云、国产化云的政务外网域、互联网域、测试域的按需建设部署和快速扩容，并按需提供商用密码安全共性服务、GPU、NPU 等新增云资源服务。

西城区政务云平台（以下称政务云平台）是支撑西城区各委办局非涉密电子政务系统运行的云计算平台，由西城区数据局信息中心统筹规划和管理，统一面向区属行政事业单位提供云计算、网络、云平台安全及相关配套服务。政务云平

台同时也是西城区政府数字经济、智慧城市、大数据发展等核心工作的技术基础，在政务数据汇聚、融合和公开等方面发挥着极大的保障作用。政务云平台急需探索完善提升云计算大数据中心公共服务支撑能力，强化数据资源分析处理和应用，推动跨部门信息共享和业务协同。

2、西城区政务云总体规划

在全区政务云平台顶层设计基础上，聚焦数字政务领域优化提升云平台技术赋能水平；实现新政务云平台全面优化提升建设工作，持续完善管理体系、稳步提升云使用率、切实做好全年重点保障等工作；同时，持续对政务云基础、云安全和云扩展资源等进行优化升级，确保各委办局业务应用稳定可靠运行，满足各部门信息系统业务迁移及未来新增上云需求。区级各单位信息系统按照“入云为常态，不入云为例外”的入云原则和“应入尽入、分工负责、重要先入、安全入云”的迁移原则,持续加强推进政务系统入云、上云、迁云等相关工作，实现政务云平台“降本增效、提质扩能、强基固链”。

进一步完善计算、存储、网络、安全防护、云监控监管、云迁移备份等基础服务和扩展类的云资源服务体系，持续深入推动区政务系统入云，积极促进更多信息系统向云平台迁移。强化顶层设计，坚持系统谋划，聚焦数字政务领域着力提升云平台的技术赋能水平，通过分期规划建设区级专题云、混合云和融合云，实现云平台对“数字+智能+重点领域业务新应用”的有效保障。持续完善管理体系，以“可持续、高发展、强保障”为发力点，稳步提升云使用率，切实做好保障支撑工作。

1.可持续。秉承集约建设的建设思路和运行模式，持续发力打造“一体云”。

2.高发展。坚持信息化安全管理创新，优化“云”办公模式，通过云数据底座实现资源融合、高效协同，助力政务办公数字化高效发展。

3.强保障。提供重保服务，保障政务云平台平稳运行，实现安全运行“零事故”。

3、西城区政务云平台需求

西城区政务云平台按电子政务网络安全要求划分为电子政务外网和互联网和测试区域，其中政务外网与与互联网与两区域间设置安全数据交换区实现不同区域间的数据安全交换。云服务商提供的云平台需与现有云资源池形成异构云平台、应满足日后对于产品的升级要求。扩容云平台考虑使用安全性和稳定性更高的国产平台进行建设。提升区级政务云平台基础设施的能力需求：不断更新完善计算、存储、网络、安全防护等云服务支撑能力，持续深入推动政务系统入云，提供全流程业务信息系统向云平台迁移和备份全方位基础支撑。国产化云平台和信创云提供以下服务包括：服务器、存储、网络设备、视频图像分析、独立安全域安全设备的安装；提供计算、存储、网络、云安全、网络带宽等虚拟化能力的虚拟化层部署所需的基础设施资源；提供运营、运维等服务的云服务应用的部署等。为全区提供政务云基础服务：云主机服务、网络服务、图形图像计算服务、存储服务、视频云存储、云安全等服务；扩展云服务：迁移服务、安全服务、完善 Saas、Paas、Daas 层等多层结构化、体系化、融合化的云计算服务和云资源服务；通用智能中枢 AI 算法（虚拟计算）管理平台、隐私计算、安全检测监测和 CDN 加速服务等增值类云服务内容。

区级政务云分为服务云、办公云、备份节点。服务云主要支撑公众服务类系统、大数据类业务系统运行；办公云主要支撑政府内部办公类业务系统运行；备份节点主要实现服务云和办公云的云主机迁移、备份、应用系统双活等业务需求。云服务商提供的政务云是我区信息化关键基础设施之一。

政务云在运行、管理、安全上坚持统一标准体系、统一监管体系和统一评估体系，实现多云统一管理体系；构建全区统一的政务云数据专区，实现多云数据的汇聚、管理和共享；构建全区统一安全保障和应急监测体系，实现多云节点和全区入云系统的安全监测和应急预警。区级政务云由区数据局牵头规划和建立统一管理体系，政务云（服务云、办公云、备份节点）由区数据局管理、组织建设运营和推广应用。区级政务云通过一套服务目录（含单价），提供标准的服务水平。

云服务商节点需在西城区政府指定的西城区机房内进行建设，实现独立安全域部署，云服务商节点定位于政务云生产数据中心，统一为区级部门提供政务云

服务，支撑应用系统实时在线运行。

1、政务外网域云资源快速扩容需求

新增设备提供的虚拟化资源应满足未来 1 年现有业务系统数据扩容升级、新增业务系统部署需要。由于现有政务外网域虚拟化资源池处理能力已近饱和，建设的国产云计算平台需要在计算能力方面满足未来的业务系统增长需要。根据近 1 年各单位信息系统建设提出的需求统计。同时，能够在短时间内实现云平台资源池的快速扩容，满足各单位业务系统部署需求。项目建设内容包括基础设施提供和云平台建设交付。

2、信息安全等保三级安全需求

现政务外网域核心出口部署的安全设备，同时部署独立安全域满足信息安全等级保护三级的安全要求，信创云、国产化云平台需要满足等保安全三级的安全要求，为各单位提供更为安全的计算、存储资源，满足各单位业务系统的安全性需要，从而使政务外网域资源池具备等保二级、等保三级、密码评估的综合提供能力。

3、云平台监控需求

现政务外网域已具备完善的安全监管平台，新建信创云平台需要提供标准的监控接口，接入现安全监管平台，实现统一的监控管理。

4、商用密码共性服务

依据《中华人民共和国密码法》等法规标准，为进一步强化各系统密码应用能力，现需针对上云系统提供商用密码共性服务，提升系统安全防护水平，切实满足信息系统密码应用基本要求。

5、云平台资源快速扩容需求

随着各单位信息化建设的快速发展，云平台需要提供快速扩容的能力，保证未来业务增长、数据量增加及新业务系统上线时，能够在短时间内实现云平台资源池的快速扩容，满足各单位业务系统部署需求。项目建设内容包括基础设施提供和云平台建设交付。

6、云平台备份、迁移需求

由云服务商提供使用单位现有虚拟化业务迁移上云，包括迁移前调研、迁移、测试、上线、技术支持服务（不包括迁移到托管区）。通过安全可靠的云平台迁移技术实现虚拟机在线平滑无缝、安全可靠迁移，迁移后系统能够达到可验证状态直接使用。

7、构建面向云计算的安全运营和应急保障服务需求

组建云平台安全体防护运营管理服务体系：实现域名安全解析、流量清洗、负载均衡、内容分发、安全审计等，提高云计算对抗攻击的能力。全面普及网络安全、数据安全、应用安全等多视角租户安全服务，建立安全态势感知平台，建立事前防御、 检测， 事中防护和事后响应的全方位安全能力。推动云计算服务模式的灾备能力建设。

4、各方职责和关系

4.1 云管理单位

北京市西城区数据局（以下简称区数据局）是西城区政务云管理单位，云服务规划、管理责任主体为区数据局，主要职责为：

1） 负责政务云的统筹规划、监督管理、制度标准规范的制定、宣传和培训，遴选并管理云服务商；

2） 负责各单位使用政务云的资源协调，使用情况的监测和统一发布；

3） 总体负责政务云建设、运维、安全监督及物理安全的管理；

4） 负责对云服务商日常工作进行监督检查和服务质量考核；

5） 负责指导并完成政务云安全检查、应急演练、统计监测等工作。

4.2 云监管单位

云监管单位受政务云管理单位的委托和指导，协助管理单位建立政务云服务监管体系，监督政务云运维管理及云服务商建设实施，承担政务云资源使用情况

监控，统一规范安全管理体系建设等。

1） 实时监测政务云资源使用情况和基础设施运行状况，统计分析监测结果，定期向管理单位报送统计报告；

2） 政务云平台的安全检查，政务云网络边界的安全监测，定期向管理单位提供政务云平台安全监测报告；

3） 配合管理单位制定政务云平台总体应急预案，定期组织开展应急演练。

4.3 云服务商

云服务商是为用户提供云计算、存储、网络及相关配套资源和服务的提供商，承担云平台物理安全、网络安全、虚拟化安全及云平台安全管理的相关责任。

1） 负责政务云平台的投资建设、运维管理、安全保障、资产管理，协助政务云使用单位的业务系统迁移入云等，提供云平台物理安全、网络安全、虚拟化安全保障服务；

2） 确保云平台可用性达到 99.99%，数据可靠性达到 99.9999%，确保云平台实现按需 7 个自然日快速扩容；

3） 按照等保三级及有关网络安全的要求建设管理云平台；承担所建云平台安全保障；确保通过等保三级测评和第三方网络安全审查；

4） 承担云平台管理工具建设，具备 VPN 管理、流量管理等方面的能力；

5） 服从政务云管理单位及云安全监管服务商的管理，协助建立政务云运维管理体系、管理制度并切实执行；按照云安全监管服务商提出的接口标准与云监管平台对接；

6） 按照网管中心管理规范要求，配合完成政务外网接入和域名解析等相关工作；

7） 协助制定政务云应急预案，定期开展政务云平台应急演练，根据政务云应急预案，指导各业务系统的应急预案制定，并配合业务系统应急演练工作，做好日常应急响应工作；

8） 接受并配合云安全监管服务商绩效考核工作；

9） 负责本单位人员的安全培训教育，确保工作人员符合岗位要求；

10） 负责政务云应用双活功能建设；

11） 云服务商需提供云架构规划咨询、应用系统部署、迁移，云平台运维，技术培训及其他技术服务。其中每个应用系统迁移云服务商须在接到迁移需求的 20 个工作日内配合委办局用户完成；

12） 承担政务云机房必要的基础环境建设及管理。

4.4 政务云使用单位

政务云使用单位（也称委办局用户或租户）是使用西城区政务云搭建电子政务外网应用的接入单位。云使用单位承担应用系统部署及管理、自身数据安全、应用系统安全等相关责任。云服务需求责任主体为使用单位，主要职责为：

1） 本单位入云信息系统的软件平台层和应用软件层的日常维护、管理、安全和应急保障；

2） 管理主体不变，负责入云信息系统自身的安全管理，建立信息系统运维和安全管理制度，负责日常运行维护管理、常规安全保障和监控预警；

3） 入云安全标准不变，信息系统仍遵循信息安全等级保护制度，做好定级备案和测评工作。

第二章 建设总体要求及说明

1、建设目标和建设模式

本次政务云建设总体要求是采购人对云服务商提出的基本要求，云服务商可进行优化，具体响应文件中的功能、性能可优于本要求。

1.1 建设目标

1. 建设符合工信部《基于云计算的电子政务公共平台顶层设计设计指南》、《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、规范的区级政务云平台。

2. 与现有云平台整合，搭建异构云平台，成为现政务外网资源池的有效补充，提升云平台的整体服务能力。融合后的管理系统可以集中管理和监控各个资源池的计算、存储、网络资源和使用情况，提供统一的资源管理、跨资源池资源部署、运维管理、服务管理和自助服务等能力。

3. 响应北京市政府“上云为常态，不上云为例外”指示精神，实现信息化建设模式的改变。由原自建云平台的重资产模式转为按需租用云服务的模式，达到资源快速交付、简化运维、提升信息化安全的目的。

4. 依据《中华人民共和国网络安全法》、《中华人民共和国密码法》等法规标准，积极响应国家监管政策和信息安全保障制度，严格落实信息系统等级保护、密码应用等有关措施，为各单位提供更安全可靠的信息技术服务和安全保护。

5. 实现各单位信息系统的集中化部署，实现各单位数据的统一汇聚。依托新建国产云平台，面向各单位提供集中式部署或可扩展的基于分布式计算的大数据服务基础支撑能力，在数据层面实现安全融合汇聚、充分共享。采用 AI 算法实现深度学习、多维度智能关联数据分析。

6. 根据政务云基础服务、扩展服务目录，实现各单位信息系统的集约化统筹管理，建立信息化项目建设标准流程，实现一点申请、审批、开通资源。

1.2 建设和运营模式

此次西城区政务云扩容采用“企业投资建设，政府采购服务”方式，在政务云建设单位的统筹指导下，由云服务商在指定的时间内完成政务云平台的建设部署。

1） 云服务商须建设不低于现有云平台同等业务服务能力的云服务平台，两个云服务平台间要实现网络互通，并能保证统一管理。

2） 政务云部署机房需和区政务外网链路打通，云服务商配合网络联调，接入现有云平台核心交换机，后期运行维护由运维单位负责。

3） 云服务商完成政务云平台本身的网络搭建和部署，政务外网由政务云管理单位提供（带宽足够满足需求），政务云汇聚接入机房至政务云承载机房之间链路由政务云管理单位提供（带宽足够满足需求）。

4） 云服务商应在政务云管理单位的指导下共同构建统一完整的政务云服务体系和标准的服务目录。政务云投入使用后，政务云管理单位以据实结算方式支付政务云（中标云服务商）服务费用。

5） 本项目最终选择 1 家云服务商与区数据局签署合同。项目支付方式：项目拟计划分三次支付中标金额（合同款），其中支付第一笔款，即约合同总额的 50%；第二次付款，即合同总额的 30%；第三次付款，即支付至项目据实结算审计总额（具体支付要求详见合同模版）。

2、总体要求

2.1 政务云总体部署要求

此次，云服务商负责同步优化扩容升级信创云平台建设，与现有国产化云平台交互通过接入现有云平台的核心网络交换设备实现互联互通。同时，扩容云平台应与现有云平台整合，成为现政务外网资源池的有效补充，提升云平台的整体服务能力。融合后的管理系统可以集中管理和监控各个资源池的计算、存储、网络资源和使用情况，提供统一的资源管理、跨资源池资源部署、运维管理、服务管理和自助服务等能力。采用购买服务形式在西城区属地自建机房内搭建独立安全域管理的电子政务外网、互联网和测试域。

2.2 对云服务商的要求

指标项	**规格要求**
云 平 台	技术方案要求：需要明确整体解决方案供应商，包括但不限于支撑政

指标项	规格要求
建设和服务要求	务云平台运行的相关核心硬件、软件、安全等关键系统。
	云服务商所采用的云平台应为具有国内自主知识产权的主流云平台产品。
	平台指标要求：当平台某资源已分配量超过该资源总量的 80%时，须承诺实现 7 个自然日快速扩容；云服务商提供的云平台整体可用性应不低于 99.99%，数据可靠性应不低于 99.9999%，同时提供测算依据。云服务商需要对服务目录中各项服务的服务水平进行描述，形成“政务云服务水平规范”。
	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、安全服务等，云服务商需要保障基础设施资源可扩展性，满足所有用户需求，能够在多租户网络流量条件下，对用户网络流量进行识别并进行精细化管理。 云平台应能提供包括计算服务、存储服务、网络服务在内的服务能力。
	云服务商双活能力要求：云服务商应具备应用、数据双活备份的平台能力，且能够为使用单位提供跨服务商云计算平台、跨数据中心的系统双活、容灾服务的支撑能力。
	带宽接入要求：政务外网和互联网的接入带宽由政务云管理单位解决
	云服务商应具备跨云平台的服务能力：云服务商应能够为使用单位提供跨云服务商云计算平台的纳管能力，以及多地域资源池的纳管能力。当出现异常情况时，可为云使用单位提供应急响应、应用及数据处置和应用及数据恢复服务。
	知识产权要求：云服务商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。云服务商云计算平台应采用国内自主研发、成熟稳定、安全可控的云计算平台产品，云平台产品具有在省部级政务云大规模部署应用案例；需要明确云平台硬件、软件设备品牌型号，

指标项	规格要求
	在云计算平台实际建设和部署中，云服务商应确保云平台核心硬件设备的品牌型号、软件版本与响应文件描述一致。在中标后签订合同前，云服务商须承诺提供主要设备和产品的厂家指标确认函。
	运维能力要求：云服务商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，为委办局提供单个用户内的业务可视化，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。
云平台安全保障要求	安全责任：承担云平台层面（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入云系统问题。针对迁移上云的业务需要与委办局确认系统安全，不会对其他业务系统造成安全攻击； 云平台建设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和权威第三方网络安全审查。
	数据保护要求：政务数据不得离开西城区政务云机房。云服务商应承诺，未经允许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。
	云服务商在未经过用户邮件、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；各业务系统、数据归属于政务云使用单位，云服务商无权支配。云平台内所有设备的维修、报废等处理须经过云安全监管单位和云管理单位审批，在云安全监管服务商监督下执行。
	应急演练：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、恢复系统及数据。指导或协助云平台使用单位开

指标项	规格要求
	展系统应急工作。
云服务标准化要求	远程访问：云服务商具备提供用户远程访问自身采购的云资源（存储、带宽、CPU 的使用率等）使用情况的能力。
	系统迁移：协助配合云使用单位完成入云迁移。
	人员要求：本项目配置的运维服务人员需具备网络、安全、虚拟化、数据库、操作系统等专业知识和技能。在服务期内，保证至少 10 人每周 7*24 小时的保障服务，配备具备两年以上云平台维护经验的运维人员，支持电话、网上值班等响应方式；任命 1 名项目经理作为政务云售前和售后的总接口人，常驻现场定期向政务云管理单位汇报工作；建立符合实际管理、运维所需要的运维团队。
	服务响应要求：为最终用户提供技术服务热线(每周 7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法；在服务期内，提供每周 7*24 小时的现场和技术支持服务，对故障 15 分钟内响应；2 小时内到达云中心机房。如果逾期未作出响应，承担由于故障所造成的全部损失。
	管理制度及规范要求：云服务商应遵循《北京市市级政务云管理办法》、《北京市西城区政务云管理办法》及政务云运维相关管理制度和流程开展工作，并具备清晰的内部管理框架和完善的管理方案。云服务商需制订满足自身业务需要的政务云服务相关制度、标准、规范和办法。
服从监管要求	云服务商需接受政务云管理单位的监管要求，并提供相关计算、存储、网络等资源监控及安全接口。
	政务云管理单位负责引导、督促、协调各政府部门应用系统入云托管服务业务，并对政务云服务过程进行整体把关；云服务商必须免费配合云服务管理单位的相关审核工作。

指标项	规格要求
	云服务商必须按照政务云管理单位要求开放云计算相关平台接口。云服务商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。
服务能力扩展要求	云服务商应具备为使用单位提供基础软件支撑服务、云迁移服务、安全防护服务、安全检测监测、CDN 加速和数据备份等服务。
	云服务商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。
	云服务商应在服务期限内，逐步增强 PaaS 层、Daas 层的服务能力，支持云数据库、大数据平台的支撑能力。

2.3 技术要求

2.3.1 机房要求

云数据中心（满足等保三级要求）由西城区数据局指定，提供给云服务商使用，机房内基础设施齐全，云服务商可直接部署使用。政务云运维单位承担运维管理职责，政务云管理单位负责服务运营过程中产生的水、电、煤气、卫生保洁等费用。

2.3.2 网络技术要求

提供互联网 IP 地址租用及链路带宽服务，做好配套的 IP 地址备案、网络策略配置工作。提供主机负载均衡服务，采用全冗余或集群架构，保证无单点故障。提供远程接入服务，进行远程接入账户管理。提供 VPN 服务，实现通过 VPN 访问系统及数据传输等功能。提供 SSL 证书服务，保证系统数据的 SSL 加密传输。提供 WAF 防护服务，保证对系统已知安全隐患进行防护，实时升级漏洞补丁，配置防护策略。

提供 WAF 防护服务，在政务云流量入口架设 WAF 防护服务，实时升级漏洞补丁，配置防护策略，起到前端防护作用。

1)、政务云平台主要划分为电子政务外网区和互联网区，互联网用户不能直接访问政务外网区。

2)、云平台需满足基于通用网络技术提供相关网络服务，能实现自动化动态的网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接。

政务外网接入要求具备政务外网的接入条件，链路稳定可靠。同时，云平台要求支持 IPv4、 IPv6 双栈协议，支持 IPv4 和 IPv6 地址能力。

3)、上云托管业务系统，不能因为部署虚拟化技术而改变原有的安全区域划分和互访规则，委办局之间应实现安全逻辑隔离，委办局内的业务通过安全组逻辑隔离。

2.3.3 云计算平台技术要求

1） 云计算平台整体技术架构应优先采用主流技术框架，选择国产具有自主知识产权且具有成功案例的软硬件产品，为平台后续长期、安全、稳定运行提供基础。云平台能够支撑目前市场上主流的操作系统和数据库产品。

2） 云计算平台整体应提供完善的安全体系架构，包含但不限于物理安全、网络安全、虚拟化安全、云平台安全和安全管理等层面内容，并为主机安全、应用安全、数据安全提供必要的服务能力。

3） 云计算平台应提供完善的接口，包含但不限管理平台、虚拟化平台、用户服务平台、网络、安全、存储系统等标准接口，具备纳管相关物理设备及系统的能力，同时具备与云监管平台、备份平台对接的能力。

4） 云平台应具备资源动态调整机制，根据业务系统运行情况进行资源的动态调整，并承诺短期内提供免费的云资源扩展服务（不超过原有资源的 20%）。

5） 政务云不允许云服务商与互联网公有云构建混合云进行统一的资源调度管理。

6） 云平台支持“一云多芯”,稳定支持基于主流技术架构以及基于 x86 架

构芯片，适配兼容国产化操作系统。

7） 信创云平台安全资源池与国产化服务器架构适配，能够满足信创云场景下的安全防护需求。

8） 托管在政务云平台上的用户业务数据不得离开政务云机房。

9） 云平台应打通虚拟机之间数据壁垒，促进数据整合。应具备通过大数据解决方案对平台内沉淀的业务数据进行采集、分析、应用的能力。云服务商通过云计算平台框架，为客户的大数据解决方案提供具有完备性、一体化、高集成的技术架构，对平台沉淀的数据进行整合、分析，并满足包括离线计算、实时分析、流计算等场景在内的大数据应用需要。提供全方位的大数据安全防护的能力，包括多租户的隔离及面向互联网应用的完备的安全防护体系。

10） 云服务商所投云平台支持 1:1 以及 N:1 容灾服务。用户可以通过管理平台申请对自己的部分或全部虚拟机做容灾，用户可以自行配置容灾策略，包括虚拟机存储的同步/异步数据复制策略，以及数据复制周期等。

11） 云服务商建设的西城区二龙路、西城区卫健委、天宁一号等数据中心节点，应能实现同城异地云平台的数据互通、主机互备、应用备份的容灾要求。

2.3.4 安全要求

云服务商应提供基础安全保障服务，基础安全保障服务是云平台层安全保障能力，包括安全管理服务（运维人员管理、机房运维管理、应急演练）和安全技术服务（物理访问控制、机房三防服务、设备访问审计、出口流量监测、本地 DDoS 防护、防火墙安全防护、防入侵监测 IPS、远程接入服务、租户隔离、租户内部访问控制、云主机监控、角色权限管理）。

云服务商应配合开展信息系统入云部署、测试、上线、运维、退出，实现入云信息系统的运维管理、应急预案等方面的要求，提供每周 7*24 小时技术支持服务。

1） 投标人所提供云平台应符合国家及行业标准、规范，云计算平台必须满足信息安全等级保护三级和密码评估测评相关要求。云服务商在云计算平台建成

半年内必须通过信息系统安全等级保护三级测评，并及时完成公安部门备案手续，云管理单位有权按照测评结果要求云服务商进行整改，云服务商需完成整改工作并通过安全测评且等级保护三级系统需每年进行测评。

2） 云服务商需要支持分步搭建政务云的互联网区和政务外网区，两个区域采用独立的物理网络系统、安全系统和云操作系统软件；

3） 云服务商此次提供独立安全域部署、云安全服务等所需的安全设备服务；

4） 在单一政务云平台内部，云服务商需要实现不同政府用户间业务应用系统及数据的安全隔离；

5） 云服务商在未经过用户邮件、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。

6） 运维及安全保障服务

云服务商提供的政务云环境应在等保三级基础上，按各业务系统具体安全需求，开展相应等保评估、检查、整改等工作。

（1）服务规范

云服务商须严格按照《北京市市级政务云管理办法》、《北京市西城区政务云管理办法》以及采购人制定的管理办法及流程等相关制度，开展标准化运维工作。

（2）服务方式

云服务商需利用监控系统或人工对机房环境、硬件设备的运行情况进行每周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。

云服务商负责设立技术支持热线，并安排专人值守，为运维工作提供 7*24 小时热线支持服务。云服务商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。

云服务商须每周和每月提供政务云服务报告，其中周报主要报告主要云资源

调整及使用情况，针对各信息系统云效率进行统计；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。

（3）安全及保密要求

云服务商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。

（4）响应的及时性

云服务商应提供高效的系统维护服务，有效防范系统风险，保证 7*24 小时电话畅通，发生故障应在 15 分钟内响应；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 1 小时内到达运维现场提供服务。系统发生宕机问题时，云服务商应在 30 分钟内响应，在 4 个小时之内使系统恢复正常。具备故障快速定位和恢复能力，故障定位排除时限不超过 30 分钟，重要信息系统故障定位排除时限不超过 10 分钟。故障处理完毕后提供相关系统宕机报告。

（5）重点保障要求

云服务商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。

（6）安全保障要求

云服务商云平台具备完备的安全防护体系和安全防护设备，具有成熟的安全运维方案，应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，应能满足不低于网络安全等级保护（GB/T22239-2019）第三级要求，并积极配合采购人根据各业务系统具体等保需求，开展相应等保评估、检查、整改等工作。

（7）业务系统迁移及部署调整要求

本项目涉及的业务系统目前在北京市政务云上平稳运行，如云服务商需进行系统迁移，应确保在 5 个工作日内完成业务系统迁移部署工作，且不能影响业务系统的正常运行，如因系统迁移导致最终用户系统损坏、数据丢失，一切后果均

由云服务商承担。

如采购人业务需要，云服务商须配合开展信息系统入云部署、测试、上线、运维、退出，配合建立入云信息系统的运维制度、应急预案等，提供 7*24 小时技术支持服务。

2.4 管理机制

2.4.1对云服务商的管理机制

考核机制

对云服务商的考核包括初期建设验收、中期建设验收、年度服务考核、合同期服务验收评价。

1)、初期建设验收

初期建设验收指在云平台初步完成建设并具备基础服务能力后开展的阶段性验收，旨在检验云平台功能和性能、云服务商提供服务的能力和云服务商持续服务的扩展能力，以确保云平台能够实现支撑基础服务、基础安全保障服务目录要求的所有功能，确保云服务商具备为用户提供标准化服务的能力。

由云管理单位组织，云安全监管服务商协助组织并具体执行对云平台初期建设成果的验收。验收内容包括：

- 检测云平台基础功能和性能指标是否实现，包括支撑基础服务目录、基础安全保障服务目录相关服务的功能。
- 审查业务支撑文档，包括用于指导用户使用政务云的“云服务商服务水平规范”、“业务系统迁移技术指导方案”、“云服务使用流程及模板”、“云内业务系统应急预案及应急演练指导书”，用于内部运维的“云运维工作方案及流程”、“云平台安全管理方案”、“云平台应急预案”、“云年度工作计划书”等。
- 审查云管理平台二次开发计划、云平台扩展功能实现计划。
- 其他事项，如机房环境的合规性等。

验收通过后，在政务云网站公示验收结果并发布“云服务商服务水平规范”、

“业务系统迁移技术指导方案”、“云服务使用流程及模板”、“云内业务系统应急预案及应急演练指导书”。

验收不通过的云服务商，限期 1 个月整改并做二次验收。

2)、中期建设阶段性验收

中期建设阶段性验收指在云平台运行 6-12 个月开展的阶段性验收，旨在检验云平台扩展能力的实现及相关运营和技术问题的整改情况，以确保云服务商能够实现招标文件规定的全部要求。

由云管理单位组织，云安全监管服务商协助组织并具体执行对云平台建设成果的验收。验收内容包括：

- 检测云平台支撑扩展服务的功能和性能指标是否实现；
- 检查云管理平台二次开发功能是否实现，是否通过等保三级测评、密码应用与安全性评估和第三方网络安全审查。
- 抽检云服务商对云管理平台的应用情况，如云主机创建和审核记录、工单记录等
- 审查相关整改完成情况（如有）
- 审查业务支撑文档的修订情况（如有）

验收通过后，在政务云网站公示验收结果并发布相关业务支撑文档修订版。

验收不通过的云服务商，视情况在验收后限期 3-6 个月整改并做二次验收。

3)、云服务商服务质量年度评价

- 云服务商运维服务绩效考核，由云安全监管服务商建立评价指标体系并具体执行
- 云平台能力年度评估
- 用户满意度调查

4)、合同期服务考核

合同期服务考核是指自服务期开始起满三年对云服务商的服务能力等进行

整体总结和评价。

失信行为

当云服务商在云服务期内出现下述情况之一的，将被视为失信行为计入企业信用报告，并“信用北京网”公示。严重的将被取消云服务商资格。

1)、云服务商在限定期限内不能满足投标文件承诺的服务要求的，如：云平台未通过等保三级测评、未通过密码应用与安全性评估、未通过第三方网络安全审查、云平台不具备资源动态调整能力等。

2)、云服务商拒不配合跨云平台业务系统双活、不配合业务系统迁出或下线。

3)、在重大保障时期因云服务商自身原因发生全局性服务中断事件，经政务云管理单位认定属实的。

4)、在服务期内，云服务商因自身技术平台或管理不善，导致用户数据流出政务云机房而造成泄露或非法利用用户数据的。

5)、经查证，云服务商存在利用政务云平台为非政务云用户提供服务的情况。

6)、发生“重大违约行为”且对云管理单位的处罚结果拒不执行的。

7)、初期建设验收未通过且整改后不合格的。中期建设验收未通过且二次验收仍不合格的，难以继续提供合格服务的。

违约责任

政务云服务商服务期内须严格遵守服务质量承诺及相关管理规定确保服务质量，对于违反服务质量承诺和服务水平约定造成服务质量下降的，由政务云管理单位进行相应的处罚。云服务商可参照《重大违约行为表》、《严重违约行为表》、《一般违约行为表》，在投标文件中制定罚则条款，承诺的罚则条款及处罚力度应不低于招标文件要求。云服务商应承诺罚则条款将被用于云服务商与招标人签订的合同以及云服务商与用户签订的云服务协议。

1)、违约行为分类

重大违约行为：云服务商服务期内的违约行为造成云平台整体故障（非不可抗拒力条件下)或重大安全事故的(根据其严重程度分为 A 级事件和 B 级事件)。

云服务商触发该违约行为将被视为“政务云失信”、取消云服务商资格，同时云管理单位将向相关部门及单位通报处罚结果。

严重违约行为：云服务商在服务期内的违约行为对用户业务系统产生一定的经济损失，但其影响和经济损失未达到重大违约行为中规定的 B 级事件的。

一般违约行为：云服务商在服务期的违约行为对用户业务系统造成的影响未达到重大违约行为和严重违约行为的其他违约行为。

2)、违约处罚

表：重大违约行为表

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（云服务商主责）	服务中断	云平台整体	因非不可抗力造成超过 30%以上业务系统中断、影响人数 50 万以上、导致 500 万元以上经济损失。	2 小时以上	A 级	1 次
	重大篡改事件	应用系统	在重大或特别重大保障期间，因云服务商的安全隐患原因造成的系统被恶意篡改事件。事件发生后云服务商未按照应急预案进行处置，造成信息安全事件处置延误。且该事件被国家级机构或媒体通报、区级领导批示或关注的。	30 分钟以上		
	数据丢失	等保三级或重要业务系统的核心业务数据	因非不可抗力造成的云平台超过 3 个业务系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要业务系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成业务系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。	——		
	服务中断	云平台整体	因非不可抗力造成超过 10%至 30%业务系统中断、影响人数 10 万以上、导致 100 万元以上经济损失。	2 小时以上	B 级	一年内 3 次以

类别		范围	影响	影响时间	事件级别	次数
	重大篡改事件	应用系统	因云服务商的安全隐患原因造成的系统被恶意篡改事件，事件发生后云服务商未按照应急预案进行处置，造成信息安全事件处置延误，且该事件被市级机构或媒体通报、区级领导批示或关注的。	30 分钟以上		上
	数据丢失	业务系统核心业务数据	因非不可抗力造成 1 个业务系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	业务系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成业务系统被恶意篡改或敏感信息泄露事件。	——		

a) 严重违约行为

罚款金额=业务系统云服务费/服务月数*惩罚系数（惩罚系数参见《严重违约行为表》）

表：严重违约行为表

序号	问题描述	惩罚系数
1	所提供的云服务可用性低于 99.99%，或数据可用性低于 99.9999%，出现问题并造成重大损失的	200%

2	因未做好系统和数据互备，由于另一家云服务商服务中断，而导致系统和数据无法正常应用的，但影响未达到B级及以上事故影响的	200%
3	因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响	600%
4	因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响	600%
5	因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响	600%
6	在云安全监管服务商已发出整改通知后未正确处置，出现问题并造成重大事故	200%
7	平均响应时间大于15分钟且小于30分钟，造成重大事故	200%
8	运维需求平均响应时间大于30分钟且小于60分钟，造成重大事故	200%
9	运维需求平均故障恢复时间大于30分钟且小于60分钟，造成重大影响	100%
10	运维需求平均故障恢复时间大于60分钟且小于120分钟，造成重大影响	200%
11	现场无人值守超过大于1小时且小于2小时，造成重大事故	100%
12	现场无人值守超过大于2小时且小于4小时，造成重大事故	200%

b） 一般违约行为

罚款金额=业务系统云服务费/服务月数*惩罚系数（惩罚系数参见《一般违约行为表》）

表：一般违约行为表

序号	**问题描述**	**惩罚系数**
1	所提供的云服务可用性达不到99.99%，或数据可用性低于99.9999%，出现问题但未造成重大损失的	50%

2	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，且在服务期内接到用户投诉此类情况 3 次以上的	20%
3	在运营期间，甲方对乙方实施月度考核，如乙方连续 3 次未能通过考核，经限期整改后仍不能达到甲方要求的	20%
4	在运营期内，如乙方未能按照用户方的扩容需求，在 7 个自然日内完成云平台的资源扩容，且经管理单位书面通知仍未能限期满足用户需求的	20%
5	因所提供的云服务或安全服务出现故障，造成某系统宕机 2 小时以上	30%
6	因所提供的云服务或安全服务出现故障，造成某系统连续宕机 3 次以上或累计 8 小时以上	60%
7	在云安全监管服务商已发出整改通知后未正确处置，出现问题的，未造成重大影响	50%
8	运维需求平均响应时间大于 15 分钟且小于 30 分钟，出现问题但未造成重大影响	30%
9	运维需求平均响应时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	50%
10	运维需求平均故障恢复时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	30%
11	运维需求平均故障恢复时间大于 60 分钟且小于 120 分钟，出现问题但未造成重大影响	50%
12	现场无人值守超过大于 1 小时且小于 2 小时，出现问题但未造成重大影响	30%
13	现场无人值守超过大于 2 小时且小于 4 小时，出现问题但未造成重大影响	50%

退出机制

1)、服务期内，如政务云服务提供商提出退出要求，需至少提前 6 个月向政务云管理单位提出退出申请。

2)、服务期内，若由于服务提供商服务能力不能满足约定要求，政务云管理单位可要求服务方退出，相关补偿费用双方另行协商；云服务商应无条件免费配合各方完成迁移和切换工作，切换期一般延续 6 个月。

3)、服务期满后，若政务使用单位和云服务商之间不再续约，云服务商应无条件免费配合各方完成迁移和切换工作，切换期一般延续 6 个月。

4)、若产生其它相关费用，由政务使用单位和云服务商另行协商。

进入退出流程后，云服务商应无条件配合政务云管理单位和用户单位妥善做好退出善后工作，云服务商应确保退出前用户业务系统的稳定性，不得因退出行为对用户业务系统造成影响，否则，根据政务云相关管理办法追究涉事云服务商责任。政务云退出流程主要包含以下阶段：

1)、发起退出流程

触发退出条件后，由云服务商发起退出流程。

2)、制定退出计划

云服务商制定科学合理的退出计划，经云安全监管服务商和云管理单位审核通过并公示后，通知用户单位。

3)、用户迁移

云服务商在退出流程发起之日起不得再接受新的用户入云申请，现有入云项目未完成的根据实际情况与用户单位协商后处理，不得因退出影响业务系统运行。退出云服务商须在规定时间内完成现有业务系统的迁移工作，应无条件配合系统迁出工作。

4)、基础设施腾退

业务系统全部迁出后，云服务商须在规定时间内完成现有云基础设施的腾退离场工作，并接受云安全监管服务商全程监督。现有云基础设施拆除前应对现有设备数据进行安全擦除并配合相关管理单位审查，审查合格后方可退出，防止因服务商设备腾退发生数据泄露事件。

统一信息发布机制

为保证政务云运营工作公开透明，云管理单位通过周报、月报、短信等不同形式通报政务云运行管理情况，通过政务云门户、工作动态等方式向政务云用户通报政务云运行、使用、发生事件、云服务商绩效考核等内容。

2.5 云服务商特殊资质要求： 无。

2.6 技术承诺（本部分为★条款，投标人未提供书面承诺，将被视为无效投标）

★1.采购人的业务系统大量依托于北京市西城区政务外网环境建设，为确保相关业务正常运行，投标人须承诺在合同签订后5个工作日内具备北京市西城区政务外网环境。

★2.投标人中标后进行系统迁移所产生的系统迁移费由投标人承担。

★3.中标人（云服务商）提供的政务云服务须按公安部等保三级的标准建设，并承诺协助采购人通过等保三级的测评和备案。

承诺函格式:

承诺函

致北京市西城区数据局：

我单位参加了西城区2025年政务云（云服务商）采购项目投标，若我单位中标，我单位在此承诺：1、在合同签订后5个工作日内具备北京市西城区政务外网环境。2、中标后进行系统迁移所产生的系统迁移费由我单位作为中标人承担。3、我单位作为中标人（云服务商）提供给采购人（北京市西城区数据局）的政务云服务将按公安部等保三级的标准建设，并将协助采购人通过等保三级的测评和备案。若我单位违背上述承诺，采购人有权取消我单位的中标资格，对我单位的违约行为采取合同约定措施。

法定代表人签字：

单位名称：（盖章）

日期:

2.7政策性采购需求

为在项目中充分落实《政府采购法》规定的“政府采购应当有助于实现国家的经济和社会发展政策目标”等相关要求，以项目为载体推动北京市环境社会治理(ESG)体系高质量发展，请供应商提供在本项目中落实ESG理念的工作措施。

2.8 项目验收及付款要求

2.8.1 项目合同金额以公开招标中标金额为准， 为完成合同约定内容、服务质量评估等各环节合格后的含税价格。甲方（采购人）分三次向乙方支付此合同的全部款项：

第一次付款：甲方向乙方支付第一笔款，即合同总额的50%。在满足先决条件： 合同签订、甲方收到乙方开具的发票并办理完审批手续后的15个工作日内

完成此次付款；

第二次付款：甲方向乙方支付第二笔款，即合同总额的 30%。在满足先决条件： 本项目服务周期满十一个月并完成阶段性验收，且甲方在收到乙方开具的发票并办理完审批手续的 15 个工作日内完成此次付款。

第三次付款：甲方向乙方支付第三笔款即支付至项目审计总额。在满足先决条件：本项目根据据实结算方式计算的年度服务费支付价格达到本项目合同总限额、最终使用量及验收合格，审计结束（财政结算、决算审计或第三方审计机构的出具审计结果），甲方在收到乙方开具的发票并办理完审批手续后的 15 个工作日内完成此次付款。

2.8.2 项目验收要求：乙方按合同要求在服务周期内完成合同约定服务内容，向甲方提出验收申请，甲方负责组织专家进行验收评审，出具书面验收报告。验收服务标准如下:

1)、中标人（云服务商）为采购人提供的服务质量应符合国家或相关行业的标准。

2)、按照对应的合同内容填写服务内容，验收标准。

（注：请根据具体服务内容在本条款内明确具体的质量要求或验收标准）

3)、中标人（云服务商）完成合同全部工作后应及时通知采购人进行最终验收。采购人组织验收合格的，采购人在验收合格报告上签字；验收不合格的，中标人（云服务商）应当在 10 个工作日内进行调整，并重新提交采购人验收。

4)、合同最终验收合格后，中标人（云服务商）应向采购人提交如下合同成果：

（1）服务事项 1：中标人（云服务商）应向采购人提供可验收的成果物如：周报等_；

（2）服务事项 2：中标人（云服务商）应向采购人提供可验收的成果物如：月报等_ ；

（3）服务事项 3：中标人（云服务商）应向采购人提供可验收的成果物如：重大活动保障服务方案和总结报告等。

3、服务目录和取费要求

3.1 取费要求

1） 政务云管理单位确定政务云规模、服务内容，每年年底按照实际服务使用量进行据实核算，由政务云管理单位统一向云服务商支付。

2） 云安全基础服务是云服务商应具备的云平台层安全保障能力，用户无需购买即可享受服务。

3） 云服务目录是本次采购服务目录，价格为年底核算最高限价。

3.2 政务云服务目录

3.2.1 政务云基础安全服务目录（必选项）

编号	服务类别	服务子类	服务项
1	安全管理服务	运维人员管理	运维人员值班管理、安全登记
2		应急演练	协助云管理单位进行安全应急演练
3	安全技术服务	租户隔离	租户虚拟化层隔离
4		租户内部访问控制	租户内部访问权限控制，用户可以自由分配
5		云主机监控	提供云上资源的基本监控，包括 CPU、GPU、NPU、内存使用率等
6		角色权限管理	提供通过代入角色实现获取操作权限
7		云虚拟防火墙	配置云虚拟防火墙规则保护租户的资产
8		虚拟 WAF	提供虚拟化 web 应用安全防护能力。包含

编号	服务类别	服务子类	服务项
			系统升级、规则库升级。网络吞吐大于150Mbps，每秒新建连接数不小于2000。

3.2.2 政务云基础服务目录（必选项）

编号	服务类别	服务子类	服务项	计价单位	报价单位
1001	计算服务	云主机服务（提供信创和非信创服务）	vCPU（主频不低于2.2GHz）	1 vCPU	元/月
1002			内存	1 GB	元/月
1003		云基础计算服务：视频、图形图像计算服务	GPU显存不低于8G，最大单精度浮点计算能力不低于0.15TFLOPS	1GPU	元/月
			GPU显存不低于12G，最大单精度浮点计算能力不低于5TFLOPS	1GPU	元/月
			GPU显存不低于16G，最大单精度浮点计算能力不低于7TFLOPS，最大双精度浮点计算能力0.2TFLOPS	1GPU	元/月
			NPU内存≥24GB，最大单精度浮点计算能力不低于7TFLOPS，最大双精度浮点计算能力0.2TFLOPS	1NPU	元/月
1004	存储服务	普通性能存储	普通存储(单盘技术指标:单盘IOPS 1000-3000)	1 GB	元/月

1005		高性能存储	高性能存储(单盘技术指标:单盘 IOPS 3000-20000)	1 GB	元/月
1006		视频云存储	满足海量视频数据的存储需求	1 TB	元/月
1007	网络服务	主机负载均衡服务	主机负载均衡服务	1 IP	元/月
1008		远程接入服务	远程接入服务	1 账号	元/月
1009		VPN 服务	SSL VPN 接入	1 套	元/月
			IPSec VPN 接入	1Mb 带宽	元/月
1010		WAF 防护	web 应用防火墙服务	1 IP（互联网）	元/月
1011		SSL 证书服务	提供 SSL 证书服务	1 域名	元/月
1012	云主机深度监控服务	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	1 主机	元/月

3.2.3 政务云基础安全保障服务目录（必选项）

政务云基础安全保障服务目录（不计费项）			
编号	**服务类别**	**服务目录**	**项目**
2001	安全管理	运维人员管理	7x24 小时运维人员管理、安全登记

2002	服务	机房运维管理	机房设备管理、安全控制
2003		应急演练	协助云使用单位进行安全应急演练
2004	安全技术服务	物理访问控制	机房进出控制、监控等
2005		机房三防服务	机房防火、防盗、防雷电
2006		设备访问审计	设备访问记录、日志统计、安全事件
2007		出口流量监测	出口流量控制、检测，并且可观测数据，互联网网络行为审计
2008		本地抗 DDoS 防护	云平台整体提供总带宽为 10Gb 的抗 DDoS 防护
2009		防火墙安全防护	出口安全
2010		防入侵监测 IPS	防入侵监测
2011		远程接入服务	免费提供 1 个远程登录堡垒机的运维账号
2012		租户隔离	租户虚拟化层隔离
2013		租户内部访问控制	租户内部访问权限控制，用户可以自由分配
2014		云主机监控	提供云上资源的基本监控，包括 CPU、内存使用率等
2015		角色权限管理	提供通过代入角色实现获取操作权限

3.2.4 政务云扩展服务目录（必选项）

编号	服务类别	服务子类	服务项	计价单位	报价单位	备注说明
3001	迁移服务	云主机迁移	每个 VM 业务迁移	1 台	元/次	由云服务商提供委办局现有虚拟化业务迁移上政务云，包括迁移前调研、迁移、测试、上线、技术支持服务。（不包括迁移到托管区） 由云服务商提供委办局
3002	安全服务	物理主机迁移	每台物理主机迁移	1 台	元/次	

						现有物理主机业务迁移上政务云，包括迁移前调研、迁移、测试、上线、技术支持服务。（不包括迁移到托管区）
3003		单机数据库迁移	数据迁移服务（包括商用数据库和开源数据库）	1 套	元/次	由云服务商提供委办局现有单机数据库业务迁移上政务云，只限于同构数据库架构迁移，包括迁移前调研、迁移、测试、上线、技术支持服务。（1 套为 1 个数据库实例）
3004		高可用数据库迁移	数据迁移服务（包括商用数据库和开源数据库）	1 套	元/次	由云服务商提供委办局现有高可用（例如 HA、ORACLE RAC)数据库业务迁移上政务云，只限于同构数据库架构迁移，包括迁移前调研、迁移、测试、上线、技术支持服务。（1 套为 1 个数据库实例）
3005		云端抗 DDOS 服务	云端抗 DDOS 服务	1 站点	元/月	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）
3006		云端 APT 防护服务	云端 APT 防护服务	1 套	元/月	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。
3007		主机杀毒服务	主机杀毒服务	1 台	元/月	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。
300		主机防	主机防护	1 台	元/月	主机防护：提供符合等

8	安全检测监测、审计服务	护				保三级要求的主机权限管理及安全防护。
3009		主机安全加固	主机安全加固	1 台	元/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。
3010		网页防篡改服务	网页防篡改服务	1 监控点	元/月	提供网页防篡改服务。通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性。
3011		主机漏洞扫描	主机漏洞扫描	1 台	元/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。
3012	其他服务	主机日志分析	主机日志分析	1 台	元/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
3013		数据库审计服务	数据库审计服务	1 套	元/月	支持 Oracle、SQL-Server、DB2、MySQL 等数据库审计。（1 套为 1 个数据库实例）。
3014		CDN 加速	提供内容加速及视频加速服务	1GB（流量）	元/月	将源站内容分发至最接近用户的节点，使用户可就近取得所需内容，提高用户访问的响应速度和成功率。
3015		本地备份服务	本地备份服务	GB	元/月	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）

3016		异地备份服务	异地备份服务	GB	元/月	通过备份策略实现文件、操作系统、数据库的异地备份（不包含备份存储空间费用）
3017	技术扩展服务	智能中枢平台服务	硬件算力服务，城市智能中枢-AI 运营管理中心、政务 AI 开发运营平台、算法场景优化服务等内容。	1	年	提供平台通用算法服务，包含：视频类、OCR 类、语音类、NLP 类等通用算法。

3.2.5 政务云商用密码安全共性服务目录（必选项）

编号	服务类别	服务子类	服务项	计价单位	报价单位	备注说明
4001	商用密码安全共性服务	密码机	云密码机	系统	元/月	为租户应用提供硬件密码能力。
4002		身份鉴别	协同签名服务 1、重要数据不可否认性； 2、有结构化数据外发、或者字符串等数据外发时，选择时间戳服务	系统	元/月	满足“应用和数据安全”层面建设要求，提供标准时间戳服务，将交易时间和交易内容固化，适用于时间敏感型业务数据的安全保护。

4003			签名验签服务	系统	元/月	满足“应用和数据安全”层面的“身份鉴别”、“数据存储完整性”等，提供PC端登录认证能力，基于国密多种算法的签名验签服务，例如：支持PKCS#1、PKCS#7、Attach等多种签名格式。
4004			动态令牌认证服务（OTP）	系统	元/月	满足“应用和数据安全”层面的“身份鉴别”。适用于业务系统为一般公众系统，如政府网站。
4005		数据传输/存储机密性、完整性	数据加解密服务1、访问控制信息完整性； 2、数据存储机密性和完整性； 3、数据传输的机密性和完整性。	系统	元/月	满足“应用和数据安全”层面建设要求，提供数据加密服务，支持多种隐私数据加密模板，隐私数据加密支持密文检索。

4006			数据库透明加密服务：该服务仅针对结构化数据。	系统	元/月	满足“应用和数据安全”层面建设要求，提供多种类型数据库透明加密服务，支持包括 MySQL、达梦、神通等主流数据库，支持表加密、数据库后置扩展列加密。
4007			文件加密服务	系统	元/月	满足“应用和数据安全”层面建设要求，提供透明的文件系统加密服务，支持 ext2、ext3 等 Linux 常见文件系统，支持 NAS、NFS 等网络存储。

4、时间进度要求

云服务商应在 50 个自然日内完成政务云平台建设和测试等工作，并投入试运行。

云服务商在服务期内应根据用户方的扩容需求，可在 15 个自然日内完成云平台的资源扩容。

5、其他

部分建设内容、边界、范围以及管理规定等需要在招标完成后（如：机柜分配和使用等），由中标方会同招标方共同商定，通过签署相关协议、合同或备忘录加以约定。

未尽事宜，由西城区政务云管理单位和云服务商再行商议。

第三章 西城区政务云服务商需求说明

1、 概述

本次采购选定的云服务商，云服务商提供计算、存储、网络、云安全、商用密码共性服务等云服务。云服务商为西城区提供统一云服务，确保业务应用稳定可靠运行，满足信息系统业务未来新增上云需求。

云服务商平台提供的服务应满足《信息安全技术云计算服务安全能力要求》（GB/T 31168-2014）、《信息安全技术云计算服务安全指南》（GB/T 31167-2014）、《北京市政务云安全技术规范—IaaS 云计算平台分册》、《北京市政务云安全技术规范—IaaS 云计算平台安全监管接口分册》、《北京市政务云安全技术规范—信息安全服务接口分册》、《云计算关键领域安全指南 V4.0》、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14 号）及国家主管部门发布的其他标准规范要求。

为了保证云平台的服务质量稳定可靠，降低云平台对电子政务业务系统的影响和风险，云服务商应在服务方案中提供“云服务质量考核标准与故障处理办法”，考核内容应包含但不限于云服务考核标准、故障处理考核标准、合同执行考核标准等，并针对云服务质量考核未达标的情况，陈述云服务商自愿承担的责任义务和惩戒措施。

1.1 服务范围

参照《北京市市级政务云管理办法》、《北京市西城区政务云管理办法》的规定，政务云按照“统筹规划、适度超前、分级管理、资源共享”的原则建设和管理，除公安、国家安全等部门以及涉密和信息安全等级保护四级（含）以上信息系统外，各单位现有信息系统应逐步迁移至政务云，凡政务云已具备服务能力的，软硬件原则上不再新购。

1.2 云服务商服务内容

云服务商提供包含但不限于如下服务：

1.2.1 科学、规范、可执行的云服务管理体系。

1.2.2 基础设施资源服务：包括计算资源服务、存储资源服务、网络资源服务及其他服务内容。

1.2.3 基础软件支撑服务：云服务商须具备对主流操作系统和主流数据库的服务能力。

1.2.4 信息安全服务：包括安全防护服务、安全监测服务、安全运维服务、安全接入服务、安全管理服务等。

商用密码共性服务：提供上云系统所需的商用密码共性服务，提升系统安全防护水平，切实满足信息系统密码应用基本要求。

1.2.5 建立健全配套制度标准：需提供基于自身平台的相关标准、管理办法及预案。

1.2.6 建立健全满足云监管服务需要的配套检测、监管手段及相应监测办法。

1.3 云服务商服务要求

云服务商需满足包含但不限于如下要求：

1.3.1 部署在西城区政务云平台上的各部门业务系统、所有数据的所有权及使用权均属于政府，云服务商无权对其进行支配。若发现云服务商未经许可对业务系统和数据进行采集和使用，政务云管理单位将对其采取惩罚措施并追究其法律责任。

1.3.2 云服务商应构建可靠稳定的平台，保障政务云平台可靠运行，可在最短时间内对用户的应用系统进行快速响应、处置和恢复。

1.3.3 云服务商提供的政务云平台整体可用性应不低于 99.99%，数据可靠性应不低于 99.9999%。

1.3.4 承担自身建设、运营的政务云平台（主要包括计算资源、存储资源、网络资源）的安全责任。

1.3.5 接受云安全监管服务商要求，并提供相关计算、存储、网络等资源监

控及安全接口，支持二次开发与定制维护。

1.3.6 禁止云服务商在政务云内搭建自身业务系统和非政务业务系统。

1.3.7 云服务商需具备为政务云用户提供优质及定制化服务的能力，方便用户了解、申请、使用、管理、监控云资源的情况。

1.3.8 对自身平台出现的重大运维问题、事故，需第一时间向云监管单位、政务云使用单位、云管理单位通告。

2、 总体技术要求

2.1 设计原则要求

2.1.1 依据招标书中针对本次扩容的需求说明内容，对本项目系统建设需求进行细化和归纳总结，要充分体现投标方系统分析的能力和对本项扩容工作相关业务和技术方面需求的理解。

2.1.2 此次扩容云平台应采用具有先进、稳定、成熟云平台技术的云平台，云服务商所投云平台应具有省部级政务云平台运营相关案例。

2.1.3 要遵循当前业界认可的、先进的技术思想和国际标准，尤其是要遵循国家和北京市电子政务及政务云平台相关标准规范。

2.1.4 要考虑软硬件支撑环境的先进性，更要考虑系统结构、应用设计和数据结构的可扩展性，以适应后续新开发和新部署系统上云的发展需求。

2.1.5 本次云平台扩展是为了承担未来西城区政府部门上云的系统，这些系统是面向各级西城区政府部门、项目单位和广大的社会公众提供相关服务的，涉及大量政府信息，因此要确保此次扩容云平台运行的稳定和安全可靠。

2.2 总体设计要求

投标人以扩展云平台的合理性、与现有云平台的融合性、进度要求为总约束合理规划，科学组织、编制可行的扩容实施方案，方案中应包括（但不限于）政务云资源规划方案，安全保障方案，应急保障方案，运维保障方案。

本期建设扩容云平台的网络出口和安全保障设备共用原政务外网区的网络出口和安全资源，达到简化网络结构、快速上线、提升云平台的整体服务能力的目的。

基础设施服务满足本期扩容政务云平台（主要包括国产化云以及信创云）的计算、存储、网络、安全等有关需求，基础设施服务层通过部署云管理平台、云调度平台、云虚拟化平台，将本期部署的硬件设备（计算设备、存储设备、网络设备）通过云计算技术构筑为计算资源池、存储资源池、网络资源池，为政务应用提供按需获取的资源。

要保障政务云计算中心的稳定高效运行，除了信息安全保障体系之外还需要一个良好的运维体系，以提供资源管理、调度管理、监控管理等运维功能。

云服务商根据对西城区政务云的理解，结合本次政务云平台扩容的要求，在投标文件中给出实际部署拓扑图。

2.3 总体技术要求

云平台须支持对多个数据中心的虚拟化资源、物理资源进行统一管理，能够实现对多个数据中心纳管资源的统一调配和发放，能够集中进行告警、性能报表和资源报表的展现。

产品提供方须能够保证对产品后续不断的更新升级，包含但不限于对于产品安全性、兼容性和功能性的升级支持。

云管理平台需要提供统一的虚拟化功能和资源池管理能力，采用业界主流的虚拟化技术，云管平台和虚拟化平台能够开放通用标准化的 API 接口，支持第三方平台云管、网管、备份平台的对接。

2.3.1 总体要求

（1） 具有自主知识产权且具有大规模部署案例的国产云、信创云平台产品；

（2） 通过 SDN 控制器实现对网络设备的自动化编排，云

平台支持 VxLAN、VLAN 等组网模式；

（3） 云平台管理节点须支持集群部署，可平滑升级扩展；

（4） 提供统一事件或故障告警展示中心，直接反映事件或故障发生的时间、触发条件、内容、级别，可对告警事件进行状态确认。

（5） 非 OEM 产品，产品为成熟商用产品，保障后续产品的连续性；

云服务商应在投标文件中描述云管理平台方案，描述云管理平台详细服务功能。

2.3.2 云管理平台要求

（1） 统一运营管理功能要求

云平台可以针对对每个部门使用的资源进行计量和计费，用户可以为不同的服务配置不同的费率，可以查看历史定价情况进行参考，并可以查看各个组织的费用情况，或者可以配置定期将费用报告发送到用户邮箱，提供截图证明。

提供虚拟数据中心（VDC）管理能力，并支持在 VDC 下再划分多级子 VDC，以匹配业主的组织/租户体系进行管理。每个 VDC 都可以分配多个数据中心的资源，管理云可以对每个 VDC（组织）可以使用的资源做配额限制。

支持虚拟机服务，配置管理虚拟机的 License。用户可以通过自己的账号登录管理平台来申请虚拟机资源，并且定义自己的虚拟机规格（包括 CPU、内存、磁盘、网卡）；申请到虚拟机后，用户可以通过管理平台对虚拟机执行开机、关机、重启、删除、远程登录、快照、克隆、重置密码等操作，也可以根据虚拟机名称、IP、ID、运行状态以及自定义标签等快速查找、过滤虚拟机。提供截图证明。

支持用户管理。可以支持用户的创建、删除、修改、查询、禁用、重置密码等操作，并且可以限定每个用户可以操作的资源范围；用户忘记密码后，可以通过管理平台通过用户的邮箱或者手机来找回密码。提供截图证明。

支持服务自定义。管理员可以灵活的定义已有服务，配置用户申请服务时需要输入的参数，例如管理员可以指定用户申请虚拟机时是自己指定虚拟机规格还是只能使用固定规格，配置好后可以发布为一个新的服务让用户申请。新的服务发布时可以分别指定用户申请、修改、删除这个服务时是否需要审批，需要被谁审批。支持管理员自定义可以线下实施的任何业务，提供统一的申请、审批、计量、开通能力。提供截图证明。

（2） 统一运维管理功能要求

支持统一的告警管理，云平台可以统一管理系统中物理设备（服务器、存储、网络设备）和虚拟资源的告警，并支持告警的清除、指派、调整级别、设置告警提示音等；支持告警转发能力，系统可以按照管理员指定的规则，将不同类型的告警通过短信或者邮件发送给不同的用户或者用户组进行处理，提供截图证明。

支持报表管理。系统支持基础的容量、资源使用、设备、告警统计报表，并支持报表的自定义呈现，管理员可以对已有的指标进行交叉组合、过滤来进行自助式的业务分析，并生成最终报表，也可以配置定期生成指定报表并发送到指定用户/用户组。

支持容量管理能力。管理员可以按照各种不同的维度（例如按数据中心、按不同资源池、不同的可用分区等）来查看计算、存储、网络资源的使用情况和分配情况，并提供容量趋势预测，评估已有资源消耗完的大致时间，提供截图证明。

支持运维权限控制，运维管理员可以监控系统内所有的物理资源和虚拟资源（而不能对用户 VDC 中的资源进行操作）

提供大屏展示能力。支持用户自定义大屏的展示内容以及布局，支持用户定义多种不同的大屏展示内容，每个大屏都支持容量、性能、资源统计、告警等的自定义展示，且可以定义每个内容的不同呈现形式（例如柱状图、饼图、仪表盘等等），提供截图证明。

提供告警统一管理的图形展示界面，提供按照用户权限展示的告警管理图形展示界面，能够提供：物理、虚拟资源的告警（包括但不限于服务器、存储、网络设备、虚拟机等）；支持通过条件快速筛选告警，筛选条件包括但不限于告警

级别（如紧急、重要等等）、告警状态（如告警是否清除/确认）、告警发生时间、告警名称、告警源、告警所属数据中心等；支持按照资源类型（例如服务器、交换机、防火墙、虚拟机、存储）的维度归类展示告警；支持用户查看告警名称、告警源、位置、来源系统、发生/清除时间、修复建议、处理记录等。

至少支持以下告警通知能力：支持告警管理页面的自动刷新和声光电告警，可以通过短信（SGIP 协议接口）或邮件方式，将符合告警策略的告警通知到指定用户，支持告警转工单的接口（可以后续根据接口协议开发对接）。

支持对系统资源、使用率自定义周期、采集频率生成统计报表和图形展示。

系统资源包含但不限于：系统内虚拟机、系统内 CPU/内存的使用率/使用量、系统内 CPU/内存的分配情况、系统内存储资源使用/分配情况、虚拟机 CPU、内存、磁盘、网络使用等。

报表展示形式包含但不限于：数据报表，饼/环/面积图、条形/柱形图、折线图、表格等；支持报表的文件导出。

2.3.3 虚拟化平台要求

（1） 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性；

（2） 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址、MAC 地址等；

（3） 支持虚拟机设备直通，用户申请虚拟机时，可以申请将 USB、GPU、SSD 等设备映射给虚拟机使用。提供截图证明。

（4） 当虚拟机操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性；

（5） 支持平台巡检功能，支持生成巡检报告并导出；

（6） 虚拟化软件可以在线进行版本升级，不同版本之间可以相互兼容；

2.3.4 云网络系统要求

（1） 上云的电子政务系统，不能因为部署虚拟化技术而改变原有的安全区域划分和互访规则，单部门内的业务通过逻辑隔离划分不同的安全域；

（2） 支持对云平台内的网络设备进行统一管理；

（3） 支持虚拟云平台（VPC）服务，用户可以通过虚拟云平台自由的创建自己的虚拟网络。用户可以自行创建自己要的多个网段，指定每个要创建的网络的网段、掩码、DNS 等，也可以指定这个网络内的路由规则以及 NAT 规则。提供截图证明。

（4） 支持用户通过管理平台为虚拟机申请弹性 IP 以及配置弹性 IP 可用带宽(QoS)。弹性 IP 可以是一组可以访问互联网的 IP 地址，用户可以将申请到的弹性 IP 绑定到应用系统的浮动 IP 或者虚拟机的指定的网卡或者某个特定的政务外网 IP 地址上，以提供虚拟机访问互联网/被互联网访问的能力；用户可以随时查看自己申请的弹性 IP 地址，这些地址是否被使用、被使用到什么地方。提供截图证明。

（5） 支持虚拟负载均衡服务，用户可以通过管理平台自助申请负载均衡器，以及配置负载均衡器的实地址（Server IP）池、虚地址（VSIP）、绑定的公网 IP 等，虚拟负载均衡支持配置四层、七层监听策略以及健康检查策略等，提供截图证明。

2.3.5 云存储系统要求

（1） 高性能存储与普通存储可按应用需求选择不同磁盘类型，实现数据按需存储；

（2） 高性能存储与普通存储应具备较强的扩展能力，存储系统可扩展容量支持 PB 级扩展；

（3） 高性能存储单盘技术指标 IOPS 3000-20000 ，普通存储单盘技术指标 IOPS 1000-3000 ；

（4） 高性能存储与普通存储采用先进的磁盘容错技术，在硬盘故障后可实现快速重构，避免重构过程中其他硬盘损坏导致的数据丢失风险；

（5） 高性能存储与普通存储可靠性达到 99.9999%；

（6） 备份存储具有可靠的数据保护机制，确保不会因硬盘故障等原因导致数据丢失。

（7） 支持云硬盘服务。用户可以通过管理平台为虚拟机申请磁盘，用户可以将申请到的磁盘空间分配给一台或者多台虚拟机使用。在操作系统支持的情况下，可以对已经在使用的云硬盘进行在线/离线扩容（提供支持在线扩容的操作系统清单），提供截图证明。

（8） 支持块存储服务、对象存储服务、文件存储服务。

2.3.6 云安全系统要求

（1） 云服务商需要做好政务云机房内的用电安全、防火安全和防水安全等基础设施安全；

（2） 云服务商需要制定完善的政务云机房内部物理设备安全操作流程及安全操作步骤，需要能够对操作流程及操作过程进行记录；记录保存最短保存期限为 1 年；并接受出入记录审计；

（3） 为了保证政务云的安全、稳定运营，云服务商需要制定完善的安全运维管理体系，制定完善的安全管理制度规范，对不同的安全区域、安全保护对象明确安全责任人；

（4） 云服务商的安全服务包括不限于如下服务：VPC、安全组、云用户业务隔离、虚拟化安全等；

（5） 云服务商要做好各自的信息安全监控，安全监控内容包含但不限于网络流量监控、各个安全设备的日志记录监控、安全设备运维操作监控和云资源运行状态监控等，可以无条件供云安全监管单位查看调取。

（6） 云平台需支持虚拟防火墙服务，用户可以通过管理平台申请虚拟防火墙

并配置防火墙规则保护自己的资产，并支持用户批量导入/导出防火墙规则。提供截图证明。

（7） 提供用户级别的安全分析和评估服务。用户可以通过管理控制台查看自己的云环境资产或用户的受攻击报告以及易受攻击的点，并且可以通过系统发起对自己云资源的安全评估以及合规性评估，平台可以给出评估报告以及修复方法和建议。

（8） 提供上云系统所需的商用密码共性服务，提升系统安全防护水平，切实满足信息系统密码应用基本要求。

（9） 政务云服务商提供基于用户的不同等级安全服务，并提供安全事态分析，满足用户不同安全级别业务系统的安全需求。

2.3.7 云平台数据库审计服务

按照采购人的具体需求提供数据库审计服务，每月对数据库操作行为进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。对用户访问数据库行为的记录、分析和汇报，生成合规报告以及事故追根溯源。在提供服务的过程中需做好与采购人和对应项目的应用开发厂商的协调沟通工作。

服务频率：每月不少于 1 次审计报告。

3、 云平台技术能力要求

3.1 云服务要求

3.1.1 平台云主机服务

指标项	规格要求
性能限制	按内存不复用方式分配资源，要求 CPU 主频≥2.4GHz
性能范围	CPU 核数可选范围 1-16 核或合理技术评估更高，内存可选范围 1-64G 或合理技术评估更高
操作系统兼容性	支持主流操作系统，需正版授权

扩展性	用户可以灵活调整云主机 CPU、内存、硬盘规格
兼容性	考虑系统兼容性要求，支撑云主机的物理服务器在云平台运营服务期间，应保持设备原厂商的一致性，如设备型号有所变更，应保证变更后设备性能相比原设备有所提升。
云主机隔离	对不同用户的虚拟主机提供安全组和 VLAN 级别的隔离，确保不同用户之间数据互不可见；云主机之间可以做到隔离保护，其中每一个云主机发生故障都不会影响同一个物理机上的其它云主机运行，每个云主机上的用户权限只限于本云主机之内，以保障系统平台的安全性。
安全组	用户可以通过管理平台配置并管理针对虚拟机的安全规则，所有在安全组里面的虚拟机默认都不能通过网络访问，只有用户指定的特定 IP 端或者其它安全组下的资源才可以访问。
管理权限	用户对云主机有完全的控制权，具有管理员权限，使用方式与传统物理主机完全一致。支持虚拟机生命周期管理，支持查询、创建、删除、安全删除、启动、关闭、重启、VNC 登录，支持虚拟机的搜索和过滤。
备份功能	支持云主机备份功能，可以实现云主机的全量备份、增量备份，支持备份周期、备份策略的设定
可操作性	支持通过云管理平台，实现申请部署与使用，提供虚拟机标签分组功能，方便用户根据业务等维度快速定位查找虚拟机资源。
弹性网络	支持虚拟路由、虚拟交换机和弹性 IP，用户可自定义虚拟主机的网络拓扑和 IP 地址；
镜像快照	创建虚拟主机时，可指定用户预先配置好的镜像文件作为模板。虚拟主机支持增量快照备份功能，提高备份效率，减小备份占用空间。
数据存储	虚拟主机底层采用分布式块存储，每个虚拟主机的镜像存储达到多副本可靠性，数据可靠性不低于 99.9999%；
高可用性	虚拟主机服务采用全冗余架构，无单点故障，平均可用性不低于 99.99%。

扩展性	支持计算能力的垂直伸缩，支持对 CPU 和内存的升级与降级操作，支持增加、减少磁盘和带宽；支持计算能力的水平伸缩，通过与负载均衡配合实现水平伸缩。
亲和性/反亲和性	支持用户申请虚拟机时即为虚拟机配置虚拟机的亲和性和反亲和性。在同一个反亲和性组中的虚拟机将尽可能分布在不同主机上，满足虚拟机的可靠性保障要求；在同一个亲和性组中的虚拟机会将虚拟机尽可能放在相同主机上，满足虚拟机启动相关性要求。支持用户查看每个亲和/反亲和性组中的虚拟机。
共享镜像	支持用户申请虚拟机时可以选择管理员提供的全局镜像、用户自己制作的私有镜像和其余用户制作的共享给用户的共享镜像；用户可以通过管理平台导入常见格式的镜像，例如 VMDK、QCOW2、VHD、ZVHD 等；用户可以查看已经上传的所有镜像，包括镜像名称、OS 类型、镜像大小等。
进程管理	支持用户管理虚拟机中进程，配置进程是否是已知进程，是否可信。

3.1.2 普通性能存储服务

指标项	规格要求
可靠性要求	提供普通存储服务，要求稳定可靠，确保数据可靠性 99.9999%。
性能要求	单盘技术指标满足 IOPS 1000-3000.
使用要求	用户可以以 1G 为最小单位进行容量申请，并可以申请直接挂载给云主机使用
架构要求	系统整体架构无单点故障
兼容要求	考虑系统兼容性要求，支撑普通性能存储的物理存储设备在云平台运营服务期间，应保持设备原厂商的一致性，如设备型号有所变更，应保证变更后设备性能相比原设备有所提升。

可操作性	支持通过云管理平台，实现申请部署与使用

3.1.3 高性能存储服务

指标项	规格要求
可靠性要求	要求稳定可靠，不会因单一部件故障、单一路径故障等原因导致业务停用、数据丢失，系统可靠性 99.9999%
性能要求	单盘技术指标满足 IOPS 3000-20000
使用要求	用户可以以 1G 为最小单位进行容量申请,并可以申请直接挂载给云主机使用
架构要求	系统整体架构无单点故障
兼容要求	考虑系统兼容性要求，支撑高性能存储的物理存储设备在云平台运营服务期间，应保持设备原厂商的一致性，如设备型号有所变更，应保证变更后设备性能相比原设备有所提升。
可操作性	支持通过云管理平台，实现申请部署与使用

3.1.4 主机负载均衡服务

指标项	规格要求
服务能力	通过云管理平台实现针每租户按需自动分配负载均衡服务的能力。总体峰值可支持每秒新建链接数不少于 40 万
均衡策略	支持加权轮询(Weighted Round Robin)、加权最小连接数调度(Weighted Least-Connection Scheduling)等流量分发策略
健康检查	可以按照指定规则对配置的虚拟主机进行健康检查,自动隔离异常状态虚拟主机，确保可用性
会话（Sessio	可对虚拟主机提供 TCP/HTTP 协议的负载均衡服务，并提供会话保持功能，在会话生命周期内，将同一会话请求转发到同一台后端虚

n）保持	拟主机
高可用性	采用全冗余或集群架构，无单点故障；平均可用性不低于 99.99%
转发规则	提供多种转发规则，满足不同业务场景的要求
扩展性	支持在线平滑升级，承载能力和网络总带宽同步线性扩容；可与虚拟主机配合提供三层架构系统的弹性扩展
可操作性	支持通过云管理平台，实现申请部署与使用

3.1.5 远程接入服务

指标项	**规格要求**
功能要求	提供堡垒机远程接入服务
运维审计	字符操作审计、图形操作审计、文件操作审计
访问控制	支持基于 IP/IP 段、用户/用户组、资产/资产组、协议、危险级别等组合策略进行访问控制，对于不合法的行为予以阻断；
	可基于运维账号的登陆时间和资产登陆时间进行访问控制；
	可基于运维操作命令进行访问控制；
	可基于主机、用户、IP 地址控制审计日志的访问权限；

3.1.6 VPN 服务：SSL VPN 接入

指标项	**规格要求**
接入方式	实现 Web 接入，TCP 接入，IP 接入等多种方式，记录完整的用户访问日志
身份管理	支持基于用户身份的管理，实现不同身份的用户拥有不同的命令执行权限，并且支持用户视图分级，对于不同级别的用户赋予不同的管理配置权限
访问控制策略	可以根据请求报文的目的 IP 地址和目的端口号、源 IP 地址和源端口号进行过滤

VPN 服务：IPSec VPN 接入

指标项	**规格要求**
国密算法	支持 SM1、SM2、SM3、SM4 国密加密算法

配置方式	通过手工配置或自动配置的方式实现 IPSec VPN 隧道的建立，支持对 IKE 策略、IPSec 策略配置及对 VPN 服务、IPSec 站点连接的申请并提供状态监控，记录完整的用户访问日志
基本功能	实现 IPsec 抗重放检测功能、反向路由注入功能，支持 IPv6 协议

3.1.7 WAF 防护

指标项	规格要求
检测算法	可精确识别包括注入、XSS 等 OWASP Top 10 WEB 通用攻击，有效应对盗链、跨站请求伪造等 WEB 特殊攻击
部署方式	可以通过透明串接或反向代理、路由模式等方式接入网络中，即可对应用层 HTTP 流量进行安全防护
黑名单	通过预定义策略及自定义规则，进行规则匹配，阻断异常流量
可操作性	支持通过云管理平台，实现申请部署与使用

3.2 云主机深度监控服务

指标项	规格要求
云主机深度监控	提供云主机 7*24 小时深度监控服务，并提供相应报告
集中告警监控	支持多维度告警/事件展现
Top 性能监控	提供常用指标的 TopN 性能视图，包括： 1） 服务器、虚拟机的CPU、内存TopN视图； 2） 网络接口流量； 3） 存储读写带宽、读写IOPS、读写IO大小。
安全事件服务	提供主机安全事件的验证、分析，并提供事件报告
应急处置服务	提供特定云主机的应急问题协助排查，协助处理应用故障等服务，并提供相应报告

值守保障服务	提供 5x8 小时的运维值守工作，不仅限于机房巡检、云平台和硬件监控，同时提供问题排查协助、协助处理应用故障等服务，并提供相应报告
报表自定义	支持报表自定义能力，用户可以自定义报表所需要字段（例如是否需要显示资源位置、时间等）、指标（例如是否同时呈现 CPU 总量/使用量/使用率等）。

3.3云基础安全保障服务要求

云服务商自身须具备下列云基础安全保障服务能力并在项目运营管理中向云使用单位提供。

3.3.1 安全管理服务：运维人员管理

指标项	规格要求
岗位设置	设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责
人员配备	至少配备的系统管理员、网络管理员、安全管理员各一名
授权和审批	根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人
离岗管理	及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备

3.3.2 安全管理服务：机房运维管理

指标项	规格要求
机房运维管理	指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理
	建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理做出规定
	机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内
	不允许在重要区域接待来访人员、公开区域上没有包含敏感信息的纸档文件、移动介质等

3.3.3 安全管理服务：应急演练

指标项	规格要求
应急演练	制定云平台重要事件的应急预案，包括应急处理流程、系统恢复流程等内容;提出上云业务系统应急演练的指导方案，配合完成业务系统应急演练。
	从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障
	定期对系统相关的人员进行应急预案培训,并进行应急预案的演练；每年至少开展 1 次云平台应急演练。

3.3.4 安全技术服务：物理访问控制

指标项	规格要求
物理访问控制	机房出入口安排专人值守，控制、鉴别和记录进入的人员
	需进入机房的来访人员须经过申请和审批流程,并限制和监控其活动范围
	对机房划分区域进行管理,区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域
	重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员

3.3.5 安全技术服务：机房三防服务

指标项	规格要求
机房环境	机房具有防震、防风和防雨
	机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；
	机房应采取区域隔离防火措施，将重要设备与其他设备隔离开
	机房利用光、电等技术设置机房防盗报警系统

3.3.6 安全技术服务：设备访问审计

指标项	规格要求
运维审计	字符操作审计、图形操作审计、文件操作审计
访问控制	支持基于 IP/IP 段、用户/用户组、资产/资产组、协议、危险级别等组合策略进行访问控制，对于不合法的行为予以阻断；
	可基于运维账号的登陆时间和资产登陆时间进行访问控制；
	可基于运维操作命令进行访问控制；
	可基于主机、用户、IP 地址控制审计日志的访问权限；

3.3.7 安全技术服务：出口流量监测

指标项	规格要求
用户行为审计	支持基于 IP、端口等自定义协议服务；
	内置 URL 分类库，支持约 100 个 URL 分类，URL 库可在线升级
	支持自定义 URL 过滤，并支持 URL 的模糊匹配，提供 web 界面配置截图；
	支持自定义关键字对象，在应用控制的时候可选择“包含”、“不包含”、“等于”、“不等于”四种匹配模式，匹配类型包含关键字和数字，提供 web 界面配置截图；
	支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其 Top 流量用户

3.3.8 安全技术服务：本地 DDoS 防护

指标项	规格要求
引流方式	支持旁路（Offline）工作模式。当发生 DDoS 攻击时，清洗设备通过 BGP 路由宣告的方式将去往被保护目标的流量牵引导入到设备处理
流量清洗	实现对 Syn flood、ICMP flood、Ack flood、Syn+Ack Flood 、DNS query request flood、TCP 连接耗尽、HTTP Get Flood（含 CC）、UDP FLOOD 攻击、TCP FIN 攻击、TCP UDP 混合攻击等攻击流量的清洗
基本功能	支持流量过滤、反欺骗、异常流量识别、协议分析和速率限制功能，支持用户黑白名单功能，支持恶意流量识别和分离，保障正常访问流量的正常通过不受影响

流量回注	设备支持干净流量回注到业务系统中去

3.3.9 安全技术服务：防火墙安全防护

指标项	规格要求
攻击防范	ARP 欺骗攻击、TCP 报文标志位不合法攻击、Large ICMP 报文攻击、地址扫描攻击和端口扫描攻击等多种恶意攻击，同时支持黑名单、MAC 绑定、内容过滤等功能
NAT 支持	提供多对一、多对多、静态网段、双向转换 、Easy IP 和 DNS 映射等 NAT 应用方式;支持多种应用协议正确穿越 NAT，提供 DNS、FTP、H.323、NBT 等 NAT ALG 功能
增强状态安全过滤	实现基础、扩展和基于接口的状态检测包过滤技术；支持对每一个连接状态信息的维护监测并动态地过滤数据包，支持对应用层协议的状态监控

3.3.10 安全技术服务：防入侵监测 IPS

指标项	规格要求
入侵防御能力	具有流量模型自学习能力，当短时间内大规模爆发的病毒导致网络流量激增时，能自动发现并阻断攻击和异常流量，以保护路由器、交换机、VoIP 系统、DNS 服务器等网络基础设施免遭各种恶意攻击
零时差防护	同步全球知名安全组织和厂商发布的安全公告，能够及时更新特征库，以定期（每周）和紧急（当重大安全漏洞被发现）两种方式发布，并自动或手动地分发到 IPS 设备中

3.3.11 安全技术服务：远程接入服务

指标项	规格要求
操作审计	多面记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。
职权管控	通过账号管控和权限组管理，实现分职权进行人员和资产的管理。
安全认证	引入双因子认证机制，防止运维人员身份冒用和复用。

3.3.12 安全技术服务：租户隔离

指标项	规格要求
实现方式	应实现云计算环境业务网络的有效隔离，包括云服务客户使用的基础设施、云服务方的管理网络以及内部局域网。应制定各应用系统的访问控制策略并实时监控策略的有效性
VPC 资源池	部门业务区中，云服务方应为不同的云服务客户分配不同的 VPC，每个 VPC 之间不能直接进行通信，同时解决不同云服务客户间可能产生的地址重叠问题
安全防护	云服务方应具备为每个云服务客户提供独立安全服务的能力，其安全防护设备的安全策略应与云服务客户共享，应对安全策略实施的有效性进行监测和控制
权限	云服务客户拥有 VPC 内部信息系统和数据完整的使用权和管理权
部署模式	具备将 VPC 内部流量通过隧道等技术导出到物理或虚拟安全防护设备的能力

3.3.13 安全技术服务：租户内部访问控制

指标项	规格要求
租户内安全	以虚拟机为单位，为不同用户提供 2～7 层的安全防护
访问路径可定义	根据云租户的业务要求定义安全访问路径，实现租户内业务系统间的访问安全

3.3.14 安全技术服务：云主机监控

指标项	规格要求
监控内容	管理员可以监控云主机的运行状况，包括 CPU、内存、磁盘利用率以及网络流量等。
统计报表	支持输出云主机监控统计报表
监控告警	云主机资源告警项支持主机 CPU 利用率、内存利用率、磁盘分区利用率、网络流量告警设置

3.3.15 安全技术服务：角色权限管理

指标项	规格要求
权限分类	可以划分系统管理员、租户管理员、用户等多种用户权限类别

权限管理	上级管理员可以创建下级管理员以及下级用户，并可以对其权限进行设置
权限调整	上级管理员可以对下级管理员以及下级用户的权限进行调整
权限监督	系统管理员无权获取租户内的云主机操作系统管理权限，无权读取用户的业务数据
	管理员对于角色权限的操作要求能够被记录、监督

3.4 云管平台的兼容性要求

支持各类主流平台及数据库。

可管理主流的虚拟化软件，实现解耦，请具体描述所支持的虚拟化软件种类及支持程度。

可以兼容当前主流的具备可虚拟化功能的硬件设备，如防火墙、负载分担、网络安全设备、交换机等，并能够对特定主流品牌的相关设备进行虚拟化管理(提供虚拟化管理的支持设备清单和可支持程度的说明)。

4、 云平台业务连续性要求

构建云主机资源池的物理服务器可用性达到 99.99%以上（有人值守），云主机可用性 99.99%，当云主机发生故障时，支持宕机无感知迁移，保障承载业务的连续性。

数据存储：

支持用户数据按照设定的硬盘 Raid 保护、两副本、三副本进行冗余存储。任意 1 个节点上的主副本数据，其备副本数据会均匀分布在其他节点上，单点故障系统不会丢失数据。

Raid 保护和两副本场景下，在资源池内，出现一块磁盘故障，整个系统不会丢失数据，不影响业务正常使用，数据可靠性 99.99%。

三副本场景下，在资源池内，出现两块磁盘同时故障整个系统不会丢失数据，不影响业务正常使用，数据可靠性 99.9999%。

5、 云服务能力要求

5.1 云服务管理体系建设能力

云服务商可参考以下管理制度要求，在响应文件中制定云服务商管理制度体系，并按照云管理单位要求，在云安全监管单位的具体指导下，调整完善相关制度规范。

5.1.1 云服务商服务水平规范

云服务商服务水平规范应全面体现云服务商所提供的云服务能力，云服务商在与云使用单位签订服务协议时应遵守规范要求，如用户需求与规范不一致，应在服务协议中明确差异。云平台投入运行后，规范将在政务云网站发布公示。规范可参考如下要求：

1） 云平台整体服务能力

云服务介绍；各方权利义务、责任边界、服务规则（服务开通、费用、中止或终止）、第三方产品或服务、服务费抵扣索赔、服务级别协议排除项等

2） 云服务目录交付质量

应根据政务云服务目录内容给出量化指标，具体内容要求应包括但不限于：服务内容说明、服务水平级别目标（如可用性、响应能力、故障恢复能力、可审查性等）、服务交付物、服务变更流程、各方职责义务、补偿方式等。

5.1.2 运维管理规范

为了保障平台的服务质量，云服务商应基于 ITSS 运维管理最佳实践编制运维管理流程，规范包括但不限于：事件/故障管理流程、变更管理流程、资源管理流程、监控与告警管理流程、备份与恢复管理流程等。

5.1.3 应急响应规范

提出云平台应急制度、应急流程规范和云平台应急演练要求，并指导用户开展业务系统应急演练。

5.2 云平台运维整体要求

5.2.1 运维服务要求

云服务商应制定机房、人员、备份、安全、设备、介质、泄密事件等管理制度，覆盖事件/故障管理、变更管理、资源监控、安全事件处置、安全通告处置等全生命周期运维流程。

提供包含日常运维、重保运维、资源优化三个方面的驻场运维服务，主动提供日、周、月、应急、巡检、监控、值班、来访等多维度、各层级日志文档。须每周和每月提供政务云服务报告，其中周报主要报告主要云资源调整及使用情况，针对各信息系统云效率进行统计；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。

云服务商须根据项目要求安排具备相应资质和经验的专业人员从事本项目工作，确保项目实施队伍的稳定，提供本地化驻场服务，保证担任重要岗位的人员具备相应专业资质。任命 1 名项目经理作为政务云售前和售后的总接口人，常驻现场工作，定期向政务云管理单位汇报工作。

项目实施过程中，云服务商应保证关键岗位人员不能随意变更，如因正当理由需要调整项目主要人员的，应当提前 1 个月通知云管理单位，获得书面同意后方可更换。

云服务商应为西城区政务云单独配置驻场运维人员及专人值守，为最终用户提供技术服务热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法。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。

驻场日常运维：不少于 1 人负责云平台核心设备日志记录审查及运维人员操作记录审查等，定期提出安全审计报告。

提供每周 7*24 运维保障服务，定期报送运行报告，做好重大活动和节假日应急值守保障服务，确保各信息系统政务云环境可靠稳定运行。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。

5.2.2 应急保障要求

云服务商应制定自身云平台的应急安全保障策略，保障平台稳定运行。应提供高效的系统维护服务，有效防范系统风险，保证每周 7*24 小时电话畅通，发生故障应在 15 分钟内响应；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 1 小时内到达运维现场提供服务。系统发生宕机问题时，应在 30 分钟内响应，在 4 个小时之内使系统恢复正常。具备故障快速定位和恢复能力，故障定位排除时限不超过 30 分钟，重要信息系统故障定位排除时限不超过 10 分钟。故障处理完毕后提供相关系统宕机报告。

1) 提供定期的应急演练服务，通过定期开展应急演练，以检验应急方案的正确性，不断加强人员的应急安全意识和应急响应的熟练程度。

2) 提供应急响应服务和安全事件处置服务，针对云平台的网络、主机及应用系统，遭到黑客攻击或例外事故出现紧急情况时，应急工程师将在第一时间内赶赴现场协助解决问题，降低安全事件造成的损失，避免安全事件的扩大化。

3) 制定信息安全事件应急响应制度及规范，建立应急响应组织架构、信息安全事件定级表、上报流程、处置流程、处置预案、总结报告等。根据应急演练及应急响应优化应急预案体系知识库。

5.2.3 云服务水平能力要求

维护人员具备故障快速定位和恢复能力，故障定位排除时限不超过 30 分钟，重要业务系统故障定位排除时限不超过 10 分钟。

云服务商应提供包括邮件、电话、即时通讯工具等响应手段。

云服务商制定严格的日常巡检计划，定期对服务器、操作系统、云平台软件、存储、等设备进行巡检，巡检周期不可超过一周时间，巡检记录需要保存 1 年。平台相关设备的各级管理口令、密码，每半年一次周期性修改，口令的设置应符合密码复杂度要求。

云平台具备完备的安全防护体系和安全防护设备，具有成熟的安全运维方案，

应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，应能满足不低于网络安全等级保护（GB/T22239-2019）第三级和密码应用及评估要求，并积极配合采购人根据各业务系统具体等保需求，开展相应等保评估、检查、整改等工作。

6、 其他要求

6.1 服务团队要求

云服务商须根据项目要求安排具备相应资质和经验的专业人员从事本项目工作，确保项目实施队伍的稳定，保证担任重要岗位的人员具备相应专业资质。任命 1 名项目经理作为政务云售前和售后的总接口人，常驻现场工作，定期向政务云管理单位汇报工作。

运维保障人员除项目经理常驻现场（每周 5*8 小时）驻场工作外，还应派 2 名保障人员驻场工作（驻场指进驻西城区二龙路新机房）。即至少应提供 3 名人员每周 5*8 小时的驻场工作。10 人保障团队人员组成包括：项目经理，1 名；2 名驻场运维人员；2 名（含）以上二线专家（二线专家指：具有 3 年以上云服务工作经验且具备相关中级（含）以上技术职称的人员）；其它保障人员。另外，其它保障人员应在特殊时期重大活动保障活动中按采购人要求提供重保期间~~么~~每天 7*24 小时现场值守和远程技术支持保障服务。

项目实施过程中，云服务商应保证关键岗位人员（包含云平台厂商原厂驻场人员）不能随意变更，如因正当理由需要调整关键岗位人员，应当提前 1 个月通知云管理单位，获得书面同意后方可更换。

云服务商应为西城区政务云单独配置驻场运维人员，为最终用户提供技术服务热线，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法。

驻场日常运维：云计算平台应保证核心服务人员不少于 1 人，负责云平台核心设备日志记录审查及运维人员操作记录审查等，定期提出安全审计报告。

6.2 云监管平台接口和数据开放要求

云服务商应按照政务云管理单位提出的接口要求和接口标准，开放相应接口，在政务云管理单位需要时配合完成对接工作。云监管平台接口包括政务云运行状态、业务数据、安全审计、重大变更以及告警等安全监管所需信息，监管信息涵盖云计算平台、云服务客户和虚拟主机等监管对象。云备份接口包括政务云业务数据等备份所需信息，涵盖平台所需备份数据信息。

主要接口内容应至少包括：

- 运行状态类相关接口

对云计算平台运行时的状态参数进行持续监测，如云计算平台状态、客户服务状态以及虚拟机和虚拟网络状态等

- 业务服务类相关接口

获取西城区政务云业务服务相关数据，如入云业务系统、云平台资产、租用服务器等信息。

- 安全审计类相关接口

对云计算平台的安全审计日志进行收集，如云计算平台系统操作日志审计、客户业务操作日志审计等。

- 重大变更类相关接口

通过对云计算平台变更时的状态参数进行持续监测，如云计算平台内核、内存以及带宽等变更情况。

- 告警类相关接口

对政务云的告警相关数据进行持续监测，如安全事件告警、运行故障告警以及性能告警等。

云服务商应能够支持多种安全监管接口、备份接口技术要求，以提供相关安全监管数据。安全监管接口类型包括网络流量接口、网络协议接口、虚拟机接口和应用程序编程接口（API）等。

- 网络流量接口

对于物理网络应支持按需引流，云计算平台的物理交换机/路由器应支持将所有或部分指定的业务流量牵引到云安全监管服务商的设备，应至少支持端口镜像方式。

对于虚拟交换机和路由设备应支持将指定流量根据指定策略牵引到云安全监管服务商的设备。

- 网络协议接口

应开启服务器、网络设备、安全设备等的 Syslog 接口，通过网络将 Syslog 消息发送到指定 Syslog 接收服务器。

应开启设备的 SNMP 协议管理接口，对部分指定网络设备进行监管。

应分配合适的以太网接口，保证网络可达并能监测到监管云平台相关设备设施。

- 虚拟机接口

支持云计算平台上传虚拟机镜像并生成虚拟机实例。

- 应用程序编程接口（API）

支持“查询-响应”和“触发器”两种方式。通过“查询-响应”的方式向云服务商查询云计算平台各种属性，例如云计算平台状态、云客户配额、虚拟机状态等。“触发器”方式，由云安全监管服务商对外提供 API 服务接口，云服务商自身发生重大变更事件时“触发”上报机制。

6.3 运维知识库体系建设要求

云服务商需提供知识库工具作为日常运维管理工作中经验累积沉淀工具，运维人员可以通过知识库功能很方便地实现对于知识的新建、审批、分类、查询、统计、管理等操作。

6.4 保密要求

为确保电子政务系统和信息的安全保密，云服务商需分别与采购人以及相关运维人员签署保密协议。

6.5 培训要求

培训工作是云服务商提高运维能力和云服务水平的重要工作之一。云服务商应至少提供以下培训：

6.5.1 内部培训

内部培训旨在提高云平台运维能力，规范运维管理。内容包括但不限于：

（1）面向项目管理人员、系统管理人员的培训，确保此类人员能清晰地了解云平台的设计理念和设计方法，掌握云平台的整体结构，以及各类云资源的申请、审核、开通、回收等管理流程。

（2）面向系统维护人员的培训，确保此类人员能理解和掌握云平台的相关技术知识，能够熟练地维护云平台，快速定位和解决系统出现的问题，保证云平台服务期间正常运转，并持续提高运维服务质量。

（3）工作人员的安全培训教育，确保工作人员符合岗位要求。

（4）云平台维护人员的定期业务培训和保密培训，重保前的业务培训和应急保障培训等。

（5）面向政务云管理单位及云安全监管服务商的培训，确保此类人员充分了解云平台的技术架构、服务水平等。

6.5.2 外部培训

云服务商应根据本项目的特点制定培训方案并提供培训，负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表，培训课程涵盖政务云平台使用和管理培训，使政务云使用单位在培训后能够独立使用相关服务功能，而不必依赖云服务商现场指导。云服务商每年应组织安排至少一次针对云使用

单位的系统入云及用户培训，培训规模应至少 50 人次。云服务商应将所有培训费用（含培训教材费）及各项支出计入资源租赁费用中，不单独报价。内容包括但不限于：

（1）面向使用单位和开发人员的技术交流，包括云架构规划咨询、应用系统部署、迁移，云平台运维及其他技术服务。

（2）面向使用单位的培训，确保云平台最终用户能理解和掌握各类云服务的使用方法和操作技巧，能够高效、熟练地基于云平台部署上层业务应用，最终使政务云使用单位在培训后能够独立使用相关服务功能，而不必依赖云服务商现场指导。

（3）面向开发人员的培训，确保其能理解和掌握基于云平台的开发规范，针对具体的业务应用场景能够充分发挥云平台的技术优势，合理地设计上层业务应用的技术架构，制订部署、迁移方案，评估云资源的容量需求。

（4）定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；每年至少开展 1 次云平台应急演练。

云服务商应在此基础上制定具有本单位特色的政务云培训方案。

6.6 最高限价

6.6.1 本项目设定最高限价，即各投标人报价时不得超过下表中的最高限价。

编号	服务类别	服务子类	服务项	计价单位	最高限价
1001	计算服务	云主机服务（提供信创和非信创服务）	vCPU（主频不低于 2.4GHz）	1 vCPU	12 元/月
1002			内存	1 GB	20 元/月
1003		云基础计算服务：视频、图	GPU 显存不低于 8G	1GPU	50 元/月
			GPU 显存不低于 12G	1GPU	120 元/月

		形图像计算服务	GPU 显存不低于 16G	1GPU	300 元/月
			NPU 显存不低于	1NPU	3500 元/月
1004	存储服务	普通存储	普通存储(单盘技术指标:单盘 IOPS 1000-3000)	1 GB	0.3 元/月
1005		高性能存储	高性能存储(单盘技术指标:单盘 IOPS 3000-20000)	1 GB	0.6 元/月
1006	网络服务	主机负载均衡服务	主机负载均衡服务	1 IP	0 元/月
1007	云主机深度监控服务	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	1 主机	1000 元/月
1008	智能中枢平台服务	硬件算力服务，城市智能中枢-AI 运营管理中心、政务 AI 开发运营平台、算法场景优化服务等内容。	提供平台通用算法服务，包含：视频类、OCR 类、语音类、NLP 类等通用算法。	1 年	1000000 元/年
1009	商用密码安全	密码机	云密码机	1 系统	800 元/月
1010		身份鉴别	协同签名服务	1 系统	100 元/月

1011	共性服务		签名验签服务	1 系统	100 元/月
1013			动态令牌认证服务（OTP）	1 系统	200 元/月
1014		数据传输/存储机密性、完整性	数据加解密服务	1 系统	300 元/月
1015			数据库透明加密服务	1 系统	300 元/月
1018			文件加密服务	1 系统	300 元/月

6.6.2 投标人不得以各种形式给予赠品、回扣或者与采购无关的其他商品、服务，否则视为投标无效。

政务云服务目录分项报价表（单位：元）

1、政务云基础服务目录分项报价

编号	服务类别	服务子类	服务项	计价单位	报价单位	单价	数量	合计
1001	计算服务	云主机服务（提供信创和非信创服务）	vCPU（主频不低于 2.2GHz）	1 vCPU	元/月		15000	
1002			内存	1 GB	元/月		26600	
1003		图形图像计算服务	GPU（显存不低于 8G，最大单精度浮点计算能力不低于 0.15TFLOPS）	1GPU	元/月		10	

1004			GPU（显存不低于 12G，最大单精度浮点计算能力不低于 5TFLOPS）	1GPU	元/月		10	
1005			GPU（显存不低于 16G，最大单精度浮点计算能力不低于 7TFLOPS，最大双精度浮点计算能力 0.2TFLOPS）	1GPU	元/月		10	
			NPU 内存≥ 24GB，最大单精度浮点计算能力不低于 7TFLOPS	1NPU	元/月		8	
1006	存储服务	普通性能存储	普通存储(单盘技术指标:单盘 IOPS 1000-3000 ）	1 GB	元/月		940000	
1007		高性能存储	高性能存储(单盘技术指标:单盘 IOPS 3000-20000 ）	1 GB	元/月		120000	
1008		视频云存储	满足海量视频数据的存储需求	1 TB	元/月		100	
1009	网络服务	主机负载均衡服务	为大型业务系统提供负载均衡服务	1 IP	元/月	/	50	/

1010		远程接入服务	每个账号结合身份验证通过VPN远程接入堡垒机进行维护	1账号	元/月		30	
1011		VPN服务	SSL VPN接入	1套	元/月		50	
			IPSec VPN接入	1Mb带宽	元/月	/	0	/
1012		SSL 证书服务	提供SSL 证书服务	1 域名	元/月	/	0	/
1013		WAF防护	web应用防火墙服务	1 IP（互联网）	元/月		20	
1014		互联网链路租用服务	互联网带宽	1 Gb（流量）	元/月		1	
1015	设备访问审计服务	访问审计服务	设备访问记录、日志统计、安全事件（云平台自带提供）	1帐户	元/月	/	100	/
1016	租户隔离	租户隔离	租户虚拟化层隔离（云平台自带提供）	1帐户	元/月	/	1000	/
1017	租户内部访问控制	内部访问控制	租户内部访问权限控制（云平台自带提供）	1个	元/月	/	1000	/
1018	云主机监控	云主机监控	提供云上资源的基本监控，包括CPU、内存使用率等（云平台自带提供）	1 账户	元/月	/	1000	/

1019	角色权限管理	云租户角色权限管理	提供通过代入角色实现获取操作权限（云平台自带提供）	1 帐户	元/月	/	1000	/
1020	云主机深度监控服务	特定云主机深度监控及运维保障服务（每周 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	1 系统	元/月		200	
以上分项报价总金额： 人民币：_____元（大写人民币：_____元）								

2、政务云扩展服务目录分项报价

编号	服务类别	服务子类	服务项	计价单位	报价单位	单价	数量	合计
2001	迁移服务、安全服务	云主机迁移 物理主机迁移	应用系统虚机至虚机迁移服务	1 个	个/系统		50	
2002								
2003		云端抗 DDOS 服务	云端抗 DDOS 服务	1 站点	元/月		10	
2004		云端 APT 防护服务	云端 APT 防护服务	1 系统	元/月		100	
2005		主机杀毒服务	主机杀毒服务	1 系统	元/月		260	
2006		主机防护	主机防护	1 系统	元/月		260	
2007		主机安全	主机安全	1 系统	元/次		80	

		加固	加固					
2008		虚拟防火墙	提供虚拟化防火墙安全能力	1 系统	元/月		10	
2009		虚拟 WAF	提供虚拟化 web 应用安全防护能力	1 域名	元/月		10	
2010		网页防篡改服务	网页防篡改服务	1 系统	元/月		1	
2011	其他服务	云安全检测监测和审计服务	提供主机漏洞扫描；主机日志分析审计服务；数据库审计服务；云网络安全等审计服务；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。	1 系统	元/月		80	

2012		密码机	云密码机	1 系统	元/月		10	
2013		身份鉴别	协同签名服务	1 系统	元/月		1	
2014			签名验签服务	1 系统	元/月		1	
2015			动态令牌认证服务（OTP）	1 系统	元/月		1	
2016		数据传输/存储机密性、完整性	数据加解密服务	1 系统	元/月		1	
2017			数据库透明加密服务	1 系统	元/月		1	
2018			文件加密服务	1 系统	元/月		1	
2019		智能外呼	交互式语音应答	每 IP（并发）	个/月		30	
2020		CDN 加速	CDN 加速	1 GB（流量）	元/月	/	50	/
2021		智能中枢平台服务	硬件算力服务，城市智能中枢-AI 运营管理中心、政务 AI 开发运	1	年		1	

			营平台、算法场景优化服务等内容。					
以上分项报价总金额： 人民币：_____元（大写人民币：_____元）								

3、第三方平台接口升级开发费用报价

第三方平台对接标准开发集成等费用报价：人民币：_____元（大写人民币：_____元）

注明：以上分项报价相加总金额为该项目投标报价总金额（价格分计算报价）。